Quick answers to common problems

Microsoft System Center 2012 R2 Compliance Management Cookbook

Over 40 practical recipes that will help you plan, build, implement, and enhance IT compliance policies using Microsoft Security Compliance Manager and Microsoft System Center 2012 R2

Andreas Baumgarten
Ronnie Isherwood
Susan Roesner

[PACKT] PUBLISHING
enterprise
professional expertise distilled

Microsoft System Center 2012 R2 Compliance Management Cookbook

Over 40 practical recipes that will help you plan, build, implement, and enhance IT compliance policies using Microsoft Security Compliance Manager and Microsoft System Center 2012 R2

Andreas Baumgarten
Ronnie Isherwood
Susan Roesner

[PACKT] PUBLISHING enterprise professional expertise distilled

BIRMINGHAM - MUMBAI

Microsoft System Center 2012 R2 Compliance Management Cookbook

First published: October 2014

Production reference: 1251014

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78217-170-6

www.packtpub.com

Cover image by Frank (layouteam@t-online.de)

Credits

Authors

Andreas Baumgarten

Ronnie Isherwood

Susan Roesner

Reviewers

Andrew Craig

Jörgen Nilsson

Nico Sienaert

Stephan Wibier

Acquisition Editor

James Jones

Content Development Editor

Arvind Koul

Technical Editor

Dennis John

Copy Editors

Sarang Chari

Shambhavi Pai

Project Coordinator

Priyanka Goel

Proofreaders

Stephen Copestake

Maria Gould

Kevin McGowan

Indexers

Hemangini Bari

Mariammal Chettiyar

Rekha Nair

Tejal Soni

Production Coordinators

Aparna Bhagat

Nitesh Thakur

Cover Work

Aparna Bhagat

About the Authors

Andreas Baumgarten is a Microsoft MVP and works as an IT Architect with the German IT service provider H&D International Group. He has been working as an IT professional for more than 20 years. Microsoft technologies have always accompanied him, and he can also look back on more than 14 years' experience as a Microsoft Certified Trainer.

Since 2008, he has been responsible for the field of Microsoft System Center technology consulting and ever since has taken part in Microsoft System Center Service Manager 2010, 2012, and 2012 R2; additionally, he has participated in the Microsoft System Center Orchestrator 2012 and 2012 R2 Technology Adoption Program with H&D.

With his deep inside-technology know-how and his broad experience across the Microsoft System Center product family and IT management, he now designs and develops private and hybrid cloud solutions for customers all over Germany and Europe.

In October 2012, 2013, and 2014, he was awarded the Microsoft Most Valuable Professional (MVP) title for System Center Cloud and Datacenter Management.

I would like to thank my colleague Jörg Tonn from H&D International Group for his helping hand and support with Microsoft System Center 2012 Operations Manager.

The book was only possible due to the efforts of a great team. I would like to acknowledge and thank my co-authors Ronnie Isherwood and Susan Roesner.

Ronnie Isherwood, MCITP, MBCS, is a technology entrepreneur who has worked in the IT industry for more than 20 years including 15 years' experience in delivering infrastructure, systems management, and virtualization technologies to government, financial, and legal companies. He has worked with Microsoft Learning Partners as a subject matter expert and technical reviewer contributing to several MCSE courses on server and cloud. In 2014, he co-founded a software development company, JE3.COM, where he works on designing infrastructure services and software solutions for the financial services industry. Ronnie is committed to the IT community and is the founder of a Microsoft Windows user group and Chairman of BCS, The Charted Institute for IT, Jersey.

I'd like to thank Samuel Erskine for giving me this opportunity and Mélinda Isherwood for supporting me tirelessly with all my technology endeavours. I would also like to acknowledge and thank my co-authors Andreas Baumgarten and Susan Roesner for their unwavering dedication and without whom this title would not have been possible.

Susan Roesner is an IT Architect with expertise in a wide range of technologies and industries (public and private), including Fortune 500 organizations. Since 2009, she has been working in Microsoft System Center technology / IT management consulting and was responsible for Microsoft System Center Virtual Machine Manager 2010, 2012, and 2012 R2, and the Microsoft System Center Data Protection Manager 2010, 2012, 2012 R2 Technology Adoption Program, in addition to all compliance aspects within the System Center family.

