

System Center 2012   
Process Pack for IT GRC  
Evaluation and Deployment Guide

Microsoft Corporation

Published: April 2012

Applies To

Process Pack for IT GRC and   
Service Manager 2012

Feedback

Send suggestions and comments about this document to [secwish@microsoft.com](mailto:secwish@microsoft.com?subject=System%20Center%20Service%20Manager%202012%20-%20Process%20Pack%20for%20IT%20GRC%20Evaluation%20and%20Deployment%20Guide%20feedback).

**IMPORTANT INFORMATION**: The *Microsoft System Center Process Pack for IT GRC* (“Process Pack for IT GRC”) is designed to facilitate compliance activities conducted by your organization’s IT experts, auditors, accountants, attorneys and other compliance professionals. The software does not replace those professionals. The Process Pack for IT GRC includes some control objectives and authority document citations plus libraries with some control activities and associated product value settings. These objectives, citations, controls and settings do not verify or guarantee fulfillment of your organization’s compliance obligations. It is the responsibility of your organization to choose the objectives, citations, controls and settings to use, modify, add or remove based on guidance from your organization’s compliance professionals. Reports and any other information provided by or generated from the software do not constitute professional compliance advice. You must consult compliance professionals to confirm compliance with specific governance, risk and compliance authority documents.

This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious.  No real association or connection is intended or should be 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. You may modify this document for your internal, reference purposes.

© 2012 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Excel, SQL Server, Visual Studio, Windows, and Windows Server are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Revision History

| **Release Date** | **Changes** |
| --- | --- |
| November 2011 | System Center 2012 Beta |
| April 2012 | System Center 2012 RTM |

Contents

[Using the Process Pack for IT GRC 1](#_Toc317173656)

[How to Use This Guide 1](#_Toc317173657)

[GRC Program and Compliance Overview 3](#_Toc317173658)

[Style Conventions 3](#_Toc317173659)

[Intended Audience 4](#_Toc317173660)

[Evaluation Guide Sample Company Information 5](#_Toc317173661)

[Task 1: Prepare the Prerequisite Infrastructure 7](#_Toc317173662)

[Step 1-1: Install Windows Server and System Center Products 8](#_Toc317173663)

[Step 1-2: Configure System Center Products Integration 9](#_Toc317173664)

[Task 2: Install Process Pack for IT GRC and Supporting Components 10](#_Toc317173665)

[Step 2-1: Install the Process Pack for IT GRC 10](#_Toc317173666)

[Step 2-2: Import Process Pack for IT GRC Reporting Components 13](#_Toc317173667)

[Start Synchronization with the Data Warehouse 13](#_Toc317173668)

[Verify the Installation of the Process Pack for IT GRC 14](#_Toc317173669)

[Verify the Installation of the Process Pack for IT GRC Cubes 15](#_Toc317173670)

[Verify the Installation of the Process Pack for IT GRC Reports 15](#_Toc317173671)

[Step 2-3: Configure Configuration Manager Connector for Compliance Test Automation 18](#_Toc317173672)

[Step 2-4: Install Compliance Libraries 20](#_Toc317173673)

[Step 2-5: Install DCM Configuration Items and Baselines 22](#_Toc317173674)

[Install Security Compliance Manager 23](#_Toc317173675)

[Export the Compliance Baselines to a DCM Pack 24](#_Toc317173676)

[Import the DCM Pack into Configuration Manager 2012 25](#_Toc317173677)

[Configure the Configuration Items 27](#_Toc317173678)

[Configure the Configuration Baselines 28](#_Toc317173679)

[Create Device Collections for Targeting Configuration Baselines 29](#_Toc317173680)

[Deploy the Configuration Baselines 31](#_Toc317173681)

[Step 2-6: Install the Process Pack for IT GRC Client Prerequisites 32](#_Toc317173682)

[Step 2-7: Install the Process Pack for IT GRC Client 34](#_Toc317173683)

[Task 3: Implement an IT GRC Management Program 37](#_Toc317173684)

[Step 3-1: Create an IT GRC management program 37](#_Toc317173685)

[Step 3-2: Add a Scope to the Program 39](#_Toc317173686)

[Step 3-3: Create Authority Documents, Control Objectives, and Control Activities for the Program 40](#_Toc317173687)

[Step 3-4: Customize an Automated Control Activity 42](#_Toc317173688)

[Step 3-5: Create a Manual Control Activity 45](#_Toc317173689)

[Step 3-6: Add the Manual Control Activity to a Control Objective 47](#_Toc317173690)

[Step 3-7: Publish the IT GRC Management Program 49](#_Toc317173691)

[Task 4: Administer an IT GRC management program 51](#_Toc317173692)

[Step 4-1: Configure Process Pack for IT GRC User Roles 51](#_Toc317173693)

[Step 4-2: Manage IT GRC Programs Using the Process Pack for IT GRC Client 55](#_Toc317173694)

[Step 4-3: Add Tests Results to a Manual Control Activity 57](#_Toc317173695)

[Step 4-4: Verify Compliance Status Using Configuration Manager Reports 58](#_Toc317173696)

[Step 4-5: Request an IT GRC Management Program Exception 60](#_Toc317173697)

[Step 4-6: Verify Compliance Status Using Process Pack for IT GRC Reports 63](#_Toc317173698)

[Appendix A: Compliance and GRC Program Overview 65](#_Toc317173699)

[Governance in the GRC Process 65](#_Toc317173700)

[Risk Management in the GRC Process 65](#_Toc317173701)

[Compliance in the GRC Process 67](#_Toc317173702)

[A GRC Example: Protecting Building Access 67](#_Toc317173703)

[Process Pack for IT GRC Terms and Concepts 68](#_Toc317173704)

[Process Pack for IT GRC Description 71](#_Toc317173705)

[Roles within an IT GRC Program 73](#_Toc317173706)

[Appendix B: Prepare SM-2012-01 Computer 77](#_Toc317173707)

[Step B-1: Review System Prerequisites 77](#_Toc317173708)

[Step B-2: Install Windows Server 2008 R2 78](#_Toc317173709)

[Step B-3: Install the AD DS Server Role 79](#_Toc317173710)

[Step B-4: Install the Web Services (IIS) Server Role 79](#_Toc317173711)

[Step B-5: Add the Required Windows Server 2008 R2 Features 81](#_Toc317173712)

[Step B-6: Create the Required User and Service Accounts 81](#_Toc317173713)

[Step B-7: Install SQL Server 2008 R2 85](#_Toc317173714)

[Step B-8: Install Service Manager 2012 88](#_Toc317173715)

[Step B-9: Install Microsoft Office Excel 2010 91](#_Toc317173716)

[Appendix C: Prepare SM-2012-02 Computer 93](#_Toc317173717)

[Step C-1: Review System Prerequisites 93](#_Toc317173718)

[Step C-2: Install Windows Server 2008 R2 94](#_Toc317173719)

[Step C-3: Install the Web Services (IIS) Server Role 94](#_Toc317173720)

[Step C-4: Add the Required Windows Server 2008 R2 Features 96](#_Toc317173721)

[Step C-5: Create the Required User and Service Accounts 96](#_Toc317173722)

[Step C-6: Install SQL Server 2008 R2 99](#_Toc317173723)

[Step C-7: Install Service Manager 2012 Data Warehouse Server 105](#_Toc317173724)

[Appendix D: Prepare CM-2012-01 Computer 111](#_Toc317173725)

[Step D-1: Review System Prerequisites 111](#_Toc317173726)

[Step D-2: Install Windows Server 2008 R2 112](#_Toc317173727)

[Step D-3: Install the Web Services (IIS) Server Role 113](#_Toc317173728)

[Step D-4: Add the Required Windows Server 2008 R2 Features 115](#_Toc317173729)

[Step D-5: Create the Required User and Service Accounts 115](#_Toc317173730)

[Step D-6: Install SQL Server 2008 R2 116](#_Toc317173731)

[Step D-7: Add the Site Server to the Local Administrators Security Group 120](#_Toc317173732)

[Step D-8: Install Configuration Manager 2012 121](#_Toc317173733)

[Step D-9: Configure the Network Access Account 123](#_Toc317173734)

[Step D-10: Configure the Configuration Manager Site Boundaries and Boundary Groups 124](#_Toc317173735)

[Step D-11: Configure the Publishing of Site Information in AD DS and DNS 126](#_Toc317173736)

[Step D-12: Add the Reporting Services Point Site System Role 126](#_Toc317173737)

[Step D-13: Configure the Compliance Evaluation Schedule 128](#_Toc317173738)

[Appendix E: Prepare OM-2012-01 Computer 131](#_Toc317173739)

[Step E-1: Review System Prerequisites 131](#_Toc317173740)

[Step E-2: Install Windows Server 2008 R2 132](#_Toc317173741)

[Step E-3: Install the Web Services (IIS) Server Role 132](#_Toc317173742)

[Step E-4: Add the Required Windows Server 2008 R2 Features 134](#_Toc317173743)

[Step E-5: Register .NET Framework with IIS 135](#_Toc317173744)

[Step E-6: Configure ISAPI and CGI Restrictions 135](#_Toc317173745)

[Step E-7: Create the Required User and Service Accounts 136](#_Toc317173746)

[Step E-8: Install SQL Server 2008 R2 137](#_Toc317173747)

[Step E-9: Install Operations Manager 2012 143](#_Toc317173748)

[Appendix F: Prepare WIN-2008R2-01 Computer 147](#_Toc317173749)

[Step F-1: Review System Prerequisites 147](#_Toc317173750)

[Step F-2: Install Windows Server 2008 R2 147](#_Toc317173751)

[Appendix G: Configure System Center Product Integration 149](#_Toc317173752)

[Step G-1: Register the Service Manager Data Warehouse 149](#_Toc317173753)

[Step G-2: Deploy Operations Manager Agents 152](#_Toc317173754)

[Step G-3: Deploy Configuration Manager Clients 160](#_Toc317173755)

[Step G-4: Configure Active Directory Connector in Service Manager 168](#_Toc317173756)

[Step G-5: Configure Operations Manager CI Connector in Service Manager 170](#_Toc317173757)

[Step G-6: Configure Configuration Manager Connector in Service Manager 173](#_Toc317173758)

[Step G-7: Verify Population of Service Manager CMDB 176](#_Toc317173759)

[Appendix H: Uninstall the Process Pack for IT GRC and Client 178](#_Toc317173760)

[Step H-1: Uninstall the Process Pack for IT GRC 178](#_Toc317173761)

[Step H-2: Uninstall the Process Pack for IT GRC Client 179](#_Toc317173762)

[Appendix I: Troubleshoot, Resolve, and Recover from Installation Issues 180](#_Toc317173763)

[Upgrading the Process Pack for IT GRC Server 180](#_Toc317173764)

[Failure during the Prerequisite Check 180](#_Toc317173765)

[Failure during Predicted Checks 181](#_Toc317173766)

[Failure Occurs in an Unpredictable Manner before Making Permanent Changes to the Management Server 181](#_Toc317173767)

[Failure Occurs in an Unpredictable Manner after Making Permanent Changes to the Management Server 182](#_Toc317173768)

[Failure Occurs in an Unpredictable Manner after Making Permanent Changes to the Database 182](#_Toc317173769)

[Troubleshooting Process Pack for IT GRC Server Installation Failures 182](#_Toc317173770)

[New installation failure 182](#_Toc317173771)

[Upgrade installation failure 183](#_Toc317173772)

[Uninstallation failure 183](#_Toc317173773)

[Upgrading the Process Pack for IT GRC Client 183](#_Toc317173774)

[Failure during Prerequisite Check 183](#_Toc317173775)

[Failure Occurs in an Unpredictable Manner before Making Permanent Changes to the Process Pack for IT GRC Client 184](#_Toc317173776)

[Failure Occurs in an Unpredictable Manner after Making Permanent Changes to the Process Pack for IT GRC Client 184](#_Toc317173777)

[Troubleshooting Client Installation Errors 185](#_Toc317173778)

[Installation failure 185](#_Toc317173779)

# Using the Process Pack for IT GRC

This *Evaluation and Deployment Guide* describes how you can use the Process Pack for IT GRC to help manage IT governance, risk management, and compliance (GRC) efforts in your organization. A process pack is a management pack for Microsoft® System Center 2012 - Service Manager that helps manage IT processes based on industry standards and best practices, such as Microsoft Operations Framework (MOF) and Information Technology Infrastructure Library (ITIL). The Process Pack for IT GRC helps provide automated compliance management for client and server computers.

Compliance affects many organizations, both large and small. Regulatory requirements are a major driver for compliance. These requirements come from organizations such as the Security and Exchange Commission (SEC) and the New York Stock Exchange (NYSE), from legislation such as Sarbanes-Oxley (SOX) and also from industry standards such as Payment Card Industry (PCI). However, even organizations that are not affected by regulatory requirements need to achieve compliance with their own organizational policies. Problems often arise when organizations initiate a compliance program because they may not be certain where to begin or how to automate the program using technology.

The Process Pack for IT GRC addresses this challenge through the use of compliance libraries. Compliance libraries provide controls that are used to help achieve compliance with IT GRC authority document citations that are maintained by international, government, or industry authorities. Other management packs are available from the [Microsoft System Center Marketplace](http://go.microsoft.com/fwlink/?LinkId=82105) that contain control activities and automation needed to take advantage of how System Center Service Manager integrates with System Center Configuration Manager and System Center Operations Manager to monitor, validate, and report on the compliance state of deployed Microsoft products. Together, these solutions help customers understand and bind complex business objectives to their infrastructures.

## How to Use This Guide

This guide provides a step-by-step process for evaluating the features and capabilities of the Process Pack for IT GRC in your test environment. Follow the guidance to see how the Process Pack for IT GRC works with System Center 2012 – Service Manager 2012, Configuration Manager, Operations Manager, Active Directory® Domain Services, and Windows Server® 2008 R2 to help you manage IT GRC compliance in your organization.

The guide is written in a sequential manner; start with the first section and then proceed forward to the completion of the guide. Additional resources to help you perform the processes in this guide are available in the appendices.

## GRC Program and Compliance Overview

Prior to evaluating the Process Pack for IT GRC in your environment, review the information in [Appendix A: Compliance and GRC Program Overview](#_Appendix_A:_Compliance_1) to help ensure you get the most out of your evaluation process. Having a good comprehension of GRC processes, GRC terms, GRC terminology, and GRC roles will help your evaluation and your ability to apply IT GRC programs within your organization.

## Style Conventions

This guidance uses the style conventions that are described in the following table.

| Element | Meaning |
| --- | --- |
| Bold font | Signifies characters typed exactly as shown, including commands, switches, and file names. User interface elements also appear in bold. |
| *Italic font* | Titles of books and other substantial publications appear in italic. |
| *<Italic>* | Placeholders set in italic and angle brackets *<Italic>* represent variables. |
| Monospace font | Defines code and script samples. |
| Note | Alerts the reader to supplementary information. |
| Important | Alerts the reader to essential supplementary information. |

## Intended Audience

This guidance is intended for individuals who are assigned the following tasks and responsibilities:

* Install, configure, and manage the Process Pack for IT GRC and related infrastructure. These individuals will install the Process Pack for IT GRC, install the IT Compliance Management Libraries, manage system-wide configuration settings, and install the prerequisite infrastructure components, including System Center Service Manager, System Center Configuration Manager, and Active Directory Domain Services (AD DS). Individuals who perform these tasks require the following user roles and permissions:
* Member of the local Administrators group on the computer running System Center Service Manager.
* Assigned the Administrator user role in System Center Service Manager.
* Member of the local Administrators group on the computer running System Center Configuration Manager.
* Assigned the Administrator user role in System Center Configuration Manager.
* Member of the Domain Admins security group in AD DS.
* Implement and manage IT GRC compliance programs. These individuals will create and manage the IT GRC program within their organizations, work with internal and external auditors to define programs and expectations, ensure the correct compliance controls and control activities are included in the compliance program, manage pre-audit and audit activities, and assign compliance-related tasks to users in the form of work items and IT GRC incident tickets. Individuals who perform these tasks require the following user roles and permissions:
* Member of the Compliance Program Manager user role in System Center Service Manager.
* Configure computers and assess IT GRC compliance. These individuals will configure the managed computers for compliance and collect the compliance results for IT GRC programs using automated and manual methods. Individuals who perform these tasks require the following user roles and permissions:
* Member of the Compliance Program Implementer user role in System Center Service Manager.
* Have sufficient permissions and privileges on the managed computers to configure the managed computers for compliance.
* Have sufficient permissions and privileges on the managed computers to collect the compliance results from the managed computers.

# Evaluation Guide Sample Company Information

Contoso, Ltd is a publicly traded company that processes credit card transactions through its e-commerce website. The Contoso e-commerce site handles transactions from all over the world.

Because the e-commerce website processes credit card transactions, it is regulated by Payment Card Industry (PCI) standards and is required to have a compliance program in place. PCI reports are transmitted to various credit card companies. In addition, PCI specialist auditors perform an annual review and produce the credit card compliance reports to the credit card companies and Contoso.

To help manage IT GRC compliance with the PCI standards, Contoso has decided to deploy the Process Pack for IT GRC for Service Manager 2012. This guide shows how Contoso created a proof-of-concept environment as part of their evaluation process.

# Task 1: Prepare the Prerequisite Infrastructure

The Process Pack for IT GRC evaluation environment described in this guide includes the computers illustrated in the following figure. The following figure also includes a high-level description of the Windows® operating systems, System Center products, and system resources for each computer.

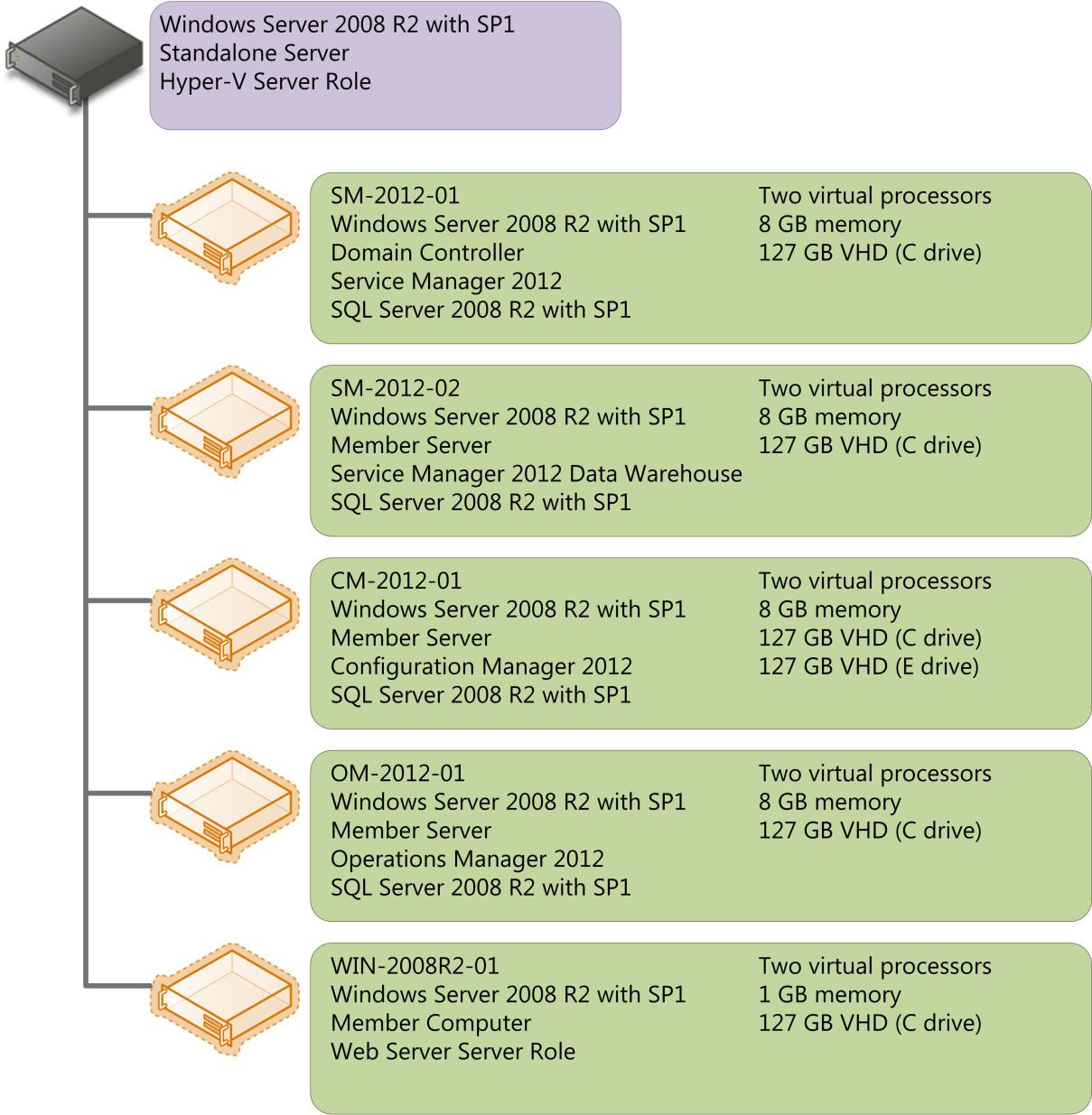
Note

The following figure shows the evaluation environment using virtual machines. However, you can also use physical computers to evaluate the Process Pack for IT GRC.

The example in this guide focuses on managing a computer running Windows Server 2008 R2. However, you can also use the Process Pack for IT GRC to help manage computers running other Windows operating systems, such as Windows 7 or Windows Server 2008. In addition, compliance test automation is also supported using Configuration Manager 2007 R2.

Note

In scenarios in which the RTW version of the Process Pack for IT GRC was previously installed, an **Upgrade Installation** should be performed. See “Appendix I: Troubleshoot, Resolve, and Recover from Installation Issues” later in this guide for more information.



To create the Process Pack for IT GRC evaluation environment, complete the following steps:

[Step 1-1: Install Windows and System Center Products](#_Install_Windows_and)

[Step 1-2: Configure System Center Products Integration](#_Step_1-2:_Configure)

## Step 1-1: Install Windows Server and System Center Products

The first step in creating the evaluation environment is to install Windows Server 2008 R2 with SP1 and the System Center products used in the evaluation environment.

Install Windows Server and the System Center products by completing the following procedures:

1. Prepare the computer running the domain controller and Service Manager 2012 management server as described in [Appendix B: Prepare the SM-2012-01 Computer](#_Appendix_B:_Prepare_2).
2. Prepare the computer running the Service Manager 2012 data warehouse management server (SM-2012-02) as described in [Appendix C: Prepare the SM-2012-02 Computer](#_Appendix_C:_Prepare_1).
3. Prepare the computer running the Configuration Manager 2012 primary site server (CM-2012-01) as described in [Appendix D: Prepare the CM-2012-01 Computer](#_Appendix_D:_Prepare_1).
4. Prepare the computer running the Operations Manager 2012 management server (OM-2012-01) as described in [Appendix E: Prepare the OM-2012-01 Computer](#_Appendix_E:_Prepare_1).
5. Prepare the computer running Windows Server 2008 R2 (WIN-2008R2-01) as described in [Appendix F: Prepare the WIN-2008R2-01 Computer](#_Appendix_F:_Prepare_1).

## Step 1-2: Configure System Center Products Integration

After Windows Server 2008 R2 with SP1 and the System Center products are deployed, configure the System Center product integration. This integration allows Service Manager to receive information from other System Center products. To use the Compliance Test Automation features of the Process Pack for IT GRC, information for all configuration items must exist in the Service Manager CMDB. Although there are several methods that can be used, the preferred method of populating the Service Manager CMDB is to use the Operations Manager CI connector, Active Directory® Domain Services (AD DS) connector, and Configuration Manager connector.

Configure the System Center product integration by performing the following procedures as described in [Appendix G: Configure System Center Product Integration](#_Appendix_G:_Configure):

[Step G-1: Register the Service Manager Data Warehouse](#_Step_H-1:_Register)

[Step G-2: Deploy Operations Manager Agents](#_Step_H-2:_Deploy)

[Step G-3: Deploy Configuration Manager Clients](#_Step_H-3:_Deploy)

[Step G-4: Configure Active Directory Connector in Service Manager](#_Step_H-4:_Configure)

[Step G-5: Configure Operations Manager CI Connector in Service Manager](#_Step_H-5:_Configure)

[Step G-6: Configure Configuration Manager Connector in Service Manager](#_Step_H-6:_Configure)

[Step G-7: Verify Population of Service Manager CMDB](#_Step_H-7:_Verify)

# Task 2: Install Process Pack for IT GRC and Supporting Components

After the System Center integration is configured and verified, install the Process Pack for IT GRC and supporting components. The supporting components include additional management packs, configuration packs, and the Process Pack for IT GRC Client.

Install the Process Pack for IT GRC and supporting components by completing the following steps:

[Step 2-1: Install the Process Pack for IT GRC](#_Step_2-1:_Install)

[Step 2-2: Import Process Pack for IT GRC Reporting Components](#_Step_2-2:_Import)

[Step 2-3: Configure Configuration Manager Connector for Compliance Test Automation](#_Step_2-3:_Configure)

[Step 2-4: Install IT Compliance Management Libraries](#_Step_2-4:_Install_1)

[Step 2-5: Install DCM Configuration Items and Baselines](#_Step_2-5:_Install)

[Step 2-6: Install the Process Pack for IT GRC Client Prerequisites](#_Step_2-6:_Install)

[Step 2-7: Install the Process Pack for IT GRC Client](#_Step_2-7:_Install)

## Step 2-1: Install the Process Pack for IT GRC

After the Service Manager management server (SM-2012-01) and the Service Manager data warehouse (SM-2012-02) are installed, install the Process Pack for IT GRC on the Service Manager management server. The Process Pack for IT GRC automatically creates the necessary folders in Service Manager 2012 for managing IT GRC control and risk programs, which are displayed in the Service Manager console. The installation process also creates cubes and reports, which are used to view compliance information about IT GRC programs, control objectives, and control activities.

