

zSCC - Overview

Today's business operate in an ever-changing and complex regulatory environment



61%

of organizations experienced a compliance lapse or violation in the past three years¹

\$2.3M

cost difference for breaches with high vs. low level of compliance failures²



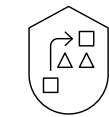
Significant Cost

Huge effort in maintaining, updating and adding new processes for compliance



Risk and Uncertainty

Susceptible to human error and uncertainty in business risk profile due to non-compliance

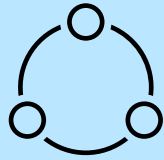


Complexity

Satisfying auditor's demands requires stitching together data from multiple sources

^{1,2}See sources in notes

The process can be challenging



Interpreting Requirements

Typically, requirements are written with distributed frameworks in mind. The responsibility to understand those requirements is up to the Line of Business (LoB) Owners, who also need to remain current with updates and changes that occur



Evidence Collection

Manually extracting configuration data and storing it in spreadsheets or distributed databases comes with many challenges including system changes, script management, missing data, etc...



Demonstrating Posture

A point in time audit report of the IBM Z platform posture for a CISO or Auditor can take weeks or months. The prolonged duration can undermine the accuracy of the final report.

“The biggest challenge that we have ... is gathering evidence for compliance” - CISO

IBM z16 is built to build

We built a powerful and secure platform for business.
Let's build the future of yours.



Predict and Automate for
Increased Decision Velocity



Secure with a Cyber Resilient
System

***Address ever-increasing
regulations with automation for
compliance leveraging the IBM Z
Security and Compliance Center***

© 2022 IBM Corporation



Modernize with
Hybrid Cloud

IBM Z Security and Compliance Center



A modern application specifically designed for progressing towards a state of continuous compliance readiness with over 300 pre-built goal validations and customizability.

→ Optimize Resources

Automates the collection and validation of facts against goals to help increase visibility into potential compliance oversights and reduce manual errors.

→ Assess Compliance Posture

Interactive dashboard provides a view of current compliance posture for PCI-DSS and NIST SP800-53 regulations to help simplify audit preparations and improve continuous compliance operations.

→ Identify Compliance Drift

Track compliance drift over time with dashboard style visualizations which display historical compliance scores, to help clients better understand their compliance posture

Reduce number of skilled resources needed for audit preparation functions by over 40%¹

Reduce audit preparation time from one month to one week²

1,2 See claims in notes

IBM z16 manages compliance at the enterprise level



IBM Z Security and Compliance Center

Security and Compliance Management

Driven by triggered evidence collection controls, Interpretation, implementation and validation of regulatory controls on IBM Z / LinuxONE



CISO / CIRO



System Engineer



Auditor

Policy-based control
Evidence collection across the IBM z16
stack Visibility of compliance posture



IBM z16 /
LinuxONE
Controls
Implementations

Hardware Specific
Controls



Runtime Controls Implementation



Operating System
Controls



Middleware Controls



Network Security
Controls



Data Security
Controls



Audit and Monitoring
Controls

IBM Z Security and Compliance Center dashboard



IBM Z Security and Compliance Center You are logged in as Admin [Log out](#)

Z Security and Compliance... / Scans / [Details](#)

PCI Review

PCI_DSS_SCOPE | PCI_DSS 3.2.1 | Validation

Mar 16, 2022 1:10 PM

Feb 16, 2022 1:10 AM

Jan 16, 2022 1:10 AM

Dec 16, 2021 1:10 AM

March 16, 2022 1:10 PM

35 Pass 11 Fail 1 Unable to perf... 0 Not applicable

Controls

47 Total controls

Failures

Drift over time

[Download report](#)

Control view
Resource view

Status Filter... Severity Filter... Search

Status	ID	Control	Severity	Resource details
Fail	1.1	Ensure the Appropriate Version/Patches for Oracle Software Is Installed	Critical	0 Pass 1 Fail 0 Unable to perf... 0 Not applicable
Fail	2.1.1	Ensure 'extproc' Is Not Present in listener config	Medium	0 Pass 1 Fail 0 Unable to perf... 0 Not applicable
Unable to perform	2.1.2	Ensure 'ADMIN_RESTRICTIONS' is set to 'ON'	-	0 Pass 0 Fail 1 Unable to perf... 0 Not applicable
Pass	2.2.1	Ensure 'AUDIT_SYS_OPERATIONS' Is Set to 'TRUE'	-	1 Pass 0 Fail 0 Unable to perf... 0 Not applicable
Pass	2.2.2	Ensure 'AUDIT_TRAIL' Is Set to 'OS', 'DB', 'XML', 'DB,EXTENDED', or 'XML,EXTENDED'	-	1 Pass 0 Fail 0 Unable to perf... 0 Not applicable
Fail	2.2.3	Ensure 'GLOBAL_NAMES' Is Set to 'TRUE'	Medium	0 Pass 1 Fail 0 Unable to perf... 0 Not applicable

IBM Z Security and Compliance Center

Aligned to client goals

Prepare for a current audit

Do you need to collect evidence for an audit?

Mitigate the risk of breach

Compliance oversights can amplify the cost of potential breaches. IT environments are more complex which increases the risk. Are you prepared?

Establish compliance as a priority

Are you increasing investment and adoption of more compliance products and services?

Shift from operating to innovation

Are highly specialized skills stuck with managing recurring audit functions?

Move from collection to observation

Do you feel there is more attention on the collection of compliance data rather than focusing on the current posture?



RACF Analyst

SETR
DSMON



Storage admin

DFP, SMS, RMM,
HSM DSS
Security
Parameters



MQ Administrator

MQ Security
Parameters



Crypto

ICSF
Security
Parameters



z/OS Systems Programmer

z/OS Settings
USS
Console
SMF



**Auditor /
Compliance /
Risk**

Request
z/OS
Security Reports



**Comm
Server**

FTP, TCP/IP, CSSMTP,
TN3270E, SSHD, INETD
Security Parameters



**CICS
Systems
Programmer**

CICS
Security
Parameters



Db2 DBA

Db2 Security
Parameters



IMS DBA

IMS
Security
Parameters



**Hardware
CPACF**

Algorithms
In Use

Now you are ready for that compliance review!



1
0

But wait. . . What if . . .

Z Security and Compliance Center

CICS
Security
Parameters

SETR
DSMON

DFP, SMS, RMM,
HSM DSS
Security
Parameters

FTP, TCP/IP, CSSMTP,
TN3270E, SSHD, INETD
Security Parameters

z/OS Settings
USS
Console
SMF

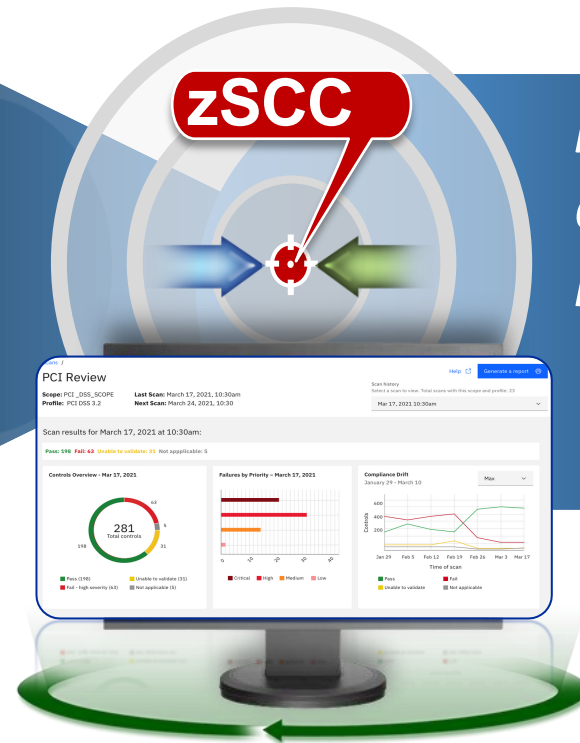
ICSF
Security
Parameters

Db2 Security
Parameters

IMS
Security
Parameters

MQ Security
Parameters

Algorithms
In Use



NIST SP 800-53

CIS

PCI DSS



Payment Card Industry Data Security Standard (PCI-DSS) 4.0

Applicable to all entities that store, process, and/or transmit cardholder data.

Typical clients:

- Banking
- Financial
- Insurance
- Retail
- Mortgage



National Institute of Standards & Technology (NIST) SP 800-53

Applicable to all US federal government agencies and contractors; referenced by local governments and private industry regulations such as PCI-DSS.

Typical clients:

- Federal govt
- State / local govt



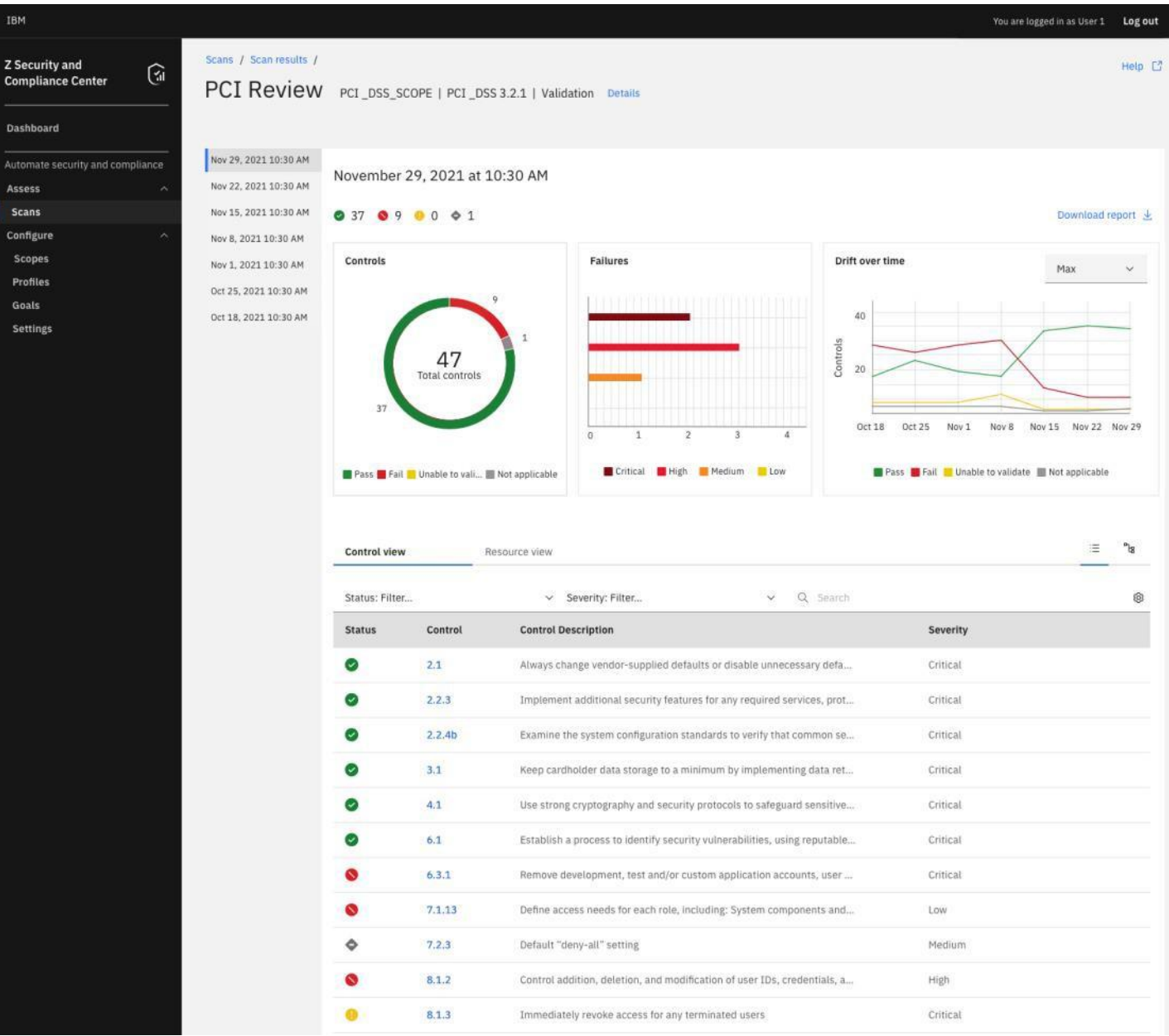
Center of Internet Security (CIS) Benchmarks

Applicable to organizations in all industries and geographies including government, business, industry and academic institutions.

