

System Center 2012   
Process Pack for IT GRC   
Operations 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%20Operations%20%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 Web site 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, Excel, and Windows PowerShell are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Revision History

|  |  |
| --- | --- |
| Release Date | Changes |
| September, 2010 | Original release of this guide. |
| February, 2011 | Service Pack 1 |
| April, 2012 | System Center 2012 release |

Contents

[Process Pack for IT GRC Operations Guide 1](#_Toc317174573)

[Style Conventions 2](#_Toc317174574)

[Intended Audience 2](#_Toc317174575)

[GRC and Program Management Overview 3](#_Toc317174576)

[Governance in the GRC Process 3](#_Toc317174577)

[Risk Management in the GRC Process 4](#_Toc317174578)

[Compliance in the GRC Process 5](#_Toc317174579)

[Process Pack for IT GRC Terms and Concepts 6](#_Toc317174580)

[Roles within an IT GRC Program 8](#_Toc317174581)

[Program Readiness Review 9](#_Toc317174582)

[Managing Risks with an IT GRC Management Program 11](#_Toc317174583)

[Create Risks for an IT GRC Management Program 12](#_Toc317174584)

[Publish the New Risks 16](#_Toc317174585)

[Add the Risks to the IT GRC Management Program 17](#_Toc317174586)

[Reporting IT GRC Information 18](#_Toc317174587)

[Predefined IT GRC Program Management Reports 19](#_Toc317174588)

[Predefined IT GRC Control Management Reports 22](#_Toc317174589)

[Predefined IT GRC Risk Management Reports 26](#_Toc317174590)

[Exception Types in IT GRC Programs 28](#_Toc317174591)

[Exporting and Importing IT GRC Management Information Using Excel 29](#_Toc317174592)

[Performing Updates to Existing IT GRC Management Information 30](#_Toc317174593)

[Creating New IT GRC Management Information 30](#_Toc317174594)

[Appendix: IT GRC Operations 31](#_Toc317174595)

[Retain Process Pack for IT GRC Compliance Data 31](#_Toc317174596)

[Manage Process Pack for IT GRC Applicability Groups 32](#_Toc317174597)

[In This Section 32](#_Toc317174598)

[About Process Pack for IT GRC Applicability Groups 32](#_Toc317174599)

[How to Assign Process Pack for IT GRC Applicability Groups to Control Activities 32](#_Toc317174600)

[Manage Process Pack for IT GRC User Roles 34](#_Toc317174601)

[In This Section 34](#_Toc317174602)

[About Process Pack for IT GRC User Roles 34](#_Toc317174603)

[Overview of Managing Process Pack for IT GRC User Roles 36](#_Toc317174604)

[How to Create a Process Pack for IT GRC User Role 37](#_Toc317174605)

[How to Add a Member to a Process Pack for IT GRC User Role 38](#_Toc317174606)

[How to Configure the Objects that Can Be Managed by a User Role Using Windows PowerShell 38](#_Toc317174607)

[How to Hide Console Tasks that the Program Implementer Cannot Use 39](#_Toc317174608)

[How Automated Control Activities are Scored Based on Managed Entity Results 40](#_Toc317174609)

# Process Pack for IT GRC Operations Guide

This 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 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), contain control activities and automation needed to take advantage of System Center Service Manager’s integration 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 infrastructure

This guide will help you understand the features and capabilities of the Process Pack for IT GRC. The following list provides brief descriptions of each section in the guide.

** IT** GRC and Program Management Overview. This section helps you understand the IT GRC processes, terms, and roles used in IT GRC management programs.

 Managing Risks with an IT GRC Program. This section helps you add risk information to an IT GRC management program.

 Reporting IT GRC Information. This section helps you run the reports that are included as a part of the Process Pack for IT GRC.

 **Managing** **Exceptions in IT GRC Programs**. This section helps you understand the types of exceptions that can be requested and how they are managed.

 Exporting and Importing IT GRC Management Information. This section helps you use the Microsoft Client add-in to export information from and import information into the Process Pack for IT GRC.

* Appendix. This section provides additional details for using the Process Pack for IT GRC.

## 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 those whose roles include the following responsibilities:

* 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.

# **GRC and Program Management Overview**

The primary objective of the Process Pack for IT GRC is to help you implement IT GRC control and risk management in your organization. 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 help 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.

## 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.
* Are 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 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.

## 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.

## Program Readiness Review

A program readiness review is used by the compliance program manager to ensure that all of the control objectives and control activities in the program are ready for an audit or management review. You can perform the readiness review on one or more control objectives in a program or for the entire program using the Start Readiness Review wizard.