 To install the Process Pack for IT GRC

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. In Windows Explorer, go to target\_folder, and then double-click Setup (where target\_folder is the folder where the Process Pack for IT GRC is extracted.)

The Process Pack for IT GRC Setup Wizard splash screen is displayed.

1. In the Process Pack for IT GRC Setup Wizard splash screen, click the Install GRC Process Pack 2012 link.

The Process Pack for IT GRC Setup Wizard starts.

1. Install the Process Pack for IT GRC using the Process Pack for IT GRC Setup Wizard and the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Product registration | 1. In Name, type Contoso IT. 2. In Organization, type Contoso LTD. 3. Select the I have read, understood, and agreed with the terms of the license agreement check box. 4. Click Next. |
| Configure Account for Data warehouse deployment | 1. In Data Warehouse management server, type SM‑2012‑02. 2. In User name, type Administrator. 3. In Password, type P@ssw0rd. 4. In Domain, select CORP. 5. Click Test Credentials.   A status message appears indicating that the credentials are accepted.   1. Click Next. |
| Installation summary | 1. Review the configuration options selected while completing the wizard. 2. Click Install. |
| Process Pack for IT GRC | The progress for installing the Process Pack for IT GRC is displayed. |
| Finished | Click Close. |

The IT GRC Knowledge Importer Wizard starts.

1. Complete the IT GRC Knowledge Importer Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Locate Knowledge Libraries | 1. Click Search automatically for latest management packs online. 2. Click Next. |
| Import Knowledge Libraries | 1. Progress bar displays the progress of downloading the Knowledge Libraries. 2. In Select the Knowledge Libraries that you would like to import, select Microsoft.ControlActivity. Win7.Library.v2.Updates. 3. Click Import.   The import process starts. |
| Completion | Click Close. |

1. Close all open windows and dialog boxes.

## Step 2-2: Import Process Pack for IT GRC Reporting Components

The Process Pack for IT GRC Setup Wizard installs the process pack into the computer running the Service Manager 2012 management server (SM-2012-01). In addition, the Process Pack for IT GRC reporting components need to be imported into the Service Manager 2012 data warehouse management server (SM-2012-02).

The Process Pack for IT GRC Setup Wizard suspends the ETL DW jobs as part of the installation process. This job and other data warehouse jobs need to be resumed for the Process Pack for IT GRC reporting components to be imported into the data warehouse management server (SM-2012-02).

Import the Process Pack for IT GRC reporting components by completing the following procedures:

1. [Start Synchronization with the Data Warehouse](#_Start_Synchronization_with)
2. [Verify the Installation of the Process Pack for IT GRC](#_Restart_Service_Manager)
3. [Verify the Installation of the Process Pack for IT GRC Cubes](#_Verify_the_Installation_1)
4. [Verify the Installation of the Process Pack for IT GRC Reports](#_Verify_the_Installation)

### Start Synchronization with the Data Warehouse

 To start synchronization of the Process Pack for IT GRC with the data warehouse

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the navigation pane, click **Data Warehouse**.
2. In the **Data Warehouse** pane, go to Data Warehouse/Data Warehouse Jobs.
3. In the results pane, click **MPSyncJob**.
4. In the **Tasks** pane, under MPSyncJob, click **Resume**.
5. In the **Tasks** pane, under Data Warehouse Jobs, click **Refresh**.

The status of the MPSyncJob job should change to Running.

1. In the Tasks pane, periodically click Refresh until the status of the MPSyncJob changes to Not Started.

Note

This process can take more than an hour to complete.

1. Close all open windows and dialog boxes.

### Verify the Installation of the Process Pack for IT GRC

 To verify the installation of the Process Pack for IT GRC

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the navigation pane, ensure the **Compliance and Risk Items** button appears.
2. In the navigation pane, click **Compliance and Risk Items**.

The following Process Pack for IT GRC top-level folders should be listed in the results pane:

* Authority Documents
* Control Management
* Exception Management
* Program Management
* Risk Management

1. Close all open windows and dialog boxes.

### Verify the Installation of the Process Pack for IT GRC Cubes

 To verify the installation of the Process Pack for IT GRC cubes

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the navigation pane, click **Data Warehouse**.
2. In the **Data Warehouse** pane, go to Data Warehouse/Cubes.

The following items should be listed in the results pane:

* Software Update Cube
* Service Manager WorkItems Cube
* Service Manager Compliance Result Cube
* Service Manager Compliance Program Detail Cube
* Service Manager ConfigItem Cube
* Power Management Cube
* Change and Activity Management Cube
* Service Manager Service Catalog Library Cubes

1. Close all open windows and dialog boxes.

### Verify the Installation of the Process Pack for IT GRC Reports

 To verify the installation of the Process Pack for IT GRC reports

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the navigation pane, click **Reports**.
2. In the **Reporting** pane, go to Reports/Compliance Reports Library/Control Management.

The following reports should be listed in the results pane:

* Control Activity Details Report
* Control Activity List Report
* Control Activity Score Report
* Control Management Change Report
* Control Objective Details Report
* Control Objective Health Report
* Control Objective List Report
* Control Objective Progress Report
* Managed Entity Result List Report

1. In the **Reporting** pane, go to Reports/Compliance Reports Library/Program Management.

The following reports should be listed in the results pane:

* Program Detail Report
* Program Health Dashboard Report
* Program Incidents List Report
* Program List Report
* Program Non-Compliance Report
* Program Readiness Review Status Report
* Program Scope Report

1. In the **Reporting** pane, go to Reports/Compliance Reports Library/Risk Management.

The following reports should be listed in the results pane:

* Inherent Risk Map
* Program Risk Report
* Residual Risk Map
* Risk Details
* Risk List by Rank Report
* Risk List Report

1. Close all open windows and dialog boxes

If the reports do not display, the problem may be that the computer running the Data Warehouse for System Center Service Manager has not processed the reports in the Process Pack for IT GRC by running the **MPSyncJob** Data Warehouse Job. By default, the **MPSyncJob** Data Warehouse Job runs once each hour. You can manually run the **MPSyncJob** Data Warehouse Job and cause the reports to appear sooner by performing the following steps:

1. In the navigation pane, click **Data Warehouse**.
2. In the **Data Warehouse** pane, go to Data Warehouse/Data Warehouse Jobs.
3. In the results pane, click **MPSyncJob**.
4. In the **Tasks** pane, click **Resume**.
5. In the **Tasks** pane, click **Refresh**.

The status of the MPSyncJob should change to Running.

1. In the **Tasks** pane, periodically click **Refresh** until the status of the MPSyncJob changes to **Not Started**.
2. Review the list of reports in the Control Management, Program Management, and Risk Management folders in the Reports pane.
3. Repeat steps 2 through 7 until the reports appear.
4. Close all open windows and dialog boxes.

For more information about troubleshooting report installation, see [Deployment Scenarios for System Center 2012 Service Manager](http://technet.microsoft.com/en-us/library/hh519675.aspx) in the System Center 2012 – Service Manager Deployment Guide.

## Step 2-3: Configure Configuration Manager Connector for Compliance Test Automation

If you will be importing IT Compliance Management Library Management Packs that include compliance test automation using Configuration Manager, you need to create a Configuration Manager connector in Service Manager 2012 specifically for the Process Pack for IT GRC.

Note

Although this guide references Configuration Manager 2012 for the example, Configuration Manager 2007 R2 is also supported.

For more information about:

* Connectors in Service Manager 2012, see [Using Connectors to Import Data into System Center 2012 - Service Manager](http://technet.microsoft.com/en-us/library/hh524326.aspx).
* Importing data from Configuration Manager into Service Manager, see [Importing Data from System Center Configuration Manager](http://technet.microsoft.com/en-us/library/hh519733.aspx).

To create a connector to Configuration Manager for compliance test automation

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Administration.
2. In the Administration pane, go to the **Administration / Connectors** location.
3. In the Tasks pane, click Create Connector, and then click Configuration Manager Connector.

The System Center Configuration Manager Connector Wizard starts.

1. Complete the System Center Configuration Manager connector wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Before You Begin | 1. Click Next. |
| General | 1. In Name, type Configuration Manager Connector for Process Pack for IT GRC. 2. In Description, type Configuration Manager connector that is used by the Process Pack for IT GRC compliance test automation information from the New York City (NYC) primary site in Configuration Manager 2012. 3. Click Next. |
| Management Pack | 1. In Management Pack, select Microsoft Service Manager IT Compliance Test Automation Transformation for SCCM 2012. 2. Click Test Connection.   The **Credentials** dialog box appears.   1. In the Credentials dialog box, in Password, type P@ssw0rd, and then click OK.   The **Test Connection** dialog box appears.   1. In the Test Connection dialog box, click OK. 2. Click Next. |
| Database | 1. In Database server name, type CM-2012-01. 2. In Database name, type CM\_NYC. 3. Click Test Connection.   The **Test Connection** dialog box appears.   1. In the Test Connection dialog box, click OK. 2. Click Next. |
| Collections | 1. Select the Select all check box. 2. Click Next. |
| Schedule | 1. Click Next. |
| Summary | 1. Review the information that you provided while completing the previous wizard pages. 2. Click Create. |
| Progress | The progress for creating the Configuration Manager connector is displayed. |
| Completion | 1. Click Close. |

The Configuration Manager Connector displays in the preview pane.

1. In the preview pane, click Configuration Manager Connector for Process Pack for IT GRC.
2. In the Tasks pane, under Configuration Manager Connector for Process Pack for IT GRC, click Synchronize Now.

The **Synchronize Now** dialog box appears.

1. In the Synchronize Now dialog box, click OK.

If you import additional Configuration Manager 2012 device collections after you configure the Configuration Manager Connector for Service Manager, edit the connector to include the additional Configuration Manager 2012 collections.

## Step 2-4: Install Compliance Libraries

Compliance Libraries contain authority documents, citations, control objectives or control activities. Control activities are developed for specific products or technologies and ship as Microsoft IT Compliance Management Libraries. All IT Compliance Management Libraries include an IT Compliance Library Management Pack, which is imported into System Center Service Manager. Some IT Compliance Management Libraries may include an IT Compliance Management Library Configuration Pack, which is an IT Compliance Management Library configuration pack and is imported into System Center Configuration Manager.

If the Service Manager Management Server has Internet connectivity, the latest Compliance Libraries can be found automatically using the Knowledge Library Update feature found on the Compliance and Risk Overview page in the Service Manager Console. These library updates can also be downloaded directly from the [Microsoft Download Center](http://go.microsoft.com/fwlink/?LinkId=201481) or from partners at the [Microsoft System Center Management Pack Catalog for Service Manager](http://pinpoint.microsoft.com/en-US/systemcenter) and then imported using the Knowledge Library Update feature’s offline mode.

After you download the appropriate IT Compliance Library Management Pack, install and configure the IT Compliance Management Library Management Packs and DCM Configuration Packs using the instructions in the IT Compliance Management Library Deployment Guide, which is included as a part of the download.

 To automatically check for and install the latest IT Compliance Management Libraries

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.
2. In the Compliance and Risk Items pane, click All Compliance and Risk Items.
3. In the Overview pane, click Check for Updates.

The IT GRC Knowledge Importer Wizard starts.

1. Complete the IT GRC Knowledge Importer Wizard using information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Specify Location for Knowledge Library Updates | 1. Select Search automatically for the latest management packs online. 2. Click Next. |
| Import Knowledge Libraries | 1. Select the libraries you wish to import, generally All. 2. Click Import. |
| Completion | 1. Review the completion status of the wizard to ensure that all selected libraries were imported. 2. Click Close. |

## Step 2-5: Install DCM Configuration Items and Baselines

The attestation of automated control activities in the Process Pack for IT GRC can be performed using the desired configuration management feature in Configuration Manager 2012. The desired configuration management feature checks the configuration settings of the managed computers and determines their adherence to the configuration baselines. The results are then sent to the automated control activity in the IT GRC management program in Service Manger 2012.

The DCM configuration items and baselines can be created manually, but it is recommended that you use configuration baselines from the Microsoft Security Compliance Manager tool as a starting point for your baselines.

Install the DCM configuration items and baselines by completing the following procedures:

1. [Install Security Compliance Manager](#_Install_Security_Compliance)
2. [Export the Compliance Baselines into a DCM Pack](#_Export_the_Compliance)
3. [Import the DCM Pack into Configuration Manager 2012](#_Import_the_DCM)
4. [Configure the Configuration Items](#_Configure_the_Configuration)
5. [Configure the Configuration Baselines](#_Configure_the_Configuration_1)
6. [Create Device Collections for Targeting Configuration Baselines](#_Create_Device_Collections)
7. [Deploy the Configuration Baselines](#_Deploy_the_Configuration)

### Install Security Compliance Manager

The desired configuration management feature in Configuration Manager 2012 compares configuration settings on the managed computers with configuration baselines that you have configured. You can create these baselines by yourself or you can obtain them through the Windows Server 2008 R2 security compliance baseline in Security Compliance Manager 2.5.

For the purposes of this guide, you will download the Security Compliance Manager 2.5 and install the security compliance baselines for Windows Server 2008 R2.

 To install Security Compliance Manager 2.5

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. In Windows Explorer, create the C:\Files folder.
3. Download [Microsoft Security Compliance Manager](http://www.microsoft.com/download/en/details.aspx?displayLang=en&id=16776) to C:\Files.
4. In Windows Explorer, in C:\Files, double-click Security\_Compliance\_Manager\_  
   Setup.exe.

The Microsoft Security Compliance Manager Setup Wizard starts.

1. Complete the Microsoft Security Compliance Manager Setup Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Welcome to the Microsoft Security Compliance Manager Setup Wizard | 1. Click Next. |
| License Agreement | 1. Review the terms of the license agreement. To accept them and continue, click I accept the terms of the license agreement. 2. Click Next. |
| Installation Folder | 1. Click Next. |
| SQL Instances Found | 1. Click Next. |
| Ready to Install | 1. Click Install. |
| Installing the Microsoft Security Compliance Manager | The progress bar displays the installation process. |
| Installation Successful | 1. Click Finish. |

### Export the Compliance Baselines to a DCM Pack

The desired configuration management feature in Configuration Manager 2012 compares configuration settings on the managed computers with configuration baselines that you have configured. You can create these baselines by yourself or you can obtain them through the Windows Server 2008 R2 security compliance baseline in Security Compliance Manager 2.0.

In this example, Contoso will implement an IT GRC management program for their e-commerce website. As a part of their program, account lockout polices in Active Directory Domain Services (AD DS) must be configured to locked accounts after five unsuccessful logon attempts. The account lock configuration settings are stored in the WS2008R2SP1 Domain Security Compliance baseline.

Note

Although other baselines would be required to implement a full IT GRC management program, only the WS2008R2SP1 Domain Security Compliance baseline will be used in this example.

 To export the domain security compliance baseline to a DCM pack

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft Security Compliance Manager, and then click Security Compliance Manager.
3. In the console tree, go to Custom Baselines / Windows Server 2008 R2 SP1 / WS2008R2SP1 Domain Security Compliance 1.0.
4. In the actions pane, under **Export**, click SCCM DCM 2007 (.cab)

The Export to SCCM DCM dialog box appears.

1. In the Export to SCCM DCM dialog box, go to C:\Files, in File name, type WS2008R2SP1\_Domain\_Security\_Compliance\_DCM, and then click Save.

The compliance baseline is exported to the DCM pack .cab file.

1. In the SCM Log dialog box, click the View Error Log link.

Notepad opens and displays the contents of the log file. The setting for **Store passwords using reversible encryption** was not exported, which is normal and does not affect the account lock baseline.

1. Review the information in the log file and then close Notepad.
2. In the SCM Log dialog box, click OK.

Windows Explorer opens to the folder where the DCM pack .cab file was exported.

1. Close all open windows and dialog boxes.

### Import the DCM Pack into Configuration Manager 2012

The baseline settings are stored in the DCM pack that you exported from Security Compliance Manager earlier in the process. That file must be imported into the desired configuration management feature in Configuration Manager 2012.

In this example, Contoso will implement the account lock configuration settings, which are stored in the DCM pack (the WS2008R2SP1\_Domain\_Security\_Compliance\_DCM.cab file) that you exported earlier in the process from Security Compliance Manager.

Note

Although other baselines would be required to implement a full IT GRC management program, only the account lockout settings in the WS2008R2SP1 Domain Security Compliance baseline will be used in this example.

 To import the DCM pack into Configuration Manager 2012

1. On CM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center 2012, click Configuration Manager, and then click Configuration Manager Console.
3. In the Configuration Manager console, in the navigation pane, click Assets and Compliance.
4. In the Assets and Compliance workspace, go to Overview / Compliance Settings / Configuration Items.
5. On the ribbon, on the Home tab, in the Create group, click Import Configuration Data.

The Import Configuration Data Wizard starts.

1. Complete the Import Configuration Data Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Select Files | 1. Click Add.   The Open dialog box appears.   1. In the Open dialog box, type \\SM-2012-01\Files\ WS2008R2SP1\_Domain\_Security\_Compliance\_ DCM.cab, and then click Open.   The Configuration Manager dialog box appears notifying you that the publisher of the .cab file could not be verified.   1. In the Configuration Manager dialog box, click Yes.   The **WS2008R2SP1\_Domain\_Security\_Compliance\_DCM.cab** file appears in the Files that contain configuration items or configuration baselines list box.   1. Select the Create a new copy of the imported configuration baselines and configuration items check box. 2. Click Next.   The **Verifying Configuration Data** dialog box appears and the progress for verifying the configuration data is displayed. |
| Summary | 1. Review the information in the Details box that that you provided while completing the previous wizard pages. 2. Click Next. |
| Progress | The progress for importing the configuration data is displayed. |
| Confirmation | 1. Click Close. |

1. The following configuration items are shown in the preview pane:

* Copy of WS2008R2SP1 Domain Security Compliance-Account Lock
* Copy of WS2008R2SP1 Domain Security Compliance-Password Attributes

### Configure the Configuration Items

The imported configuration items contain preconfigured thresholds for determining configuration compliance. You can configure the configuration items to meet the requirements established by your organization.

In this example, Contoso has a policy that accounts are locked after five unsuccessful logon attempts. The configuration item Microsoft Baselines WS2008R2SP1 Domain Security Compliance 1.0-Account Lock contains a preconfigured threshold of locking an account after 50 unsuccessful logon attempts. You will configure this configuration item to match the Contoso account lockout policy.

 To configure the configuration item for account lockout

1. On CM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center 2012, click Configuration Manager, and then click Configuration Manager Console.
3. In the Configuration Manager console, in the navigation pane, click Assets and Compliance.
4. In the Assets and Compliance workspace, go to Overview / Compliance Settings / Configuration Items.
5. In the preview pane, click Copy of WS2008R2SP1 Domain Security Compliance-Account Lock.
6. On the ribbon, on the Home tab, in the Properties group, click Properties

The Copy of WS2008R2SP1 Domain Security Compliance-Account Lock Properties dialog box opens.

1. In the Copy of WS2008R2SP1 Domain Security Compliance-Account Lock Properties dialog box, on the Compliance Rules tab, click Account lockout threshold where Condition contains Equals 50, and then click Edit.

The Edit Rule dialog box appears.

1. In the Edit Rule dialog box, in the following values, type 5, and then click OK.

The value in the Condition column is updated to Equals 5.

1. In the Copy of WS2008R2SP1 Domain Security Compliance-Account Lock Properties dialog box, click OK.

### Configure the Configuration Baselines

Configuration baselines contain one or more configuration items. You assign configuration baselines to the device collection that you want to assess. The appropriate configuration items need to be added to the configuration baseline.

In this example, the .cab file that we imported previously created configuration items and a configuration baseline. For the purposes of the example, only the Copy of WS2008R2SP1 Domain Security Compliance-Account Lock configuration item will be used.

 To configure the configuration baselines

1. On CM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center 2012, click Configuration Manager, and then click Configuration Manager Console.
3. In the Configuration Manager console, in the navigation pane, click Assets and Compliance.
4. In the Assets and Compliance workspace, go to Overview / Compliance Settings / Configuration Baselines.
5. In the preview pane, click Copy of WS2008R2SP1 Domain Security Compliance.
6. On the ribbon, on the Home tab, in the Properties group, click Properties.

The Copy of WS2008R2SP1 Domain Security Compliance Properties dialog box opens.

1. In the Copy of WS2008R2SP1 Domain Security Compliance Properties dialog box, on the Evaluation Conditions tab, in Configuration data, click Copy of WS2008R2SP1 Domain Security Compliance-Password Attributes, click Remove, and then click OK.

Now the Copy of WS2008R2SP1 Domain Security Compliance configuration baseline only contains the Copy of WS2008R2SP1 Domain Security Compliance-Account Lock configuration item.

### Create Device Collections for Targeting Configuration Baselines

Device collections in Configuration Manager provide a way to select the target computers that you want to assess their configuration baselines. The type of compliance assessments that you want to perform may require you to create a computer collection for each compliance program.

The device collection is used for targeting the configuration baseline you will create. The configuration baseline is applied to the device collection.

Note

This device collection needs to match the scope of the IT GRC management program created in Service Manager.

In this example, Contoso will create a device collection that includes all the computers for their e-commerce website.

 To create a device collection for targeting configuration baselines

1. On CM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center 2012, click Configuration Manager, and then click Configuration Manager Console.
3. In the Configuration Manager console, in the navigation pane, click Assets and Compliance.
4. In the Assets and Compliance workspace, go to Overview / Device Collections.
5. On the ribbon, on the Home tab, in the Create group, click Create Device Collect

The Create Device Collection Wizard starts.

1. Complete the Create Device Collection Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| General | 1. In Name, type Contoso E-Commerce Web Site Computers. 2. In Comment, type Computers that are a part of the Contoso e-commerce web site. 3. Click Browse.   The Select Collection dialog box appears.   1. In the Select Collection dialog box, click All Systems, and then click OK. 2. Click Next. |
| Membership Rules | 1. Click Add Rule, and then click Direct Rule.   The Create Direct Membership Rule Wizard starts.   1. Complete the Create Direct Membership Rule Wizard by performing the following steps: 2. On the Welcome page, click Next. 3. On the Search for Resources page, in Resource class, select System Resource; in Attribute name, select Name; in Value, type %; and then click Next. 4. On the Select Resources page, select the check box next to CM-2012-01, OM-2012-01, SM-2012-02, and WIN-2008R2-01, and then click Next. 5. On the Summary page, click Next. 6. On the Progress page, view the progress for creating the new membership rule. 7. On the Completion page, click Close. 8. Click Next. |
| Summary | 1. Review the information in the Details box that that you provided while completing the previous wizard pages. 2. Click Next. |
| Progress | The progress for creating the device collection is displayed. |
| Confirmation | 1. Click Close. |

The Contoso E-Commerce Web Site Computers collection appears in the preview pane.

### Deploy the Configuration Baselines

After the device collection is created, deploy the configuration baseline to the device collection. Deploying the configuration baseline configures the desired configuration management feature to start collecting the compliance status of the computers in the device collection.

 To deploy the configuration baselines

1. On CM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center 2012, click Configuration Manager, and then click Configuration Manager Console.
3. In the Configuration Manager console, in the navigation pane, click Assets and Compliance.
4. In the Assets and Compliance workspace, go to Overview / Compliance Settings / Configuration Baselines.
5. In the preview pane, click Copy of WS2008R2SP1 Domain Security Compliance.
6. On the ribbon, on the Home tab, in the Deployment group, click Deploy.

The Deploy Configuration Baselines dialog box appears.

1. Complete the Deploy Configuration Baselines dialog box by performing the following steps and then click OK:
2. In Collection, click **Browse**.

The Select Collection dialog box appears.

1. In the Select Collection dialog box, select Device Collections, click Contoso E-Commerce Web Site Computers, and then click OK.
2. In Simple schedule, select 30 minutes.

In the preview pane, the **Status**, **Deployed**, and **Date Modified** columns are updated to reflect that the configuration baseline is deployed.

## Step 2-6: Install the Process Pack for IT GRC Client Prerequisites

The Process Pack for IT GRC Client requires the Visual Studio® Tools for Office System 3.0 runtime with Service Pack 1. Install the Visual Studio Tools for Office System 3.0 runtime and then install the Software Updates Visual Studio Tools for the Office System 3.0 Runtime (KB949258). These must be installed prior to installing the Process Pack for IT GRC Client.

 To install the Visual Studio Tools for Office System 3.0 runtime

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Download the [Microsoft Visual Studio Tools for the Microsoft Office system (version 3.0 Runtime) (x86)](http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=23656) (VSTOR30.exe) to download\_folder (where download\_folder is the folder to which you downloaded the Microsoft Visual Studio Tools for the Microsoft Office system).
3. Download the [Microsoft Visual Studio Tools for the Microsoft Office System (version 3.0 Runtime) Service Pack 1 (x86)](http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=1132) (vstor30sp1-KB949258-x86.exe) to download\_folder.
4. In Windows Explorer, go to download\_folder, and then double-click VSTOR30.exe.

The Visual Studio Tools for Office system 3.0 Runtime Setup Wizard starts.

1. Complete the Visual Studio Tools for Office system 3.0 Runtime Setup Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Welcome to Visual Studio Tools for Office system 3.0 Runtime Setup | 1. Click Next. |
| License Terms | 1. Review the license terms. To continue, select the I have read and accept the license terms check box. 2. Click Install. |
| Installing components | The progress bar displays the installation process. |
| Setup Complete | 1. Click Finish. |

1. In Windows Explorer, go to download\_folder, and then double-click vstor30sp1-KB949258-x86.exe.

The Software Updates Visual Studio Tools for the Office System 3.0 Runtime (KB949258) Setup Wizard starts.