Before joining H&D International Group, she worked in the finance sector and in Compliance / IT Security, working on projects such as SOX and ISMS implementations, on compliance audits (internal and external), and compliance policy/process creation.

First, I want to give a big thank you to Samuel Erskine for his great and challenging reviews that drove me toward better clarity on information I wanted to provide in the chapters. He also made it quite easy for me, as a first-time author, to understand the processes and get the job done. I also want to give thanks to Dejan Milic from H&D International Group for providing me with in-depth answers to all my questions on System Center 2012 R2 Configuration Manager.

I should also thank the team at Packt Publishing for working with us through this project. Thanks to Arvind for making sure we stuck to the schedule and to James Jones for making it so easy to work with him and for answering all my questions. Also, thanks to Stephan Wibier and Nico Sienaert, who helped make the chapters so much better with their comments and feedback.

Lastly, I want to thank my co-author, Andreas Baumgarten, who provided valuable ideas for several of the chapters and was always there when things needed to get done. Thank you to Ronnie Isherwood who took over from Samuel Erskine on such short notice to complete the last chapters and help make the book better.

About the Reviewers

Andrew Craig is a System Center Configuration Manager specialist. He has developed and delivered several Configuration Manager projects over the last 7 years in the UK and Switzerland.

He currently lives in Switzerland and works for Syliance IT Services as a senior consultant, where he actively contributes to the System Center community, speaking at community events, delivering TechNet sessions, and participating in Internet forums, such as myITForum.

Huge thanks to Samuel Erskine for introducing me to System Center back in the day in the UK and for the many adventures along the way.

Jörgen Nilsson works as a principal consultant at Onevinn AB in Sweden, working with systems management. Jörgen has over 20 years' experience in working as a consultant and is also an MCT. In 2011, he was awarded the MVP title for Enterprise Client Management. He is also an accomplished speaker and has given presentations at Microsoft Management Summit (MMS) and TechED 2014.

You can find his blog at `http://ccmexec.com`.

Nico Sienaert is 34 years old, lives in Belgium, and has more than 13 years' experience with Systems Management and related solutions. For several years, he has been working on numerous System Center implementations in Belgium and abroad.

Currently, he's working for Getronics, a world-wide system integrator, as Lead Infrastructure Consultant.

Nico is a frequent speaker on Microsoft and non-Microsoft events and writes blogs for the System Center user group in Belgium.

Microsoft awarded Nico the Microsoft MVP title for Enterprise Client Management. At this moment, he works closely with the Microsoft Product Team on Mobile Device Management.

He is the moderator of the TechNet forum for Configuration Manager MDM. Nico also works as a "virtual" employee for Microsoft as v-Technology Solutions Professional.

You can follow Nico on Twitter (`@nsienaert`) to stay up to date with the System Center landscape.

Nico believes that *technology never stops, and you always need to be prepared for the future*. Hence, he likes this quote from Wayne Gretzky:

> *"A good hockey player plays where the puck is. A great hockey player plays where the puck is going to be."*

I would like to thank my daughter, Laura, and girlfriend, Kristel, for their support in pursuing this time-consuming passion of mine—IT.

It was a great experience reviewing this book; I hope you like it.

Stephan Wibier is a senior consultant and an all-round IT geek, specializing in Microsoft Backend Services. He has specialized in OS deployment using tools, such as WDS/MDT and System Center Configuration Manager.

His interest in the IT business goes way back to the early '80s, starting with the good-old Commodore 64. After that, it was only a matter of time before the virus hit hard. He got certified in several areas of Microsoft products and still keeps up with the new and fabulous changes in the modern IT market.

Stephan is known for his pragmatic style, approaching problems as changes or opportunities.

www.PacktPub.com

Support files, eBooks, discount offers, and more

For support files and downloads related to your book, please visit `www.PacktPub.com`.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.PacktPub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `service@packtpub.com` for more details.

At `www.PacktPub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

`http://PacktLib.PacktPub.com`

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can search, access, and read Packt's entire library of books.

Why subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print, and bookmark content
- On-demand and accessible via a web browser

Free access for Packt account holders

If you have an account with Packt at `www.PacktPub.com`, you can use this to access PacktLib today and view 9 entirely free books. Simply use your login credentials for immediate access.

Instant updates on new Packt books

Get notified! Find out when new books are published by following `@PacktEnterprise` on Twitter or the *Packt Enterprise* Facebook page.

