

Keeping Up With Security and Compliance on IBM Z

Bill White

Didier Andre

Lindsay Baer

Julie Bergh

Giovanni Cerquone

Joe Cronin

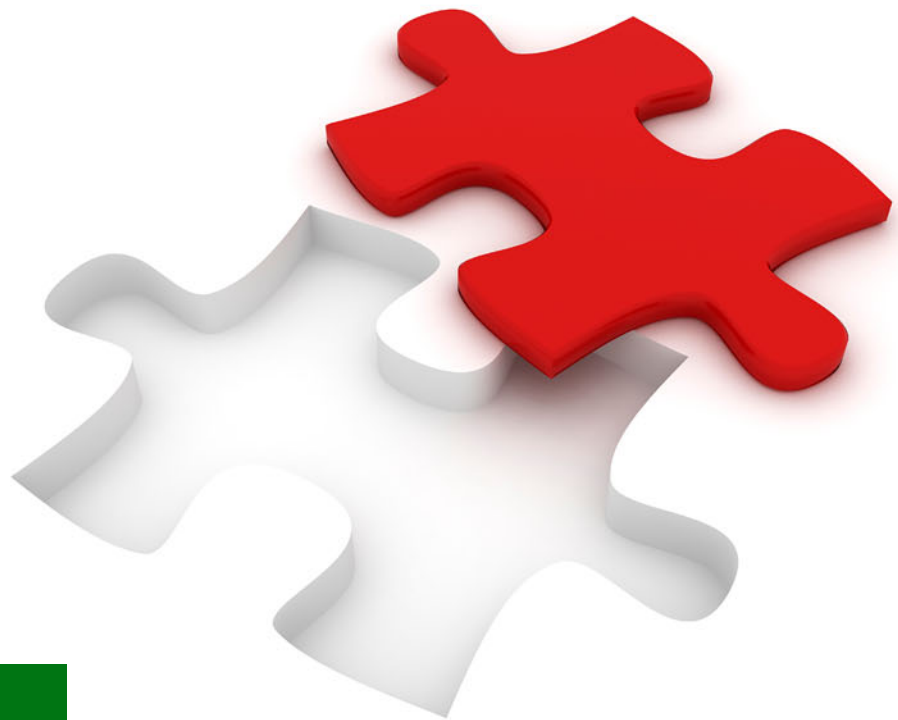
Diego Encarnacion

Wayne O'Brien

Marius Otto

Toobah Qadeer

Laurie Ward



 **Security**

IBM Z



IBM Redbooks

Keeping Up With Security and Compliance on IBM Z

June 2023

Note: Before using this information and the product it supports, read the information in “Notices” on page vii.

First Edition (June 2023)

This edition applies to IBM Z Security and Compliance Center Version 1 Release 1.0.7 (5655-CC1).

© Copyright International Business Machines Corporation 2023. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	vii
Trademarks	viii
Preface	ix
Authors	ix
Now you can become a published author, too!	xi
Comments welcome	xi
Stay connected to IBM Redbooks	xi
Chapter 1. Compliance as a top priority and challenge	1
1.1 What is a compliance posture	2
1.1.1 What regulations apply to your business	2
1.2 Understanding the challenges for IBM Z	3
1.2.1 Applying regulatory requirements can be ambiguous	4
1.2.2 Gathering compliance evidence is a costly effort	4
1.2.3 A compliance posture can change (drift) over time	5
1.2.4 Creating compliance reports is time-consuming and error-prone	5
1.2.5 A challenge for auditors to obtain trustworthy data	5
1.3 IBM Z Security and Compliance Center fits into your security strategy	6
1.3.1 Compliance mapping	6
1.3.2 Increasing speed through automation	7
1.3.3 Managing compliance drift	7
1.3.4 Creating customizable reports	8
1.3.5 Building auditor trust	8
1.4 Building blocks of regulatory frameworks	9
1.5 Targeted user roles and authorization controls	10
1.6 A closer look at IBM Z Security and Compliance Center	11
Chapter 2. Staying on top of security and compliance	13
2.1 Security posture versus compliant posture	14
2.2 Where are you on your security and compliance journey	15
2.3 Knowing your options	16
2.4 Establishing a baseline	18
2.5 Scheduling regular reviews and audits	18
2.6 Identifying the most vulnerable areas	22
2.7 Performing gap analysis and risk assessment	23
2.8 Creating an action plan	26
Chapter 3. Understanding the solution	27
3.1 Reference architecture	28
3.1.1 Evidence collection	28
3.1.2 Evidence presentation	30
3.2 Workflow for a validation scan	31
3.2.1 A closer look at z/OS Compliance Integration Manager processing	32
3.3 A single source of the truth	33
3.3.1 SMF considerations	37
3.4 Solution-defined roles and responsibilities	38
3.5 Evidence collection and reports	40
3.5.1 Running a scan	42

3.5.2	Generating a report	44
3.6	Solution prerequisites	46
3.6.1	Requirements for deploying Red Hat OpenShift Container Platform on IBM zCX for Red Hat OpenShift	46
3.6.2	Requirements for deploying Red Hat OpenShift Container Platform in virtual machines	47
3.6.3	Operating system requirements	48
3.6.4	z/OS middleware requirements	48
3.7	Deployment readiness	48
Chapter 4. Exploring security and compliance use cases		51
4.1	Use case 1: Using a predefined profile to prepare for an audit	52
4.1.1	Problem statement	52
4.1.2	Solving this challenge with IBM Z Security and Compliance Center	52
4.1.3	Looking forward	54
4.2	Use case 2: Using a custom profile to prepare for an audit	54
4.2.1	Problem statement	54
4.2.2	Solving this challenge with IBM Z Security and Compliance Center	55
4.2.3	Looking forward	56
4.3	Use case 3: Providing compliance evidence for an auditor	57
4.3.1	Problem statement	57
4.3.2	Solving this challenge with IBM Z Security and Compliance Center	57
4.3.3	Looking forward	58
4.4	Use case 4: Reviewing compliance at a high level	59
4.4.1	Problem statement	59
4.4.2	Solving this challenge with IBM Z Security and Compliance Center	59
4.4.3	Looking forward	60
4.5	Use case 5: Reviewing compliance on a recurring basis	60
4.5.1	Problem statement	60
4.5.2	Solving this challenge with IBM Z Security and Compliance Center	60
4.5.3	Looking forward	61
4.6	Use case 6: Monitoring a specific component for compliance drift	62
4.6.1	Problem statement	62
4.6.2	Solving this challenge with IBM Z Security and Compliance Center	62
4.6.3	Looking forward	63
Chapter 5. Validating security and compliance postures		65
5.1	Preparing IBM Z Security and Compliance Center	66
5.1.1	Defining a scope	66
5.1.2	Optional: modifying goal parameters	70
5.2	Using a predefined profile to prepare for an audit	72
5.2.1	Viewing existing profiles	73
5.2.2	Starting a new scan	74
5.2.3	Viewing the scan results	76
5.3	Using a custom profile to prepare for an audit	79
5.3.1	Creating a custom profile by using an existing profile	80
5.3.2	Creating a custom profile from scratch	82
5.4	Providing compliance evidence for an auditor	88
5.5	Reviewing compliance at a high level	93
5.6	Reviewing compliance regularly	98
5.7	Monitoring a specific component for compliance drift	100
Appendix A. How to find and remediate failing goals		101
	Identifying failing controls that need further investigation	102

Finding the suggested remedial area from a failed goal	104
Appendix B. SMF record type 1154 overview.	107
From where are records collected	108
Application domain	108
CICS	108
IBM MQ	109
IMS	109
Db2	109
Storage domain	109
DFSMSdfp	110
DFSMSRMM	110
DFSMSshm	111
DFSMSdss	111
Network domain	111
z/OS domain	112
Console	112
UNIX Systems Services	113
SMF	114
Security domain	114
RACF	114
ICSF	114
CPACF	115
Abbreviations and acronyms	117

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.


COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

CICS®	IBM z16™	z/VM®
Db2®	RACF®	z15®
IBM®	Redbooks®	z16™
IBM Services®	Redbooks (logo)  ®	zEnterprise®
IBM Z®	z/OS®	

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat, JBoss, and OpenShift are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Preface

Non-compliance can lead to increasing costs. Regulatory violations involving data protection and privacy can have severe and unintended consequences. In addition, companies must keep pace with changes that arise from numerous legislative and regulatory bodies. Global organizations have the added liability of dealing with national and international-specific regulations.

Proving that you are compliant entails compiling and organizing data from multiple sources to satisfy auditor's requests. Preparing for compliance audits can be a major time drain, and maintaining, updating, and adding new processes for compliance can be a costly effort.

How do you keep constant changes to regulations and your security posture in check? It starts with establishing a baseline: knowing and understanding your current security posture, comparing it with IBM Z® security capabilities, and knowing the latest standards and regulations that are relevant to your organization. IBM Z Security and Compliance Center can help take the complexity out of your compliance workflow and the ambiguity out of audits while optimizing your audit process to reduce time and effort.

This IBM Redbooks® publication helps you make the best use of IBM Z Security and Compliance Center and aid in mapping all the necessary IBM Z security capabilities to meet compliance and improve your security posture. It also shows how to regularly collect and validate compliance data, and identify which data is essential for auditors.

After reading this document, you will understand how your organization can use IBM Z Security and Compliance Center to enhance and simplify your security and compliance processes and postures for IBM z/OS® systems.

This publication is for IT managers and architects, system and security administrators, and security auditors and Chief Information Security Officers (CISOs).

Authors

This book was produced by a team of specialists from around the world working with IBM Redbooks.

Bill White is an IBM Redbooks Project Leader and Senior IT Infrastructure Specialist at IBM® Poughkeepsie, New York.

Didier Andre is a Senior Technical Specialist with expertise in IBM Z Security working for the IBM Washington Systems Center. He joined IBM France in 2001 as an experienced system programmer supporting multiple clients before moving to the US in 2015, where he worked for IBM Systems Lab Services as a security expert and leading the security team over 6 years.

Lindsay Baer is a content designer at IBM Poughkeepsie, where she creates various resources for users to learn about and interact with products. She has worked in the education design space for over 10 years and holds a Master of Science degree in Instructional Technology & Media from Columbia University. Her area of expertise includes products across the IBM Z security portfolio. She has written extensively for IBM Z content solutions.

Julie Bergh is an IBM Z Security Technical Lead for the Americas. She comes from a long career on the front lines of the cybersecurity practice as a CISO, Architect, Consultant, Specialist, and Audit Director. During her career, Julie has regularly shared her accredited expertise in IBM Z Security.

Giovanni Cerquone is an IBM Certified Expert IT Specialist and Open Group Master Certified Technical Specialist working for IBM Infrastructure supporting multiple clients with a focus on z/OS security. He has over 35 years of experience with IBM mainframe technologies, and joined IBM in 2007. Giovanni holds a degree in Computer Science from Central de Venezuela University, majoring in Database Management and Mathematics. His areas of expertise include z/OS security, IBM CICS® TS, IBM RACF®, the IBM zSecure suite of products, and others. Giovanni is a security migration specialist who has led complex migrations from CA ACF2 and CA Top Secret to RACF for multiple clients.

Joe Cronin is the North American lead Cybersecurity subject matter expert (SME) in IBM Services®. He has been a systems programmer and engineer, presenter, and educator for over 40 years. His focus has been in security architecture, governance, compliance, audit, identity management, and design. He has a broad depth of knowledge across IBM z/OS and distributed systems.

Diego Encarnacion is a Design Researcher and User Experience Designer who is based out of Poughkeepsie, New York. He started his career in design 5 years ago at IBM, and has focused on improving the IBM Z Security portfolio through user insights, spanning security compliance, threat management, and AI use cases for security. He leads the IBM Z Security Design team.

Wayne O'Brien is a content developer at IBM Poughkeepsie, where he develops user manuals and online help for various software products. He holds a Master of Science degree in Technical Communications from Rensselaer Polytechnic Institute (RPI) of Troy, New York. Wayne has written extensively on computer security, z/OS installations and upgrades, and IBM z/OS Management Facility (IBM z/OSMF).

Marius Otto is a Senior IBM Z Security Technical Sales Specialist from The Netherlands, with 30 years of mainframe experience, ranging from application programming to system programming and technical sales. With almost 15 years at IBM, Marius spent a few years in the IBM zSecure development lab, where he gained valuable experience in the IBM zSecure suite and mainframe security in general. He recently returned to Technical Sales, focusing on IBM Z Security to lead the EMEA team that helps clients secure the most securable platform in the world.

Toobah Qadeer is a brand technical specialist with IBM Z Security and has been with IBM since 2018. She holds a degree in Mathematics and has a keen interest in security technologies on the mainframe. As the UKI IBM Z Security lead, Toobah's areas of expertise include IBM zSecure suite, IBM Z Multi-Factor Authentication, and z/OS security. She has valuable experience working with clients to understand their concerns and secure their platforms against cyberthreats.

Laurie Ward is an IBM software engineer who has worked at IBM for over 35 years on IBM mainframe software. She worked for 20 years as a designer and developer for RACF product functions on z/OS and IBM z/VM®. She has expertise in IBM z/OS® security and integrity, and recently helped collect z/OS compliance data points for the IBM Z Security and Compliance Center.

A special thanks to the following people for their contributions to this project:

Anuja Deedwaniya, Cecilia Carranza Lewis, Pradeep Parameshwaran, Eysha Shirrine Powers, Eva Yan, Michael Zagorski

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at: ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:

ibm.com/redbooks

- ▶ Send your comments in an email to:

redbooks@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, IBM Redbooks
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- ▶ Find us on LinkedIn:

<http://www.linkedin.com/groups?home=&gid=2130806>

- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>

- ▶ Stay current on recent Redbooks publications with RSS Feeds:

<http://www.redbooks.ibm.com/rss.html>



Compliance as a top priority and challenge

The IT world, particularly in the last decade, is a world that is dominated by regulatory compliance. It is common to see new regulatory frameworks, across all industries and the world, introduced at an ever-increasing rate. Many reasons exist for this trend, including how the cost of a data breach today can be astronomical. A study that was conducted by the [Ponemon Institute](#) found that the average cost of a single breach to a company's data is \$4 million, and a study that was conducted by the [Association for Intelligent Information Management](#) found that the average cost to a corporation for a regulatory non-compliance was \$14.82 million.

Further, the public is becoming more aware of the need for data privacy and data protection, especially for the organizations that process sensitive data, such as personal identifiable information (PII). How banks, government entities, and other crucial organizations manage our personal data has come to be both a moral and business imperative. As IBM Z exhibits its security strengths to the rest of the industry, we know that properly implementing and displaying sound security and compliance postures is a top goal for organizations and enterprises worldwide.

These reasons are precisely why IBM developed a strategy for compliance on its platforms. We understand from conversations with our clients that they need clear mappings of regulatory frameworks to IBM Z security capabilities. We also understand that the process for collecting evidence of information, security controls, and demonstrating compliance with auditors is manual, costly, and time-consuming.

A solution that can help address today's compliance challenges and untangle the audit process is IBM Z Security and Compliance Center. It provides compliance mapping against established security controls, which simplifies the experience for auditors and evidence collectors. Using an intuitive dashboard, your organization can collect compliance data from the IBM Z platforms through automated scans and generate custom reports for auditing purposes. This solution saves valuable time and effort and helps your organization manage compliance drift and changes to your security posture.

This chapter covers the following topics:

- ▶ 1.1, “What is a compliance posture” on page 2
- ▶ 1.2, “Understanding the challenges for IBM Z” on page 3
- ▶ 1.3, “IBM Z Security and Compliance Center fits into your security strategy” on page 6
- ▶ 1.4, “Building blocks of regulatory frameworks” on page 9
- ▶ 1.5, “Targeted user roles and authorization controls” on page 10
- ▶ 1.6, “A closer look at IBM Z Security and Compliance Center” on page 11

1.1 What is a compliance posture

Security and compliance are two concepts that are often spoken of interchangeably, but significant differences exist between them. For example, compliance regulations cyberthreats regulatory bodies and tend to evolve over time. In contrast, cyberthreats are constant, unpredictable, and always changing. Depending on the role that you serve in your organization, you might focus on ensuring compliance with industry regulations or you might focus on blocking or mitigating incoming cyberthreats.

Compliance is adherence to a regulatory framework. A system's compliance status (its compliance posture) is measured in “snapshots” at various points in time.

Compliance starts with identifying what data is present and what data must be protected. Worldwide, many standards and regulations are established for protecting sensitive data. Most of these standards are concerned with protection of data:

- ▶ In storage (data at-rest)
- ▶ During transactions (data in-use)
- ▶ While traversing network connections (data in-flight)

Although some standards specify the technologies that are required for compliance, encryption can be applied to achieve compliance for all of them. In addition, often there are requirements for granular access control, authentication services, and periodic auditing.

1.1.1 What regulations apply to your business

A critical need is to determine what guidelines and rules meet your regulatory needs. Here are examples of well-known regulatory frameworks:

- ▶ Payment Card Industry Data Security Standard (PCI DSS)
- ▶ Health Insurance Portability and Accountability Act (HIPAA)
- ▶ Control Objectives for Information and Related Technologies (COBIT)
- ▶ International Organization for Standardization (ISO)

Many businesses and governmental organizations use the National Institute of Standards and Technology (NIST) as a starting base line. Then, they might apply stronger standards when wanted.

The regulations that apply to various industries are frequently updated to reflect what is happening in the cybersecurity aspect of their industries. Laws, policies, and regulations might differ from one geographic location to the next. Many companies set rules that are stronger than their local governing entity or establishments.

As examples, let us look at a few of the various industries:

- ▶ Healthcare companies must ensure patient privacy, safety, and security.
- ▶ National and local governments face organizational challenges in meeting the evolving expectations of citizens and businesses. Examples include ensuring that government employees can access their data anywhere at any time while having proper controls in place to secure citizens' data.
- ▶ Academic institutions must ensure the privacy of their students' records and personal information.
- ▶ National energy and electrical infrastructure must be safeguarded to eliminate risk and prevent disruption in the power grid.
- ▶ Retail and consumer businesses must secure consumer data and personal information.
- ▶ Telecommunications and media companies must ensure that customer data and data-in-flight are not compromised and that networks are secure.
- ▶ Travel and shipping firms must ensure the safety of travelers and cargo.
- ▶ Automobile manufacturers, with automobiles becoming increasingly computer-based, must ensure that vehicles are secure from malicious hacking.
- ▶ As manufacturers increase the level of automation in factories and rely more on the Internet of Things (IoT), they require safeguards for everything in the supply chain, from third-party vendors to robots on the factory floor.

For highly regulated industries, achieving continuous compliance is a critical step toward protecting customer and application data. Historically, that process was difficult and manual, which placed organizations at risk. It is difficult to keep up with the regulations without some tool to gather information and compare to the latest regulations. Now, with IBM Z Security and Compliance Center, you can integrate automatic security and compliance checks into everyday workflows that are designed to minimize risk.

For more information and a further explanation of security and compliance postures, see 2.1, “Security posture versus compliant posture” on page 14.

1.2 Understanding the challenges for IBM Z

Preparing for a compliance audit can be resource-intensive and tedious. The process can require dozens of specialized professionals and months to complete a single report. When an audit report is ready for review, the auditor must make sense of information from an IBM Z perspective. This manual process is difficult, lengthy, and can cause confusion and frustration for all stakeholders who are involved.

Many factors contribute to the painstaking experience of manually conducting an audit. With security standards frequently adapting to our ever-changing world, it is challenging to stay on top of each new update. Doing so requires access to experts, research, and lots of patience. Auditors, who often have little experience with IBM Z environments, in turn have difficulty interpreting compliance standards outside of a distributed computing system. Although security regulations and regular compliance audits are necessary to help businesses safeguard their data, a solution that can simplify the audit process is needed.

How do we identify what compliance rules should be followed and how do we consistently check that we are meeting and enforcing the rules?

In an IBM User Research study over multiple years, we found that there are four primary challenges that staff face when preparing for an audit:

- ▶ Applying regulatory requirements can be ambiguous.
- ▶ Gathering compliance evidence is a costly effort.
- ▶ Your compliance posture can change (drift) over time.
- ▶ Creating compliance reports is time consuming and error prone.
- ▶ For auditors, it can be challenging to obtain trustworthy data.

Examine each challenge in the sections that follow.

1.2.1 Applying regulatory requirements can be ambiguous

Understanding how regulatory requirements, both internal and external, apply to IBM Z can be challenging. Regulations are sometimes written in vague legal language, and are often written with distributed environments in mind.

For example, a core requirement for PCI DSS is to “isolate” all workloads that process cardholder data. On a Linux, UNIX, or Windows system, this isolation is achieved by “standing up” a new physical system. In contrast, achieving an isolated environment on an IBM Z platform is done through workload separation and virtual isolation.

Sometimes, it might seem impossible to achieve compliance because certain requirements seem incompatible with IBM Z platforms. For example, many regulations require systems to run “anti-virus software”. Although this task is simple to achieve on Linux, UNIX, or Windows, traditional anti-virus software on IBM Z does not exist because the platform never has had a virus in its history due to safeguards built into the platform's architecture at all layers of the stack.

This challenge is exacerbated by the fact that the auditors themselves have varying degrees of proficiency in IBM Z security. Although some auditors understand how access control and data protection (for example) work on IBM Z, other auditors might not understand its basic premises, so their interpretations of what must be done to achieve compliance might differ drastically.

This situation presents staff with uncertainty and increased risk of audit failure because there is no common understanding of what must be done to achieve compliance.

As a result, your staff might spend large amounts of resources on compliance without any sense of whether the auditor will accept it as valid. In fact, the auditors themselves might require hours of education on the platform.

To meet this challenge, your organization needs a clear one-to-one translation of how each regulatory requirement can be achieved by using IBM Z capabilities. For more information about this topic, see 1.3.1, “Compliance mapping” on page 6.

1.2.2 Gathering compliance evidence is a costly effort

Collecting the information that is needed to demonstrate compliance to an auditor can be a cumbersome task because an audit encompasses the entire IBM Z stack, so many subject matter experts (SMEs) (10 on average, although this number might go as high as 20) might be involved in giving the Compliance Lead the information that they need. On average, it is estimated that collecting data can take months, and the driver of this effort must coordinate with individual component owners, entering information manually into a spreadsheet, and making this data comprehensible to an auditor (who might not understand the platform).

To meet this challenge, your organization needs an automated way to collect compliance data across the IBM Z platform. For more information, see 1.3.2, “Increasing speed through automation” on page 7.

1.2.3 A compliance posture can change (drift) over time

Gathering compliance evidence is not a trivial task, even just to check a compliance posture at one point in time. Auditors often want to know whether your environment trends in a positive or negative direction. Given how long it takes to gather evidence without a centralized solution that automates the process, achieving a sense of compliance drift is unfeasible.

To meet this challenge, your organization needs an expedient way to track compliance drift over time, in a format that is easily understood. For more information, see 1.3.3, “Managing compliance drift” on page 7.

1.2.4 Creating compliance reports is time-consuming and error-prone

To demonstrate your organization's compliance standing, the Compliance Lead might be asked to create a report of the system's compliance posture that is shared with stakeholders and auditors. Typically, creating such a report is no small effort, and it might need to be done multiple times as non-compliance issues are found and addressed. Further, different stakeholders require different levels of report details. Executives might require a high-level overview, and your security team likely needs a granular description of each goal and the logic that is used to check it. Lastly, without a standard format, compliance reports can lack uniformity.

To meet this challenge, your organization needs a facility for generating compliance reports quickly as often as needed, with adjustable levels of detail, and in an attractive visual format. For more information, see 1.3.4, “Creating customizable reports” on page 8.

1.2.5 A challenge for auditors to obtain trustworthy data

At the heart of any audit is the need for *trustworthy* data. “Trustworthy” can mean different things to different auditors, but generally, it means that the data that is submitted for an audit is clearly timestamped, from a clear source, and immutable. Today, auditors often have trouble verifying whether compliance data that is submitted for IBM Z platforms is trustworthy.

To meet this challenge, your organization needs compliance reports that auditors can trust. For more information, see 1.3.5, “Building auditor trust” on page 8.

1.3 IBM Z Security and Compliance Center fits into your security strategy

IBM Z Security and Compliance Center is the latest progression in the IBM security strategy for compliance. It revolves around three major initiatives that have been undertaken by IBM Z development:

- ▶ For high-priority regulatory frameworks, clearly define the types of data across the various components that can be used to help demonstrate compliance with certain requirements. This action is a “translation” of regulatory frameworks to IBM Z specific security controls. IBM domain experts use these translations in ways that reduce ambiguity in the IBM Z audit process (see 3.2, “Workflow for a validation scan” on page 31).
- ▶ Collect and report compliance data regarding high-priority regulatory frameworks. With the introduction of the IBM Z Security and Compliance Center, and a standardized means of generating compliance data (SMF 1154 record types), you have an efficient and trustworthy way of preparing for an audit while reducing the time and resources that are spent on compliance (see 3.3, “A single source of the truth” on page 33).
- ▶ Enhance the IBM Z platform in ways that make it easier to become compliant, by investing in solutions that directly address high-priority requirements (see 2.3, “Knowing your options” on page 16).

1.3.1 Compliance mapping

One of the most challenging aspects of audit preparation is staying current with ever-changing security standards and then interpreting them for IBM Z environments. To combat this challenge, IBM convened over 40 SMEs (internal and external) to work together on a solution. These leading industry experts, representing professionals from auditing firms, CIOs, and lab services, contributed their expertise to map existing standards to the IBM Z environment, ensuring reliability and accuracy in the process. This effort led to the ability for one-for-one mapping against set standards, removing the complexity and ambiguity from the audit reporting process.

Compliance mapping is at the heart of the IBM Z Security and Compliance Center. It enables users to check their compliance posture against security standards like PCI DSS, NIST SP800-53, and Center for Internet Security (CIS), covering nearly every industry in the private and public sector. For z/OS, the IBM Z Security and Compliance Center brings together evidence from RACF, UNIX Systems Services, CICS, IBM Db2®, IBM MQ, Communications Server (TCP/IP, FTP, TN3270E, CSSMTP, SSHD, and InetD), ICSF, Consoles, DFSMS (DFP, RMM, Hardware Security Module (HSM), and DSS), IMS, and SMF.

Through an interactive dashboard, you can scan those resources to generate reports quickly and comprehensively. Workflows built in to the solution make this process seamless through automated fact collection and standards mapping. The collected facts found through this process are compared against the security standards that you defined in your profile.

The IBM Z Security and Compliance Center provides pre-determined profiles for PCI DSS, NIST SP800-53, and CIS, and pre-built goals. These goals are individual checks for validations against control and subcontrol level rule changes over a period. IBM Z Security and Compliance Center also provides the flexibility to create custom profiles, and you can choose to add or omit various checks to those profiles depending on your needs.

1.3.2 Increasing speed through automation

When teams are asked to comply with an audit, it can take weeks or months for skilled individuals to sift through information that is needed by the auditor. This process fails to holistically capture drift, and it requires the involvement of experts and other specialized professionals, which can be an arduous and cumbersome experience.

By introducing automation through the IBM Z Security and Compliance Center, the time and resources that are needed for an audit are reduced, which frees up teams and individuals to get back to their daily work.

When you conduct a scan of all compatible IBM Z components, a signal is sent to the targeted components to generate compliance data in enhanced z/OS SMF records. Initial user research indicates that the need for IT expertise is reduced by over 40%, enabling resources to be rededicated back to other core business efforts. By expediting the data-gathering process through automation, you can schedule scans on an ongoing basis without having to sacrifice time or resources. As a result, you can spend more time being proactive in strengthening your compliance posture.

In addition, many factors such as fostering new technology and tactics to drive business can put a strain on an organization's continuous compliance. One of the keys to solving this issue is automation, so it is a vital step in the journey for continuous compliance.

1.3.3 Managing compliance drift

Traditionally, creating a compliance report has been a resource-intensive process, which often takes months to complete. The manual nature of these reports means that by the time one is completed, the information that is included might be outdated or missing key trends that occurred. This occurrence is known as *drift*, and it can jeopardize the standing of your compliance. Managing IBM Z compliance manually has other side effects as well, including staying on top of maintenance, updates, and adding new processes for compliance, which all can contribute to drift.

With the IBM Z Security and Compliance Center, you can track your compliance drift over time with dashboard-style visualizations that display historical compliance scores. This centralized, interactive dashboard provides a consolidated view of baseline standards for the IBM Z environment, which you can use to help identify any potential drift from those standards. This dashboard grants you continuous monitoring, which helps you stay current. Reports can be generated over a period and synced together to create a full picture of your compliance posture.

You can use these reports to identify whether you are managing your environment according to set security standards, and if you are introducing risk in how you are operating your environment. Dynamic monitoring means that you can be more confident in understanding the scope of your drift, and therefore create informed plans to remediate it.

1.3.4 Creating customizable reports

IBM Z Security and Compliance Center provides great flexibility as you prepare for an audit. The central dashboard delivers an interactive view of your compliance posture and details, including a drift view that is based on control deviations and detailed scan results.

Through this interface, you can generate detailed reports, display the actual logic that is used to validate collected facts, or configure information that facilitates compliance. You also can customize profiles with goals that map to several regulatory frameworks, and change parameters or determine compensating controls. From there, you can store your collections in a database to visualize historical facts, validate against them, and refer to historical compliance scores to track drift.

With each report that you generate, you see the context around the severity of control deviations from PCI DSS, NIST SP800-53, and CIS. If compensating controls are in order, then you can use reports to demonstrate your compliance posture and ensure that it is as rigorously regulated as the original requirement. Insights from these reports can be used to help you determine ways to exceed baseline security standards wherever possible.

With IBM Z Security and Compliance Center, customized reports can give stakeholders across the board the level of specificity they are looking for. High-level reporting serves the needs of executives, and the detailed mapping of regulatory frameworks to IBM Z Security controls delivers on what staff and auditors require.

Whether you are a business line owner, Chief Information Security Officer (CISO), engineer, system administrator, or auditor, IBM Z Security and Compliance Center can take complexity out of the audit process and help track continuous compliance of your infrastructure.

1.3.5 Building auditor trust

The primary concern for auditors is compliance validation. Auditors must scrutinize collected facts to determine whether they indicate compliance, which is made difficult when they often represent only a single point in time. Job conditions add to the challenge because auditors are frequently shuffled from organization to organization, must quickly immerse themselves in new environments, and strain to translate regulations that might be too broad or complex. Furthermore, auditors might be unfamiliar with IBM Z environments, which can increase the time that it takes to interpret facts and affect the accuracy of their validation.

The IBM Z Security and Compliance Center is designed to ease some of the largest challenges that auditors face when assessing compliance. With this solution, auditors can access reports that provide high-level management views and more detailed information. Compliance mapping enables auditors to quickly compare collected facts against security standards, and the reports are written in plain, industry-wide language. These reports are marked by timestamps and cannot be modified, and they include a visible chain of custody, which is critical for trust. Auditors can use these reports to track a compliance posture over time, and identify changes in the configuration of components and the environment. For convenience, reports are available through a web-based application, and translating them does not require prior knowledge of IBM Z terminology.

Given the transparency of this process, auditors can feel confident in the integrity of the reports that they receive. The IBM Z Security and Compliance Center provides auditors with results that they can trust while also reducing the effort that is spent manually interpreting standards, which leads to more accurate assessments of your overall security and compliance postures.

1.4 Building blocks of regulatory frameworks

In Chapter 4, “Exploring security and compliance use cases” on page 51,” we examine common scenarios that are likely to match your organization's objectives for achieving regulatory compliance. Before we do so, let us look briefly at the basic “building blocks” of regulatory frameworks: *goals*, *controls*, and *profiles*. Understanding how these concepts relate to each other is key to understanding how compliance is measured.

We describe the terms first:

- ▶ **Goal:** A technical check against an expected system setting, such as a default value for a security setting parameter. A goal that fails a check might indicate a noncompliance issue.
- ▶ **Control:** Consists of one or more goals that map to specific industry-regulatory requirements. Controls can be broad guidelines, such as security requirements to encrypt data-at-rest or prevent unprivileged access to confidential systems.
- ▶ **Profile:** A set of controls that represents an entire regulatory framework. The profile determines what is checked when you run a validation scan in IBM Z Security and Compliance Center.

IBM Z Security and Compliance Center comes with predefined goals, controls, and profiles that you can use to manage and validate compliance in your IBM Z environment. In a predefined profile, the controls map directly to an industry regulation, such as PCI DSS, or a security framework, such as NIST or CIS.

You can create your own custom profiles by using a selection of hundreds of goals that come with the solution. A custom profile can be created by using a predefined profile as a base, or you can create a profile from scratch by selecting from a list of available goals that you want to meet. With a custom profile, you choose only the controls and goals that are relevant for your business.

In addition, an extensive set of predefined mappings can be imported from IBM Z Security and Compliance Center as a basis for your own security procedures. Through this process, the solution can be used to prepare for audits that are specific to your organization's requirements.

Figure 1-1 shows how goals are mapped to controls, which in turn comprise a profile.

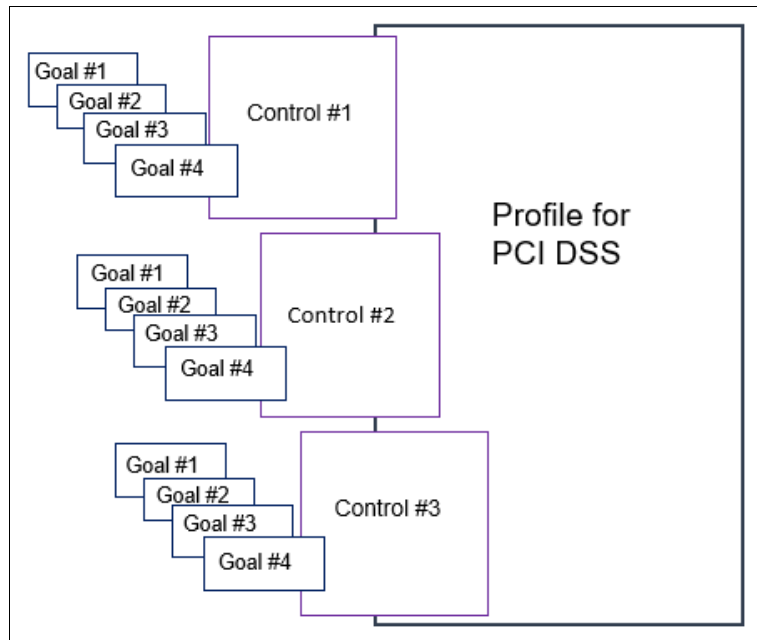


Figure 1-1 Building blocks

The goals, controls, and profiles, which are defined by the IBM Z Security team and based on the most current IBM Z security capabilities, were validated by auditors. Because the solution enables you to inspect the controls and goals that it validates, you can see exactly which component is being checked.

In Chapter 5, “Validating security and compliance postures” on page 65, we work with a predefined profile and a custom profile that is created from scratch.

1.5 Targeted user roles and authorization controls

IBM Z Security and Compliance Center is intended to be incorporated into your organization's existing compliance processes and teams. As a security analysis tool, it is designed to be secure always. Because IBM Z Security and Compliance Center creates standardized reports with both high-level and detailed reporting on compliance status, it includes granular, role-based authorization for controlling user access to scan data and reports. In this way, IBM Z Security and Compliance Center maintains the separation of duties between, for example, Compliance Leads, report viewers, and those responsible for administering the compliance evidence-gathering process.

The following *personas* are the most likely to be involved in using the solution:

- ▶ **Compliance Lead:** Responsible for ensuring that an organization is audit-ready and able to produce a report for an auditor.
- ▶ **Evidence Provider:** Responsible for collecting and reviewing compliance data with the goal of improving your organization's compliance status (or posture).

In your organization, these roles might be known by different titles.

Also, the following personas might be involved indirectly, as consumers of the generated compliance reports:

- ▶ CISO
- ▶ Internal auditor
- ▶ External auditor

The CISO is responsible for overseeing your organization's protection of company and customer data, and I/T infrastructure and assets. The auditor is responsible for verifying that your organization adheres to compliance standards.

Also needed are the z/OS system administrator and z/OS security administrator, who are involved with installing, maintaining, and securing the solution.

Specific to IBM Z Security and Compliance Center is an administration role, who is responsible for managing the solution after installation. This user authorizes other users, operates the solution dashboard, and updates the solution software whenever required.

To help your team get started quickly, IBM Z Security and Compliance Center includes predefined roles that can be used to map the appropriate personas to roles, and grant the appropriate level of authority to each.

Section 3.4, “Solution-defined roles and responsibilities” on page 38 describes the predefined roles and shows how to use them to control access to IBM Z Security and Compliance Center in your organization.

1.6 A closer look at IBM Z Security and Compliance Center

IBM Z Security and Compliance Center consists of a collection of z/OS and Linux on IBM Z elements that retrieve, validate, and report on the compliance status of a particular scope of components in the IBM Z environment.

The IBM Z Security and Compliance Center infrastructure is installed as a set of microservices in Red Hat OpenShift on z/OS by using IBM z/OS Container Extensions (IBM zCX). The solution integrates with various software components on the IBM Z platform to collect and validate compliance data.

Your z/OS system must be enabled for collecting compliance data. The solution includes two components that must be installed on each z/OS image and enabled for collecting and supplying the data to the solution for validation.

Your Linux on IBM Z images should be configured with appropriate users, which IBM Z Security and Compliance Center uses to gather compliance information.

Note: This publication is focused on ensuring the compliance of z/OS systems; the subject of Linux on IBM Z is not addressed.

IBM Z Security and Compliance Center can be deployed on an IBM z15® or IBM z16™ by using the latest supported versions of the z/OS operating system and several middleware products, such as CICS, IMS, IBM MQ, and Db2.

For information about how IBM Z Security and Compliance Center is packaged and distributed by IBM, and its system prerequisites, see 3.6, “Solution prerequisites” on page 46.



Staying on top of security and compliance

Each organization might have different positions on security and compliance postures. However, for most, attaining the highest level for these postures is a journey. Keeping up with regulatory changes to stay compliant or leveraging IBM Z security capabilities to create a secure perimeter based on a [zero trust](#) model requires continuous oversight.

To improve your security and compliance postures, you first must know what end goal you want to reach and where you stand today (establish a baseline). Then, you must perform gap analysis and assess risk to determine which areas to focus on when applying actions.

This chapter helps you understand the difference between being compliant and being secure. We guide you through the basic steps for improving security and compliance postures, and the role that IBM Z Security and Compliance Center plays in the process.

This chapter covers the following topics:

- ▶ 2.1, “Security posture versus compliant posture” on page 14
- ▶ 2.2, “Where are you on your security and compliance journey” on page 15
- ▶ 2.3, “Knowing your options” on page 16
- ▶ 2.4, “Establishing a baseline” on page 18
- ▶ 2.5, “Scheduling regular reviews and audits” on page 18
- ▶ 2.6, “Identifying the most vulnerable areas” on page 22
- ▶ 2.7, “Performing gap analysis and risk assessment” on page 23
- ▶ 2.8, “Creating an action plan” on page 26

2.1 Security posture versus compliant posture

The National Institute of Standards and Technology (NIST) defines [security posture](#) as “the security status of an enterprise's networks, information, and systems based on information assurance resources (for example, people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. Synonymous with security status.”

The NIST definition relates to information assurance practices through the controls that are associated with information security: confidentiality, integrity, and availability. It also makes provision for processes and procedures that are related to controlling the security of the resources by implementing mechanisms for the backup of enterprise resources, restore of resources to preserve their integrity, and detection and reaction to cyberthreats. These controls might be specific to each enterprise and in general internally defined practices.

NIST does not have a definition for compliance posture, yet professionals working with compliance have a sense of what compliance posture might refer to, that is, organizations' adherence to compliance regulatory standards for security compliance. The keyword here is *regulatory*.

The online Merriam-Webster dictionary defines [compliance](#) as “conformity in fulfilling official requirements” and [posture](#) as a “state or condition at a given time especially concerning capability in particular circumstances”.

From these definitions, you can construct a definition for compliance posture as fulfilling official requirements at a given point in time.

Thus, compliance posture is oriented to adhering to established requirements that are in effect, official, and independent of the organization's internal requirements. We can apply this definition to enterprise security. These established requirements depend on the industry type: financial, manufacturing, health insurance, and others, and government- or global-related regulations that are industry-neutral. Because these requirements and regulations are defined by independent entities, they are global in scope.

From both definitions, security posture and compliance posture, it also follows that the former focuses on monitoring and reporting the status change of your enterprise security controls, and the latter focuses on how you comply with any requirements, policies, or regulations that apply to your industry. Security posture is more oriented toward demonstrating internal controls that are associated to the enterprise resources, and compliance posture is oriented toward complying with external regulations. The latter tends to change less often than the former because of the official nature of the requirements.

We can say that for highly regulated industries or even for industries that want to follow best practices,¹ the controls for security posture and the requirements for the compliance posture are getting closer and closer, with some overlap on some controls and requirements.

From a practical point of view, this overlapping leads to situations where not all your internal controls map to a regulatory control. Concurrently, not all the regulatory controls are addressed by your internal controls.

¹ NIST defines a [best practice](#) as “A procedure that has been shown by research and experience to produce optimal results and that is established or proposed as a standard suitable for widespread adoption”.

From this situation, several challenges emerge, such as:

- ▶ For regulatory controls that are not addressed by your internal controls, organizations must work toward adding internal controls that map those regulatory controls and align with their specifications.
- ▶ Organizations also must implement policies, processes, methods, and procedures to demonstrate adherence to those new controls.

For most organizations, internal and regulatory controls are forcing them to revisit their existing security posture. In practical terms, their internal controls are amended to incorporate those controls from regulatory controls. The effect of this paradigm shift is that by demonstrating your compliance posture you, in principle, also demonstrate your security posture.

This is the case if you can incorporate your internal controls, which are required by your organization's security policies, as part of a wider set of regulatory controls that address both internal security and external regulatory controls.

This situation is where IBM Z Security and Compliance Center adds value to your organization because it provides the following facilities:

- ▶ Defines your internal controls and adds them to a compliance and regulatory framework that you must comply with as an integrated and consolidated evaluation framework as a custom control.
- ▶ Gradually (progressively) implements processes to show the integrated or consolidated status of your enterprise compliance readiness based on the requirements of a given regulatory framework.

In practical terms, with IBM Z Security and Compliance Center, you can demonstrate compliance with the applicable regulatory framework, which concurrently demonstrates your security posture because the former can be augmented with your enterprise requirements.

In short, IBM Z Security and Compliance Center is designed to provide a centralized and integrated solution that demonstrates the security and compliance postures of your IBM Z platform by mapping the business-oriented language of regulatory frameworks to the IBM Z platform-specific security controls, and seamlessly reporting the results.

2.2 Where are you on your security and compliance journey

There is a perception among IT professionals that the IBM Z platform is the most *secure* in the industry. However, we suggest that the IBM Z platform is better referred to as the most *securable* in the industry. Even though security is designed into all layers of the IBM Z stack since inception, IBM always has given you the flexibility to enable or use those security features and functions depending on your distinct business requirements. Therefore, it is important to understand which security mechanisms are available and consciously decide about their use.