1. Complete the Software Updates Visual Studio Tools for the Office System 3.0 Runtime (KB949258) Setup Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Welcome to Visual Studio Tools for the Office System 3.0 Runtime (KB949258) software update | 1. Click Next. |
| Microsoft Software License Terms | 1. Review the license terms. To continue, select the I have read and accept the license terms check box. 2. Click Install. |
| Installing the software update | The progress bar displays the installation process. |
| The software update has been installed successfully. | 1. Click Finish. |

1. Close all open windows and dialog boxes.

## Step 2-7: Install the Process Pack for IT GRC Client

The Process Pack for IT GRC Client integrates with Microsoft Office Excel® 2007 or 2010. The Process Pack for IT GRC Client allows you to access the IT GRC programs, control objectives, and control activities managed by the Process Pack for IT GRC. You can use the Process Pack for IT GRC Client to import the information into Excel, modify the information, and then save the modified information back into the Process Pack for IT GRC.

You can install the Process Pack for IT GRC Client on any computer that has Microsoft Office Excel 2007 or 2010 installed and has connectivity with the computer running Service Manager 2012 and the Process Pack for IT GRC. There are 32-bit and 64-bit versions of the Process Pack for IT GRC Client for the corresponding 32-bit or 64-bit versions of Excel 2007 or 2010. Install the appropriate version of the Process Pack for IT GRC Client for the version of Excel that is installed.

 To install the Process Pack for IT GRC Client

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. In Windows Explorer, go to target\_folder, and then double-click Setup (where target\_folder is the folder to which the Process Pack for IT GRC is extracted.)

The Process Pack for IT GRC Setup Wizard splash screen is displayed.

1. In the Process Pack for IT GRC Setup Wizard splash screen, click the Install GRC Process Pack 2012 Client link.

The Process Pack for IT GRC Setup Wizard starts.

1. Install the Process Pack for IT GRC using the Process Pack for IT GRC Setup Wizard and the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Product registration | 1. In Name, type Contoso IT. 2. In Organization, type Contoso LTD. 3. Review the license terms. To continue, select the I have read, understood, and agreed with the terms of the license agreement check box. 4. Click Next. |
| Install Location | 1. Click Next. |
| Installation summary | 1. Review the configuration options selected while completing the wizard. 2. Click Install. |
| Process Pack for IT GRC Client | The progress for installing the Process Pack for IT GRC is displayed. The **Microsoft Office Customization Installer** dialog box appears.   1. In the Microsoft Office Customization Installer dialog box, click Install.   The installation process continues.   1. In the Microsoft Office Customization Installer dialog box, click Close. |
| Setup completed successfully | 1. Click Close. |

 To verify the Process Pack for IT GRC Client installation

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click **Start**, click **All Programs**, click **Microsoft Office**, and then click **Microsoft Excel 2010**.

Excel 2010 starts. The Welcome to Microsoft Office 2010 dialog box appears.

1. In the Welcome to Microsoft Office 2010 dialog box, click Use Recommended Settings, and then click OK.

The Microsoft Excel 2010 startup process completes.

1. On the ribbon, on the File tab, click Options.

The **Excel Options** dialog box opens.

1. In the Excel Options dialog box, in the navigation pane, click Add-Ins.
2. In the details pane, in manage, select COM Add-ins, and then click Go.

The **COM Add-Ins** dialog box opens.

1. In the COM Add-Ins dialog box, select the check box next to Service Manager Process Pack for IT GRC Add-In 2012, and then click OK.
2. In Excel, on the ribbon, ensure the **Service Manager** tab is present.

# Task 3: Implement an IT GRC Management Program

The primary objective of the Process Pack for IT GRC is to help you implement IT GRC control and risk management in your organization. Your first step, after installation, is to implement your IT GRC management program. The program will be based on authority document citations and includes the control objectives and control activities to help you perform IT GRC control management.

Implement an IT GRC management program by completing the following steps:

[Step 3-1: Create an IT GRC Management Program](#_Step_3-1:_Create)

[Step 3-2: Add a Scope to the Program](#_Step_3-2:_Add)

[Step 3-3: Create Authority Documents, Control Objectives, and Control Activities for the Program](#_Step_3-4:_Create)

[Step 3-4: Customize an Automated Control Activity](#_Step_3-5:_Customize)

[Step 3-5: Create a Manual Control Activity](#_Step_3-6:_Create)

[Step 3-6: Add the Manual Control Activity to a Control Objective](#_Step_3-7:_Add)

[Step 3-7: Publish the IT GRC Management Program](#_Step_3-9:_Publish)

## Step 3-1: Create an IT GRC management program

Programs define the boundaries for the compliance and risk process efforts or projects in your organization. Programs define the security within a boundary by defining user permissions in the program. This approach allows delegation of tasks based on user roles within the program.

Programs also establish boundaries for other IT GRC items, such as items in the Risk Management and Control Management folders. These boundaries allow the program manager for the Program to manage risks and controls specifically for the program.

 To create an IT GRC management program

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.
2. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items / Program Management / All Programs location.
3. In the Tasks pane, under Program Management, click Create Program.

The Program Management <prog\_id> - - Draft form opens (where prog\_id is the unique program identifier that was created.)

1. Complete the Program Management <prog\_id> - - Draft form by performing the steps in the following table for each tab and then clicking OK.

| On this tab | Do this |
| --- | --- |
| General | 1. In Title, type Credit Card Processing Compliance Program (PCI DSS). 2. In Owner, type CORP\Administrator. 3. In Business Justification, type Contoso credit card processing compliance (PCI DSS) program for corporate e-commerce site. |
| Settings | 1. Review the value in Program Control Activity Threshold Default Value.   This value affects the final compliance score for each automated control activity within the program. The score is produced at report time. Value directly affects the number of allowable compliant and non-compliant results. When the value is set to 100%, the individual test results for each automated control activity will need to be 100% compliant.  Note  This threshold value is only used when scoring automated control activities. Manual control activities are scored based on manual assertion. |

The Credit Card Processing Compliance Program (PCI DSS) appears in the details pane with a status of Draft.

## Step 3-2: Add a Scope to the Program

Scopes allow you to limit the number of computers that are included in a program. You can add multiple scopes to a program so that you can precisely target the program to the appropriate managed devices in your environment. Add scope to your program using the following table and instructions.

Note

Later in the process you will create a device collection in Configuration Manager 2012 that will be used to assign configuration baselines. Ensure that you include the same computers in both places so that the automated control activities will work properly.

 To add a scope to the IT GRC management program

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.
2. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items / Program Management / All Programs location.
3. In the Results pane, click Credit Card Processing Compliance Program (PCI DSS).
4. In the Tasks pane, click Edit.

The Program Management <prog\_id> - - Credit Card Processing Compliance Program (PCI DSS) – Draft form opens (where prog\_id is the unique program identifier for the program.)

1. In the Program Management <prog\_id> - - Credit Card Processing Compliance Program (PCI DSS) – Draft form, on the General tab, in the Scope section, in the Configuration Items in Scope list box, click Add.

The Select objects form appears.

1. In the Select objects form perform the following steps and then click OK:
2. In the drop-down list box for filtering, select Computer.

The Available objects list box is refreshed to display only computers.

1. In the Available objects list box, click WIN-2008R2-01, click Add.

The computers appear in the Selected objects list box.

1. The selected computers appear in the Configuration Items in Scope list box.
2. In the Program Management <prog\_id> - - Credit Card Processing Compliance Program (PCI DSS) – Draft form, click OK.

## Step 3-3: Create Authority Documents, Control Objectives, and Control Activities for the Program

After you create an IT GRC management program, you are ready to create authority documents, control objectives, and control activities for the program (in this example, the Credit Card Processing Compliance program). Creating control objectives and control activities for the program defines which control objectives are to be accomplished in the program. Import the control objectives and control activities to the program using the following table and instructions.

Note

As you run the Create Controls from Library Wizard, note the number of control activities that are created for the program. These control activities illustrate the dramatic reduction of effort required to implement an IT GRC management program because of the number of predefined control activities that are automatically generated.

 To create control objectives and control activities for the IT GRC management program

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.
2. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items / Program Management / All Programs location.
3. In the Results pane, click Credit Card Processing Compliance Program (PCI DSS).
4. In the Tasks pane, click Create Controls from Library.

The Create Controls from Library Wizard starts.

1. Complete the Create Controls from Library Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Before you Begin | 1. Click Next. |
| Program Selection | 1. In Select a Program that you own, where the Categories, Control Objectives and Activities will be imported, select Credit Card Processing Compliance Program (PCI DSS). 2. Click Next. |
| Library Selection | 1. Select the Microsoft.AuthorityDocument.Library check box, and then click Add. 2. Select the Microsoft.ControlObjective.Library check box, and then click Add. 3. Select the Microsoft.ControlActivity.WS2008R2.Library check box, and then click Add. 4. Click Next. |
| Authority Document Selection | 1. Select Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures check box, and then click Add. 2. Click Next. |
| Control Objective Selection | 1. Review the list of categories and control objectives selected by default (approximately 132). 2. Click Next. |
| Control Activity Selection | 1. Review the list of control activities selected by default (approximately 55). 2. Click Next. |
| Summary | 1. Review the list of selected control objectives and control activities. 2. Click Create.   Note  This operation can take a long period of time to complete. |
| Completion | 1. Review the completion status of the wizard, specifically if any control objectives or control activities failed. 2. Click Close. |

## Step 3-4: Customize an Automated Control Activity

The automated control activities that you created using the Create Controls from Library Wizard may need to be customized based on your organization’s policy or requirements.

In this example, Contoso has an existing policy that requires an account to be locked after five unsuccessful logon attempts. The descriptive text of the automated control activity needs to reflect this policy. In addition, other information needs to be configured that is specific to the program, such as the technology used, if the control activity can be shared, the level of the control activity, and the priority of the control activity.

 To customize an automated control activity

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.
2. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items / Program Management / All Programs location.
3. In the Results pane, click Credit Card Processing Compliance Program (PCI DSS).
4. In the Tasks pane, click Edit.

The Program Management <id> - Credit Card Processing compliance Program (PCI DSS) – Draft form opens (where id is the automatically generated program identifier).

1. In the Program Management < id> - Credit Card Processing compliance Program (PCI DSS) – Draft form, on the Framework tab, go to PC<id> Identity and Access Management / PC<id> Access Management / CO<id> Account Lock (where id is the unique identifier assigned to each item).
2. Click Open.

The Control Objective CO <id> - Account Lock – Draft form opens.

1. In the Control Objective CO <id> - Account Lock – Draft form, perform the following steps and then click OK.
2. In Owner, type CORP\Administrator.
3. In the Tasks pane, click Publish Control Objective.

The Publish dialog box appears, confirming you want to publish the control objective.

1. In the Publish dialog box, click Yes.

The Control Objective Publish task dialog box appears, confirming that the control objective was successfully published.

1. In the Publish dialog box, click OK.

The Program Management < id> - Credit Card Processing compliance Program (PCI DSS) – Draft form appears.

1. In the Program Management < id> - Credit Card Processing compliance Program (PCI DSS) – Draft form, on the Framework tab, go to PC<id> Identity and Access Management / PC<id> Access Management / CO<id> Account Lock / CMCA<id> Account Lock (where id is the unique identifier assigned to each item).

Tip

There will be multiple CMCA<id> Account Lock automated control activities. Select the automated control activity with the lower identifier number. For example, if your environment has CMCA63 Account Lock and CMCA62 Account Lock, select CMCA62 Account Lock.

1. Click Open.

The **Configuration Manager Control Activity CMCA<*id*> - Account Lock – Pending** form appears.

1. In the Configuration Manager Control Activity CMCA<id> - Account Lock – Pending form, configure the General tab by performing the following steps:
2. In Description, add the following text to the end of the existing text.

Contoso policy is to lock accounts after five unsuccessful logon attempts.

1. In Owner, type CORP\Administrator.
2. In Shared, select Yes.
3. In Technology, select Windows Server 2008 R2.
4. In Level, select 1.
5. In Priority, select 2.
6. In the Tasks pane, click Activate Control Activity.

The Activate dialog box opens, confirming you want to activate the control activity.

1. In the Activate dialog box, click Yes.

The Control Activity Activation Task dialog box opens, notifying you that the activation process was successful.

1. In the Control Activity Activation Task dialog box, click OK.
2. In the Configuration Manager Control Activity CMCA<id> - Account Lock – Pending form, click the Validation tab, perform the following steps, and then click OK:
3. In Test ID, click Associate Test.

The **Select objects** dialog box appears.

1. In the Select object dialog box, click Copy of WS2008R2SP1 Domain Security Compliance-Account Lock, and then click OK.

The values in the Test ID and Test Name boxes relate to a configuration item that is managed by the desired configuration manager in Configuration Manager. The values here relate to the corresponding configuration item in desired configuration manager. These relations tie specific control activities to specific configuration items in desired configuration manager.

1. Review the information in the Test Summary box.

The text in the Test Summary box describes how the automated assertion is performed using the desired configuration manager pack in Configuration Manager.

The Configuration Manager Control Activity CMCA<id> - Account Lock – Pending form closes and the control activity is updated.

1. In the Program Management <id> - Credit Card Processing compliance Program (PCI DSS) – Draft form, click OK.
2. Close all open windows and dialog boxes.

## Step 3-5: Create a Manual Control Activity

The control activities that you created using the Create Controls from Library Wizard include only automated control activities. However, certain aspects of IT GRC management can only be done manually. Manual control activities allow you include these manual assertions of compliance into your IT GRC management program.

In this example, Contoso needs to evaluate the compatibility of their e-commerce application with the policies in the IT GRC management program. Because this activity must be performed manually, a corresponding manual control activity will be created.

 To create a manual control activity

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.
2. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items / Control Management / Control Activities / Manual Control Activities / All Manual Control Activities location.
3. In the Tasks pane, click Create Manual Control Activity.

The Manual Control Activity <mca\_id> - - New form opens (where mca\_id is the manual control activity identifier that was automatically generated).

1. Complete the Manual Control Activity <mca\_id> - - New form by performing the following steps and then clicking OK.
2. In Title, type Assess the applicability of program policies to current e-commerce web application.
3. In Description, type Determine whether the program policies affect the e-commerce web application.
4. In Owner, type CORP\Administrator.
5. In Type, select Detective.
6. In Technology, select Windows Server 2008 R2.

The manual control activity appears in the details pane with a status of Pending. Now the control activity must be activated.

1. In the details pane, click the control activity with the title of Assess the applicability of program policies to current e-commerce web application.
2. In the tasks pane, click Activate Control Activity.

The Activate dialog box appears, confirming that you want to activate the control activity.

1. In the Activate dialog box, click Yes.
2. In the tasks pane, click Refresh.

The list of manual control activities refreshes and the status of the control activity changes to Active.

1. Close all open windows and dialog boxes.

## Step 3-6: Add the Manual Control Activity to a Control Objective

After you create the manual control activity you need to add it to a control objective within the program created earlier in the process. You can add the manual control activity to a control activity in the framework of the program.

Also, control objectives need to be published before they can be included as part of the compliance evaluation. As a part of the process for adding the manual control activity, you will also publish the control objective to which the manual control activity is assigned.

In this example, the Credit Card Processing Compliance Program program implemented by Contoso includes the Policy Needs Assessment control objective, which is intended to assess the compliance policies and their effect on the existing IT infrastructure. To add the manual control activity to this control objective, complete the steps in the following procedure.

 To add the manual control activity to a control objective

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.
2. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items / Program Management / All Programs location.
3. In the Results pane, click Credit Card Processing Compliance Program (PCI DSS).
4. In the Tasks pane, click Edit.

The Program Management <id> - Credit Card Processing compliance Program (PCI DSS) – Draft form opens (where id is the automatically generated program identifier).

1. In the Program Management < id> - Credit Card Processing compliance Program (PCI DSS) – Draft form, on the Framework tab, go to <id> IT Process Management / <id> Policy Management / <id> Policy Needs Assessment (where id is the unique identifier assigned to each item).
2. Click Open.

The Control Objective < id> - Policy Needs Assessment - Draft form opens.

1. In the Control Objective < id> - Policy Needs Assessment - Draft form, perform the following steps and then click OK.
2. In Owner, type CORP\Administrator.
3. In the Tasks pane, click Publish Control Objective.

The Publish dialog box appears, confirming that you want to publish the control objective.

1. In the Publish dialog box, click Yes.

The Control Objective Publish task dialog box appears, confirming that the control objective was successfully published.

1. In the Publish dialog box, click OK.

The Program Management < id> - Credit Card Processing compliance Program (PCI DSS) – Draft form appears.

1. In the Program Management < id> - Credit Card Processing compliance Program (PCI DSS) – Draft form, click Add Control Activity.

The Select objects dialog box opens.

1. Complete the Select objects dialog box by performing the following steps and then clicking OK.
2. In the filter area, in the drop-down list box, select Manual Control Activity.

The <id> Windows Server 2008 R2 Assess the applicability of program policies to current e-commerce web application appears in the Available objects list box (where id is the control activity identifier).

1. Click <id> Windows Server 2008 R2 Assess the applicability of program policies to current e-commerce web application, and then click Add.

The manual control activity appears in the Selected objects list box.

The <id> Windows Server 2008 R2 Assess the applicability of program policies to current e-commerce web application control activity appears beneath the <id> Policy Needs Assessment control objective.

1. In the Program Management <id> - Credit Card Processing compliance Program (PCI DSS) – Draft form, click OK.

## Step 3-7: Publish the IT GRC Management Program

After you create the control objectives and control activities for the program you created, the Credit Card Processing Compliance Program, you are ready to publish it using the Publish Program task. You publish a program to change its status from Draft to Published and use the program in your production environment.

 To publish the IT GRC management program

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.
2. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items / Program Management / All Programs location.
3. In the Results pane, click Credit Card Processing Compliance Program (PCI DSS).
4. In the Tasks pane, click Publish Program.

The Publish dialog box opens.

1. In the Publish dialog box, click Yes.

The Program Publish Task dialog box opens, notifying that the program will be in a pending state for a short period of time until it is approved.

1. In the Program Publish Task dialog box, click OK.
2. In the Tasks pane, under All Programs, click Publish Program.

The status of the program changes to Published.

1. Close all open windows and dialog boxes.

# Task 4: Administer an IT GRC management program

After you implement your IT GRC management program, you must perform the day-to-day administration tasks.

To administer an IT GRC management program, perform the following steps:

[Step 4-1: Configure Process Pack for IT GRCUser Roles](#_Step_4-1:_Configure)

[Step 4-2: Manage IT GRC Programs Using the Process Pack for IT GRC Client](#_Step_4-2:_Manage)

[Step 4-3: Add Tests Results to a Manual Control Activity](#_Step_4-3:_Add)

[Step 4-4: Verify Compliance Status Using Configuration Manager Reports](#_Step_4-4:_Verify)

[Step 4-5: Request an IT GRC Compliance Management Program Exception](#_Step_4-5:_Configure)

[Step 4-6: Verify Compliance Status Using Process Pack for IT GRC Reports](#_Step_4-6:_Verify)

## Step 4-1: Configure Process Pack for IT GRC User Roles

In System Center Service Manager, the security rights that allow users to access or update information are defined in a user role profile. A user role profile is a named collection of access rights and usually corresponds to employees’ business responsibilities. Each user role profile controls access to entities that are stored in and managed through System Center Service Manager, including programs, control objectives, control activities, and risks.

The Process Pack for IT GRC includes user role profiles that build on and extend the existing System Center Service Manager user profiles. These Process Pack for IT GRC user role profiles are specific to the Process Pack for IT GRC.

Users who perform specific user roles are assigned to a user role profile. Some of the user roles for the Process Pack for IT GRC are members of the user role profiles that are specific to the Process Pack for IT GRC. Other user roles for the Process Pack for IT GRC are members of the System Center Service Manager user role profiles.

The following table lists the Process Pack for IT GRC user roles, the user role profile to which the user role is assigned, and a brief description of the user role.

| User role | User role profile | Description |
| --- | --- | --- |
| Administrator | Administrators | Responsible for installation of the Process Pack for IT GRC, IT Compliance Management Libraries, and the ongoing management of system wide configuration settings. |
| Compliance Program Manager | Compliance Program Manager | Responsible for the management of IT GRC programs within their organization and helps ensure that the organization is in compliance with authority document citations. |
| Compliance Program Implementer | Compliance Program Implementer | Responsible for the management of control objectives, control activities, and risks. Also responsible for managing the day-to-day tasks, such as performing control activity compliance tests or updating risk information. |
| Compliance Program Read Only Users | Read-Only Operators | Responsible for viewing IT GRC entities, such as programs, control objectives, control activities, and risks. Also responsible for creating compliance incidents. |
| Library Author | Authors | Responsible for customizing the Process Pack for IT GRC or the IT Compliance Management Libraries. Also responsible for creating new management packs that work with the Process Pack for IT GRC. These users are also typically members of the Administrator user role profile in their authoring environment. |

For more information about user roles in System Center Service Manager, see [About User Roles](http://technet.microsoft.com/en-us/library/hh519690.aspx).

In this example, Contoso has a user, PilarA, who will perform the Compliance Program Implementer user role. You will create the Compliance Program Implementer user role and then add PilarA to that user role.

 To configure user roles for the Process Pack for IT GRC

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Administration.
2. In the Administration pane, go to the Administration / Security / User Roles location.
3. In the Tasks pane, click Create User Roles, and then click Compliance Program Implementer.

The Create User Role Wizard starts.

1. Complete the Create User Role Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Before you Begin | 1. Click Next. |
| General | 1. In Name, type Contoso Compliance Program Implementer. 2. In Description, type User role that allows user to edit programs in their queue scope and any configuration items in their group scope. 3. Click Next. |
| Management Packs | 1. Click Select All. 2. Click Next. |
| Queues | 1. Click Next. |
| Configuration item Groups | 1. Click Provide access only to the select groups. 2. Select the check box next to the following names:  * System.Compliance.ApplicabilityGroup * Applicability.InstanceGroupWindowsServer2008R2Group  1. Click Next. |
| Catalog item Groups | 1. Click Next. |
| Tasks | 1. Click Next. |
| Views | 1. Click Next. |
| Form Templates | 1. Click Next. |
| Users | 1. Click Add. 2. The Select Users or Groups dialog box appears. 3. In the Select Users or Groups dialog box, in Enter the object names to select, type PilarA, click Check Names, and then click OK.   PilarA@corp.contoso.com appears in the Selected users list box.   1. Click Next. |
| Summary | 1. Review the list of user role selections made during the wizard. 2. Click Create. |
| Completion | 1. Review the completion status of the wizard. 2. Click Close. |

The Contoso Compliance Program Implementer user role appears in the list of user roles. You would perform a similar task to create a Compliance Program Manager user role for Contoso.

## Step 4-2: Manage IT GRC Programs Using the Process Pack for IT GRC Client

Although the IT GRC program can be totally managed in the Service Manager Console, there are instances in which you may wish to make bulk updates to the IT GRC program. For example, you might want to set the Owner and Assigned To fields for all control objectives or control activities in a program.

The Process Pack for IT GRC Client is an Excel add-in that allows you to load the information from your IT GRC program into Excel. After the information is loaded, you can manipulate the information as you would with any other information in Excel. After you have completed your updates, you can publish your updates back to the IT GRC program.

 To manage an IT GRC program using the Process Pack for IT GRC Client

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.
2. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items / Program Management / All Programs location.
3. In the Results pane, click Credit Card Processing Compliance Program (PCI DSS).
4. In the Tasks pane, click Open Program in Excel.

Microsoft Excel 2010 starts and loads the IT GRC information into the spreadsheet.

The Program Management <id> - Credit Card Processing compliance Program (PCI DSS) – Draft form opens (where id is the automatically generated program identifier).

1. In Excel, on the Control Objectives worksheet tab, in the first row, record the values in the ID and Title columns.
2. In the Owner column, click the drop-down box on the cell, and click Select from User Picker.

The Select User dialog box appears.

1. In the Select User dialog box, in the User Name column, click Administrator, and then click OK.
2. In the Assigned to column, click the drop-down box on the cell, and click Select from User Picker.

The Select User dialog box appears.

1. In the Select User dialog box, in the User Name column, click Administrator, and then click OK.
2. On the ribbon, on the Service Manager tab, in the Service Manager GRC Item group, click Publish.

The updates are published to Service Manager as shown by the status message in the lower left corner of the status bar in Excel. After the updates are published, the Publish Results dialog box appears.

1. In the Publish Results dialog box, review the published control objectives, and then click **OK**.
2. The data is refreshed from Service Manager.
3. Close all open windows and dialog boxes.

You could use this same method to make mass updates to the program items or to do global search and replace.

## Step 4-3: Add Tests Results to a Manual Control Activity

A manual control activity is a control activity that requires manual attestation of the compliance state. For example, if part of the IT GRC management program is to determine application compatibility with the compliance policies, that activity can only be performed manually. After the activity is performed, you need to record the results of the compliance activity in the manual control activity.

In this example, Contoso has a manual control activity that requires application compatibility testing with the compliance policies, which created the manual control activity earlier in the process. Based on testing, the e-commerce application was found to be compatible with the compliance polices. In this step, you will configure the test results for the manual control activity.

 To add test results to the manual control activity

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.
2. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items / Control Management / Manual Control Activities / All Manual Control Activities location.
3. In the Results pane, click Assess the applicability of program policies to current e-commerce web application.
4. In the Tasks pane, click Add Result.

The Select Template form opens.

1. In the Select Template form, click Compliant, and then click OK.

The Control Activity Results – CAR<id> form opens (where id is the automatically generated manual control activity results identifier).

1. In the Control Activity Results – CAR<id> form, in Details, type Upon performance of application test matrix, application is found to be compatible with compliance policies and settings.

You could also add any files that would serve as supporting evidence that the control activity results are compliant. For example, you could attach the output of a test matrix that shows the application is compatible with the compliance settings.

1. In the Control Activity Results – CAR<id> form, click OK.

This process would need to be repeated for each manual control activity that you have in an IT GRC management program.

## Step 4-4: Verify Compliance Status Using Configuration Manager Reports

You can use compliance reports in Configuration Manager 2012 to help you identify whether compliance information is being collected from the managed computers. Specifically, you can determine which configuration items within a configuration baseline are out of compliance.