Table of Contents

Preface

Compliance is a requirement for any company regardless of its size and configuration. Being compliant will generate benefits for your company. Take your customer purchase, sales, and invoice data as an example. Regardless of where this data resides—in an Excel sheet or Customer Relationship Management system—if the server system this data is on is stolen because it was not protected, even by a simple lock, then your company has ended up having multiple problems, and you become non-compliant. In that case:

- Your company might not be able to fulfill your customer orders or send quotes, leading to loss of revenue.
- If you are not able to regain this information, you will have a reputational issue, as customers will find out about it and not trust you any longer. In the worst-case scenario, they may cancel further work with your business.
- Your business is non-compliant because you breached data protection laws which state that sensitive data should be protected.

Being compliant will not only help you to save money in the long term and potentially keep your managers out of jail, it could also lead to competitive advantages.

In recent years, more and more companies have demanded certain certifications or adherence to standards from participants in a tender. So, being compliant with certain standards will provide you with a competitive advantage.

This book will start you on your journey to creating a compliance program and realizing the benefits of implementing this program using Microsoft Security Compliance Manager and the Microsoft System Centre family.

We will start with the basic recipes that you should have as the absolute minimum and, with each chapter, add greater complexity.

Although throughout this book, we refer to System Center 2012, all examples have been tested on System Center 2012 R2.

What this book covers

Chapter 1, *Starting the Compliance Process for Small Businesses*, covers the initial recommended critical tasks to start a compliance program. It offers hands-on advice on how and where to start at a very basic level. It looks at different regulatory requirements and shows how to interpret them, how to understand the scope, and how to plan for controls.

Chapter 2, *Implementing the First Steps of Basic Compliance*, discusses and provides steps to start a compliance program with the free Microsoft Security Compliance Manager. Within the Microsoft environment, this tool, in addition to Best Practice Analyzer, offers tremendous help with no additional costs in starting a basic compliance program. The required steps are provided in the chapter.

Chapter 3, *Enhancing the Basic Compliance Program Using Microsoft System Center 2012 Configuration Manager*, provides task steps to create a GPO compliance baseline using Microsoft System Center 2012 Configuration Manager.

Chapter 4, *Monitoring the Basic Compliance Program*, provides task steps to monitor for breaches or adherence to your compliance program. Further recipes provide information on implementation and configuration/usage of Audit Collection Services, which is specifically designed for various compliance tasks.

Chapter 5, *Starting an Enterprise Compliance Program*, focuses on larger businesses that already have at least a basic IT security program in place. It is a planning chapter that provides steps leading to an enterprise-wide compliance program. It also provides explanations and examples while introducing the key steps to a successful implementation.

Chapter 6, *Planning a Compliance Program in Microsoft System Center 2012*, provides recipes on how to integrate the System Center products. The recipes use hands-on examples to show the required planning and implementation that must be made to align the System Center tools with the compliance process.

Chapter 7, *Configuring a Compliance Program in Microsoft System Center 2012 Service Manager*, is focused on recipes that aid in the creation of a compliance program using Microsoft System Center 2012 Service Manager. It provides information on how to centralize compliance information within Microsoft SCSM 2012.

Chapter 8, *Automating Compliance Processes with Microsoft System Center 2012*, focuses on automated centralization of control status information within the System Center family. In addition, it provides information on how to implement steps so that further automation is possible.

Chapter 9, *Reporting on Compliance with System Center 2012*, provides recipes on report functionalities within the System Center family. The recipes show how to create reports based on the controls created in the previous chapters.

Appendix, *Useful Websites and Community Resources*, shows that, with the System Center product family being similar to most Microsoft products, all System Center products have an extended solutions partner community. All of them have an extensive active support base on the World Wide Web. This appendix lists some of the sites that provide readymade solutions and extensive real-world dynamic content on System Center. In addition, resources are provided for compliance questions, including official (governmental) websites providing information for small businesses that want to understand their obligations, in addition to focusing resources on more technical security/compliance issues to understand the landscape that a business is working in.