The program readiness review is created using the following table and instructions.

|  |  |
| --- | --- |
| Information needed | Value |
| Program | Credit Card Processing Compliance Program |
| <review\_program\_work\_item\_title> | Credit Card Processing Compliance Program Readiness Work Item |
| <review\_start\_date> | Today |
| <review\_end\_date> | Two months from today |
| <categories\_control\_objectives> | PC5 / Policy Needs Assessment |

To perform a program readiness review of an existing program using the Start Readiness Review wizard

|  |
| --- |
| 1. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.  The System Center Service Manager Console starts.  2. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.  3. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items/Program Management/All Programs location.  4. In the Results pane, click <program> (where program is the name of the program that you want to modify).  5. In the Tasks pane, click Start Readiness Review.  The Start Readiness Review wizard starts.  6. Complete the following pages in the Start Readiness Review wizard using the provided information, and accepting the defaults unless otherwise specified.  a. On the Before you Begin page, click Next.  On the Program Selection page  b. In Program Title, select <program> (where program is the name of the program for which you want to check readiness).  c. Click Next.  On the Review Activity Details page  d. In Review Program Work Item Title, type <review\_program\_work\_item\_title> (where review\_program\_work\_item\_title is the title you wish to assign to the work item title for the readiness review).  e. In Review Program Start Date, select <review\_start\_date> (where review\_start\_date is the starting date for the readiness review work item).  f. In Review Program End Date, select <review\_end\_date> (where review\_end\_date is the ending date for the readiness review work item).  g. Click Next.  On the Control Objective Selection page  h. In Select Categories and Control Objectives, select <categories\_control\_objectives> (where categories\_control\_objectives are the categories and control objectives to be selected for the readiness review).  i. Click Next.  On the Summary page  j. Review the list of configuration settings for creating the work item.  k. Click Create.  On the Completion page  l. Review the status of the Control Objectives Summary.  m. Click Close. |

The work item created by the wizard is visible in the Work Items/Activity Management/Manual Activities/All Activities location. For more information about the work items in System Center Service Manager, see the topic "Managing Activities and Changes" in the System Center Service Manager Help, which is included with System Center Service Manager.

# Managing Risks with an IT GRC Management Program

You can manage risks with an IT GRC program using the Process Pack for IT GRC. You can create a new IT GRC management program to manage risks or you can add risks to an existing program. IT GRC control management and risk management can be performed in separate programs or in the same program. This scenario provides a simple example of how to manage the risks for a new e-commerce application that is being deployed into the production environment.

To add risks to your IT GRC program in the Process Pack for IT GRC, complete the steps in the following list. Detailed information about each step is provided in the subsections that follow the list.

* Create risks for the IT GRC management program.
* Publish the new risks.
* Add the risks to the risk management program.

## Create Risks for an IT GRC Management Program

After you identify the risks you want to manage, you are ready to create risks for the IT GRC management program. Each risk has calculated values that help identify the inherent risk and any residual risk that has not been mitigated. The following table lists the risk configuration settings and their relationship to each other.

|  |  |
| --- | --- |
| Setting | Description |
| Impact | Indicates the impact that the risk has on the success of the program and is measured on a scale from 1 to 5, where 1 represents the least impact and 5 represents the greatest impact. |
| Likelihood | Indicates the likelihood that the risk will occur and is measured on a scale from 1 to 5, where 1 represents the least likelihood and 5 represents the greatest likelihood. |
| Control Level | Indicates the level of control over the risk and is measured on a scale from 1 to 5, where 1 represents the least level of control and 5 represents the greatest level of control. |
| Inherent Risk | A calculated value that indicates the value of the risk without any account for the control of the risk. The value is calculated by multiplying the value in Impact by the value in Likelihood. For example, if the value in Impact is 2 and the value in Likelihood is 4, then Inherent Risk will be 8. |
| Residual Risk | A calculated value that indicates the residual value of the risk after factoring in the control of the risk. The value is calculated by multiplying the value in Impact by the value in Likelihood and subtracting the value in Control Level. For example, if the value in Impact is 2, the value in Likelihood is 4, and the value in Control Level is 4, then Residual Risk will be 4. |
| Risk Response | Specify what action to take regarding the risk based on the value in Residual Risk. The possible values are:  · Accept, when both of the following are true:  · Impact is greater than 1 but less than 3.  · Likelihood is greater than 1 but less than 3.  · Avoid, when both of the following are true:  · Impact is greater than 1 but less than 3.  · Likelihood is greater than 3 but less than 5.  · Reduce, when both of the following are true:  · Impact is greater than 3 but less than 5.  · Likelihood is greater than 1 but less than 3.  · Share, when both of the following are true:  · Impact is greater than 3 but less than 5.  · Likelihood is greater than 3 but less than 5. |

Create a risk using the following table and instructions.