A good analogy is home security. A home can have the best modern home-security system that is installed, connected to a 24x7 control room for monitoring, and have the most solid doors and locks, but if you leave home without activating the security system and locking the doors, it is wide open to any intruder. There is no access control or monitoring of entry to the home, and equally important, no one is monitoring what the pets, left inside, are up to.

The same applies to the IBM Z platform: Even though security mechanisms are built into the platform, it is up to the organization to establish their own security perimeter.

To determine where you are on your journey, you must understand where you started from; where you currently find yourself; and more importantly, where you are heading. It might be difficult to remember your starting point, but gauging where you are is a matter of comparing yourself to the best industry standards that are available. These standards were compiled by security experts, and are used by external parties to measure you against.

On compliance regulation, such as Payment Card Industry Data Security Standard (PCI DSS), you can review your last audit reports and establish the steps that you need to take to either correct or at least mitigate any adverse audit findings. For security, you might want to measure your environment to meet even more stringent industry standards, such as the National Institute of Standards in Technology (NIST 800-53) or the Defense Information Systems' Security Technical Implementation Guide (DISA-STIG). This measurement shows any discrepancies between what is deemed the industry standard and where your organization finds itself today. This measurement also shows you the end goal that you should be aiming toward.

IBM Z Security and Compliance Center can help you understand your options, establish a baseline, run regular scans to measure improvements, and provide guidance about how to achieve the necessary improvements.

2.3 Knowing your options

IBM Z Security and Compliance Center provides validation for major industry acknowledged regulatory standards, such as PCI DSS, NIST, and Center for Internet Security (CIS) benchmarks. The current available number of 571 goals are defined through three available profiles that reflect the regulatory standards and validate the optimal leverage of the IBM Z security capabilities.

IBM Z Security and Compliance Center is designed to be extended and enhanced to keep up with future changes of the regulatory standards, which are driven both by new attack vectors and the evolving IBM Z Security capabilities. A prime example of this situation is the preemptive usage of quantum-safe encryption algorithms in IBM z15 and IBM z16. Even though the usage of these algorithms is not yet an industry standard or a regulatory requirement, there will come a time when it will be, which will lead to applicable goals being added to IBM Z Security and Compliance Center.

In addition, you can use these *standard* profiles with their specific goals to establish your compliance posture, and you can use a combination, if not all, of these available goals to establish a customized profile to gauge your security posture. To do so, create your own security posture profile and include the goals that are relevant to your organization. This configuration can lead to a more targeted review of your IBM Z Security components.

After a scan is run, you can review each IBM Z Security component in the validation report. Participating components and products generate compliance data through SMF records. IBM Z Security and Compliance Center evaluates the compliance data and maps it to the appropriate goal IDs. The goal IDs can be found in the validation reports (see Figure 2-9 on page 25, for example).

With IBM z16, rich security features are provided at all layers of the stack:

- ▶ A processor with quantum-safe memory protection. Also, co-processors like CP Assist for Cryptographic Function (CPACF) and the Crypto Express8S acting as Hardware Security Modules (HSMs) for hardware encryption of data at-rest.

In IBM Z Security and Compliance Center, you can select goal IDs² that start with *4049xxx* for ICSF and *4128xxx* for CPACF to validate the cryptography and co-processor usage.

- ▶ Firmware with quantum-safe secure boot technology with a built-in dual-signature scheme that validates the chain of trust from the processor through the firmware into the operating system. The Call-Out for monitoring and Remote Code Load for IBM Z Firmware features enable the secure and remote update of this firmware.
- ▶ A hypervisor enables workload isolation in the form of logical partitions (LPARs), virtual machines (VMs), and IBM Secure Service Containers. In addition, Crypto Express coprocessors can be configured to support multiple cryptographic domains that are assigned to LPARs. A domain acts as an isolated and independent cryptographic device with its own master key.³
- ▶ An operating system that provides a System Authorization Facility (SAF) acting as a common focal point for all components and applications requiring or providing resource access control, regardless of which security manager a client uses. In addition, External Security Managers (ESMs) can be optimally configured to provide the best available security verification.

In IBM Z Security and Compliance Center, you can select goal IDs that start with *4083xxx* for validation of a correct RACF configuration.

- ▶ Network traffic to and from (data in-flight) your IBM Z platform can be protected with the latest standards.

In IBM Z Security and Compliance Center, you can select goal IDs that start with *4001xxx*, *4002xxx*, *4003xxx*, and *4004xxx* to validate the usage of later versions of SSL and Transport Layer Security (TLS) encryption and other network protection measures for connectivity to your IBM Z platforms.

- ▶ Storage with management and access control measures can ensure data at-rest is secure, regardless of whether that data is encrypted.

In IBM Z Security and Compliance Center, you can select goal IDs that start with *4052xxx* for validation of access control to DFSMSrmm. The rest of the DFHSMS functions (*hsm*, *dfp*, and *dss*) are covered with goal IDs that start with *4096xxx* and *4097xxx*.

- ▶ Applications and middleware can enforce and leverage the security layers that are provided by the hardware, operating system, network, and storage environments with the supplied security capabilities to validate authentication and authority to process transactions and access data.

In IBM Z Security and Compliance Center, you can select goal IDs that start with *4080xxx* for CICS, *4081xxx* for Db2, *4082xxx* for IBM MQ, and *4085xxx*, *4086xxx*, and *4087xxx* for IMS to validate the usage of system-supplied security measures.

For more information about the security capabilities on IBM Z platforms, see [Mainframes](#).

² A *goal ID* consists of 7 digits. The second, third, and fourth digits represent the SMF 1154 record subtype. For more information, see Appendix B, “SMF record type 1154 overview” on page 107.

³ A *master key* is a special key-encrypting key (KEK) that is in a tamper-responding, Crypto Express adapter.

2.4 Establishing a baseline

Whether you want to establish a baseline for your compliance posture or security posture, you have the same basic starting point. Decide on the scope of the z/OS systems that will be your target, as described in 5.1.1, “Defining a scope” on page 66.

Then, and this will depend on whether the goal is to become compliant or improve security, decide on which profile to use. If your aim is becoming compliant, then one of the PCI DSS, NIST, or CIS profiles is selected (see 5.2.1, “Viewing existing profiles” on page 73). If your aim is improving your security posture, create your own customized profile that includes the goals that are relevant to your environment. As example, do not include goals that cover Db2 security if you do not have Db2 implemented in your systems. For a step-by-step guide on doing this task, see 5.3.1, “Creating a custom profile by using an existing profile” on page 80 and 5.3.2, “Creating a custom profile from scratch” on page 82.

The last preparatory step in IBM Z Security and Compliance Center is to set up a recurring scan to establish your baseline and use as a regularly scheduled scan. With this scan, you can monitor any movement, either positive or negative, in your compliance or security posture improvement journey. The scan also can be used to run on an ad hoc basis after remedial actions take place to confirm that your remediation had the wanted effect.

When you establish the mechanism to create your first posture review, you can run this scan to establish your provisional baseline results.

After careful deliberation with all stakeholders and those responsible for security in your z/OS systems, these results can be reviewed and adjusted according to relevancy and priority. During this process, as fine-tuning of the baseline occurs, multiple scans can be run to compare variations among the results.

When all stakeholders agree on the final result set, all previous result sets can be deleted, and a new scan runs to serve as baseline scan result in the IBM Z Security and Compliance Center repository. This baseline can be used to compare all future scan results against it.

Note: Running scans is an iterative process that is repeated whenever anything changes in your environment.

For example, if you start using Db2, it changes the scope because introducing a database into your system necessitates the addition of new goals and controls to be validated to ensure that you are protecting the data in that database sufficiently. Hence, these additional goals require you to re-establish your altered baseline going forward.

2.5 Scheduling regular reviews and audits

In practical terms, security and compliance postures are getting closer, with overlapping of some controls and regulations. This situation has resulted in the need for developing processes and procedures that allow organizations to assess their configuration against a given regulatory framework and provide a report showing the level of compliance when compared to the industry or global regulatory frameworks.

The associated challenges include the rigid nature of your security controls because they depend on your implemented configuration. Changes in your configuration might lead to changes to the processes and procedures that implement such controls. Often, you cannot generate a change report of your controls without amending the underlying procedures that generate said reports or without supporting changes to your configuration.

As a result of this dependency, reports that are associated with your security or compliance posture are point-in-time and configuration-based, which typically are not an effortless way to relate the results with the actual state of the configuration. Implementing a recurring security or compliance posture reporting strategy is not possible because the underlying artifacts that extract and process configuration information must be modified to support changes to the configuration.

Moreover, because of the configuration dependency, it is difficult to implement a process to demonstrate compliance progress because you manually must designate a configuration as a baseline for comparison purposes. The practical effect is that your compliance posture is not current regarding your running configuration, and you cannot demonstrate progress on a unified report.

With IBM Z Security and Compliance Center, you can adopt a better compliance posture approach by running your regulatory rules against your environment configuration on a recurring, scheduled basis. To accomplish this task, use the collector module of IBM Z Security and Compliance Center to gather information about your environment and resource configurations, and validate that information against your specific standards and the regulatory framework that is associated to your industry or selected by your organization.

With IBM Z Security and Compliance Center, you can define recurring validation reports that automatically initiate the collector module and use the current configuration of the environment along with the selected standards to report your compliance posture, which automatically incorporate the latest configuration changes and how the evaluation of the controls were affected by such changes. In addition, by selecting multiple instances of the recurring reports, you are presented with comparison capabilities to show compliance progress.

For example, you can schedule daily validation reports for those regulatory controls that need close monitoring, like when non-compliance can result in fines and penalties to the organization. With this flexibility, you can implement a dynamic audit and compliance approach based on the automatic detection of configuration changes.

By using the IBM Z Security and Compliance Center dashboard, you can select specific completed scans to evaluate your compliance posture as it changes over time. In our case, we want to review completed scans (called WSC-ZHBPLEX - PCI DSS - Daily) to monitor compliance drift over a week (see Figure 2-1).

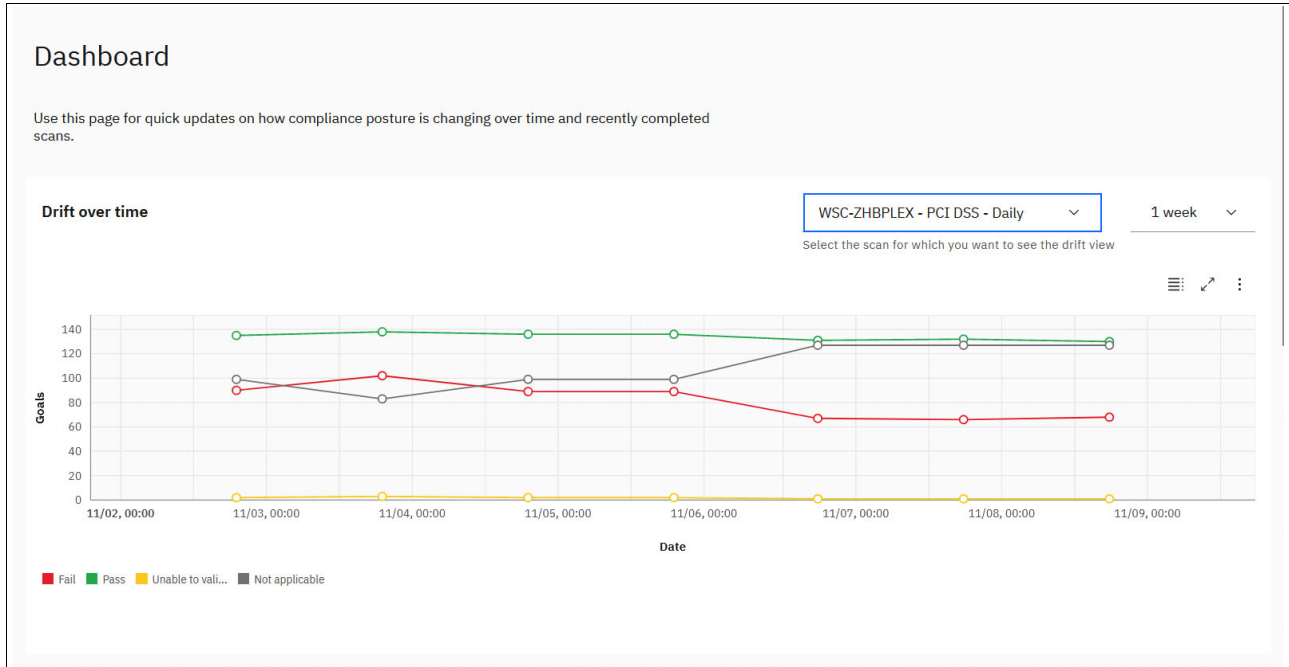


Figure 2-1 Compliance drift over time

The second part of the dashboard shows the total number of defined validations, which are broken down by type (recurring or on-demand), and the list of scans. A list of scans is on the right (see Figure 2-2).

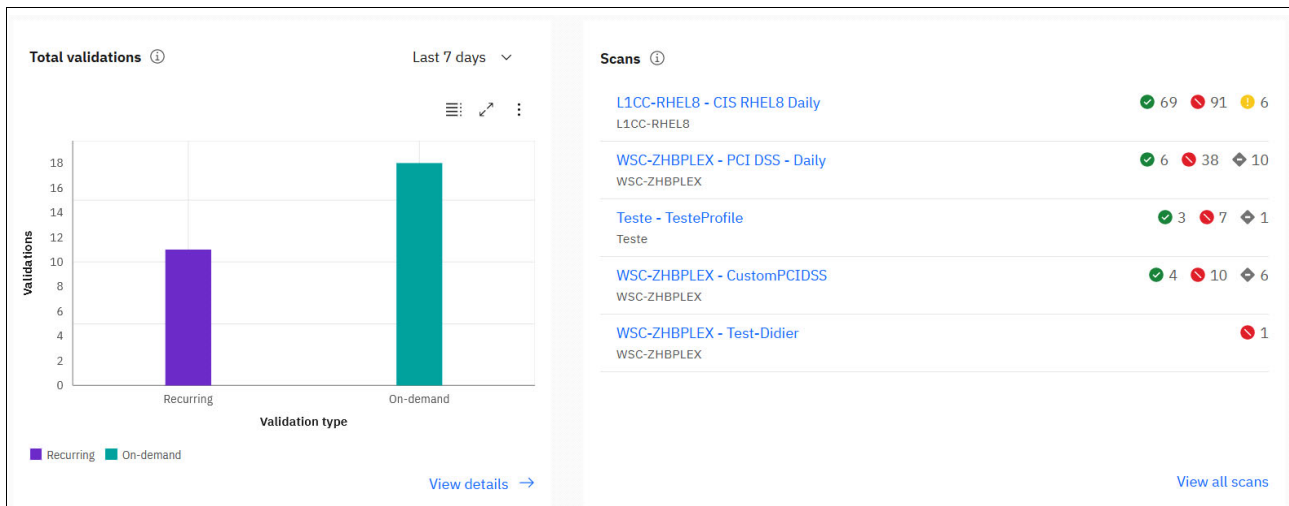


Figure 2-2 Validation breakdown

Select **View details** to get a full list of defined reports (validations), as shown in Figure 2-3 on page 21.

Validation	Scope	Profile	Type	Total
Teste - TesteProfile	Teste	TesteProfileCreation	On-demand	4
WSC-ZHBPLEX - CustomPCIDSS	WSC-ZHBPLEX	Custom PCI DSS 3.2.1 for zOS	On-demand	9
WSC-ZHBPLEX - Test-Didier	WSC-ZHBPLEX	Test-Didier	On-demand	2
WSC-ZHBPLEX - PCIDSS3.2.1f	WSC-ZHBPLEX	PCI DSS 3.2.1 for zOS	On-demand	1
L1CC-RHEL8 - CustomPCIDSS	L1CC-RHEL8	Custom PCI DSS 3.2.1 for zOS	On-demand	1
L1CC-RHEL8 - CISRedHatEnt	L1CC-RHEL8	CIS Red Hat Enterprise Linux 8 on IBM Z Linux Benchmark 1.0.0	On-demand	1
L1CC-RHEL8 - CIS RHEL8 Daily	L1CC-RHEL8	CIS Red Hat Enterprise Linux 8 on IBM Z Linux Benchmark 1.0.0	Recurring	5
WSC-ZHBPLEX - PCI DSS - Daily	WSC-ZHBPLEX	PCI DSS 3.2.1 for zOS	Recurring	6

Figure 2-3 Total validations

You can view a further graphical display of the results by selecting a validation report. In our example, we select WSC-ZHBPLEX - PCI DSS - Daily (see Figure 2-4).

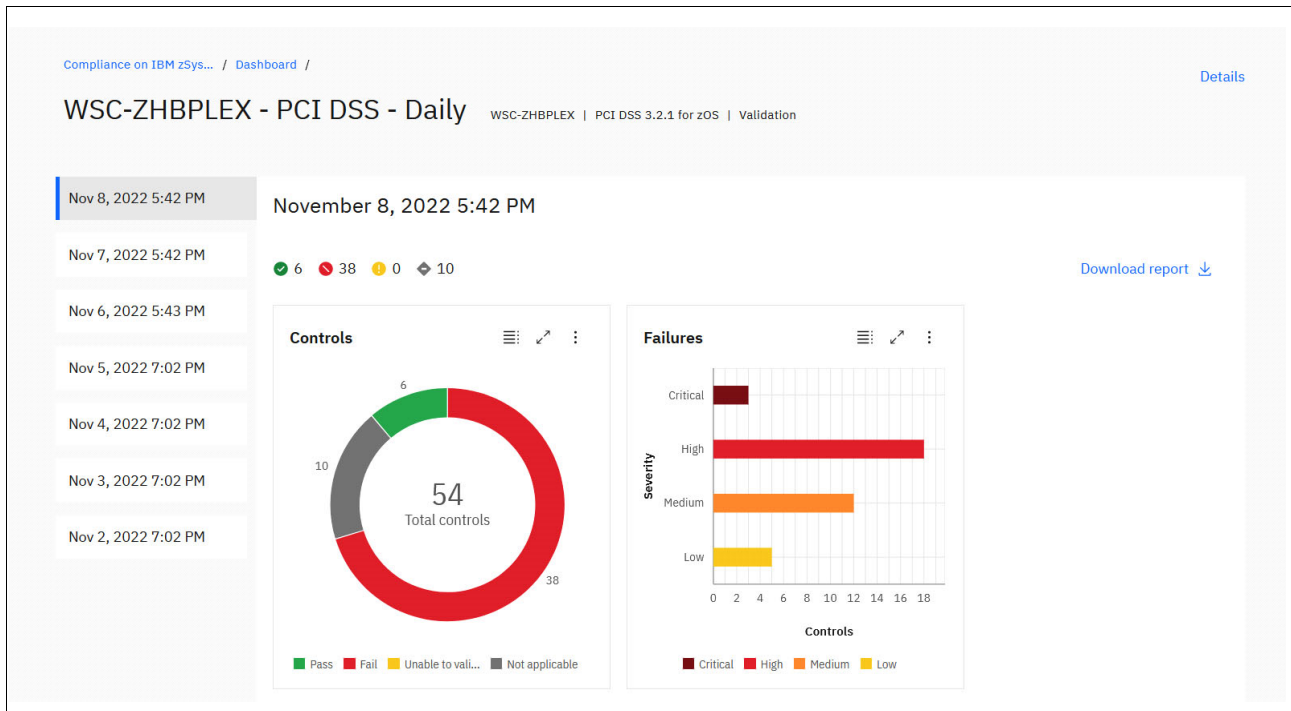


Figure 2-4 Validation report

To summarize, without IBM Z Security and Compliance Center, organizations that need to demonstrate their security or compliance posture must continuously spend resources and time in amending existing processes that implement evaluation controls to match the running configuration and support any new or amended regulation that is used to demonstrate the compliance posture. With IBM Z Security and Compliance Center, demonstrating your security and compliance postures is straightforward because the solution automatically detects configuration changes and regulation changes, and includes evaluation results as part of the consolidated validation report that is available in dashboard.

2.6 Identifying the most vulnerable areas

IBM Z Security and Compliance Center classifies the severity of failures from an industry standards point of view by using the underlying regulatory compliance framework that was used for the scan. The potential exposure a particular lapse in your security posture (a security setting that is either not in place or configured incorrectly to ensure the most secure position, as deemed by the regulatory standards) is rated from Critical, High, Medium, to Low. By using this classification, you quickly can identify the areas that are deemed most vulnerable because a misconfiguration of security parameters.

From looking at the scan results on the dashboard, you can filter the severity to remove the clutter of controls that passed validation, and therefore do not require remedial action. With the sorting column, it is easy to sort the Critical failures to the top, as shown in Figure 2-5.

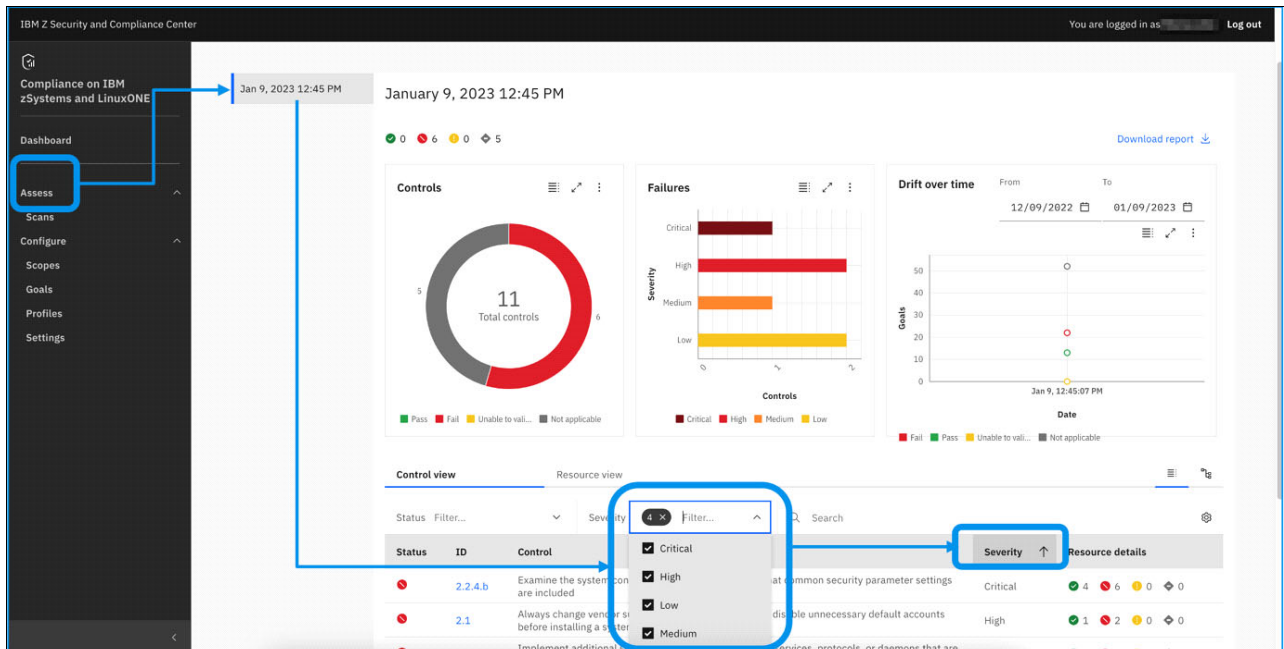


Figure 2-5 Options to isolate and sort failing controls according to severity

In this manner, you can isolate the failed controls and prioritize them according to the implied compromise that they pose to your security or compliance posture.

After you isolate the failing control, look at the control as a whole because a control typically consists of one or more goals. Some of these goals passed, and some of them did not. All goals within a control must pass for the control to pass validation.

2.7 Performing gap analysis and risk assessment

Focusing on the Critical and High severity failures is a good starting point to identify gaps and do a proper risk assessment for your environment. However, although focusing on the Critical and High severity failures is a logical departure point, it is not necessarily the only consideration.

Many controls share goals, which imply that remediating these failed goals might lead to a quicker way for more controls to pass validation and improve your security posture with less effort than resolving issues with uniquely used goals, as shown in Figure 2-6.

External Control Id	Description	Parent	GOAL Id	zSCC Tags
Profile Name: PCI DSS 3.2.1 for zOS ID: 4001004 Check whether IP packet filtering and IPsec are enabled on all TCP/IP stacks				
1	Install and maintain a firewall configuration to protect cardholder data			
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment	1		
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic	1.2	4001004	IBM,ZOS;EDMM-SERVER,TCPIP
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment	1		
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet	1.3	4001004	IBM,ZOS,COMM-SERVER,TCPIP
2	Do not use vendor-supplied defaults for system passwords and other security parameters			
2.1	Always change vendor supplied defaults and remove or disable unnecessary default accounts before installing a system on the network	2	4081001, 4083007, 4083008, 4085015, 4085016, 4087001, 4085014, 4085017, 4087002, 4085018	IBM,ZOS,DB2,IMS,RACF,CONNECT
2.2	Develop configuration standards for all system components	2		
2.2.0	Develop configuration standards for all system components	2.2	4096006	IBM,ZOS,SMF,GLOBAL
2.2.a	Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards	2.2	4079002	IBM,ZOS,INETD
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system	2.2	4079001	IBM,ZOS,INETD
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure	2.2	4002012, 4002007, 4003003, 4002011, 4002009, 4001014, 4002003, 4002008, 4002004, 4002002, 4003008, 4002005, 4002010, 4002001	IBM,ZOS,FTP,TN3270E,COMM-SERVER,TCPIP
2.2.4.0	Configure system security parameters to prevent misuse	2.2.4	4049008, 4049002, 4049004, 4049005, 4049006, 4052009, 4077001, 4078003, 4052007, 4077004, 4049007, 4077002, 4049003, 4077003, 4050001, 4052008, 4049017	USS,IBM,ZOS,DFSMS,SSHD,ICSF,RMM,CONSOLE
2.2.4	Configure system security parameters to prevent misuse	2.2		
2.2.4.b	Examine the system configuration standards to verify that common security parameter settings are included	2.2.4	4001005, 4001013, 4001004, 4001006, 4001008, 4003005, 4001012, 4001002, 4001003, 4001009	IBM,ZOS,TN3270E,COMM-SERVER,TCPIP
2.3.0	Encrypt all non-console administrative access using strong cryptography	2.3	4078005, 4078001	IBM,ZOS,SSHD
2.3	Encrypt all non-console administrative access using strong cryptography	2		
2.3.d	Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations	2.3	4078007, 4078006, 4078002	IBM,ZOS,SSHD

Figure 2-6 A goal that is defined to more than one control

To address failing goals that occur multiple times, a best practice is to plot the failing goals, which are derived from the failing controls, and then assign them a weight by combining their control-inherited severity with the number of times that they are flagged. The result is a matrix that can help you decide which implicated areas (goals) to focus on for remedial actions. An example of such a matrix is shown in Figure 2-10 on page 26.

To explain this approach, we created a simple custom profile with only 11 controls that uses the first two control groups from the provided PCI DSS profile, as shown in Figure 2-7.

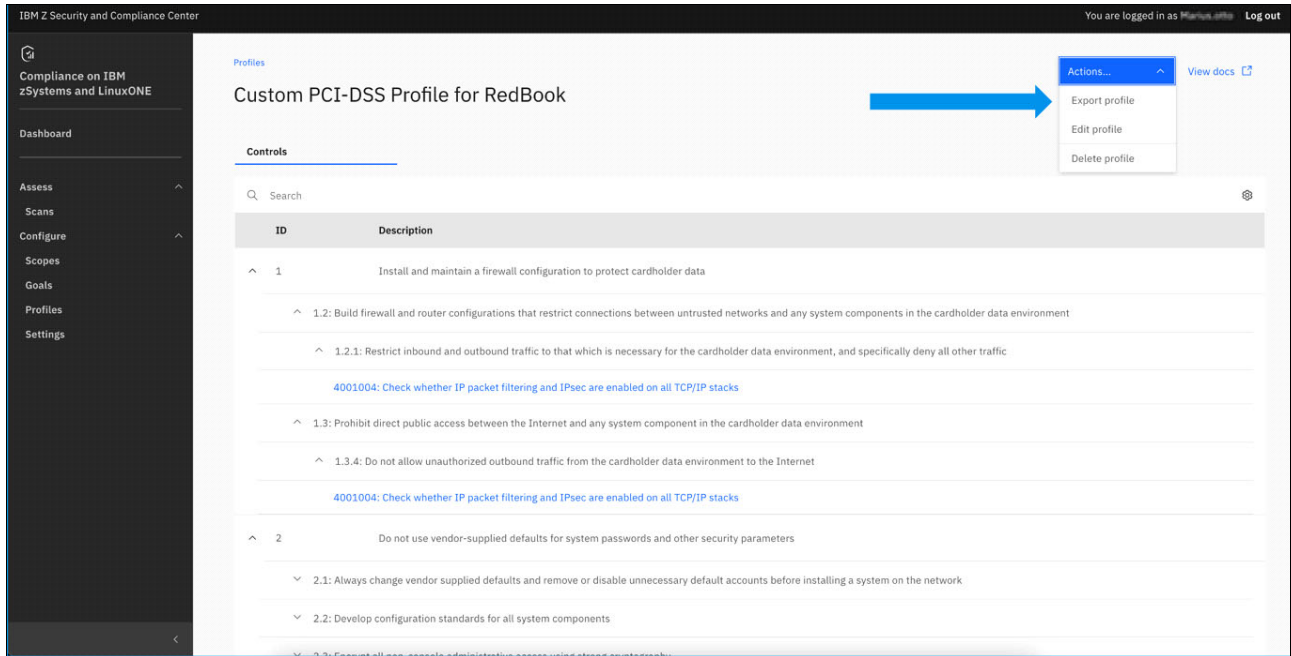


Figure 2-7 Custom profile created with limited controls

Note: A profile also can be viewed in xlsx format by using the **Export profile** function.

After running the scan and then looking at the exported report, it is easy to see which controls failed and the severity of these failures, as shown in an excerpt from the downloaded report in Figure 2-8 on page 25.

Validation Summary per Control					Number of IT Resources				
Control ID	Description	Overall Status	Severity	Pass	Fail	Unable	N/A	Total	
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic	FAIL	Low		1			1	
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet	FAIL	Low		1			1	
2.1	Always change vendor supplied defaults and remove or disable unnecessary default accounts before installing a system on the network	FAIL	High	1	2		7	10	
2.2.0	Develop configuration standards for all system components	N/A					1	1	
2.2.a	Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards	N/A					1	1	
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system	N/A					1	1	
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure	FAIL	High	7	7			14	
2.2.4.0	Configure system security parameters to prevent misuse	FAIL	Medium	1	7		37	45	
2.2.4.b	Examine the system configuration standards to verify that common security parameter settings are included	FAIL	Critical	4	6			10	
2.3.0	Encrypt all non-console administrative access using strong cryptography	N/A					2	2	
2.3.d	Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations	N/A					3	3	

Figure 2-8 Scan results with the status for each control that was validated

This view is only the high-level view of the controls, which is augmented with a description indicating how many goals passed or failed. To understand which of the underlying goals failed or passed, click the links within the report to view the details for each control, as shown in Figure 2-9.

Goal ID	Description	Status	Severity	Pass	Fail	Unable	N/A	Total
4001002	Check whether IP packet forwarding is disabled on all TCP/IP stacks	FAIL	Medium	0	1	0	0	1
4001003	Check whether ICMP redirects are ignored on all TCP/IP stacks	FAIL	Medium	0	1	0	0	1
4001004	Check whether IP packet filtering and IPsec are enabled on all TCP/IP stacks	FAIL	Low	0	1	0	0	1
4001005	Check that TCP low ports are restricted	FAIL	High	0	1	0	0	1
4001006	Check that UDP low ports are restricted	FAIL	High	0	1	0	0	1
4001008	Check whether SNMP TCP/IP subagent community name is specified	FAIL	Critical	0	1	0	0	1
4001009	Check whether SNMP TCP/IP subagents are configured to prevent SET requests	PASS	High	1	0	0	0	1
4001012	Check whether TCP/IP stacks are configured to require UDP checksum processing	PASS	High	1	0	0	0	1
4001013	Check whether TCP/IP stacks are configured to limit the size of UDP queues	PASS	High	1	0	0	0	1
4003005	Check whether TN3270E SNMP subagent community name is specified when the subagent is activated	PASS	Critical	1	0	0	0	1

Figure 2-9 Details of goals and their status included in a specific Control 2.2.4.b

From this point, it is easier to focus on the failed goals. Extract the failed goal ID, details, and severity from each goal. Assign a combined weight to each by using the severity (*Low* = 1, *Medium* = 2, *High* = 3, *Critical* = 4) multiplied with the goal ID occurrence count. The result is a matrix, as shown in Figure 2-10. Sorted on combined weight in descending order indicates clearly which areas should be focused on and in which order. With this example, you see that the Critical and High severity failures should take precedence, but a Low severity failure occurred multiple times, so those Low occurrences might take precedence over a Medium severity failure that occurs only once.

Profile name	Control ID	Goal ID	Severity	Severity Weight	Occurance Weight	Combined Weight	Detail
Custom PCI-DSS Profile for RedBook	2.2.4.b	4001008	Critical	4	1	4	One or more TCP/IP stacks configured with SNMP public community. SMF1154_C_JOBNAME: [TCPIP] SMF1154_1_MGMTSAAGENT: [161]
Custom PCI-DSS Profile for RedBook	2.2.4.b	4001005	High	3	1	3	One or more TCP/IP stacks do not restrict access to TCP ports 1-1023. SMF1154_C_JOBNAME: [TCPIP]
Custom PCI-DSS Profile for RedBook	2.2.4.b	4001006	High	3	1	3	One or more TCP/IP stacks do not restrict access to UDP ports 1-1023. SMF1154_C_JOBNAME: [TCPIP]
Custom PCI-DSS Profile for RedBook	2.2.3	4003003	High	3	1	3	One or more TN3270E server TELNETPARMS statements are configured with unsatisfactory inactivity timeout values. SMF1154_C_JOBNAME: [TN3270] SMF1154_3_TNTPPORTNUM: [23] SMF1154_3_TNTPPORTIPADDR4: [0.0.0.0] SMF1154_3_TNTPPORTLINK: []
Custom PCI-DSS Profile for RedBook	2.1	4083008	High	3	1	3	Db2 using installation default ID. SMF1154_81_DB2SSNAME: [DB1C]
Custom PCI-DSS Profile for RedBook	1.2.1	4001004	Low	1	3	3	One or more TCP/IP stacks have IP Security disabled for IPv4 and/or IPv6. SMF1154_C_JOBNAME: [TCPIP]
Custom PCI-DSS Profile for RedBook	1.3.4	4001004	Low	1	3	3	One or more TCP/IP stacks have IP Security disabled for IPv4 and/or IPv6. SMF1154_C_JOBNAME: [TCPIP]
Custom PCI-DSS Profile for RedBook	2.2.4.b	4001004	Low	1	3	3	One or more TCP/IP stacks have IP Security disabled for IPv4 and/or IPv6. SMF1154_C_JOBNAME: [TCPIP]
Custom PCI-DSS Profile for RedBook	2.2.4.b	4001002	Medium	2	1	2	One or more TCP/IP stacks allows IP packet forwarding for IPv4 and/or IPv6. SMF1154_C_JOBNAME: [TCPIP]
Custom PCI-DSS Profile for RedBook	2.2.4.b	4001003	Medium	2	1	2	One or more TCP/IP stacks honor ICMP redirects for IPv4 and/or IPv6. SMF1154_C_JOBNAME: [TCPIP]
Custom PCI-DSS Profile for RedBook	2.2.3	4002003	Medium	2	1	2	One or more FTP daemons are configured with improper umask values. SMF1154_C_JOBNAME: [FTPSERVE] SMF1154_2_FDCFPOR: [21]
Custom PCI-DSS Profile for RedBook	2.2.3	4002005	Medium	2	1	2	One or more FTP daemons are not configured to verify the client IP address on passive data connections. SMF1154_C_JOBNAME: [FTPSERVE] SMF1154_2_FDCFPOR: [21]
Custom PCI-DSS Profile for RedBook	2.2.3	4002011	Medium	2	1	2	One or more FTP daemons are configured to allow users to manipulate JES data beyond the logged-in user ID scope. Ensure proper access control through the SAF JESJOBS and JESSPOOL classes. SMF1154_C_JOBNAME: [FTPSERVE] SMF1154_2_FDCFPOR: [21]
Custom PCI-DSS Profile for RedBook	2.2.3	4002012	Medium	2	1	2	One or more FTP daemons are configured to allow clients to direct data connections to a different IP address through the PORT or EPRT commands. SMF1154_C_JOBNAME: [FTPSERVE] SMF1154_2_FDCFPOR: [21]
Custom PCI-DSS Profile for RedBook	2.2.4.0	4049002	Medium	2	1	2	ICSF Key Store Policy key token authorization checking is not enable
Custom PCI-DSS Profile for RedBook	2.2.3	4002002	Low	1	1	1	One or more FTP daemons are configured with an improper inactivity timeout value. SMF1154_C_JOBNAME: [FTPSERVE] SMF1154_2_FDCFPOR: [21]
Custom PCI-DSS Profile for RedBook	2.2.3	4002004	Low	1	1	1	One or more FTP daemons are not configured to mask identifying information about the server. SMF1154_C_JOBNAME: [FTPSERVE] SMF1154_2_FDCFPOR: [21]
Custom PCI-DSS Profile for RedBook	2.2.4.0	4049003	Low	1	1	1	ICSF duplicate key token checking is not enable
Custom PCI-DSS Profile for RedBook	2.2.4.0	4049004	Low	1	1	1	ICSF symmetric key label export controls are not enable
Custom PCI-DSS Profile for RedBook	2.2.4.0	4049006	Low	1	1	1	ICSF granular key label access controls are disabled
Custom PCI-DSS Profile for RedBook	2.2.4.0	4049007	Low	1	1	1	ICSF KGUP CSFKEYS authority control is disabled
Custom PCI-DSS Profile for RedBook	2.2.4.0	4049008	Low	1	1	1	ICSF CSFKEYS PKA ECC token private-key name checking is disabled
Custom PCI-DSS Profile for RedBook	2.2.4.0	4049017	Low	1	1	1	ICSF CHECKAUTH keyword is NO in installation options dataset. SAF checking will be bypassed for supervisor state and system key callers
Custom PCI-DSS Profile for RedBook	2.1	4081001	Low	1	1	1	z/OS Security Server RACF default passwords have not been disabled

Figure 2-10 Failed goals that are sorted according to their weighted impact on achieving your posture goal

2.8 Creating an action plan

When the gap analysis is completed and a security or compliance posture improvement priority list is compiled, such as described in 2.6, “Identifying the most vulnerable areas” on page 22, the list can be used to consult with stakeholders. Typically, this list aimed more toward the z/OS security roles to investigate whether a change is feasible, advisable, and executable within your environment.

Derive your own priorities and align them with other priorities in your environment and schedule the remedial activities.

The roles that are tasked with the remedial activities can reference the guidance that is provided by IBM Z Security and Compliance Center to understand what must be altered to correct a failure. For more information and examples, see Appendix A, “How to find and remediate failing goals” on page 101.



Understanding the solution

The design of IBM Z Security and Compliance Center incorporates best practices that IBM gathered as a result of an ongoing collaboration with clients and industry stakeholders working together to address the complexity of customer issues that are related to compliance auditing. These best practices are identified by experience by IBM and by using the collective experience from many clients operating in different industries and in different geographical markets.

In this chapter, we examine the IBM Z Security and Compliance Center architecture and show how, in a typical end-to-end workflow, IBM Z hardware and software components work together to validate security and compliance postures. Further, we list the system prerequisites that you must meet to get started with IBM Z Security and Compliance Center.

This chapter covers the following topics:

- ▶ 3.1, “Reference architecture” on page 28
- ▶ 3.2, “Workflow for a validation scan” on page 31
- ▶ 3.3, “A single source of the truth” on page 33
- ▶ 3.4, “Solution-defined roles and responsibilities” on page 38
- ▶ 3.5, “Evidence collection and reports” on page 40
- ▶ 3.6, “Solution prerequisites” on page 46
- ▶ 3.7, “Deployment readiness” on page 48

3.1 Reference architecture

IBM Z Security and Compliance Center consists of a collection of z/OS and Linux on IBM Z elements that retrieve, validate, and report on the compliance status of a particular scope of components in the IBM Z environment.

IBM Z Security and Compliance Center was designed and developed with two distinct parts:

- ▶ *Evidence collection*, which is integrated into various z/OS components or as part of the supported applications that are deployed on either z/OS or Linux on IBM Z.
- ▶ *Evidence presentation*, which runs either on a Red Hat OpenShift Container Platform natively on Linux on IBM Z or in an IBM z/OS Container Extensions (IBM zCX) environment.

Note: This book is focused on ensuring the compliance of z/OS systems; the subject of Linux on IBM Z is not addressed.

3.1.1 Evidence collection

Evidence collection consists of the Evidence Providers (z/OS components and applications) that participate in the evidence collection process.

IBM Z Security and Compliance Center uses existing native components of z/OS, such as IBM z/OS Management Facility (IBM z/OSMF), Common Event Adapter (CEA), and Event Notification Facility (ENF) to facilitate the communication flow with the Evidence Providers that are deployed in z/OS. Evidence is contributed by each applicable component through an SMF 1154 record type, which was introduced in z/OS V2R4 or later for compliance information logging.

Some components in z/OS, typically with applicable security controls that must be surfaced to the IBM Z Security and Compliance Center analyzer, historically can generate and write their own SMF records. These components, such as RACF, extract the relevant information from within their own control blocks to compile their specific SMF 1154 subtype record.

Other components or applications, such as IMS, cannot write SMF records. To enable those applications to participate in the evidence collection process, z/OS Compliance Integration Manager (IBM zCIM) was created to write SMF records on their behalf.

The components and applications participating directly and the ones that use IBM zCIM are shown in Figure 3-1 on page 29.

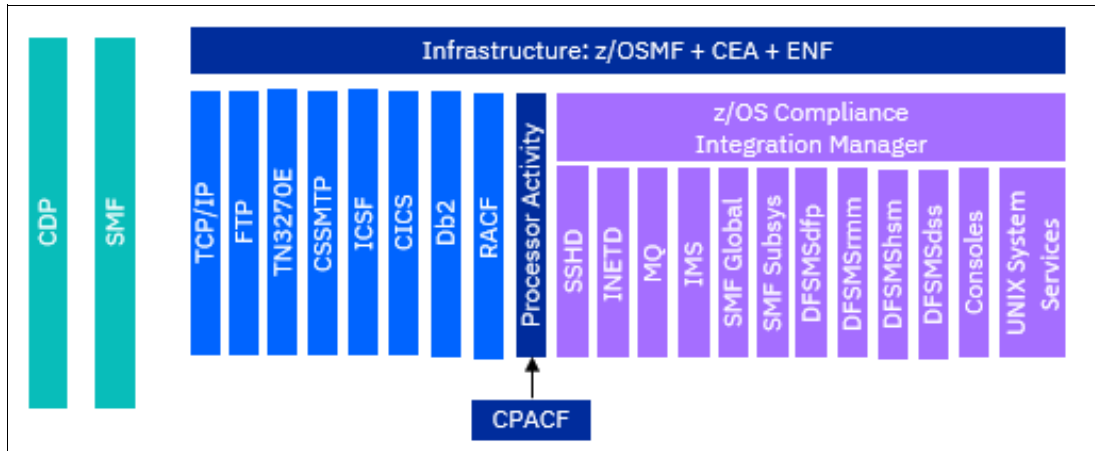


Figure 3-1 z/OS components and applications that participate as Evidence Providers

SMF type 1154 provides compliance data

In z/OS V2R4 and later (with PTFs), the process of collecting evidence (compliance data) is helped by SMF record type 1154. This new record type is used to collect system settings and other forms of compliance data.