Typical clients:

- Banking
- Financial
- Insurance
- Retail
- Mortgage
- Federal govt
- State / local govt

IBM Z Security and Compliance Center



Compliance Posture Management with a browser-based dashboard experience

- Generate detailed reports to enable executives, administrators, and auditors to understand compliance metrics with ease
- Track compliance drift over time

System Generated Facts

- Fact collection from IBM Z stack (z/OS and Linux on Z)
- Crypto Usage Tracking (CPACF and ICSF)

Industry Standard Readiness

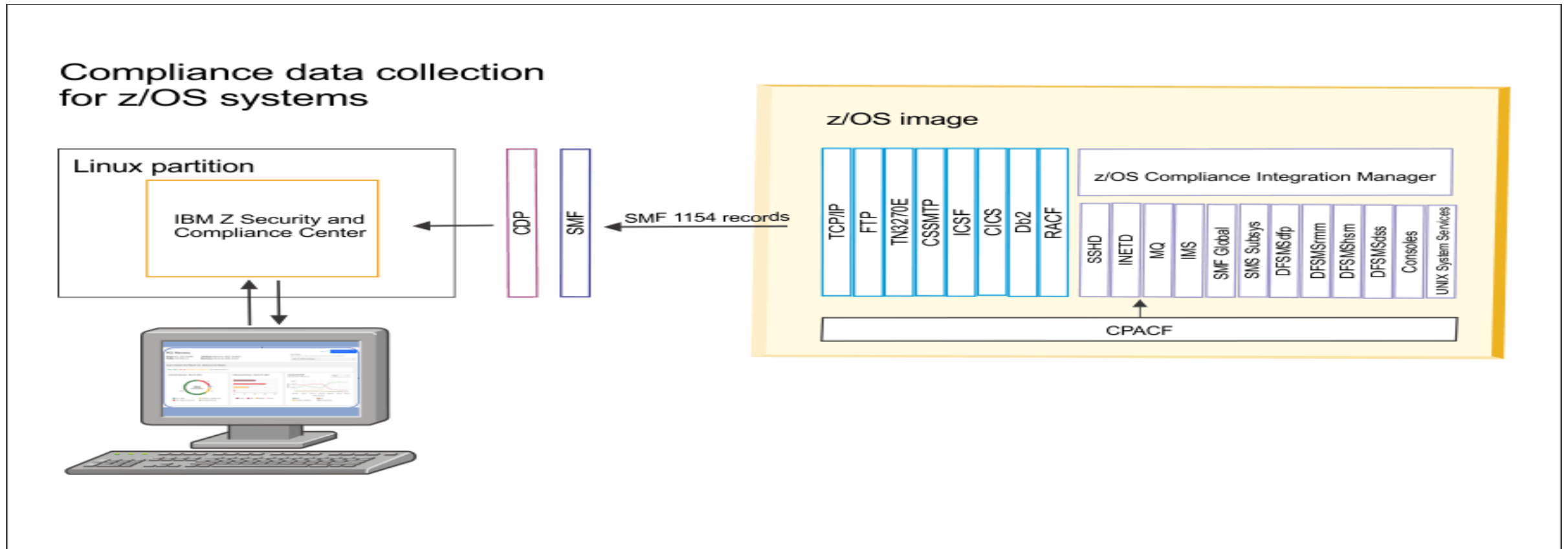
- Pre-defined profiles for PCI DSS , NIST SP800-53, CIS Benchmarks (subset of controls initially)



IBM Security
 IBM Cloud
 IBM Research
 IBM Z

IBM Z Security & Compliance Center collectors connect to a resource, such as z/OS or Linux on Z, and scan for compliance data. For z/OS, the collector connects to a z/OSMF compliance REST API which triggers sysplex-wide compliance data collection using an ENF86 signal.

Participating z/OS components and products listen for the new ENF86 signal. When received, these components write compliance data to SMF 1154 records associated with a unique subtype. The SMF records are streamed to IBM Z Security & Compliance Center using the Common Data Provider. Then, the IBM Z Security & Compliance Center maps the compliance data to the appropriate regulatory controls associated with a profile for validation, display and reporting.