|  |  |
| --- | --- |
| Information needed | Value |
| <risk\_title> | Servers are ready for deployment in production environment. |
| <risk\_description> | Purchase, deliver, and burn-in of server computers must be completed in time to meet deployment schedule for new e-commerce application. |
| <risk\_owner> | User account that is to be the owner of the new risk |
| <risk\_assigned\_to> | User account that is assigned the new risk |
| <risk\_impact> | 5 |
| <risk\_likelihood> | 2 |
| <risk\_control\_level> | 5 |
| <risk\_response> | Reduce |

To create a new risk

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.  The System Center Service Manager Console starts.  2. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.  3. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items/Risk Management/All Risks location.  4. In the Tasks pane, click Create Risk.  The Risk <RID> – New dialog box appears (where RID is the identifier of the new risk).  5. Complete the tabs on the Risk <RID>– New dialog box, and then click OK.   |  |  | | --- | --- | | Tab | Description | | General | Contains basic information about the risk, including:   Title of the risk.   Description of the risk.   Owner of the risk.   User who the risk is assigned to.   Impact of the risk, which can be a value from 1 to 5, where 1 represents the least impact and 5 represents the greatest risk.   Likelihood of the risk, which can be a value from 1 to 5, where 1 represents the least likelihood and 5 represents the greatest likelihood.   Control level of the risk, which can be a value from 1 to 5, where 1 represents the least control and 5 represents the greatest control.   Risk Response, which can be a value of Accept, Avoid, or Reduce.   Response plan for mitigating the risk.   Associated activities.   Due date. | | Framework | Contains a hierarchy of items within the program and buttons for adding the items, including program categories, risks, control objectives, and control activities. | | Related Items | Contains other items managed in the Compliance and Risk Items pane that relate to this risk, including:   List of related incidents   List of supporting control activities   List of supporting control objectives   List of related work items   List of attached files  Note: On lower resolution computer displays you can click the arrow next to each item to collapse or expand the list of related items. | | Approval | Contains a list of all the review activities. | | History | Contains a list of all the changes made to the risk. |   The results pane in the All Risks <number> view refreshes to display the list of risks (where number is the total number of risks). |

## Publish the New Risks

After you create the new risk, you are ready to publish the risk. Publish the risk using the following table and instructions.

|  |  |
| --- | --- |
| Information needed | Value |
| <risk\_title> | Servers are ready for deployment in production environment. |

To publish an existing risk

|  |
| --- |
| 1. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.  The System Center Service Manager Console starts.  2. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.  3. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items/Risk Management/All Risks location.  4. In the Results pane, click <risk> (where risk is the name of the risk that you want to publish).  5. In the Tasks pane, click Publish Risk. |

The Results pane in the All Risks <number> view refreshes to display the list of all risks (where number is the total number of risks). The status of a risk just after you create it is set to Draft. The status of risk after you publish it is set to Pending, and this action also initiates a Service Manager review activity. After the review activity is approved, the status of the risk is set to Published. After it is approved, the risk appears in the Risks: Published view.

## Add the Risks to the IT GRC Management Program

After you create the risks for the IT GRC management program you created, you are ready to add the risks to the program.

Add a risk to the program using the following table and instructions.

|  |  |
| --- | --- |
| Information needed | Value |
| <program> | Credit Card Processing Compliance Program |
| <risk\_title> | Servers are ready for deployment in production environment. |

To add a risk to an existing program

|  |
| --- |
| 1. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.  The System Center Service Manager Console starts.  2. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.  3. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items/Program Management/All Programs location.  4. In the Results pane, click <program> (where program is the name of the program that you want to modify).  5. In the Tasks pane, click Edit.  The Program Management property dialog box appears.  6. In the Program Management dialog box, on the Framework tab, click the arrow beside <program\_name> to expand the program framework hierarchy.  7. In the Framework list box, select a category and then click Add Risk.  The Select objects dialog box appears and the list of existing risks is displayed.  8. On the Select objects dialog box, click <risk\_title>, click Add, and then click OK (where risk\_title is the title of the risk).  The risk appears in the Framework list box in the Program Management.  9. In the Program Management dialog box, click OK. |

The results pane in the All Programs view refreshes to display the list of programs.

# Reporting IT GRC Information

The Process Pack for IT GRC provides two different mechanisms for reporting your IT GRC management program information. A predefined and customized Microsoft Online Analytical Processing (OLAP) compliance data cube that connects to the data warehouse to retrieve data is provided for you to manipulate using Microsoft Excel® in a tabular fashion. More information can be found in the [Using Advanced Analytics](http://technet.microsoft.com/en-us/library/hh495576.aspx) topic from Microsoft TechNet.

Several predefined IT GRC control and risk management reports are also provided to help you manage IT GRC controls and risks in your organization. One set of reports is specifically designed for control management, one set for program management, and another set for risk management.