The SMF 1154 record represents compliance data that is divided into subtype records, each representing a different z/OS component or application. Participating z/OS components and applications are enhanced to gather the applicable goal proof-points; build and write these proof-points to their respective SMF 1154 subtype records; and do so on demand from a triggered ENF 86 signal.

z/OS is further enhanced to enable the collection of compliance data from the IBM z16 CP Assist for Cryptographic Function (CPACF) counters and several z/OS applications and components.

These enhancements are available in new releases of z/OS and participating applications. Therefore, IBM Z Security and Compliance Center requires that the z/OS operating system and participating Evidence Providers meet a specified software level.

The usage of SMF record type 1154 and its subtypes for collecting compliance data is described in 3.3, “A single source of the truth” on page 33.

z/OS Compliance Integration Manager creates SMF records

The IBM zCIM started task is a component of IBM Z Security and Compliance Center, which runs on z/OS and creates the SMF 1154 records for compliance data gatherers. Some components and applications write the SMF 1154 records directly, and others rely on IBM zCIM to write the records on their behalf.

Deploy an instance of IBM zCIM on each z/OS system that participates in compliance data collection.

IBM zCIM is delivered with IBM Z Security and Compliance Center.

For more information about configuring IBM zCIM, see *IBM Z Security and Compliance Center Guide*, SC31-5705.

IBM Z Common Data Provider provides access to SMF records

IBM Z Common Data Provider provides the infrastructure for accessing IT operational data like SMF records from z/OS systems and streams it to the target platform in a consumable format. IBM Z Common Data Provider includes a web-based configuration tool that is provided as a plug-in for IBM z/OSMF.

An instance of IBM Z Common Data Provider must be installed and configured on each z/OS logical partition (LPAR) from which you want to collect and analyze SMF data.

IBM Z Common Data Provider is delivered with IBM Z Security and Compliance Center.

For information about configuring IBM Z Common Data Provider, see *IBM Z Security and Compliance Center Guide*, SC31-5705.

3.1.2 Evidence presentation

Evidence presentation is the part of IBM Z Security and Compliance Center that is visible to the user. This part of the solution consists of numerous microservices that run in Red Hat OpenShift Container Platform, each with its own unique function. Evidence presentation includes the user interface (UI) or dashboard, and functions including UI management, access control, database control, logging, and monitoring. The goal of this architecture is to provide a simplified process for collecting and validating compliance data through a common GUI.

Specifically, the microservices provide the following functions to IBM Z Security and Compliance Center:

- ▶ Enable the collection of goals from Evidence Providers.
- ▶ Analyze compliance data streams by using Apache Kafka.
- ▶ Securely store compliance data.
- ▶ Map compliance data to the controls that are applicable to the specific chosen regulatory framework profile.
- ▶ Present compliance data to the user in a visibly attractive format on the UI dashboard from which reports can be generated.

Figure 3-2 shows the microservices architecture of IBM Z Security and Compliance Center.

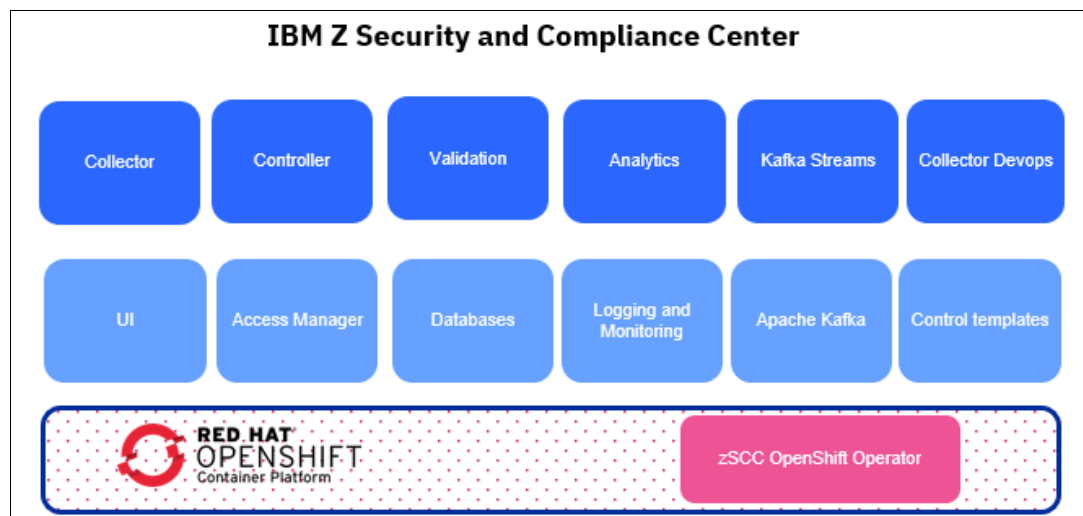


Figure 3-2 IBM Z Security and Compliance Center microservices architecture

As shown in Figure 3-3 on page 31, evidence collection drives several different components and microservices:

- ▶ The Collector microservice, through a z/OSMF REST API, notifies the z/OS CEA to trigger an ENF 86 signal. Each participating z/OS component or application listens for this signal. On receiving it, they begin collecting goal proof-points.
- ▶ z/OS components that can write their own SMF records gather a snapshot of the defined security information and create their specific SMF 1154 subtype records.
- ▶ Some z/OS components and applications cannot write SMF records. In these cases, IBM zCIM writes SMF records on their behalf. For more information about IBM zCIM processing, see Figure 3-4.
- ▶ All participating components and applications, including IBM zCIM, write their collected evidence data that is captured in their respective SMF 1154 subtype records to SMF.
- ▶ In IBM Z Common Data Provider, the System Data Engine, by using the defined SMF data stream names, formats the data from the SMF 1154 record with the applicable JSON templates and sends it to the collector's Logstash on a protocol that supports Transport Layer Security (TLS).

The communication between IBM Z Security and Compliance Center and your evidence-providing environments is encrypted with TLS in both directions and happens solely within your own intranet domain, so your compliance data is always protected.

3.2.1 A closer look at z/OS Compliance Integration Manager processing

In IBM zCIM, the started task CKCS1154 listens for the ENF 86 signal; invokes an internal process manager to trigger the collection of configuration and subsystem security information that uses CKFCOLL; and creates a temporary CKFREEZE file, as shown in Figure 3-4.

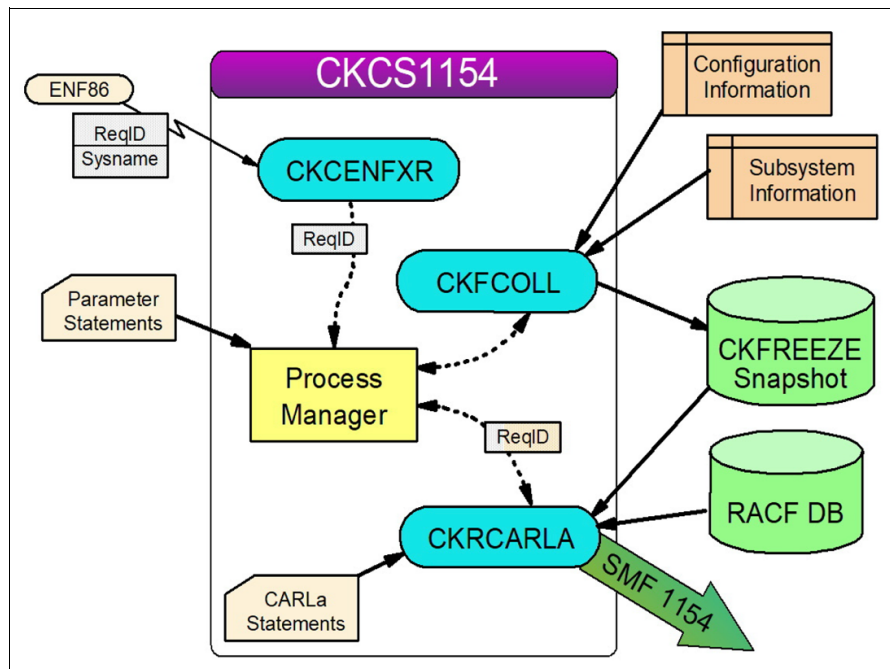


Figure 3-4 z/OS Compliance Integration Manager internal workflow

After all relevant information is captured in the CKFREEZE file, the CKRCARLA process is started to ingest this information, format it, and build the specific SMF 1154 subtype records by using CARLa scripts.

3.3 A single source of the truth

In simplest terms, proving compliance means demonstrating that your data is protected adequately according to the governing regulations to which it must adhere. Data is typically protected from cyberthreats through a combination of the following items:

- ▶ **Authentication:** Requires an identity (such as a user ID) and a secret (such as a password) to log in to a system.
- ▶ **Access control:** Establishes a set of policies to determine which users can access certain data and services (authorization).
- ▶ **Encryption:** Applies a cryptographic key and a cryptographic algorithm to a piece of data to prevent unauthorized disclosure of the data.¹

These methodologies and technologies, which have been part of the z/OS operating system since its inception, are continuously enhanced as the cyberthreat landscape evolves. As the multitude of security controls and parameter settings that are available in z/OS keep evolving, more are added with each new release of z/OS and its supported components and applications.

Likewise, the regulatory compliance frameworks also continue to evolve, and new requirements must be met with each new version of these frameworks.

To support this evolution, a single source of the truth is required; for this purpose, the SMF record type 1154 was created. It serves as a repository of a z/OS system's security controls that is auditable, immutable, signed, and timestamped to ensure that it represents a true reflection of a systems' security posture.

The SMF 1154 record is designed to group z/OS component and application compliance data into representative subtype records. To enable identification, each subtype includes an SMF extended header, which is defined by the IFASMFH macro and an SMF 1154 common type header, which defined by the IFAR1154 macro. The remainder of the subtype data is specific to the selected component or application.

Table 3-1 lists, at the time of writing, the SMF 1154 record subtypes for the z/OS components and applications that participate in compliance data gathering.

Table 3-1 Categorized subtypes of SMF Record type 1154

Subtype	Description	z/OS domain	Goal tags	Data protection role
01	TCP/IP stack	Network	TCPIP COMM SERVER	User of authentication, access control, and encryption services for secure network traffic
02	FTP daemon	Network	FTP COMM SERVER	User of authentication, access control, and encryption services for secure network traffic
03	TN3270	Network	TN3270E COMM SERVER	User of authentication, access control, and encryption services for secure network traffic

¹ *Getting Started with z/OS Data Set Encryption, SG24-8410*

Subtype	Description	z/OS domain	Goal tags	Data protection role
04	CSSMTP	Network	CSSMTP COMM SERVER	User of authentication, access control, and encryption services for secure network traffic
49	ICSF	Security	ICSF	Provider of software and hardware that uses CPACF, and encryption services to z/OS components and applications
50	z/OS Consoles	Operating System	CONSOLE	User of authentication, access control, and encryption services for secure system operations
51	DFSMSdfp	Storage	DFSMS RMM	User of authentication, access control, and encryption services for secure data processing
52	DFSMSrmm	Storage	DFSMS RMM	User of authentication, access control, and encryption services for secure data processing
53	DFSMSshsm	Storage	DFSMS RMM	User of authentication, access control, and encryption services for secure data processing
54	DFSMSdss	Storage	DFSMS RMM	User of authentication, access control, and encryption services for secure data processing
77	z/OS UNIX System Services	Operating System	UNIX System Services	User of authentication, access control, and encryption services for secure system operations.
78	SSHD	Network	SSHD	User of authentication, access control, and encryption services for secure network traffic
79	InetD	Network	InetD	User of authentication, access control, and encryption services for secure network traffic
80	CICS TS for z/OS	Applications	SIT CICS TCPIPS	User of authentication, access control, and encryption services for secure application transaction processing
81	Db2 for z/OS	Applications	Db2	User of authentication, access control, and encryption services for secure database processing
82	IBM MQ region	Applications	IBM MQ	User of authentication, access control, and encryption services for secure application transaction processing
83	RACF	Security	RACF	Provider of both authentication and access control services to the rest of the z/OS components and applications
85	IMS control region and IMS OTMA	Applications	IMS	User of authentication, access control, and encryption services for secure application transaction processing

Subtype	Description	z/OS domain	Goal tags	Data protection role
86	IMS operation manager	Applications	OM IMS	User of authentication, access control, and encryption services for secure application transaction processing
87	IMS Connect	Applications	CONNECT IMS	User of authentication, access control, and encryption services for secure application transaction processing
96	SMF global reporting options	Operating System	SMF GLOBAL	Logger of authentication, access control, and encryption configurations and usage by z/OS components and applications
97	SMF subsystem reporting options	Operating System	SUBSYS SMF	Logger of authentication, access control, and encryption configurations and usage by z/OS components and applications.
128	CPACF	Security	PROCESSOR ACTIVITY	Provider of hardware encryption services to z/OS components and applications

The SMF 1154 record subtypes are grouped into the z/OS domains, which each play a role in a data protection methodology by performing authentication, controlling access, or encrypting either data-at-rest or data-in-flight. The interoperability of the z/OS components and applications means that this protection typically happens in a combined fashion. For example, a network component (such as TN3270) uses a security component (such as RACF), which then uses an encryption component (such as ICSF) to ensure that the communication and the data in transit between z/OS and a client is encrypted and secure. The roles of the z/OS components and applications can roughly be categorized as either a *User*, a *Provider*, or a *Logger* of security services and configurations that are required for a data protection methodology.

The expectation is that this list will expand with new releases of the solution as other z/OS components or applications, including ones from independent software vendors, start to participate in the evidence collection process.

Table 3-1 on page 33 also includes a column listing the “Goal tags” that are associated with each subtype in IBM Z Security and Compliance Center Goals, which are directly related to the areas that the goal covers. This detail can be seen by selecting **Configure** → **Goals** in the dashboard and looking at the expansion of any goal. For example, in Figure 3-5, the expansion of Goal ID:4086002, which is tagged with OM and IMS and is in the Application category, shows that the SMF 1154 subtype 86 record holds the validation data.

The same principle applies to Goal ID:4087001, which is tagged with CONNECT and IMS, also is in the Application category. The SMF 1154 subtype 87 record holds the validation data.

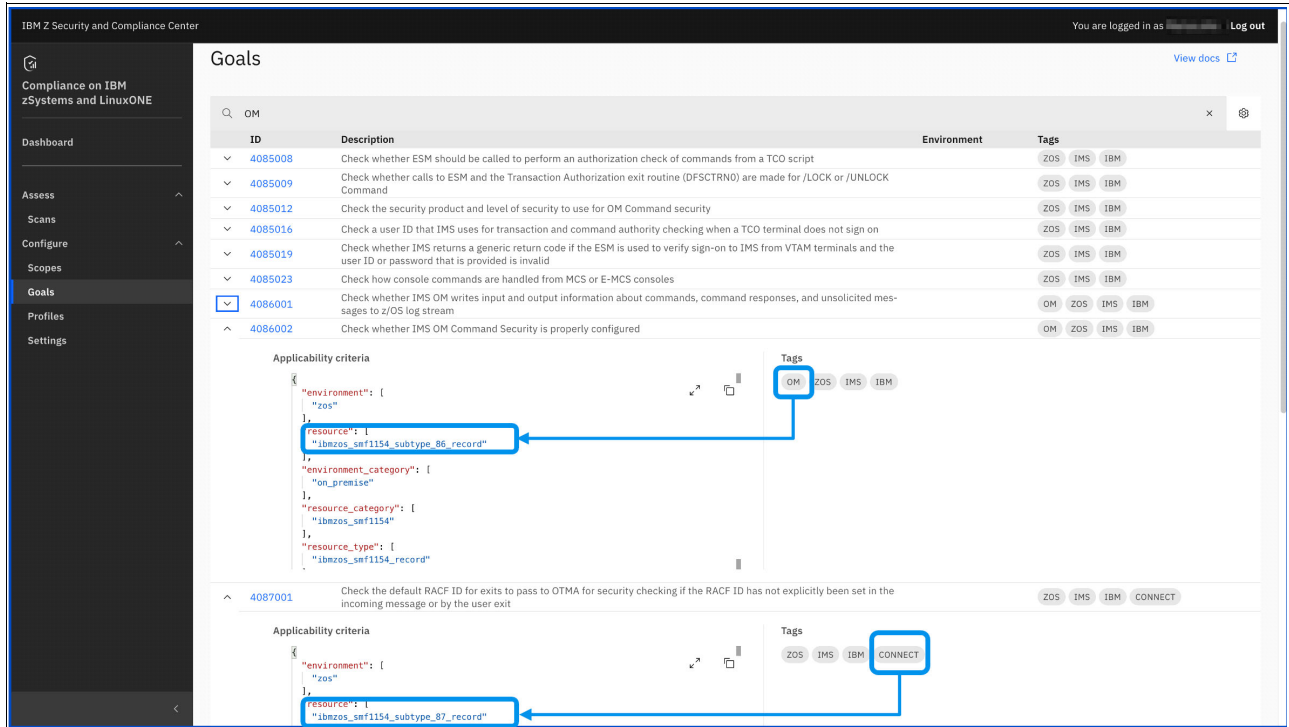


Figure 3-5 Correlation between Goal tags and the SMF 1154 subtype record

In summary, the SMF 1154 records serve as the crucial compliance data repository, which acts as evidence input to the compliance auditing process (with reports as output).

Note: For the most current information about SMF 1154 record subtypes, see *z/OS MVS System Management Facilities for Version 2 Release 5, SA38-0667*.

For more information about the SMF 1154 record subtypes, see Appendix B, “SMF record type 1154 overview” on page 107.

3.3.1 SMF considerations

During the writing of this IBM Redbooks publication, several SMF setup actions were taken to ensure the best performance and availability of the solution. The following best practices are provided for your consideration and possible use.

Using log streams

Consider using z/OS log streams to give real-time access to SMF data to the IBM zCIM component for generating its part of the SMF 1154 records, and to IBM Z Common Data Provider because it streams the records to the collector microservice.

Evaluate your settings for parmlib member SMFPRMxx:

- ▶ For improved performance, define in-storage (**INMEM** parameter) log streams.
- ▶ If you have the IBM zEnterprise® Data Compression (IBM zEDC) software feature enabled, consider using the **COMPRESS** parameter with the LOGSTREAM definition.
- ▶ Along with the **COMPRESS** parameter, and to improve performance further, you can use the **PERMFI**X parameter. By fixing buffers in memory for communication with zEDC, the overall SMF performance benefits.

Depending on your memory constraints, you can use up to 2 GB of fixed pages for SMF records compression. Even if the minimum value is 1M for **PERMFI**X, SMF can use up to 2 MB of fixed storage.

The best parameter setting for your rate of SMF record generation can be tuned through evaluating SMF statistics that are obtained from your SMF type 23 records.

Retaining records for auditors

Even if the SMF records are directly streamed to IBM Z Security and Compliance Center after generation on request through the ENF 86 signal, the records can be stored on z/OS for audit purposes.

When using SMF **LOGSTREAMS**, the retention of the SMF 1154 records by the system logger is determined by the **RETPD** and **AUTODELETE** parameters:

- ▶ **RETPD** defines the retention period, in days, for the SMF log data. Typically, audit-related data should be kept for a longer period than performance-related data.
- ▶ **AUTODELETE** specifies whether the system logger deletes the log data or whether it relies on an external process, such as using the **IFASMF**DL utility for the SMF log streams with the keywords **ARCHIVE**, which “dumps” the records and then deletes them, or the **DELETE** keyword, which deletes the selected records.

Using the **IFASMF**DL utility with the **DUMP** or **ARCHIVE** parameter transfers the SMF records from the log streams to another media (disk or tape data sets) where a specific retention period can be set through a disk or tape management subsystem.

Depending on your policy and audit requirements, the retention period varies.²

There are different requirements between government regulations or industry regulations. For example, in the US, the Sarbanes-Oxley Act (SOX) requires that financial transactional data is kept for 7 years, and the Health Insurance Portability and Accountability Act (HIPAA) requires health information to be retained for 6 years.

² The National Institute of Standards and Technology (NIST) provides guidance in the NIST publication SP 800-53.

Some regulations have specific requirements for data that is related to individuals and privacy, but the SMF records that are generated by IBM Z Security and Compliance Center do not contain any sensitive personal information (SPI). Therefore, such requirements should not apply unless a specific enterprise policy requires it.

Protecting records from tampering

As with any data that is used as input to audits, ensure that the data is not tampered with to preserve evidence and ensure integrity.

The best way to prevent tampering is to enable SMF record signing. The digital signature can be the same for all the records or specific to a log stream.

SMF digital signatures are based on a token and a key (RSA or ECC). When enabled, SMF data is “signed” before being processed by the system logger:

- ▶ A hash is computed for every record of every type belonging to the signed log stream.
- ▶ Periodically, SMF digitally signs the hash by using the private key that is associated with the log stream and stores it as a signature record.
- ▶ At the SMF interval, a new signature for all the hashed records also is stored.

When the log streams are moved to a different media (disk or tape), the **NOSIGTRIP** parameter must be specified to carry forward the signature records.

When required, the SMF data signature can be verified by using the digital signature public key with the **IFASMFDP** utility by using the **NOSGISTRIP** and **SIGVALIDATE** parameters.

Dual signatures can use a quantum-safe algorithm, which requires ICSF HCR77D1 and an IBM z15 or later. For more information, *Transitioning to Quantum-Safe Cryptography on IBM Z*, SG24-8525.

For more information about the SMF digital signature process, see *z/OS MVS System Management Facilities for Version 2 Release 5*, SA38-0667.

3.4 Solution-defined roles and responsibilities

IBM Z Security and Compliance Center is designed to provide different views of the compliance process to fulfill the requirements for each role that are specific to their needs. For example, an auditor with little or no need to have knowledge about IBM Z security needs a different view of the security and compliance posture than the one for the Compliance Lead, who needs to administer both the process and evidence collection, and possibly partake in remediation activities.

IBM Z Security and Compliance Center offers different role-based authorization levels within the application itself, apart from the z/OS system and security administration roles that are needed for the installation, maintenance, and support of the z/OS components and applications acting as Evidence Providers.

Also, for many organizations, the separation of duties between Compliance Viewers and auditors, and those responsible for administering the compliance evidence gathering process, is important. On the evidence-provisioning side, IBM Z Security and Compliance Center requires a system administration role that is responsible for installation, maintenance, and support of the different z/OS components and applications participating in evidence collection.

In most organizations, this role is separated into the z/OS Security administrator and that of the system administrators that are responsible for installing and maintaining the operating system and subsystems, such as CICS, IMS, or Db2.

Although it is not a best practice, these roles might even be combined in some enterprises, but the roles must perform in unison to deploy IBM Z Security and Compliance Center to participate in evidence collection and reporting.

In addition, these roles can help with remediation activities to improve the compliance posture on z/OS from identified compliance failures. (For more examples of remediation activities, see Appendix A, “How to find and remediate failing goals” on page 101.)

With the ability to assign different roles and inherited authorization levels to users, you can grant each user the access level that is required to perform only their role in the compliance process. This approach is one of the underpinnings of the zero trust model to establish a state of *least privilege*, so that no user or application has any more access than is needed. In essence, *ability* should *not* exceed authority.

For this approach, IBM Z Security and Compliance Center uses customized Keycloak UIs for login, registration, administration, and account management. Keycloak is an open-source software application that you can use to do single sign-on with Identity and Access Management. It is aimed at modern web applications and RESTful web services, and it is developed by JBoss, which is a division of Red Hat.

With IBM Z Security and Compliance Center, it is possible to define three types of roles:

- ▶ A *Compliance Administrator* is responsible for managing IBM Z Security and Compliance Center during and after installation. A user with this level of authority can authorize other users, operate the dashboard, and keep the software up to date.
- ▶ A *Compliance User* is responsible for using the dashboard to query system compliance and generate compliance reports for auditors to review.
- ▶ A *Compliance Viewer* is permitted only to view pages of the dashboard, such as scan results and defined scopes.

Table 3-2 summarizes compliance roles, responsibilities, and authorizations, and maps them to the three roles that are defined to IBM Z Security and Compliance Center.

Table 3-2 IBM Z Security and Compliance Center defined roles with responsibilities and authorization

Defined roles	Compliance role	Responsibilities	Authorization level
Compliance Administrator	Compliance Lead	Managing IBM Z Security and Compliance Center during and after installation.	<p>A user with this level of authority can authorize other users, operate the dashboard, and keep the software up to date. Specifically, this role can do the following tasks:</p> <ul style="list-style-type: none"> ▶ Keep the user base in sync with the LDAP database. ▶ Manage user definitions and maintenance. ▶ Define scopes, collectors within these scopes, and define the credentials that are required for these collectors. ▶ Manage scan result retention. ▶ Manage the audit logs.

Defined roles	Compliance role	Responsibilities	Authorization level
Compliance User	Evidence Provider	Responsible for using the dashboard to query system compliance and generate compliance reports for auditors to review.	This role can create, update, or delete objects in the dashboard. This role cannot access the user administration control area.
Compliance Viewer	Chief Information Security Officer (CISO) or internal auditor	Responsible for reviewing and interpreting the compliance reports and representing the compliance results to external auditors. This role also might drive remediation actions to improve the compliance posture.	This role is permitted only to view pages of the dashboard, such as scan results and defined scopes. This role cannot do the following tasks: <ul style="list-style-type: none"> ▶ Create, delete, or update objects in the dashboard. ▶ Access the user administration control area.
	CISO or external auditor	Typically, the CISO or external auditor might be granted short-term access as a Compliance Viewer, if deemed necessary.	This role normally views only the reports that are generated either in PDF or CSV format, so it does not require access.

To define users and roles in IBM Z Security and Compliance Center, click the **Administration Console** tab, and then select **Configure** → **Access Management** (see Figure 3-6).

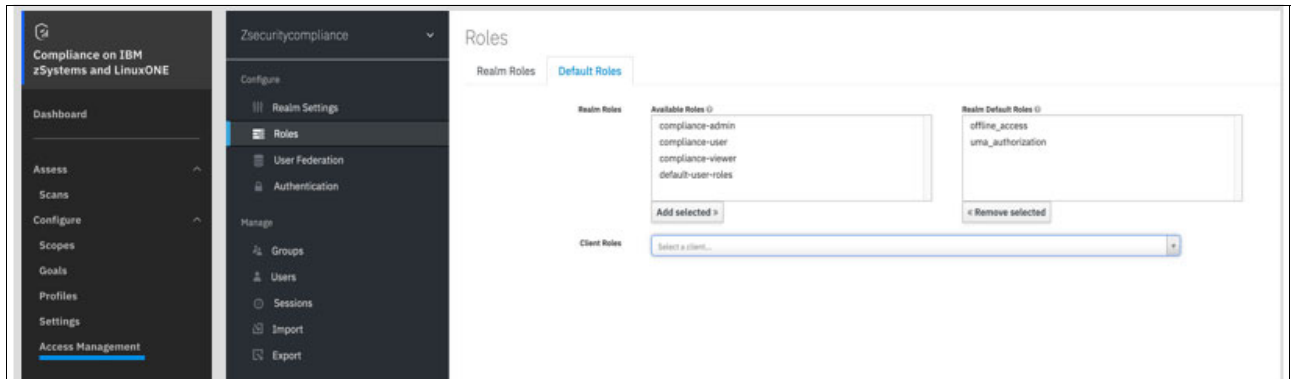


Figure 3-6 Defining users and assigning roles

3.5 Evidence collection and reports

The process of creating reports starts with the collection of evidence from the systems that are checked for compliance. This task happens through a scan that is done by IBM Z Security and Compliance Center on a schedule that you determine. When the scan completes, IBM Z Security and Compliance Center displays the detailed results in the UI dashboard, from which you can review the compliance posture for your systems. The dashboard identifies potential non-compliance so that you can determine the appropriate action to take, such as performing remediation actions or documenting risk findings and compensating controls.

After a scan, you can choose to download a detailed report that can be used to provide compliance data to stakeholders and auditors.

The main steps for using IBM Z Security and Compliance Center are summarized in Figure 3-7 on page 41.

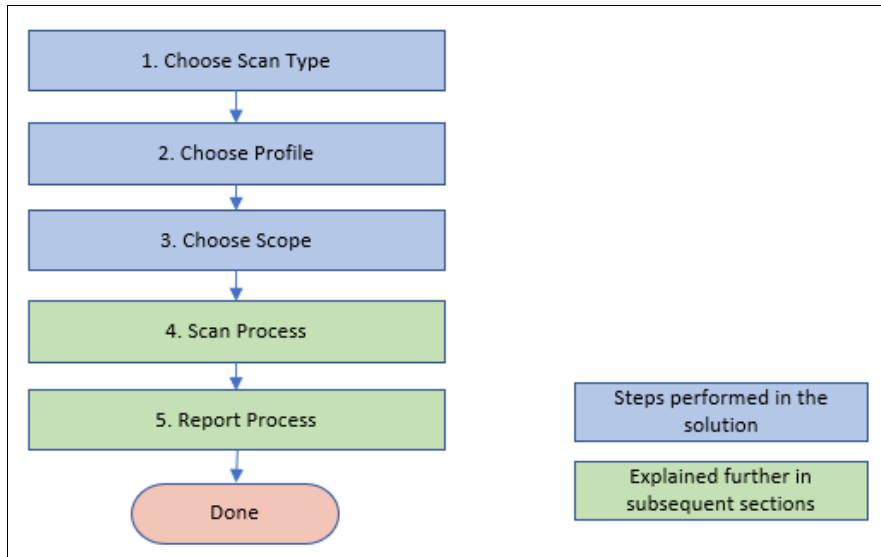


Figure 3-7 Main steps of the evidence collection and reporting process

The numbered steps in Figure 3-7 are as follows:

1. Choose Scan Type: Usually, you choose to run a validation scan. This type of scan reads compliance data from a z/OS system and compares the results to your choice of regulatory standards, which you choose in step 2 (the profile).

Other available scan types include the following ones:

- Discovery: Returns a list of systems that are in scope for validation.
- Fact Collection: Returns SMF data about the systems that were detected during a discovery scan.
- Fact Validation: Compares facts that already were collected to your choice of regulatory standards.

Note: A validation scan includes discovery and fact collection.

2. Choose Profile: When you choose a profile, you select the security controls against the system to be validated. A profile is a collection of related controls that correlate to a regulatory framework.

You can select a predefined profile that is populated with a list of controls that you can validate against, or you can create a custom profile to define the list of controls that you want to validate against.

IBM Z Security and Compliance Center includes predefined profiles for the following regulatory frameworks and security standards:

- PCI DSS
- NIST SP 800-53
- Center for Internet Security (CIS) Critical Security Controls

3. Choose Scope: Choose which z/OS systems are included in the scan. By creating scopes in IBM Z Security and Compliance Center, you target your scans to a specific area of your business, such as a specific system or set of systems. You can run scans of specific scopes to determine system availability, configuration settings, and adherence to regulatory controls, as defined in the profile.

If you are getting started with IBM Z Security and Compliance Center, choose one system. As you become more familiar with the solution, you can add more systems to the scope for your scans. Eventually, you can choose to run a scan for all systems within a sysplex or all systems that run production workloads.

Figure 3-8 shows a scope that includes a subset of z/OS systems in a multi-system environment. During a validation scan, compliance data is collected from two z/OS systems (SYS1 and SYS2) in PLEX1 and two z/OS systems (P01 and P02) in PLEX2. No other systems are defined to the scope.

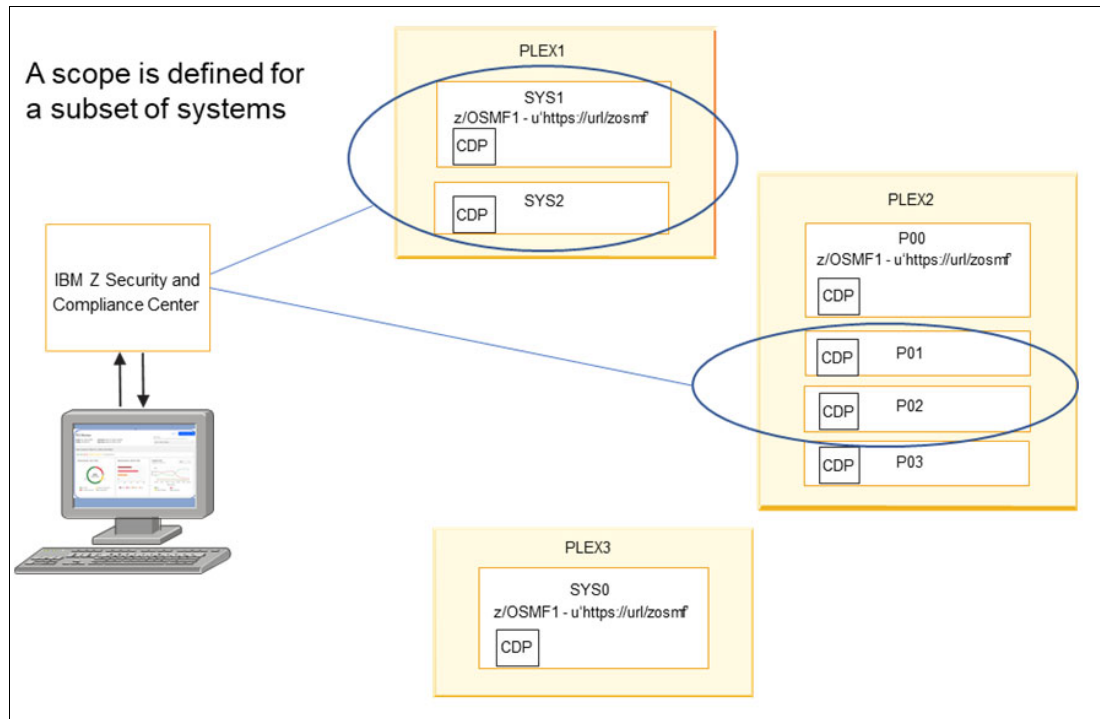


Figure 3-8 A scope for a subset of systems

4. Scan Process: During the scan process, you iteratively run a scan, view its results, and perform remediation of non-compliance. Do this task until you are satisfied with the scan output. We look at this iterative cycle more closely in 3.5.1, "Running a scan" on page 42.
5. Report Process: You can produce a report in a PDF or spreadsheet format that shows your current compliance posture. The Compliance Lead³ can distribute this report to stakeholders, such as the CISO or application owners. These parties can review the report and provide feedback on system compliance.

The reports can be large. As with running scans, you might want to iteratively produce and review reports until your reviewers are satisfied with the report output. We look at this process more closely in 3.5.2, "Generating a report" on page 44.

3.5.1 Running a scan

During the scan process, the Compliance Lead runs a scan and examines its output in the IBM Z Security and Compliance Center dashboard.

The steps for running a scan and working with the results are summarized in Figure 3-9 on page 43.

³ For a description of roles and responsibilities, see Table 3-2 on page 39.

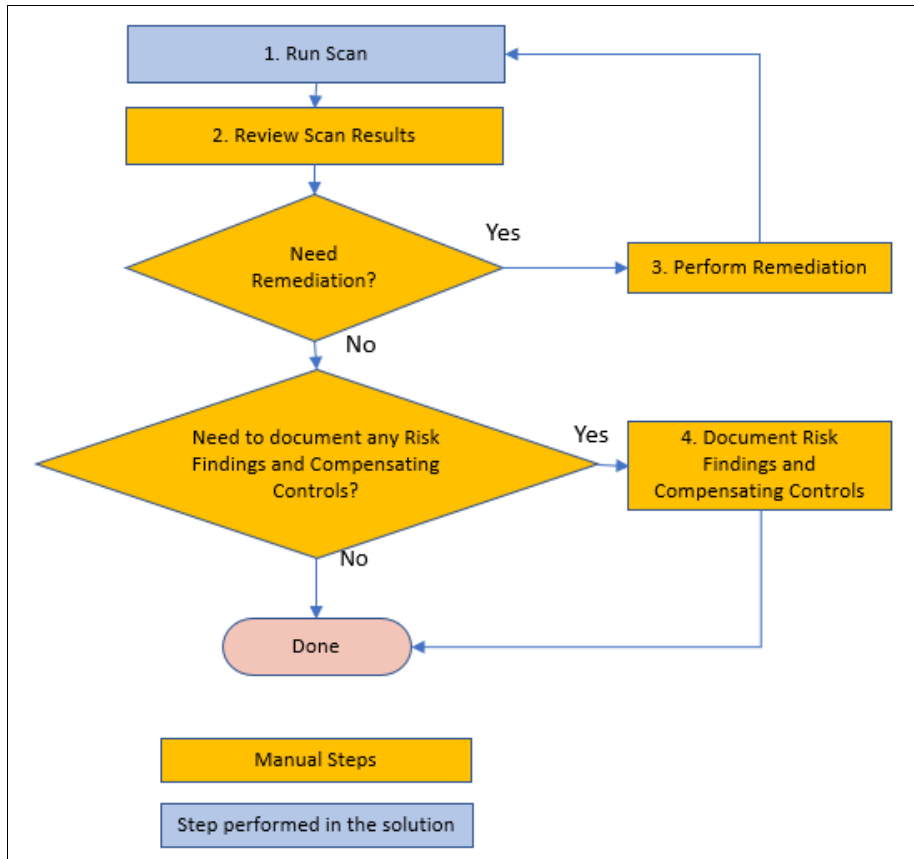


Figure 3-9 Scan process

The numbered steps in Figure 3-9 are as follows:

1. Run Scan: You might do this action multiple times. The scan should have been set up in steps 1 on page 41 - 3 on page 41 by choosing the scan type, profile, and scope. The Compliance Lead can now choose the option to run an on-demand validation scan.

Note: Depending on the following factors, validation in the Run Scan step can take several minutes to complete:

- ▶ Number of goals to be validated
- ▶ Number of systems in the scope to be validated
- ▶ Available system resources (CPUs, memory, storage, and networking)

2. Review Scan Results: The scan results can be viewed from the IBM Z Security and Compliance Center dashboard. The controls that are non-compliant can be examined further in the solution, down to the field in the SMF record that caused the control to be non-compliant. For more information about the non-compliant items in the scan results, see Appendix A, “How to find and remediate failing goals” on page 101.
3. Perform Remediation: For any non-compliant items, the Compliance Lead should determine whether remediation is needed. The remediation might be done by a z/OS administrator, such as a RACF or network administrator. For example, if the RACF control for APF libraries is non-compliant, the RACF administrator might need to change the UACC (universal access) setting in a RACF profile.

With some controls in the solution, you can update the default parameters that are associated with specific goals. For example, there is a z/OS Communication Server goal that checks the configured inactivity timeout value. The default goal checks for a timeout value of 1 - 900 seconds. If your local standards call for a shorter maximum timeout value, you can set the range for this goal to a shorter interval.

Another example is the RACF password interval. The default goal checks for the maximum password life of 90 days. If your local policy is to have passwords expire after 60 days, you can set the default to 60 instead of 90.

4. Document risk findings and compensating controls: If a non-compliant item is not remediated, the Compliance Lead should document the risk finding, or determine whether a compensating control must be put in place.

The PCI DSS standards recognize that a company might need to use a compensating control based on their environment. The PCI DSS standards provide details about what is required for a compensating control. For example, in the PCI DSS standard there is a requirement to have an anti-malware solution deployed on the systems, but there is no anti-malware software solution for z/OS.

What a company might provide as a compensating control is to document their overall approach to z/OS maintenance and the software that is installed on z/OS. IBM provides some guidelines in a document titled [z/OS Preventive Maintenance Strategy to Maintain System Availability](#).

Important: As a best practice, upgrade 2 - 4 times per year to the latest RSU Preventive Maintenance that is available. HIPER and PE fixes should be reviewed weekly and installed weekly or monthly if possible. HIPER fixes can be ordered and received for immediate installation if needed. Security and Integrity APARs and Red Alerts should also be monitored regularly.

IBM also provides the IBM Z and LinuxONE Security Portal, which provides information about potential vulnerabilities on IBM Z software products. For more information, see the [FAQ document](#).

3.5.2 Generating a report

During the report process, you examine the reports that are produced by IBM Z Security and Compliance Center. As with the steps in the scan process, you might need to perform this process iteratively, reviewing the reports instead of the scan output in the IBM Z Security and Compliance Center dashboard.

The steps for generating a report and reviewing it are summarized in Figure 3-10 on page 45.

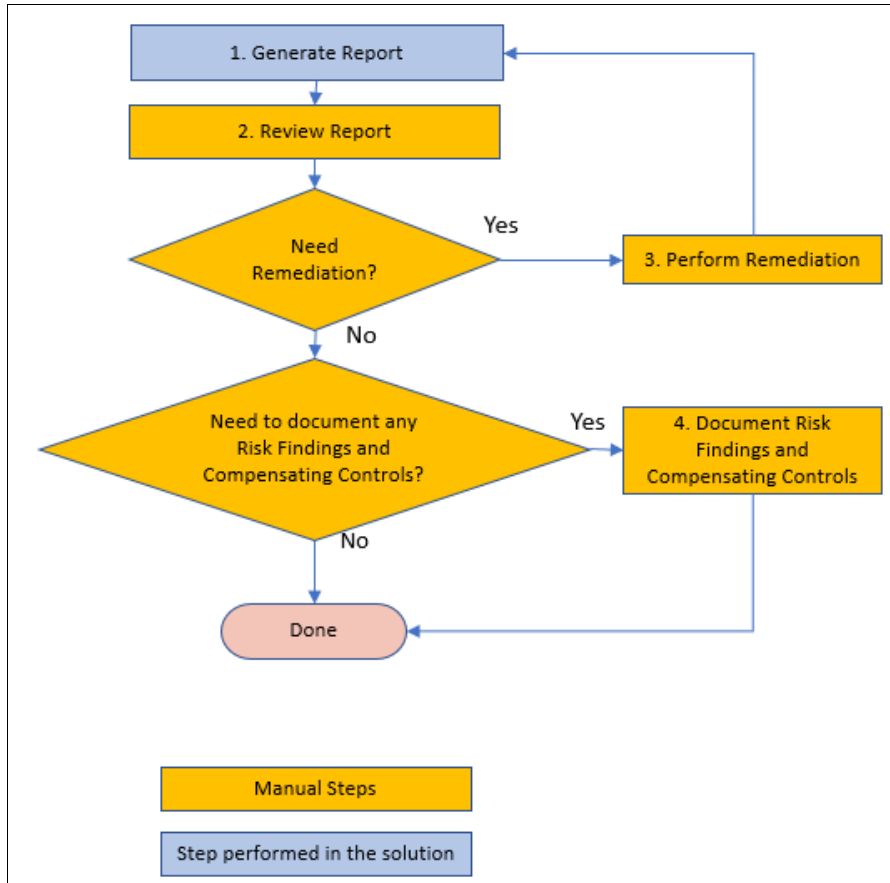


Figure 3-10 Report process

The numbered steps in Figure 3-10 are as follows:

1. **Generate Report:** For any scan that you run, you can optionally download a report in PDF format or spreadsheet (XLSX) format. You also can choose to create a delta report to compare two scans. There are options to include different details in the report. For example, you can choose to include only a scan summary.