What you need for this book

In order to complete all the recipes in this book, you will need a minimum of three virtual or physical servers configured with the following:

- Security Compliance Manager 3.0 and System Center 2012 R2 (or 2012) Configuration Manager
- System Center 2012 R2 (or 2012) Operations Manager with Microsoft SQL Server
- System Center 2012 R2 (or 2012) Service Manager

The following is the list of technologies the recipes depend on and their relevant versions used for this book:

- Microsoft Active Directory (Windows Server 2008 R2 and above)
- Microsoft SQL Server 2008 SP3 and above (for the System Center products)

The required software and deployment guides of the System Center 2012 R2 product can be found at the official Microsoft website at `http://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2/default.aspx`.

The authors recommend using the online Microsoft resource due to the frequency of updates to the product's requirements. Also, note that the dynamic nature of the Internet may require you to search for updated links listed in this book.

Who this book is for

The target audience of this book is administrators, security professionals, or IT managers trying trying to understand compliance capabilities. In addition, it targets compliance teams and process owners responsible for designing and implementing compliance and IT security within their businesses.

The recipes in this book start at the beginner's level and add more complexity with each chapter on compliance topics based on System Center. The ultimate goal is to provide the reader with knowledge on how to start the compliance process by understanding regulatory requirements; to enhance their existing skills in System Center with regard to compliance settings; and, most importantly, to share the experience of seasoned technology implementers.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. In addition, certain terms are used within this book. As there are no universal unique meanings to them, the most important terms are explained within the next paragraph. After that, examples are provided of the styles used and an explanation of their meaning.

The following are some terms used in the book:

Terms used in book	Description
Regulatory requirement	The laws or industry standards applicable to a business and that are imposed by authorized institutes such as a government.
(Compliance) Framework	This is a set of guidelines that details an approach designed to adhere to regulations. It outlines rules to achieve this goal based on the organization's business processes and (internal) controls.
Authority document	This specifies the requirements that a company must adhere to. They may take different forms such as laws, regulations, industry best practices, customer contracts, or internal policies. It is essential that they are similar to regulatory requirements. Sometimes, certain control objectives are spelled out in them, but most often businesses have to determine those themselves.
Control objectives	Control objectives are most often abstract. They answer the questions '"what" and "why". Therefore, they can be defined by someone who understands compliance but doesn't have an in-depth technological knowledge. For example, the German data protection law specifies that transferred customer data has to be protected. So the control objective would be "data protection".
Control activities	These are activities to help ensure that requirements, stated in policies to address risks, are met. They answer the questions of "who", "where", "when", and "how." Therefore, they have to be defined by someone who has in-depth technical knowledge. Control activities may take different forms such as approvals, segregation of duties, reviews, and so on. Based on the previous example, the control activity defines who is responsible for protecting the data, which systems to include, and how data should be protected.

Terms used in book	Description
Program	A program gives a structure to compliance management. It contains authority documents and their mapping to control objectives, control activities, and documentation for the results of those controls; it might also contain risk assessments and further documentation. Quite often it is tool-assisted.
Risk management	This is the process of identifying, assessing, and managing risks. Based on company risk level, it includes the decision on whether to minimize, monitor, or control the probability and impact of those risks. Issues with negative outcomes from those risks will be transferred, minimized, or accepted.

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "The provided path is the default one; please modify it for your configuration. On the destination system, start the `LocalGPO.msi` file."