These reports provide IT GRC status at a program level, control objective level, control activity level, and risk level. The reports also include hyperlinks to subordinate reports that provide information about the configuration information for individual programs, control objectives, control activities, and risks.

You can run IT GRC management reports in the Reporting pane in the System Center Service Manager console. The IT GRC management reports are generated by the SQL Reporting Services, which is installed on the System Center Service Manager Data Warehouse Server.

The parameters for running each report can be configured through the Parameter Control Header section of each report. For example, you can filter report results by a specific IT GRC program in the “Parameter Control Header” section of the Control Management Progress Report.

For more information about troubleshooting running reports, see the following sections in the System Center Service Manager Deployment Guide, which is installed as a part of the System Center Service Manager download:

 “Install a Service Manager data warehouse and data warehouse database”

 “Troubleshoot data warehouse jobs”

## Predefined IT GRC Program Management Reports

The following table lists the IT GRC program management reports that are included in the Process Pack for IT GRC and a brief description of each report. The IT GRC control management reports are located in the Reporting/Compliance Reports Library folder.

|  |  |
| --- | --- |
| Report | Description |
| Program Health Dashboard Report | Added in Service Pack 1, this report provides comprehensive information about the health and status of one or more of your IT GRC programs. This report can be filtered by:  ****** Start date  ****** End date  ****** Time Zone  ****** Status  ****** Program – an optional field. If no program is specified, all programs in the system will be returned.  ****** Owned By – an optional field that will limit the list of returned programs to ones owned by the specified user. |
| Program Incidents List Report | Added in Service Pack 1, this report lists all compliance incidents related to any control objective, control activity, or risk managed in your IT GRC program. This report can be filtered by:  ****** Start date  ****** End date  ****** Time Zone  ****** ID  ****** Program – a single, specific IT GRC program  ****** Support Group – Tier 1, 2, or 3 support  ****** Resolution Category – how the incident was resolved  ****** Classification Category – of the incident  ****** Status – of the incident  ****** Priority – of the incident  ****** Urgency – of the incident  ****** Source – of the incident  ****** Assigned To – the person the incident is assigned to  ****** Affected Configuration Item – limits the report to incidents affecting one or more configuration items |
| Program Detail Report | Added in Service Pack 1, this report provides comprehensive information about all attributes of a single IT GRC program and can be filtered by:  ****** Start date  ****** End date  ****** Time Zone  ****** Program – a single, specific IT GRC program |
| Program Non-Compliance Report | Added in Service Pack 1, this report is similar to the Program Detail Report but only displays items that are negatively affecting the health of the program. This report can be filtered by:  ****** Start date  ****** End date  ****** Time Zone  ****** Program – a single, specific IT GRC program |
| Program List Report | This report lists the existing IT GRC programs and can be filtered by:  ****** Start date  ****** End date  ****** Time Zone  ****** Program – an optional field. If no program is specified, all programs in the system will be returned.  ****** Owned By – an optional field that will limit the list of returned programs to ones owned by the specified user  ****** Status |
| Program Readiness Review Status Report | This report lists the readiness status of an IT GRC program and can be filtered by:  ****** Start date  ****** End date  ****** Time Zone  ****** Review Start Date  ****** Review End Date  ****** Review time zone  ****** Review stage  ****** Level  ****** Priority  ****** Program  ****** Owned By  ****** Assigned to  ****** Authority document ID  ****** Status  ****** Category  ****** Type – to optionally filter the report to only include the specified types of control objectives |
| Program Scope Report | This report lists the scope of an IT GRC program and can be filtered by:  ****** Program  ****** Start date  ****** End date  ****** Time Zone |

## Predefined IT GRC Control Management Reports

The following table lists the IT GRC control management reports that are included in the Process Pack for IT GRC and a brief description of each report. The IT GRC control management reports are located in the Reporting/Compliance Reports Library/Control Management folder.