You might generate a report multiple times if remediation is needed.

2. **Review Report:** The Compliance Lead can review the report themselves, or they can distribute the report to stakeholders, such as the CISO or application owners. These parties can review the report and provide feedback on system compliance. The controls that are non-compliant can be examined further in the reports, down to the field in the SMF record that caused the control to be non-compliant.
3. **Perform Remediation:** For any non-compliant items, the Compliance Lead should determine whether remediation is needed. This step is the same as Step 3 on page 43.
4. **Document risk findings or compensating controls:** If a non-compliant item is not remediated, the Compliance Lead should document the risk finding or determine whether a compensating control should be put in place. This step is the same as Step 4 on page 44.

3.6 Solution prerequisites

IBM Z Security and Compliance Center must be deployed in the Red Hat OpenShift Container Platform, which can run either in IBM zCX or on a VM running in a z/VM or RHEL KVM LPAR.

Important: The prerequisites that are listed in this section are current at the time of writing. For the latest information, see *IBM Z Security and Compliance Center Guide*, SC31-5705.

IBM Z Security and Compliance Center is offered for the IBM Z platform as product ID (PID) 5655-CC1. It is a one-time charge (OTC) product for IBM z15 or IBM z16.

On an IBM z16, the hardware provides CPACF firmware to enable crypto counter statistics to track cryptographic algorithms, bit lengths, and key security usage. The CPACF counters provide evidence for compliance (which cryptography is used), performance (frequency of cryptography use), and configuration (proof of change).

IBM also offers an equivalent solution for IBM LinuxONE, IBM LinuxONE Security and Compliance Center, which is orderable as PID 5655-LC1. It is an OTC product for IBM LinuxONE III or IBM LinuxONE Emperor 4.

3.6.1 Requirements for deploying Red Hat OpenShift Container Platform on IBM zCX for Red Hat OpenShift

To deploy Red Hat OpenShift Container Platform on IBM zCX for Red Hat OpenShift, ensure that your system meets the minimum systems requirements, as described in Table 3-3.

Table 3-3 Minimum requirements for IBM zCX deployment

Hardware	<ul style="list-style-type: none">▶ IBM z15 or IBM z16.▶ One network adapter (Open Systems Adapter (OSA)). An existing OSA should be sufficient, assuming that enough spare bandwidth is available and TCP/IP DVIPA is enabled.▶ One LPAR with six zIIP processors with SMT2 enabled.
Red Hat OpenShift Container Platform + IBM Z Security and Compliance Center	<ul style="list-style-type: none">▶ Three IBM zCX for Red Hat OpenShift Container Platform instances for control plane machines.▶ Two IBM zCX for Red Hat OpenShift Container Platform appliance instances for compute machines.▶ One IBM zCX for Red Hat OpenShift Container Platform appliance instance for the temporary bootstrap machine.

Memory	<ul style="list-style-type: none"> ▶ 16 GB for each Red Hat OpenShift Container Platform control plane machine. ▶ 8 GB for each Red Hat OpenShift Container Platform compute machine. ▶ 16 GB for the temporary Red Hat OpenShift Container Platform bootstrap machine.
Storage	<ul style="list-style-type: none"> ▶ 100 GB per node. ▶ 1 TB persistent storage, such as NFS storage, to allow for sufficient capacity for the accumulation and retention of scan result data over time. ▶ z/OS VSAM linear data sets are used for the IBM zCX for Red Hat Enterprise Linux CoreOS (RHCOS) disks. To reach the minimum required DASD size for RHCOS installations, you require extended address volume (EAV) storage.

3.6.2 Requirements for deploying Red Hat OpenShift Container Platform in virtual machines

To install the solution on a VM running in either a z/VM or Red Hat KVM LPAR, ensure that your system meets the minimum system requirements, as described in Table 3-4.

Table 3-4 Minimum requirements for deployment in virtual machines

Hardware	<ul style="list-style-type: none"> ▶ IBM z15, IBM z16, IBM LinuxONE III, or LinuxONE Emperor 4. ▶ One z/OS network adapter (OSA). An existing OSA should be sufficient, assuming that enough spare bandwidth is available. ▶ Six Integrated Facility for Linux (IFL) processors with SMT2 enabled, which can be shared across different nodes.
Red Hat OpenShift Container Platform installation ^a	<ul style="list-style-type: none"> ▶ Three control nodes. ▶ Two compute nodes.
IBM Z Security and Compliance Center ^a	<ul style="list-style-type: none"> ▶ One compute node. ▶ One or two IFL processors (shared, depending on workload). ▶ 3 TB of persistent storage (depending on workload).
Memory	<ul style="list-style-type: none"> ▶ 16 GB for each control node. ▶ 32 GB for each compute node.
Storage	<ul style="list-style-type: none"> ▶ 120 GB per node.

a. Dedicated resources are needed.

3.6.3 Operating system requirements

z/OS V2R5 and V2R4 are enhanced to enable the collection of compliance data from IBM z16 CPACF counters and several participating z/OS applications and components. Also, participating applications and components collect and write compliance data to SMF 1154 records that are associated with its unique subtype.

This support requires PTFs for z/OS V2R5 and z/OS V2R4 that enable compliance data collection. To identify and install the specific PTFs, use the following fix category (FIXCAT), which is designated specifically for compliance data collection support:

`IBM.Function.Compliance.DataCollection`

Collection of compliance data that is on Linux on IBM Z requires the following software levels:

- ▶ Prerequisite operating system details:
 - RHEL 7.x or 8.x
 - SUSE Linux Enterprise Server on IBM Z 15.x
 - Ubuntu Server LTS 20.04 or later
- ▶ Middleware and software Evidence Providers:
 - RHEL 8.4 KVM (or later) or z/VM
 - Prerequisite operating system details:
 - Oracle Database 19c
 - PostgreSQL version 13.x or 14.x

3.6.4 z/OS middleware requirements

The following z/OS middleware products can participate in compliance data collection:

- ▶ CICS TS 6.1
- ▶ Db2 13 for z/OS
- ▶ IMS 15 with PTFs for APAR PH42600
- ▶ IBM MQ 9.2.0

Details about collecting compliance data from z/OS middleware products is provided in the documentation for each product:

- ▶ [CICS Transaction Server for z/OS Version 6.1: SMF 1154 subtype 80 record](#)
- ▶ [Db2 Version 13 for z/OS: Db2 for z/OS in IBM Documentations](#)
- ▶ [IMS Version 15: IMS in IBM Documentation](#)
- ▶ [IBM MQ Version 9.2: IBM MQ in IBM Documentation](#)

3.7 Deployment readiness

When deploying IBM Z Security and Compliance Center, you do not need to have all supported software levels in place at once. You can still derive value from any individual z/OS component or application that is at the required software level.

Also, not having the most current hardware and software levels does not imply that you cannot use IBM Z Security and Compliance Center, but more proof-points (goals) will surface as the environment becomes more inline with the latest hardware and software levels.

At the time of writing, IBM Z Security and Compliance Center contains more than 1170 goals covering validation-points across z/OS and Linux on IBM Z.

Further, the goals are included in one or more controls for each predefined profile, such as for PCI DSS. The controls can be used to build your own custom profile. (For a short description of profiles, controls, and goals, see 1.4, “Building blocks of regulatory frameworks” on page 9.)

Figure 3-11 shows how a profile uses controls, and groups some goals to accomplish compliance validation.

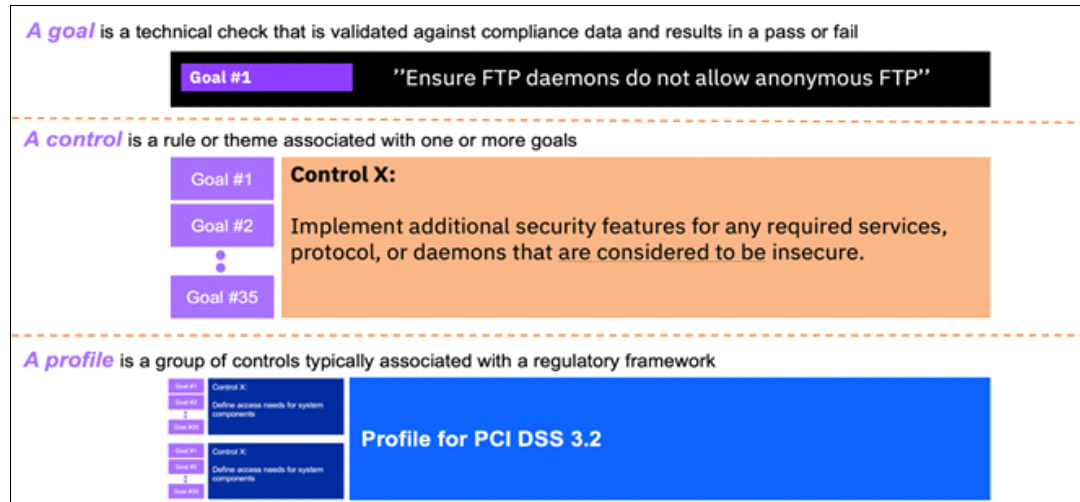


Figure 3-11 Understanding profiles, controls, and goals

Table 3-5 shows the number of goals that are applicable to each predefined profile with a clear distinction between z/OS components running on either IBM z15 or IBM z16. The additional CPACF goals with the IBM z16 and the goals for applications are listed separately.

Table 3-5 Number of z/OS related goals tabulated per profile

Breakdown of goals	IBM z15 or IBM z16	IBM z16 (CPACF)	CICS	Db2	IMS	IBM MQ	Total
Total number of goals (% of all goals)	392 (69%)	101 (18%)	16 (3%)	7 (1%)	36 (6%)	19 (3%)	571
PCI DSS goals (% of PCI DSS goals)	294 (62%)	101 (21%)	16 (3%)	7 (1.5%)	36 (8%)	19 (4.5%)	473
CIS goals (% of CIS goals)	347 (70%)	101 (20%)	15 (3%)	7 (1%)	28 (6%)	0 (0%)	498
NIST goals (% of NIST goals)	249 (62%)	101 (25%)	16 (4%)	5 (1%)	31 (8%)	0 (0%)	402

Table 3-6 illustrates an environment that includes an IBM z15 and z/OS V2R5. CICS and Db2 still need the required levels to enable the capturing of goals (proof-points) and writing of the SMF 1154 subtype records. IMS or IBM MQ are not used in this environment. The example shows an upgrade path to achieve elevated compliance for PCI DSS after upgrading software levels and migrating to an IBM z16.

Table 3-6 Example of increasing compliance coverage that is achieved by upgrading (with number of goals)

Upgrade path	Goals				Percentage of coverage
	Applicable		Not applicable		
z/OS V2R5 on IBM z15 (Current state)	z/OS	294	CPACF	101	294 z/OS goals / (473 total PCI DSS goals - 36 IMS goals - 19 IBM MQ goals) 294 / 418 = 70%
			Db2	7	
			CICS	16	
			IMS	36	
			IBM MQ	19	
After upgrading to Db2 V13, and still on IBM z15	z/OS	294	CPACF	101	(294 z/OS goals + 7 Db2 goals) / (473 total PCI DSS goals - 36 IMS goals - 19 IBM MQ goals) 301 / 418 = 72%
			Db2	7	
			IMS	36	
			IBM MQ	19	
After upgrading CICS to TS 6.1, and still on IBM z15	z/OS	294	IMS	36	(294 z/OS goals + 7 Db2 goals + 16 CICS goals) / (473 total PCI DSS goals - 36 IMS goals - 19 IBM MQ goals) 317 / 418 = 76%
			Db2	7	
	CICS	16	CPACF	101	
After migrating to an IBM z16	z/OS	294	IMS	36	(294 z/OS goals + 7 Db2 goals + 16 CICS + 101 CPACF goal) / (473 total PCI DSS goals - 36 IMS goals - 19 IBM MQ goals) 418 / 418 = 100%
			Db2	7	
	CICS	16			
	CPACF	101			



Exploring security and compliance use cases

In this chapter, we explore several use case scenarios in which IBM Z Security and Compliance Center can play a role in the journey toward continuous compliance. We describe how this solution can be used by the different security team members in your organization. We show how IBM Z Security and Compliance Center can be used to prepare for audits, validate system settings, and create reports for auditors to review.

This chapter covers the following topics:

- ▶ 4.1, “Use case 1: Using a predefined profile to prepare for an audit” on page 52
- ▶ 4.2, “Use case 2: Using a custom profile to prepare for an audit” on page 54
- ▶ 4.3, “Use case 3: Providing compliance evidence for an auditor” on page 57
- ▶ 4.4, “Use case 4: Reviewing compliance at a high level” on page 59
- ▶ 4.5, “Use case 5: Reviewing compliance on a recurring basis” on page 60
- ▶ 4.6, “Use case 6: Monitoring a specific component for compliance drift” on page 62

We walk you through the setup process for these use case scenarios by using IBM Z Security and Compliance Center in Chapter 5, “Validating security and compliance postures” on page 65.

4.1 Use case 1: Using a predefined profile to prepare for an audit

The Compliance Lead is preparing for a future audit of their IBM Z platform against the requirements for Payment Card Industry Data Security Standard (PCI DSS). IBM Z Security and Compliance Center supplies a predefined profile for PCI DSS (and other regulatory frameworks), which the Compliance Lead can use to prepare for this audit.

In this use case, IBM Z Security and Compliance Center is used to compare the SMF data it collects from the IBM Z platform to the controls that are specified in the PCI DSS standard. The resulting report can be used to search for non-compliance.

4.1.1 Problem statement

In the past, the PCI auditor asked for printouts of several z/OS settings for examination, such as:

- ▶ RACF **SETROPTS LIST** command output
- ▶ RACF DSMON report
- ▶ TCP/IP profile data set

The Compliance Lead does not know how the various z/OS settings map to the PCI DSS requirements or what settings the auditor is expecting to find. Sometimes, the auditor might provide a checklist or spreadsheet that lists their control objectives. Sometimes, the auditor might provide the checklist or spreadsheet before the audit.

As the Compliance Lead prepares for the audit, they review the PCI DSS guidelines. It is not easily understood how each one corresponds to specific z/OS controls. For example, PCI DSS Control 2.1 states:

“Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.”

The Compliance Lead is not sure what the auditor will look for to ensure compliance to this control.

4.1.2 Solving this challenge with IBM Z Security and Compliance Center

With IBM Z Security and Compliance Center, the Compliance Lead can use the predefined profile for PCI DSS to see which z/OS settings map to which PCI controls.

The steps for using a predefined profile to prepare for an audit are summarized in Figure 4-1 on page 53.

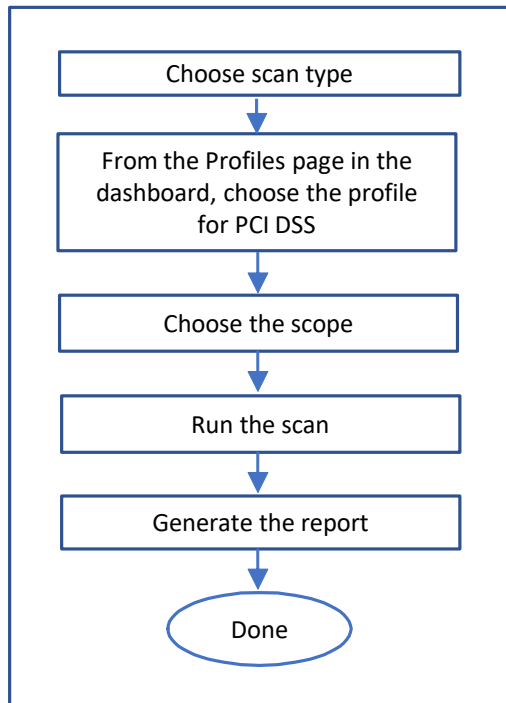


Figure 4-1 Using a predefined profile

The steps are as follows:

1. Choose scan type: Here, the Compliance Lead chooses to run a validation scan to read compliance data from the IBM Z platform.
2. Choose profile: From the IBM Z Security and Compliance Center dashboard, select the **Profiles** page to see the list of predefined profiles. In this use case, the Compliance Lead selects the predefined profile for PCI DSS. Based on this profile, IBM Z Security and Compliance Center compares the SMF data that it collects from the IBM Z platform to the controls that are included in the PCI DSS standard.
3. Choose scope: The scope determines which z/OS systems are included in the scan.
4. Run the scan: The Compliance Lead can iteratively run the scan, view its results in the dashboard, and perform remediation of non-compliance. The dashboard and reports can be examined for non-compliant settings.
5. Generate the report: The Compliance Lead produces a physical report that shows the current compliance posture. The Compliance Lead can distribute this report to stakeholders, such as the Chief Information Security Officer (CISO) or application owners. These parties can review the report and provide feedback on system compliance.

The detailed steps for performing this activity are shown in 5.2, “Using a predefined profile to prepare for an audit” on page 72.

In the dashboard, you can examine the predefined profile for PCI DSS. You can expand each control to see what goals are associated with it. For example, if you expand PCI DSS control 2.1, you can see several goals that are listed, including one that says, “4083007: Check that RACF default system user ID (IBMUUSER) has been revoked”. This is an example of how a control is mapped to a specific z/OS capability.

Note: The example that is used in this use case is a PCI audit. However, the use case can be applied similarly to prepare for a National Institute of Standards and Technology (NIST) or Center for Internet Security (CIS) audit.

4.1.3 Looking forward

As the Compliance Lead becomes more familiar with IBM Z Security and Compliance Center, preparing for an audit becomes much easier. The dashboard provides most of the information that an auditor must see, either displayed on the dashboard itself or in generated reports. We look more closely at the reports later.

4.2 Use case 2: Using a custom profile to prepare for an audit

In addition to the predefined profiles that are supplied with IBM Z Security and Compliance Center for PCI DSS, NIST, and CIS controls, there is an option to create your own custom profiles. With a custom profile, you define the list of controls that you would like to validate against.

You might use a custom profile to do the following tasks:

- ▶ Accommodate other types of audits, such as an internal, in-house audit.
- ▶ Supplement or replace any manual procedures, checklists, and programs that you use for compliance checking.
- ▶ Import a combination of controls and goals from the predefined profiles.

You can build a custom profile from an existing predefined profile, or you can create one from scratch. Usually, you might find it easier to start by choosing among the 571 existing goals in IBM Z Security and Compliance Center to create a custom profile that meets the needs of your organization.

Let us explore this extended capability of IBM Z Security and Compliance Center.

4.2.1 Problem statement

The Compliance Lead is asked by the CISO¹ to help the organization prepare for an upcoming security audit of its systems.

This audit is internal. It is intended to validate the systems for compliance against the organization's set of security standards. The internal audit is not specifically against PCI, NIST, or CIS controls.

The company has checklists and proprietary programs that it used for previous audits. The Compliance Lead hopes to prove compliance with the CISO by using the organization's own proprietary checklists and programs.

The organization uses a mix of both distributed systems and IBM Z platforms. The distributed side of the business has a familiar set of guidelines that the Compliance Lead can use to quickly check settings in a straight-forward manner. The CISO likes this outcome.

¹ For a description of roles and responsibilities, see Table 3-2 on page 39.

However, the IBM Z side of things is less certain. The Compliance Lead does not know how z/OS capabilities map to the checklists. For the internal audit, the Compliance Lead must somehow determine how to correlate those same internal guidelines to z/OS security controls.

4.2.2 Solving this challenge with IBM Z Security and Compliance Center

With IBM Z Security and Compliance Center, you can create your own profiles. When you build a custom profile, you can choose a combination of controls and goals to validate. You can create a profile by using a predefined profile as a base, or you can create a profile from scratch by selecting from a list of available goals that you want to meet.

With IBM Z Security and Compliance Center, the Compliance Lead's effort shifts to creating a custom profile based on controls that are available to pick and choose from IBM Z Security and Compliance Center.

In this sense, IBM Z Security and Compliance Center provides the Compliance Lead with a “library” of 571 goals. The work now lies in understanding those goals and determining which to include in the custom profile to be used for the internal audit.

The steps for creating and using a custom profile are summarized in Figure 4-2.

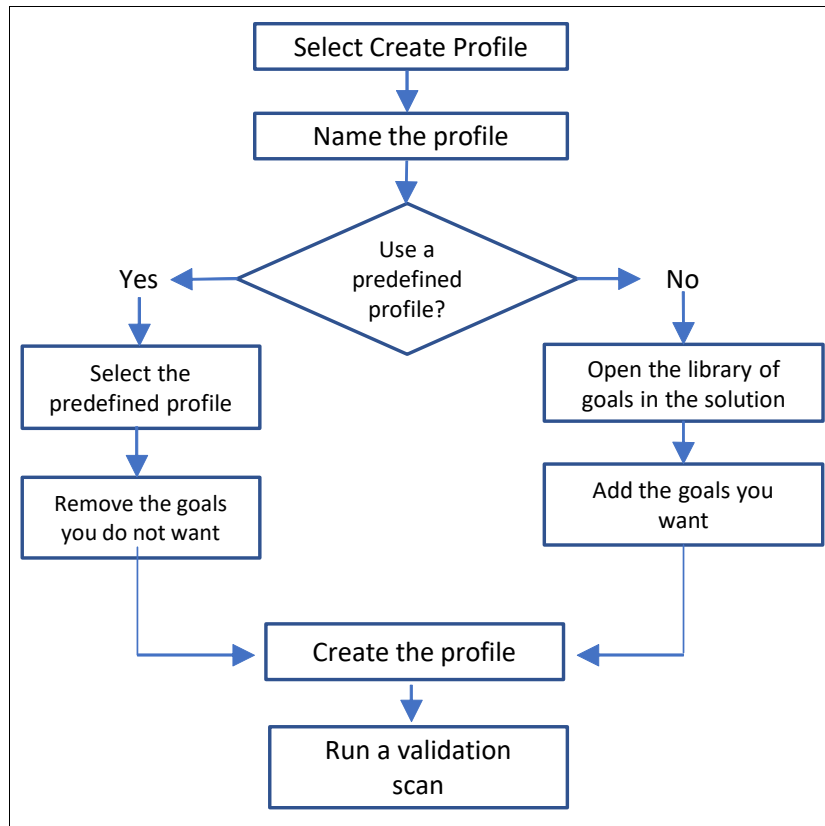


Figure 4-2 Custom profile process

The steps are as follows:

1. From the dashboard, select **Configure** → **Profiles** → **Create**.
2. Name your profile and add a description.

3. Choose between using a predefined profile as a base or building one from scratch. Select **Yes** for using the predefined profile, or **No** for building from scratch.
4. Review the controls and goals for the selected profile. Expand each control to see the goals that it verifies. Use the table search to narrow the results to specific items, such as all goals that mention RACF in the title or description. For more information about goals, see the Goals page.
5. Select the corresponding box for the goals that you want to include.
6. Create the profile.
7. Run a validation scan.

The detailed steps for performing this activity are shown in 5.3, “Using a custom profile to prepare for an audit” on page 79.”

Note: When you run a validation scan, the compliance data is collected from each system that is defined in the scope. Instead of running a validation scan for each custom profile that you create (or change), you can collect data from the systems in a scope once, and then run a fact validation scan for any profile. For example, if you change a custom profile, there is no need to collect data from the z/OS systems again to run the new custom profile. Instead, you can run a fact validation scan on existing data from a previous validation scan. Do this from the dashboard on the Scopes page, as shown in 5.1.1, “Defining a scope” on page 66.

4.2.3 Looking forward

As the Compliance Lead becomes more familiar with the IBM Z Security and Compliance Center library of goals, they can become more proactive, continually refine the custom profiles, and even anticipate new compliance regulations.

Also, a decision to comply with other regulatory frameworks for which predefined profiles are not available can be made, such as the General Data Protection Regulation (GDPR) for European clients, and Sarbanes-Oxley (SOX) for US-based clients. The Compliance Lead can use the 571 goals that are supplied with IBM Z Security and Compliance Center to design custom profiles that map controls of IBM Z platforms to the requirements of those regulations.

4.3 Use case 3: Providing compliance evidence for an auditor

The Compliance Lead is asked by the CISO to help the organization prepare for an upcoming audit of its systems. This audit is an external audit. The auditor will evaluate how well the organization's systems perform according to PCI DSS requirements. The organization uses a mix of both distributed systems and IBM Z platforms.

The auditor has little or no knowledge about the IBM Z platform, and therefore does not know how z/OS capabilities map to the PCI DSS requirements. To help cope with this aspect of the audit, the auditor has a checklist of recommended z/OS settings that they typically rely on.

4.3.1 Problem statement

The auditor must gather information from the z/OS environment to complete the various aspects of the PCI DSS audit. When they look at the detailed requirements for PCI DSS, they want to check various items:

- ▶ What network security controls are in place?
- ▶ What policies and procedures are in place, and are they up to date?
- ▶ Are system components configured and secured?
- ▶ What cryptography is in place?
- ▶ How is stored account data protected?

For z/OS, an auditor usually asks for RACF information to start. They ask for the output of the RACF **SETROPTS LIST** command and the DSMON report. This information is IBM Z specific and contains the options that are set in RACF. Some items that are checked in the **SETROPTS LIST** output include SAUDIT, OPERAUDIT, PROTECTALL FAIL, and password settings. In the DSMON report, the auditor looks for items such as the following ones:

- ▶ How many people have the RACF **SPECIAL** attribute?
- ▶ How many users are revoked?
- ▶ Are changes to RACF resources being audited?
- ▶ Are system-critical data sets protected?

All this information uses IBM Z terminology, and auditors might need assistance to interpret the information.

4.3.2 Solving this challenge with IBM Z Security and Compliance Center

With IBM Z Security and Compliance Center, an auditor can easily check specific z/OS specific security settings and how they map to a regulatory framework, such as PCI DSS. The auditor does not need to understand the mainframe terminology.

For example, IBM Z Security and Compliance Center gathers information on cryptography algorithms and displays whether the algorithms comply with a specific standard. The dashboard lists the PCI DSS requirements and shows the level of compliance for each.

In a generated report, the auditor can verify the date and timestamps for the report to ensure that no one modified the report, which is known as ensuring that the “chain of evidence” is valid and complete.

Also, the auditor can compare the current report with historical data to see whether there are any changes from previous reports. This information is available on the dashboard chart that is titled “Drift over time”.

The steps for creating an audit report are summarized in Figure 4-3.

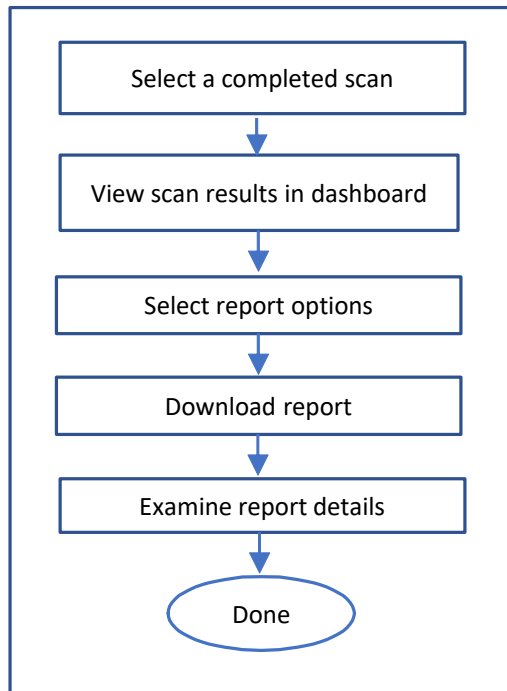


Figure 4-3 Audit report process

The steps are as follows:

1. From the dashboard, select the scan to be used for the audit (select **Assess** → **Scans**). In this case, choose a completed PCI DSS scan.
2. Review the scan results and verify that the correct scan is selected.
3. For report options, select the level of detail that is required for the audit, such as **Detailed**. Also, choose the download format (**PDF**).
4. Download the report in a portable format (PDF) for printing or distribution through email.

Note: The example that is used in this use case is a PCI DSS audit. However, this use case can be applied similarly to prepare for a NIST or CIS audit.

The detailed steps for performing this activity are shown in 5.4, “Providing compliance evidence for an auditor” on page 88.

4.3.3 Looking forward

As auditors become more familiar with IBM Z Security and Compliance Center, they see how the scan reports clearly show compliant and non-compliant items for each system. They will not need to spend as much time understanding IBM Z terminology.

4.4 Use case 4: Reviewing compliance at a high level

Various executives (“CxOs”) (such as the CISO or CSO) and even business owners must see reports to ensure that their respective areas comply with the regulations of their industry. Normally, they are looking at detailed line-item reports from IBM Z platforms. These reports use IBM Z terminology. The CISO (or Compliance Lead, Risk Officer, Line of Business owner, or Privacy Officer) wants to see a high-level status for compliance.

4.4.1 Problem statement

CxOs are busy people and need to quickly ensure that regulatory requirements are met. CxOs want an easy-to-read-and-understand report that shows their compliance posture within their respective industries. Graphical reports make it even easier to understand and determine where they stand against their regulatory requirements.

4.4.2 Solving this challenge with IBM Z Security and Compliance Center

IBM Z Security and Compliance Center can generate compliance reports in various levels of detail, from a high level to a detailed level, depending on the stakeholder:

- ▶ An executive summary report, which shows the date that the report was generated; the type of report (for example, PCI DSS); the number of items checked; whether the checks passed or failed; and the severity level of the checks (critical, high, medium, or low).
- ▶ A report that shows the validation summary by control. This report breaks down the control and shows the overall status, severity, and what checks passed or failed.
- ▶ A detailed report that takes the information from the validation summary by control report and provides the specific details of the items that are tested.

The CxO might need the executive summary report, and the next level of management might request the validation summary by control report. The people who need to address failed checks need the detailed report.

The steps for reviewing compliance at a high level are summarized in Figure 4-4.

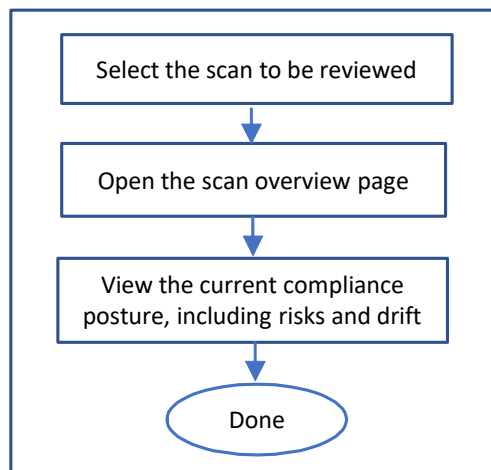


Figure 4-4 Reviewing compliance at a high level

The steps are as follows:

1. From the dashboard, select the scan to be reviewed.
2. From the Scan Overview page, you can see at a glance the status of your current compliance posture.
3. Review the details to see which items failed in the scan and whether your compliance posture is improving or degrading (or “drifting”) over time.

You might prefer to re-run a scan for a period, or download a copy of the high-level report. The detailed steps for performing this activity are shown in 5.5, “Reviewing compliance at a high level” on page 93.

4.4.3 Looking forward

Various reports for different stakeholders are easy to produce whenever a scan is performed. The reports can be tailored to the level that each stakeholder needs. The CISO and CSO can review the graphical and numerical representation of the compliance status at a high level. They will become familiar with the reports that are produced by the solution and quickly view the compliance status of their IBM Z platforms.

4.5 Use case 5: Reviewing compliance on a recurring basis

Compliance is an ongoing process. After the Compliance Lead runs scans and is satisfied with the compliance posture, they should review the compliance posture regularly to identify any gaps that appeared.

4.5.1 Problem statement

Rather than waiting for an audit, the Compliance Lead plans to check the compliance of their z/OS systems regularly. One reason is that it is easier and preferable to handle any non-compliant items when they appear, instead of before an audit. The Compliance Lead does not want to waste time manually collecting data and comparing reports.

4.5.2 Solving this challenge with IBM Z Security and Compliance Center

With IBM Z Security and Compliance Center, the Compliance Lead can use the compliance dashboard to run scans automatically regularly and monitor compliance changes over time.

First, the Compliance Lead must set up a recurring scan. They set up a new scan by choosing the profile and scope, and then specify how often to run the scan. For example, they can choose to run the scan once every month or twice a week.

After the recurring scan runs more than once, the dashboard displays a graphical chart titled “Drift over time”. It shows the number of goals that passed and failed for each scan, along with the date of each scan. When the Compliance Lead sees the number of failures increase from an earlier scan, they can investigate further by reviewing the details of the latest scan. By reviewing the “Drift over time” chart, they can monitor when the compliance status changes for the systems.

You do not need to collect facts from the z/OS systems in your scope every time you use a custom profile. If you have a custom profile for the RACF administrator and another custom profile for the Db2 administrator, you can run one fact collection scan and then two fact validation scans. You can run a fact validation scan on any existing fact collection scan or validation scan. For more information about doing this task with custom profiles, see step 1 on page 84.

The steps for reviewing compliance regularly are shown in Figure 4-5.

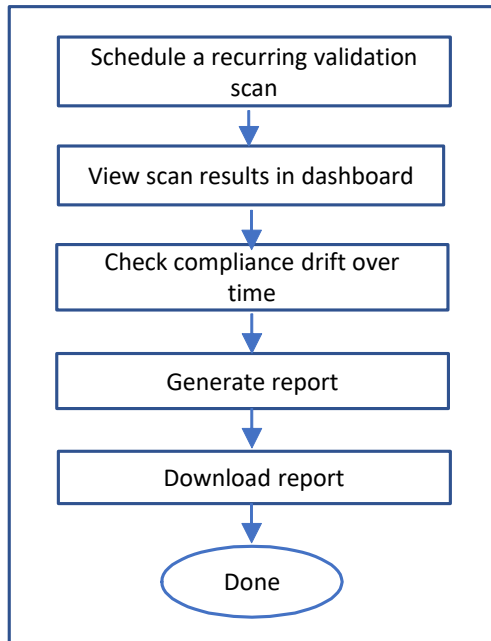


Figure 4-5 Reviewing compliance regularly

The steps are as follows:

1. From the dashboard, create a scan in the Scans page.
2. Request an automated scan and indicate how often the scan should be repeated.
3. After the scan runs a number of times, check the scan results page. Select the view for “Compliance drift over time”.
4. Create the report by clicking **Generate Report** and select **Delta report** to compare two points in time.
5. Optionally, download a copy of the report.

The detailed steps for performing this activity are shown in 5.6, “Reviewing compliance regularly” on page 98.

4.5.3 Looking forward

The Compliance Lead will spend much less time collecting data and reports to prove compliance. The solution runs recurring scans, and the Compliance Lead reviews the dashboard and the “Drift over time” page regularly.

Continuous compliance becomes much easier to manage.

4.6 Use case 6: Monitoring a specific component for compliance drift

The Compliance Lead might be especially interested in compliance drift for specific z/OS components. Ideally, the Compliance Lead can monitor z/OS components for compliance drift over any specified period.

4.6.1 Problem statement

In earlier audits, the auditor focused on particular z/OS components, such as Security Server (RACF). In these cases, the Compliance Lead relied on other z/OS component experts to gather the data, such as a RACF administrator or network administrator. Each administrator might have checklists that they follow or manual ways in which they collect data to show an auditor.

This work can be time-intensive. Having a way to scrutinize a particular component for compliance drift is helpful.

4.6.2 Solving this challenge with IBM Z Security and Compliance Center

Using the IBM Z Security and Compliance Center dashboard, you have all the compliance data in one place. There are more than 571 goals in IBM Z Security and Compliance Center, so it is difficult for a Compliance Lead to understand all of them. You need help from other security administrators, such as network and RACF administrators to review the compliance data, and that is possible by using custom profiles.

As described in 4.2, “Use case 2: Using a custom profile to prepare for an audit” on page 54, you can use the IBM Z Security and Compliance Center dashboard to create custom profiles, which group the goals that are related to one or more components. For example, you can create one custom profile containing all goals that are related to RACF and one custom profile containing all goals that are related to Db2. You can run scans with these custom profiles, create reports from the scans, and then distribute the reports to the respective administrators to handle. You also can show each administrator the “Drift over time” chart on the dashboard to help them visualize how the component's compliance posture changed over time.

Instead of distributing reports to other security administrators, each administrator can be granted access to the IBM Z Security and Compliance Center dashboard. Then, they can run the custom scans that were set up for them or schedule recurring scans. With access to the dashboard, they can monitor drift and perform remediation when non-compliant settings are discovered.

The steps for monitoring compliance drift are shown in Figure 4-6 on page 63.

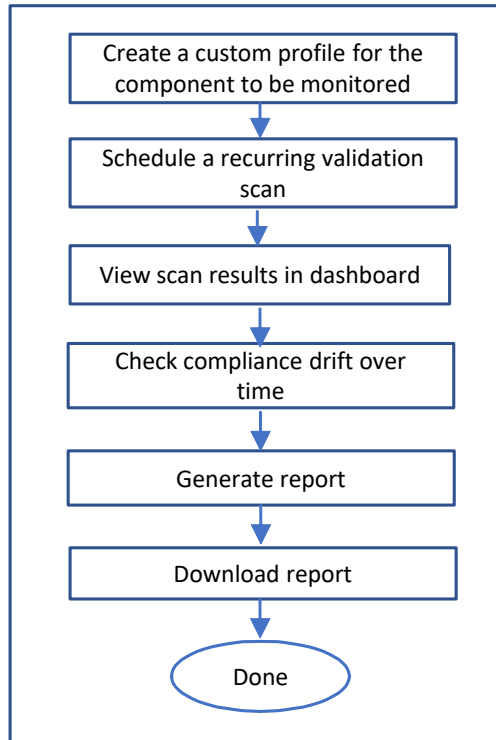


Figure 4-6 Monitoring for compliance drift

The steps are as follows:

1. From the dashboard, select a custom profile for the component to be monitored. The steps are the same as for 4.2, “Use case 2: Using a custom profile to prepare for an audit” on page 54, but select only the goals that are related to the component.
2. You can expand each control to see the goals that it verifies. Use the table search to narrow the results to specific items, such as all goals that mention RACF in the title or description. More details for each goal can be found on the Goals page. Select the corresponding box for the goals that you want to include.
3. Create the profile.
4. Request an automated scan and indicate how often the scan should be repeated.
5. After the scan is run a number of times, check the scan results page. Select the view for “Compliance drift over time”.
6. Create the report by clicking **Generate Report** and select “Delta report” to compare two points in time.
7. Optionally, download a copy of the report.

The detailed steps for performing this activity are shown in 5.7, “Monitoring a specific component for compliance drift” on page 100.

4.6.3 Looking forward

As administrators become more familiar with the solution dashboard and the reports that are produced by IBM Z Security and Compliance Center, they spend less time collecting and reviewing compliance data. To focus on specific areas, they can review the custom profiles that show only the controls for their respective components.



Validating security and compliance postures

The intent of this chapter is to provide clarity around how IBM Z Security and Compliance Center GUI can function in everyday use. The chapter also helps ground the concepts that have been described so far by demonstrating how the use case scenarios that are described in Chapter 4, “Exploring security and compliance use cases” on page 51 can be deployed.

Before using IBM Z Security and Compliance Center to monitor and validate your security and compliance postures, plan the *scopes*, *profiles*, and *goals* that will be used, and who has access to the validation reports. Although these attributes can be modified at any time, you should develop a consensus around them with your team before starting the scan and report processes.

The scenarios that are described in this chapter assume the following setup activities were completed:

- ▶ IBM Z Security and Compliance Center was installed, including all dependent products.
- ▶ Credentials were created for each person who uses IBM Z Security and Compliance Center.
- ▶ Connections were created for each z/OS system from which compliance data will be collected.
- ▶ Credentials to access the systems in scope were entered and mapped.

For more information about setup, installation, configuration, deployment, and usage of IBM Z Security and Compliance Center, see *IBM Z Security and Compliance Center Guide*, SC31-5705.

This chapter covers the following topics:

- ▶ 5.1, “Preparing IBM Z Security and Compliance Center” on page 66
- ▶ 5.2, “Using a predefined profile to prepare for an audit” on page 72
- ▶ 5.3, “Using a custom profile to prepare for an audit” on page 79
- ▶ 5.4, “Providing compliance evidence for an auditor” on page 88
- ▶ 5.5, “Reviewing compliance at a high level” on page 93

- ▶ 5.6, “Reviewing compliance regularly” on page 98
- ▶ 5.7, “Monitoring a specific component for compliance drift” on page 100

5.1 Preparing IBM Z Security and Compliance Center

This section provides the necessary steps to prepare IBM Z Security and Compliance Center for use. It describes how to set up a scope. Customization of goals and profiles are described in the following sections of this chapter.

Begin by opening a web browser to the login page for the IBM Z Security and Compliance Center. For example:

```
http://scc-ui-ibmz-scc.apps.<cluster-name>.<cluster-base-domain>1
```

When the main page of IBM Z Security and Compliance Center opens, enter a username and password, and then click **Login** (see Figure 5-1).

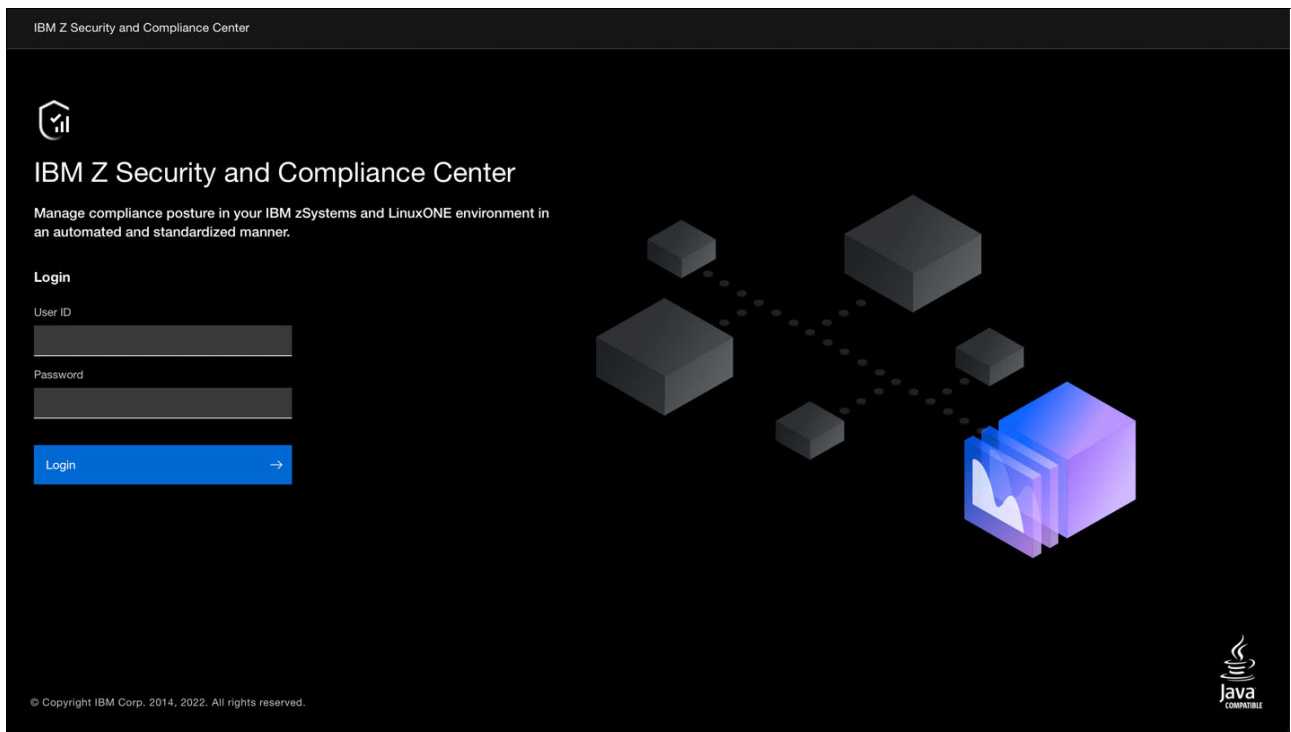


Figure 5-1 Login window

5.1.1 Defining a scope

After you log in, start by defining a scope. A *scope* is a set of systems from which compliance data (evidence) is collected when a scan runs. You can create as many scopes as needed. It might be useful to create scopes that pertain to different parts of your environment. For example, you can create a scope that contains every system that processes sensitive customer data, or a scope that contains every system that comprises a development sandbox environment. Different scopes might contain the same systems.