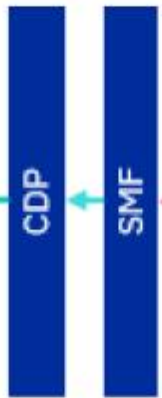


Red Hat OpenShift Container Platform

Scan z/OS Systems



5

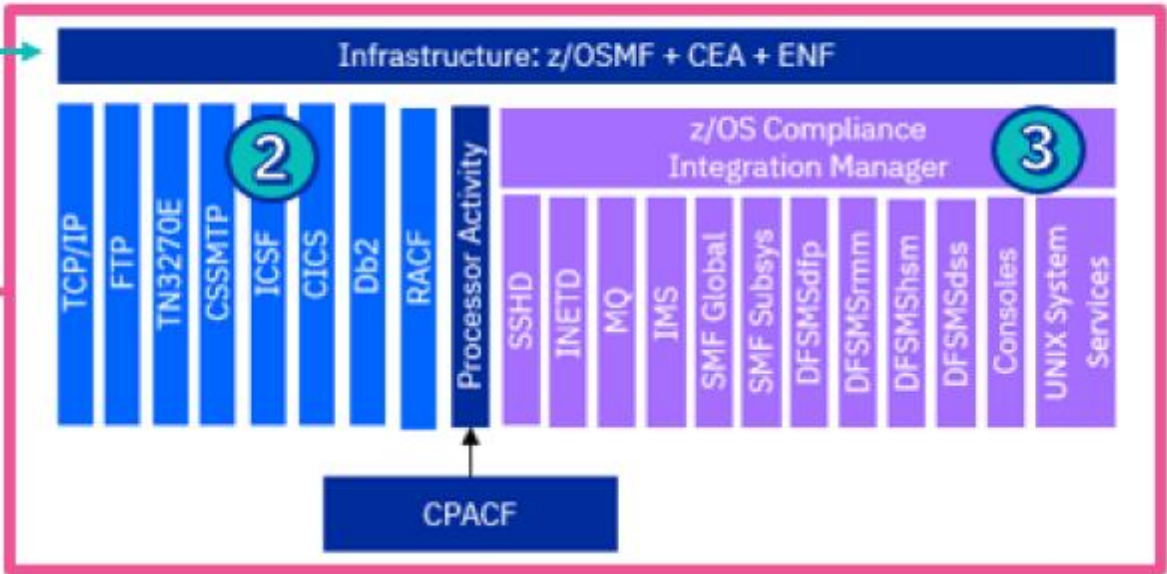


SMF1154

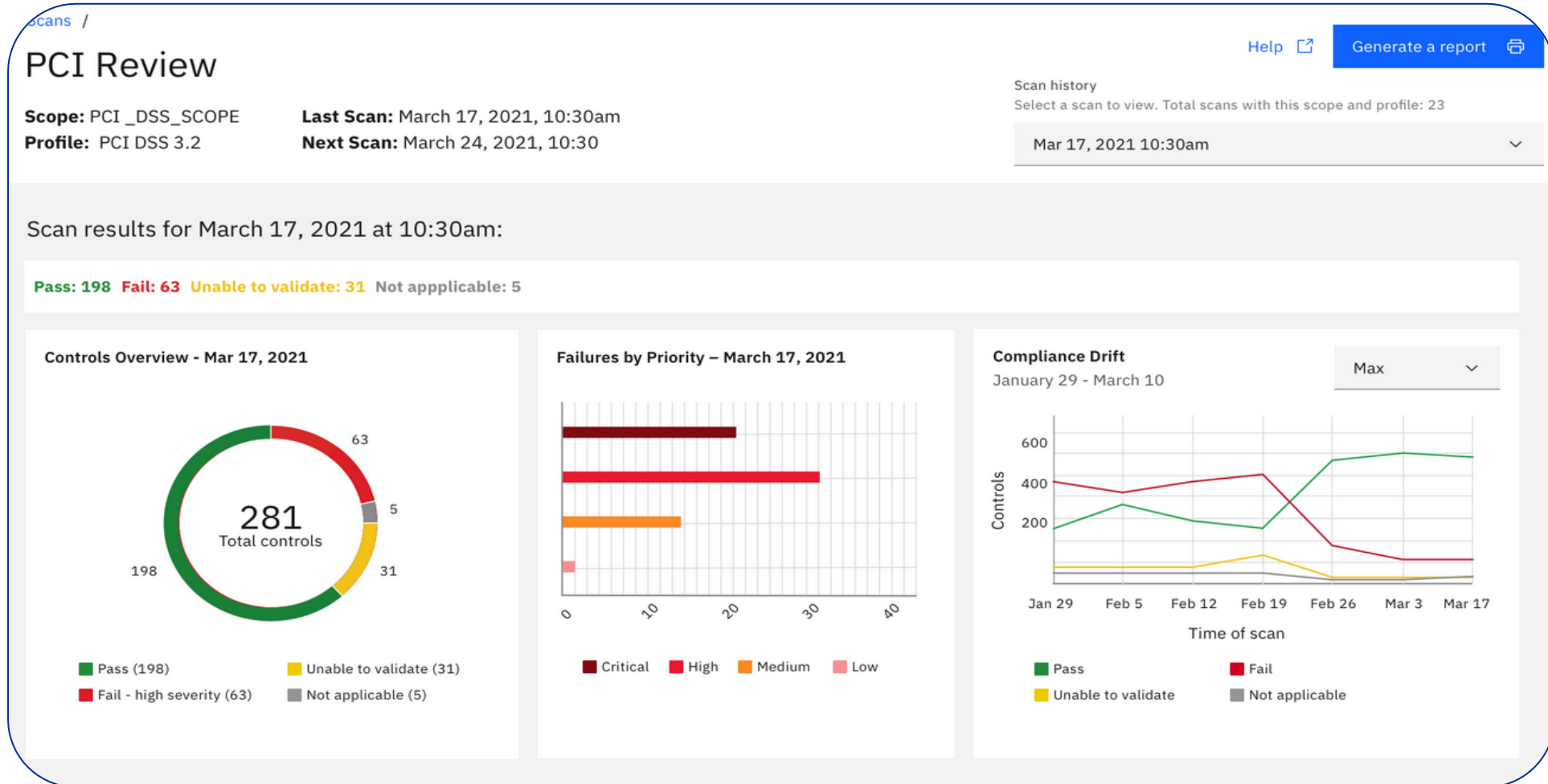
4

1

z/OS



Combined Report



Multiple Dates

Apr 6, 2023 1:58 PM

Apr 6, 2023 8:25 AM

Apr 6, 2023 7:52 AM

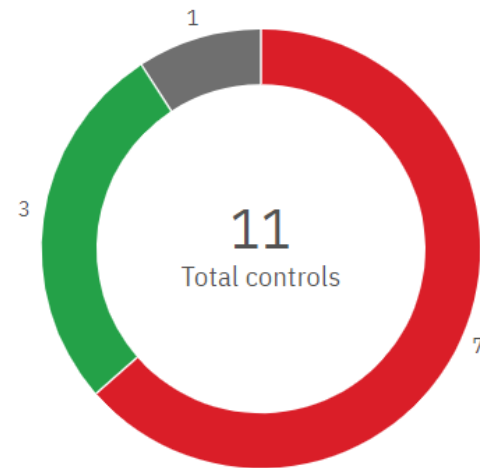
Mar 28, 2023 1:17 PM

April 6, 2023 1:58 PM

✓ 3 ✗ 7 ! 0 ⚡ 1

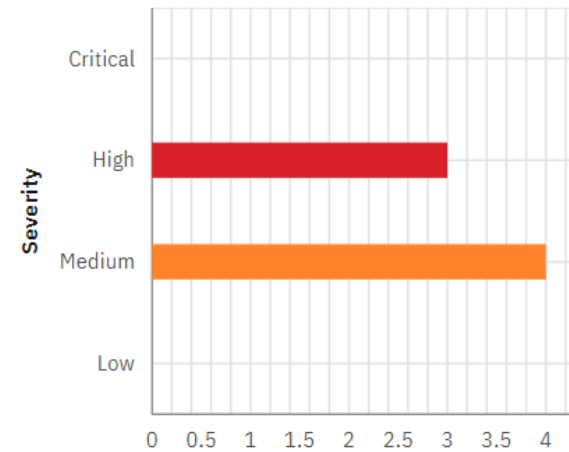
[Download report](#) ↓

Controls



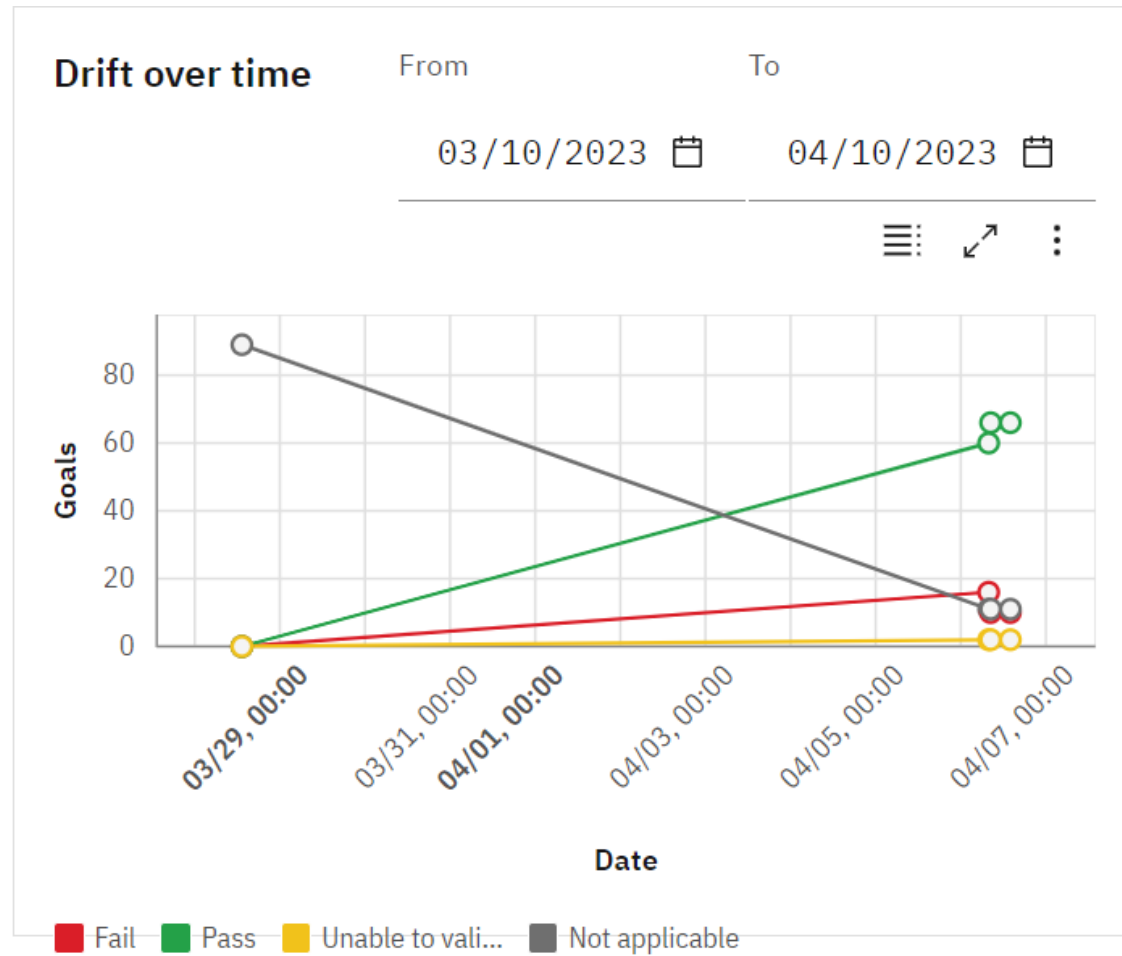
■ Pass ■ Fail ■ Unable to vali... ■ Not applicable

Failures



■ Critical ■ High ■ Medium ■ Low

Drift Over Time



Run History

ZHBPLEX

Systems in the ZHBPLEX Sysplex

More info

Event history

Event history

Type

All



Search



Event time	Type	Status message	Status
2023-04-06 6:00 PM	Validation	Validation completed	✓
2023-04-06 1:47 PM	Validation	Validation completed	✓
2023-04-06 8:14 AM	Validation	Validation completed	✓
2023-04-06 7:41 AM	Validation	Validation completed	✓
2023-03-28 1:07 PM	Validation	Validation completed	✓
2023-03-28 1:04 PM	Discovery	Discovery completed	✓
2023-03-28 1:03 PM	Discovery	Discovery completed	✓

Custom Report











Status	ID	Control	Severity	Resource details
	8.2.2	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis	-	1 0 0 0
	8.2.4	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed	Medium	1 1 0 0
	8.2.5	Access for terminated users is immediately revoked	Medium	1 1 0 0
	8.2.6	Inactive user accounts are removed or disabled within 90 days of inactivity	Medium	1 1 0 0
	8.2.8	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session	Medium	4 5 1 0
	8.3.1	All user access to system components for users and administrators is authenticated	High	0 1 0 0
	8.3.2	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components	High	63 1 1 0
	8.3.4	Invalid authentication attempts are limited	-	1 0 0 0
	8.3.6	If passwords/passphrases are used as authentication factors, they meet the following minimum level of complexity	High	3 1 0 0

z/OS Profiles

Profiles

[View docs](#) 

A profile is a collection of related controls. After you gather the configuration information of your resources and prepare your systems for scanning, you can create profiles to define the list of controls that you'd like to validate against.

Type: All 	 zos 		Create 	
Name	Description	Type	Controls	
CIS v8 for zOS	CIS Critical Security Controls v8 for zOS	Predefined	23	
Custom PCI DSS	Custom profile based on PCI DSS 4.0 for zOS	Custom	11	
NIST SP 800-53 R4 for zOS	NIST Security and Privacy Controls 800-53 Rev. 4 for zOS	Predefined	48	
PCI DSS 3.2.1 for zOS	PCI DSS 3.2.1 for zOS	Predefined	57	
PCI DSS 4.0 for zOS	PCI DSS 4.0 for zOS	Predefined	48	

NIST SP 800-53

NIST SP 800-53 – Web View

NIST SP 800-53 R4 for zOS

ID	Description
✓ AC	Access Control
✓ AU	Audit and Accountability
✓ CM	Configuration Management
✓ IA	Identification and Authentication
✓ MA	Maintenance
✓ PS	Personnel Security

NIST SP 800-53 – Web View

NIST SP 800-53 R4 for zOS

ID	Description
^ AC	Access Control
v AC-2: Account Management	
v AC-3: Access Enforcement	
v AC-6: Least Privilege	
v AC-7: Unsuccessful Logon	
v AC-11: Session Lock	
v AC-12: Session Termination	
v AC-16: Security Attributes	
v AC-17: Remote Access	

NIST SP 800-53 – Web View

NIST SP 800-53 R4 for zOS

ID	Description
^ AC	Access Control
^ AC-2: Account Management	
^ AC-2(7): Role-based Schemes	
^ AC-2(a): Identifies and selects types of information system accounts to support organizational missions/business functions	
^ AC-2(d): Specifies authorized users of the information system, group and role membership, and access authorizations and other attributes for	
^ AC-2(e): Requires approvals by organization-defined personnel or roles for requests to create information system accounts	
^ AC-2(f): Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures	

NIST SP 800-53 – Web View

NIST SP 800-53 R4 for zOS

^ AC-2: Account Management

∨ AC-2(7): Role-based Schemes

∨ AC-2(a): Identifies and selects types of information system accounts to support organizational missions/business functions

^ AC-2(d): Specifies authorized users of the information system, group and role membership, and access authorizations and other attributes for

4050003: Check whether the RACF User IDs defined as a console with LOGON(AUTO) have the OPERATIONS attribute

4050004: Check whether the RACF User IDs defined as a console with LOGON(AUTO) have the GROUP OPERATIONS attribute

4050005: Check whether the RACF User IDs defined as a console with LOGON(AUTO) have the SPECIAL attribute

4050006: Check whether the RACF User IDs defined as a console with LOGON(AUTO) have the GROUP SPECIAL attribute

4050007: Check whether the RACF User IDs defined as a console with LOGON(AUTO) have the AUDITOR attribute

4050008: Check whether the RACF User IDs defined as a console with LOGON(AUTO) have the GROUP AUDITOR attribute

4050009: Check whether the RACF User IDs defined as a console with LOGON(AUTO) have the ROAUDIT attribute

NIST SP 800-53 – Web View

NIST SP 800-53 R4 for zOS

^ AC-16: Security Attributes

[4002003: Check whether FTP daemons are configured with an appropriate umask value](#)

^ AC-17: Remote Access

^ AC-17(2): The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions

[4001001: Check whether all TCP/IP stacks have AT-TLS enabled](#)

[4002006: Check whether FTP daemons are configured to use AT-TLS to encrypt FTP control and data connections](#)

[4003001: Check whether the TELNETPARMS statements for all TN3270E servers have AT-TLS enabled on all ports](#)

[4003002: Check whether the PARMSGROUP statements for all TN3270E servers specify connection type values that are consistent with AT-TLS](#)

[4004001: Check whether CSSMTP servers are configured to always use AT-TLS to encrypt connections to their target mail servers](#)

NIST SP 800-53 – Spreadsheet

	A	B
1	profilename	NIST SP 800-53 R4 for zOS
2	profilemnemonic	ZOS_NIST_800_53_R4
3	profiledescription	NIST Security and Privacy Controls 800-53 Rev. 4 for zOS
4	##METAINFO ENDS##	
5	ExternalControlld	Description
6	AC	Access Control
7	AC-2	Account Management
8	AC-2(7)	Role-based Schemes
9	AC-2(7)(a)	Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access ...
10	AC-2(a)	Identifies and selects types of information system accounts to support organizational missions/business functions
11	AC-2(d)	Specifies authorized users of the information system, group and role membership, and access authorizations and other attributes for each account
12	AC-2(e)	Requires approvals by organization-defined personnel or roles for requests to create information system accounts
13	AC-2(f)	Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions
14	AC-3	Access Enforcement
15	AC-6	Least Privilege
16	AC-6(9)	The information system audits the execution of privileged functions
17	AC-6(10)	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/cou
18	AC-7	Unsuccessful Logon

NIST SP 800-53 – Spreadsheet

profilename	NIST SP 800-53 R4 for zOS									
profilemnemonic	ZOS_NIST_800_53_R4									
profiledescription	NIST Security and Privacy Controls 800-53 Rev. 4 for zOS									
##METAINFO ENDS##										
ExternalControllId	Descriptio	Parent	ControllId	Tags						
AC	Access Control									
AC-2	Account M AC									
AC-2(7)	Role-base AC-2									
AC-2(7)(a)	Establishe	AC-2(7)	4080003,4	RACF,USS,CONNECT,HSM,IMS,DFP,DSS,DFSMS,RMM,SIT,CONSOLE,IBM,OM,CICS,ZOS						
AC-2(a)	Identifies	AC-2	4079005	IBM,ZOS,INETD						
AC-2(d)	Specifies	AC-2	4080003,4	RACF,USS,CONNECT,HSM,DB2,IMS,DFP,DSS,DFSMS,RMM,SIT,CONSOLE,IBM,OM,CICS,ZOS						
AC-2(e)	Requires	AC-2	#####	IBM,CONNECT,OM,IMS,ZOS						
AC-2(f)	Creates,	AC-2	#####	RACF,SIT,IBM,DB2,CICS,ZOS						
AC-3	Access En	AC	4080003,4	RACF,USS,HSM,DB2,DFP,DSS,DFSMS,RMM,SIT,CONSOLE,IBM,CICS,ZOS						
AC-6	Least Privi AC									
AC-6(9)	The inform	AC-6	4077057	USS,IBM,ZOS						
AC-6(10)	The inform	AC-6	#####	DFSMS,IBM,ZOS,DFP						
AC-7	Unsuccess AC									