Any command-line input or output is written as follows:

```
set /a x=1
:Start
net use o: \\<Name of a monitored Domain Controller\c$ /
User:Administrator hjghkgkjhgkjg
set /a x=%x%+1
if %x% NEQ 20 goto Start
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "Click on the Star button next to the **Active Directory Containers** label."

Warnings or important notes appear in a box like this.

Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to `feedback@packtpub.com`, and mention the book title via the subject of your message.

If there is a book that you need and would like to see us publish, please send us a note in the **SUGGEST A TITLE** form on `www.packtpub.com` or e-mail `suggest@packtpub.com`.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on `www.packtpub.com/authors`.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting `http://www.packtpub.com/support`, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from `http://www.packtpub.com/support`.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at `questions@packtpub.com` if you are having a problem with any aspect of the book, and we will do our best to address it.

1

Starting the Compliance Process for Small Businesses

This chapter covers the initial planning tasks to be worked through before you start with your compliance program. The recipes for this chapter are as follows:

- Planning the scope of the basic compliance program
- Understanding possible controls for compliance
- Evaluating the efforts of controls
- Bringing it all together into a basic compliance program

Introduction

All companies must adhere to regulatory requirements and as such, require a compliance program. For example, when a company trades, it must adhere to its local tax requirements; even a small company must have certain controls in place to ensure it remains compliant. Also, if a company accepts credit card payments, it must have controls in place to ensure it is compliant with the Payment Card Industry Data Security Standard (PCI DSS).

When creating a compliance program, it makes sense to develop processes that will benefit the business. For example, having good controls in place will simplify the audit process, lower insurance premiums, or simply protect against fines.

The purpose of the following recipes is to help you identify and plan a compliance program using System Center in conjunction with other Microsoft technologies. The examples are provided throughout the book, demonstrating how they will benefit your company.

This chapter identifies and defines the first steps in your compliance process based on regulatory standards or similar requirements and how they relate to business objectives. It provides information on how to address compliance requirements with the help of controls. It offers advice on how to interpret authority documents to extract those controls. The book specifically focuses on technical controls.

Planning the scope of a basic compliance program

Scoping is one of the keys to a successful compliance program. Irrespective of company size, you have to decide what to include and what to leave out. When scoping the requirements, take into account all the relevant business, legal, regulatory, and contractual compliance requirements. Requirements will vary from industry to industry and from country to country. Most countries have business accelerators or government agencies providing free advice; make the most of any available service to collect information for your compliance program.

Getting ready

To determine compliance requirements, different information sources can be included to assist program development during the scope-definition phase. The following list provides some potential resources:

- **Company resources**: They can include the company lawyer and internal stakeholders, such as business unit managers from the Human Resources, Finance, Operations, and Information Technology departments; they should know regulatory and contractual compliance requirements for their specific areas.
- **External resources**: They include the following:
  - **Private organizations**: This may include the Financial Accounting Standards Board, the IT Compliance Institute, or the IT Governance Institute that offer advice and information.
  - **National organizations**: They represent the industry interests and/or legal structures of a company
- **Internet resources**: Generally, they will be specific to each country; the following are some examples:
  - **US**: The Sarbanes-Oxley act is mandatory in the US and includes the regulation of financial practice and corporate governance (`http://www.soxlaw.com/index.htm`).
  - **For small business administration**: A dedicated site is available that includes all the government contacts for compliance (`http://www.sba.gov/`).

- **UK**: Companies Act 2006 (`http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf`). More information for UK businesses including information on tax or export compliance can be found on the government website at `https://www.gov.uk/`.
- **Australia**: The following website may offer a starting point: `http://www.standards.org.au/Pages/default.aspx`.
- **Germany**: Basic information is offered by the following guide: `www.bitkom.org/files/documents/BITKOM_Leitfaden_Compliance.pdf`.

How to do it...

In order to define a scope, the following steps have to be taken:

- Understand your business compliance requirements and focus on the most critical business processes. Ask yourself the question: What is the primary product or service the business offers? Understand what is relevant to achieve any process or deliver products and/or services, for example, business units, people, applications, systems, data, and devices.
- Research the regulatory, contractual, and internal requirements using external resources and internal stakeholders.

Based on the information collected, define your *in scope* and *out of scope* objectives.

How it works...

There are two aspects to scope definition. The first aspect is, "*What company assets should you include?*" The second aspect is, "*Which regulatory requirements or standards to include in your compliance program?*"

Scope definition defined by the business

From a company perspective, the scope definition will include assets, such as physical locations, business units, equipment, application systems, and so on.