¹ For the cluster name and cluster base domain values, check with your network or system administrator.

Rarely, an entire IBM Z environment is in scope for an audit. Therefore, it might be reasonable to select only those systems that will be audited.

To create a scope, complete the following steps:

1. Under the **Configure** menu, click **Scopes**, and then click **Create** (see Figure 5-2).

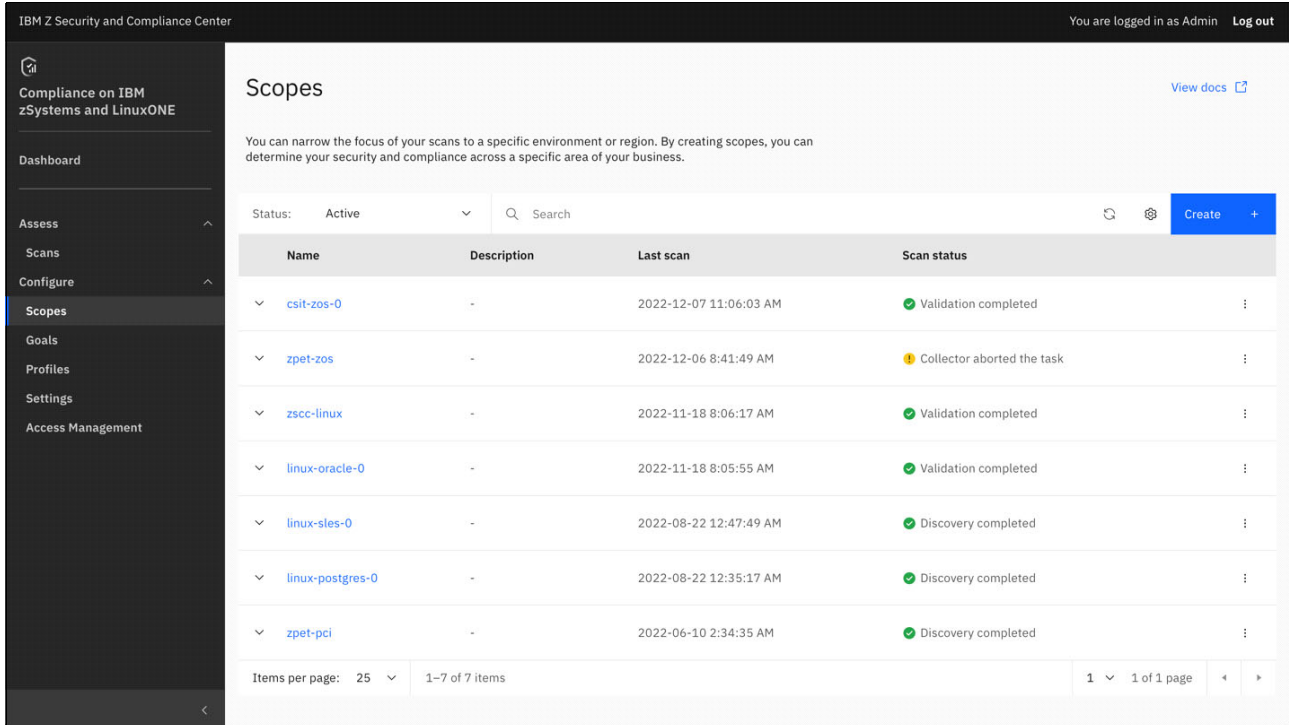


Figure 5-2 Creating a scope

2. Enter a name and a description for the scope into the Create a scope window fields (see Figure 5-3), then click **Next**.

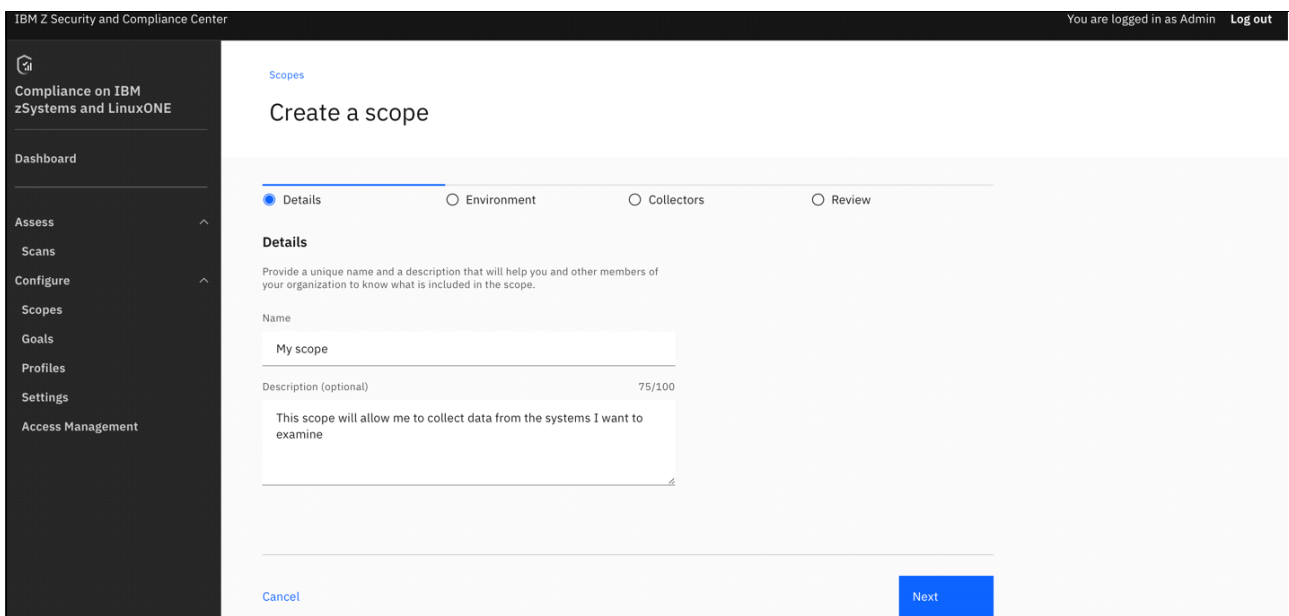


Figure 5-3 Create a scope window (1 of 2)

3. Specify the type of environment for the scope (see Figure 5-4). You can choose between **z/OS** and **Linux on IBM Z** (For our example, we selected **z/OS**).

You can select the IBM z/OS Management Facility (IBM z/OSMF) instances for the scope. In our case, we chose two IBM z/OSMF instances for two sysplexes. You can select as many sysplexes as necessary. Each sysplex must have an IBM z/OSMF server running on one of its systems, and it must be associated with that server).

For z/OS scopes, you may enable or disable “Auto-discovery scan.” Enabling it automatically and periodically finds new resources (systems) in scope, based on the IBM z/OSMF instances selected. We enable auto-discovery to scan for new resources weekly.

Click **Next**.

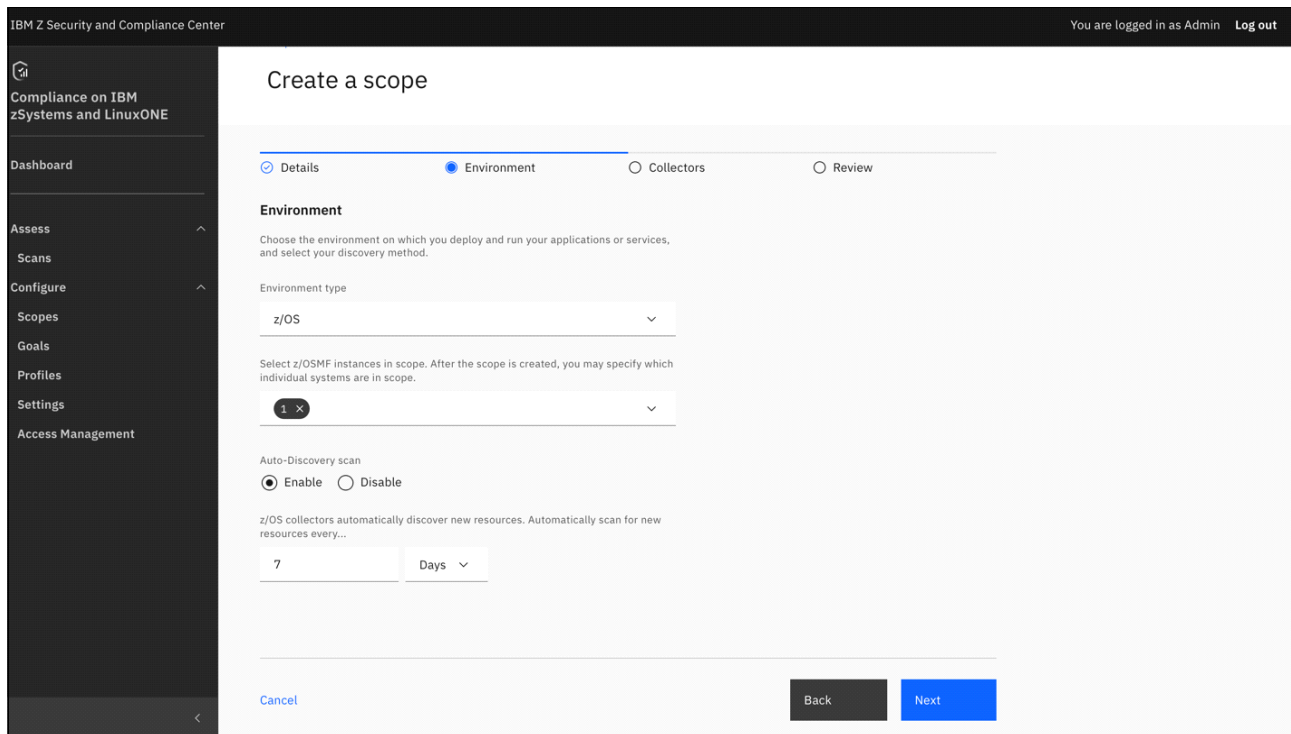


Figure 5-4 Create a scope (2 of 2)

4. On the next page, select the collector to use. Usually, there is only one collector to choose.
5. Review and confirm the details of the scope, and then click **Create** to create the scope.

After the scope is created, credentials for each IBM z/OSMF connection in the scope must be added (see Figure 5-5 on page 69). Credentials are the authority that is required to access a system resource, such as the username and password or certificates. Credentials are added in the settings page for each scope where credentials are required.

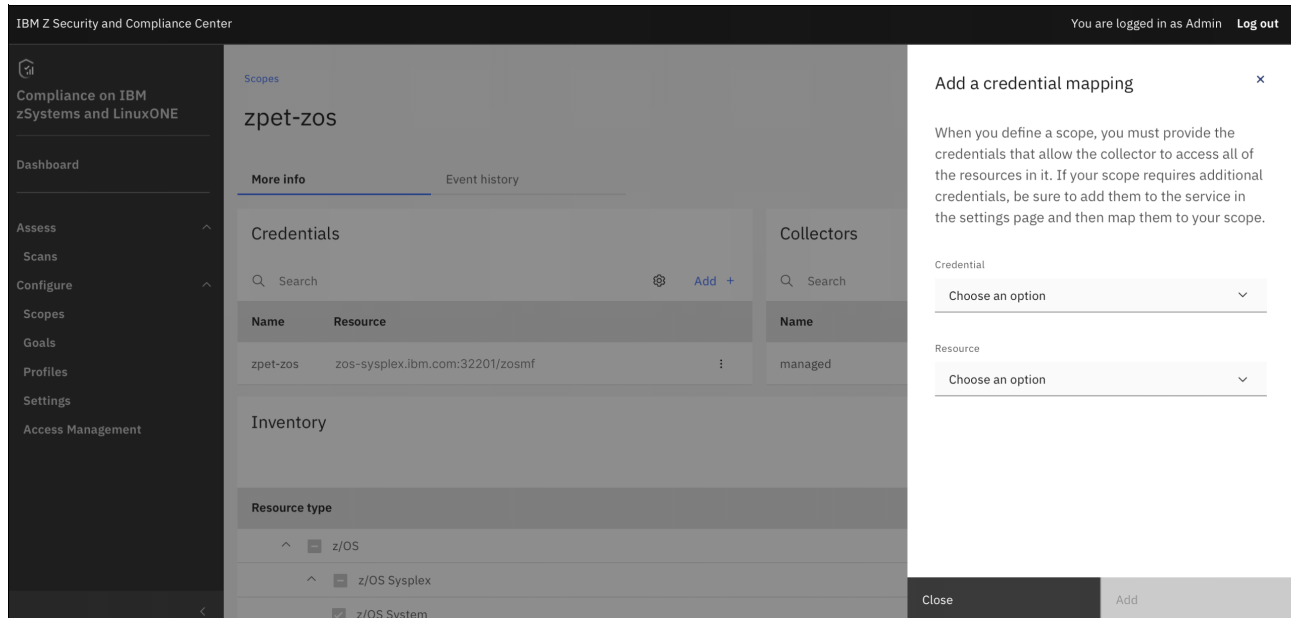


Figure 5-5 Adding credentials

To add credentials, complete the following steps:

1. Go to the Settings page and click the **Credentials** tab.
You see a table with all the saved credentials. You can use the same credentials across multiple systems and scopes.
2. Click **Add** at the right of the table header.
3. Enter a name, description, the credential type, and required fields. Click **Create** to save the credential.
4. When you save the credentials that you intend to use in the scope, go to the Scopes page and select your scope.

5. In the Credentials tile, click **Add** at the table header (see Figure 5-6).

A side pane opens. Specify which credential that you want to add to the scope, and which resource it maps to.

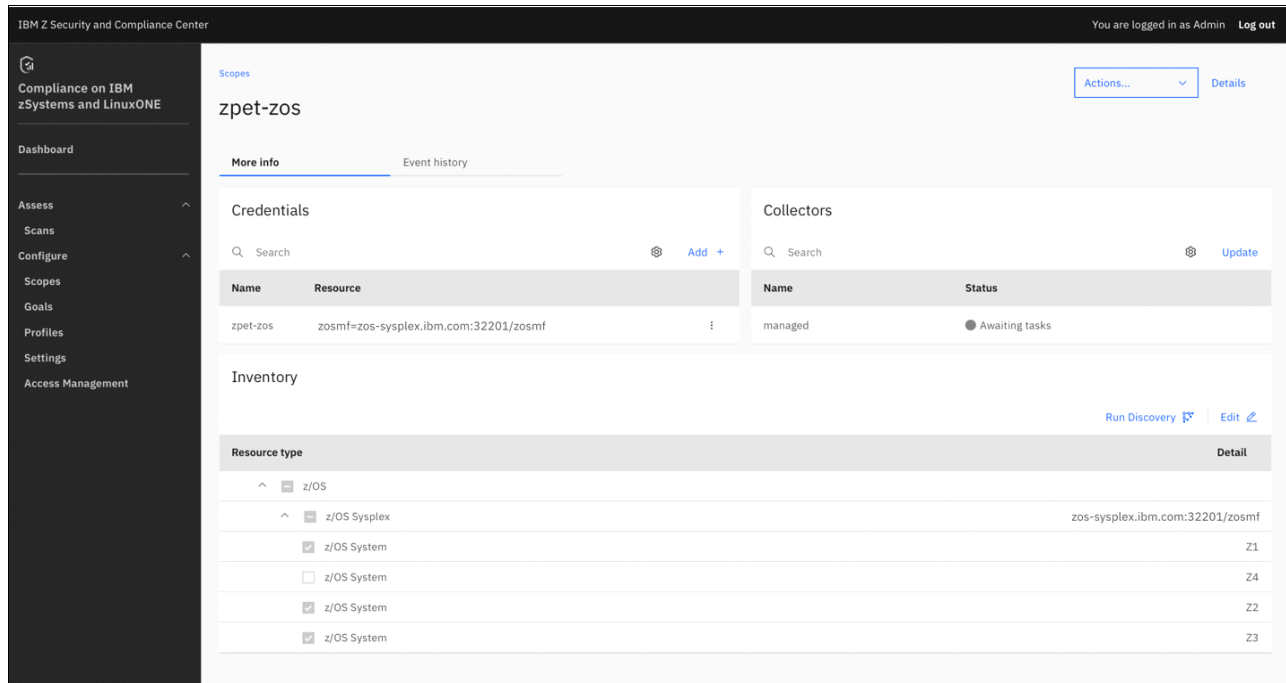


Figure 5-6 Selecting resources for credentials

If you scroll down, you can see the inventory, where you get a full list of every system in scope in a topographical view.

Select the systems that are in or out of scope by selecting the checkboxes on the left of each row. You can specify what is in or out of scope at the system or logical partition (LPAR) level of granularity.

If a discovery scan is completed, any newly discovered systems are not automatically added to the scope. Instead, they appear in the Scope “Inventory.” Resources in the inventory may be assigned to this scope by selecting the checkbox next to it in the Inventory table.

5.1.2 Optional: modifying goal parameters

Every predefined goal in IBM Z Security and Compliance Center has its own set of parameters, that is, values that it checks against, relative to the goal, which is based on the SMF 1154 records. However, you might need to modify certain predefined goals based on different security criteria, such as ensuring that passwords are a certain length in characters and numerical values (minimum password length).

Important: Be careful when modifying the predefined goal parameters. As a best practice, change them to reflect a more *stringent* set of standards.

You can modify the predefined goal parameters through the GUI by completing the following steps:

1. Select **Setting**, and then click the **Goal parameters** tab to open a list of different profiles (see Figure 5-7).

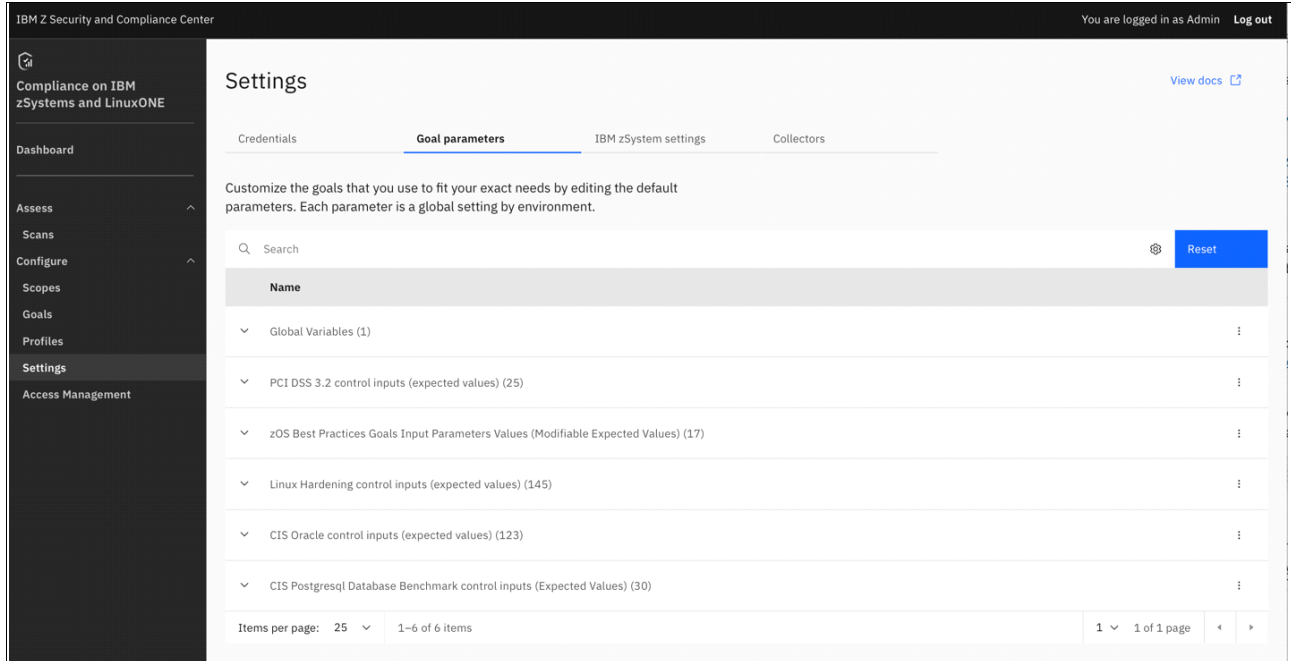


Figure 5-7 Selecting goal parameters

2. Click the overflow menu (the three dots) at the right edge of the table row of the profile to view the goal parameters. A window (see Figure 5-8) opens that shows the parameters that can be modified.

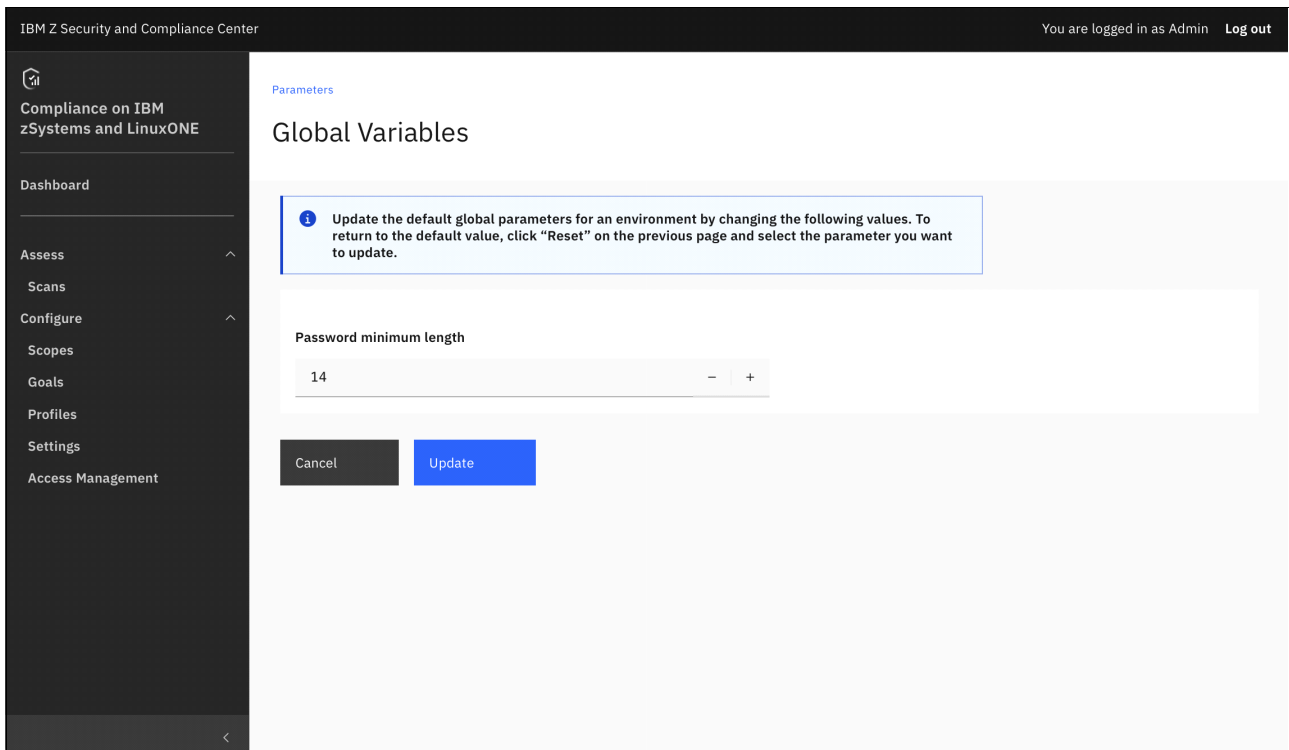


Figure 5-8 Changing the default global parameter values

3. Use the text and number input fields to modify the parameters, and then click **Update** to save them.

Important: Although the parameters are shown in a profile-specific manner, the changes to the parameters are global, which means that if you modify the goal parameter value, the new value is used every time that goal is used in a validation, regardless of the profile that is used.

5.2 Using a predefined profile to prepare for an audit

There is definite value in using the predefined profiles for Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST), and Center for Internet Security (CIS) that come with IBM Z Security and Compliance Center because those profiles are defined by IBM security experts that fully understand the capabilities of the IBM Z platform and the regulatory requirements. These profiles lend credibility to the compliance reports that are generated by IBM Z Security and Compliance Center in the eyes of auditors.

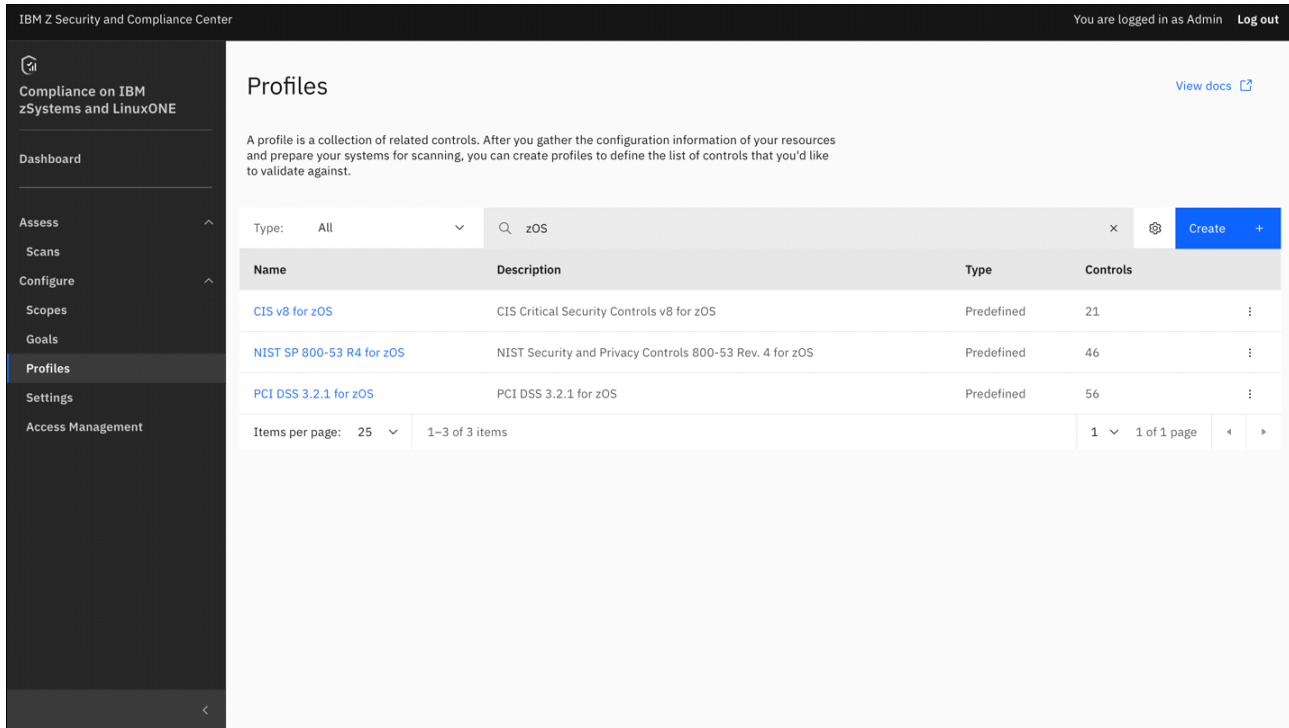
Consider preparing for an upcoming audit for PCI DSS, as described in 4.1, “Use case 1: Using a predefined profile to prepare for an audit” on page 52.

5.2.1 Viewing existing profiles

Before you start a scan, you must determine which profile that you want to use. To do so, complete the following steps:

1. Under the **Configure** menu, select **Profiles**, and then click the **z/OS** tab (see Figure 5-9).

In the Profiles window, a full list of every profile that the IBM Z Security and Compliance Center has access to is displayed. Many of these profiles include one-to-one mappings of regulatory requirements to IBM Z controls. They are known as *predefined profiles*. Predefined profiles exist for PCI DSS, NIST SP 800-53, and CIS.



The screenshot displays the 'Profiles' page in the IBM Z Security and Compliance Center. The page title is 'Profiles' and it includes a 'View docs' link. A descriptive text explains that a profile is a collection of related controls. Below this is a search bar with 'zOS' entered and a 'Create' button. A table lists three predefined profiles:

Name	Description	Type	Controls
CIS v8 for zOS	CIS Critical Security Controls v8 for zOS	Predefined	21
NIST SP 800-53 R4 for zOS	NIST Security and Privacy Controls 800-53 Rev. 4 for zOS	Predefined	46
PCI DSS 3.2.1 for zOS	PCI DSS 3.2.1 for zOS	Predefined	56

At the bottom of the table, there are pagination controls: 'Items per page: 25', '1-3 of 3 items', and '1 of 1 page'.

Figure 5-9 Viewing a predefined profile

2. Click the relevant profile. For our environment, we chose PCI DSS 3.2.1 for z/OS (see Figure 5-10).

Here, you can see every goal (technical check) that is used to evaluate whether your environment is compliant with the regulation or profile. Clicking each goal shows more information about that goal.

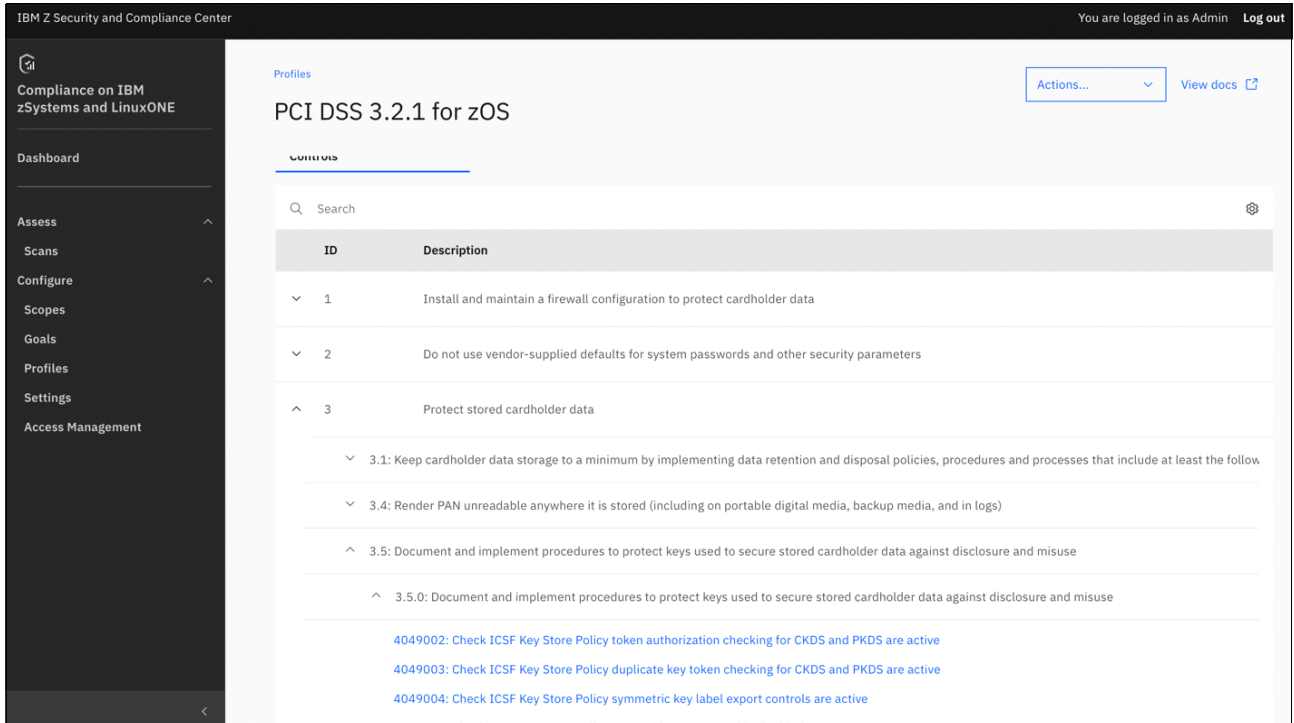


Figure 5-10 Predefined profile details

5.2.2 Starting a new scan

With a scope created (as described in 5.1.1, “Defining a scope” on page 66) and a profile selected, start a new scan by completing the following steps:

1. Select **Scans**, click the **Scans** tab, and then click **New Scan** to start the process (see Figure 5-11 on page 75).

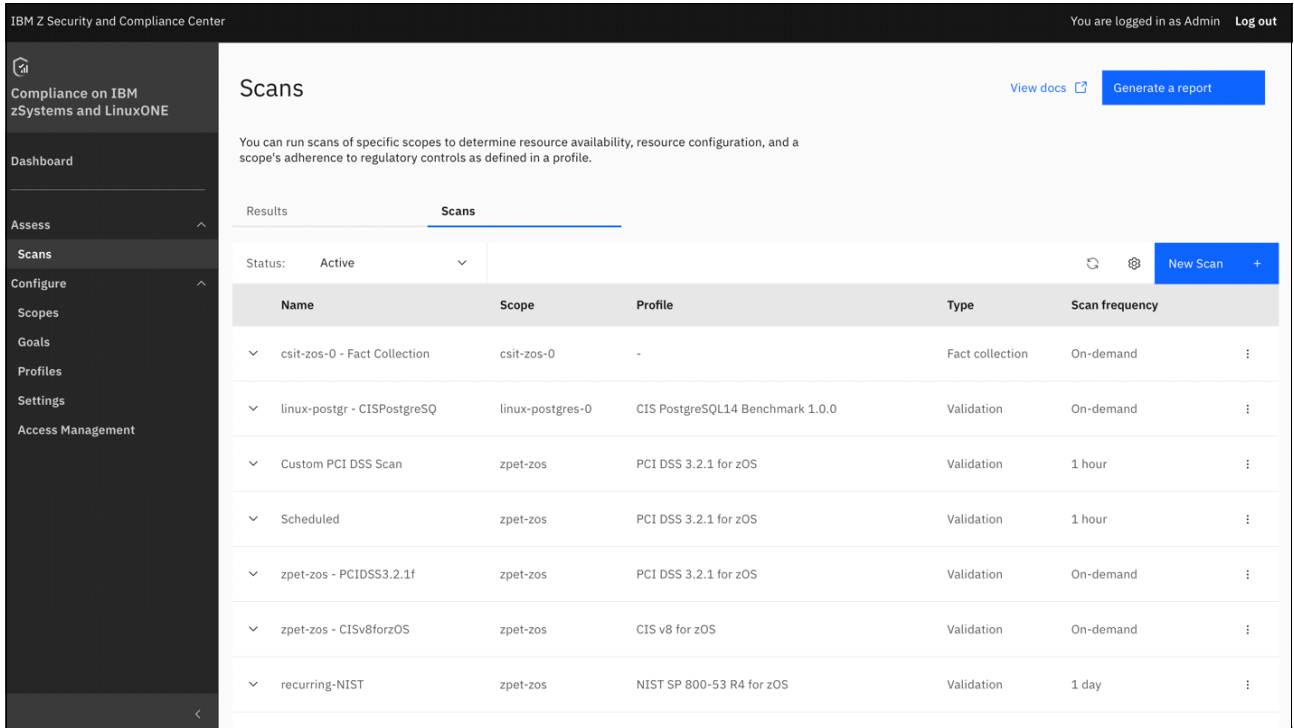


Figure 5-11 Starting a new scan

A side pane opens, where you enter basic information about the new scan, including a name, description, scan type, scope, and profile (see Figure 5-12).

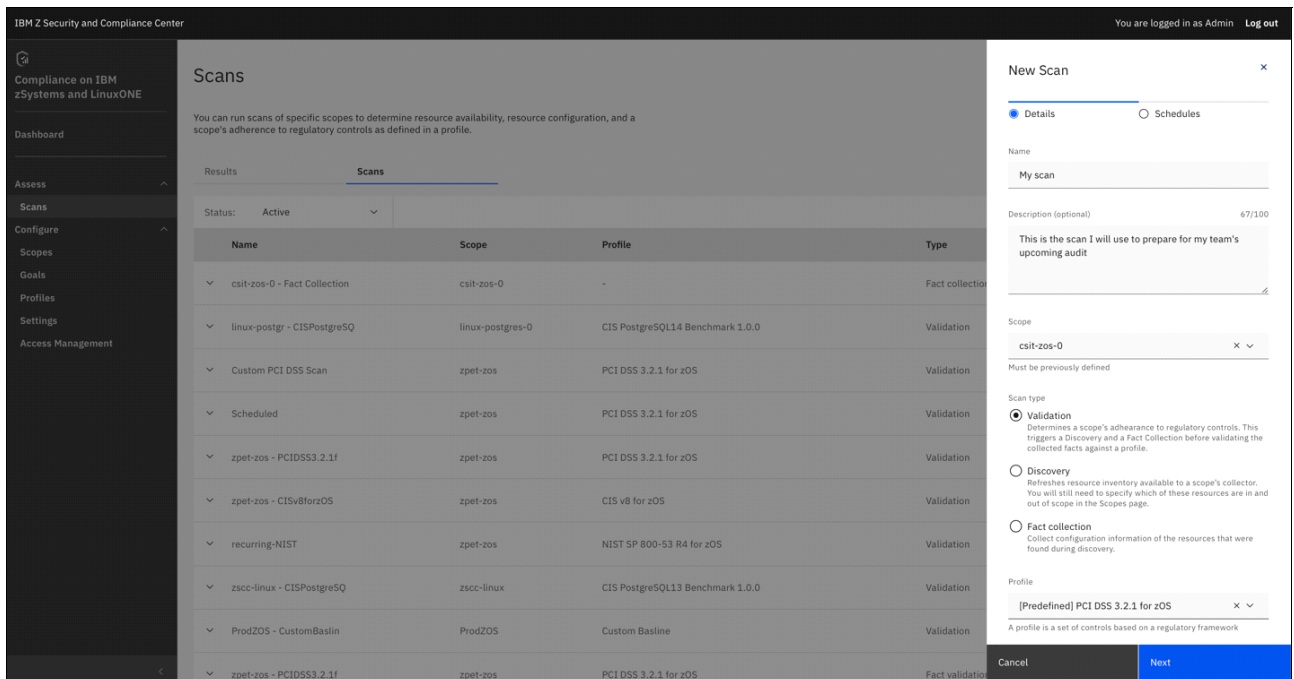


Figure 5-12 New scan information

There are three types of scans:

- In a *discovery scan*, the solution looks for any new systems that belong to a scope. So, if you recently brought a new system online, this solution is a good way to ensure that the scope contains all the resources that you want in it.
- In a *fact collection scan*, the solution collects all data from your environment for every system in the specified scope.
- In a *validation scan*, the solution collects all data from your environment for every system in scope, and then runs that data against a profile to assess your environment’s compliance with that profile.

For our environment, we are interested in the validation scan.

2. Configure “automatically repeat” to help assess compliance drift over time. Having the scan automatically repeat is a best practice. You will not see the “compliance drift over time” view if you do multiple, ad hoc scans rather than automatic repeating scans.

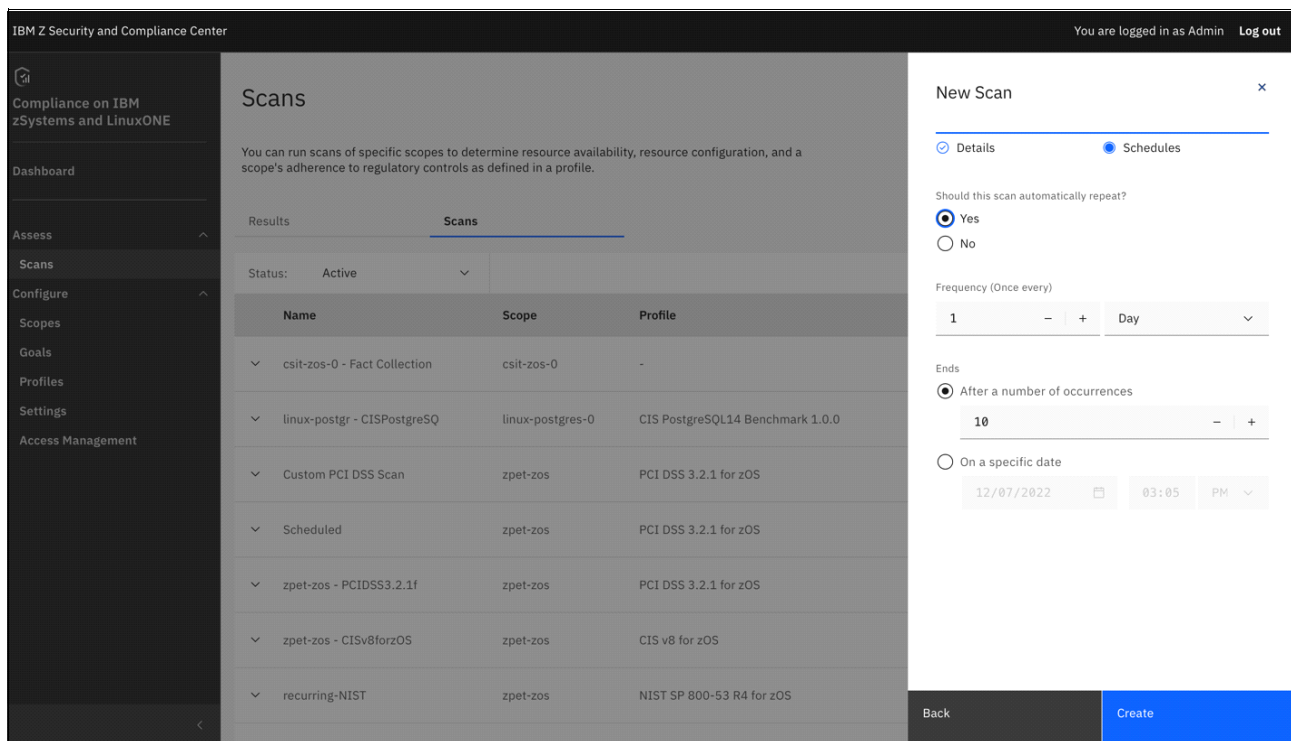


Figure 5-13 Selecting a scan type

The context in which the scan is created can determine how frequently it should recur: Sometimes, you might want it to happen yearly, and in other cases, you might want it to happen daily.