PCI DSS 4.0

PCI DSS 4.0 Web View

PCI DSS 4.0 for zOS

Controls

🔍 Search

ID	Description
1	Install and Maintain Network Security Controls
2	Apply Secure Configurations to All System Components
3	Protect Stored Account Data
4	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
6	Develop and Maintain Secure Systems and Software

PCI DSS 4.0 Web View

PCI DSS 4.0 for zOS

ID	Description
^ 1	Install and Maintain Network Security Controls
v	1.2: Network security controls (NSCs) are configured and maintained
v	1.3: Network access to and from the cardholder data environment is restricted
^ 2	Apply Secure Configurations to All System Components
v	2.2: System components are configured and managed securely

PCI DSS 4.0 Web View

2 Apply Secure Configurations to All System Components

2.2: System components are configured and managed securely

- 2.2.1: Configuration standards are developed, implemented, and maintained
 - 2.2.2: Vendor default accounts are managed and system components cannot be accessed using default passwords
 - 2.2.4: Only necessary services, protocols, daemons, and functions are enabled
 - 2.2.5: System components cannot be compromised by exploiting insecure services, protocols, or daemons
 - 2.2.6: System security parameters are configured to prevent misuse
 - 2.2.7: All non-console administrative access is encrypted using strong cryptography
-

PCI DSS 4.0 Web View

- 2 Apply Secure Configurations to All System Components

- 2.2: System components are configured and managed securely

- 2.2.1: Configuration standards are developed, implemented, and maintained

- 2.2.1.0: Configuration standards are developed, implemented, and maintained

- [4079002: Check whether the startup user account for the z/OS UNIX Telnet server is properly defined](#)

- 2.2.1.c: Verify that system configuration standards are applied when new systems are configured and verified as be

- [4096006: Check whether the SMF system identifier is set to the default value](#)

PCI DSS 4.0 Web View

^ 2.2.2: Vendor default accounts are managed and system components cannot be accessed using default passwords

4081001: Check the installation specified default ID has been changed

4083007: Check that RACF default system user ID (IBMUSER) has been revoked

4083008: Check that the default passwords used by the RACF RVARY command are not in use

4085014: Check the user ID that IMS uses if the primary MTO does not sign on for transaction authorization checking

4085015: Check the application ID that is to be used when calling the ESM during sign on

4085016: Check a user ID that IMS uses for transaction and command authority checking when a TCO terminal does no

4085017: Check whether IMS is to discard transaction reply messages for static VTAM terminals when the current user

4085018: Check the user ID if the WTOR does not sign on for transaction authorization checking

4087001: Check the default RACF ID for exits to pass to OTMA for security checking if the RACF ID has not explicitly be

4087002: Check the TCP/IP APPL name defined to RACF in the PTKTDATA statement

PCI DSS 4.0 Web View

^ 2.2.7: All non-console administrative access is encrypted using strong cryptography

^ 2.2.7.0: All non-console administrative access is encrypted using strong cryptography

4049018: Check that weak algorithm DES56 is not in use

4049019: Check that weak algorithm DES112 is not in use

4049020: Check that weak algorithm DES168 is not in use

4049021: Check that weak algorithm RSA512 is not in use

4049022: Check that weak algorithm RSA1024 is not in use

4049023: Check that weak algorithm ECCBP160 is not in use

4049024: Check that weak algorithm ECCBP192 is not in use

4049025: Check that weak algorithm ECCP192 is not in use

4049026: Check that weak algorithm RC4 is not in use

PCI DSS 4.0 Web View

^ 3.6: Cryptographic keys used to protect stored account data are secured

^ 3.6.1: Procedures are defined and implemented to protect cryptographic keys used to protect stored account data again

∨ 3.6.1.0: Procedures are defined and implemented to protect cryptographic keys used to protect stored account data

∨ 3.6.1.1: A documented description of the cryptographic architecture is maintained and available

∨ 3.6.1.2: Secret and private keys used to encrypt/decrypt stored account data are stored in a secure form that prevents

∨ 3.6.1.3: Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary

∨ 3.6.1.4: Cryptographic keys are stored in the fewest possible locations

PCI DSS 4.0 Web View

^ 3.6: Cryptographic keys used to protect stored account data are secured

^ 3.6.1: Procedures are defined and implemented to protect cryptographic keys used to protect stored account data again

^ 3.6.1.0: Procedures are defined and implemented to protect cryptographic keys used to protect stored account data

4049002: Check ICSF Key Store Policy token authorization checking for CKDS and PKDS are active

4049003: Check ICSF Key Store Policy duplicate key token checking for CKDS and PKDS are active

4049004: Check ICSF Key Store Policy symmetric key label export controls are active

4049005: Check ICSF Key Store Policy Key archive use control is disabled

4049006: Check ICSF Key Store Policy Granular key label access controls are enabled

4049007: Check ICSF KGUP CSFKEYS authority control is enabled

4049008: Check ICSF CSFKEYS PKA ECC token private-key name checking is enabled

PCI DSS 4.0 – Spreadsheet

profilenan	PCI DSS 4.0 for zOS
profilemn	ZOS_PCI_DSS_4_0
profiledes	PCI DSS 4.0 for zOS
	##METAINFO ENDS##
ExternalCo	Description
	1 Install and Maintain Network Security Controls
	1.2 Network security controls (NSCs) are configured and maintained
1.2.1	Configuration standards for NSC rulesets are defined, implemented and maintained
	1.3 Network access to and from the cardholder data environment is restricted
1.3.1	Inbound traffic to the CDE is restricted to only traffic that is necessary
1.3.2	Outbound traffic from the CDE is restricted to only traffic that is necessary
	2 Apply Secure Configurations to All System Components
	2.2 System components are configured and managed securely
2.2.1.0	Configuration standards are developed, implemented, and maintained
2.2.1	Configuration standards are developed, implemented, and maintained
2.2.1.c	Verify that system configuration standards are applied when new systems are configured and verified as being in place before or immediately after a sy
2.2.2	Vendor default accounts are managed and system components cannot be accessed using default passwords
2.2.4	Only necessary services, protocols, daemons, and functions are enabled
2.2.5	System components cannot be compromised by exploiting insecure services, protocols, or daemons

PCI DSS 4.0 – Spreadsheet

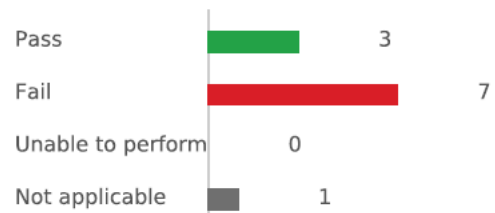
A	B	C	D	E	F	G	H	I	J
profilenam	PCI DSS 4.0 for zOS								
profilemn	ZOS_PCI_DSS_4_0								
profiledes	PCI DSS 4.0 for zOS								
##METAINFO ENDS##									
ExternalCo	Descriptio	Parent	Controlld	Tags					
	1	Install and Maintain	Network Security	Controls					
	1.2	Network s	1						
1.2.1	Configurat	1.2	4001004	ZOS,COMM SERVER,IBM,TCPIP					
	1.3	Network a	1						
1.3.1	Inbound t	1.3	4001004	ZOS,COMM SERVER,IBM,TCPIP					
1.3.2	Outbound	1.3	4001004	ZOS,COMM SERVER,IBM,TCPIP					
	2	Apply Secure Configurations to All System Components							
	2.2	System co	2						
2.2.1.0	Configurat	2.2.1	4079002	ZOS,INETD,IBM					
2.2.1	Configurat	2.2							
2.2.1.c	Verify that	2.2.1	4096006	ZOS,GLOBAL,SMF,IBM					
2.2.2	Vendor de	2.2	#####	DB2,ZOS,CONNECT,IBM,RACF,IMS					
2.2.4	Only nece:	2.2	#####	ZOS,INETD,COMM SERVER,TN3270E,IBM,TCPIP					
2.2.5	System co	2.2	#####	ZOS,COMM SERVER,TN3270E,IBM,FTP,TCPIP					

PCI Report

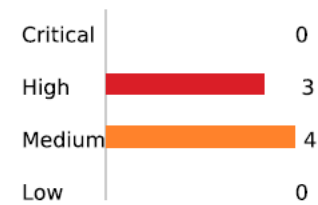
Executive Summary

Report Generated	2023-04-10 11:49:41 PM GMT
FACTs Collected	2023-04-06 06:58:38 PM GMT
Validation Performed	2023-04-06 06:58:47 PM GMT
Report Profile	Custom PCI DSS
Scope	ZHBPLEX
Report run by	jbergh

Result	Critical	High	Medium	Low	Total
Passed:		1	2		3
Failed:		3	4		7
Unable to Perform:					
Not Applicable:					1
TOTAL:		4	6		11



Summary By Controls



Failures By Severity

PCI Report

Validation Summary per Control

Validation Summary per Control				Number of IT Resources				
Control ID	Description	Overall Status	Severity	Pass	Fail	Unable	N/A	Total
8.2.2	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis	PASS		1				1
8.2.4	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed	FAIL	Medium	1	1			2
8.2.5	Access for terminated users is immediately revoked	FAIL	Medium	1	1		1	3
8.2.6	Inactive user accounts are removed or disabled within 90 days of inactivity	FAIL	Medium	1	1			2
8.2.8	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session	FAIL	Medium	4	5	1	2	12
8.3.1	All user access to system components for users and administrators is authenticated	FAIL	High		1		3	4
8.3.2	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components	FAIL	High	63	1	1		65
8.3.4	Invalid authentication attempts are limited	PASS		1				1
8.3.6	If passwords/passphrases are used as authentication factors, they meet the following minimum level of complexity	FAIL	High	3	1		2	6
8.3.9	If passwords/passphrases are used as the only authentication factor for user access then either it must be changed at least once every 90 days, OR the security posture of accounts is dynamically analyzed	PASS		1				1
8.3.11	Authentication factors such as physical or logical security tokens, smart cards, or certificates must only be used by the user to which it is assigned	N/A					3	3

PCI Report

Control Details

Control ID: 8.2.8

Control Description: If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session

Goals: 12

Severity	Controls Status: FAIL
Medium	

Status	Pass	Fail	Unable	N/A	Total
Resources	4	5	1	2	12

Goal ID	Description	Status	Severity	Pass	Fail	Unable	N/A	Total
4001014	Check whether TCP/IP stacks are configured with a proper FINWAIT timeout	PASS	High	1	0	0	0	1
4002002	Check whether FTP daemons are configured with an appropriate inactivity timeout value	PASS	Low	1	0	0	0	1
4003003	Check whether TELNETPARMS statements for all TN3270E servers are configured with appropriate inactivity timeout values	PASS	High	1	0	0	0	1
4079003	Check whether the timeout value for z/OS UNIX Telnet server session is properly configured	FAIL	Low	0	1	0	0	1
4081006	Check the allowed idle time of an active server thread	PASS	Low	1	0	0	0	1
4096001	Check whether the 'maximum amount of time that a TSO/E user address space is allowed to wait continuously' is properly configured	FAIL	Medium	0	1	0	0	1
4096002	Check whether the 'maximum amount of time that a started task address space is allowed to wait continuously' is properly configured	FAIL	Medium	0	1	0	0	1
4096003	Check whether the 'maximum amount of time that a job or TSO/E user address space is allowed to wait continuously' is properly configured	FAIL	Medium	0	1	0	0	1
4096005	Check whether the amount of real time that SMF allows data to remain in an SMF buffer is properly configured	FAIL	Medium	0	1	0	0	1

PCI Report – Algorithm check

Control Details

Control ID: 8.3.2

Control Description: Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components