|  |  |
| --- | --- |
| Report | Description |
| Control Activity Score Report | Added in Service Pack 1, this is the primary report used to view the program’s control activities and their compliance scores. This report can be filtered by:  ****** Start date  ****** End date  ****** Time Zone  ****** Program – a single, specific IT GRC program  ****** Owned By – an optional field that will limit the list of returned control activities to ones owned by the specified user  ****** Last Score – limits the returned control activities to ones with the specified last compliance score  ****** Result Start Date  ****** Result End Date  ****** Time Zone |
| Control Activity Details Report | This report provides a comprehensive view of a single control activity and can be filtered by:  ****** Control Activity |
| Control Activity List Report | This report lists control activities in the system and can be filtered by:  ****** Start date  ****** End date  ****** Time Zone  ****** Program – an optional field. If no program is specified, all programs in the system will be returned.  ****** Owned By – an optional field that will limit the list of returned control activities to ones owned by the specified user  ****** Last Score – limits the returned control activities to ones with the specified last compliance score  ****** Result Start Date  ****** Result End Date  ****** Time Zone  ****** Authority Document  ****** Status  ****** Validation Type  ****** Level  ****** Priority |
| Control Objective Health Report | Added in Service Pack 1, this is the primary report used to view the health of your control objectives. This report can be filtered by:  ****** Start date  ****** End date  ****** Time Zone  ****** Program – a single, specific IT GRC program  ****** Owned By – an optional field that will limit the list of returned control activities to ones owned by the specified user |
| Control Management Change Report | This report displays the changes in control objectives between two points in time as specified in the Start Date and the End Date report parameters. This report allows you to click hyperlinks so that you can see additional details about control objects and control activities in the report. |
| Control Objective Details Report | This report provides a comprehensive view of a single control objective and can be filtered by:  ****** Control Objective |
| Control Objective List Report | This report lists control objectives in the system and can be filtered by:  ****** Program  ****** Authority document category  ****** Authority document title  ****** Start date  ****** End date  ****** Owned by  ****** Status  ****** Assigned to |
| Control Objective Progress Report | This report lists the progress of control objectives between two points in time as specified in the Start Date and the End Date report parameters. This report allows you to click hyperlinks so that you can see further details about control objects and control activities in the report. |
| Managed Entity Result List Report | This report lists the configuration items that are included in the scope of your IT GRC program and that are used to calculate a score for their associated control activity. This report can be filtered by:  ****** Program  ****** Control activity  ****** Result start date  ****** Result end date  ****** Time Zone  ****** Result Value |

## Predefined IT GRC Risk Management Reports

The following table lists the IT GRC risk management reports that are included in the Process Pack for IT GRC and a brief description of each report. The IT GRC risk management reports are located in the Reporting/GRC Reports Library/Risk Management folder.

|  |  |
| --- | --- |
| Report | Description |
| Program Risks Report | Added in Service Pack 1, this report lists all risks associated with the program or any control objective or control activity managed in your IT GRC program. This report can be filtered by:  ****** Start date  ****** End date  ****** Time Zone  ****** Program – a single, specific IT GRC program  ****** Owned By – an optional field that will limit the list of returned control activities to ones owned by the specified user  ****** Risk Response  ****** Rank  ****** Inherent Risk Greater Than |
| Inherent Risk Map | This report displays a scatter chart of the risks based on their likelihood to occur (on the x axis) and their impact if they occur (on the y axis). The report is divided into four quadrants which represent the risk classification and helps identify the top risks. |
| Residual Risk Map | This report displays a scatter chart of the risks based on the level of control over the risk (on the x axis) and their impact if they occur (on the y axis).The report is divided into four quadrants which represent the risk classification and helps identify the top risks. |
| Risk Details | This report lists the configuration details of a single risk and is linked from other reports. |
| Risk List by Rank Report | This report lists risks in the system grouped by Risk Rank and can be filtered by:  ****** Program  ****** Start date  ****** End date  ****** Time Zone  ****** Owned by  ****** Status  ****** Assigned to  ****** Due Date  ****** Impact  ****** Likelihood  ****** Control Level |
| Risk List Report | This report lists risks in the system and can be filtered by:  ****** Program  ****** Start date  ****** End date  ****** Time Zone  ****** Owner  ****** Rank  ****** Due Date  ****** Status  ****** Assigned to  ****** Impact  ****** Likelihood  ****** Control Level |

# Exception Types in IT GRC Programs

Exception management is essential to managing an IT GRC management program. In some instances, assessments, alerts, or incidents reveal evidence of noncompliance that relate 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 exceptions to the IT GRC 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 noncompliance 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 affect 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, they should never have been included in the program scope. To resolve this problem, the IT pro requests an exception to exclude the four virtual machines when scoring the PCI Audit program and 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 is submitted, it must be approved using Service Manager Work Item Review Activity. After approval, the exception will be applied to the IT GRC compliance scoring and reports.

# Exporting and Importing IT GRC Management Information Using Excel

You can import and export IT GRC information (including programs, control objectives, and control activities) to and from the Process Pack for IT GRC using the Process Pack for IT GRC Excel Client add-in. The following table lists the usage scenarios for the Excel Client add-in.

|  |  |
| --- | --- |
| Scenario | Description |
| Perform bulk updates to IT GRC information | Allows you to make bulk updates to IT GRC information. For example, assigning an owner to multiple control objectives. |
| Create new IT GRC information | Allows you to create new IT GRC information interactively or from other sources, such as Microsoft Excel spreadsheets. This allows you import IT GRC information from other systems or sources of IT GRC information. |

## Performing Updates to Existing IT GRC Management Information

You can make updates to existing IT GRC management information using the Process Pack for IT GRC Excel Client add-in. You can make updates to individual items or you can perform bulk updates to any number of items in the IT GRC management information, including programs, control objectives, and control activities. After you make the modifications in Excel, the Excel Client add-in automatically updates the information in the System Center Service Manager CMDB.