Configuration Manager 2012 includes a number of compliance reports that you can use to help you identify compliance with configuration baselines and to troubleshoot compliance assessments in the Process Pack for IT GRC. Because the automated control activities in the Process Pack for IT GRC are updated based on the configuration baselines in Configuration Manager 2012, you must first determine whether the configuration baselines are collecting the appropriate information.

 To verify compliance status using Configuration Manager reports

1. On CM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center 2012, click Configuration Manager, and then click Configuration Manager Console.

The Configuration Manager Console starts.

1. In the Configuration Manager console, in the **Navigation** pane, click Monitoring.
2. In the **Monitoring** workspace, go to Overview / Reporting / Reports.
3. In the preview pane, click the Category column heading.

The reports are now sorted by the value in the Category column.

1. In the preview pane, scroll down until you can see the list of reports that belong to the Compliance and Settings Management – Compliance category.

The reports in the Compliance and Settings Management – Compliance category all relate to the desired configuration management feature in Configuration Manager 2012.

1. In the preview pane, click List of assets by compliance state for a configuration baseline.
2. On the ribbon, on the Home tab, in the Report Group group, click Run.

The List of assets by compliance state for a configuration baseline report opens.

1. Run the List of assets by compliance state for a configuration baseline report by performing the following steps:
2. In Configuration Baseline Name, click Values.

The Parameter Value dialog box appears.

1. In the Parameter Value dialog box, click Copy of WS2008R2SP1 Domain Security Compliance, and then click OK.
2. Click View Report.

The report is displayed and shows the list of computers in the device collection you created earlier in the process.

1. View the compliance state of each device as displayed in the Compliance State column in the report.

Currently all computers have a compliance state of Non-Compliant because the account lock configuration setting does not match the baseline settings.

1. Close all open windows and dialog boxes.

## Step 4-5: Request an IT GRC Management Program Exception

Exception management is essential to managing an IT GRC management program. In some instances, assessments, alerts, or incidents reveal evidence of non-compliance related to specific technologies or services. However, it is not always possible or economical to immediately remediate discovered issues.

In these instances, the decisions and ensuing activities are documented as an exception to the IT GRC compliance management program. Exception management provides for the creation, approval, constraint definition, execution, and tracking of justifiable exceptions to control and asset applicability.

The Process Pack for IT GRC supports the following types of exceptions:

* Control activity scope exceptions. This type of exception allows a user to exclude specific control activities from being included in compliance scoring.

For example, an IT pro manages a line of business applications that does not support passwords greater than six characters. The organization’s configuration policy requires all passwords to be a minimum of eight characters. The application is slated to be retired within the next six months, but it is undesirable for the computers running the application to be on the non-compliance reports for the next six months. The IT pro requests an exception for the computers running the application so that they will be noted on future reports but not negatively impact compliance reporting until the application is retired. The exception will include any control activities that require a password greater than eight characters.

* IT GRC program scope exceptions. This type of exception excludes specific computers from within the scope of an IT GRC program.

For example, an IT pro discovers that four virtual machines in a test environment were incorrectly included in the scope of their PCI audit management program, which has been running for seven months. Because the virtual machines do not have any actual production or sensitive data on them, the virtual machines should never have been included in the program scope. To resolve this problem, the IT Pro requests an exception, which will exclude the four virtual machines when scoring the PCI Audit program and to properly notate the audit reports. The exception will include all control activities for these four virtual machines.

* GRC policy exceptions. This type of exception excludes control activities that are not applicable to the organization.

For example, a program implementer looks at a compliance report for a PCI audit management program and discovers that one of the control activities has only failing results. After reviewing the control activity, the program implementer determines that the control activity was incorrectly added to the program and is testing a requirement that does not apply to the organization. The program implementer requests an exception to exclude this control activity from all future compliance reports for the remainder of the audit year.

After the exception has been submitted, it must be approved using Service Manager Work Item Review Activity. After approval, the exception will be applied to the IT GRC scoring.

In this example, Contoso inadvertently added the Service Manager 2012 data warehouse management server (SM-2012-02) to the program scope. In this step, you will request an IT GRC management program exception to exclude the Service Manager 2012 data warehouse management server (SM-2012-02).

 To request an IT GRC management program exception

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.
2. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items / Program Management / All Programs location.
3. In the Results pane, click Credit Card Processing Compliance Program (PCI DSS).
4. In the Tasks pane, click Request for Exception.

The Exception EX<id> - - New form opens (where id is the automatically generated exception identifier).

1. In the Exception EX<id> - - New form, perform the following steps and then click OK:
2. In Title, type SM-2012-02 Incorrectly Added to Program Scope.
3. In Description, type Service Manager 2012 data warehouse management server (SM-2012-02) was inadvertently added to the program scope and should not be included as a part of the compliance assessment.
4. In Requested Start Date, select <start\_date> (where start\_date is the date one month ago).
5. In Requested End Date, select <end\_date> (where end\_date is the date one year from now).
6. In Approver, type CORP\Administrator.
7. In Affected Configuration Items, click Add.

The Select objects dialog box opens.

1. In the Select objects dialog box, in the drop-down list box in the filter, select Device, click SM-2012-02, click Add, and then click OK.

SM-2012-02 appears in the Affected Configuration Items list box.

The Exception EX<id> - - New form closes.

1. In the Compliance and Risk pane, go to the All Compliance and Risk Items / Exception Management / All Exceptions location.
2. In the Results pane, click SM-2012-02 Incorrectly Added to Program Scope.
3. In the Tasks pane, click Request for Approval.

The Request for Approval dialog box opens, confirming that you want to request approval for the exception.

1. In the Request for Approval dialog box, click Yes.

The Request for Approval dialog box opens, notifying you that the exception was submitted.

1. In the Request for Approval dialog box, click OK.

 To approve the IT GRC management program exception

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Work Items.
2. In the Work Items pane, go to the Work Items / Activity Management / Review Activities/ All Activities location.
3. In the Results pane, click New Exception Approval: EX<id>: SM-2012-02 Incorrectly Added to Program Scope: Review Activity form opens (where id is the automatically generated exception identifier).
4. In the Tasks pane, click Approve.

The Comments dialog box appears.

1. In the Comments dialog box, in Comments, type Consensus is that SM-2012-02 was incorrectly added to the program scope for the Credit Card Processing Compliance Program (PCI DSS) program and should be allowed as an exception, and then click OK.
2. In the Work Items pane, go to the Work Items / Activity Management / Review Activities/ Approved Activities location.
3. In the Tasks pane, click Refresh.

The New Exception Approval: EX<id>: SM-2012-02 Incorrectly Added to Program Scope: Review Activity activity appears in the list of approved activities.

1. Close all open windows and dialog boxes.

## Step 4-6: Verify Compliance Status Using Process Pack for IT GRC Reports

The Process Pack for IT GRC includes reports that can be used for viewing compliance status. You can run these reports within the Service Manager Console. The reports can be used for viewing compliance scoring and determining the progress of the IT GRC management program.

To verify compliance status using Process Pack for IT GRC reports



1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the Navigation pane, click Reporting.
2. In the Reporting pane, go to the Reports / Compliance Reports Library / Control Management location.
3. In the Results pane, click Managed Entity Result List Report.
4. In the Tasks pane, click Run Report.

The Managed Entity Result List Report opens.

1. In the Managed Entity Result List Report, in Select Program click Add.

The Select dimension object dialog box opens.

1. In the Select dimension object dialog box, click the **Search** button, click **Credit Card Processing Compliance Program (PCI DSS)**, and then click **OK**.
2. In the Tasks pane, click Run Report.

The report is generated and the output is displayed.

1. Review the values in the Result column.

The values in the Result column for each computer should correlate to the status you saw in the report you ran in Configuration Manager 2012 earlier in the process.

1. Close all open windows and dialog boxes.

# 

# Appendix A: Compliance and GRC Program Overview

Compliance is the final step in the governance, risk management, and compliance (GRC) process. GRC helps organizations to identify risks, mitigate those risks, and verify that the risks continue being mitigated over time. Centralization of auditing systems helps to manage GRC efforts. Centralization of auditing systems also improves the efficiency of compliance auditing. These techniques will lower auditing costs and minimize disruption to daily operations.

## Governance in the GRC Process

Governance consists of the actions taken to address the risks identified during the risk assessment. Governance occurs when both automated and manual policies, methods, tasks, practices, systems, and training are put into place to mitigate identified risks. To enact governance, organizations design controls that include control objectives and activities.

The following activities are examples of how to apply governance to protect sensitive data:

* Create policies that describe proper handling of sensitive data.
* Train employees on data handling policies.
* Apply policies to systems that store sensitive data.
* Monitor and log handling of sensitive data to ensure that policies are followed.

## Risk Management in the GRC Process

Risk management is a program to mitigate or remove risks. It starts with an assessment of each area of an organization to determine where risks may exist. Each department, such as security, operations, sales, and development, can perform its own risk assessments. To begin with, organizations should work with a compliance auditor to perform a risk assessment of their organization. After risks are identified, they should be prioritized, and an action plan should be put into place that is based on those priorities.

A risk action plan should consider techniques to manage risk that fall into one or more of the following categories:

| Technique | Description |
| --- | --- |
| Avoidance | This technique eliminates the risk by withdrawing from or not becoming involved with the action that would incur the risk. |
| Reduction | This technique mitigates or optimizes the risk through preemptive actions. |
| Sharing | This technique shares the risk with other entities by transferring the risk, outsourcing the risk, or insuring against the risk. |
| Retention | This technique accepts the risk and provides appropriated budget for resolving the risk. |

The risk management plan should prioritize each risk and then determine how each risk will be addressed: Should the risk be ignored, mitigated, or avoided?

Organizations are often concerned with risks that may be addressed through aspects of information technology management, including data input, data output and data access management. The following types of risks often concern business organizations:

* Compliance risks. Risks that the organization may incur by not adhering to appropriate statues and regulations.
* Operational or transaction risks. Risks that the organization may incur that are associated with the delivery of products and services.
* Litigation risks. Risks associated with real or threatened litigation.
* Reputation risks. Risks associated with financial loss as a result of damage to an organization’s reputation.

The following are examples of how to address the risk involved with storing credit card information for each of the risk plan techniques:

* Avoidance. Don’t collect credit card information.
* Reduction. Mitigate the risk by improving protection of credit card information.
* Sharing. Outsource part of the risk by obtaining a qualified vendor to handle the credit card information.
* Retention. Ignore the risk and do not improve protection of credit card data. Instead, choose to accept losses if the credit card information is compromised.

## Compliance in the GRC Process

Compliance is the validation that identified risks are being mitigated (lowered or lessened) through operational tasks that are also called *controls*. The following are examples of how risks can be validated:

* For each identified risk, is there a policy in place for avoiding or mitigating the risk?
* Have the appropriate people been informed of the policies?
* Have the policies been deployed via processes, software, or IT controls?
* Are policies being monitored to ensure compliance, and when breaches in policy occur are they quickly remediated?

For true compliance, each step must be verifiable by an auditor. Such verification is often achieved through audit reports, event logs, video tapes, and version history.

The following are examples of how to verify compliance:

* Show that policies have been developed to address identified risks.
* Show that policies have been deployed where appropriate.
* Prove that policies have been in place and followed during the enforcement period.

## A GRC Example: Protecting Building Access

Consider an example of how you could apply GRC guidelines to assessing the need for protecting building access. The first step is to determine the risk and the risk tolerance, then to identify the governance methods (also known as control objectives and control activities) which offset the risk, and finally to validate that the actual tools and tasks in place are in compliance with governance and manage and reduce risk. These steps are detailed in the following table.

| Component | Description |
| --- | --- |
| Risk assessment | While performing a risk assessment of the building, you might determine that a security policy is necessary to reduce the risk of loss of computer and office equipment, personal items, and intellectual property due to theft. There could also be a risk to employees from attack or robbery. The building itself could be vandalized. Any of these risks could negatively affect an organization’s bottom line if they were to materialize. |
| Governance | After the assessment is completed, a set of policies and processes are defined and prioritized for implementation. Policies are created on proper building access and the protection of entryways. Training is provided to employees on these policies. Electronic locks are placed on doors that can only be opened with employee badges. Badges are assigned to employees, limiting their access to buildings based on need. Cameras and guards are placed at vulnerable locations to help enforce policies. |
| Compliance | To validate compliance with the organization’s access policies to management or for the purposes of an audit, the entrance logs can be reviewed to show that the logs are properly collecting data and the employees listed in the logs had a legitimate need to access the building. The tapes from the camera can be reviewed to ensure that employees were following access policies and that non-employees were not getting into the building. In addition, an auditor could interview guards and read past news reports to validate that incidents involving the building had not occurred. |

## Process Pack for IT GRC Terms and Concepts

For this evaluation guide you will implement an IT GRC management program (or compliance program) for a fictitious company, Contoso. To obtain the full benefit of the evaluation guide, familiarize yourself with the following terminology and taxonomy:

* Compliance program. Within GRC, a logical grouping of managed entities, IT controls, risks, and policies created to manage compliance efforts for a particular authority document. IT GRC programs:
* Define a collection of risks, control objectives, control activities, and compliance results. These collections allow the IT GRC program manager to manage the risks and controls specifically for a program.
* Define user roles and rights by establishing user permissions in the program. This approach allows delegation of tasks based on user roles within the program, and prohibits unauthorized review of control status within the program.
* Is used to manage compliance efforts for a particular scope. Program scope is the managed resources defined within a program (for example, servers, clients, services, and administrators.)
* Internal control. An accounting or system procedure designed to promote efficiency, or assure the implementation of a policy, or safeguard assets or avoid fraud and error.
* Authority document. The primary source of requirements, including regulations, standards, and policies; these documents are referenced within GRC. Authority documents are often produced by government regulating bodies, industry groups that create guidelines that meet regulating body expectations, and industry groups that create guidelines and standards in an effort to self-regulate companies that operate within the industry.

GRC authority documents contain expectations as written by an authority, such as a government entity, a standards body, or an organization’s written policy. A GRC authority document may contain risk mitigation requirements that stipulate specific or generalized configuration, operation, or other service parameters that apply to an organization, its personnel, its business processes, and its technologies.

Many types of authority documents exist, including the following examples:

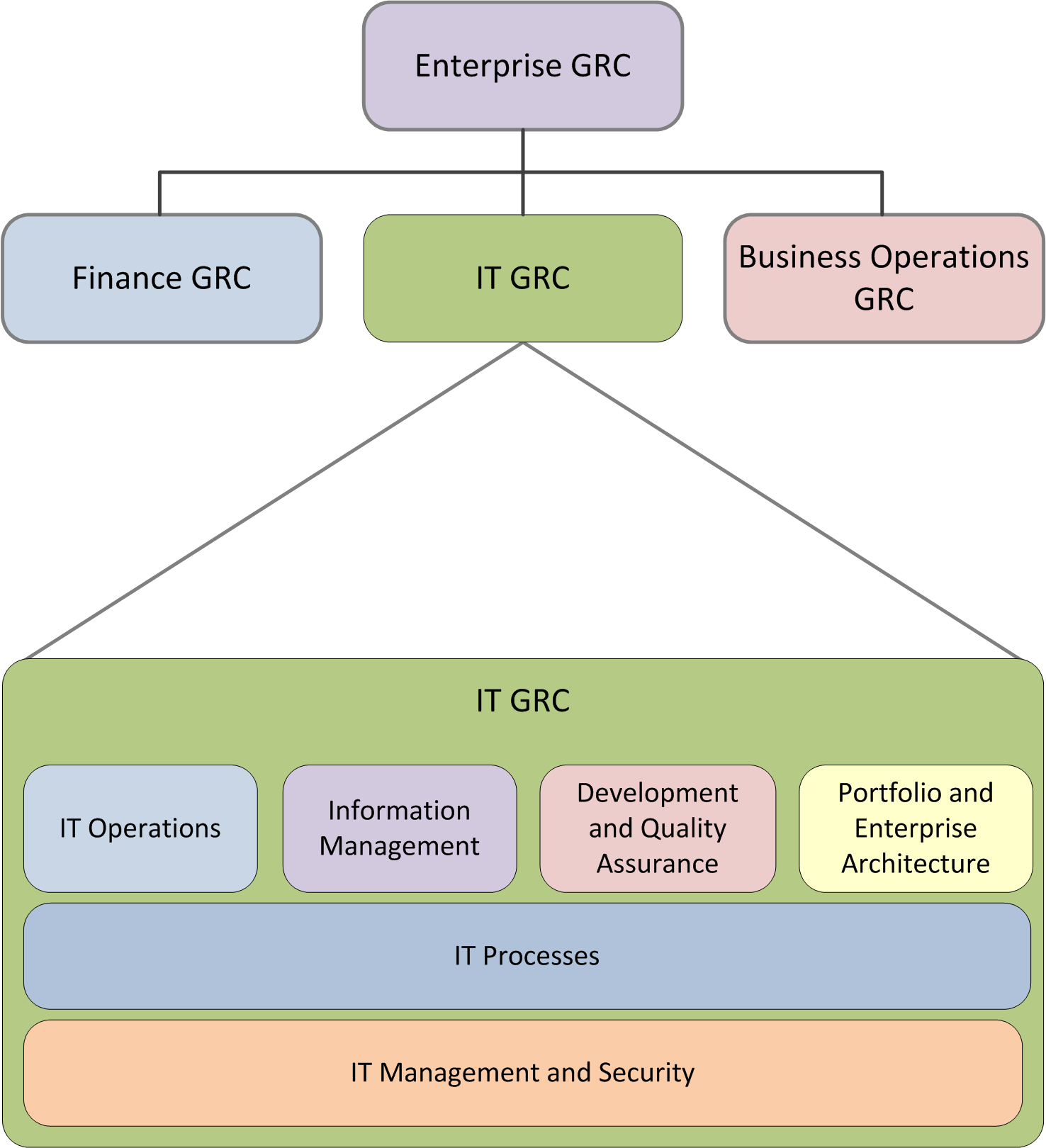
* Sarbanes Oxley Act of 2002 (SOX). SOX is a law that requires enhanced corporate responsibility and disclosures; it is enforced by the Security and Exchange Commission (SEC) and related bodies. The SEC enforces laws that regulate investor information with regard to securities information for publicly traded companies. Laws such as the Securities Act of 1933 require publicly traded companies to produce and distribute financial statements. Financial statements are produced in accordance with industry standards, including Generally Accepted Accounting Principles (GAAP).
* Payment Card Industry (PCI). Created by the Payment Card Industry Security Standards Council to enhance and regulate payment card data security. Payment cards are issued by companies such as Visa and MasterCard. PCI is an industry self-regulating standard by which organizations that process credit card transactions must adhere to internal control frameworks and specifications to ensure safe handling of cardholder information.
* Health Insurance Portability and Accountability Act (HIPAA). A law enacted by Congress in 1996 that protects workers health insurance coverage. This law also establishes national standards for electronic transactions processed by healthcare providers (including doctors and hospitals), insurance plans, and employers. The standards address the security and privacy of health data.
* Framework. Within a program, a framework is a way of classifying, grouping, and displaying controls.
* Risk. A specific, unrealized, but potential harm that could adversely affect an organization’s business objectives. As a result of risk, an organization might incur costs or might fail to attain a potential benefit. Risk is measured in terms of impact and probability. Risks may be associated with control objectives, control activities, or other risks.
* Control objective. A description of the specific results that should be achieved to manage risks identified through the risk assessment. An objective is a description of the desired state. The control objective can be identified as a harmonized statement of authority document requirements that must be achieved.
* Control activity. A task performed with the clear intention of satisfying a desired control objective. It often takes the form of prescriptive guidance that details the required implementation needed to satisfy an objective on a specific platform.
* Automated control activity. Automated control activities use Microsoft System Center Configuration Manager to validate configuration settings against predefined baselines. The results from Configuration Manager (and any threshold defined in the program or in the control activity form) are used to determine the control activity’s compliance.
* Manual control activity. Manual control activities require users to manually assert the result of the activity. An individual will use forms and screens to manually enter the activity information into the program.
* Control categories. Control objectives and control activities that affect similar information technology operations and are grouped together to clearly manage the control environment.
* Control sub-categories. A lower level of category (grouping of individual control objectives) that helps organize the information in a meaningful way.

The following are examples of control categories and objectives:

* Control category: identity and access management
* Control sub-category: access management
* Control objective: security requires a complex password
* Control activity: password complexity is configured to require all users to include alpha and numeric characters.
* Control test automation. The Process Pack for IT GRC uses the Desired Configuration Management feature in Configuration Manager along with supplied product specific baselines to enable control test automation. The Configuration Manager connector in Service Manager 2012 populates the Service Manager data warehouse database with control test results, which are processed for validation against compliance objectives.
* Threshold. The minimum percentage of applicable managed entities in the program scope that must be compliant for a control activity to be considered compliant.

## Process Pack for IT GRC Description

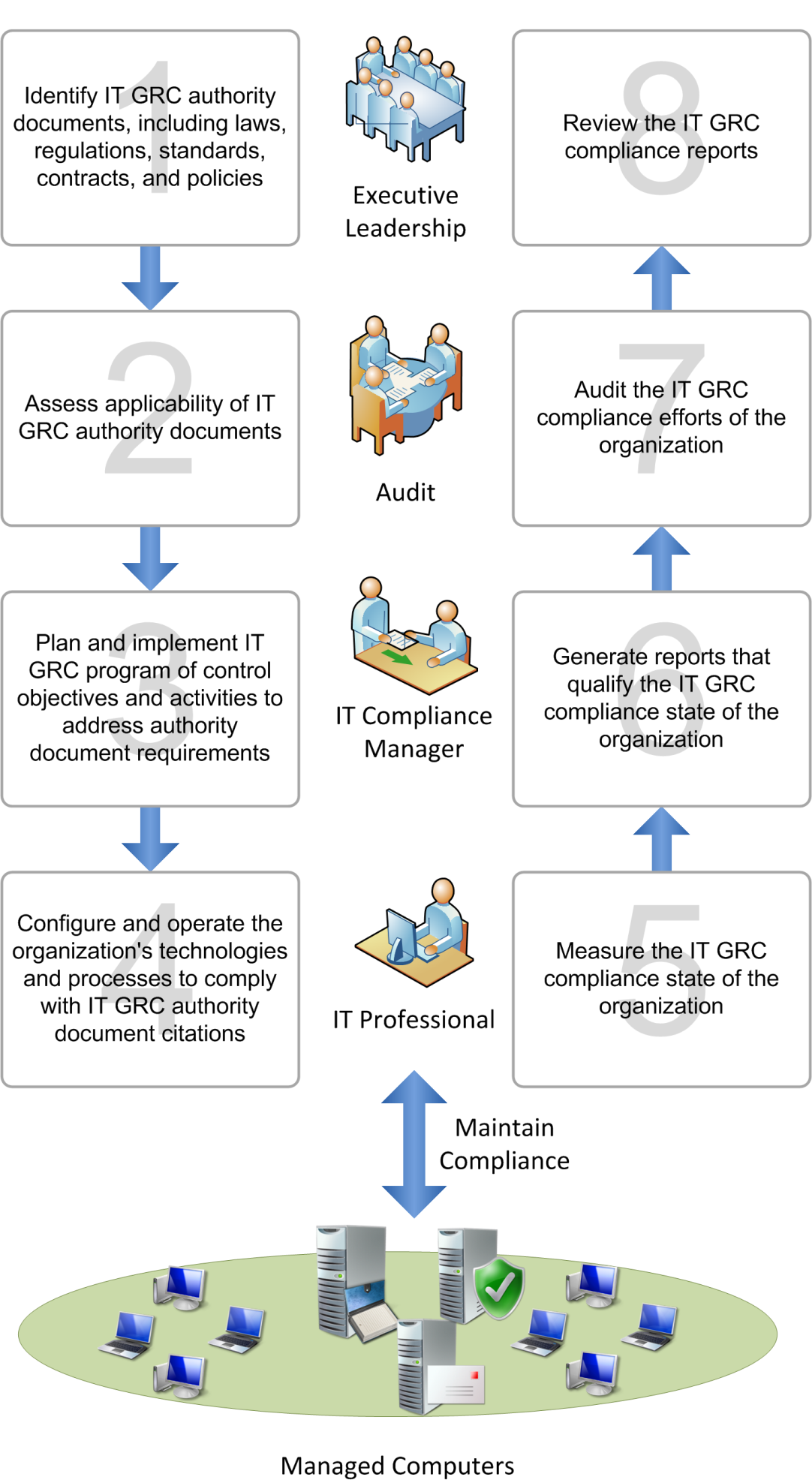
The Process Pack for IT GRC provides automated compliance management for client and server computers. The following diagram illustrates how IT GRC fits within an enterprise GRC framework. Note the Process Pack for IT GRC focuses solely on IT GRC and not on other aspects of the enterprise GRC (such as financial and accounting or business operations).



## Roles within an IT GRC Program

Within any organization there are individuals who manage GRC-specific programs, information, and distribution of information. In creating an IT GRC program, you should be aware of the human resources (roles) that support the IT GRC program.

GRC-specific information is used to support business operations as well as internal and external audits. Most of the information captured is confidential and may be used for internal and external reporting. With the Process Pack for IT GRC, role–based access is configured to include the basic roles for individuals within an organization who define and work with an IT GRC program, as illustrated in the following figure.