Goals: 56

Severity	Controls Status: FAIL
High	

Status	Pass	Fail	Unable	N/A	Total
Resources	63	1	1		65

Goal ID	Description	Status	Severity	Pass	Fail	Unable	N/A	Total
4049018	Check that weak algorithm DES56 is not in use	PASS	High	2	0	0	0	2
4049019	Check that weak algorithm DES112 is not in use	PASS	High	2	0	0	0	2
4049020	Check that weak algorithm DES168 is not in use	PASS	High	2	0	0	0	2
4049021	Check that weak algorithm RSA512 is not in use	PASS	High	2	0	0	0	2
4049022	Check that weak algorithm RSA1024 is not in use	PASS	High	2	0	0	0	2
4049023	Check that weak algorithm ECCBP160 is not in use	PASS	High	2	0	0	0	2
4049024	Check that weak algorithm ECCBP192 is not in use	PASS	High	2	0	0	0	2
4049025	Check that weak algorithm ECCP192 is not in use	PASS	High	2	0	0	0	2
4049026	Check that weak algorithm RC4 is not in use	PASS	High	2	0	0	0	2
4080015	Check whether password are redacted in line traces	PASS	Medium	1	0	0	0	1
4083012	Check that RACF is encrypting stored passwords	FAIL	High	0	1	0	0	1
4128001	Check that weak algorithm KM-DEA is not in use	PASS	High	1	0	0	0	1
4128003	Check that weak algorithm KM-TDEA-128 is not in use	PASS	High	1	0	0	0	1
4128005	Check that weak algorithm KM-TDEA-192 is not in use	PASS	High	1	0	0	0	1
4128007	Check that weak algorithm KM-Encrypted-DEA is not in use	PASS	High	1	0	0	0	1
4128008	Check that weak algorithm KM-Encrypted-TDEA-128 is not in use	PASS	High	1	0	0	0	1

PCI DSS – Drift Report

Executive Summary

Share File
Invite other

Report Date/ Time	2023-04-10 11:47:42 PM GMT
Profile used in report	Custom PCI DSS
Scope used in report	ZHBPLEX
Report run by	jbergh
Results Overview	<p>Passed: 0 of 11 controls</p> <p>Failed: 0 of 11 controls</p> <p>Unable To Perform: 0 of 11 controls</p> <p>Not Applicable: 11 of 11 controls</p>
Profile Details	<p>Created By: admin</p> <p>Created On: 2023-03-28 06:00:46 PM GMT</p> <p>Modified By: admin</p> <p>Modified On: 2023-03-28 06:00:46 PM GMT</p>

PCI DSS – Drift Report

Validation Summary

Control ID #	Description	2023-03-28 18-17	2023-04-06 18- 58
8.2.2	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis	N/A	PASS
8.2.4	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed	N/A	FAIL
8.2.5	Access for terminated users is immediately revoked	N/A	FAIL
8.2.6	Inactive user accounts are removed or disabled within 90 days of inactivity	N/A	FAIL
8.2.8	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session	N/A	FAIL
8.3.1	All user access to system components for users and administrators is authenticated	N/A	FAIL
8.3.2	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components	N/A	FAIL

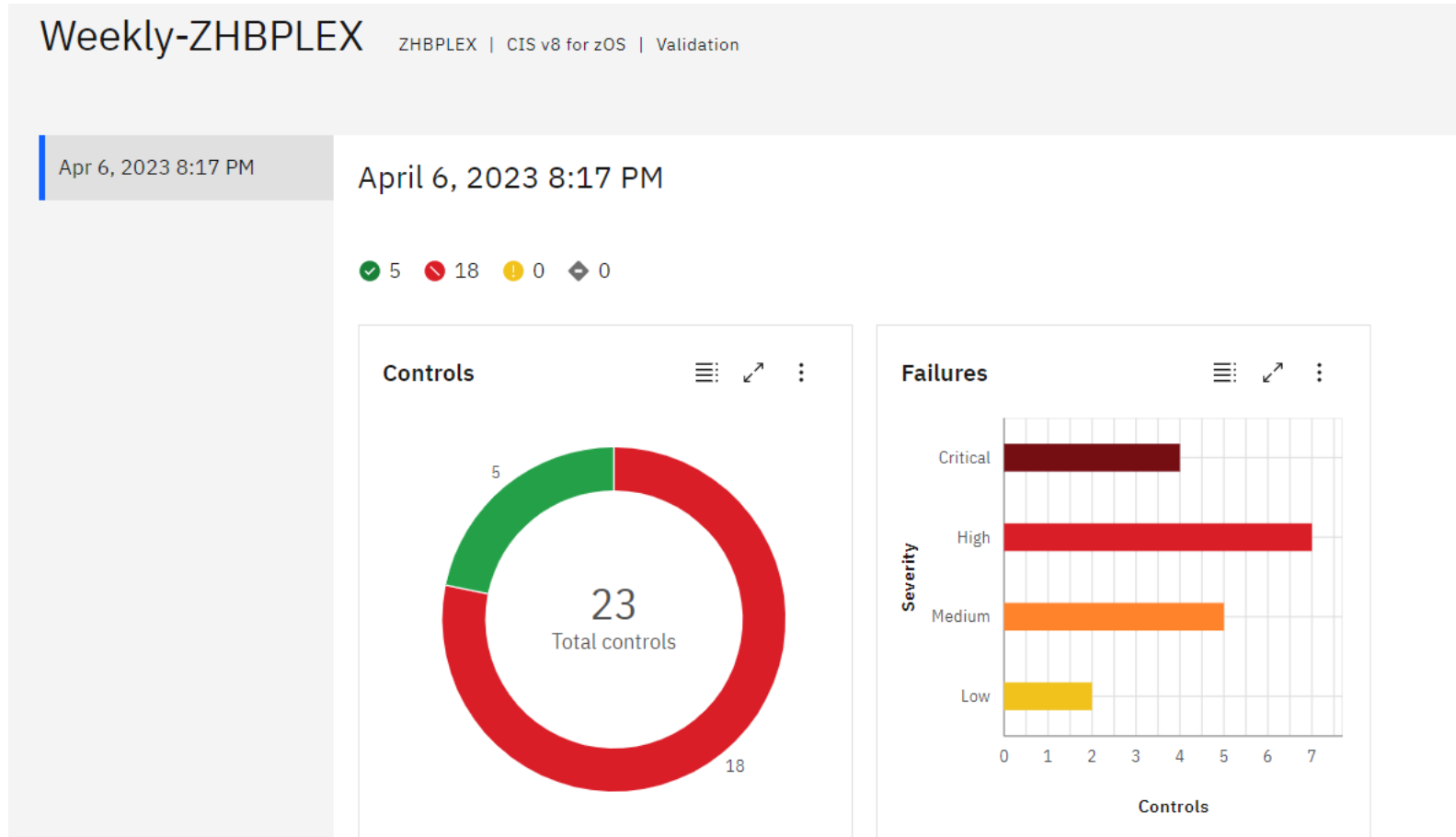
CIS

CIS Web View

CIS v8 for zOS

- ▼ 3 Data Protection
- ▼ 4 Secure Configuration of Enterprise Assets and Software
- ▼ 5 Account Management
- ▼ 6 Access Control Management
- ▼ 8 Audit Log Management
- ▼ 13 Network Monitoring and Defense

CIS Web View



CIS Web View

Status	Filter...	Severity	Filter...	Q Search	
Status	ID	Control	Severity	Resource details	
	3.1	Establish and Maintain a Data Management Process	Medium	1 4 0 0	
	3.3	Configure Data Access Control Lists	Critical	40 112 1 1469	
	3.9	Encrypt Data on Removable Media	High	122 5 0 0	
	3.10	Encrypt Sensitive Data in Transit	Critical	2 5 2 0	
	3.11	Encrypt Sensitive Data at Rest	High	122 6 0 0	
	3.12	Segment Data Processing and Storage Based on Sensitivity	High	2 1 0 0	
	4.1	Establish and Maintain a Secure Configuration Process	Critical	13 36 1 750	
	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Medium	0 1 0 0	
	4.3	Configure Automatic Session Locking on Enterprise Assets	Medium	4 4 1 0	
	4.4	Implement and Manage a Firewall on Servers	Low	0 1 0 0	

CIS Web View

Configure Data Access Control Lists ×

Control ID	Severity	Status	Number of goals
3.3	Critical	FAIL	137

Goals

Pass Fail Unable to validate Not applicable

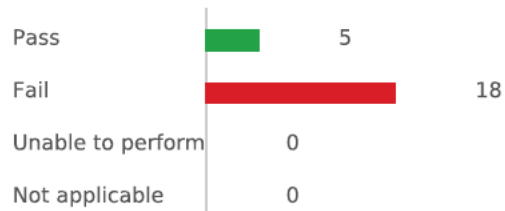
ID: 4002003	Check whether FTP daemons are configured with an appropriate umask value	<input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0	✓ 0 ✗ 1 ! 0 ⚡ 0 ▾
ID: 4002009	Check whether FTP daemons allow clients to use the SITE DEBUG command. If they do, SAF SERVAUTH access controls should be in place	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0	✓ 1 ✗ 0 ! 0 ⚡ 0 ▾
ID: 4002010	Check whether FTP daemons allow clients to use the SITE DUMP command. If they do, SAF SERVAUTH access controls should be in place	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0	✓ 1 ✗ 0 ! 0 ⚡ 0 ▾
ID: 4002011	Check whether FTP daemons limit JES access to logged-in user ID scope	<input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0	✓ 0 ✗ 1 ! 0 ⚡ 0 ▾
ID: 4002012	Check whether FTP daemons limit use of the PORT and EPRT commands	<input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0	✓ 0 ✗ 1 ! 0 ⚡ 0 ▾
ID: 4049002	Check ICSF Key Store Policy token authorization checking for CKDS and PKDS are active	<input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0	✓ 0 ✗ 1 ! 0 ⚡ 0 ▾
ID: 4049003	Check ICSF Key Store Policy duplicate key token checking for CKDS and PKDS are active	<input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0	✓ 0 ✗ 1 ! 0 ⚡ 0 ▾

CIS Report

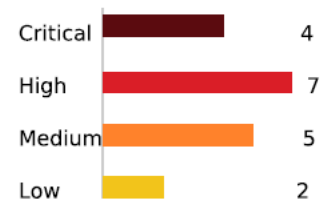
Executive Summary

Report Generated	2023-04-11 12:01:15 AM GMT
FACTs Collected	2023-04-06 11:10:54 PM GMT
Validation Performed	2023-04-07 01:17:37 AM GMT
Report Profile	CIS v8 for zOS
Scope	ZHBPLEX
Report run by	admin

Result	Critical	High	Medium	Low	Total
Passed:		3	1	1	5
Failed:	4	7	5	2	18
Unable to Perform:					
Not Applicable:					
TOTAL:	4	10	6	3	23



Summary By Controls



Failures By Severity

CIS Report

Validation Summary per Control

Control ID	Description	Overall Status	Severity	Number of IT Resources				
				Pass	Fail	Unable	N/A	Total
3.1	Establish and Maintain a Data Management Process	FAIL	Medium	1	4			5
3.3	Configure Data Access Control Lists	FAIL	Critical	40	112	1	1,515	1,668
3.9	Encrypt Data on Removable Media	FAIL	High	122	5			127
3.10	Encrypt Sensitive Data in Transit	FAIL	Critical	2	5	2	1	10
3.11	Encrypt Sensitive Data at Rest	FAIL	High	122	6			128
3.12	Segment Data Processing and Storage Based on Sensitivity	FAIL	High	2	1			3
4.1	Establish and Maintain a Secure Configuration Process	FAIL	Critical	13	36	1	758	808
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	FAIL	Medium		1		1	2
4.3	Configure Automatic Session Locking on Enterprise Assets	FAIL	Medium	4	4	1	2	11
4.4	Implement and Manage a Firewall on Servers	FAIL	Low		1			1
4.7	Manage Default Accounts on Enterprise Assets and Software	FAIL	Critical	2	3		7	12
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	PASS		2				2
5.1	Establish and Maintain an Inventory of Accounts	PASS		1				1
5.2	Use Unique Passwords	PASS		2				2