## Creating New IT GRC Management Information

You can create new IT GRC management information using the Process Pack for IT GRC Client add-in. You can create individual items or you can create any number of IT GRC management information items, including programs, control objectives, and control activities.

Create new IT GRC management control objective using the information in the following table.

|  |  |
| --- | --- |
| Information needed | Value |
| Program | Credit Card Processing Compliance Program |
| <IT\_GRC\_item\_type> | Control Activities |
| <control\_activity\_title> | Post IT GRC policy information on bulletin boards in all cafeterias and kitchens. |
| <control\_activity\_description> | Necessary to post IT GRC policy information on bulletin boards in public gathering places so that employees are informed of the changes. |
| <control\_activity\_procedure type> | Manual |
| <control\_activity\_type> | Policy(PCA) |
| Owner | User account to be configured as the owner of the control activity |
| <assigned\_to> | User account to be configured as the assigned to of the control activity |

# Appendix: IT GRC Operations

This section provides additional information for using the Process Pack for IT GRC.

# Retain Process Pack for IT GRC Compliance Data

By default, the System Center Service Manager data warehouse database retains information for three years. Therefore, compliance data managed by the Process Pack for IT GRC is retained in the data warehouse database for three years and then is groomed (deleted) from the database.

If you need to retain Process Pack for IT GRC compliance data longer than three years, do the following:

1. Perform regular backups of the System Center Service Manager databases to retain the compliance data longer than three years.

2. Retain the backups based on the requirements of your organization.

3. Create a duplicate of the production System Center Service Manager environment that can be used to generate reports on archived data, such as in a virtualized environment.

4. If compliance data is needed beyond a three-year period, restore the appropriate database backups to the environment created in the previous step.

5. Generate the necessary reports based on the restored archived data.

You can use any available method for performing backups of the System Center Service Manager databases. For more information about backing up System Center Service Manager, see the [System Center Service Manager Disaster Recovery Guide](http://technet.microsoft.com/en-us/library/ff625768.aspx).

# Manage Process Pack for IT GRC Applicability Groups

This section provides an overview of applicability groups in the Process Pack for IT GRC and includes procedures that you can use to work with applicability groups.

Tip

The applicability groups feature in the Process Pack for IT GRC requires the operating system version information for all configuration items in the System Center Service Manager CMDB. For more information, see the section “Create a System Center Configuration Manager Connector to Populate and Synchronize the Service Manager CMDB” in the *Process Pack for* IT GRC Evaluation and Deployment Guide.

## In This Section

About Process Pack for IT GRC Applicability Groups

 Provides an overview of applicability groups in the Process Pack for IT GRC.

How to Assign Process Pack for IT GRC Applicability Groups to Control Activities

 Describes how to assign Process Pack for IT GRC applicability groups to control activities.

## About Process Pack for IT GRC Applicability Groups

Process Pack for IT GRC applicability groups contain a list of managed computers in your environment. Each control activity can be assigned one or more applicability groups, which allows you to configure control activities to apply to specific managed computers in your environment.

First, create the Process Pack for IT GRC applicability groups based on your organization. Then, assign one or more applicability groups to the control activities in your IT GRC program.

## How to Assign Process Pack for IT GRC Applicability Groups to Control Activities

You can assign one or more Process Pack for IT GRC applicability groups to a control activity in the Service Manager Console.

To assign a Process Pack for IT GRC applicability group to a control activity

|  |
| --- |
| 1. Click Start, click All Programs, click Microsoft System Center, click Service Manager 2012, and then click Service Manager Console.  The System Center Service Manager Console starts.  2. In the Service Manager Console, in the Navigation pane, click Compliance and Risk Items.  3. In the Compliance and Risk Items pane, go to the All Compliance and Risk Items/Control Management/Control Activities/All Automated Control Activities location.  4. In the Results pane, click <control\_activity> (where control\_activity is the name of the control activity that you want to edit).  5. In the Tasks pane, click Edit.  The Control Activity property form displays.  6. On the Control Activity form, on the General tab, under Applicable Groups, click Add.  The Select Objects dialog box appears.  7. Complete the Select Objects dialog box by performing the following steps:  a. In Available objects, click <applicability\_group> (where applicability\_group is the name of the applicability group you wish to add to the control activity), and then click Add.  The applicability group appears in the Selected objects list box.  Tip  You can use the Search by name box to help search for a specific applicability group.  b. Continue to perform step 7a until all the appropriate applicability groups are selected.  c. Click OK.  The selected applicability groups appear in the Applicability Groups list box.  Tip  You can remove unnecessary applicability groups by clicking the applicability group and then clicking Remove.  8. In the Control Activity form, click OK. |

# Manage Process Pack for IT GRC User Roles

This section provides an overview of user roles in the Process Pack for IT GRC and includes procedures that you can use to work with user roles.