Define the roles in the following table by first identifying the enterprise-specific function and daily tasks they may perform and then by identifying the Process Pack for IT GRC security role that may be assigned to the enterprise specific functional role. You should have an idea of the individual roles and should be able to help identify where access and information is designated to a specific role type. The following table includes examples of enterprise main roles and Process Pack for IT GRC roles within the team of individuals who use, implement, and work with an IT GRC program.

| Job Title | Responsibility | Process Pack for IT GRC Role |
| --- | --- | --- |
| IT Professionals | * Configure and manage Service Manager 2012 * Configure Process Pack for IT GRC * Manage computers for compliance | * Service Manager Administrators * Domain Admins * Compliance Program Implementer |
| IT Compliance Manager | * Define IT GRC programs * Work with auditors, business management, and staff to define correct compliance controls and activities | * Compliance Program Manager * Author |
| Audit | * Execute and manage IT GRC programs * Manage pre-audit and audit activities and compliance-related tasks | Compliance Program Manager |
| Business Management | * Execute tasks within business operations that support control objectives and activities * Gather and submit information related to the performance and results of control activities | Compliance Program Manager |
| Executive Leadership | * Identify regulatory and industry standards * Review and approve the results of compliance programs | None (these users generally receive reports) |

# 

# Appendix B: Prepare SM-2012-01 Computer

For purposes of this guide, Service Manager 2012 management server runs on the computer named SM-2012-01. Install the prerequisite software, server roles, and services on this computer.

Note

This section assumes that you are creating a new Service Manager 2012 infrastructure. If you are using an existing Service Manager 2012 infrastructure, review the steps in this section and substitute existing resource names for the resources created in this section (such as the computer name and shared network folders).

Prepare the SM-2012-01 computer for use by performing the following steps:

[Step B-1: Review System Prerequisites](#_Step_B-1:_Review)

[Step B-2: Install Windows Server 2008 R2](#_Step_B-2:_Install)

[Step B-3: Install the AD DS Server Role](#_Step_B-3:_Install)

[Step B-4: Install the Web Services (IIS) Server Role](#_Step_B-4:_Install)

[Step B-5: Add the Required Windows Server 2008 R2 Features](#_Step__B-5:)

[Step B-6: Create the Required User and Service Accounts](#_Step_B-6:_Create)

[Step B-7: Install SQL Server 2008 R2](#_Step_B-7:_Install)

[Step B-8: Install Service Manager 2012](#_Step_B-8:_Install)

[Step B-9: Install Microsoft Office Excel 2010](#_Step_B-9:_Install)

## Step B-1: Review System Prerequisites

The SM-2012-01 computer runs Service Manager 2012 and SQL Server 2008 R2. The computer runs the Windows Server 2008 R2 operating system with Service Pack 1 and the following server roles installed:

* Active Directory Domain Services (AD DS)
* Web Server

The system resources of the computer are as follows:

* Dual quad-core processor running at 2.66 (GHz) or faster
* 8 gigabytes (GB) or more of physical memory
* One disk partition that has 100 GB or more of available disk space; it will become the drive C partition
* One CD-ROM or DVD-ROM drive that will be assigned the drive letter D

## Step B-2: Install Windows Server 2008 R2

Use the information in the following table to install Windows Server 2008 R2 with Service Pack 1. Accept default values unless otherwise specified.

Note

For information on the permissions required to setup the Service Manager server, the data warehouse server, and SQL Server Reporting services see the “[Account Used for Running Setup](http://technet.microsoft.com/en-us/library/hh495629.aspx)” topic in System Center TechCenter on Microsoft TechNet.

| When prompted for | Provide these values |
| --- | --- |
| Where do you want to install Windows? | Disk 0 Unallocated Space |
| Password | Any strong password |
| Computer name | SM-2012-01 |
| Format for volumes C and E | NTFS |
| TCP/IP configuration | Configure with a static IP address configuration, with the other TCP/IP configuration options as appropriate for the environment. |

## Step B-3: Install the AD DS Server Role

AD DS is required to provide authentication and act as a repository for configuration values for the Microsoft products and technologies, such as Microsoft SQL Server 2008 R2, Service Manager 2012, Configuration Manager 2012, and Operations Manager 2012.

To install AD DS, add the Active Directory Domain Services server role and then run the DCPROMO Wizard to configure the computer as a domain controller. Install AD DS using the information in the following table, accepting any defaults unless otherwise specified.

| When prompted | Do this |
| --- | --- |
| For the domain type | Create a new domain in a new forest. |
| For the fully qualified domain name (FQDN) | Type corp.contsoso.com. |
| For the forest functional level | Select Windows Server 2008 R2. |
| To install the DNS Server service as part of the domain controller installation process | Click Yes. |

## Step B-4: Install the Web Services (IIS) Server Role

Install the Web Services (IIS) server role with the role services listed in the following table, which are required for SQL Server 2008 R2 and Service Manager 2012. Unless otherwise specified, use the default values.

| Role service | Status |
| --- | --- |
| Web Server | Installed |
| Common HTTP Features | Installed |
| Static Content | Installed |
| Default Document | Installed |
| Directory Browsing | Installed |
| HTTP Errors | Installed |
| HTTP Redirection | Installed |
| WebDAV Publishing | Installed |
| Application Development | Installed |
| ASP.NET | Installed |
| .NET Extensibility | Installed |
| ASP | Not installed |
| CGI | Not installed |
| ISAPI Extensions | Installed |
| ISAPI Filters | Installed |
| Server Side Includes | Not installed |
| Health and Diagnostics | Installed |
| HTTP Logging | Installed |
| Logging Tools | Installed |
| Request Monitor | Installed |
| Tracing | Installed |
| Custom Logging | Not installed |
| ODBC Logging | Not installed |
| Security | Installed |
| Basic Authentication | Not installed |
| Windows Authentication | Installed |
| Digest Authentication | Not installed |
| Client Certificate Mapping Authentication | Not installed |
| IIS Client Certificate Mapping Authentication | Not installed |
| URL Authorization | Not installed |
| Request Filtering | Installed |
| IP and Domain Restriction | Not installed |
| Performance | Installed |
| Static Content Compression | Installed |
| Dynamic Content Compression | Not installed |
| Management Tools | Installed |
| IIS Management Console | Installed |
| IIS Management Scripts and Tools | Not installed |
| Management Service | Not installed |
| IIS 6 Management Compatibility | Installed |
| IIS 6 Metabase Compatibility | Installed |
| IIS 6 WMI Compatibility | Installed |
| IIS 6 Scripting Tools | Not installed |
| IIS 6 Management Console | Not installed |
| FTP Publishing Service | Not installed |
| FTP Server | Not installed |
| FTP Management Console | Not installed |
| IIS Hostable Web Core | Not installed |

## Step B-5: Add the Required Windows Server 2008 R2 Features

In addition to installing the required Windows Server 2008 R2 server roles, add the following required features in Server Manager in the Features Summary section:

* Background Intelligent Transfer Service (BITS)
* Remote Differential Compression

## Step B-6: Create the Required User and Service Accounts

Service Manager 2012 and SQL Server 2008 R2 require user accounts during the installation process. The following table lists the information needed to create these accounts.

| Create this account | With these settings |
| --- | --- |
| SQL Server Agent service account | 1. In First name, type SQL Agent. 2. In Last name, type Service Account. 3. In User logon name, type SQLAgent. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. Make the account a member of the Domain Admins security group. 8. In Description, type Service account used to run SQL Server 2008 R2Agent service. |
| SQL Server Database Engine service account | 1. In First name, type SQL DB Engine. 2. In Last name, type Service Account. 3. In User logon name, type SQLDBEngine. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. Make the account a member of the Domain Admins security group. 8. In Description, type Service account used to run SQL Server 2008 R2 database engine. |
| SQL Server Reporting Services service account | 1. In First name, type SQL Reporting. 2. In Last name, type Service Account. 3. In User logon name, type SQLReport. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. Make the account a member of the Domain Admins security group. 8. In Description, type Service account used to run SQL Server 2008 R2 reporting services. |
| SQL Server Analysis Services service account | 1. In First name, type SQL Analysis. 2. In Last name, type Service Account. 3. In User logon name, type SQLAnalysis. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. Make the account a member of the Domain Admins security group. 8. In Description, type Service account used to run SQL Server 2008 R2 analysis services. |
| Service Manager management group administrators | 1. In First name, type Service Manager. 2. In Last name, type Management Group Admin. 3. In User logon name, type SMMgtGrpAdmin. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. Make the account a member of the Domain Admins security group. 8. In Description, type Account that is able to administer the Service Manager management group. |
| Service Manager services account | 1. In First name, type Service Manager. 2. In Last name, type Services Account. 3. In User logon name, type SMSvcsAcct. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. Make the account a member of the Domain Admins security group. 8. In Description, type Service account used to run the Service Manager services. |
| Service Manager workflow account | 1. In First name, type Service Manager. 2. In Last name, type Workflow Account. 3. In User logon name, type SMWorkflow. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. Make the account a member of the Domain Admins security group. 8. In Description, type Service account used to run Service Manager workflows. |
| User account that will be assigned the Compliance Program Implementer user role | 1. In First name, type Pilar. 2. In Last name, type Ackerman. 3. In User logon name, type PilarA. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. Make the account a member of the Domain Admins security group. 8. In Description, type User account that will be made assigned the Compliance Program Implementer user role in the Process Pack for IT GRC. |
| User account that will be assigned the Compliance Program Implementer user role | 1. In First name, type Pilar. 2. In Last name, type Ackerman. 3. In User logon name, type PilarA. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. Make the account a member of the Domain Admins security group. 8. In Description, type User account that will be made assigned the Compliance Program Implementer user role in the Process Pack for IT GRC. |

## Step B-7: Install SQL Server 2008 R2

Before installing Service Manager 2012, install SQL Server 2008 R2.

Note

To enable all SQL Server 2008 R2 features, install the Web Services (IIS) server role before installing SQL Server 2008 R2.

To install SQL Server 2008 R2

1. Start the SQL Server Installation Center.
2. In the SQL Server Installation Center, in the navigation pane, click Installation.
3. In the details pane, click New installation or add features to an existing installation.

The SQL Server 2008 R2 Setup Wizard starts.

1. Install SQL Server 2008 R2 using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Setup Support Rules | Click OK. |
| Product Key | Click Next. |
| License Terms | 1. Select the I accept the license terms check box. 2. Click Next. |
| Setup Support Files | Click Install. |
| Setup Support Rules | 1. Ensure no critical results exist for the rules. 2. Click Next. |
| Setup Role | 1. Click SQL Server Feature Installation. 2. Click Next. |
| Feature Selection | 1. Select Database Engine Services check box. 2. Select Full-Text Search check box. 3. Select Management Tools - Complete check box. 4. Click Next. |
| Installation Rules | Click Next. |
| Instance Configuration | Click Next. |
| Disk Space Requirements | Click Next. |
| Server Configuration | 1. For SQL Server Agent, in Account Name, type CORP\SQLAgent, in Password, type P@ssw0rd. 2. For SQL Server Database Engine, in Account Name, type CORP\SQLDBEngine, in Password, type P@ssw0rd. 3. For SQL Server Reporting Services, in Account Name, type CORP\SQLReport, in Password, type P@ssw0rd. 4. Click Next. |
| Database Engine Configuration | 1. Click Add Current User. 2. Click Next. |
| Error Reporting | Click Next. |
| Installation Configuration Rules | Click Next. |
| Ready to Install | Click Install. |
| Complete | Click Close. |

1. Close the SQL Server Installation Center.
2. Install any updates, service packs, or hotfixes.

To configure Windows Firewall for SQL Server 2008 R2 access

1. Click Start, click Administrative Tools, and then click Windows Firewall with Advanced Security.
2. In the console tree, click Inbound Rules.
3. In the Actions pane, click New Rule.

The New Inbound Rule Wizard starts.

1. Complete the New Inbound Rule Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Rule Type | Click Port and then click Next. |
| Protocols and Ports | 1. Click TCP. 2. Click Specific local ports. 3. In Specific local ports, type 1433. 4. Click Next. |
| Action | Click Next. |
| Profile | Click Next. |
| Name | 1. In Name, type SQL Server Database Engine (TCP-In). 2. In Description, type Rule to allow inbound access to SQL Server database engine. 3. Click Finish. |

1. Close all open windows and dialog boxes.

## Step B-8: Install Service Manager 2012

When the other products and technologies have been installed, install Service Manager 2012. The configuration of SM-2012-01 supports Service Manager 2012 for this sample. The configuration of computers in the production network may vary. To find out more about the prerequisites for installing Service Manager 2012, see [System Requirements for System Center 2012 - Service Manager](http://technet.microsoft.com/en-us/library/hh519636.aspx).

To install Service Manager 2012

1. Start the System Center 2012 - Service Manager installation.
2. On the System Center 2012 - Service Manager splash screen, click the Install a Service Manager management server hyperlink.

The Service Manager Setup Wizard starts.

1. Complete the Service Manager Setup Wizard using the information in the following table. Accept the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Product registration | 1. In Name, type Contoso IT. 2. In Organization, type Contoso Ltd. 3. In Product key, type product\_key (where product\_key is the Service Manager 2012 product key). 4. Review the License terms. 5. Select the I have read, understood, and agree with the terms of the license terms check box. 6. Click Next. |
| Installation location | Click Next. |
| System check results | 1. Review the system check results and ensure that no critical problems are found. 2. Click Next. |
| Configure the Service Manager database | Click Next. |
| Configure the Service Manager management group | 1. In Management group name, type SM New York City. 2. Click Browse.   The Select User or Group dialog box appears.   1. In the Select User or Group dialog box, type SMMgtGrpAdmin, click Check Names, and then click OK. 2. Click Next. |
| Configure the account for Service Manager services | 1. Click Domain account. 2. In User name, type SMSvcsAcct. 3. In Password, type P@ssw0rd. 4. In Domain, select CORP. 5. Click Test Credentials. 6. Click Next. |
| Configure the Service Manager workflow account | 1. Click Domain account. 2. In User name, type SMWorkflow. 3. In Password, type P@ssw0rd. 4. In Domain, select CORP. 5. Click Test Credentials. 6. Click Next. |
| Help improve System Center Service Manager | 1. Select the appropriate option based on your desire to participate in the Customer Experience Improvement Program 2. Click Next. |
| Installation summary | Click Install. |
| Installing Service Manager management server | Monitor the progress of the Service Manager management server installation. |
| Setup completed successfully | 1. Review the status of the setup process. 2. Clear the Open the Encryption Backup or Restore Wizard after Setup closes check box. 3. Click Close. |

1. Close all open windows and dialog boxes.

When the wizard is complete, the Service Manager 2012 management server is installed.

## Step B-9: Install Microsoft Office Excel 2010

The Process Pack for IT GRC Client uses Microsoft Office Excel 2010. Install Microsoft Office Excel 2010 as a prerequisite for the Process Pack for IT GRC Client, which will be installed in [Step 2-6: Install the Process Pack for IT GRC Client Prerequisites](#_Step_2-6:_Install). You can install other Office 2010 applications, such as Microsoft Office Word 2010, at the same time, but they are not required to complete this evaluation guide.

Install the 32-bit version of Office Excel 2010 using the default installation options.

Note

This guide assumes you are installing the 32-bit version of Office Excel 2010.

# 

# Appendix C: Prepare SM-2012-02 Computer

For purposes of this guide, System Center 2012 - Service Manager data warehouse runs on the computer named SM-2012-02. Install the prerequisite software, server roles, and services on this computer.

Note

This section assumes that you are creating a new Service Manager 2012 infrastructure. If you are using an existing Service Manager 2012 infrastructure, review the steps in this section and substitute existing resource names for the resources created in this section (such as the computer name and shared network folders).

Prepare the SM-2012-02 computer for use by completing the following steps:

[Step C-1: Review System Prerequisites](#_Step_C-1:_Review)

[Step C-2: Install Windows Server 2008 R2](#_Step_C-2:_Install)

[Step C-3: Install the Web Services (IIS) Server Role](#_Step_C-3:_Install)

[Step C-4: Add the Required Windows Server 2008 R2 Features](#_Step_C-4:_Add)

[Step C-5: Create the Required User and Service Accounts](#_Step_C-5:_Create)

[Step C-6: Install SQL Server 2008 R2](#_Step_C-6:_Install)

[Step C-7: Install Service Manager 2012 Data Warehouse Server](#_Step_C-7:_Install)

## Step C-1: Review System Prerequisites

The SM-20120-02 computer runs Service Manager 2012 data warehouse and SQL Server 2008 R2 Reporting Services. The computer runs the Windows Server 2008 R2 operating system with Service Pack 1 and the following server roles installed:

* Web Server

The system resources of the computer are as follows:

* Dual quad-core processor running at 2.66 (GHz) or faster
* 8 gigabytes (GB) or more of physical memory
* One disk partition that has 100 GB or more of available disk space; it will become the drive C partition
* One CD-ROM or DVD-ROM drive that will be assigned the drive letter D

## Step C-2: Install Windows Server 2008 R2

Use the information in the following table to install Windows Server 2008 R2 with Service Pack 1 for SM-2012-02. Accept default values unless otherwise specified.

|  |  |
| --- | --- |
| When prompted for | Provide these values |
| Where you want to install Windows | Disk 0 Unallocated Space |
| Password | Any strong password |
| Computer name | SM-2012-02 |
| Format for volumes C and E | NTFS |
| TCP/IP configuration | Configure with a static IP address configuration, with other TCP/IP configuration options as appropriate for the environment. |
| Domain membership | Member server in corp.contoso.com domain. |

## Step C-3: Install the Web Services (IIS) Server Role

Install the Web Services (IIS) server role with the role services listed in the following table, which are required for SQL Server 2008 R2 Reporting Services and Service Manager 2012 data warehouse. Unless otherwise specified, use the default values.

| Role service | Status |
| --- | --- |
| Web Server | Installed |
| Common HTTP Features | Installed |
| Static Content | Installed |
| Default Document | Installed |
| Directory Browsing | Installed |
| HTTP Errors | Installed |
| HTTP Redirection | Installed |
| WebDAV Publishing | Installed |
| Application Development | Installed |
| ASP.NET | Installed |
| .NET Extensibility | Installed |
| ASP | Not installed |
| CGI | Not installed |
| ISAPI Extensions | Installed |
| ISAPI Filters | Installed |
| Server Side Includes | Not installed |
| Health and Diagnostics | Installed |
| HTTP Logging | Installed |
| Logging Tools | Installed |
| Request Monitor | Installed |
| Tracing | Installed |
| Custom Logging | Not installed |
| ODBC Logging | Not installed |
| Security | Installed |
| Basic Authentication | Not installed |
| Windows Authentication | Installed |
| Digest Authentication | Not installed |
| Client Certificate Mapping Authentication | Not installed |
| IIS Client Certificate Mapping Authentication | Not installed |
| URL Authorization | Not installed |
| Request Filtering | Installed |
| IP and Domain Restriction | Not installed |
| Performance | Installed |
| Static Content Compression | Installed |
| Dynamic Content Compression | Not installed |
| Management Tools | Installed |
| IIS Management Console | Installed |
| IIS Management Scripts and Tools | Not installed |
| Management Service | Not installed |
| IIS 6 Management Compatibility | Installed |
| IIS 6 Metabase Compatibility | Installed |
| IIS 6 WMI Compatibility | Installed |
| IIS 6 Scripting Tools | Not installed |
| IIS 6 Management Console | Not installed |
| FTP Publishing Service | Not installed |
| FTP Server | Not installed |
| FTP Management Console | Not installed |
| IIS Hostable Web Core | Not installed |

## Step C-4: Add the Required Windows Server 2008 R2 Features

In addition to installing the required Windows Server 2008 R2 server roles, add the following required features in Server Manager in the Features Summary section:

* .NET Framework 3.5.1

## Step C-5: Create the Required User and Service Accounts

Service Manager 2012 data warehouse requires user accounts during the installation process. The following table lists the information needed to create these accounts. SQL Server 2008 R2 Reporting Services will use user accounts that were created during the SM-2012-01 configuration process.

| Create this account | With these settings |
| --- | --- |
| Service Manager data warehouse management group administrators | 1. In First name, type SM Data Warehouse. 2. In Last name, type Management Group Admins. 3. In User logon name, type SMDWMgtGrpAdmin. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. Make the account a member of the Domain Admins security group. 8. In Description, type Account that is able to administer the Service Manager data warehouse management group. |
| Service Manager data warehouse run as account | 1. In First name, type SM Data Warehouse. 2. In Last name, type Service Account. 3. In User logon name, type SMDWRunAsAcct. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. Make the account a member of the Domain Admins security group. 8. In Description, type Service account used as the run as account for the Service Manager data warehouse. |
| Service Manager data warehouse reporting account | 1. In First name, type SM Data Warehouse. 2. In Last name, type Reporting Account. 3. In User logon name, type SMDWReporting. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. In Description, type Service account used by SQL Server Reporting Services to access the DWDataMart database. |
| Service Manager data warehouse analysis account | 1. In First name, type SM Data Warehouse. 2. In Last name, type Analysis Account. 3. In User logon name, type SMDWAnalysis. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. In Description, type Service account used by Service Manager to access the OLAP cubes provided by SQL Server Analysis Services. |

## Step C-6: Install SQL Server 2008 R2

Before installing Service Manager 2012 data warehouse, install SQL Server 2008 R2.

Note

To enable all SQL Server 2008 R2 features, install the Web Services (IIS) server role before installing SQL Server 2008 R2.

To install SQL Server 2008 R2

1. Start the SQL Server Installation Center.
2. In the SQL Server Installation Center, in the navigation pane, click Installation.
3. In the details pane, click New installation or add features to an existing installation.

SQL Server 2008 R2 Setup Wizard starts.

1. Install SQL Server 2008 R2 using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Setup Support Rules | Click OK. |
| Product Key | Click Next. |
| License Terms | 1. Select the I accept the license terms check box. 2. Click Next. |
| Setup Support Files | Click Install. |
| Setup Support Rules | 1. Ensure no critical results exist for the rules. 2. Click Next. |
| Setup Role | 1. Click SQL Server Feature Installation. 2. Click Next. |
| Feature Selection | 1. Select Database Engine Services check box. 2. Select Reporting Services check box. 3. Select Full-Text Search check box. 4. Select Analysis Services check box. 5. Select Reporting Services check box. 6. Select Management Tools - Complete check box. 7. Click Next. |
| Installation Rules | Click Next. |
| Instance Configuration | Click Next. |
| Disk Space Requirements | Click Next. |
| Server Configuration | 1. For SQL Server Agent, in Account Name, type CORP\SQLAgent, in Password, type P@ssw0rd. 2. For SQL Server Database Engine, in Account Name, type CORP\SQLDBEngine, in Password, type P@ssw0rd. 3. For SQL Server Analysis Services, in Account Name, type CORP\SQLAnalysis, in Password, type P@ssw0rd. 4. For SQL Server Reporting Services, in Account Name, type CORP\SQLReport, in Password, type P@ssw0rd. 5. Click Next. |
| Database Engine Configuration | 1. Click Add Current User. 2. Click Next. |
| Analysis Services Configuration | 1. Click Add Current User. 2. Click Next. |
| Reporting Services Configuration | Click Next. |
| Error Reporting | Click Next. |
| Installation Configuration Rules | Click Next. |
| Ready to Install | Click Install. |
| Complete | Click Close. |

1. Close the SQL Server Installation Center.

To install SQL Server 2008 R2 Service Pack 1

1. In Windows Explorer, go to target\_folder (where target\_folder is the name of the folder where SQL Server 2008 R2 SP1 is located).
2. In Windows Explorer, double-click SQLServer2008R2SP1-KB2528583-x64-ENU.exe

The **Extracting Files** dialog box appears. The service pack files are extracted to a local folder. After the files are extracted, the Microsoft SQL Server 2008 R2 Service Pack 1 setup wizard starts.

1. Install SQL Server 2008 R2 SP1 using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| SQL Server 2008 R2 update | Click Next. |
| License Terms | 1. Select the I accept the license terms check box. 2. Click Next. |
| Select Features | Click Next. |
| Check Files In Use | 1. Ensure no critical results exist. 2. Click Next. |
| Ready to update | 1. Verify the features to be updated are correct. 2. Click Update. |
| Update Progress | The progress is displayed for updating the SQL Server features. |
| Complete | Click Close. |

1. Install any additional updates or hotfixes.

To configure Windows Firewall for SQL Server 2008 R2 Access

1. Click Start, click Administrative Tools, and then click Windows Firewall with Advanced Security.
2. In the console tree, click Inbound Rules.
3. In the Actions pane, click New Rule.

The New Inbound Rule Wizard starts.

1. Complete the New Inbound Rule Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Rule Type | Click Port and then click Next. |
| Protocols and Ports | 1. Click TCP. 2. Click Specific local ports. 3. In Specific local ports, type 80. 4. Click Next. |
| Action | Click Next. |
| Profile | Click Next. |
| Name | 1. In Name, type SQL Server Reporting Services (TCP-In). 2. In Description, type Rule to allow inbound access to SQL Server Reporting Services. 3. Click Finish. |

1. In the Actions pane, click New Rule.

The New Inbound Rule Wizard starts.

1. Complete the New Inbound Rule Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Rule Type | Click Port and then click Next. |
| Protocols and Ports | 1. Click TCP. 2. Click Specific local ports. 3. In Specific local ports, type 1433. 4. Click Next. |
| Action | Click Next. |
| Profile | Click Next. |
| Name | 1. In Name, type SQL Server Database Engine (TCP-In). 2. In Description, type Rule to allow inbound access to SQL Server database engine. 3. Click Finish. |

1. Close all open windows and dialog boxes.

To configure SQL Server 2008 R2 Reporting Services

1. Click Start, click All Programs, click Microsoft SQL Server 2008 R2, click Configuration Tools, and then click Reporting Services Configuration Manager.

The **Reporting Services Configuration Connection** dialog box is displayed.

1. In the Reporting Services Configuration Connection dialog box, click Connect.

The Reporting Services Configuration Manager console is displayed.

1. In the Reporting Services Configuration Manager console, in the navigation pane, go to SM-2012-02\MSSQLSERVER / Web Service URL.
2. In the preview pane, click Apply.

The Web Service URL is configured. The results of the configuration process are displayed at the bottom of the preview pane.

1. In the Reporting Services Configuration Manager console, in the navigation pane, go to SM-2012-02\MSSQLSERVER / Database.
2. In the preview pane, click Change Database.

The Report Server Database Configuration Wizard starts.