CIS Report

Control ID: 3.3

Control Description: Configure Data Access Control Lists

Goals: 137

Severity	Controls Status: FAIL
Critical	

Status	Pass	Fail	Unable	N/A	Total
Resources	40	112	1	1,515	1,668

Goal ID	Description	Status	Severity	Pass	Fail	Unable	N/A	Total
4002003	Check whether FTP daemons are configured with an appropriate umask value	FAIL	Medium	0	1	0	0	1
4002009	Check whether FTP daemons allow clients to use the SITE DEBUG command. If they do, SAF SERVAUTH access controls should be in place	PASS	Low	1	0	0	0	1
4002010	Check whether FTP daemons allow clients to use the SITE DUMP command. If they do, SAF SERVAUTH access controls should be in place	PASS	Low	1	0	0	0	1
4002011	Check whether FTP daemons limit JES access to logged-in user ID scope	FAIL	Medium	0	1	0	0	1
4002012	Check whether FTP daemons limit use of the PORT and EPRT commands	FAIL	Medium	0	1	0	0	1
4049002	Check ICSF Key Store Policy token authorization checking for CKDS and PKDS are active	FAIL	Medium	0	1	0	0	1
4049003	Check ICSF Key Store Policy duplicate key token checking for CKDS and PKDS are active	FAIL	Low	0	1	0	0	1
4049004	Check ICSF Key Store Policy symmetric key label export controls are active	FAIL	Low	0	1	0	0	1
4049005	Check ICSF Key Store Policy Key archive use control is disabled	PASS	Low	1	0	0	0	1
4049006	Check ICSF Key Store Policy Granular key label access controls are enabled	FAIL	Low	0	1	0	0	1
4049007	Check ICSF KGUP CSFKEYS authority control is enabled	FAIL	Low	0	1	0	0	1
4049008	Check ICSF CSFKEYS PKA ECC token private-key name checking is enabled	FAIL	Low	0	1	0	0	1
	Check whether miscellaneous and future DESMS storage							

Keeping Up With Security and Compliance on IBM zSystems

Bill White

Didier Andre

Lindsay Baer

Julie Bergh



Additional Information

z/OS Compliance Data Collection Infrastructure

A new [z/OSMF compliance REST API](#) invokes the Common Event Adapter (CEA) to drive an ENF86 signal through to participating z/OS components and products.

z/OSMF support requires z/OS 2.4 or later with PTFs for APAR PH37308

Upon receiving the ENF86 signal, participating z/OS components and products [collect and write compliance data](#) to their associated SMF1154 subtype records.

CEA support requires z/OS 2.4 or later with PTFs for APAR OA61443

[SMF 1154 records](#) provide compliance evidence. A different subtype is assigned to each participating z/OS component or product.

SMF support requires z/OS 2.4 or later with PTFs for APAR OA61444. See component PTFs on subsequent slides.

The [Common Data Provider](#) streams SMF 1154 records to the [IBM Z Security and Compliance Center](#) for validation, display and reporting.

CDP support requires version 5.1 with PTFs for APAR OA63087.

Comm Server: TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of industry-standard protocols and applications that enable you to share data and computing resources with other computers, both IBM and non-IBM. By using TCP/IP commands at your workstation, you can perform tasks and communicate easily with a variety of other systems and workstations. z/OS Communications Server enables the user to interactively run TCP/IP applications (TCP/IP commands) from both the Time Sharing Option (TSO) and the z/OS shell.

Compliance data collection for Comm
Server: TCP/IP requires z/OS 2.4 or
later and PTFs for PH37372

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to use strong cryptography and security to safeguard sensitive cardholder data during transmission over open, public networks.


- *What does this mean for TCP/IP?*
- *Which TCP/IP controls are relevant?*
- *Will the auditor understand Comm Server terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

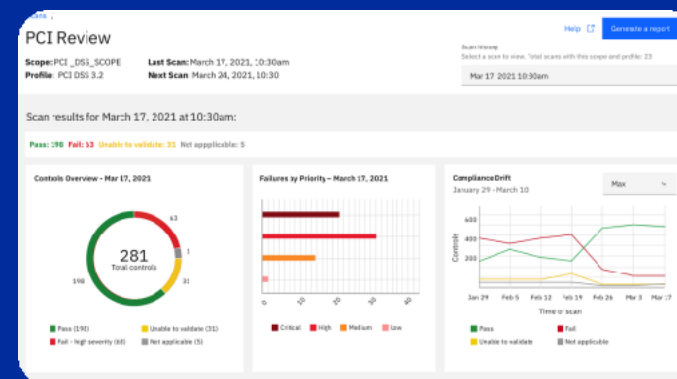
 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations,
collects and validates compliance data.

For z/OS 2.4 and later,
automatically collect data from
SMF Type 1154 Subtype 1 to

- ✓ Check whether all TCP/IP stacks have AT-TLS enabled
- ✓ Check whether IP packet forwarding is disabled on all TCP/IP stacks
- ✓ Check whether TCP/IP stacks are configured to audit important events
- ✓ ... and more!

Comm Server: FTP

z/OS Communications Server provides a set of communications protocols that support peer-to-peer connectivity functions for both local and wide-area networks, including the most popular wide-area network, the Internet. z/OS Communications Server also provides performance enhancements that can benefit a variety of TCP/IP applications.

The FTP command runs the FTP client program that enables you to transfer data sets and files between your local host and another host running an FTP server. Using the FTP command and its subcommands, you can sequentially access multiple hosts without leaving the FTP client.

Compliance data collection for
Comm Server: FTP requires z/OS
2.4 or later and PTFs for PH37372

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to implement additional security features for any required services, protocols, or daemons that are considered insecure.


- *What does this mean for FTP?*
- *Which FTP controls are relevant?*
- *Will the auditor understand Comm Server terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations,
collects and validates compliance data.

For z/OS 2.4 and later,
automatically collect data from
SMF Type 1154 Subtype 2 to

- ✓ Check that anonymous FTP daemons do not allow anonymous FTP
- ✓ Check whether FTP daemons reveal any IP addresses, hostnames, port numbers, or server OS level information in FTP replies
- ✓ ... and more!

Comm Server: TN3270E

Telnet is a terminal emulation protocol. With Telnet, users can log on to remote host applications as though they were directly attached to that host. Telnet protocol requires that the user have a Telnet client that emulates a type of terminal that the host application can understand. The client connects to a Telnet server, which communicates with the host application. The Telnet server acts as an interface between the client and host application.

The TN3270E Telnet server (Telnet) provides access to z/OS VTAM SNA applications on the MVS host using Telnet TN3270E, TN3270, or linemode protocol. Telnet acts as an interface between IP and SNA networks. End users in an IP network connect to Telnet, which is also a VTAM application.

Compliance data collection for Comm Server: TN3270E requires z/OS 2.4 or later and PTFs for PH37372

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to re-authenticate to re-activate terminals or sessions idle for more than 15 minutes.

- *What does this mean for TN3270E?*
- *Which TN3270E controls are relevant?*
- *Will the auditor understand Comm Server terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

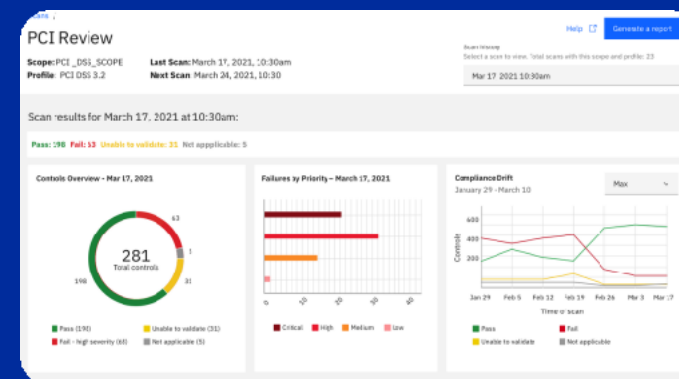
 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance with the z16 IBM Security & Compliance Center



Maps IBM Z capabilities to regulations, collects and validates compliance data.

For z/OS 2.4 and later, automatically collect data from SMF Type 1154 Subtype 3 to

- ✓ Check whether TELNETPARMS statements for all TN3270E servers are configured with appropriate inactivity timeouts
- ✓ Check whether PARMGROUP statements for all TN3270E servers specify appropriate inactivity timeout values
- ✓ ... and more!

Comm Server: CSSMTP

z/OS Communications Server provides a set of communications protocols that support peer-to-peer connectivity functions for both local and wide-area networks, including the most popular wide-area network, the Internet. z/OS Communications Server also provides performance enhancements that can benefit a variety of TCP/IP applications.

The Communication Server SMTP (CSSMTP) application is a mail forwarding SMTP client. CSSMTP processes data sets that are in the JES spool file that contain mail messages and then forwards the mail messages to a target server.

Compliance data collection for Comm Server: CSSMTP requires z/OS 2.4 or later and PTFs for PH37372

Interpreting Regulations

Without z16


For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to **record audit trail entries for all system components for each event.**

- *What does this mean for CSSMTP?*
- *Which CSSMTP controls are relevant?*
- *Will the auditor understand Comm Server terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations, collects and validates compliance data.

For z/OS 2.4 and later, automatically collect data from **SMF Type 1154 Subtype 4** to

- ✓ Check whether CSSMTP servers are configured to always use AT-TLS
- ✓ Check whether CSSMTP servers are configured to audit important events
- ✓ ... and more!

ICSF

Integrated Cryptographic Services Facility (ICSF) provides the application programming interfaces by which applications request cryptographic services. ICSF callable services and programs can be used to generate, maintain, and manage keys that are used in cryptographic operations to:

- Protect data
- Protect and distribute additional keys
- Verify message integrity
- Generate, protect and verify PINs
- Generate and verify signatures

Compliance data collection
for ICSF requires z/OS 2.4 or
later and PTFs for OA61977

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to render a personal account number (PAN) unreadable anywhere it is stored using approaches such as strong cryptography.


- *What does this mean for ICSF?*
- *Which ICSF controls are relevant?*
- *Will the auditor understand ICSF terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

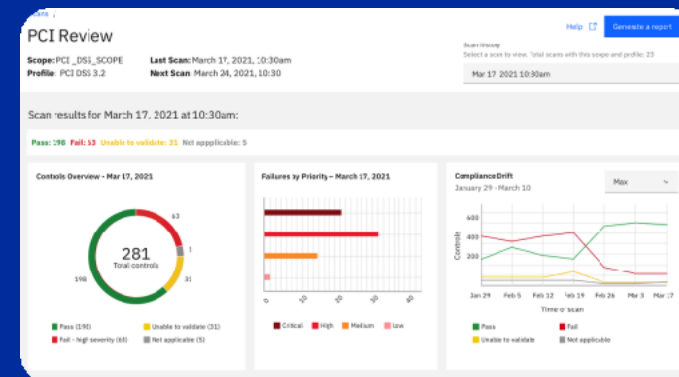
 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations,
collects and validates compliance data.

For z/OS 2.4 and later,
automatically collect data from
SMF Type 1154 Subtype 49 to

- ✓ Check that weak algorithm DES56 is not in use
- ✓ Check that weak algorithm DES112 is not in use
- ✓ Check that weak algorithm SHA1 is not in use
- ✓ ... and more!

Consoles

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to **re-authenticate to re-activate terminals or sessions idle for more than 15 minutes.**


- *What does this mean for Consoles?*
- *Which Consoles controls are relevant?*
- *Will the auditor understand Consoles terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

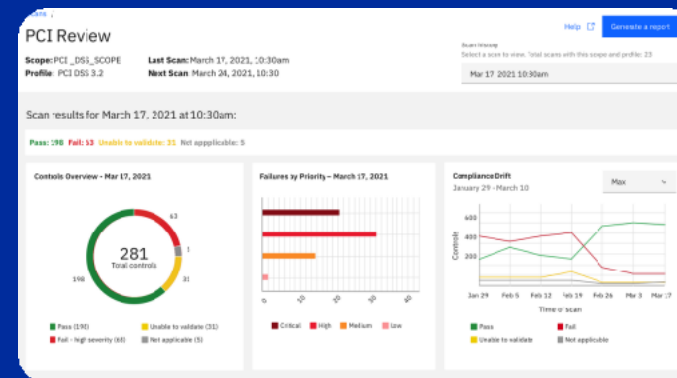
Operating z/OS involves the following:

- Console operations or how operators interact with z/OS to monitor or control the hardware and software.
- Message and command processing that forms the basis of operator interaction with z/OS and the basis of z/OS automation.

Generally, operators on a z/OS system receive messages and enter commands on MCS and SMCS consoles.

- MCS consoles are devices that are locally attached to a z/OS system and provide the basic communication between operators and z/OS.
- SMCS consoles use z/OS Communications Server to provide communication between operators and z/OS instead of direct I/O to the console device.