## In This Section

About Process Pack for IT GRC User Roles

Provides an overview of the user roles in the Process Pack for IT GRC.

Overview of Managing Process Pack for IT GRC User Roles

Describes the high-level process for managing Process Pack for IT GRC user roles.

How to Create a Process Pack for IT GRC User Role

Describes how to create a Process Pack for IT GRC user role from one of the Process Pack for IT GRC user role profiles.

How to Add a Member to a Process Pack for IT GRC User Role

Describes how to add a member to an existing Process Pack for IT GRC user role.

How to Configure the Objects that Can Be Managed by a User Role Using Windows PowerShell®

Describes how to configure the objects that can be managed by an existing Process Pack for IT GRC user role using the AddTypeToRoleScope.ps1 Windows PowerShell script.

## About 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 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).

## Overview of Managing Process Pack for IT GRC User Roles

Use the following high-level process for managing Process Pack for IT GRC user roles:



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Create groups of objects for an existing program as described in [How to Create a Group in Service Manager](http://technet.microsoft.com/en-us/library/hh519778.aspx) using the information from the following table.   |  |  |  | | --- | --- | --- | | Group name | Dynamic member class | Dynamic member criteria | | <program name> scope group | Program | <policy item> title equals <Program title> | | Shared control objectives | Control objective | <compliance policy item> shared equals Yes | | Shared control activities | Control activity | <compliance work item> shared equals Yes | | Shared risks | Risk | <compliance policy item> shared equals Yes |   For more information about groups, queues, and lists in Service Manager, see [Using Groups, Queues, and Lists in Service Manager](http://technet.microsoft.com/en-us/library/ff461050.aspx).  2. Specify the groups of objects that can be managed by user roles by using one of the following methods:   Select the four groups that were created in Step 1 and all groups that begin with ApplicabilityInstanceGroup when you create the user role. The groups are selected on the Groups page in the User Role Wizard in the Service Manager Console as described in [How to Create a User Role](http://technet.microsoft.com/en-us/library/hh495651.aspx).  Note: Depending on the number of objects selected in the groups, this process can affect the performance of Service Manager. Instead, consider using the AddTypeToRoleScope.ps1 Windows PowerShell script as described in the “How to Configure the Scope for a Process Pack for IT GRC User Role” section in this guide.   Configuring the groups after the user role is created by editing the user role. You can update the groups that are selected for the user role in the Groups section on the properties form of the user role.  Note: Depending on the number of objects selected in the groups, this process can affect the performance of Service Manager. Instead, consider using the AddTypeToRoleScope.ps1 Windows PowerShell script as described in the “How to Configure the Scope for a Process Pack for IT GRC User Role” section in this guide.   Configuring the groups after the user role is created by running the AddTypeToRoleScope.ps1 Windows PowerShell script. The advantage to this method is described in the “How to Configure the Scope for a Process Pack for IT GRC User Role” section in this guide. |

## How to Create a Process Pack for IT GRC User Role

The process for creating a Process Pack for IT GRC user role is the same as creating a System Center Service Manager user role. Create the user role based on the list of user role profiles listed in the “About Process Pack for IT GRC User Roles” section. The Compliance Program Manager or Compliance Program Implementer user role profiles are the user role profiles that are unique to the Process Pack for IT GRC.

For more information about how to create a user role in System Center Service Manager, see [How to Create a User Role](http://technet.microsoft.com/en-us/library/hh495651.aspx).

## How to Add a Member to a Process Pack for IT GRC User Role

The process for adding users as a member of a Process Pack for IT GRC user role profile is the same as adding users as members of a System Center Service Manager user role profile. For more information about how to add a member to a user role in System Center Service Manager, see [How to Add a Member to a User Role](http://technet.microsoft.com/en-us/library/hh519704.aspx).

## How to Configure the Objects that Can Be Managed by a User Role Using Windows PowerShell

After you create a Process Pack for IT GRC user role based on the Compliance Program Manager or the Compliance Program Implementer user role profiles, you need to configure the object groups (scope) that can be managed by the newly created user role. You can configure the object groups using the Service Manager Console or by running the AddTypeToRoleScope.ps1 Windows PowerShell script. The AddTypeToRoleScope.ps1 Windows PowerShell script is located in the <service\_manager\_root>\IT GRC Process Pack folder (where service\_manager\_root is the root folder where you installed System Center Service Manager).