1. Complete the Report Server Database Configuration Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Action | Click Next. |
| Database Server | 1. In Server Name, type SM-2012-02. 2. Click Test Connection.   The Test Connection dialog box appears.   1. In the Test Connection dialog box, click OK. 2. Click Next. |
| Database | Click Next. |
| Credentials | Click Next. |
| Summary | Click Next. |
| Progress and Finish | 1. Verify that no errors occur during the configuration process. 2. Click Finish. |

1. In the Reporting Services Configuration Manager console, in the navigation pane, go to SM-2012-02\MSSQLSERVER / Report Manager URL.
2. In the preview pane, click Apply.

The Report Manager URL is configured. The results of the configuration process are displayed at the bottom of the preview pane.

1. In the Reporting Services Configuration Manager console, in the navigation pane, go to SM-2012-02\MSSQLSERVER / Database.
2. In the preview pane, click Exit.

## Step C-7: Install Service Manager 2012 Data Warehouse Server

When the other products and technologies have been installed, install the Service Manager 2012 data warehouse management server. The configuration of SM-2012-02 supports the Service Manager 2012 data warehouse management server for this sample. The configuration of computers in the production network may vary.

To install the Service Manager 2012 data warehouse management server

1. Start the System Center 2012 - Service Manager installation.
2. On the System Center 2012 - Service Manager splash screen, click the Install a Service Manager data warehouse management server hyperlink.

The Service Manager Setup Wizard starts.

1. Complete the Service Manager Setup Wizard using the information in the following table. Accept the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Product registration | 1. In Name, type Contoso IT. 2. In Organization, type Contoso Ltd. 3. In Product key, type product\_key (where product\_key is the Service Manager 2012 product key). 4. Review the **License terms**. 5. Select the I have read, understood, and agree with the terms of the license terms check box. 6. Click Next. |
| Installation location | Click Next. |
| System check results | 1. Review the system check results and ensure that no critical problems are found. 2. Click Next. |
| **Configure the data warehouse** databases | 1. Click Staging and Configuration. 2. In Database Server, type SM-2012-02. 3. In SQL Server instance, select Default.   The Staging and Configuration and Repository data warehouse databases show positive status.   1. Click Data Mart. 2. In Database Server, type SM-2012-02. 3. In SQL Server instance, select Default.   The Data Mart data warehouse database shows positive status.   1. Click Next. |
| **Configure additional  data warehouse data marts** | 1. Click OM Data mart. 2. In Database Server, type SM-2012-02. 3. In SQL Server instance, select Default.   The OM Data mart data warehouse database shows positive status.   1. Click CM Data mart. 2. In Database Server, type SM-2012-02. 3. In SQL Server instance, select Default.   The CM Data mart data warehouse database shows positive status.   1. Click Next. |
| Configure the Service Manager management group | 1. In Management group name, type DW\_New York City. 2. Click Browse.   The **Select User or Group** dialog box appears.   1. In the Select User or Group dialog box, type SMDWMgtGrpAdmin, click Check Names, and then click OK. 2. Click Next. |
| Configure the reporting server for the data warehouse | 1. Review the status of the SQL Server Reporting Services URL. 2. Click Next. |
| Configure the account for Service Manager services | 1. Click Domain account. 2. In User name, type SMDWRunAsAcct. 3. In Password, type P@ssw0rd. 4. In Domain, select CORP. 5. Click Test Credentials. 6. Click Next. |
| Configure the reporting account | 1. In User name, type SMDWReporting. 2. In Password, type P@ssw0rd. 3. In Domain, select CORP. 4. Click Test Credentials. 5. Click Next. |
| Configure Analysis Services for OLAP cubes | Click Next. |
| Configure the Analysis Services credential | 1. In User name, type SMDWAnalysis. 2. In Password, type P@ssw0rd. 3. In Domain, select CORP. 4. Click Test Credentials. 5. Click Next. |
| Help improve System Center Service Manager | 1. Select the appropriate option based on your desire to participate in the Customer Experience Improvement Program. 2. Click Next. |
| Installation summary | Click Install. |
| Installing Service Manager management server | Monitor the progress of installing the Service Manager management server. |
| Setup completed successfully | 1. Review the status of the setup process. 2. Clear the Open the Encryption Backup or Restore Wizard after Setup closes check box. 3. Click Close. |

1. Close all open windows and dialog boxes.

When the wizard is complete, the Service Manager 2012 management server is installed.

# 

# Appendix D: Prepare CM-2012-01 Computer

For purposes of this guide, System Center 2012 - Configuration Manager runs on the computer named CM-2012-01. Install the prerequisite software, server roles, and services on this computer.

Note

This section assumes that you are creating a new Configuration Manager 2012 infrastructure. If you are using an existing Configuration Manager 2012 infrastructure, review the steps in this section and substitute existing resource names for the resources created in this section (such as the computer name and shared network folders).

Prepare the CM-2012-01 computer for use by performing the following steps:

[Step D-1: Review System Prerequisites](#_Step_D-1:_Review)

[Step D-2: Install Windows Server 2008 R2](#_Step_D-2:_Install)

[Step D-3: Install the Web Services (IIS) Server Role](#_Step_D-3:_Install)

[Step D-4: Add the Required Windows Server 2008 R2 Features](#_Step_D-4:_Add)

[Step D-5: Create the Required User and Service Accounts](#_Step_D-5:_Create)

[Step D-6: Install SQL Server 2008 R2](#_Step_D-6:_Install)

[Step D-7: Add the Site Server to the Administrators Security Group](#_Step_D-7:_Add)

[Step D-8: Install Configuration Manager 2012](#_Step_D-8:_Install)

[Step D-9: Configure the Network Access Account](#_Step_D-9:_Configure)

[Step D-10: Configure the Configuration Manager Site Boundaries](#_Step_D-10:_Configure)

[Step D-11: Configure the Publishing of Site Information in AD DS and DNS](#_Step_D-11:_Configure)

[Step D-12: Add the Reporting Services Point Site System Role](#_Step_D-12:_Add)

[Step D-13: Configure the Compliance Evaluation Schedule](#_Step_D-13:_Configure)

## Step D-1: Review System Prerequisites

The CM-20120-01 computer runs Configuration Manager 2012 and SQL Server 2008 R2. The computer runs the Windows Server 2008 R2 operating system with Service Pack 1 and the following server roles installed:

* Web Server

The system resources of the computer are as follows:

* Dual quad-core processor running at 2.66 (GHz) or faster
* 8 gigabytes (GB) or more of physical memory
* One disk partition that has 100 GB or more of available disk space; it will become the drive C partition
* One CD-ROM or DVD-ROM drive that will be assigned the drive letter D
* One disk partition that has 16 GB or more of available disk space; it will become partition E

## Step D-2: Install Windows Server 2008 R2

Use the information in the following table to install Windows Server 2008 R2 with Service Pack 1 for CM-2012-01. Accept default values unless otherwise specified.

| When prompted for | Provide these values |
| --- | --- |
| Where do you want to install Windows? | Disk 0 Unallocated Space |
| Password | Any strong password |
| Computer name | CM-2012-01 |
| Format for volumes C and E | NTFS |
| TCP/IP configuration | Configure with a static IP address configuration, with the other TCP/IP configuration options as appropriate for the environment. |
| Domain membership | Member server in corp.contoso.com domain. |

## Step D-3: Install the Web Services (IIS) Server Role

Install the Web Services (IIS) server role with the role services listed in the following table, which are required for SQL Server 2008 R2 and Configuration Manager 2012. Unless otherwise specified, use the default values.

| Role service | Status |
| --- | --- |
| Web Server | Installed |
| Common HTTP Features | Installed |
| Static Content | Installed |
| Default Document | Installed |
| Directory Browsing | Installed |
| HTTP Errors | Installed |
| HTTP Redirection | Installed |
| WebDAV Publishing | Installed |
| Application Development | Installed |
| ASP.NET | Installed |
| .NET Extensibility | Installed |
| ASP | Not installed |
| CGI | Not installed |
| ISAPI Extensions | Installed |
| ISAPI Filters | Installed |
| Server Side Includes | Not installed |
| Health and Diagnostics | Installed |
| HTTP Logging | Installed |
| Logging Tools | Installed |
| Request Monitor | Installed |
| Tracing | Installed |
| Custom Logging | Not installed |
| ODBC Logging | Not installed |
| Security | Installed |
| Basic Authentication | Not installed |
| Windows Authentication | Installed |
| Digest Authentication | Not installed |
| Client Certificate Mapping Authentication | Not installed |
| IIS Client Certificate Mapping Authentication | Not installed |
| URL Authorization | Not installed |
| Request Filtering | Installed |
| IP and Domain Restriction | Not installed |
| Performance | Installed |
| Static Content Compression | Installed |
| Dynamic Content Compression | Not installed |
| Management Tools | Installed |
| IIS Management Console | Installed |
| IIS Management Scripts and Tools | Not installed |
| Management Service | Not installed |
| IIS 6 Management Compatibility | Installed |
| IIS 6 Metabase Compatibility | Installed |
| IIS 6 WMI Compatibility | Installed |
| IIS 6 Scripting Tools | Not installed |
| IIS 6 Management Console | Not installed |
| FTP Publishing Service | Not installed |
| FTP Server | Not installed |
| FTP Management Console | Not installed |
| IIS Hostable Web Core | Not installed |

## Step D-4: Add the Required Windows Server 2008 R2 Features

In addition to installing the required Windows Server 2008 R2 server roles, add the following required features in Server Manager in the Features Summary section:

* Background Intelligent Transfer Service (BITS)
* Remote Differential Compression
* .NET Framework 3.5.1

## Step D-5: Create the Required User and Service Accounts

Configuration Manager 2012 requires user accounts during the installation process. The following table lists the information needed to create these accounts. SQL Server 2008 R2 will use user accounts that were created during the SM-2012-01 configuration process.

| Create this account | With these settings |
| --- | --- |
| System Center Configuration Manager Client Network Access account | 1. In First name, type CM 2012. 2. In Last name, type Client Network Access. 3. In User logon name, type CMNetAccess. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. In Description, type Service account used as the network access account for Configuration Manager 2012 Client. |
| System Center Configuration Manager Client push account | 1. In First name, type CM 2012. 2. In Last name, type Client Push Account. 3. In User logon name, type CMClientPush. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. In Description, type Service account used to perform Configuration Manger Client push. |

## Step D-6: Install SQL Server 2008 R2

Before installing Configuration Manager 2012, install SQL Server 2008 R2.

Note

To enable all SQL Server 2008 R2 features, install the Web Services (IIS) server role before installing SQL Server 2008 R2.

To install SQL Server 2008 R2

1. Start the SQL Server Installation Center.
2. In the SQL Server Installation Center, in the navigation pane, click Installation.
3. In the details pane, click New installation or add features to an existing installation.

The SQL Server 2008 R2 Setup Wizard starts.

1. Install SQL Server 2008 R2 using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Setup Support Rules | Click OK. |
| Product Key | Click Next. |
| License Terms | 1. Select the I accept the license terms check box. 2. Click Next. |
| Setup Support Files | Click Install. |
| Setup Support Rules | 1. Ensure no critical results exist for the rules. 2. Click Next. |
| Setup Role | 1. Click SQL Server Feature Installation. 2. Click Next. |
| Feature Selection | 1. Select Database Engine Services check box. 2. Select Reporting Services check box. 3. Select Full-Text Search check box. 4. Select Management Tools - Complete check box. 5. Click Next. |
| Installation Rules | Click Next. |
| Instance Configuration | Click Next. |
| Disk Space Requirements | Click Next. |
| Server Configuration | 1. For SQL Server Agent, in Account Name, type CORP\SQLAgent, in Password, type P@ssw0rd. 2. For SQL Server Database Engine, in Account Name, type CORP\SQLDBEngine, in Password, type P@ssw0rd. 3. For SQL Server Reporting Services, in Account Name, type CORP\SQLReport, in Password, type P@ssw0rd. 4. Click Next. |
| Database Engine Configuration | 1. Click Add Current User. 2. Click Next. |
| Reporting Services Configuration | Click Next. |
| Error Reporting | Click Next. |
| Installation Configuration Rules | Click Next. |
| Ready to Install | Click Install. |
| Complete | Click Close. |

1. Close the SQL Server Installation Center.

To install SQL Server 2008 R2 Service Pack 1

1. In Windows Explorer, go to target\_folder (where target\_folder is the name of the folder where you downloaded SQL Server 2008 R2 SP1).
2. In Windows Explorer, double-click SQLServer2008R2SP1-KB2528583-x64-ENU.exe

The **Extracting Files** dialog box appears. The service pack files are extracted to a local folder. After the files are extracted, the Microsoft SQL Server 2008 R2 Service Pack 1 setup wizard starts.

1. Install SQL Server 2008 R2 SP1 using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| SQL Server 2008 R2 update | Click Next. |
| License Terms | 1. Select the I accept the license terms check box. 2. Click Next. |
| Select Features | Click Next. |
| Check Files In Use | 1. Ensure no critical results exist. 2. Click Next. |
| Ready to update | 1. Verify the features to be updated are correct. 2. Click Update. |
| Update Progress | The progress is displayed for updating the SQL Server features. |
| Complete | Click Close. |

1. Install any additional updates or hotfixes.

To configure Windows Firewall for SQL Server 2008 R2 access

1. Click Start, click Administrative Tools, and then click Windows Firewall with Advanced Security.
2. In the console tree, click Inbound Rules.
3. In the Actions pane, click New Rule.

The New Inbound Rule Wizard starts.

1. Complete the New Inbound Rule Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Rule Type | Click Port and then click Next. |
| Protocols and Ports | 1. Click TCP. 2. Click Specific local ports. 3. In Specific local ports, type 1433. 4. Click Next. |
| Action | Click Next. |
| Profile | Click Next. |
| Name | 1. In Name, type SQL Server Database Engine (TCP-In). 2. In Description, type Rule to allow inbound access to SQL Server database engine. 3. Click Finish. |

1. Close all open windows and dialog boxes.

## Step D-7: Add the Site Server to the Local Administrators Security Group

When all computers are in the same forest, manually add the site server computer account to the local Administrators group on each computer. Complete this step before configuring the computer as a site system.

To add the site server to the Administrators security group

1. Click Start, point to Administrative Tools, and then click Server Manager.
2. In the Server Manager console tree, go to Server Manager (CM-2012-01) / Configuration / Local Users and Groups / Groups.
3. In the details pane, right-click Administrators, and then click Properties.
4. In the Administrators Properties dialog box, click Add.
5. In the Select Users, Contacts, Computers, or Groups dialog box, click Object Types.
6. In the Object Types dialog box, in Object types, select Computers, and then click OK.
7. In the Select Users, Contacts, Computers, or Groups dialog box, in Enter the object names to select, type CM-2012-01. Click Check Names, and then click OK.
8. In the Administrators Properties dialog box, click OK.
9. Close any open windows and dialog boxes.

## Step D-8: Install Configuration Manager 2012

When the other products and technologies have been installed, install Configuration Manager 2012. Before doing so, however, extend the Active Directory schema so that computers can locate the distribution points, service locator points, and other server roles. Also, you can extend the schema after you have installed Configuration Manager 2012. For more information about how to extend the Active Directory schema for Configuration Manager 2012, see [Prepare Active Directory for Configuration Manager](http://technet.microsoft.com/en-us/library/21b20921-7997-4b8c-bf1e-ec4c476620cc(TechNet.10)#BKMK_PrepAD).

After extending the Active Directory schema, install Configuration Manager 2012. The configuration of CM-2012-01 supports Configuration Manager 2012 for this sample. The configuration of computers in the production network may vary. To find out more about the prerequisites for installing Configuration Manager 2012, see [Supported Configurations for Configuration Manager](http://technet.microsoft.com/en-us/library/gg682077.aspx).

To install Configuration Manager 2012

1. Start the System Center 2012 Configuration Manager installation.
2. On the System Center 2012 Configuration Manager splash screen, click the Install hyperlink.

The Microsoft System Center 2012 Configuration Manager Setup Wizard starts.

1. Complete the Microsoft System Center 2012 Configuration Manager Setup Wizard using the information in the following table. Accept the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Before You Begin | Click Next. |
| Getting Started | Click Next. |
| Microsoft Software License Terms | Select the I accept these license terms check box, and then click Next. |
| Update Prerequisite Components | In Download and use the latest updates. Updates will be saved to the following location, type C:\CMDownloads, and then click Next. |
| Server Language Selection | Click Next. |
| Client Language Selection | Click Next. |
| Site and Installation Settings | 1. In Site code, type NYC. 2. In Site name, type New York City Site. 3. Click Next. |
| Primary Site Installation | 1. Click Install the primary site as a stand-alone site.   The Configuration Manager dialog box appears, confirming that you want to install this site as a stand-alone site.   1. In the Configuration Manager dialog box, click Yes. 2. Click Next. |
| Database Information | Click Next. |
| SMS Provider Settings | Click Next. |
| Client Computer Communication Settings | Click Configure the communication method on each site system role, and then click Next. |
| Site System Roles | Click Next. |
| Customer Experience Improvement Program Configuration | Click Next. |
| Settings Summary | Click Next. |
| Prerequisite Check | Click Begin Install. |
| Install | 1. Monitor the installation process until complete. 2. Click Close. |

1. Close all open windows and dialog boxes.

When the wizard is complete, Configuration Manager 2012 is installed.

## Step D-9: Configure the Network Access Account

The Configuration Manager client needs an account to provide credentials when accessing the Configuration Manager distribution points and shared folders. This account is called the Network Access account. The CMNetAccess account was created earlier in the process to use as the Network Access account.

To configure the Network Access account

1. Click Start, point to All Programs, and then point to Microsoft System Center. Point to Configuration Manager 2012, and then click ConfigMgr Console.
2. In the Configuration Manager console, in the navigation pane, click Administration.
3. In the Administration workspace, go to Overview / Site Configuration / Sites.
4. In the preview pane, click NYC - New York City Site.
5. On the ribbon, click Settings, click Configure Site Components, and then click Software Distribution.
6. In the Software Distribution Properties dialog box, click the Network Access Account tab.
7. In Network Access Account, click Specify the account that accessed network locations, click Set, and then click New Account.

The Windows User Account dialog box appears.

1. Complete the Windows User Account dialog box using the information in the following table, and then click OK.

| For this | Do this |
| --- | --- |
| User name | Type CORP\CMNetAccess |
| Password | Type P@ssw0rd |
| Confirm password | Type P@ssw0rd |

1. In the Software Distribution Properties dialog box, click OK.
2. Close any open windows.

## Step D-10: Configure the Configuration Manager Site Boundaries and Boundary Groups

The Configuration Manager client needs to know the boundaries for the site. Unless the site boundaries are specified, the client assumes that the computer running Configuration Manager 2012 is in a remote site. Add a site boundary based on the IP subnet that the virtual machines use. Then add the site boundary to a site boundary group.

To create a Configuration Manager site boundary

1. Click **Start**, point to **All Programs**, and then point to **Microsoft System Center**. Point to **Configuration Manager 2012**, and then click **ConfigMgr Console**.
2. In the Configuration Manager console, in the navigation pane, click Administration.
3. In the Administration workspace, go to Overview / Hierarchy Configuration / Boundaries.
4. On the Ribbon, click Create Boundary.

The Create Boundary dialog box opens.

1. Complete the Create Boundary dialog box using the information in the following table, and then click OK.

Note

For this sample, the site boundary is specified by network address. However, you can also specify site boundaries using an AD DS site name or an IP address range.

| For this | Do this |
| --- | --- |
| Description | Type IP Subnet Boundary. |
| Type | Select IP subnet. |
| Network | Type network\_address (where network\_address is the network address of the subnet where the computers are installed). |
| Subnet mask | Type subnet\_mask (where subnet\_mask is the subnet mask of the subnet where the computers are installed). |

To add the Configuration Manager site boundary to a site boundary group

1. In the Configuration Manager console, in the navigation pane, click Administration.
2. In the Administration workspace, go to Overview / Hierarchy Configuration / Boundary Groups.
3. On the Ribbon, click Create Boundary Group.

The Create Boundary Group dialog box opens.

1. Complete the General tab of the Create Boundary Group dialog box using the information in the following table.

| For this | Do this |
| --- | --- |
| Name | New York City Boundary Group |
| Description | Boundary group for the site boundaries at the New York City site. |
| Boundaries | 1. Click Add.   The **Add Boundaries** dialog box appears.   1. In the Add Boundaries dialog box, select site\_boundary, and then click OK (where site\_boundary is the site boundary you created earlier in the process).   The site boundary appears in the list of boundaries. |

1. Complete the References tab of the Create Boundary Group dialog box using the information in the following table, and then click OK.

| For this | Do this |
| --- | --- |
| Site assignment | Select the Use this boundary group for site assignment check box. |
| Content location | 1. Click Add.   The **Add Site Systems** dialog box appears.   1. In the Add Site Systems dialog box, select \\CM-2012-01.corp.contoso.com, and then click OK.   The site system server appears in the list of site system servers. |

1. Close any open windows.

## Step D-11: Configure the Publishing of Site Information in AD DS and DNS

The Configuration Manager client needs to locate the various Configuration Manager 2012 server roles. Modify the site properties to publish the site information in AD DS and in DNS.

To configure the publishing of site information in AD DS and in DNS

1. Click Start, point to All Programs, and then point to Microsoft System Center. Point to Configuration Manager 2012, and then click ConfigMgr Console.
2. In the Configuration Manager console, in the navigation pane, click Administration.
3. In the Administration workspace, go to Overview / Site Configuration / Sites.
4. In the preview pane, click NYC - New York City Site.
5. On the ribbon, click Properties.
6. In the New York City Site Properties dialog box, on the Publishing tab, verify that the corp.contoso.com Active Directory forest is listed, and then click Cancel.
7. Close any open windows.

## Step D-12: Add the Reporting Services Point Site System Role

To view Configuration Manager reports, you need to add the Reporting Services Point site system role. You add this role using the Site System Roles Wizard.

 To add the Reporting Services Point site system role

1. On CM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center 2012, click Configuration Manager, and then click Configuration Manager Console.

The Configuration Manager Console starts.

1. In the Configuration Manager console, in the navigation pane, click Administration.
2. In the Administration workspace, go to Overview / Site Configuration / Servers and Site System Roles.
3. In the preview pane, click \\CM-2012-01.corp.contoso.com.
4. On the ribbon, on the Home tab, in the Server group, click Add Site System Roles.

The Add Site System Roles Wizard starts.

1. Complete the Add Site System Roles Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| General | Click Next. |
| System Role Selection | 1. Select the Reporting services point check box. 2. Click Next. |
| Reporting Services Point | 1. Click Verify.   The status Successfully verified appears next to the Verify button.   1. Click Set, and then click New Account.   The Windows User Account dialog box opens.   1. Complete the Windows User Account dialog box by performing the following steps and the click OK. 2. In User name, type CORP\SQLReport. 3. In Password and Confirm Password, type P@ssw0rd. 4. Click Next. |
| Summary | 1. Review the information in the Details box that that you provided while completing the previous wizard pages. 2. Click Next. |
| Progress | The progress for adding the site system role is displayed. |
| Confirmation | Click Close. |

1. Close any open windows or dialog boxes.

## Step D-13: Configure the Compliance Evaluation Schedule

The result status for automated control activities in the Process Pack for IT GRC are automatically updated from configuration baselines in the desired configuration management feature in Configuration Manager 2012. By default, the Configuration Manager Client evaluates compliance every seven days. For the purposes of this guide, reduce this time to 10 minutes so that compliance will be checked more frequently.

Note

Reducing the schedule to evaluating compliance every 10 minutes in a production environment would place a heavy demand on system resources. This change is only being made to make the compliance status change faster in the evaluation environment.

 To configure the compliance evaluation schedule

1. On CM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center 2012, click Configuration Manager, and then click Configuration Manager Console.

The Configuration Manager Console starts.

1. In the Configuration Manager console, in the navigation pane, click Administration.
2. In the Administration workspace, go to Overview / Client Settings.
3. In the preview pane, click Default Client Agent Settings.
4. On the ribbon, on the Home tab, in the Properties group, click Properties.

The Default Settings dialog box opens.

1. In the Default Settings dialog box, in the navigation pane, go to Compliance Settings.
2. In the details pane, under Schedule compliance evaluation, click Schedule.

The Configure Client Setting dialog box opens.

1. In the Configure Client Setting dialog box, in Run every, select 10 Minutes, and then click OK.
2. In the Default Settings dialog box, click OK.
3. Close all open windows and dialog boxes.

# 

# Appendix E: Prepare OM-2012-01 Computer

For purposes of this guide, System Center 2012 - Operations Manager runs on the computer named OM-2012-01. Install the prerequisite software, server roles, and services on this computer.

Note

This section assumes that you are creating a new Operations Manager 2012 infrastructure. If you are using an existing Operations Manager 2012 infrastructure, review the steps in this section and substitute existing resource names for the resources that you create (such as the computer name and shared network folders).