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



With the IBM Z Security and Compliance Center, automatically collect data from **SMF Type 1154 Subtype 50** to

- ✓ Check whether auto sign-off time for Master, MCS and SMCS consoles is properly configured
- ✓ Check whether the console logon setting for Master, MCS and SMCS consoles is properly configured
- ✓ ... and more!

Compliance data collection for Consoles requires **the IBM Z Security & Compliance Center**

Maps IBM Z capabilities to regulations, collects and validates compliance data.

DFSMSdfp

DFSMS comprises a suite of related data and storage management products for the z/OS system. DFSMS is an operating environment that helps automate and centralize the management of storage based on the policies that your installation defines for availability, performance, space, and security.

DFSMSdfp provides:

- Storage management
- Tape mount management
- Data management
- Device management
- Distributed data success
- Advanced copy servers
- Object access method

Compliance data collection for DFSMSdfp requires **the IBM Z Security & Compliance Center**

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to establish access control that is set to “deny all” by default.

- *What does this mean for DFSMS?*
- *Which DFSMS controls are relevant?*
- *Will the auditor understand DFSMS terminology?*

Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

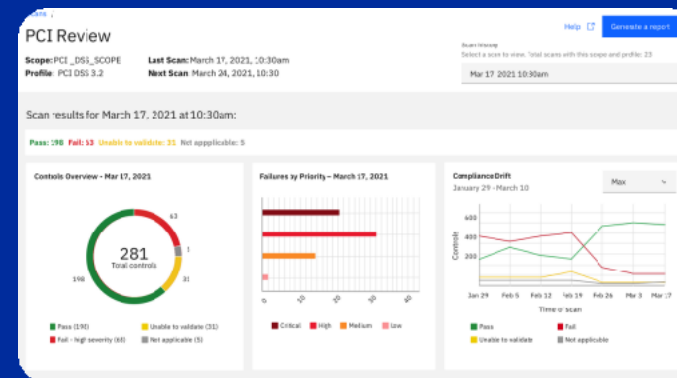
 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations, collects and validates compliance data.

With the IBM Z Security and Compliance Center, automatically collect data from **SMF Type 1154 Subtype 51** to

- ✓ Check whether the authority to rename non-SMS system data sets is restricted
- ✓ Check whether SMS settings are protected against modification
- ✓ ... and more!

DFSMSrmm

DFSMS comprises a suite of related data and storage management products for the z/OS system. DFSMS is an operating environment that helps automate and centralize the management of storage based on the policies that your installation defines for availability, performance, space, and security.

DFSMSrmm manages your removable media resources, including tape cartridges and reels. It provides:

- Library management
- Shelf management
- Volume management
- Data Set management

Compliance data collection for DFSMSrmm requires **the IBM Z Security & Compliance Center**

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to implement automated audit trails for all system components.

- *What does this mean for DFSMS?*
- *Which DFSMS controls are relevant?*
- *Will the auditor understand DFSMS terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

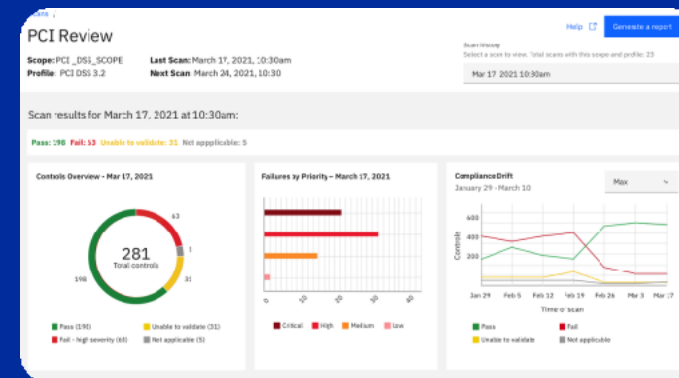
 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



With the IBM Z Security and Compliance Center, automatically collect data from **SMF Type 1154 Subtype 52** to

- ✓ Check whether RMM audit records are generated
- ✓ Check whether RMM security records are generated
- ✓ ... and more!

Maps IBM Z capabilities to regulations, collects and validates compliance data.

DFSMSHsm

DFSMS comprises a suite of related data and storage management products for the z/OS system. DFSMS is an operating environment that helps automate and centralize the management of storage based on the policies that your installation defines for availability, performance, space, and security.

DFSMSHsm provides:

- Storage management
- Space management
- Tape mount management
- Availability management

Compliance data collection for DFSMSHsm requires **the IBM Z Security & Compliance Center**

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to establish access control that is set to “deny all” by default.

- *What does this mean for DFSMS?*
- *Which DFSMS controls are relevant?*
- *Will the auditor understand DFSMS terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations, collects and validates compliance data.

With the IBM Z Security and Compliance Center, automatically collect data from **SMF Type 1154 Subtype 53** to

- ✓ Check whether adding a migration volume is protected
- ✓ Check whether backups of all data sets are protected
- ✓ Check whether storage admin LIST commands are protected
- ✓ ... and more!

DFSMSdss

DFSMS comprises a suite of related data and storage management products for the z/OS system. DFSMS is an operating environment that helps automate and centralize the management of storage based on the policies that your installation defines for availability, performance, space, and security.

DFSMSdss provides:

- Data movement and replication
- Space management
- Data backup and recovery
- Data set and volume conversion

Compliance data collection for DFSMSdss requires **the IBM Z Security & Compliance Center**

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to establish access control that is set to “deny all” by default.

- *What does this mean for DFSMS?*
- *Which DFSMS controls are relevant?*
- *Will the auditor understand DFSMS terminology?*

Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



With the IBM Z Security and Compliance Center, automatically collect data from **SMF Type 1154 Subtype 54** to

- ✓ Check whether authority to copy data sets is protected
- ✓ Check whether authority to move data sets is protected
- ✓ Check whether authority to dump data sets is protected
- ✓ ... and more!

Maps IBM Z capabilities to regulations, collects and validates compliance data.

USS

The UNIX System Services element of z/OS is a UNIX operating environment, implemented within the z/OS operating system. It is also known as z/OS UNIX. The z/OS support enables two open systems interfaces on the z/OS operating system: an application programming interface (API) and an interactive shell interface.

Compliance data collection for USS requires **the IBM Z Security & Compliance Center**

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to **configure system parameters to prevent misuse.**

- *What does this mean for USS?*
- *Which USS controls are relevant?*
- *Will the auditor understand USS terminology?*

Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations, collects and validates compliance data.

With the IBM Z Security and Compliance Center, automatically collect data from **SMF Type 1154 Subtype 77** to

- ✓ Check whether the LOGNAME environment variable is marked as read-only in /etc/profile file
- ✓ Check whether the umask variable is properly configured
- ✓ ... and more!

Comm Server: SSHD

- z/OS OpenSSH provides secure encryption for both remote login and file transfer. Some of the utilities that it includes are:
- **ssh**, a z/OS client program for logging into a z/OS shell. It can also be used to log into other platform's UNIX shells. It is an alternative to rlogin.
 - **scp** for copying files between networks. It is an alternative to rcp.
 - **sftp** for file transfers over an encrypted ssh transport. It is an interactive file transfer program similar to ftp.
 - **sshd**, a daemon program for ssh that listens for connections from clients. The z/OS OpenSSH implementation of sshd supports SSH protocol version 2. SSH protocol version 1 is no longer supported.

Compliance data collection for Comm
Server: SSHD requires **the IBM Z
Security & Compliance Center**

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to **encrypt all non-console administrative access using strong cryptography.**


- *What does this mean for SSHD?*
- *Which SSHD controls are relevant?*
- *Will the auditor understand Comm Server terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations,
collects and validates compliance data.

With the IBM Z Security and Compliance Center, automatically collect data from **SMF Type 1154 Subtype 78** to

- ✓ Check whether z/OS OpenSSH sshd daemon is configured to only use the SSHv2 protocol
- ✓ Check whether OpenSSH is running in FIPS 140-2 mode with all applicable cipher algorithms implemented using ICSF
- ✓ ... and more!

Comm Server: INETD

z/OS Communications Server provides a set of communications protocols that support peer-to-peer connectivity functions for both local and wide-area networks, including the most popular wide-area network, the Internet. z/OS Communications Server also provides performance enhancements that can benefit a variety of TCP/IP applications.

The inetd program is a generic listener program used by such servers as z/OS UNIX TELNETD and z/OS UNIX REXECD. Other servers such as z/OS UNIX FTPD have their own listener program and do not use inetd.

Compliance data collection for Comm
Server: INETD requires **the IBM Z
Security & Compliance Center**

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to enable only necessary services, protocols, daemons, etc as required for the function of the system.


- *What does this mean for INETD?*
- *Which INETD controls are relevant?*
- *Will the auditor understand Comm Server terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

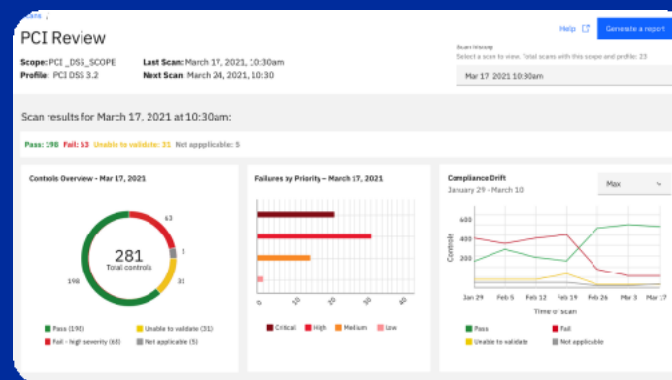
 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations,
collects and validates compliance data.

With the IBM Z Security and Compliance Center, automatically collect data from SMF Type 1154 Subtype 79 to

- ✓ Check whether the restricted network services are provided by the inetd daemon
- ✓ Check whether the startup user account for the z/OS UNIX Telnet server is properly defined
- ✓ ... and more!

CICS Transaction Server for z/OS

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to limit access to system components and cardholder data to only those individuals whose job requires such access.


- *What does this mean for CICS?*
- *Which CICS controls are relevant?*
- *Will the auditor understand CICS terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

CICS Transaction Server, often called simply CICS, is a powerful, mixed-language application server that runs on z/OS.

An application server provides an environment to host applications. It can provide services to solve many concerns, such as security, transactionality, or exchanging data between new and existing applications. Developing custom enterprise-grade solutions for these issues is difficult and can take time away from focusing on what the application is intended to do for the business. Importantly, CICS can provide these services to applications that are composed of components written in different programming languages.

Interpreting Regulations & Demonstrating Compliance with the z16 IBM Security & Compliance Center



For z/OS 2.4 and later, automatically collect data from SMF Type 1154 Subtype 80 to

- ✓ Check that security is on in all CICS regions
- ✓ Check that only authorized users can run programs
- ✓ Check that only authorized users can access files
- ✓ ... and more!

Db2 for z/OS

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to change vendor-supplied defaults and remove or disable unnecessary default accounts.


- *What does this mean for Db2?*
- *Which Db2 controls are relevant?*
- *Will the auditor understand Db2 terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Db2 for z/OS is a relational database management system that runs on the mainframe.

A relational database is a database in which all of the data is logically contained in tables. These databases are organized according to the relational model. In a relational database, referential integrity ensures data integrity by enforcing rules with referential constraints, check constraints, and triggers. You can rely on constraints and triggers to ensure the integrity and validity of your data, rather than relying on individual applications to do that work.

With Db2 for z/OS, you can define and manipulate your data by using structured query language (SQL). SQL is the standard language for accessing data in relational databases.

Continuous Compliance for z/OS / May 2022 / ©
2022 IBM Corporation

Compliance data collection
for Db2 for z/OS requires
Db2 v13

Interpreting Regulations & Demonstrating Compliance with the z16 IBM Security & Compliance Center



Maps IBM Z capabilities to regulations,
collects and validates compliance data.

For z/OS 2.4 and later,
automatically collect data from
SMF Type 1154 Subtype 81 to

- ✓ Check whether the installation specified default ID has been changed
- ✓ Check whether Db2 is configured to use a security port
- ✓ Check whether Db2 is configured to require authorization
- ✓ ... and more!