For a small or medium-sized company, defining a scope based on the compliance requirements shouldn't be a problem. Most likely, everything has to be included because data of critical applications are directly used in day-to-day business operations. In this case, separating your *in scope* part of the company and the *out of scope* part of the company might prove impossible or impractical.

Many smaller companies view compliance as a daunting task and don't start it at all. To avoid this problem, a phased approach is possible. The only consideration for a successful execution of this approach is the ability to define a self-contained scope. The benefit is that results from the first step can be incorporated into the next phase to improve on the compliance process.

For larger or more complex businesses, your decision as to what to include should be based on the following considerations:

- **Physical scope**: This includes locations or business units that have to adhere to compliance obligations.
- **Logical scope**: This includes all networks, application systems, data, and devices up to endpoint devices that use/process data that are part of the compliance obligation.

In addition, avoid situations where business units, applications, systems, or devices are both in scope and out of scope, because these could lead to breaches in your compliance program. For example, if some users are processing transaction data within an application but have limited privileges, they may be considered out of scope, whereas the IT administrator may have privileges to change data and that needs to be in scope.

That means that physical or logical separation must be possible.

Scope definition defined by regulatory, standard, contractual, or internal requirements

The other question that has to be answered for scope definition is, *"What requirements have to be met in order to be compliant?"*

Questions that should be asked are as follows:

- What are the *basic* regulatory, standard, or contractual requirements that have to be met? (This will determine which authority documents to focus on as a priority.)
- Which regulatory or standard requirements create a high risk for the business in the event of a failure?

The first question is based on the size and legal structure of a business and the industry the company is based in. The following list provides three examples of compliance areas that have to be considered:

- **Tax compliance**: Regardless of the business size, tax compliance starts with creating the business and complies with controls used in most countries that demand registration of your business and regular tax declarations. These controls will include the creation of orders and invoices that show relative tax information and the recording of payments.
- **Accounting compliance**: Just as before, regardless of size, most countries have regulatory or standard requirements demanding integrity or accuracy displayed in an annual financial statement, where the type and content depend on the size and legal structure of your company.
- **IT compliance**: As with contractual requirements, these can be in the form of software license compliance or regulatory requirements, such as data protection.

As an example of IT data protection compliance, let's look at the example from the preface, where we talked about the purchase process and systems holding customer and purchase information. To most companies, the business process that requires this information or data will be critical. Therefore, it should be considered for *in scope*.

The next question that has to be answered is, "*Which regulatory, standard, contractual, or internal requirements must be met?*" Data protection laws are one of those *basic* requirements focusing on protection of the personal data held on individuals. The financial information you hold on your customers, such as their identity information, credit card, or bank information, will fall under this category. Data protection laws vary from country to country; however, they all focus on protecting the data. Ensure that you review the respective laws; information on these laws is generally available and is easy to understand. For example, the authority document of the German protection law **Bundesdatenschutzgesetz** (**BDSG**) makes it fairly easy to understand the scope as it states in Appendix to §9 paragraph 1:

1. Prevent unauthorized access to data processing systems that process or use personalized information (physical access control)
2. Prevent unauthorized usage of data processing systems (access control)

Based on those two requirements, all locations (or just rooms), applications, networks, and devices that process, transmit, or store that information should be in scope.

The **Payment Card Industry Data Security Standard** (**PCI DSS**) is an example of *high risk* for businesses that accept, process, transmit, or store credit card data. In the event of failure in complying with PCI DSS, credit card companies, such as Visa, American Express, or MasterCard, may revoke the right to process credit card data. This could prove fatal for businesses relying on credit card payments from their customers. For those businesses, PCI DSS will definitely be *in scope* for fulfillment of an authority document.

An example on how to start with scope definition

Creating a network or architecture map is a great help in order to decide what to include to fulfill the BDSG or PCI DSS requirements. Even if you include everything in your scope, it is important to understand the relationship between your application systems, data flow, and connection points to the outside, meaning everything that is beyond your company network (for example, Internet connections). As shown in the previous example, regulatory requirements focus on specific areas. The data protection laws define certain requirements that have to be met by people (user accounts), applications, systems, and devices that handle the data. You can limit the scope of those requirements to only the relevant systems, devices, or business units.

Using a phased approach, you can start simple and then add details as you move forward with your compliance program. After the initial creation, start adding details of the systems in the network map. An important piece of information is the application used (for example, Exchange), the operating system, and the data flow of your in-scope application systems.