3. Click **Create**. A confirmation message appears at the upper right.

5.2.3 Viewing the scan results

After the validation scan runs, you can see the results on the “Scan” page by clicking the **Results** tab (see Figure 5-14 on page 77). An at-a-glance view of when the scan was run and the number of controls that passed or failed is provided.

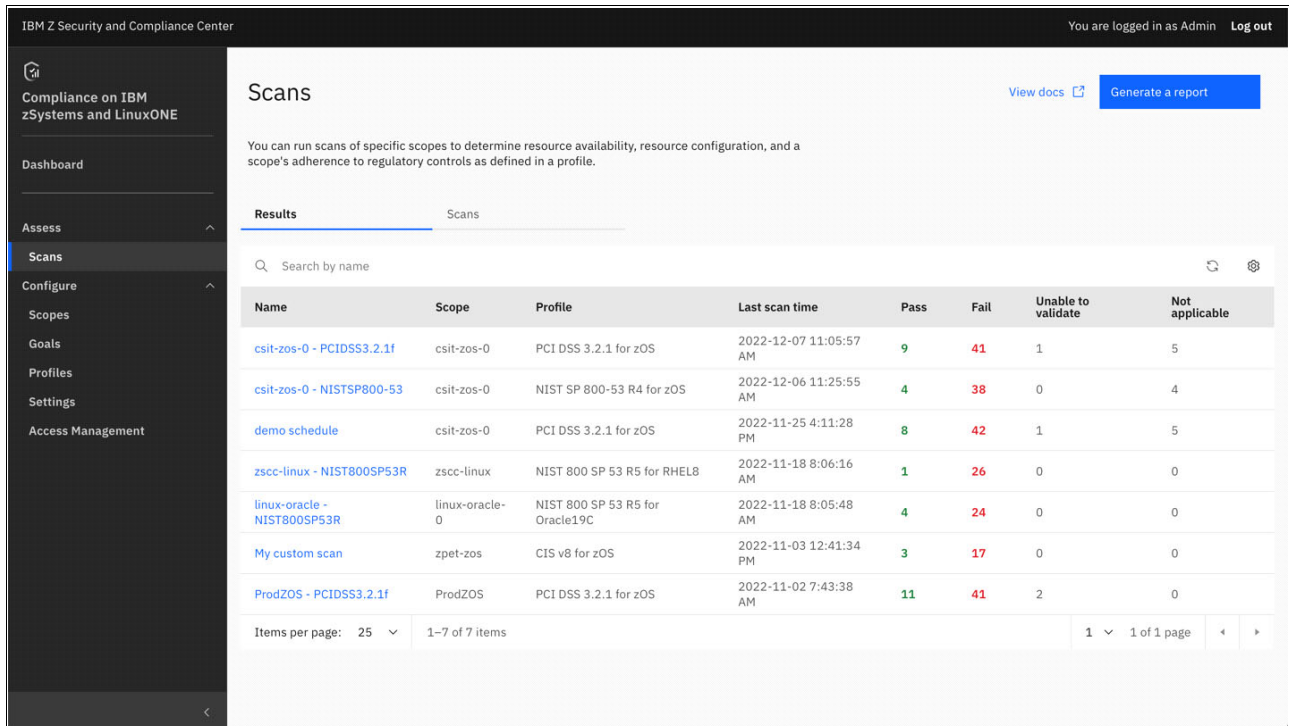


Figure 5-14 List of scan results

If more information is needed, you can click the name of the scan for more details. A detailed account of the validation scan results is shown in Figure 5-15.

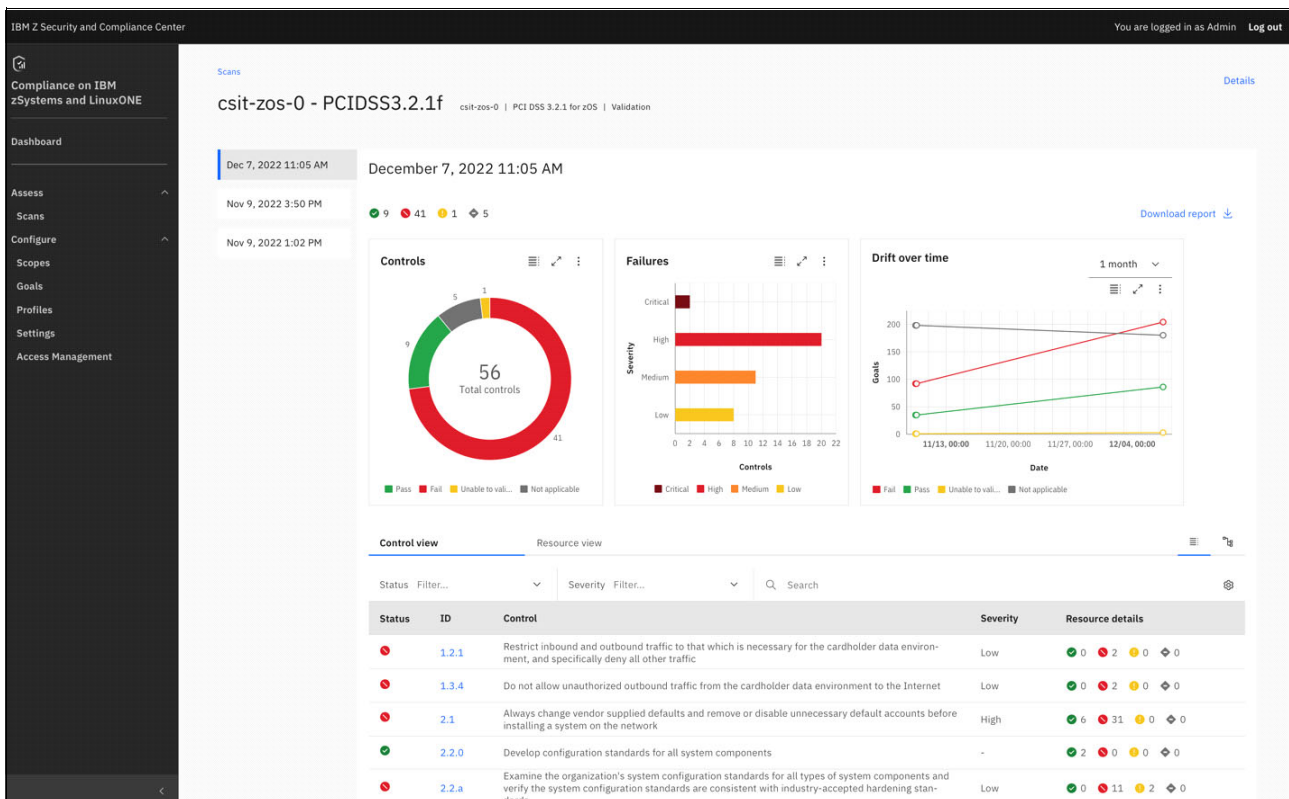


Figure 5-15 Detailed scan results

At the top of the Results page, there are three widgets for high-level summaries of a compliance posture:

- ▶ The donut chart provides a breakdown of the security controls that were evaluated by using the collected data. You can see how many controls passed, failed, or were “unable to validate” or not applicable.
- ▶ The second widget takes all the failures and displays each by severity level: critical, high, medium, or low.
- ▶ The third widget shows compliance drift over time. Increasingly, auditors are looking for a continuous account of compliance and how it is changing with time. With this line chart, you have the number of controls and their status displayed over time.

Auditors typically look for comparisons between one point in time to another. By clicking the timestamps at the upper left, you see the scan data at different points in time.

With the widgets, someone like a Chief Information Security Officer (CISO) can easily get access to high-level compliance reporting, where compliance posture and how it is changing on an ongoing basis can be understood.

Someone like a security architect or system programmer might want more details. At the lower part of window, you see a complete list of every security control that was tested against the collected data. You see an icon that represents the control status (such as pass or fail), and a unique control ID number that matches the requirement number in the original regulation (if you are using predefined profile). You see the link between the control and the regulation. You can see a description of the control, severity level, and resource details (a more granular breakdown of what was tested for the control and what passed or failed).

Clicking a control opens the control details pane (see Figure 5-16). The goals are individual technical checks that are written for IBM Z components that were tested as part of the control. You can click a goal to view more information about it, and the results for that goal, such as a table showing every resource that was tested, and the expected and actual values.

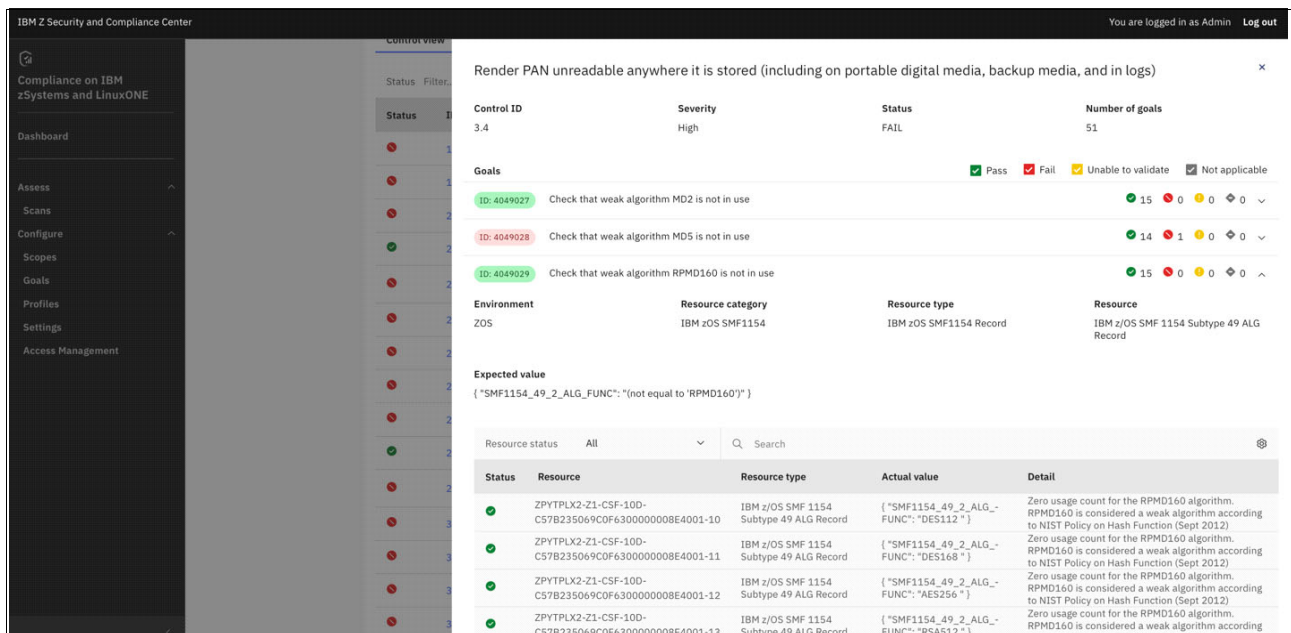


Figure 5-16 Viewing control details

Staff should be able to use this page to determine, with pinpoint accuracy, which parts of their environment must be addressed for successful and thorough remediation.

Note: Tables in the IBM Z Security and Compliance Center GUI are sortable, filterable, and searchable.

Reports of the scans can be downloaded (see Figure 5-17). The “Detailed” report generates a full list of all the control and goals information as a CSV or PDF. The “Delta” report can use two points in time. IBM Z Security and Compliance Center produces a spreadsheet of every security control and its status for two points in time.

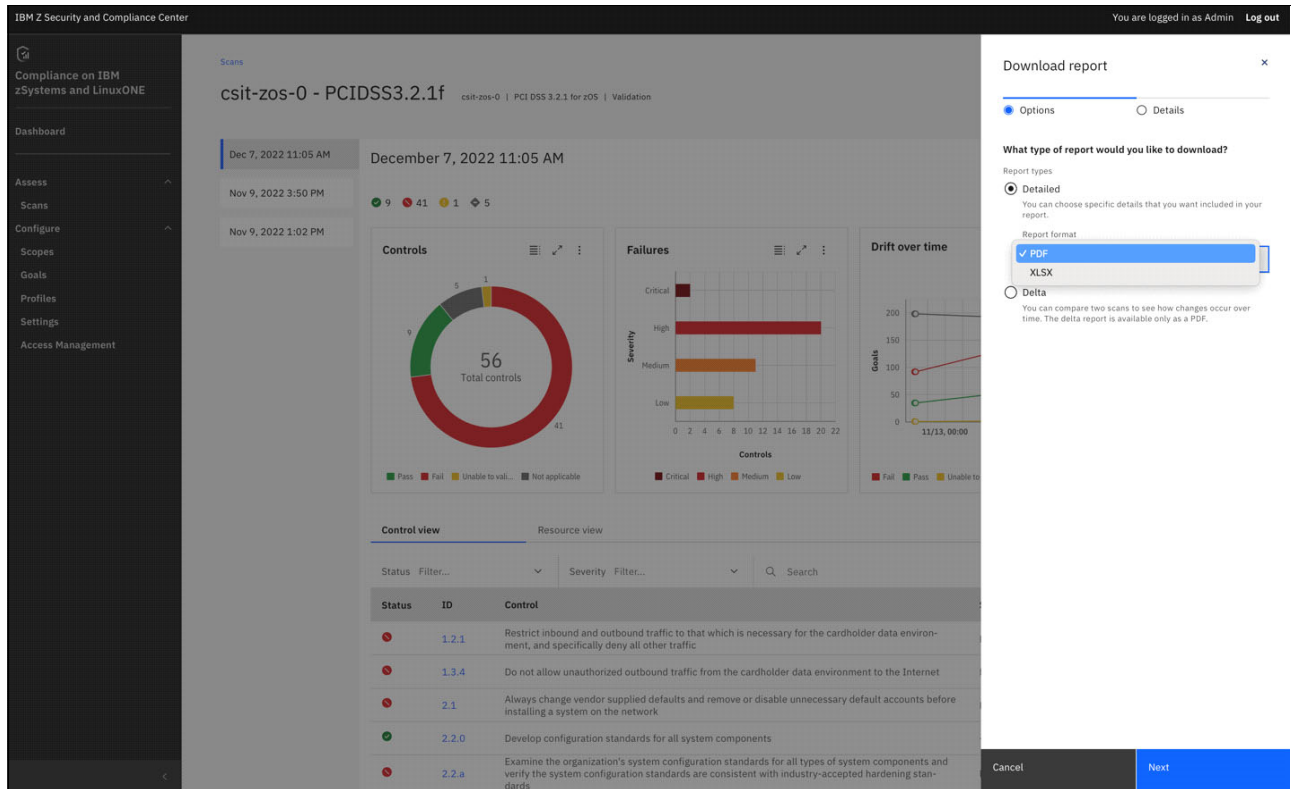


Figure 5-17 Downloading reports

5.3 Using a custom profile to prepare for an audit

Although the predefined profiles for PCI DSS, NIST, and CIS are useful, there might be other reasons to create a custom profile. For example:

- ▶ If your CISO or security team has a set of business-specific security requirements.
- ▶ If you have an audit for a regulatory framework that does not have a predefined profile.
- ▶ If you want to monitor compliance drift for a specific component.

There are two ways to create a custom profile: Either you use an existing profile and remove, add, or modify the controls as needed, or start from scratch.

Note: You cannot modify or remove controls from a predefined profile. However, you can create a profile from a predefined profile so that you choose only the controls and goals that are relevant for your requirement.

Consider preparing for an upcoming audit by using a custom profile, as described in 4.2, “Use case 2: Using a custom profile to prepare for an audit” on page 54.

5.3.1 Creating a custom profile by using an existing profile

To create your own profile from an existing profile, complete the following steps:

1. Click **Create** at the upper right of the table (see Figure 5-18) on the Profiles page (selected in the left pane).

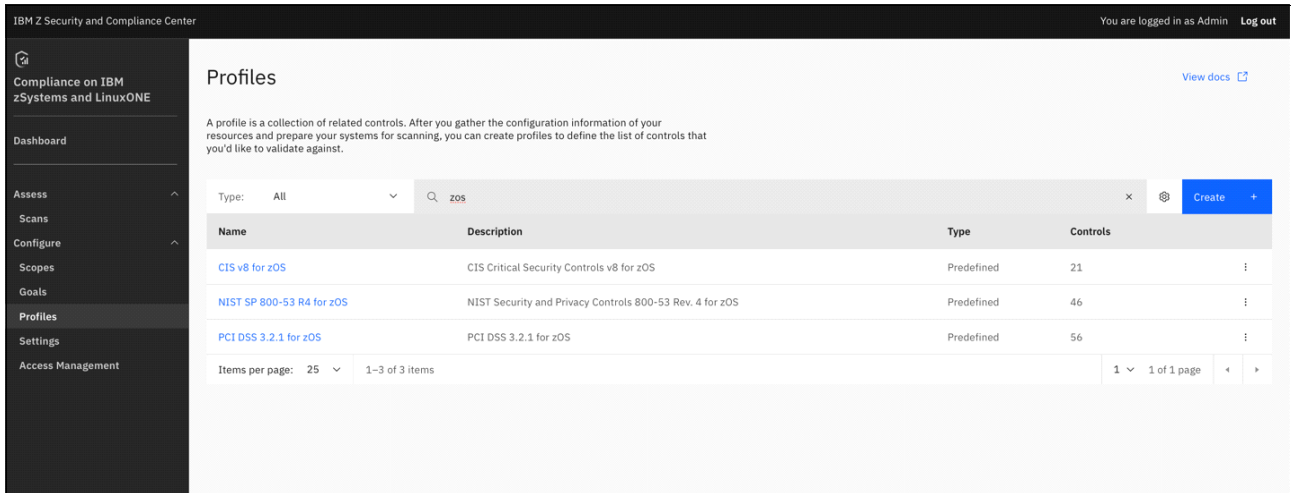


Figure 5-18 Creating a profile

The window that is shown in Figure 5-19 opens, where you can provide a name and description of your profile, and specify whether to pre-populate the profile with controls and goals from an existing profile.

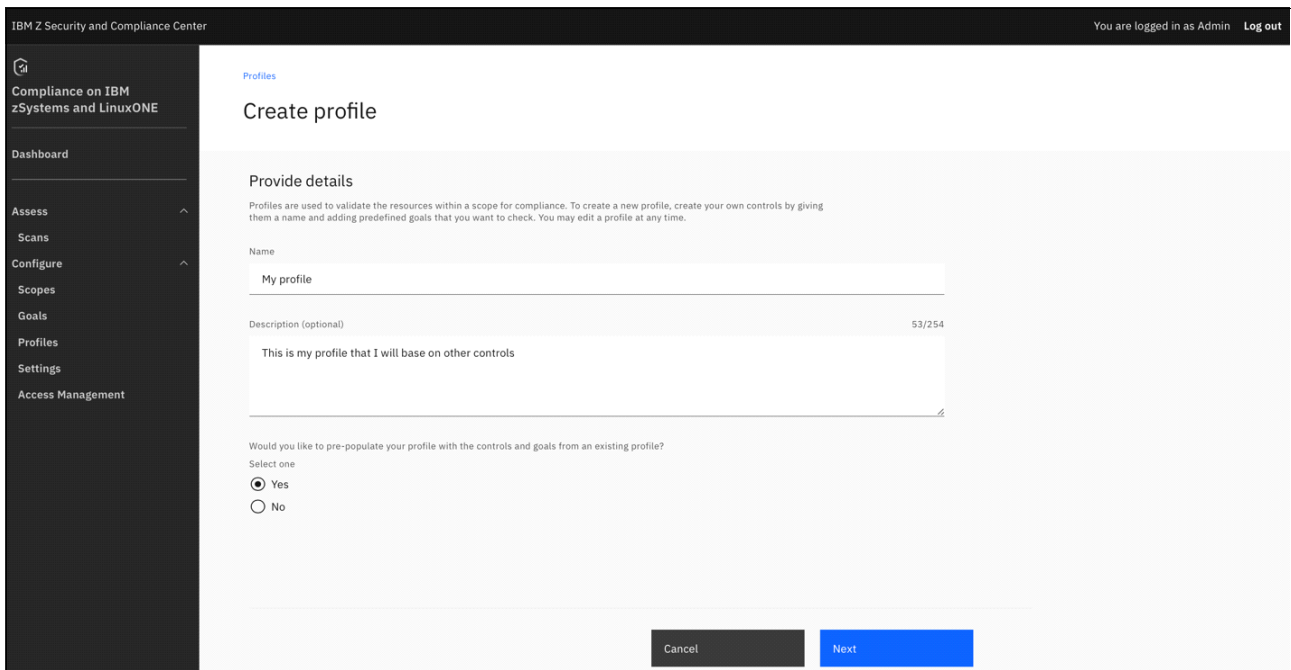


Figure 5-19 Creating a profile by using an existing profile

2. Click **Yes** to base the profile on an existing profile. Select any of the existing profiles (predefined or custom) and which controls to populate from that profile. A profile can be based on multiple profiles.

Sometimes, you might want to create a profile that is based on a subset of the controls of different profiles. For example, you know that the internal security requirements that your CISO wants to follow are based on NIST SP800-53. In this case, you might want to use the NIST SP800-53 profile as the base profile, and select only the controls that you know apply to your internal requirements.

3. Use the checkboxes at the left of the table (see Figure 5-20) to import the existing profiles.

Note: A profile can also be viewed in xlsx format by using the **Export profile** function (see Figure 2-7 on page 24).

The screenshot shows the 'Create profile' page in the IBM Z Security and Compliance Center. The page title is 'Create profile' and the breadcrumb is 'Profiles /'. Below the title is the section 'Import existing profiles' with a sub-header 'Import existing profiles' and a note: 'The profiles selected below will act as the base of your new profile. Their controls and goals will be in your new profile, and you will be able to select which ones to remove in the next page.' Below this is a search bar and a table of existing profiles. The table has columns for 'Name', 'Type', and 'Goals'. Each row has a checkbox in the 'Name' column.

Name	Type	Goals
<input type="checkbox"/> Global Control Library	Predefined	1026
<input type="checkbox"/> CIS Red Hat Enterprise Linux 7 Benchmark 2.2.0	Predefined	193
<input type="checkbox"/> CIS Red Hat Enterprise Linux 8 Benchmark 1.0.0	Predefined	166
<input type="checkbox"/> CIS SUSE Linux Enterprise 12 Benchmark 2.1.0	Predefined	197
<input type="checkbox"/> PCI DSS 3.2.1 for SUSE12	Predefined	10
<input type="checkbox"/> NIST 800 SP 53 R5 for SUSE12	Predefined	31
<input type="checkbox"/> CIS SUSE Linux Enterprise 15 Benchmark 2.1.0	Predefined	197
<input type="checkbox"/> PCI DSS 3.2.1 for SUSE15	Predefined	10
<input type="checkbox"/> NIST 800 SP 53 R5 for SUSE15	Predefined	31

Figure 5-20 Importing existing profiles

4. After you select the profiles for your custom profile, you can select controls from each profile (see Figure 5-21). You can select the entire control or only certain subcontrols.

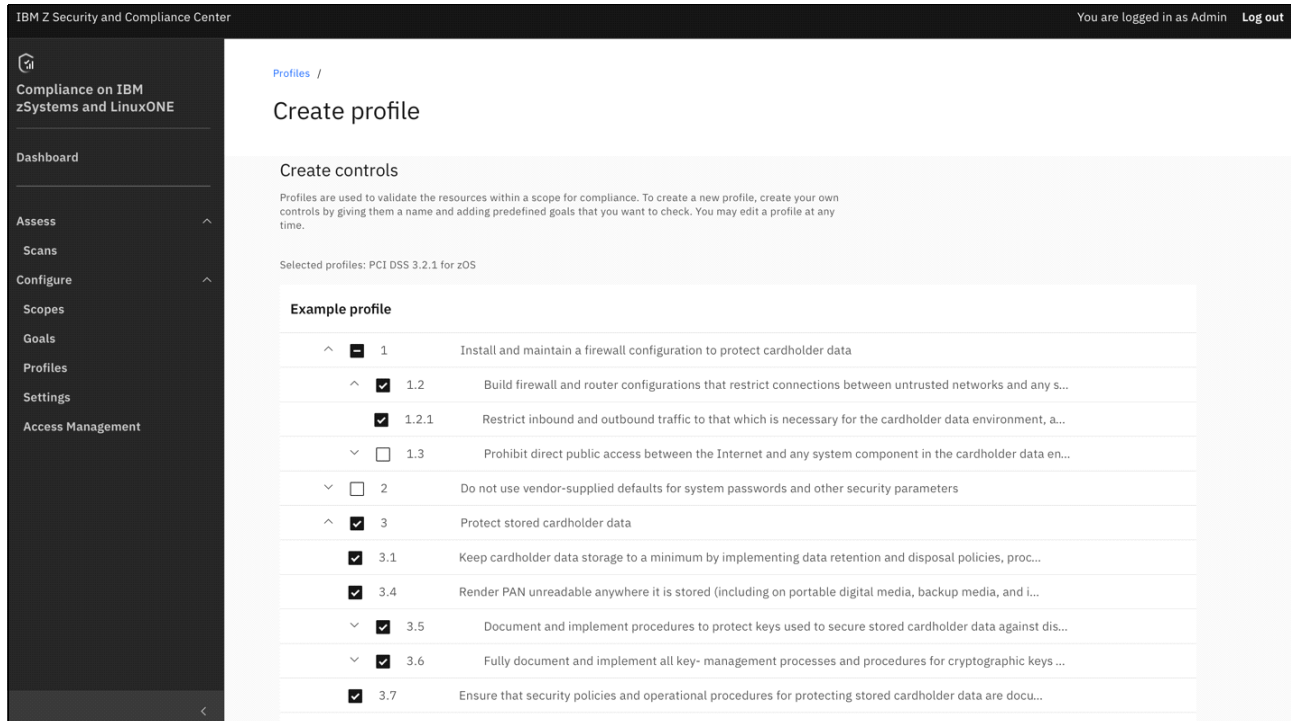


Figure 5-21 Selecting controls and subcontrols

5. After you select the controls that should populate the custom profile, click **Create**. You return to the profiles page. You should see your newly defined profile in the profiles table.

You are now ready to use your profile for a validation scan. To see how this task is done, go to 5.2.2, “Starting a new scan” on page 74.

5.3.2 Creating a custom profile from scratch

A profile can be created from scratch by selecting a goal from a list of available goals that you must meet. To create a profile from scratch, complete the following steps:

1. Select **Configure** → **Profiles**, and then click **Create**.

The window that is shown in Figure 5-22 on page 83 opens. Define your profile and give it a name, description, and whether you want to start from scratch.

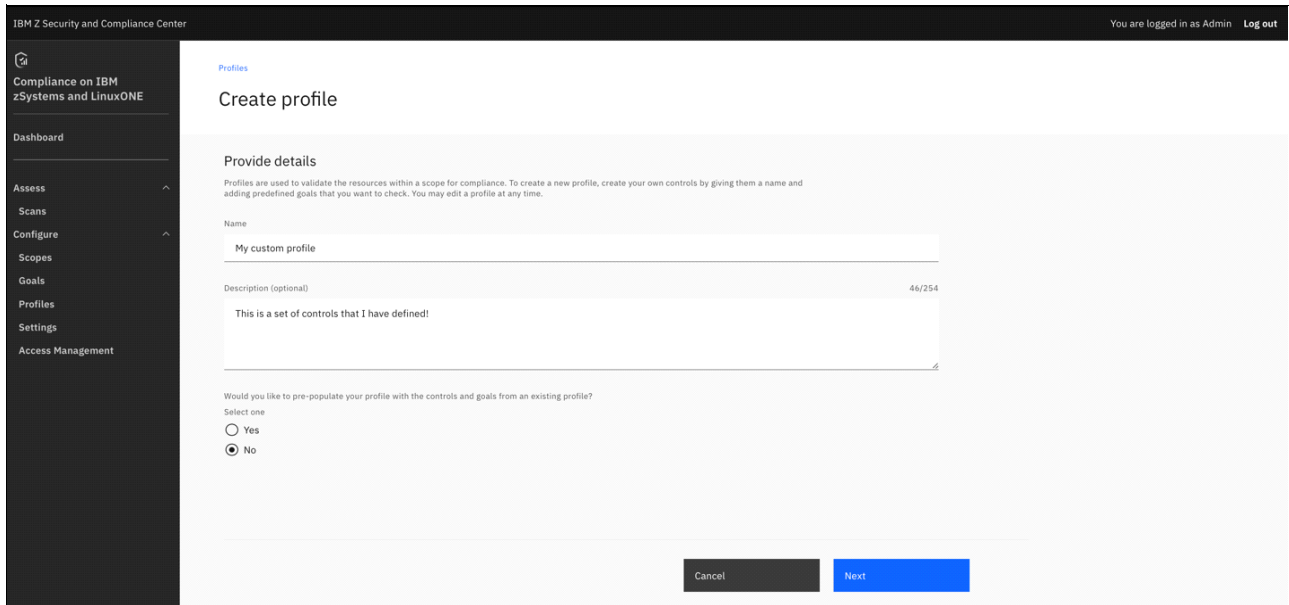


Figure 5-22 Profile details

2. Click **No** to define your own controls from scratch. You can add as many controls as needed. You can define a control number, description, and select the goals to add to the control.
3. Click **Next**, and then click **Add Controls** (see Figure 5-23). You can create as many controls as you want.

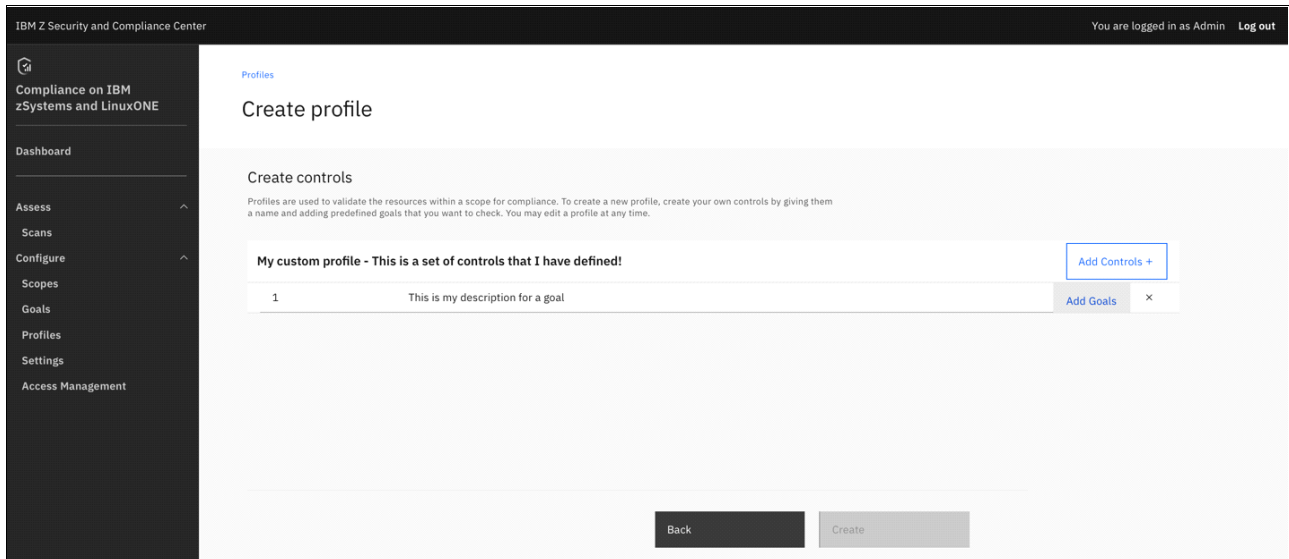


Figure 5-23 Creating controls

4. Click **Add Goals** to specify the goals that will be tested to validate whether the control passes or fails (the control passes only if every goal that is contained within it passes).

The Global Goals Library window opens (see Figure 5-24). It is a list of every goal that IBM Z Security and Compliance Center can perform. You also can use the search field at the top of the Global Goals Library to quickly find relevant goals to include in each control. Tags help specify the IBM z/OS component to which the goal is relevant.

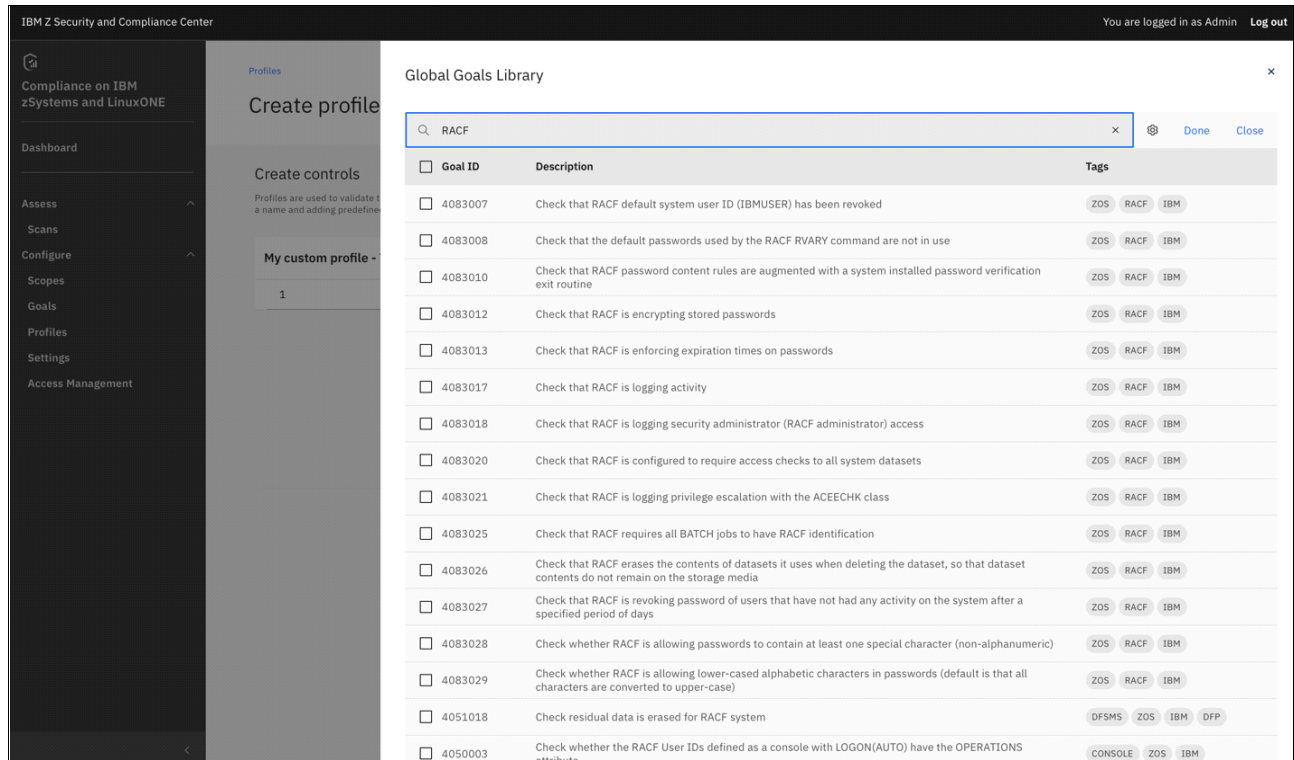


Figure 5-24 Global Goals Library: a RACF search

5. Using the checkboxes on the left, select the goals that you want added to each control.
6. After you define your controls, click **Create**. You return to the profiles page. You should see your newly defined profile in the profiles table.

You are now ready to use your profile for a scan. You have two options.

- ▶ Run a validation scan, which collects data from the z/OS systems that are defined to your scope and compares the facts that are collected to the goals in your custom profile. To see how this task is done, go to 5.2.2, “Starting a new scan” on page 74.
- ▶ Run a fact validation scan. You can run a fact validation scan on any existing fact collection scan or validation scan. You do not need to collect data from the z/OS systems that are defined to your scope if you have already previously done so.

To run a fact validation scan, complete the following steps:

1. In the left pane of the GUI, select **Configure** → **Scopes** (see Figure 5-25 on page 85).

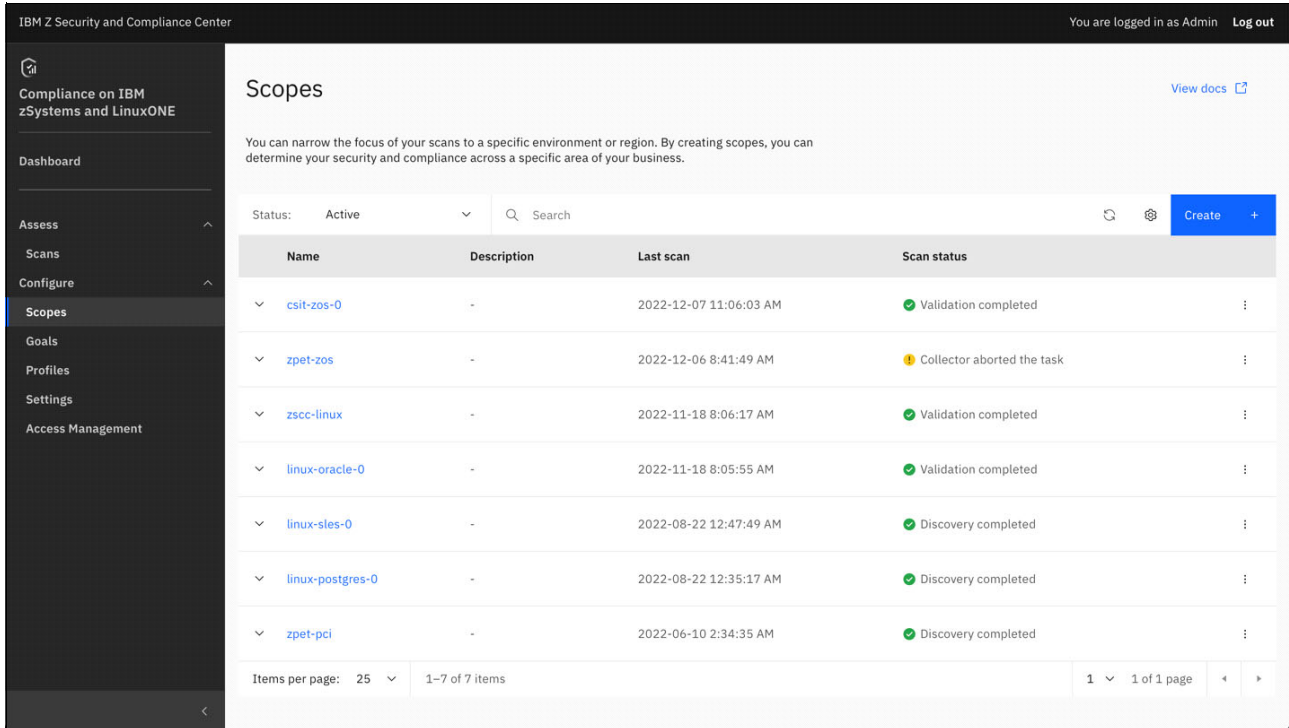


Figure 5-25 Selecting a scope

- Click the name of the scope that you want to run the fact validation scan against. A history of scans appears (see Figure 5-26).

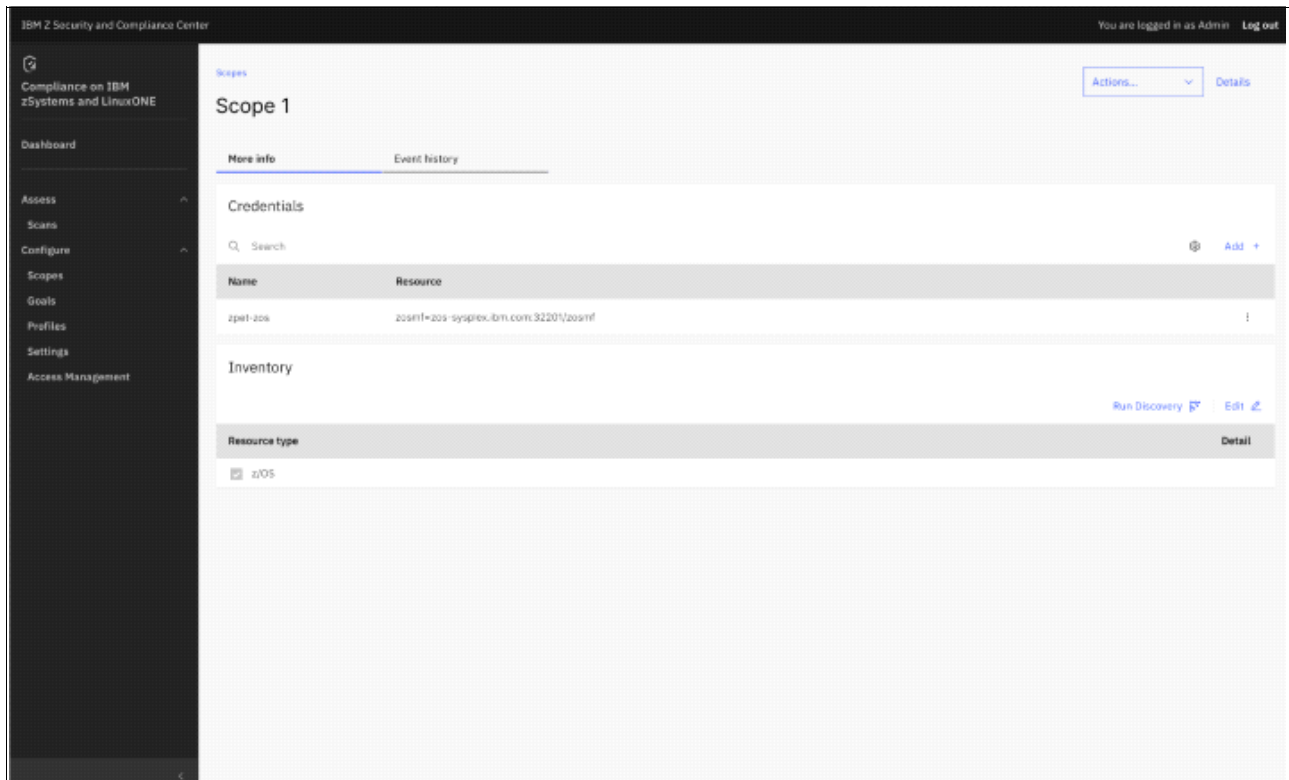


Figure 5-26 History of scans

- From the history of scans, click the name of the scan that you want to validate (see Figure 5-27). You may select any validation, fact validation, or fact collection scan.

Note: You cannot run a fact validation on a discovery scan because these scans do not collect data.