MQ for z/OS

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to use strong cryptography and security to safeguard sensitive cardholder data during transmission over open, public networks.

- *What does this mean for MQ?*
- *Which MQ controls are relevant?*
- *Will the auditor understand MQ terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

 TSO / MVS Commands?

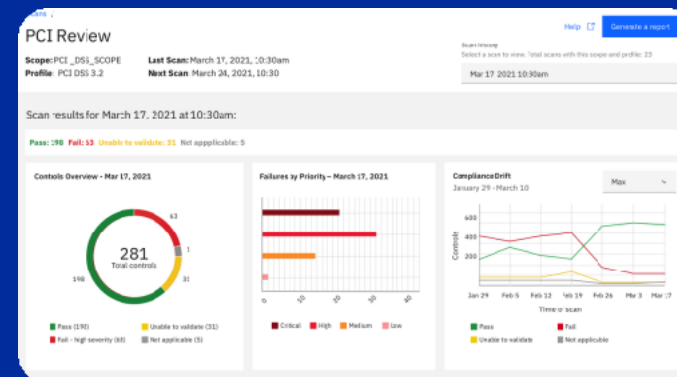
 ISPF Panels?

 SMF Records?

Which records?

IBM Message Queue (MQ) supports the exchange of information between applications, systems, services and files by sending and receiving message data via messaging queues. This simplifies the creation and maintenance of business applications. IBM MQ works with a broad range of computing platforms and can be deployed across a range of different environments including on-premise, in cloud, and hybrid cloud deployments. IBM MQ supports a number of different APIs including Message Queue Interface (MQI), Java Message Service (JMS), REST, .NET, IBM MQ Light and MQTT.

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



With the IBM Z Security and Compliance Center, automatically collect data from **SMF Type 1154 Subtype 82** to

- ✓ Check whether Advanced Message Security (AMS) capabilities are available to the queue manager
- ✓ Check whether MQ security is active
- ✓ ... and more!

Compliance data collection for IBM MQ for z/OS requires **the IBM Z Security & Compliance Center**

Maps IBM Z capabilities to regulations, collects and validates compliance data.

RACF

Resource Access Control Facility (RACF) is a security program. It is a component of the Security Server for z/OS. RACF controls what you can do on the z/OS operating system. You can use RACF to protect your resources. RACF protects information and other resources by controlling the access to those resources. RACF provides security by:

- Identifying and verifying users
- Authorizing users to access protected resources
- Recording and reporting access attempts

Compliance data collection for RACF requires z/OS 2.4 or later and PTFs for OA61933

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to control addition, deletion, and modification of user IDs, credentials, and other identifier objects.


- *What does this mean for RACF?*
- *Which RACF controls are relevant?*
- *Will the auditor understand RACF terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations, collects and validates compliance data.

For z/OS 2.4 and later, automatically collect data from SMF Type 1154 Subtype 83 to

- ✓ Check that RACF is active: installed, operational, and not in FAILSOFT mode
- ✓ Check that the RACF Authorized Caller Table (ICHAUTAB) contains no entries
- ✓ ... and more!

IMS for z/OS

Information Management System (IMS) is a message-based transaction manager and hierarchical-database manager for z/OS for online transaction processing (OLTP) and online batch processing. External applications can use transactions to interact with applications that run inside IMS.

IMS is one of the predominant database and transaction processing systems across a multitude of sectors, including banking, manufacturing, finance, healthcare, aerospace, communication, government, and retail.

Compliance data collection for IMS for z/OS requires PTFs for PH42600 and the **IBM Z Security & Compliance Center**

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to assign unique user IDs and ensure proper user authentication management.

- *What does this mean for IMS?*
- *Which IMS controls are relevant?*
- *Will the auditor understand IMS terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

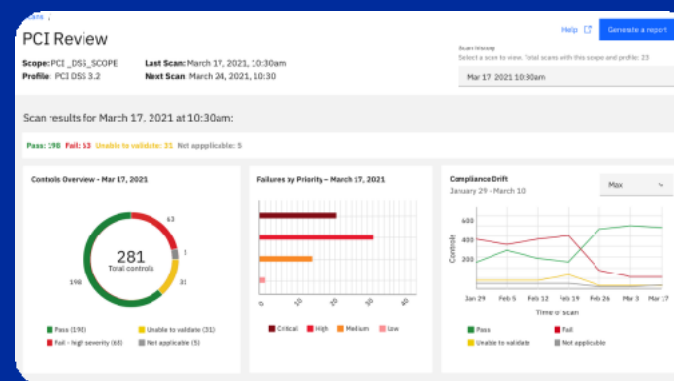
 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations, collects and validates compliance data.

With the IBM Z Security and Compliance Center, automatically collect data from **SMF Type 1154 Subtype 85** to

- ✓ Check whether the password re-verification function is activated
- ✓ Check whether IMS uses a user Id to check security of direct and non-direct routed transactions.
- ✓ ... and more!

SMF

System management facilities (SMF) collects and records system and job-related information that to use in:

- Billing users
- Reporting reliability
- Analyzing the configuration
- Scheduling jobs
- Summarizing direct access volume activity
- Evaluating data set activity
- Profiling system resource use
- Maintaining system security

Compliance data collection for SMF requires **the IBM Z Security & Compliance Center**

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to use file integrity monitoring or change detection software on logs to ensure that log data cannot be changed without generating alerts.


- *What does this mean for SMF?*
- *Which SMF controls are relevant?*
- *Will the auditor understand SMF terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

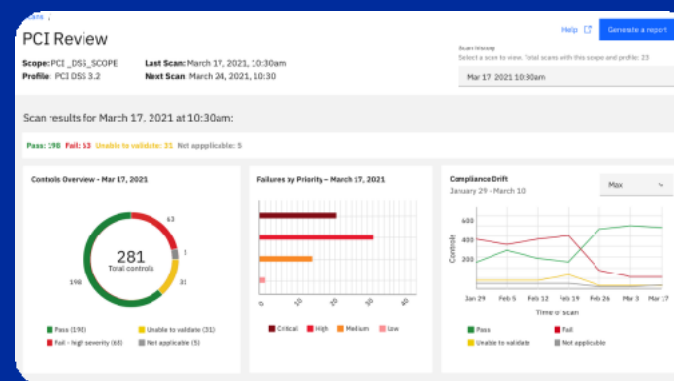
 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations, collects and validates compliance data.

With the IBM Z Security and Compliance Center, automatically collect data from SMF Type 1154 Subtype 96 and 97 to

- ✓ Check whether SMF is going to digitally sign the records that are being recorded for the log stream
- ✓ Check whether the SMF system identifier is set to the default value.
- ✓ ... and more!

Processor Activity CPACF

CP Assist for Cryptographic Functions (CPACF) is a set of z/Architecture instructions provided by the Message Security Assist (MSA) facility and its extensions. It is available on all CPs, including zIIPs, IFLs, and General Purpose CPUs. CPACF performs various cryptographic functions and supports clear and protected keys. CPACF provides significantly improved performance for many cryptographic operations.

z16 is enhanced with processor activity instrumentation to count cryptographic operations. Consequently, z/OS has been enhanced to capture crypto usage data for z/OS workloads in SMF 0, 30 and 1154 records.

Compliance data collection for Processor Activity requires z/OS 2.4 or later with PTFs for OA61511 and z16

Interpreting Regulations

Without z16

For example, the Payment Card Industry Data Security Standard (PCI-DSS) requires organizations to render a personal account number (PAN) unreadable anywhere it is stored using approaches such as strong cryptography.

- *What does this mean for CPACF?*
- *Which CPACF instructions are relevant?*
- *Will the auditor understand CPACF terminology?*


Demonstrating Compliance

Without z16

- *Where to look for evidence?*
- *How much time will it take?*
- *Who needs to be involved?*
- *Is the evidence sufficient?*

 TSO / MVS Commands?

 ISPF Panels?

 SMF Records?

Which records?

Interpreting Regulations & Demonstrating Compliance *with the z16 IBM Security & Compliance Center*



Maps IBM Z capabilities to regulations, collects and validates compliance data.

With z16 running z/OS 2.4 and later, automatically collect data from SMF Type 1154 Subtype 128 to

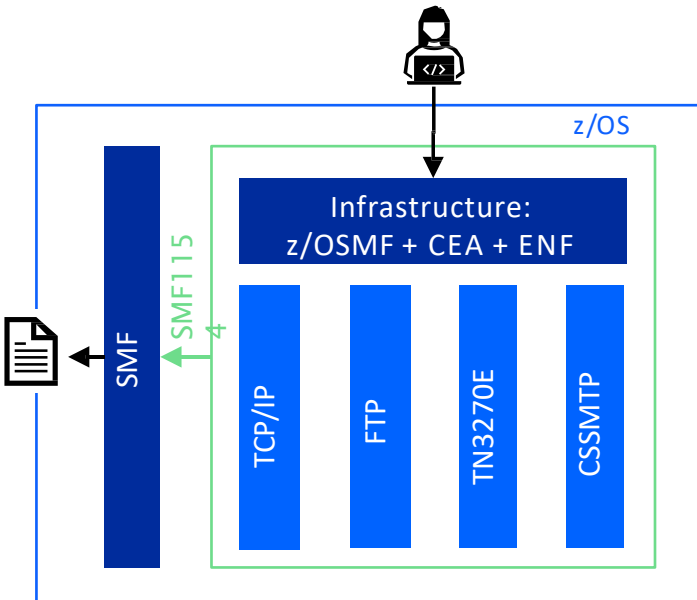
- ✓ Check that clear key operation KM-AES-256 is not in use
- ✓ Check that weak algorithm KM-DEA is not in use
- ✓ Check that weak algorithm KM-Encrypted-DEA is not in use
- ✓ ... and more!

Quick Start Guide

SMF1154 Verification

A z/OSMF compliance REST interface triggers sysplex-wide compliance data collection using an ENF86 signal. Participating z/OS components and products listen for the new ENF86 signal. When received, these components write compliance data to SMF 1154 records associated with a unique subtype.

As a quick start, you can configure z/OSMF to initiate compliance data collection for z/OS Communications Server. You will verify that you receive the new SMF 1154 records.



Step 1: Enable z/OSMF

Install PTFs for the following core infrastructure components on z/OS 2.4 or later.

- z/OSMF:PH37308
- CEA:OA61443

Configure the z/OSMF nucleus on your system and add the Compliance plug-in.

Use the Add > System action in the z/OSMF Systems table to add sysplex members to z/OSMF.

Enable the Compliance plug-in and restrict user authorization.

Authorize the z/OSMF server user ID to issue event notification facility (ENF) code 86. For example:

```
RDEFINE SERVAUTH CEA.SIGNAL.ENF86 UACC(NONE)
PERMIT CEA.SIGNAL.ENF86 CLASS(SERVAUTH) ID(IZUSVR) ACCESS(READ)
SETR RACLIST(SERVAUTH) REFRESH
```

Start z/OSMF using autostart at IPL or through an automation product.

Step 2: Enable SMF

Install PTFs for the following core infrastructure component on z/OS 2.4 or later.

- SMF:OA61444

On every participating z/OS system, edit the SMFPRMxx member to collect SMF 1154 records. Add 1154 to the list of record types that are currently specified on the TYPE= option.

Step 3: Collect data from z/OS Communications Server

Install PTFs for the following z/OS Communications Server components on z/OS 2.4 or later.

- TCP/IP:PH37372
- FTP:PH37372
- TN3270E:PH37372
- CSSMTP:PH37372

Step 4: Verify data from z/OS Communications Server

The [z/OS client web enablement toolkit](#) can invoke the z/OS Compliance REST interface to drive the collection of compliance data. The requestid parameter identifies the data collection request and can be correlated with the output in the SMF 1154 records.

After sending an HTTP request to collect compliance data, inspect the requestid and output in the SMF1154 subtype 1, 2, 3, 4 records.

Next: Collect data from additional z/OS components

Install PTFs for additional products and components on z/OS V2R5 and z/OS V2R4 to 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

Next+: Validate data with the IBM Z Security and Compliance Center

For details on additional configuration for the IBM Z Security & Compliance Center, see the "IBM Z Security and Compliance Center" guide.

Let's take a quick look at the doc...