There's more...

You can use a degree of automation to create a network map. System Center Operations Manager is one of the tools that will help to create such a map. This will ensure that an automated diagram of your network and device landscape is created in an efficient and time-saving manner. In addition, this provides dynamic updating of your network map.

System Center Operations Manager offers different views. The **Network Vicinity Dashboard** view shows the relationship between network devices and computer (Windows Server) systems. It is a good starting point for a network map.

To view the Network Vicinity Dashboard, perform the following steps:

1. Open System Center 2012 R2 Operations Manager console.
2. Select the **Monitoring** workspace.
3. Expand the **Network Monitoring** folder.
4. Choose the device class you want to see; here, we choose **Network Devices**.
5. Go to the **Tasks** pane and click on **Network Vicinity Dashboard**.
6. The dashboard opens. Select **Show Computers** in the toolbar on top of the dashboard to view network and computer systems.

Optionally, to change the level of connections displayed in the dashboard, change the value of **Hops** in the toolbar.

Understanding possible controls for compliance

This recipe identifies controls that may be used to fulfill compliance requirements. In addition, it maps those controls to technologies and tools such as System Center.

Getting ready

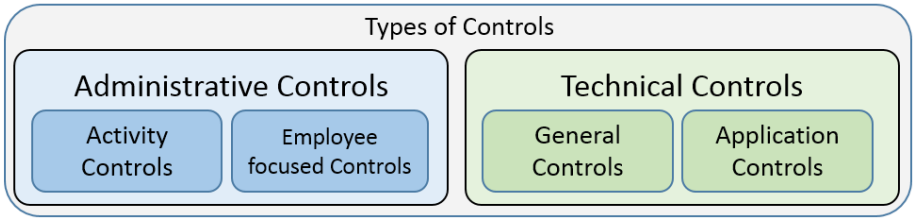
Understand your business and the scope for the compliance program based on the *Planning the scope of a compliance program* recipe.

How to do it...

Controls have two aspects to consider. On one hand, controls will provide you with a handle to fulfill compliance requirements. On the other hand, controls help you define processes and how tasks are done within the company. The most important thing to remember is *keeping it simple*. Most authority documents demand evidence of compliance but allow you to decide on the actual implementation and use of technology. Wherever possible, use automated controls based on the company's existing technologies.

The type of control implemented as part of the compliance process depends on the acceptance of your auditor, scope, the criticality of the requirement, or (simply) the budget and resources available.

The following illustration provides an overview of the type of controls:



The controls are explained as follows:

- **Administrative controls**: They are most often process-related controls. For example, they influence or shape the **activity** of a process. Another example is that they reduce inefficiency and/or inconsistency.
- **Employee-focused controls**: They could include training, such as security awareness. The goal is to ensure that the employee knows what he or she is supposed to do and how.
- **Technical controls**: They focus on controls related to technical systems.
- **General controls**: They focus on the overall IT environment. The goal is to ensure that all IT operations are running in a secure and failure-free manner.
- **Application controls**: They are, as the name indicates, focused on the application level. The goal is to ensure that the processing, saving, exporting, and so on of data are correct. For example, technical controls exist to ensure the principles of orderly bookkeeping.

Regardless of compliance requirements, the implementation of administrative and technical controls is essential to ensure the survival of your company. Without any controls, the orderly conduct of business is not possible. In almost any company, some controls exist; however, they might not be obvious, as they are already integrated into the technologies used, or they may exist and not be documented.

There are also different characteristics to controls. Those include the following:

- **Manual controls**: They are always performed by a person.
- **Automated controls**: They are performed by an IT system.
- **Preventive controls**: They try to guard against a risk or an undesired situation from occurring.
- **Detective controls**: They collect data and try to discover inconsistency or whether a risk has occurred based on the collected data. Therefore, the undesired event has taken place, but it will be reported in some way to act upon.

With regard to the fulfillment of compliance requirements, the characteristic of a control must be weighted differently. For example, the most desirable control is an automated, preventive one followed by an automated detective one. Automated controls are viewed as more consistent and are not subject to personal interpretation. Therefore, an auditor will always favor those over manual ones. Keep this in mind when deciding on controls.

How it works...

The kind of control to use always depends on the situation of the company and the risk the control is supposed to address. Several factors influencing the decision of controls are listed here:

- The size of your company
- The legal structure of the company
- Services or products offered
- Employee qualifications

First, let's focus on an **administrative control**. One requirement might be to ensure the prevention of process inconsistency. The risk might be process inefficiency or an undesired activity by an employee. One example is having the right to enter supplier or customer data including financial data and the right for payment up to a certain limit. In this case, the employee could alter the bank details and then issue a payment; alternatively, the employee could split a payment into two if the bill is higher than his or her allowed payment limit.

The most desired control would be an **automated preventive** one. In this example, a role-based access control would prevent the first example, as most modern purchase order systems allow the creation of roles and tying those to certain rights or areas. The preventive measure here provides segregation of duty by splitting the process between two employees, preventing risk.

An **automated detective** control could be to check whether bank information for a certain supplier or customer has been changed right before a payment. To mitigate the second example, check if several payments have been made within a short timeframe with the same reference number.