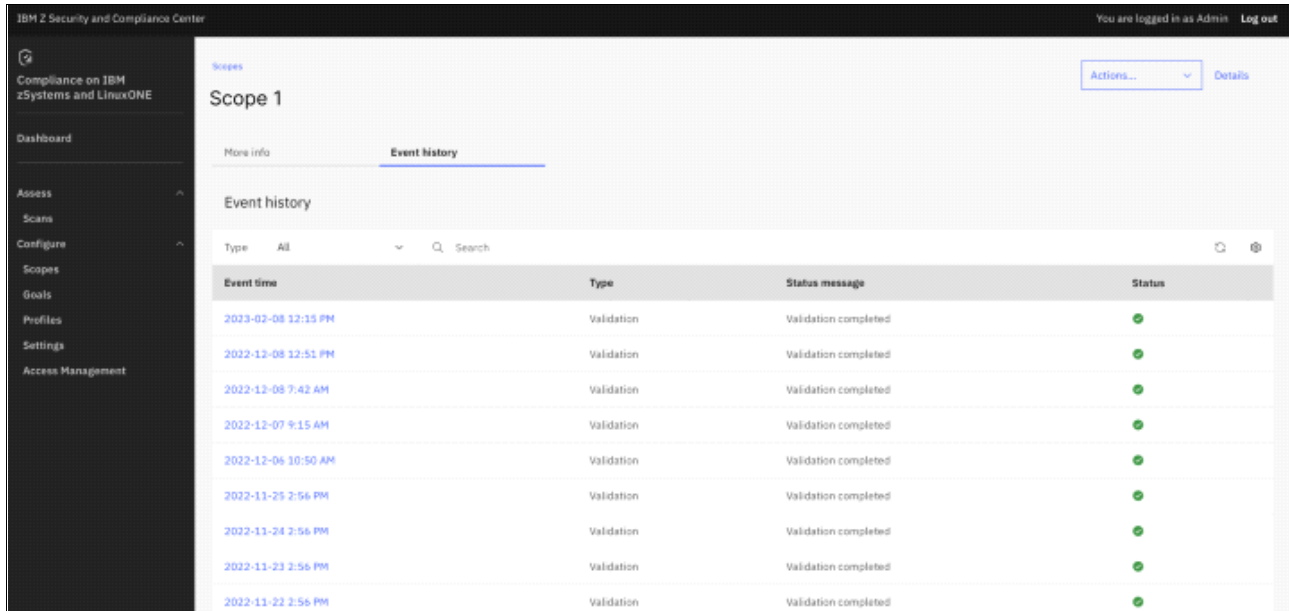


Figure 5-27 List of scans

- Click **Validate** at the upper right of the Results table. The window that is shown in Figure 5-28 on page 87 opens, where you can indicate the profile to run the validation against.

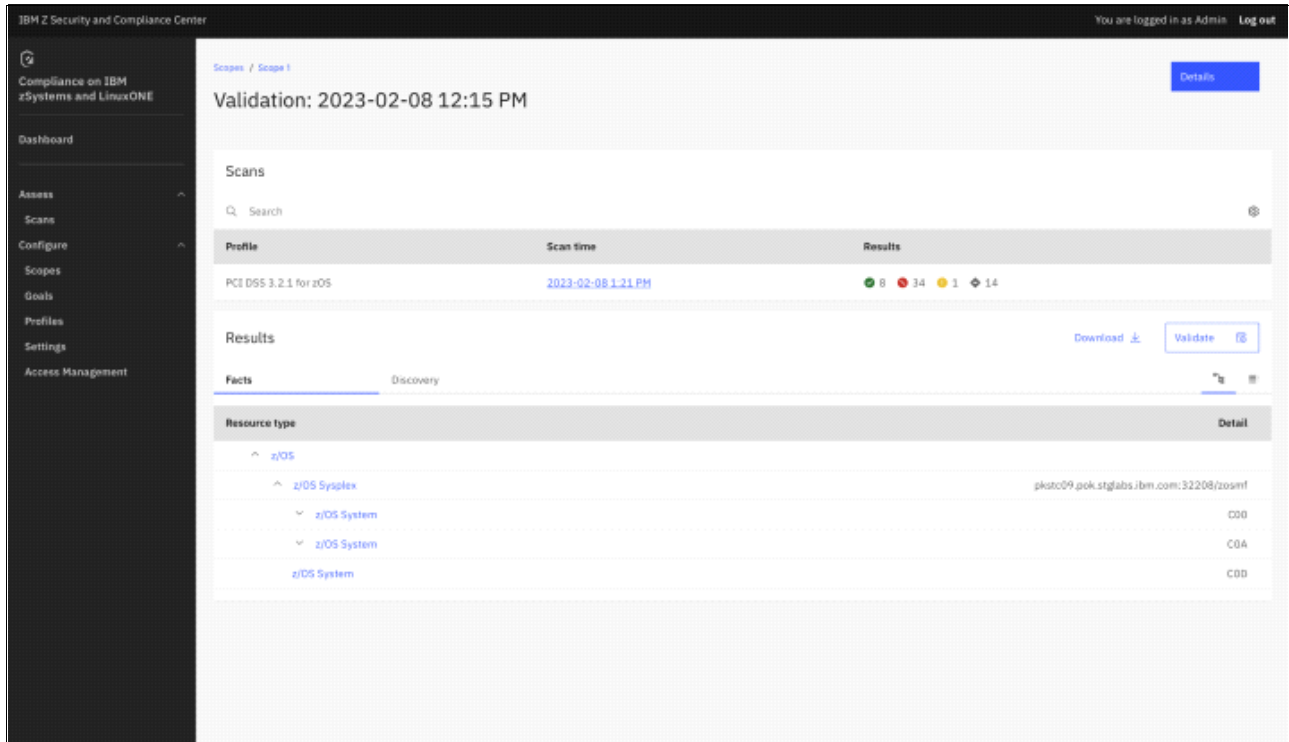


Figure 5-28 Profile for validation

5. Click **Create** (see Figure 5-29).

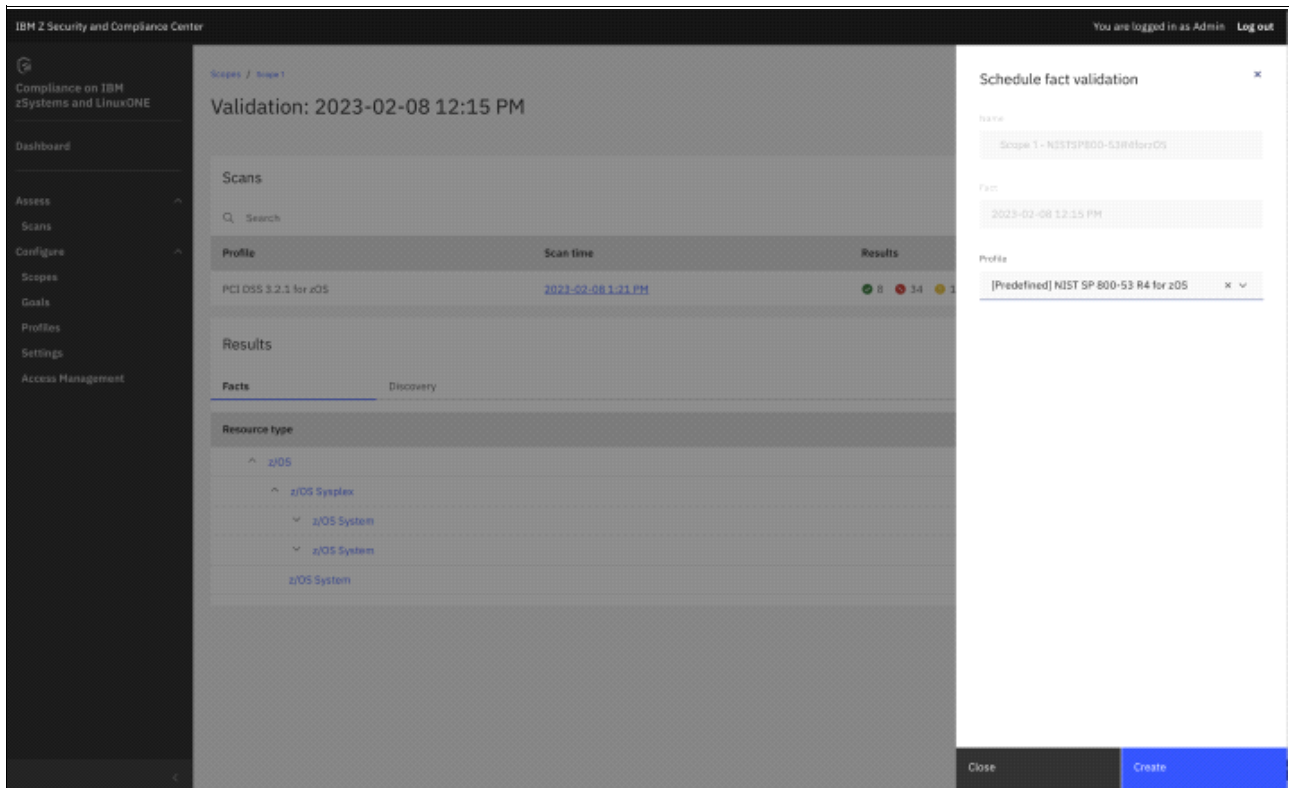


Figure 5-29 Schedule fact validation window

5.4 Providing compliance evidence for an auditor

When the IBM Z Security and Compliance Center scope is defined and the scan is run by using the pre-determined regulatory framework that is chosen for the audit, you can look at the result and present it to auditors. The auditors can be internal or external to the organization.

There are different report options to show the details that are applicable to the specific target audience or intended purpose. This report is produced by the Compliance Viewer during an audit process, and the aim is to produce a report with only as much detail as required to fulfill audit requirements. Including too much detail, such as the exact nature of the failures, risks the report becoming too complex for auditors with little or no knowledge of the IBM Z platform.

Note: The example that is used in this section is a PCI DSS audit, but it can be used similarly for a NIST or CIS audit.

The auditor is preparing to audit IBM Z platforms against the PCI DSS 3.2.1 requirements, as described in 4.3, “Use case 3: Providing compliance evidence for an auditor” on page 57. To do so, they complete the following steps:

1. From the IBM Z Security and Compliance Center dashboard, select **Assess** → **Scans**, and then select the relevant scan for the audit report to be generated (see Figure 5-30).

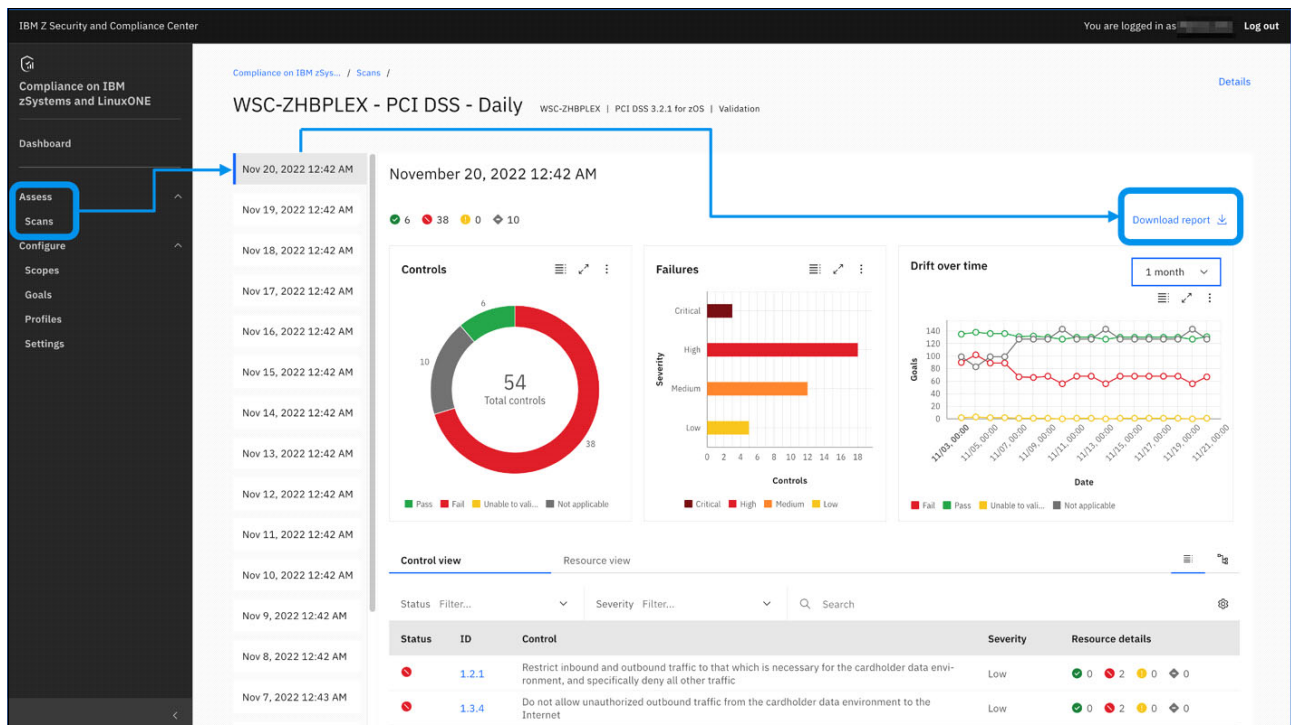


Figure 5-30 Accessing scans

The window shows the Dashboard view of this specific scan with details about the scope; the regulation that is applicable (PCI DSS 3.2.1 in this example); when this scan ran and a quick view of the number of controls validated; how many controls passed; and how many failed. Also shown is the severity of the failed controls and the drift over time (depending on the time frame that is chosen from the drop-down list (1 month in this example)).

- After confirming that this scan result is correct for the report that will be generated, click **Download Report** at the upper right of the window. A dialog box opens at the right, where the report options must be selected (see Figure 5-31).

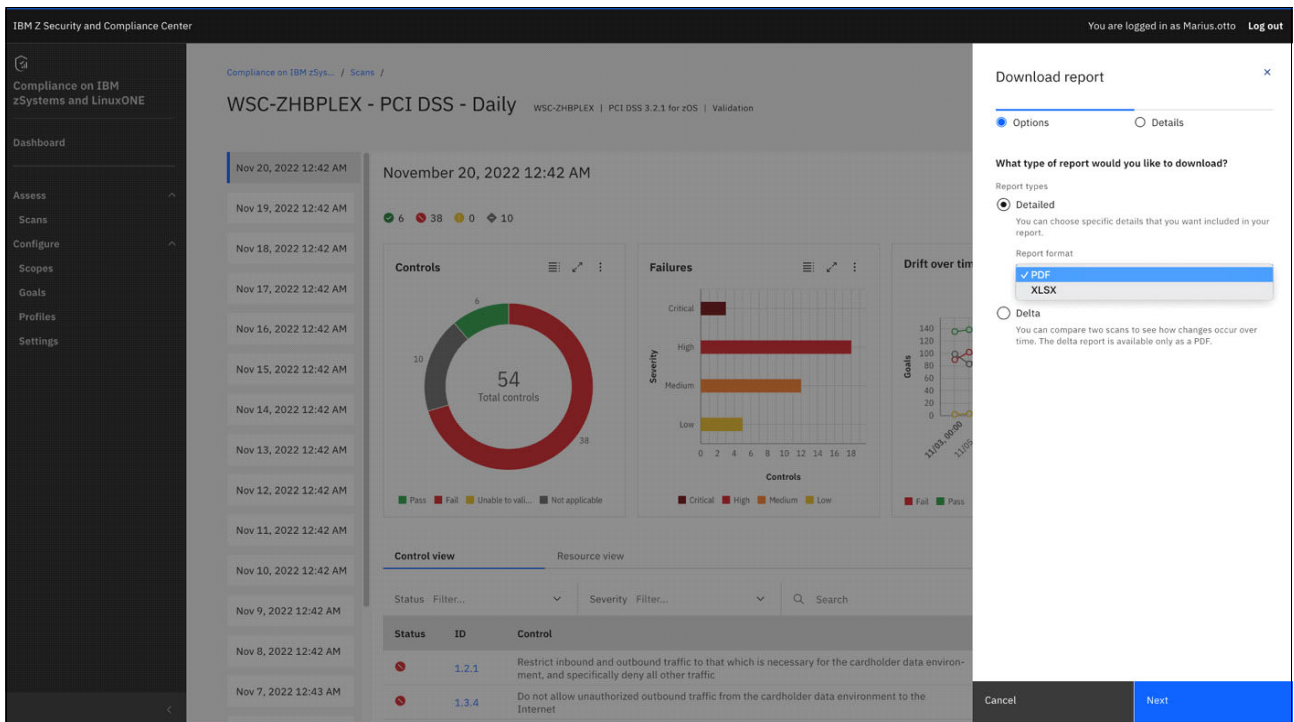


Figure 5-31 Type of report to be downloaded

For auditing purposes, select **Detailed** in PDF format to generate an easy-to-read report that can be shared with an auditor. If you want the Compliance Lead to track the drift and investigate any newly failing controls, select **Delta**.

When the selections are made, click **Next**.

3. Select the level of detail that is required for the report (see Figure 5-32).

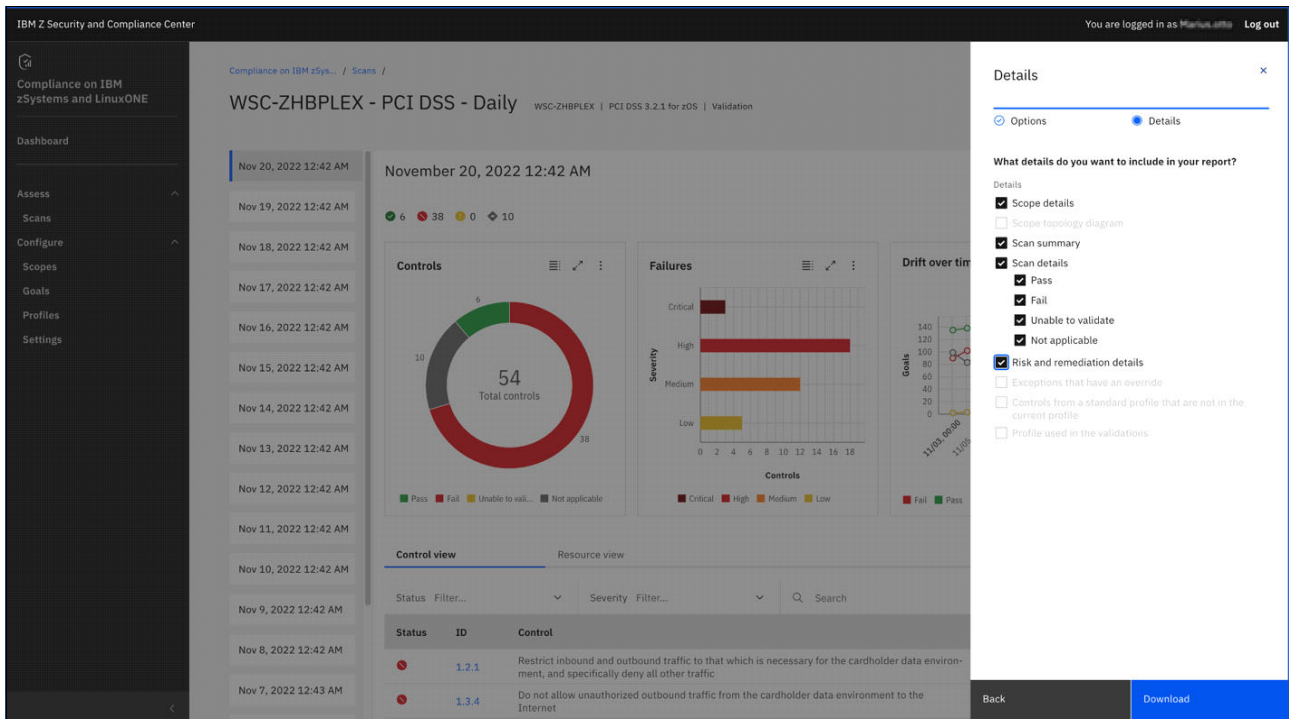


Figure 5-32 Selecting the level of detail for the report

4. Click **Download** to download the report.

Figure 5-33 shows the Executive Summary. It includes the regulatory framework name (for example, PCI 3.2.1 for z/OS), the total number of controls that are validated, and how many passed and how many failed. It is a good, high-level view of the compliance posture that is measured against the profile that is used by this scan, as required for this audit.

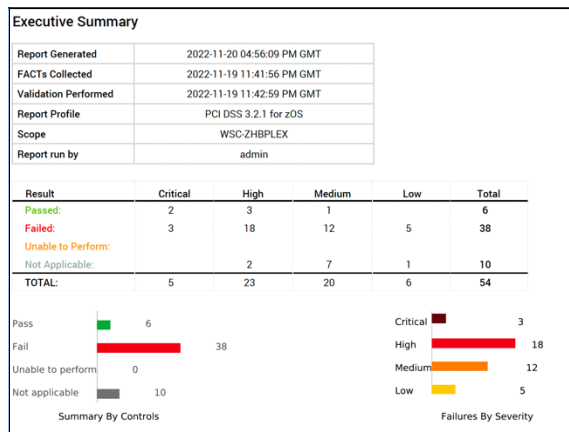


Figure 5-33 Executive Summary

Selecting **Scope details** shows the timestamps of when the scan ran, and the full scope of the z/OS sysplexes and selected z/OS LPARs from the sysplexes that provided evidence input for this scan (see Figure 5-34 on page 91).

Profile Details	
Created By:	IBM Z
Created On:	2022-11-02 05:23:24 PM GMT
Last Modified By:	IBM Z
Last Modified On:	2022-11-02 05:25:46 PM GMT
Filters Applied to Validation Details	
IT Resources:	Pass, Fail, Unable to Perform, N/A
Scope Details	
Collectors Used:	Region(s):
• IBM-zcollector	
IT Resources per Type:	
• IBM z/OS System - 2	
• IBM z/OS - 1	
• IBM z/OS Sysplex - 1	

Figure 5-34 Scope details

Selecting **Scan details** produces a list of all controls in table form (see Figure 5-35) according to the regulatory framework that is validated against (for example, the mapping of the regulatory framework controls to z/OS specific security parameter settings).

Control ID	Description	Overall Status	Severity	Number of IT Resources				
				Pass	Fail	Unable	N/A	Total
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs)	FAIL	High	54	1			55
3.5.0	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse	FAIL	Medium	1	6			7
3.5.1	Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture	FAIL	Low		6			6
3.5.3	Store secret and private keys used to encrypt/decrypt cardholder data	FAIL	Medium	51	3			54
3.6.0	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data	FAIL	Medium	1	12			13
3.6.1	Generation of strong cryptographic keys	FAIL	High	64	1			65
3.6.3	Secure cryptographic key storage	FAIL	Medium	51	3			54
3.7	Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties	FAIL	Low		6			6
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks	FAIL	Critical	2	8		5	15
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as high, medium, or low) to newly discovered security vulnerabilities	FAIL	Medium		2			2
6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers	PASS		2				2
6.3.2	Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes)	FAIL	Low		1			1
7.1.0	Limit access to system components and cardholder data to only those individuals whose job requires such access	PASS		2			1	3

Figure 5-35 Scan details

Each control description is a link that takes you directly to the Validation Details view of the control (see Figure 5-36). It also points to the underlying goals that were validated. Listed are the high-level control statement for each goal, the specific SMF 1154 record subtype, expected values, and the actual values that are produced by the scan. These details can be used for remedial action. For the z/OS system administrator, they can link the SMF 1154 record subtype to the actual z/OS component and security parameter in question.

Goal Details
Control: [2.1 Always change vendor supplied defaults and remove or disable unnecessary default accounts before installing a system on the network](#)
Goal ID: 4083008
Description: Check that the default passwords used by the RACF RVARY command are not in use

Severity	GOAL Status: FAIL	Status	Pass	Fail	Unable	N/A	Total
High		Resources	2	0	0	0	2

Goal Target: ZOS / IBM zOS SMF1154 / IBM zOS SMF1154 Record / IBM z/OS SMF 1154 Subtype 83 Record
Expected Value: {
 "SMF1154_83_1_RACFRVSP": "1",
 "SMF1154_83_1_RACFRVSV": "0",
 "SMF1154_83_1_RACFRVTP": "1",
 "SMF1154_83_1_RACFRVTV": "0"
 }
 }

Resource ID	Resource Type	Status	Actual Value	Detail
ZPYTPLX5-Z3- RACF-10DYB8Y23456BCB290 000000009590004	IBM z/OS SMF 1154 Subtype 83 Record	FAIL	{ "SMF1154_83_1_RACFRVSP": "1", "SMF1154_83_1_RACFRVSV": "1", "SMF1154_83_1_RACFRVTP": "1", "SMF1154_83_1_RACFRVTV": "1" }	z/OS Security Server RACF default passwords have not been disabled
ZPYTPLX5-Z1- RACF-10DYB8Y23456BCB290 000000009590004	IBM z/OS SMF 1154 Subtype 83 Record	FAIL	{ "SMF1154_83_1_RACFRVSP": "1", "SMF1154_83_1_RACFRVSV": "1", "SMF1154_83_1_RACFRVTP": "1", "SMF1154_83_1_RACFRVTV": "1" }	z/OS Security Server RACF default passwords have not been disabled

Figure 5-36 Validation Details

If selected, the report also contains the Validation Details section, where the results of each control validation are shown (whether the control passed or failed).

For audit purposes, it is advisable to include all these details for the auditor to view, except perhaps the “Risk and remediation details”, which are more applicable to whomever undertakes remedial action.

When these selections are made, click **Download** at the lower right to download the report. The full dashboard (see Figure 5-37 on page 93) reappears with a small box stating that the report is being generated. When the report is generated (the duration depends on the size of the scope, that is, the amount of data that is collected from the number of sources within the scope), the download to your local machine occurs automatically (make sure pop-up windows and downloads are enabled for this website).

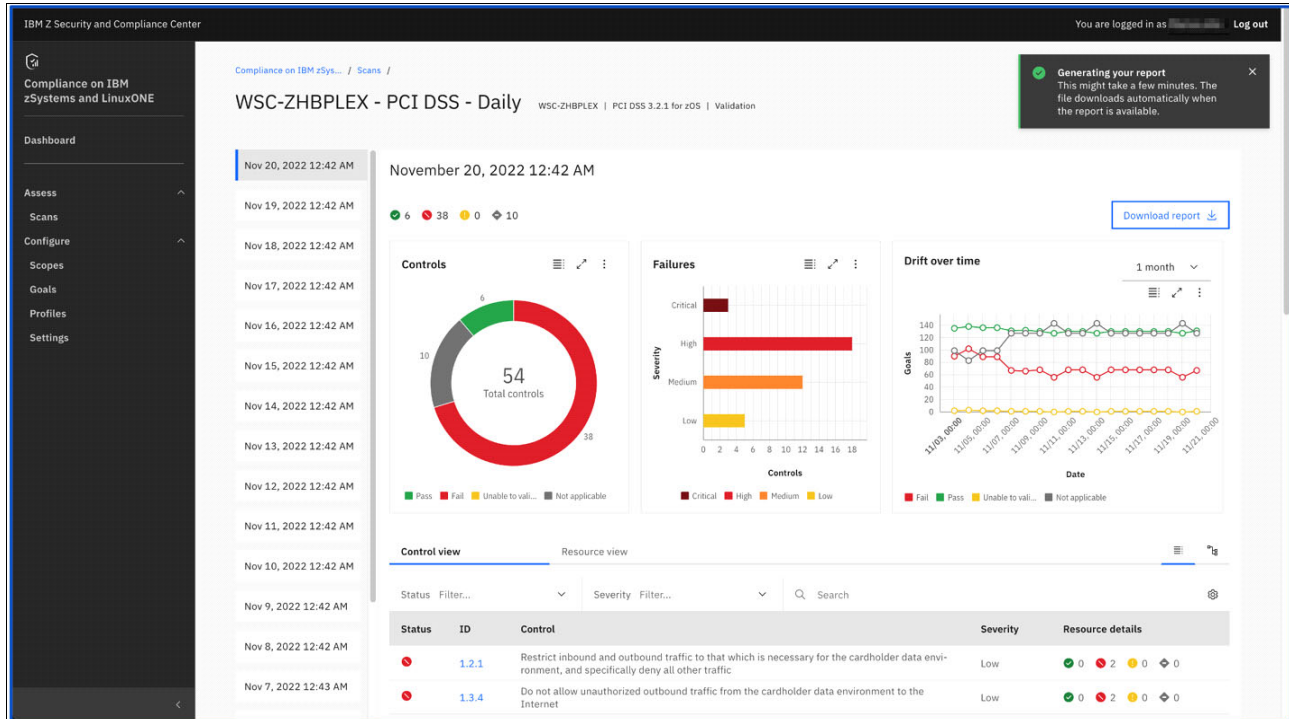


Figure 5-37 Downloading the report

Open the download folder to obtain the PDF document. You can now print it or email it to the auditing team.

5.5 Reviewing compliance at a high level

An efficient way to get a high-level view of your compliance posture is to look at the dashboard and select the last scan of the scope that you want to review (as described in 5.4, “Providing compliance evidence for an auditor” on page 88) because the dashboard provides an at-a-glance view about how well your compliance posture is faring; how severe the risks are with the controls that have failed; and whether your compliance posture is improving or degrading over time.

Review 4.4, “Use case 4: Reviewing compliance at a high level” on page 59.

Reviewing your compliance posture on a high level can be accomplished in two ways:

- ▶ If you know which scan that you want to review, select on the dashboard the scan name and duration for which to show the compliance drift (see Figure 5-38).

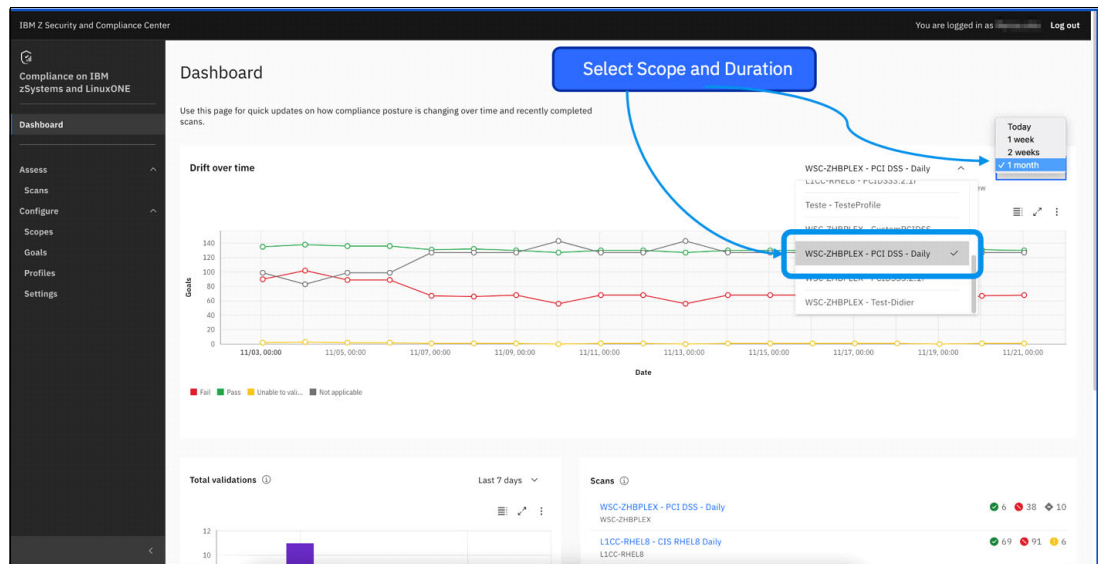


Figure 5-38 Selecting a scope from the dashboard

- ▶ If you do not know which scan that you want to review, search for it by using the search bar, which limits the results to your search criteria. From this resulting list, choose the scan that you want to review (see Figure 5-39).

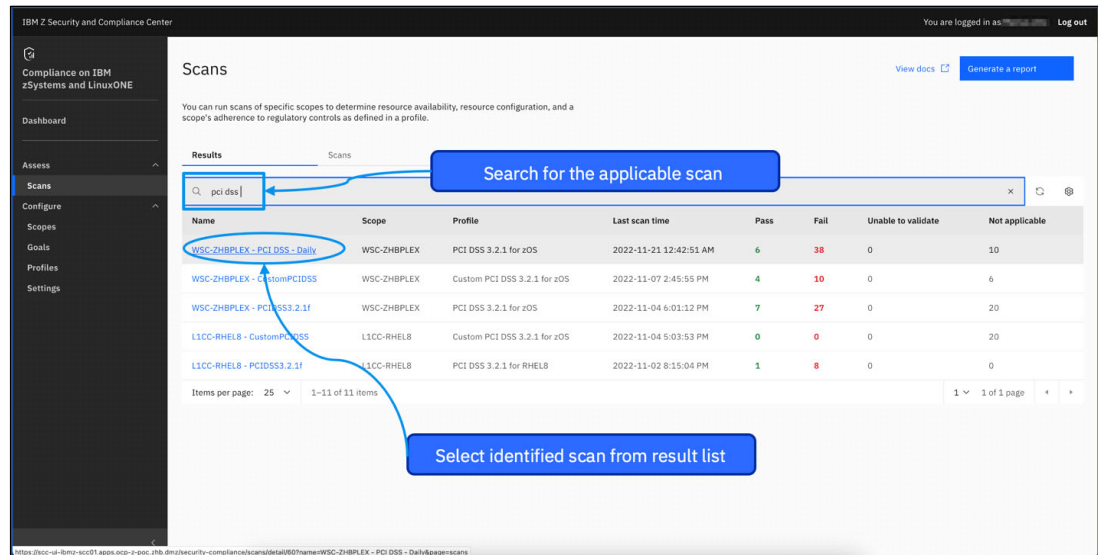


Figure 5-39 Selecting a profile from a search

Selecting the scan opens a scan overview window, where you can view the posture, risks, and drift of your compliance posture (see Figure 5-40 on page 95).

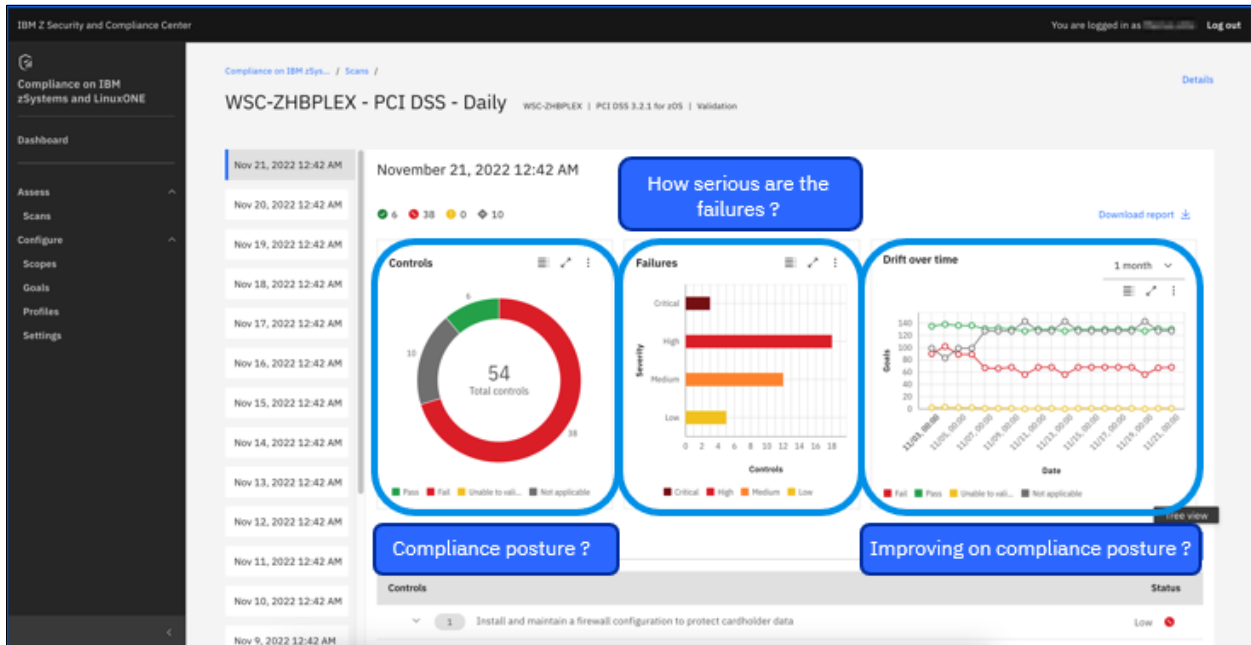


Figure 5-40 Reviewing a compliance posture

This method is a best practice because it is intuitive, and provides the most visibly appealing way for gaging where you are on your compliance journey.

Alternatively, you can generate and review a report directly from IBM Z Security and Compliance Center by completing the following steps:

1. Select **Assess** → **Scans**, and then click **Generate a report** (Figure 5-41).

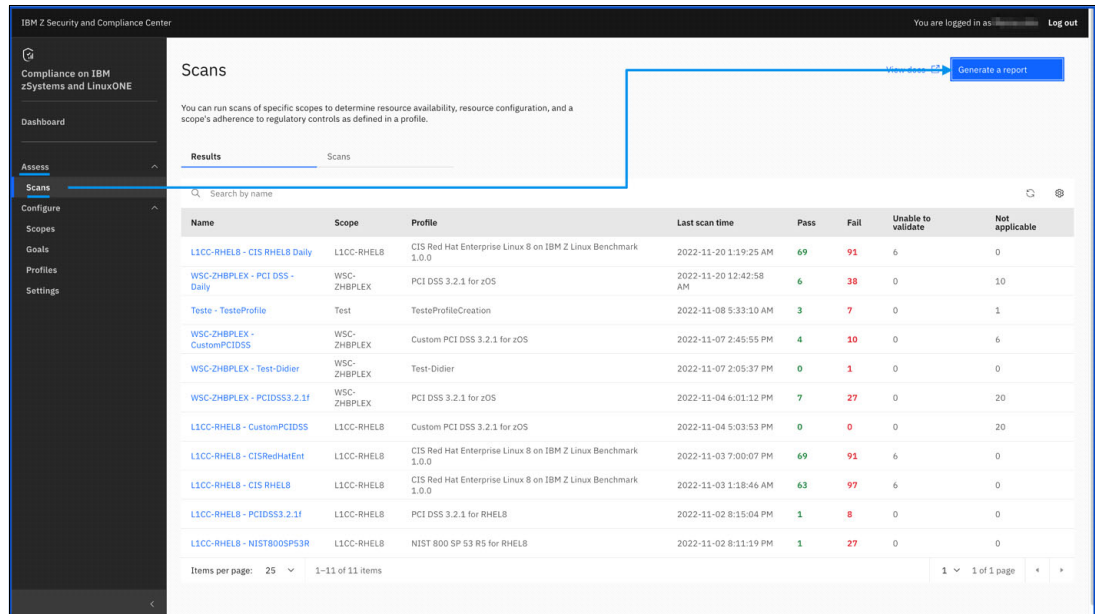


Figure 5-41 Generating a report from a scan

A pane appears at the right. Select the scopes that you want.

2. When the scope is selected, click **Next** (see Figure 5-42).

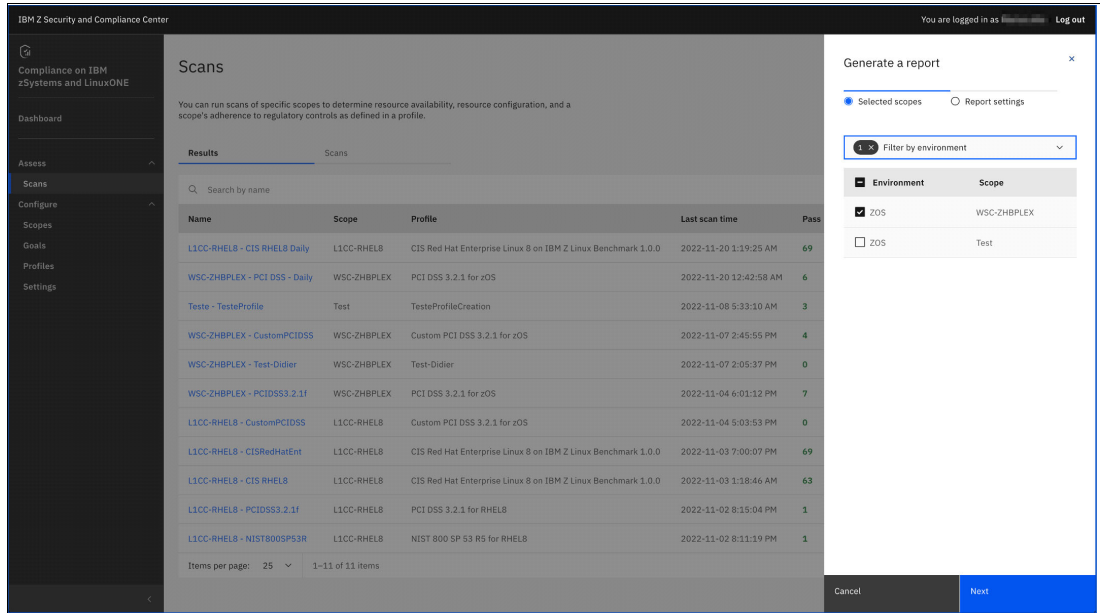


Figure 5-42 Selecting a scope

3. Select the period for which the report must be generated. When these selections are made, click **Generate report** (see Figure 5-43).

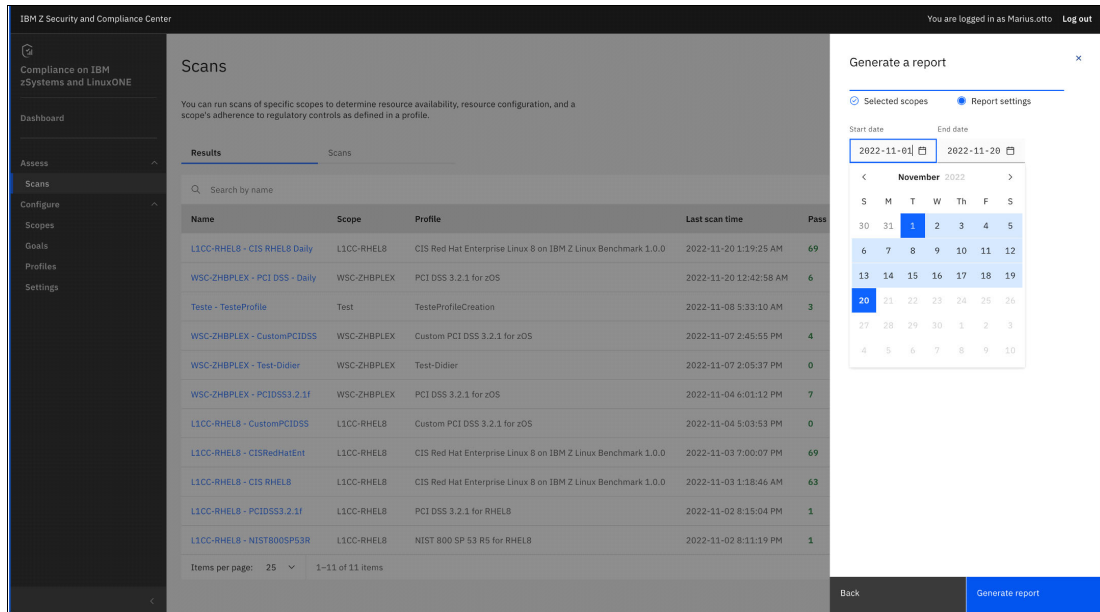


Figure 5-43 Selecting a period

The full dashboard (see Figure 5-44 on page 97) reappears with a small box stating that the report is being generated. When the report is generated (the duration depends on the size of the scope, that is, the amount of data that is collected from the number of sources within the scope), the download to your local machine occurs automatically (make sure pop-up windows and downloads are enabled for this website).