To configure the objects that can be managed by a user role using Windows PowerShell

|  |
| --- |
| 1. Log on to the computer running the Service Manager Console with an account that has the following permissions:   Member of the local Administrators group on the computer   Administrator in Service Manager  2. Start Windows PowerShell. For guidance in doing so, see [Starting Windows PowerShell](http://msdn.microsoft.com/en-us/library/ms714415(VS.85).aspx).  3. At a Windows PowerShell command prompt, type the following command, and then press Enter (where service\_manager\_root is the root folder where you installed System Center Service Manager and server\_name is the name of the computer running System Center Service Manager).  cd “<service\_manager\_root>\IT GRC Process Management Pack”  4. At the Windows PowerShell command prompt, type the following command, and then press Enter (where user\_role is the name of the user role you created).  .\AddTypeToRoleScope.ps1 -server "server\_name" -RoleName "<user\_role>" -TypeToAdd "Software Updates"  Note  The preceding command should be entered on one line. Display limitations might cause it to display on more than one line.  5. Repeat step 4 for each the following object types, substituting them for “Software Updates” in the command in step 4:   "Knowledge Article"   "Domain User or Group"   "Software Items"   "Incident"   * “Software Updates”    "Business Service"   * "Exception" * "Configuration Manager DCM Compliant CI" * "Manual Control Activity" * "Control Objective" * "Control Activity" * "Risk"   6. Exit the Windows PowerShell command prompt.  7. Close all open windows and dialog boxes.  Note  If you make any changes to the Compliance User Roles using the Service Manager console, you will need to rerun the Windows PowerShell script because the console changes overwrite all changes made by the PowerShell script. |

## How to Hide Console Tasks that the Program Implementer Cannot Use

Although the Program Implementer role is unable to create controls or risks and add them to a program, by default the “Create Controls from Library Wizard” console task is still viewable. If a person assigned to that role tries to run the wizard, an error will display.

To remove a console task from the Program Implementer’s view

|  |
| --- |
| 1. Log in as Administrator in the Service Manager Console.  2. Go to Security and then User roles.  3. Click Create User Role and then click Compliance Program Implementer.  4. In the User Role Creation wizard, do the following:  a. Click Next on the Before You Begin page.  b. Give a name to the Program Implementer role and click Next on the General page.  c. Click Select All on the Management Packs page and then click Next.  d. Click Next on the Groups page after making the necessary configuration changes.  e. Click Next on the Queues page after making the necessary configuration changes.  f. On the Tasks page, select the Provide Access to only selected tasks radio button. In the list below the button, unselect the Create controls from library and **Create Risk from Library** tasks. |

# How Automated Control Activities are Scored Based on Managed Entity Results

Managed Entity Results (MERs) form the basis of an automated control activity’s (CA) score. A managed entity result is either a test result generated automatically using Desired Configuration Manager or a manually attested result of Compliant, Non-Compliant, Unknown, or Error. A control activity’s score is calculated at report time using the current scope and applicability group and any approved Scope or Process exceptions. When the subset of applicable MERs is determined, the CA score is calculated in the following order:

1. If the number of Compliant MERs is greater than or equal to the CA’s threshold, the CA receives a score of Meets Expectations.

2. Next, if the number of Non-Compliant MERs is greater than 100% minus the CA’s threshold, the CA receives a score of Fails Expectations.

3. If neither of the above conditions is true, the CA receives a score of Unknown.

Example Calculation 1

Assume the CA has a threshold set to 60% and 90 MERs comprised of 54 Compliant results, 14 Non-Compliant results, 4 Error results, and 18 Unknown results.

 In this case, a CA Score of “Meets Expectations” is assigned as 54 Compliant MERs is ≥ 54, 60% of the applicable results.

Example Calculation 2

Assuming the same threshold of 60% and a new set of MERs comprised of 40 Compliant MERs, 40 Non-Compliant MERs, 2 Error MERs, and 8 Unknown MERs.

 In this case, a CA Score of “Fails Expectations” is assigned as 40 Compliant MERs are not ≥ 54 (60% of the applicable results) and 40 Non-Compliant MERs are > 36 (90 total MERs x (100% – threshold%)).

Example Calculation 3

Assuming the same threshold of 60% and a new set of MERs comprised of 4 Compliant MERs, 36 Non-Compliant MERs, 14 Error MERs, and 36 Unknown MERs.

 In this case, a CA Score of “Unknown” is assigned as 4 Compliant MERs are not ≥ 54 (60% of the applicable results) and 36 Non-Compliant MERs are not > 36 (90 total MERs x (100% – threshold%)).