Prepare the OM-2012-01 computer for use by completing the following steps:

[Step E-1: Review System Prerequisites](#_Step_E-1:_Review)

[Step E-2: Install Windows Server 2008 R2](#_Step_E-2:_Install)

[Step E-3: Install the Web Services (IIS) Server Role](#_Step_E-3:_Install)

[Step E-4: Add the Required Windows Server 2008 R2 Features](#_Step_E-4:_Add)

[Step E-5: Register .NET Framework with IIS](#_Step_E-5:_Register)

[Step E-6: Configure ISAP and CGI Restrictions](#_Step_E-6:_Configure)

[Step E-7: Create the Required user and Service Accounts](#_Step_E-7:_Create)

[Step E-8: Install SQL Server 2008 R2](#_Step_E-8:_Install)

[Step E-9: Install Operations Manager 2012](#_Step_E-9:_Install)

## Step E-1: Review System Prerequisites

The OM-20120-01 computer runs Operations Manager 2012 and SQL Server 2008 R2. The computer runs the Windows Server 2008 R2 operating system with Service Pack 1 and the following server roles installed:

* Web Server

The system resources of the computer are as follows:

* Dual quad-core processor running at 2.66 (GHz) or faster
* 8 gigabytes (GB) or more of physical memory
* One disk partition that has 100 GB or more of available disk space; it will become the drive C partition
* One CD-ROM or DVD-ROM drive that will be assigned the drive letter D

## Step E-2: Install Windows Server 2008 R2

Use the information in the following table to install Windows Server 2008 R2 with Service Pack 1 for OM-2012-01. Accept default values unless otherwise specified.

| When prompted for | Provide these values |
| --- | --- |
| Where do you want to install Windows? | Disk 0 Unallocated Space |
| Password | P@ssw0rd |
| Computer name | OM-2012-01 |
| Format for volumes C and E | NTFS |
| TCP/IP configuration | Configure with a static IP address configuration, with the other TCP/IP configuration options as appropriate for the environment. |
| Domain membership | Member server in corp.contoso.com domain. |

## Step E-3: Install the Web Services (IIS) Server Role

Install the Web Services (IIS) server role with the role services listed in the following table, which are required for SQL Server 2008 R2 and Operations Manager 2012. Unless otherwise specified, use the default values.

| Role service | Status |
| --- | --- |
| Web Server | Installed |
| Common HTTP Features | Installed |
| Static Content | Installed |
| Default Document | Installed |
| Directory Browsing | Installed |
| HTTP Errors | Installed |
| HTTP Redirection | Installed |
| WebDAV Publishing | Installed |
| Application Development | Installed |
| ASP.NET | Installed |
| .NET Extensibility | Installed |
| ASP | Not installed |
| CGI | Installed |
| ISAPI Extensions | Installed |
| ISAPI Filters | Installed |
| Server Side Includes | Not installed |
| Health and Diagnostics | Installed |
| HTTP Logging | Installed |
| Logging Tools | Installed |
| Request Monitor | Installed |
| Tracing | Installed |
| Custom Logging | Not installed |
| ODBC Logging | Not installed |
| Security | Installed |
| Basic Authentication | Not installed |
| Windows Authentication | Installed |
| Digest Authentication | Not installed |
| Client Certificate Mapping Authentication | Not installed |
| IIS Client Certificate Mapping Authentication | Not installed |
| URL Authorization | Not installed |
| Request Filtering | Installed |
| IP and Domain Restriction | Not installed |
| Performance | Installed |
| Static Content Compression | Installed |
| Dynamic Content Compression | Not installed |
| Management Tools | Installed |
| IIS Management Console | Installed |
| IIS Management Scripts and Tools | Not installed |
| Management Service | Not installed |
| IIS 6 Management Compatibility | Installed |
| IIS 6 Metabase Compatibility | Installed |
| IIS 6 WMI Compatibility | Installed |
| IIS 6 Scripting Tools | Not installed |
| IIS 6 Management Console | Not installed |
| FTP Publishing Service | Not installed |
| FTP Server | Not installed |
| FTP Management Console | Not installed |
| IIS Hostable Web Core | Not installed |

## Step E-4: Add the Required Windows Server 2008 R2 Features

In addition to installing the required Windows Server 2008 R2 server roles, add the following required features in Server Manager in the Features Summary section:

* .NET Framework 3.5.1

## Step E-5: Register .NET Framework with IIS

The .NET Framework version 4 needs to be registered with IIS to allow the Operations Manager Web Console feature to work correctly. Register the .NET Framework using the aspnet\_regiis.exe tool, which is provided with .NET Framework version 4.

To register the .NET Framework with IIS

1. Start a command prompt.
2. Enter the following command and then press Enter.

cd C:\Windows\Microsoft.NET\Framework64\v4.0.30319

The default directory changes to the .NET Framework version 4.

1. Enter the following command and then press Enter.

aspnet\_regiis.exe -i

The.NET Framework version 4 is registered with IIS.

1. Exit the command prompt.

## Step E-6: Configure ISAPI and CGI Restrictions

The ISAPI and CGI restrictions in IIS must be configured correctly to allow .NET Framework version 4 to function properly, which is required by the Operations Manager Web Console feature. By default, the .NET Framework version 4 is not allowed (disabled).

To configure ISAPI and CGI restrictions

1. Click Start, click Administrative Tools, and then click Internet Information Services Manager.

The Internet Information Services Manager console starts.

1. In the Internet Information Services Manager console, in the console tree, click OM‑2012‑01.
2. In the preview pane, under IIS, click ISAPI and CGI Restrictions.
3. In the preview pane, click ASP.NET v4.0.30319.

Note

You must enable the 64-bit version of ASP.NET v4.0.30319, which has a path of C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet\_isapi.dll.

1. In the Actions pane, click Allow.
2. Close all open windows and dialog boxes.

## Step E-7: Create the Required User and Service Accounts

Operations Manager 2012 requires user accounts during the installation process. The following table lists the information needed to create these accounts. SQL Server 2008 R2 will use user accounts that were created during the SM-2012-01 configuration process.

| Create this account | With these settings |
| --- | --- |
| Operations Manager Client action account | 1. In First name, type Operations Manager. 2. In Last name, type Action Account. 3. In User logon name, type OMAction. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. In Description, type Service account used as the action account for Operations Manager 2012 management server. |
| Configuration Manager data reader account | 1. In First name, type Operations Manager. 2. In Last name, type Data Reader. 3. In User logon name, type OMDataRead. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. In Description, type Service account used by Operations Manager 2012 management server to read from the operational database. |
| Configuration Manager data write account | 1. In First name, type Operations Manager. 2. In Last name, type Data Write. 3. In User logon name, type OMDataWrite. 4. In Password and Confirm password, type P@ssw0rd. 5. Clear the User must change password at next logon check box. 6. Select the Password never expires check box. 7. In Description, type Service account used by Operations Manager 2012 management server to write to the operational database. |

## Step E-8: Install SQL Server 2008 R2

Before installing Operations Manager 2012, install SQL Server 2008 R2.

Note

To enable all SQL Server 2008 R2 features, install the Web Services (IIS) server role before installing SQL Server 2008 R2.

To install SQL Server 2008 R2

1. Start the SQL Server Installation Center.
2. In the SQL Server Installation Center, in the navigation pane, click Installation.
3. In the details pane, click New installation or add features to an existing installation.

The SQL Server 2008 R2 Setup Wizard starts.

1. Install SQL Server 2008 R2 using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Setup Support Rules | Click OK. |
| Product Key | Click Next. |
| License Terms | 1. Select the I accept the license terms check box. 2. Click Next. |
| Setup Support Files | Click Install. |
| Setup Support Rules | 1. Ensure no critical results exist for the rules. 2. Click Next. |
| Setup Role | 1. Click SQL Server Feature Installation. 2. Click Next. |
| Feature Selection | 1. Select Database Engine Services check box. 2. Select Reporting Services check box. 3. Select Full-Text Search check box. 4. Select Management Tools - Complete check box. 5. Click Next. |
| Installation Rules | Click Next. |
| Instance Configuration | Click Next. |
| Disk Space Requirements | Click Next. |
| Server Configuration | 1. For SQL Server Agent, in Account Name, type CORP\SQLAgent, in Password, type P@ssw0rd. 2. For SQL Server Database Engine, in Account Name, type CORP\SQLDBEngine, in Password, type P@ssw0rd. 3. For SQL Server Reporting Services, in Account Name, type CORP\SQLReport, in Password, type P@ssw0rd. 4. Click Next. |
| Database Engine Configuration | 1. Click Add Current User. 2. Click Next. |
| Reporting Services Configuration | Click Next. |
| Error Reporting | Click Next. |
| Installation Configuration Rules | Click Next. |
| Ready to Install | Click Install. |
| Complete | Click Close. |

1. Close the SQL Server Installation Center.

To install SQL Server 2008 R2 Service Pack 1

1. In Windows Explorer, go to target\_folder (where target\_folder is the name of the folder where you downloaded SQL Server 2008 R2 SP1).
2. In Windows Explorer, double-click SQLServer2008R2SP1-KB2528583-x64-ENU.exe

The Extracting Files dialog box appears. The service pack files are extracted to a local folder. After the files are extracted, the Microsoft SQL Server 2008 R2 Service Pack 1 setup wizard starts.

1. Install SQL Server 2008 R2 SP1 using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| SQL Server 2008 R2 update | Click Next. |
| License Terms | 1. Select the I accept the license terms check box. 2. Click Next. |
| Select Features | Click Next. |
| Check Files In Use | 1. Ensure no critical results exist. 2. Click Next. |
| Ready to update | 1. Verify the features to be updated are correct. 2. Click Update. |
| Update Progress | The progress is displayed for updating the SQL Server features. |
| Complete | Click Close. |

1. Install any additional updates or hotfixes.

To configure Windows Firewall for SQL Server 2008 R2 access

1. Click Start, click Administrative Tools, and then click Windows Firewall with Advanced Security.
2. In the console tree, click Inbound Rules.
3. In the Actions pane, click New Rule.

The New Inbound Rule Wizard starts.

1. Complete the New Inbound Rule Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Rule Type | Click Port and then click Next. |
| Protocols and Ports | 1. Click TCP. 2. Click Specific local ports. 3. In Specific local ports, type 1433. 4. Click Next. |
| Action | Click Next. |
| Profile | Click Next. |
| Name | 1. In Name, type SQL Server Database Engine (TCP-In). 2. In Description, type Rule to allow inbound access to SQL Server database engine. 3. Click Finish. |

1. Close all open windows and dialog boxes.

To configure SQL Server Agent service to start automatically

1. Click Start, click Administrative Tools, and then click Services.

The Services console is displayed.

1. In the Services console, in the details pane, right-click SQL Server Agent, and then click Properties.

The **SQL Server Agent (MSSQLSERVER) Properties** dialog box is displayed.

1. In the SQL Server Agent (MSSQLSERVER) Properties dialog box, in Startup type, click Automatic.
2. In the Service status area, if the service is not already started, click Start.
3. Click OK.
4. Close all open windows.

To configure Windows Firewall for SQL Server 2008 R2 Reporting Services

1. Click Start, click Administrative Tools, and then click Windows Firewall with Advanced Security.
2. In the console tree, click Inbound Rules.
3. In the Actions pane, click New Rule.

The New Inbound Rule Wizard starts.

1. Complete the New Inbound Rule Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Rule Type | Click Port and then click Next. |
| Protocols and Ports | 1. Click TCP. 2. Click Specific local ports. 3. In Specific local ports, type 80. 4. Click Next. |
| Action | Click Next. |
| Profile | Click Next. |
| Name | 1. In Name, type SQL Server Reporting Services (TCP-In). 2. In Description, type Rule to allow inbound access to SQL Server Reporting Services. 3. Click Finish. |

1. Close all open windows and dialog boxes.

To configure SQL Server 2008 R2 Reporting Services

1. Click Start, click All Programs, click Microsoft SQL Server 2008 R2, click Configuration Tools, and then click Reporting Services Configuration Manager.

The Reporting Services Configuration Connection dialog box is displayed.

1. In the Reporting Services Configuration Connection dialog box, click Connect.

The Reporting Services Configuration Manager console is displayed.

1. In the Reporting Services Configuration Manager console, in the navigation pane, go to OM-2012-01\MSSQLSERVER.
2. In the preview pane, click Start.

The Report Server starts. The results of the configuration process are displayed at the bottom of the preview pane.

1. In the preview pane, click Exit.

## Step E-9: Install Operations Manager 2012

When the other products and technologies have been installed, install Operations Manager 2012. The configuration of OM-2012-01 supports Operations Manager 2012 for the Process Pack for IT GRC evaluation environment. The configuration of computers in the production network may vary. To find out more about the prerequisites for installing Operations Manager 2012, see [Supported Configurations for System Center 2012 - Operations Manager](http://technet.microsoft.com/en-us/library/hh205990.aspx).

To install Operations Manager 2012

1. Start the System Center 2012 - Operations Manager Setup process from installation media.
2. On the System Center 2012 - Operations Manager Setup splash screen, click the Install hyperlink.

The Microsoft System Center 2012 - Operations Manager Setup Wizard starts.

1. Complete the System Center 2012 - Operations Manager Setup Wizard using the information in the following table. Accept the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Please read this license agreement | Select the I have read, understood, and agree with the terms of the license agreement check box, and then click Next. |
| Select features to install | 1. Select the Management server check box. 2. Select the Management console check box. 3. Select the Web console check box. 4. Select the Reporting server check box. 5. Click Next. |
| Select installation location | Click Next. |
| Proceed with Setup | Click Next. |
| Specify an installation option | 1. In Management group name, type OM New York City. 2. Click Next. |
| Configure the operational database | 1. In Server name and instance name, type OM‑2012‑01. 2. Click Next. |
| Configure the data warehouse database | 1. In Server name and instance name, type OM‑2012‑01. 2. Click Next. |
| SQL Server instance for reporting services | Click Next. |
| Specify a web site for use with the Web console | Click Next. |
| Select an authentication mode for use with the Web console | Click Next. |
| Configure Operations Manager accounts | 1. For Management server action account, in Domain\User Name, type CORP\OMAction, in Password, type P@ssw0rd. 2. For Data Reader account, in Domain\User Name, type CORP\OMDataRead, in Password, type P@ssw0rd. 3. For Data Writer account, in Domain\User Name, type CORP\OMDataWrite, in Password, type P@ssw0rd. 4. Click Next. |
| Help improve Operations Manager | 1. Select the appropriate options based on your organization’s requirements. 2. Click Next. |
| Installation Summary | 1. Review the installation options selected during the wizard. 2. Click Install. |
| Installation progress | 1. Monitor the installation process until complete. 2. Click Close. |

1. Close all open windows and dialog boxes.

When the wizard is complete, Operations Manager 2012 is installed.

# 

# Appendix F: Prepare WIN-2008R2-01 Computer

For purposes of this guide, Windows Server 2008 R2 runs the File Service server role on the computer named WIN‑2008R2‑01. Install the prerequisite software, server roles, and services on this computer.

Note

This section assumes that you are installing a new computer running Windows Server 2008 R2 as a part of the Process Pack for IT GRC evaluation environment. If you are using an existing server, review the steps in this section and substitute existing resource names for the resources that you create (such as the computer name and shared network folders).

Prepare the WIN-2008R2-01 computer for use by completing the following steps:

[Step F-1: Review System Prerequisites](#_Step_F-1:_Review)

[Step F-2: Install Windows Server 2008 R2](#_Step_F-2:_Install)

## Step F-1: Review System Prerequisites

The WIN-2008R2-01 computer is a member server that runs the Windows Server 2008 R2 operating system with Service Pack 1 and the following server roles installed:

* File Services

The system resources of the computer are as follows:

* Single quad-core processor running at 2.66 (GHz) or faster
* 1 gigabyte (GB) or more of physical memory
* One disk partition that has 100 GB or more of available disk space; it will become the drive C partition
* One CD-ROM or DVD-ROM drive that will be assigned the drive letter D

## Step F-2: Install Windows Server 2008 R2

Use the information in the following table to install Windows Server 2008 R2 with Service Pack 1 for WIN-2008R2-01. Accept default values unless otherwise specified.

| When prompted for | Provide these values |
| --- | --- |
| Where do you want to install Windows? | Disk 0 Unallocated Space |
| Password | P@ssw0rd |
| Computer name | WIN-2008R2-01 |
| Format for volumes C and E | NTFS |
| TCP/IP configuration | Configure with a static IP address configuration, with the other TCP/IP configuration options as appropriate for the environment. |
| Domain membership | Member server in corp.contoso.com domain. |

# 

# Appendix G: Configure System Center Product Integration

For purposes of this guide, Windows Server 2008 R2 runs the File Service server role on the computer named WIN‑2008R2‑01. Install the prerequisite software, server roles, and services on this computer.

Note

This section assumes that you are installing a new computer running Windows Server 2008 R2 as a part of the Process Pack for IT GRC evaluation environment. If you are using an existing server, review the steps in this section and substitute existing resource names for the resources that you create (such as the computer name and shared network folders).

Configure the System Center product integration by completing the following steps:

[Step G-1: Register the Service Manager Data Warehouse](#_Step_G-1:_Register)

[Step G-2: Deploy Operations Manager Agents](#_Step_G-2:_Deploy)

[Step G-3: Deploy Configuration Manager Clients](#_Step_G-3:_Deploy)

[Step G-4: Configure Active Directory Connector in Service Manager](#_Step_G-4:_Configure)

[Step G-5: Configure Operations Manager CI Connector in Service Manager](#_Step_G-5:_Configure)

[Step G-6: Configure Configuration Manager Connector in Service Manager](#_Step_G-6:_Configure)

[Step G-7: Verify Population of Service Manager CMDB](#_Step_G-7:_Verify)

## Step G-1: Register the Service Manager Data Warehouse

After the Service Manager management server (SM-2012-01) and the Service Manager data warehouse (SM-2012-02) are installed, register the Service Manager data warehouse with the Service Manager management server. Register the Service Manager data warehouse using the Data Warehouse Registration Wizard in the Service Manager Console on SM-2012-01.

 To register the Service Manager data warehouse

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the navigation pane, click Administration.
2. In the details pane, under the Register with Service Manager’s Data Warehouse area, click the Register with Service Manager Data Warehouse link.

The Data Warehouse Registration Wizard starts.

1. Complete the Data Warehouse Registration Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Before You Begin | Click Next. |
| Data Warehouse | 1. In Server name, type SM-2012-02. 2. Click Test Connection. 3. Click Next. |
| Credentials | 1. Click Next.   The Credentials dialog box appears.   1. In the Credentials dialog box, in Password, type P@ssw0rd, and then click OK. |
| Summary | 1. Review the information provided while completing the wizard. 2. Click Create. |

1. Close all open windows and dialog boxes.

 To verify the Service Manager data warehouse registration

1. On SM-2012-01, log on using CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.

The Service Manager Console starts.

1. In the Service Manager Console, in the navigation pane, click Data Warehouse.
2. In the Data Warehouse pane, go to Data Warehouse / Data Warehouse Jobs.
3. In the preview pane, monitor the status of the Data Warehouse Jobs.
4. If any of the jobs have failed, resume the job.

The following data warehouse jobs should be running:

* Extract\_DW\_New York City
* Load.Common
* Transform.Common
* MPSyncJob

Note

Typically, failed data warehouse jobs will resume automatically. However, restarting the jobs manually reduces the length of time for the data warehouse jobs to complete.

1. Periodically close and open the Service Manager Console to refresh the navigation pane.

Note

When you start the Service Manager Console the System Center Service Manager dialog box is displayed that notifies you the report deployment process is in progress. When the dialog box is no longer displayed, then the report deployment process is complete.

1. Continue steps 3 – 7 until the reports are deployed in the reporting services.
2. Do not proceed with additional steps until Reporting is displayed in the navigation pane and the reports are displayed in the Reporting pane.

## Step G-2: Deploy Operations Manager Agents

The Operations Manager agent needs to be deployed to all the computers in the Process Pack for IT GRC evaluation environment. OM-2012-01 already is running an Operations Manager 2012 management server and requires no Operations Manager agent. However, all the other computers require an Operations Manager agent. Deploy Operations Manager agents using the Computer and Device Management Wizard.

 To configure Group Policy to enable Windows Firewall ports for Operations Manager agent installation

1. On SM-2012-01, log on as CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click Administrative Tools, and then click Group Policy Management.
3. In the Group Policy Management console, in the console tree, go to Group Policy Management / Forest: corp.contoso.com / Domains / corp.contoso.com / Group Policy Objects.
4. In the console tree, right-click Group Policy Objects, and click New.

The New GPO dialog box appears.

1. In the New GPO dialog box, in Name, type Operations Manager Firewall Policy, and then click OK.

The Operations Manager Firewall Policy appears in the details pane.

1. In the details pane, right-click Operations Manager Firewall Policy, and then click Edit.
2. The Group Policy Management Editor console opens with the Operations Manager Firewall Policy being edited.
3. In the Group Policy Management Editor console, in the console tree, go to Computer Configuration / Policies / Windows Settings / Security Settings / Windows Firewall with Advanced Security / Windows Firewall with Advanced Security / Inbound Rules.
4. In the console tree, right-click Inbound Rules, and click New Rule.

The New Inbound Rule Wizard starts.

1. Complete the New Inbound Rule Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Rule Type | 1. Click Port. 2. Click Next. |
| Protocol and Ports | 1. Click TCP. 2. Click Specific local ports. 3. In Specific local ports, type 135, 137, 139, 445, 5723, 1024-5000, 49152-65535. 4. Click Next. |
| Action | Click Next. |
| Profile | Click Next. |
| Name | 1. In Name, type Operations Manager Agent (TCP-In). 2. In Description, type Allow inbound traffic to the Operations Manager agent on TCP ports 135, 137, 139, 445, 5723, 1024-5000, and 49152-65535. 3. Click Finish. |

1. In the console tree, right-click Inbound Rules, and click New Rule.

The New Inbound Rule Wizard starts.

1. Complete the New Inbound Rule Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Rule Type | 1. Click Port. 2. Click Next. |
| Protocol and Ports | 1. Click UDP. 2. Click Specific local ports. 3. In Specific local ports, type 135, 137, 139, 445, 5723, 1024-5000, 49152-65535. 4. Click Next. |
| Action | Click Next. |
| Profile | Click Next. |
| Name | 1. In Name, type Operations Manager Agent (UDP-In). 2. In Description, type Allow inbound traffic to the Operations Manager agent on UDP ports 135, 137, 139, 445, 5723, 1024-5000, and 49152-65535. 3. Click Finish. |

1. Close the Group Policy Management Editor.
2. In the Group Policy Management console, in the console tree, go to Group Policy Management / Forest: corp.contoso.com / Domains / corp.contoso.com.
3. In the console tree, right-click corp.contoso.com, and then click Link an Existing GPO.

The Select GPO dialog box appears.

1. In the Select GPO dialog box, in Group Policy objects, click Operations Manager Firewall Policy, and then click OK.
2. Close all open windows and dialog boxes.
3. Run gpupdate.exe /force on the following computers:

* SM-2012-01
* SM-2012-01
* CM-2012-01
* WIN-2008R2-01

 To deploy Operations Manager agents using the agent push method

1. On OM-2012-01, log on as CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click System Center 2012 - Operations Manager, and then click Operations Console.
3. In the Operations Manager console, in the navigation pane, click Administration.
4. In the Administration workspace, go to Administration / Device Management.
5. In the preview pane, under the Actions area, click Configure computers and devices to manage.

The Computer and Device Management Wizard starts.

1. Complete the Computer and Device Management Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Discovery Type | 1. Click Windows computers. 2. Click Next. |
| Auto or Advanced? | 1. Click Advanced Discovery. 2. In Computer and Device Classes, select Servers and Clients. 3. Click Next. |
| Discovery Method | 1. Click Scan Active Directory. 2. Click Configure.   The Find Computers dialog box appears.   1. In the Find Computers dialog box, click OK. 2. Click Next. |
| Administrator Account | Click Create. |
| Discovery is in progress | The progress for discovering Windows computers is displayed. |
| Select Objects to Manage | 1. Review the list of Windows computers discovered.   The list of Windows computers should include the following:   * SM-2012-01 * SM-2012-02 * CM-2012-01 * WIN-2008R2-01  1. Select the check box next to the following Windows computers:  * CM-2012-01 * WIN-2008R2-01   Note  SM-2012-01 and SM-2012-02 were not selected because the Operations Manager must be manually installed on computers running Service Manager management server or Service Manager data warehouse management server .   1. Select All. 2. Click Next. |
| Summary | Click Finish. |

1. In the **Administration** pane, in Administration / Device Management / Pending Management, monitor the status of the agent installation process.

If any of the agents fail to install, restart the agent installation process.

Note

In virtualized environments, the lack of available system resources could cause agent installation failure. Ensure that the necessary system resources are available on the Operations Manager management server and on the managed computers.

1. Continue to monitor the status of the agent installation process until all agents are installed.
2. In the **Administration** pane, in Administration / Device Management / Agent Managed, ensure all the computers are listed.

If any of the agents are not in the node, restart the agent installation process.

 To deploy Operations Manager agents on the computers running Service Manager

1. On SM-2012-01, log on as CORP\Administrator with a password of P@ssw0rd.
2. Start the System Center 2012 - Operations Manager Setup process from installation media.
3. On the System Center 2012 - Operations Manager Setup splash screen, click the Local agent hyperlink.

The Operations Manager Agent Setup Wizard starts.

1. Complete the Operations Manager Agent Setup Wizard using the information in the following table. Accept the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Please read this license agreement | Select the I have read, understood, and agree with the terms of the license agreement check box, and then click Next. |
| Select features to install | 1. Select the Management server check box. 2. Select the Management console check box. 3. Select the Web console check box. 4. Select the Reporting server check box. 5. Click Next. |
| Select installation location | Click Next. |
| Proceed with Setup | Click Next. |
| Specify an installation option | 1. In Management group name, type OM New York City. 2. Click Next. |
| Configure the operational database | 1. In Server name and instance name, type OM‑2012‑01. 2. Click Next. |
| Configure the data warehouse database | 1. In Server name and instance name, type OM‑2012‑01. 2. Click Next. |
| SQL Server instance for reporting services | Click Next. |
| Specify a web site for use with the Web console | Click Next. |
| Select an authentication mode for use with the Web console | Click Next. |
| Configure Operations Manager accounts | 1. For Management server action account, in Domain\User Name, type CORP\OMAction, in Password, type P@ssw0rd. 2. For Data Reader account, in Domain\User Name, type CORP\OMDataRead, in Password, type P@ssw0rd. 3. For Data Writer account, in Domain\User Name, type CORP\OMDataWrite, in Password, type P@ssw0rd. 4. Click Next. |
| Help improve Operations Manager | 1. Select the appropriate options based on your organization’s requirements. 2. Click Next. |
| Installation Summary | 1. Review the installation options selected during the wizard. 2. Click Install. |
| Installation progress | 1. Monitor the installation process until complete. 2. Click Close. |

1. Close all open windows and dialog boxes.

## Step G-3: Deploy Configuration Manager Clients

The Configuration Manager Client needs to be deployed to all the computers in the Process Pack for IT GRC evaluation environment. Deploy the Configuration Manager Client using the Computer and Device Management Wizard.