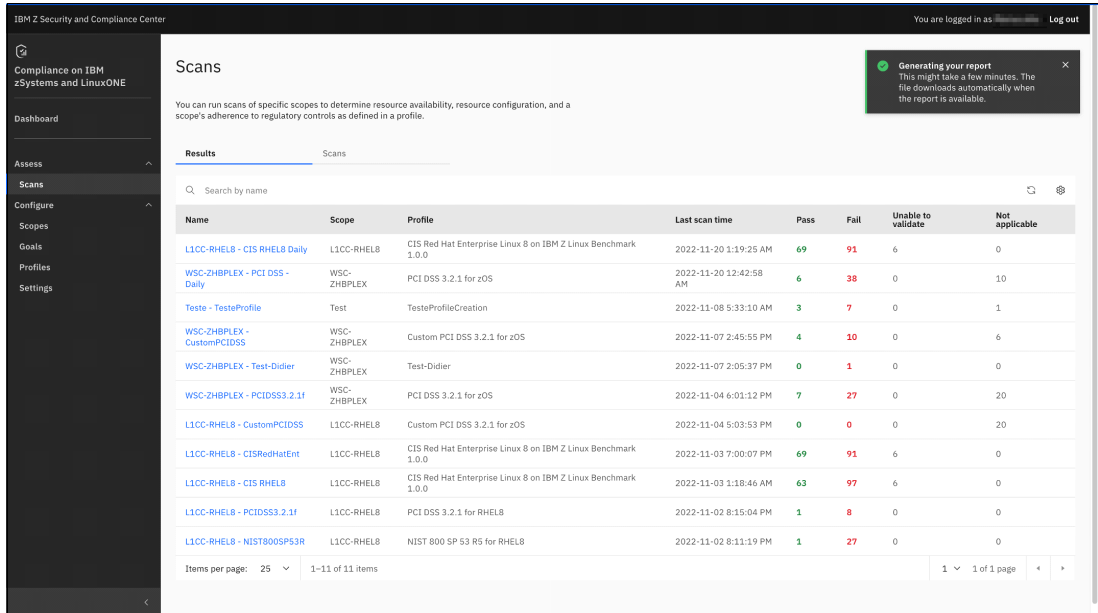


Figure 5-44 Generating the report

Open the download folder to obtain the PDF document. It shows an Executive Summary Report with validation results per scope (see Figure 5-45).

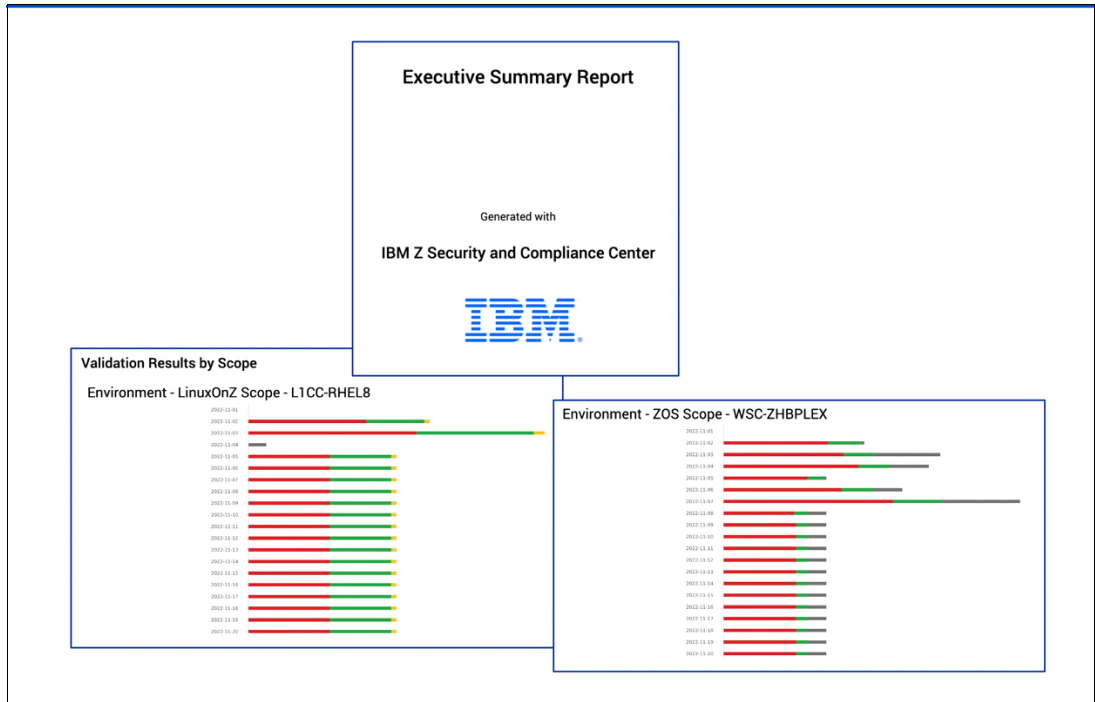


Figure 5-45 Executive summary

This report view does not show the same amount of detail as the dashboard GUI view. As a best practice, use IBM Z Security and Compliance Center GUI for assessing compliance posture at a high level.

5.6 Reviewing compliance regularly

Being compliant is continuous. Staying on track with changing regulations, identifying security gaps over time, and making sure that the right security capabilities are enabled are all critical to being compliant. Regular internal audits are a great way to uncover inadequate security controls that lead to not being compliant (also known as compliance drift).

With IBM Z Security and Compliance Center, you can set up recurring scans. After multiple recurring scans run, a compliance drift view becomes available.

Review compliance as described in 4.5, “Use case 5: Reviewing compliance on a recurring basis” on page 60.

To review compliance regularly, set up a recurring validation scan by creating a scan. Click the **Scans** tab in the Scans page, and then click **New Scan**.

As shown in Figure 5-46, you are prompted whether you want the scan to automatically repeat. Select **Yes**, and indicate how frequently scans should be performed.

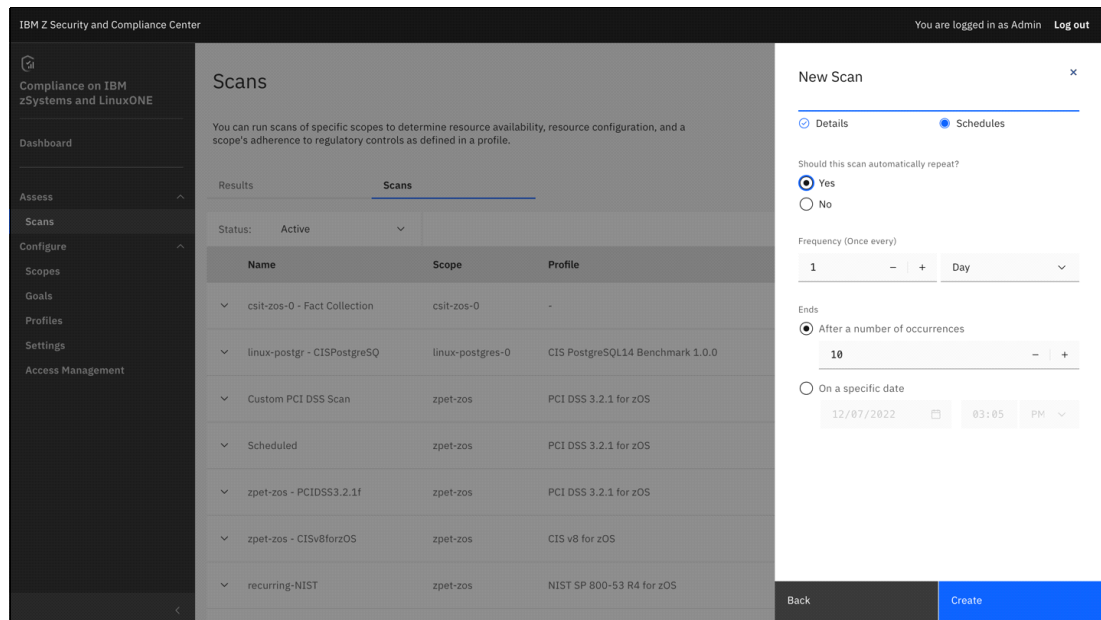


Figure 5-46 Setting up recurring scans

After multiple instances of the recurring scan have occurred, you can view compliance drift (see Figure 5-47 on page 99). Go to the scan results page, and open the **Compliance drift over time** widget. The widget shows a line chart that shows the change over time for the number of controls that passed, failed, been unable to validate, and are non-applicable. This widget can be expanded, and you can modify the period.

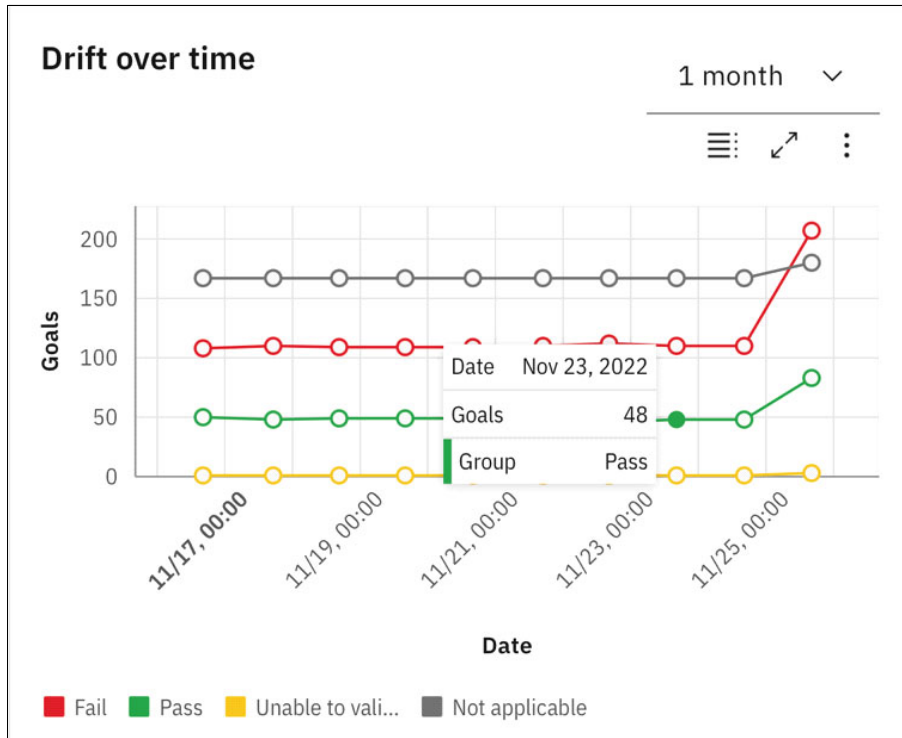


Figure 5-47 Compliance drift over time

To get a better understanding of which controls have gone out of compliance, use the Delta report feature to get a side-by-side comparison of compliance at the goal level of one point in time to another one.

To obtain this report, click “Generate report” at the upper right, select **Delta report**, and then indicate two points in time that you want to compare.

Comparing which controls failed to the ones that passed before might be a useful strategy in figuring out which compliance gaps to remediate (Figure 5-48).

Validation Summary			
Control ID #	Description	2022-10-27 18-00	2022-10-22 17-57
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic	FAIL	FAIL
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet	FAIL	FAIL
2.1	Always change vendor supplied defaults and remove or disable unnecessary default accounts before installing a system on the network	FAIL	FAIL
2.2.0	Develop configuration standards for all system components	PASS	PASS
2.2.a	Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards	FAIL	FAIL
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system	FAIL	FAIL
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure	FAIL	FAIL

Figure 5-48 Validation summary

5.7 Monitoring a specific component for compliance drift

As described in 4.6, “Use case 6: Monitoring a specific component for compliance drift” on page 62, it is best practice to create a custom profile from scratch, as described in 5.3.2, “Creating a custom profile from scratch” on page 82. In this profile, include all goals that are related to the component that you are monitoring compliance for by using the search bar and tags to filter through goals.

When that profile is created, you may use it in a recurring scan to monitor the compliance posture about this component. To do this task, complete the steps that are described in 5.6, “Reviewing compliance regularly” on page 98.



How to find and remediate failing goals

IBM Z Security and Compliance Center analyzes security parameter values that are captured by the different z/OS components and applications. These values are reflected in SMF records that are returned from a target system after a scan. Each goal is compared with the specific value that is returned by the controls for which the scan ran. If the goal deviates from the returned value, it is flagged as Failed.

This appendix shows how to use IBM Z Security and Compliance Center to identify the reason why a prescribed goal is failing by using a validation report.

This appendix covers the following topics:

- ▶ “Identifying failing controls that need further investigation” on page 102
- ▶ “Finding the suggested remedial area from a failed goal” on page 104

Identifying failing controls that need further investigation

While looking at the scan results on the IBM Z Security and Compliance Center dashboard, you see that a control clearly indicates a passed or failed status at the left side of the window. On the right side of the window, the number of goals that either passed or failed for that specific control are shown.

In Figure A-1, Control 2.1 of the Payment Card Industry Data Security Standard (PCI DSS) profile shows as Failed because two goals that are grouped under this control failed. Control 2.1 suggests that the default vendor-supplied passwords be changed or to disable the default vendor-supplied accounts during installation of the application.

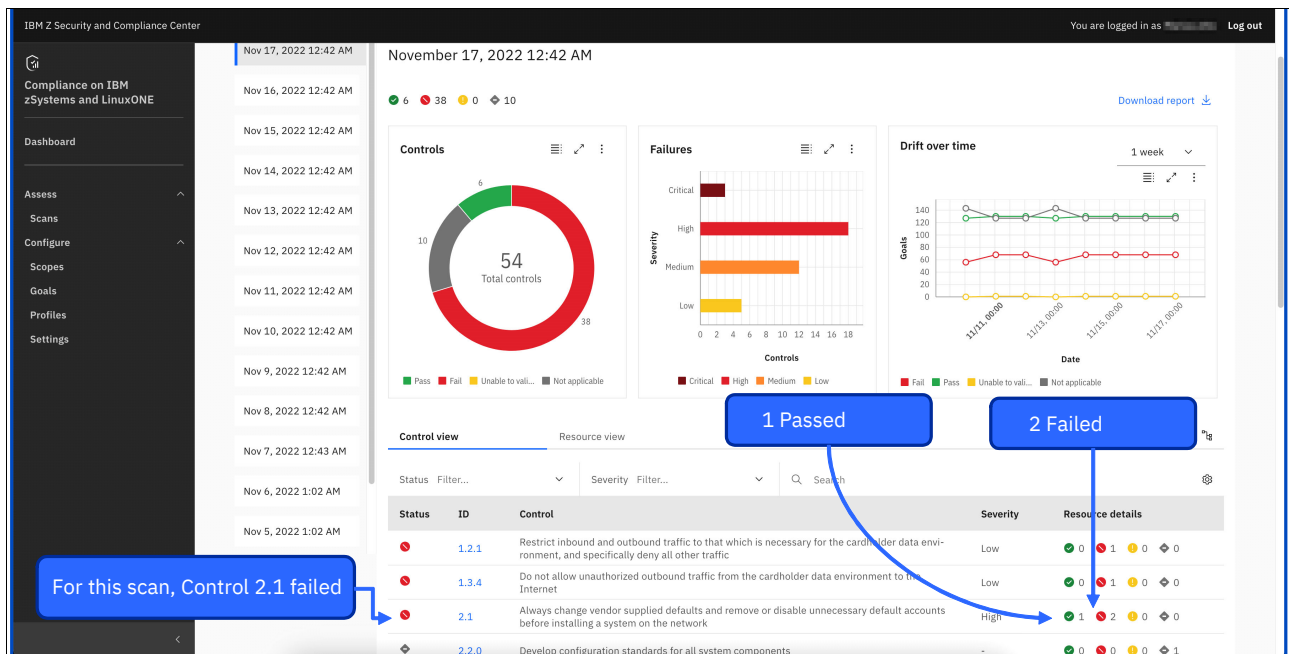


Figure A-1 Scan results showing passed or failed controls and goals

One goal passed (Goal ID 4083007), which requires the user to revoke the default supplied IBM RACF user ID (see Figure A-2 on page 103). The IBMUSER user ID is intended for use only during the initial installation process. After installation, the IBMUSER user ID should be revoked so that it cannot be used by unauthorized users.

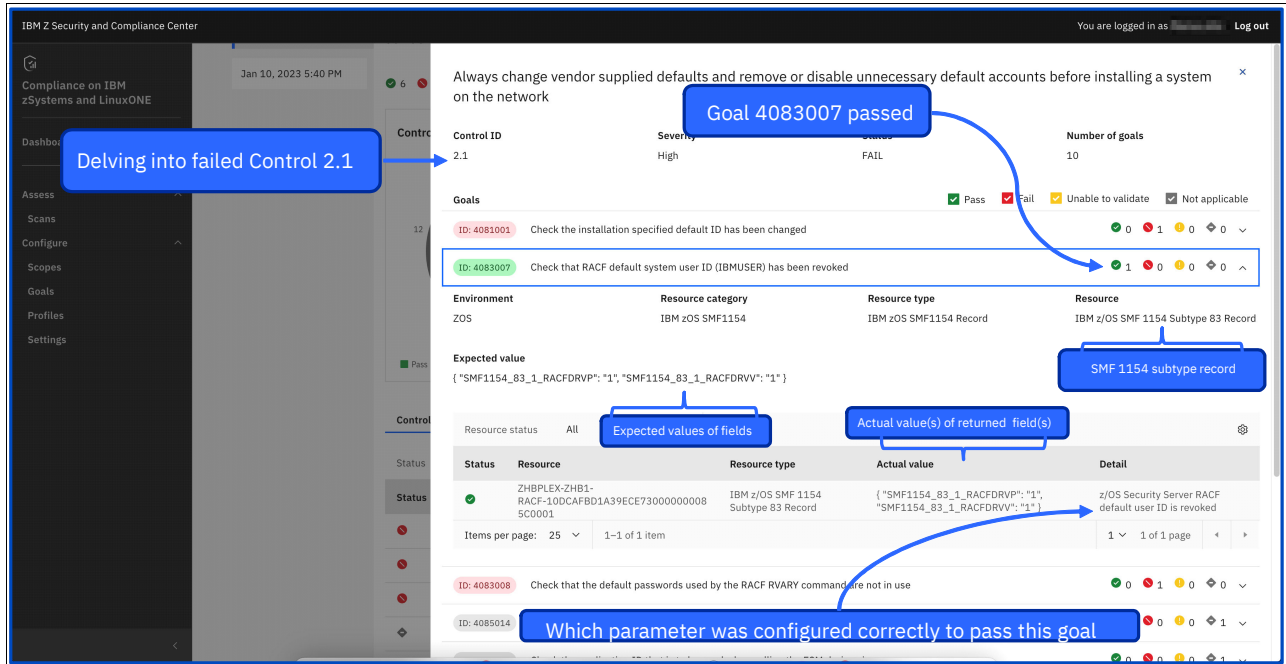


Figure A-2 A failed control with a passing goal showing that the expected configuration was applied correctly

Now, you delving into the failing goals and understand what you must remediate to pass and strengthen your security or compliance posture.

The first goal that failed (Goal ID 4083001), which stipulates that your Db2 subsystem should not be using the default-supplied installation user ID “IBMUSER” (it should be changed after the installation process completes). Even though you revoked this user ID, all usage of this user ID should be discontinued. In a scenario where you kept the “IBMUSER” as the default user ID for your Db2 installation by omission, a simple RACF **RESUME** of this user ID by a malicious user results in open access to your Db2 subsystem and the data in it.

The second failed goal (Goal ID 4083008), which verifies that the RACF **RVARY** default password should have been changed, fails. This situation is a highly sensitive oversight because the **RVARY** command can switch, activate, or deactivate RACF databases without an IPL, so a malicious user can bypass z/OS security that is enforced by RACF completely. For more information, see *z/OS Security Server RACF System Programmer's Guide*, SA23-2287.

Finding the suggested remedial area from a failed goal

While investigating the control failure, it is clearly shown which goals failed (see Figure A-4 on page 105). Furthermore, expanding a failed goal shows the actual values that are returned from the specific SMF 1154 record subtype, what was expected by IBM Z Security and Compliance Center to pass this goal, and hence what should be remediated to pass this goal and its derived control in the future.

IBM Z Security and Compliance Center also indicates what should be changed on the z/OS target system to remediate the compliance failure.

To continue the example of these failed goals, examine the details of Goal ID 4083001. When you expand this goal, you see that the returned value in SMF1154 subtype 81 indicates that Db2 runs with the IBM supplied default installation user ID “IBMUSER” still in effect. In this instance, any other value than “IBMUSER” is expected, but not in this situation.

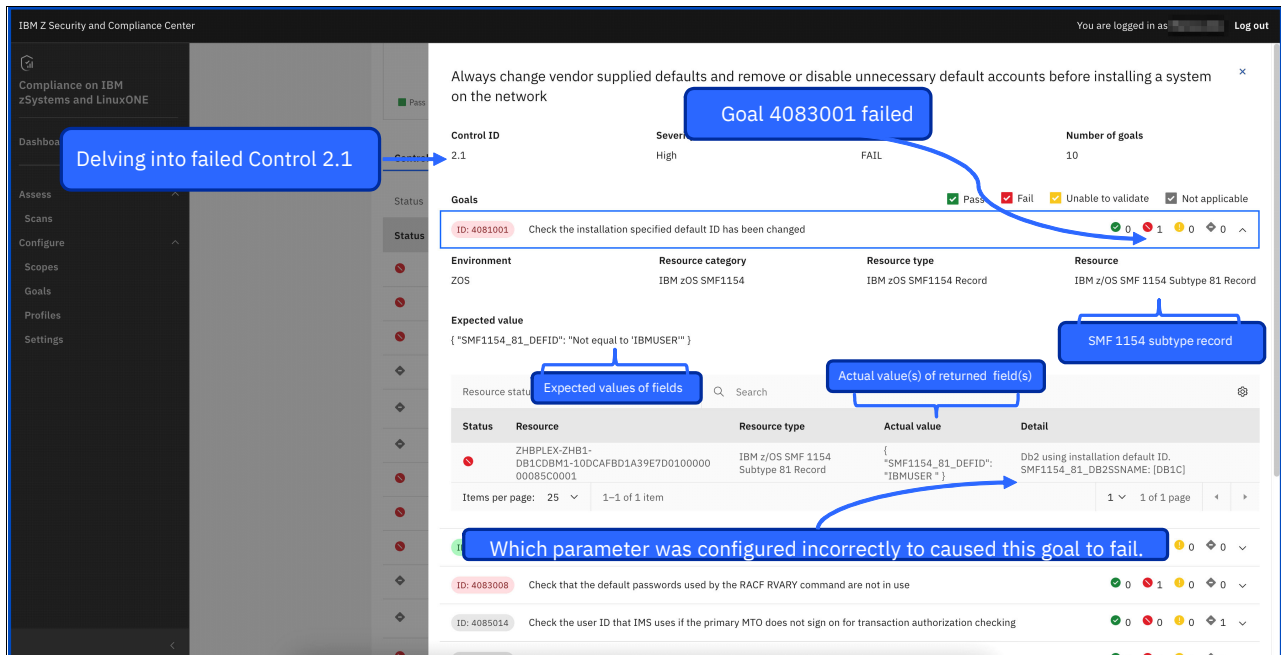


Figure A-3 Failing PCI DSS Control 2.1 with failing Goal ID 4083001

The second failing goal (Goal ID 4083008), which verifies that the RACF RVARy default password should have been changed, fails (see Figure A-4 on page 105).



SMF record type 1154 overview

IBM Z Security and Compliance Center uses SMF record type 1154 with its various subtypes that were introduced with z/OS V2R5. This appendix gives an overview of the different subtypes that are gathered by IBM Z Security and Compliance Center.

For more information, see *z/OS MVS System Management Facilities for Version 2 Release 5*, SA38-0667.

This appendix covers the following topics:

- ▶ “From where are records collected” on page 108
- ▶ “Application domain” on page 108
- ▶ “Storage domain” on page 109
- ▶ “Network domain” on page 111
- ▶ “z/OS domain” on page 112
- ▶ “Security domain” on page 114

From where are records collected

At a high level, SMF 1154 records are collected from the following domains in an IBM Z platform (see Table B-1).

Table B-1 SMF 1154 records: component domains

Application	Storage	Network	z/OS	Security
IBM CICS	DFSMSdfp	Communications Server	Console	RACF
IBM IMS	DFSMSRMM	TCP/IP	UNIX Systems Services	ICSF
IBM Db2	DFSMSHsm	FTP	SMF	CP Assist for Cryptographic Function (CPACF)
IBM MQ	DFSMSdss	TN3270E		
		CSSMTP		
		SSHD		
		InetD		

The following sections go into more detail about the information that is sent to IBM Z Security and Compliance Center through the SMF 1154 record subtypes (based on domain).

Application domain

The components in the application domain consist of CICS, IBM MQ, IMS, and Db2.

CICS

For CICS subtype 80, the following information in various sections is checked:

- ▶ *Section 1* of the record reflects the **SIT** options that are relevant to security:
 - **SEC=YES/NO**: Is CICS using an External Security Manager (ESM), such as RACF?
 - Identify the CICS default user.
 - **XUSER = YES/NO**: Is surrogate user checking done?
 - **RACFSYNC = YES/NO**: Does CICS listen to ENF 71 signals from RACF indicating changes to user and group profiles?
 - What CICS RACF classes are active?
 - Is security enforced on Transactions (XTRAN), Commands (XCMD), Files (XFCT), Programs (XPPT), Journals (XJCT), Temporary Storage queues (XTST), Transient Data Queues (XDCT), and so on?

- ▶ *Section 2* of the record contains the region usage tags.
With CICS region tagging, you can identify the region based on the CICS APPLID, the CICS region user ID, and job name for the region. Tagging enables the unique identification and grouping of CICS regions into functional groups, making it easier for auditors to determine a region's relevancy and usage.
- ▶ *Section 3* of the record contains the CICS service level. The most recent maintenance (PTFs or APARs) for the region are listed.
- ▶ *Section 4* of the record contains the CICS resources. This section is optional and lists active resources that are not conformant.

IBM MQ

For IBM MQ subtype 82, the security profiles that are defined for IBM MQ, that is, whether security is enforced for subsystem, channels, processes, queues, and so on, are checked.

IMS

For IMS subtypes 85, 86, and 87, the following items are checked:

- ▶ IMS Control region name and security parameters
- ▶ IMS Connect client name and security parameters
- ▶ IMS Operations Manager's command protection settings

Db2

For Db2 subtype 81, the following items are checked:

- ▶ Db2 subsystem name and the default user ID.
- ▶ How security is granted to users (for example, RACF with no security), and how admin authority is granted.

Storage domain

The components in the storage domain consist of DFSMSdfp, DFSMSRMM, DFSMSHsm, and DFSMSdss. These components are part of DFSMS, which is the z/OS component that helps you manage your z/OS attached Storage.

- ▶ DFSMSdfp controls data, DASD, and tape storage for the operating system. It acts as a link between the processor and connected storage devices to provide management utilities.
- ▶ DFSMSdss provides data movement utilities to help with moving or copying data between volumes. It also manages space, backup, and recovery.
- ▶ DFSMSHsm helps with backup and recovery during disaster recovery or archiving of data for optimal DASD space management.
- ▶ DFSMSRmm manages removable data, such as tapes or optical disks.

DFSMSdfp

For DFSMSdfp Subtype 51, the following items are checked:

- ▶ From a RACF perspective, **SETROPTS** parameters like **PROTECTALL**, **EGN**, **TAPEDSN**, **RETPD**, **ADSP**, **REALDSN**, **OPERAUDIT**, **SAUDIT**, **WHEN(PROGRAM)**, and others are checked.
- ▶ Certain classes are checked to see whether they are active, such as DATASET, FACILITY DASDVOL, TAPEVOL, and CSFKEYS.
- ▶ Some specific profiles are checked:
 - STGADMIN.DPDSRN.dsname
 - STGADMIN.IDC.other, STGADMIN.IDC.other
 - STGADMIN.IFG.other
 - STGADMIN.IFG.READVTOC.volser
 - STGADMIN.IGD.ACTIVATE.CONFIGURATION
 - STGADMIN.IGG.ALTER.SMS
 - STGADMIN.IGG.CATALOG.SECURITY.CHANGE
 - STGADMIN.IGG.DEFDEL.UALIAS
 - STGADMIN.IGG.DELGDG.FORCE
 - STGADMIN.IGWSHCDS.other
 - FACILITY STGADMIN.IGG.CATALOG.SECURITY.BOTH
 - STGADMIN.ICK.other
 - STGADMIN.IDC.DCOLLECT
 - FACILITY STGADMIN.IDC.DCOLLECT.xxxxxxxx
 - FACILITY IDA.VSAMEXIT.xxxxxxxx
 - OPERCMDS MVS.MODIFY.STC.CATALOG.CATALOG.SECURE
 - OPERCMDS MVS.MODIFY.STC.CATALOG.CATALOG.SECURE

DFSMSRMM

For DFSMSRMM Subtype 52, the following items are checked:

- ▶ Certain classes are checked to see whether they are active, such as e TAPEDSN, RETPD, and TAPEVOL.
- ▶ Some specific profiles are checked:
 - FACILITY STGADMIN.EDG.VRS
 - FACILITY STGADMIN.EDG.MASTER
 - FACILITY STGADMIN.EDG.RESET.SSI
 - FACILITY STGADMIN.EDG.INERS.WRONGLABEL
 - FACILITY STGADMIN.EDG.LIST
 - FACILITY STGADMIN.EDG.VRS
- ▶ In DEVSUPxx, some items are checked:
 - TAPEAUTHDSN
 - TAPEAUTHF1
 - TAPEAUTHRC4
 - TAPEAUTHRC8
- ▶ In EDGRMxx, some items are checked:
 - OPMODE
 - MASTEROVERRIDE
 - TPRACF
 - BLP
 - EDM
 - SMFAUD

- SMFSEC
- Hardware Security Module (HSM)

DFSMSHsm

For DFSMSHsm Subtype 53, the items that are checked include some of the following specific profiles:

- ▶ FACILITY STGADMIN.ARC.ADDVOL
- ▶ FACILITY STGADMIN.ARC.ARECOVER
- ▶ FACILITY STGADMIN.ARC.AUTH
- ▶ FACILITY STGADMIN.ARC.CANCEL
- ▶ FACILITY STGADMIN.ARC.BDELETE
- ▶ FACILITY STGADMIN.ARC.FRDELETE
- ▶ FACILITY STGADMIN.ARC.DELETE
- ▶ FACILITY STGADMIN.ARC.FIXCDS
- ▶ FACILITY STGADMIN.ARC.LIST
- ▶ FACILITY STGADMIN.ARC.other
- ▶ FACILITY STGADMIN.ARC.PATCH
- ▶ FACILITY STGADMIN.ARC.QUERY
- ▶ FACILITY STGADMIN.ARC.RECOVER.NEWNAME
- ▶ FACILITY STGADMIN.ARC.REPORT
- ▶ FACILITY STGADMIN.ARC.SETSYS
- ▶ FACILITY STGADMIN.ARC.STOP

DFSMSdss

For DFSMSdss Subtype 54, the items that are checked include some of the following profiles:

- ▶ FACILITY STGADMIN.ADR.STGADMIN.other
- ▶ FACILITY STGADMIN.DMO.CONFIG
- ▶ FACILITY STGADMIN.ADR.STGADMIN.COPY
- ▶ FACILITY STGADMIN.ADR.STGADMIN.DUMP
- ▶ FACILITY STGADMIN.ADR.STGADMIN.DUMP.DELETE
- ▶ FACILITY STGADMIN.DMO.other
- ▶ FACILITY STGADMIN.ADR.STGADMIN.COPY.DELETE
- ▶ FACILITY STGADMIN.ADR.other
- ▶ FACILITY STGADMIN.ADR.STGADMIN.PRINT
- ▶ FACILITY STGADMIN.ADR.STGADMIN.COPY.RENAME
- ▶ FACILITY STGADMIN.ADR.STGADMIN.RESTORE
- ▶ FACILITY STGADMIN.ADR.STGADMIN.RESTORE.RENAME
- ▶ FACILITY STGADMIN.ANT.other

Network domain

The component in the network domain is z/OS Communications Server (TCP/IP, TN3270E, CSSMTP, FTP, SSHD, and InetD). The subtypes are as follows:

- ▶ For Subtype 01, TCP/IP items that are checked include some of the following items:
 - The date and time that the TCP/IP stack started
 - SYSPLEX group name
 - IPv6 configuration information

- IPv4 configuration information
- TCP configuration information, for example:
 - AT and Transport Layer Security (TLS) active
 - Port range
 - UDP configuration information
 - Global configuration information
 - Port configuration information
 - Management configuration information
 - Network access configuration information
- ▶ For Subtype 02, FTP items that are checked include some of the following items:
 - FTP daemon general configuration section
 - FTP daemon configuration data section
- ▶ For Subtype 03, TN3270E items that are checked include some of the following items:
 - TN3270E Telnet server TelnetGlobals section
 - Common parameters
 - TN3270E Telnet server TelnetParms section
 - TN3270E Telnet Server ParmsGroup section
 - Client ID structure
 - TN3270E Telnet Server ParmsMap section
 - TN3270E Telnet Server LUMap section
 - TN3270E Telnet Server PrtMap section
 - TN3270E Telnet Server Restrict Appl section
- ▶ For Subtype 04, CSSMTP, items that are checked include some of the following items:
 - CSSMTP identification section
 - CSSMTP configuration section
 - CSSMTP target server section
 - CSSMTP configuration data section
- ▶ For Subtype 78, SSHD items that are checked include some of the following items:
 - Protocol version
 - Ciphers
 - Mac algorithms
- ▶ For Subtype 79, INDETD items that are checked include some of the following items:
 - Service
 - Protocol
 - Socket
 - User ID

z/OS domain

The components in the z/OS domain consist of Console, UNIX Systems Services, and SMF.

Console

For Console subtype 50, items that are checked include some of the following items:

- ▶ Whether a logon is required.
- ▶ The user ID of the logged-on console.
- ▶ Whether the console was from NetView, TSO, or CICS.
- ▶ The default group of the console logon.

UNIX Systems Services

For UNIX Systems Services subtype 77, items that are checked include some of the following ones:

- ▶ Various parameters in BPXPRMxx
- ▶ Startup Proc
- ▶ Superuser
- ▶ TTYGROUP
- ▶ Whether a logon is required
- ▶ Various RACF profiles:
 - FACILITY BPX.CONSOLE
 - FACILITY BPX.CF
 - FACILITY BPX.MAP
 - FACILITY BPX.SHUTDOWN
 - FACILITY BPX.UNLIMITED.OUTPUT
 - FACILITY BPX.JOBNAME
 - FACILITY BPX.STOR.SWAP
 - FACILITY BPX.DAEMON
 - FACILITY BPX.DAEMON
 - FACILITY BPX.DAEMON.HFSCCTL
 - FACILITY BPX.FILEATTR.APF
 - FACILITY BPX.FILEATTR.PROGCTL
 - FACILITY BPX.FILEATTR.SHARELIB
 - FACILITY BPX.POE
 - FACILITY BPX.STICKYSUG.pppppppp
 - FACILITY BPX.SUPERUSER
 - FACILITY BPX.SERVER
 - FACILITY BPX.SERVER
 - FACILITY BPX.DAEMON.other
 - FACILITY BPX.DEBUG
 - FACILITY BPX.other
 - FACILITY BPX.SMF
 - FACILITY BPX.WLMSEVER
 - UNIXPRIV SUPERUSER.FILESYS.DIRSRCH
 - UNIXPRIV SUPERUSER.FILESYS
 - UNIXPRIV SUPERUSER.FILESYS
 - UNIXPRIV SUPERUSER.FILESYS
 - UNIXPRIV SUPERUSER.FILESYS.CHOWN
 - UNIXPRIV CHOWN.UNRESTRICTED
 - UNIXPRIV SUPERUSER.PROCESS.GETPSENT
 - UNIXPRIV SUPERUSER.PROCESS.KILL
 - UNIXPRIV SUPERUSER.FILESYS.PFSCCTL
 - UNIXPRIV SUPERUSER.SETPRIORITY
 - UNIXPRIV SUPERUSER.FILESYS.MOUNT
 - UNIXPRIV SUPERUSER.FILESYS.MOUNT
 - UNIXPRIV SUPERUSER.PROCESS.PTRACE
 - UNIXPRIV SUPERUSER.FILESYS.QUIESCE
 - UNIXPRIV SUPERUSER.FILESYS.VREGISTER
 - UNIXPRIV SUPERUSER.FILESYS.CHANGEPERMS
 - UNIXPRIV SHARED.IDS
 - UNIXPRIV SUPERUSER.other
 - UNIXPRIV SUPERUSER.IPC.RMID

- UNIXPRIV SUPERUSER.FILESYS.USERMOUNT
- UNIXPRIV SUPERUSER.FILESYS.USERMOUNT

SMF

For SMF subtypes 96 and 97, some items that are checked include the following ones:

- ▶ SMFPRMxx member (for example, TSO, SYS, or STC)?
- ▶ Are records being signed?
- ▶ Log streams?

Security domain

The components in the security domain consist of RACF, ICSF, and CPACF.

RACF

In the RACF subtype 83, some information is collected on basic **SETROPTS** commands. Here are some examples of the checks that are made during an IBM Z Security and Compliance Center scan:

- ▶ Are the following parameters active: **SAUDIT**, **CMDVIOL**, and **OPERAUDIT**?
- ▶ Parameters that are related to passwords, for example:
 - Mixed case.
 - Special characters.
 - Password interval.
 - Password algorithm (legacy or KDFAES).
 - Are **RVAR**y passwords the default?
- ▶ Is RACF in **PROTECTALL FAIL**?
- ▶ Is **ERASE(ALL)** active?
- ▶ Is the ACEECHK class active and RACLISTed?
- ▶ Is IBMUSER revoked?

Select system critical libraries like APF libraries; data sets that are used by RACF; and PARMLIB data sets and LINKLIB data sets. List whether there was UACC, or ID(*) checks the audit values.

ICSF

For ICSF the subtype 49, there are checks for some of the following information:

- ▶ ICSF - Class profiles access section:
 - Is RACF in **PROTECTALL** mode?
 - Is the XFACILIT class active and RACLISTed?
 - Are the following profiles defined:
 - CSF.CKDS.TOKEN.CHECK.LABEL.WARN
 - CSF.CKDS.TOKEN.CHECK.LABEL.FAIL
 - CSF.PKDS.TOKEN.CHECK.LABEL.WARN
 - CSF.PKDS.TOKEN.CHECK.LABEL.FAIL
 - CSF.CKDS.TOKEN.CHECK.DEFAULT.LABEL
 - CSF.PKDS.TOKEN.CHECK.DEFAULT.LABEL
 - CSF.CKDS.TOKEN.NODUPLICATES

- CSF.PKDS.TOKEN.NODUPLICATES
 - CSF.XCSFKEY.ENABLE.AES
 - CSF.XCSFKEY.ENABLE.DES
 - CSF.CSFKEYS.AUTHORITY.LEVELS.WARN
 - CSF.CSFKEYS.AUTHORITY.LEVELS.FAIL
 - CSF.KDS.KEY.ARCHIVE.USE
 - CSF.KDS.KEY.ARCHIVE.DATA.DECRYPT
 - CSF.KGUP.CSFKEYS.AUTHORITY.CHECK
 - CSF.CSFKEYS.ECC.PRIVATEKEYNAME.ENABLE
 - Various AUDITKEYLIFECKDS – Label / TOKENS(LABEL())
 - Various AUDITKEYLIFECPKDS – Label / TOKENS(LABEL())
 - Various AUDITKEYLIFETKDS – Label / TOKENS(LABEL())
 - AUDITKEYUSGCKDS(LABEL()) / Tokern
 - AUDITKEYUSGPKDS(LABEL())
 - AUDITPKCS11USG(TOKENOBJ())
- If defined, what format is the CKDS?
 - If defined, what format is the PKDS?
 - If defined, what format is the TKDS?
- ▶ ICSF – Label Access controls section:
 - Is the CSFSERV, CSFKEYS, CRYPTOZ, or XCSFKEYS class active and RACFlisted?
 - Is the profile in WARN mode?
 - Is ID(*) defined?
 - What ID defined for the UACC?
 - What are the data set profiles protecting the KDS?
 - Is the profile in WARNING mode? What is defined for ID(*)? What is defined for UACC?
 - ▶ ICSF – KDS – access control section
 - ▶ ICSF – Algorithm Data – Check for weak algorithms:
 - AES 128, 192, or 256?
 - DES 112, 168, or 56?
 - RSA 1024 or 2048?
 - SHA 512 or 224?

CPACF

CPACF counters provide evidence for compliance through subtype 128, which includes hardware encryption services to z/OS components and applications, such as:

- ▶ A cryptography algorithm helps determine the strength of the algorithm.
- ▶ The frequency of cryptography is used to help derive performance information.
- ▶ Proof of change is used to show modifications to the configuration.

Abbreviations and acronyms

CEA	Common Event Adapter	SOX	Sarbanes-Oxley Act
CIS	Center for Internet Security	SPI	sensitive personal information
CISO	Chief Information Security Officer	TLS	Transport Layer Security
COBIT	Control Objectives for Information and Related Technologies	UI	user interface
CPACF	CP Assist for Cryptographic Function	VM	virtual machine
EAV	extended address volume		
ENF	Event Notification Facility		
ESM	External Security Manager		
FIXCAT	fix category		
GDPR	General Data Protection Regulation		
HIPAA	Health Insurance Portability and Accountability Act		
HSM	Hardware Security Module		
IBM	International Business Machines Corporation		
IBM zCIM	IBM z/OS Compliance Integration Manager		
IBM zCX	IBM z/OS Container Extensions		
IBM zEDC	IBM zEnterprise Data Compression		
IBM z/OSMF	IBM z/OS Management Facility		
IFL	Integrated Facility for Linux		
IoT	Internet of Things		
ISO	International Organization for Standardization		
JSON	JavaScript Object Notation		
KEK	key-encrypting key		
LPAR	logical partition		
NIST	National Institute of Standards and Technology		
OSA	Open Systems Adapter		
PCI DSS	Payment Card Industry Data Security Standard		
PID	product ID		
PII	personal identifiable information		
RHCOS	Red Hat Enterprise Linux CoreOS		
RHEL	Red Hat Enterprise Linux		
RPI	Rensselaer Polytechnic Institute		
SAF	System Authorization Facility		
SLES	SUSE Linux Enterprise Server		
SME	subject matter expert		

Redbooks

Keeping Up With Security and Compliance on IBM Z

(0.2"spine)
0.17" x 0.473"
90 x 249 pages



SG24-8540-00

ISBN 0738461172

Printed in U.S.A.

Get connected