 To configure the Client Push Installation account

1. On CM-2012-01, log on as corp\administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center 2012, click Configuration Manager, and then click Configuration Manager Console.
3. In the Configuration Manager console, in the navigation pane, click Administration.
4. In the Administration workspace, go to Administration / Site Configuration / Sites.
5. In the preview pane, click NYC – New York City Site.
6. On the ribbon, on the Home tab, in the Settings group, click Client Installation Settings, and then click Client Push Installation.

The **Client Push Installation Properties** dialog box opens.

1. In the Client Push Installation Properties dialog box, on the Accounts tab, click the New button, and then click New Account.

The **Windows User Account** dialog box appears.

1. In the Windows User Account dialog box, in User name, type CORP\CMClientPush.
2. In the Windows User Account dialog box, in Password and Confirm password, type P@ssw0rd.
3. In the Client Push Installation Properties dialog box, click OK.
4. Close all open windows and dialog boxes.

 To configure Group Policy to enable Windows Firewall ports for Configuration Manager Client installation

1. On SM-2012-01, log on as CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click Administrative Tools, and then click Group Policy Management.
3. In the Group Policy Management console, in the console tree, go to Group Policy Management / Forest: corp.contoso.com / Domains / corp.contoso.com / Group Policy Objects.
4. In the console tree, right-click Group Policy Objects, and click New.

The **New GPO** dialog box appears.

1. In the New GPO dialog box, in Name, type Configuration Manager Client Firewall Policy, and then click OK.

The Operations Manager Firewall Policy appears in the details pane.

1. In the details pane, right-click Operations Manager Firewall Policy, and then click Edit.
2. The Group Policy Management Editor console opens with the Operations Manager Firewall Policy being edited.
3. In the Group Policy Management Editor console, in the console tree, go to Computer Configuration / Policies / Windows Settings / Security Settings / Windows Firewall with Advanced Security / Windows Firewall with Advanced Security / Inbound Rules.
4. In the console tree, right-click Inbound Rules, and click New Rule.

The New Inbound Rule Wizard starts.

1. Complete the New Inbound Rule Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Rule Type | 1. Click Port. 2. Click Next. |
| Protocol and Ports | 1. Click TCP. 2. Click Specific local ports. 3. In Specific local ports, type 67, 68, 80, 135, 137, 139, 443, 445, 2701, 2702, 5723, 1024-5000, 49152-65535. 4. Click Next. |
| Action | Click Next. |
| Profile | Click Next. |
| Name | 1. In Name, type Configuration Manager Client (TCP-In). 2. In Description, type Allow inbound traffic to the Configuration Manager Client on TCP ports 67, 68, 80, 135, 137, 139, 443, 445, 2701, 2702, 5723, 1024-5000, and 49152-65535. 3. Click Finish. |

1. In the console tree, right-click Inbound Rules, and click New Rule.

The New Inbound Rule Wizard starts.

1. Complete the New Inbound Rule Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Rule Type | 1. Click Port. 2. Click Next. |
| Protocol and Ports | 1. Click UDP. 2. Click Specific local ports. 3. In Specific local ports, type 67, 68, 80, 135, 137, 139, 443, 445, 2701, 2702, 5723, 1024-5000, 49152-65535. 4. Click Next. |
| Action | Click Next. |
| Profile | Click Next. |
| Name | 1. In Name, type Configuration Manager Client (UDP-In). 2. In Description, type Allow inbound traffic to the Operations Manager Client on UDP ports 67, 68, 80, 135, 137, 139, 443, 445, 2701, 2702, 5723, 1024-5000, and 49152-65535. 3. Click Finish. |

1. In the console tree, right-click Inbound Rules, and click New Rule.

The New Inbound Rule Wizard starts.

1. Complete the New Inbound Rule Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Rule Type | 1. Click Predefined. 2. In Predefined, select File and Printer Sharing. 3. Click Next. |
| Predefined Rules | Click Next. |
| Action | 1. Click Allow the connection. 2. Click Finish. |

1. In the console tree, right-click Inbound Rules, and click New Rule.

The New Inbound Rule Wizard starts.

1. Complete the New Inbound Rule Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Rule Type | 1. Click Predefined. 2. In Predefined, select Windows Management Instrumentation (WMI). 3. Click Next. |
| Predefined Rules | Click Next. |
| Action | 1. Click Allow the connection. 2. Click Finish. |

1. Close the Group Policy Management Editor.
2. In the Group Policy Management console, in the console tree, go to Group Policy Management / Forest: corp.contoso.com / Domains / corp.contoso.com.
3. In the console tree, right-click corp.contoso.com, and then click Link an Existing GPO.

The **Select GPO** dialog box appears.

1. In the Select GPO dialog box, in Group Policy objects, click Configuration Manager Client Firewall Policy, and then click OK.
2. Close all open windows and dialog boxes.
3. Run gpupdate.exe /force on the following computers:

* SM-2012-01
* SM-2012-01
* CM-2012-01
* WIN-2008R2-01

 To configure Active Directory System Discovery

1. On CM-2012-01, log on as corp\administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center 2012, click Configuration Manager, and then click Configuration Manager Console.
3. In the Configuration Manager console, in the navigation pane, click Administration.
4. In the Administration workspace, go to Administration / Hierarchy Configuration / Discovery Methods.
5. In the preview pane, click Active Directory System Discovery.
6. On the ribbon, click Properties.

The **Active Directory System Discovery Properties** dialog box is displayed.

1. In the Active Directory System Discovery Properties dialog box, on the General tab, select the Enable Active Directory System Discovery check box.
2. On the General tab, in Active Directory containers, click the New button.

The New Active Directory Container dialog box appears.

1. In the New Active Directory Container dialog box, click Browse.

The **Select New Container** dialog box appears.

1. In the Select New Container dialog box, click corp, and then click OK.
2. In the New Active Directory Container dialog box, click OK.

The LDAP query is displayed in the **Active Directory containers** list box.

1. In the Active Directory System Discovery Properties dialog box, click OK.
2. In the preview pane, click Active Directory System Discovery.
3. On the ribbon, in the Discovery Method group, click Run Full Discovery Now.

The **Configuration Manager** dialog box appears.

1. In the Configuration Manager dialog box, click Yes.

The discovery process is initiated. The progress of the discovery process can be monitored by viewing the list of devices in Assets and Compliance \ Overview \ Devices in the Assets and Compliance workspace. All computers should be discovered.

You can troubleshoot the discovery process by viewing the corresponding log file, adsysdis.txt, in the %Program Files%\Microsoft Configuration Manager\Logs folder.

After the discovery process is complete, deploy the Configuration Manager client to the computers using the client push method.

 To deploy the Configuration Manager client using the client push method

1. On CM-2012-01, log on as corp\administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center 2012, click Configuration Manager, and then click Configuration Manager Console.
3. In the Configuration Manager console, in the navigation pane, click Assets and Compliance.
4. In the Administration workspace, go to Assets and Compliance / Overview / Devices.
5. In the preview pane, select the following devices:

* CM-2012-01
* OM-2012-01
* SM-2012-01
* SM-2012-02
* WIN-2008R2-01

1. On the ribbon, on the Home tab, in the Device group, click Install Client.

The Install Client Wizard starts.

1. Complete the Install Client Wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Before You Begin | Click Next. |
| Installation Options | 1. Select the Allow the client software to be installed on domain controllers check box. 2. Select the Install the client software from a specified site check box. 3. Click Next. |
| Summary | 1. Review the information in the Details box that that you provided while completing the previous wizard pages. 2. Click Next. |
| Progress | The progress for creating the task sequence is displayed. |
| Completion | Click Close. |

The installation of the Configuration Manager client begins on the selected devices.

1. In the Administration pane, in Administration / Device Management / Pending Management, monitor the status of the agent installation process.

If any of the agents fail to install, restart the agent installation process.

Note

In virtualized environments, the lack available system resources could cause agent installation failure. Ensure that the necessary system resources are available on the Operations Manager management server and on the managed computers.

1. Continue to monitor the status of the Configuration Manager Client Installation process until all clients are installed.
2. In the **Administration** pane, in Administration / Device Management / Agent Managed, ensure all the computers are listed.

If any of the devices are not listed, perform view the Configuration Manager Client Installation logs at the following locations:

* Initial client installation bootstrap in the C:\Program Files\Microsoft Configuration Manager\Logs\ccm.txt file on CM-2012-01.
* Remainder of client installation process in the ccmsetup.txt, client.msi.txt , and dism.txt files in the C:\Windows\ccmsetup\ folder on the computer where the client is being installed.

Note

You can periodically run device discovery to help reduce the time for the devices to appear in the Agent Managed node after the client successfully installs.

## Step G-4: Configure Active Directory Connector in Service Manager

The Active Directory Connector in Service Manager 2012 is used to collect information about user and computer objects in Active Directory Domain Services (AD DS). The connector allows automatic population of the Service Manager Configuration Management Database (Service Manager CMDB) using information from AD DS.

 To configure the Active Directory connector for Service Manager

1. On SM-2012-01, log on as CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.
3. In the Service Manager console, in the navigation pane, click Administration.
4. In the Administration pane, go to Administration / Connectors.
5. In the Tasks pane, click Create connector, and then click Active Directory connector.
6. The Active Directory connector wizard starts.
7. Complete the Active Directory connector wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Before You Begin | Click Next. |
| General | 1. In Name, type Active Directory Connector - corp.contoso.com. 2. In Description, type Active Directory connector that synchronizes user and group objects from the corp.contoso.com domain. 3. Click Next. |
| Domain/OU | 1. Click Test Connection.   The Credentials dialog box appears.   1. In the Credentials dialog box, in Password, type P@ssw0rd, and then click OK.   The Test Connection dialog box appears.   1. In the Test Connection dialog box, click OK. 2. Click Next. |
| Select objects | Click Next. |
| Summary | 1. Review the information that you provided while completing the previous wizard pages. 2. Click Create. |
| Progress | The progress for creating the Active Directory connector is displayed. |
| Completion | Click Close. |

The Active Directory Connector displays in the preview pane.

1. In the preview pane, click Active Directory Connector – corp.contoso.com.
2. In the Tasks pane, under Active Directory Connector – corp.contoso.com, click Synchronize Now.

The **Synchronize Now** dialog box appears.

1. In the Synchronize Now dialog box, click OK.

## Step G-5: Configure Operations Manager CI Connector in Service Manager

The Operations Manager CI Connector in Service Manager 2012 is used to synchronize configuration items in the operational database in Operations Manager 2012 with the Service Manager CMDB in Service Manager 2012. The connector allows automatic population of the Service Manager CMDB using information from Operations Manager 2012 configuration items.

Note

Ensure that you import all Operations Manager 2012 Management Packs for your monitoring scenarios into Operations Manager 2012 prior to configuring the Operations Manager CI Connector in Service Manager.

 To configure the Operations Manager CI connector for Service Manager

1. On SM-2012-01, log on as CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.
3. In the Service Manager console, in the navigation pane, click Administration.
4. In the Administration pane, go to Administration / Connectors.
5. In the Tasks pane, under Connectors, click Create connector, and then click Operations Manager CI connector.
6. The Operations Manager CI connector wizard starts.
7. Complete the Operations Manager CI connector wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Before You Begin | Click Next. |
| General | 1. In Name, type Operations Manager CI Connector – OM New York City Management Group. 2. In Description, type Operations Manager CI connector that synchronizes configuration items from the OM New York City management group in Operations Manager 2012. 3. Click Next. |
| Server Details | 1. In Server name, type OM-2012-01. 2. Click Test Connection.   The Credentials dialog box appears.   1. In the Credentials dialog box, in Password, type P@ssw0rd, and then click OK.   The Test Connection dialog box appears.   1. In the Test Connection dialog box, click OK. 2. Click Next. |
| Management Packs | 1. Select the Select all check box. 2. Click Next. |
| Schedule | Click Next. |
| Summary | 1. Review the information that you provided while completing the previous wizard pages. 2. Click Create. |
| Progress | The progress for creating the Active Directory connector is displayed. |
| Completion | Click Close. |

The Operations Manager CI Connector displays in the preview pane.

1. In the preview pane, click Operations Manager CI Connector – OM New York City Management Group.
2. In the Tasks pane, under Operations Manager CI Connector – OM New York City Management Group, click Synchronize Now.

The **Synchronize Now** dialog box appears.

1. In the Synchronize Now dialog box, click OK.

If you import additional Operations Manager 2012 Management Packs after you configure the Operations Manager CI Connector for Service Manager, edit the connector to include the additional Operations Manager 2012 Management Packs to include any configuration items define in the Management Packs

## Step G-6: Configure Configuration Manager Connector in Service Manager

The Configuration Manager Connector in Service Manager 2012 is used to synchronize user and devices discovered by Configuration Manager 2012 with the Service Manager CMDB in Service Manager 2012. The connector allows automatic population of configuration items using information from Configuration Manager 2012.

Prior to configuring the Configuration Manager Connector in Service Manager 2012, grant the Operational Database Account access to the Configuration Manager 2012 site database. Otherwise, the connector will be unable to read the information in the site database.

 To grant the Operational Database Account access to the Configuration Manager site database

1. On CM-2012-01, log on as CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft SQL Server 2008 R2, and then click SQL Server Management Studio.

The SQL Server Management Studio console starts and the Connect to Server dialog box is displayed.

1. In the Connect to Server dialog box, click Connect.

The SQL Server Management Studio console completes the startup process.

1. In the SQL Server Management Studio console, in Object Explorer, go to CM‑2012‑01 / Security / Logins.
2. In Object Explorer, right-click Logins, and then click New Login.

The **Login – New** dialog box is displayed.

1. In the Login – New dialog box, in Login Name, type corp\SMSvcsAcct.
2. In Default database, click CM\_NYC.
3. In Select a page, click User Mapping.
4. In Users mapped to this login, select the check box next to CM\_NYC.
5. In CM\_NYC, in Default Schema, click the ellipse.

The **Select Schema** dialog box appears.

1. In the Select Schema dialog box, click Browse.

The **Browse for Objects** dialog box appears.

1. In the Browse for Objects dialog box, select the check box next to [db\_datareader],.
2. In Database role membership for CM\_NYC, select db\_datareader, and then click OK.
3. In the Select Schema dialog box, click OK.
4. In the Login – New dialog box, click OK.
5. Close all open windows and dialog boxes.

 To configure the Configuration Manager connector for Service Manager

1. On SM-2012-01, log on as CORP\Administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.
3. In the Service Manager console, in the navigation pane, click Administration.
4. In the Administration pane, go to Administration / Connectors.
5. In the Tasks pane, under Connectors, click Create connector, and then click Configuration Manager connector.
6. The Configuration Manager connector wizard starts.
7. Complete the Configuration Manager connector wizard using the information in the following table, accepting the defaults unless otherwise specified.

| On this wizard page | Do this |
| --- | --- |
| Before You Begin | Click Next. |
| General | 1. In Name, type Configuration Manager Connector – New York City (NYC) Site. 2. In Description, type Configuration Manager connector that synchronizes users and devices from the New York City (NYC) primary site in Configuration Manager 2012. 3. Click Next. |
| Management Pack | 1. In Management pack, select System Center 2012 - Configuration Manager Connector Configuration. 2. Click Next. |
| Database | 1. In Database server name, type CM-2012-01. 2. In Database name, type CM\_NYC. 3. Click Test Connection.   The **Credentials** dialog box appears.   1. In the Credentials dialog box, in Password, type P@ssw0rd, and then click OK.   The **Test Connection** dialog box appears.   1. In the Test Connection dialog box, click OK. 2. Click Next. |
| Collections | 1. Select the Select all check box. 2. Click **Next**. |
| Schedule | Click Next. |
| Summary | 1. Review the information that you provided while completing the previous wizard pages. 2. Click Create. |
| Progress | The progress for creating the Active Directory connector is displayed. |
| Completion | Click Close. |

The Configuration Manager Connector displays in the preview pane.

1. In the preview pane, click Configuration Manager Connector –New York City (NYC) Site.
2. In the Tasks pane, under Configuration Manager Connector –New York City (NYC) Site, click Synchronize Now.

The **Synchronize Now** dialog box appears.

1. In the Synchronize Now dialog box, click OK.

If you import additional Configuration Manager 2012 device collections after you configure the Configuration Manager Connector for Service Manager, edit the connector to include the additional Configuration Manager 2012 collections.

## Step G-7: Verify Population of Service Manager CMDB

After you have deployed the Active Directory connector, Operations Manager CI connector, and Configuration Manager connector, verify that the Service Manager CMDB is being properly populated by the connectors.

 To configure Client Push Installation account

1. On SM-2012-01, log on as corp\administrator with a password of P@ssw0rd.
2. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.
3. In the Service Manager console, in the navigation pane, click Configuration Items.
4. In the Configuration Items workspace, go to Configuration Items / Computers / All Windows Computers.
5. In the preview pane, view the list of computers that exist in the Service Manager CMDB.

The list of computers displayed should be as follows:

* CM-2012-01.corp.contoso.com
* OM-2012-01.corp.contoso.com
* SM-2012-01.corp.contoso.com
* SM-2012-02.corp.contoso.com
* WIN-2008R2-01.corp.contoso.com

If any of the computers are missing from the list, ensure the computers are in AD DS, Operations Manager 2012, and Configuration Manager 2012. Also, try immediate synchronization of each connector.

1. Close all open windows and dialog boxes.

# Appendix H: Uninstall the Process Pack for IT GRC and Client

The Process Pack for IT GRC and Process Pack for IT GRC client can be uninstalled using the Programs and Features applet found in Control Panel on those computers in which it is installed.

Uninstall the Process Pack for IT GRC and client using the following steps:

[Step H-1: Uninstall](#_Step_H-1:_Uninstall) the Process Pack for IT GRC

[Step H-2: Uninstall the Process Pack for IT GRC Client](#_Step_H-2:_Uninstall)

## Step H-1: Uninstall the Process Pack for IT GRC

To uninstall the Process Pack for IT GRC

1. Log on to the computer running System Center 2012 – Service Manager with an account that has the following permissions:

* Member of the local Administrators group on the computer
* Administrator in Service Manager

1. Click **Start**, click **Control Panel**.
2. In Control Panel, double-click **Programs and Features**.
3. In the list of installed programs, click **Process Pack for IT GRC**, and then click **Uninstall**.

The Programs and Features dialog box appears.

1. In the **Programs and Features** dialog box, click **Yes**.

The Process Pack for IT GRC is removed from the list of installed programs.

1. Close all open windows and dialog boxes.

When the process completes, the Process Pack for IT GRC is uninstalled and the Compliance and Risk Items navigation button should be removed from the Service Manager Console.

## Step H-2: Uninstall the Process Pack for IT GRC Client

To uninstall the Process Pack for IT GRC Client



1. Log on to the computer running the Process Pack for IT GRC Client with an account that has the following permissions:

* Member of the local Administrators group on the computer

1. Click **Start**, click **Control Panel**.
2. In Control Panel, double-click **Programs and Features**.
3. In the list of installed programs, click **Process Pack for IT GRC Client**, and then click **Uninstall**.

The Microsoft Office Customization Installer dialog box appears.

1. In the **Microsoft Office Customization Installer** dialog box, click **OK**.

The Process Pack for IT GRC Client is removed from the list of installed programs.

Close all open windows and dialog boxes.

# Appendix I: Troubleshoot, Resolve, and Recover from Installation Issues

Process Pack for IT GRC server and client installation failures can be caused by software, hardware, or network issues which leave the system in an unstable state. The following subsections provide additional information to assist you in identifying and resolving upgrade installation issues.

## Upgrading the Process Pack for IT GRC Server

Issues preventing the successful completion of an upgrade installation of the Process Pack for IT GRC server could occur in one of five phases of the upgrade process. The steps you need to perform to recover from a failed upgrade vary depending on which phase the failure occurred in. The five phases follow:

 Failure during the prerequisite check.

 Failure during predicted checks.

 Failure occurs in an unpredictable manner before making permanent changes to a management server.

 Failure occurs in an unpredictable manner after making permanent changes to a management server.

 Failure occurs in an unpredictable manner after making permanent changes to the database.

### Failure during the Prerequisite Check

Before the installation of IT GRC Process Pack begins, a prerequisite check is made for certain requirements. If a condition exists that is not optimal but that does not impede Process Pack for IT GRC functionality, you will see a warning message.

If a condition exists that indicates an absolute requirement for Process Pack for IT GRC was not met, you will see a failure message that indicates what action you need to take. For example, you will need to install System Center 2012 – Service Manager prior to installing Process Pack for IT GRC.

If you see either a warning or a failure message, you can cancel the installation and make the necessary changes and then reinstall the Process Pack for IT GRC. All failure conditions must be addressed and corrected before the installation or upgrade can proceed.

### Failure during Predicted Checks

After any failures that were identified during the prerequisite check have been corrected, pressing Next on the Prerequisites page will start the upgrade or installation of Process Pack for IT GRC. The following checks are performed during the installation or upgrade process:

 That the specified data warehouse database exists.

 That the System Center Data Access service could log on with the set of credentials you supplied.

 That the System Center Management Configuration service could log on with the set of credentials you supplied.

 That the Setup program can access the file location for the Service Manager installation.

### Failure Occurs in an Unpredictable Manner before Making Permanent Changes to the Management Server

During installation or upgrade, errors can occur. If an error occurs before any permanent changes are made to the Service Manager or data warehouse management server, for example before making changes to the SQL database or before importing management packs, you can correct the issue and retry the installation or upgrade.

### Failure Occurs in an Unpredictable Manner after Making Permanent Changes to the Management Server

If an error occur after permanent changes are made to the Service Manager or data warehouse management server, the error message that displays will not include a Retry button.

In such a situation you will need to reinstall the original version of the affected management server and you will need the backup of the encryption key. For the Service Manager Management server, the encryption key is only available if you make a backup before starting the upgrade. For more information, see the topic "How to Back Up the Encryption Key in Service Manager" in the [Disaster Recovery Guide for System Center 2012 – Service Manager](http://technet.microsoft.com/en-us/library/hh495602.aspx).

### Failure Occurs in an Unpredictable Manner after Making Permanent Changes to the Database

If an error occurs after other permanent changes are made, for example, after importing of management packs or any other time data is written into a database, the error message that displays will not include a Retry button. At this point your only option is to press Close and begin a disaster recovery process to restore your databases. This recovery is only possible if you have backed up your databases before starting the upgrade process. For more information, see the topic "Backing Up Service Manager Databases" in the [Disaster Recovery Guide for System Center 2012 – Service Manager](http://technet.microsoft.com/en-us/library/hh495602.aspx).

### Troubleshooting Process Pack for IT GRC Server Installation Failures

#### **New installation failure**

1. Retry installation. If it fails again, go to step 2.
2. Uninstall the Process Management Pack using Control Panel. Validate if successfully uninstalled. If successful, try reinstallation. If reinstallation fails, go to step 3.
3. Refer to the [Disaster Recovery Guide for System Center 2012 – Service Manager](http://technet.microsoft.com/en-us/library/hh495602.aspx) for more information.

#### **Upgrade installation failure**

1. Retry the upgrade installation. If it fails again, go to step 2.
2. Uninstall with data kept and retry server upgrade. If this step fails, go to step 3.
3. Refer to the [Disaster Recovery Guide for System Center 2012 – Service Manager](http://technet.microsoft.com/en-us/library/hh495602.aspx) for more information.

#### **Uninstallation failure**

* Retry the uninstallation. If it fails again, refer to the [Disaster Recovery Guide for System Center 2012 – Service Manager](http://technet.microsoft.com/en-us/library/hh495602.aspx) for more information.

## Upgrading the Process Pack for IT GRC Client

Issues preventing the successful completion of an upgrade installation of the Process Pack for IT GRC client could occur in one of three phases of the upgrade process. The steps you need to perform to recover from a failed upgrade vary depending on which phase the failure occurred in. The three phases are as follows:

 Failure during the prerequisite check.

 Failure occurs in an unpredictable manner before making permanent changes to a client.

 Failure occurs in an unpredictable manner after making permanent changes to a client.

### Failure during Prerequisite Check

Before the installation of Process Pack for IT GRC client begins, a prerequisite check is made for certain requirements.

If a condition exists that indicates an absolute requirement for the Process Pack for IT GRC client was not met, you will see a failure message that indicates what action you need to take. For example, you will need to install the System Center 2012 – Process Pack for IT GRC for Service Manager on the System Center 2012 – Service Manager management server prior to installing System Center 2012 – Process Pack for IT GRC client.

If you see either a warning or a failure message, you can cancel the installation and make the necessary changes and then reinstall the Process Pack for IT GRC client. All failure conditions must be addressed and corrected before the installation or upgrade can proceed.

### Failure Occurs in an Unpredictable Manner before Making Permanent Changes to the Process Pack for IT GRC Client

If any failures are identified during the client installation process before permanent changes are made, the client installation will automatically roll back. Such failures might include installing or upgrading Excel VSTO 3.0, or creating the Excel component. If the installation fails, then all components will be reverted. Should this occur you should try to run the upgrade install again.

### Failure Occurs in an Unpredictable Manner after Making Permanent Changes to the Process Pack for IT GRC Client

If any failures are identified after the client installation process has made permanent changes, the client installation will need to be manually uninstalled through Programs and Features applet in the computer’s Control Panel. After it is removed, the client can be installed again.

### Troubleshooting Client Installation Errors

#### Installation failure

1. Try to reinstall the GRC SP1 Excel add-in. If this fails, go to step 2.
2. Uninstall the GRC SP1 Excel add-in if it is still in Control Panel. If this fails, go to step 3.
3. Uninstall VSTO 3.0 SP1.
4. Reinstall VSTO 3.0 SP1.
5. Reinstall the GRC SP1 Excel add-in.