IDUG

2025

Atlanta, GA | June 8-12

NA Db2 TECH CONFERENCE

Isn't she aDORAble? A DBAs guide to DORA, PCI DSS V4.0.1 and how to survive an audit!

Roy Boxwell, SEGUS Inc.

Session Code: D11

Platform:

Db2 z/OS

AGENDA

1. DORA/PCI DSS v4.0.1 – What are they?
2. DORA – Highlights
3. PCI DSS – Highlights
4. Vulnerability checks
5. Summary

AGENDA

1. DORA/PCI DSS v4.0.1 – What are they?
2. DORA – Highlights
3. PCI DSS – Highlights
4. Vulnerability checks
5. Summary

DORA/PCI DSS v4.0.1 – What are they (1|6)

Arrived on the 17th of January 2025:

Digital

Operational

Resilience

Act

DORA/PCI DSS v4.0.1 – What are they (2|6)

Arrived on the 31st of March 2025:

Payment Card Industry

Data Security Standard

V4.0.1

DORA/PCI DSS v4.0.1 – What are they (3|6)

Both are all about:

1) **Keeping your customer data safe**
2) **Keeping your site up to standard**
3) **Audit & Test**

DORA is for the EU and any FINTECH that works within.

PCI DSS is for the USA and Global markets primarily for, but not limited to, Credit Card companies.

Both have the same message –

“Do what you can to keep everything safe and compliant!”

DORA/PCI DSS v4.0.1 – What are they (4|6)

DORA combines a whole bunch of disparate European regulations into one unified whole for the complete finance sector (FINTECH) with some exemptions e.g. for so called microenterprises.

It was formulated on the 14th December 2022.

It came into force on the 17th January 2025.

This was a massive change in FINTECH and *not* for "just audit" as resilience is not really just about audit, is it?

DORA/PCI DSS v4.0.1 – What are they (5|6)

The DORA paperwork covers *everything* to do with being resilient in data processing (ICT – Information and Communication Technology) and covers these major points:

- **Security**
- **Operations**
- **Recoverability**
- **Test**

Here's a link, directly to the English pdf: Publications Office (europa.eu)

Or as text: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

DORA/PCI DSS v4.0.1 – What are they (6|6)

The PCI DSS paperwork also covers *everything* to do with data processing and covers these major points:

- **Installation**
- **Security**
- **Protecting data**
- **Develop and Maintain secure systems**
- **Restricted access**
- **Operations & Monitoring**
- **Test**

Here's a link, directly to the pdf: Just Published: PCI DSS v4.0.1

Or as text: https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1

AGENDA

1. DORA/PCI DSS v4.0.1 – What are they?
2. DORA – Highlights
3. PCI DSS – Highlights
4. Vulnerability checks
5. Summary

DORA - Highlights (1|18)

Chapter 2 Section II Article 6 ICT risk management framework

Paragraphs

2. …to ensure that all information assets and ICT assets are adequately protected from risks including damage and **unauthorised access or usage**.

4. Financial entities shall ensure appropriate **segregation and independence** of ICT risk management functions, control functions, and internal audit functions, according to the three lines of defence model…

6. The ICT risk management framework of financial entities, other than microenterprises, shall be subject to **internal audit** by auditors on **a regular basis** in line with the financial entities' audit plan. Those auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity.

DORA - Highlights (2|18)

Chapter 2 Section II Article 8 Identification

Paragraphs

1. … financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review **as needed, and at least yearly**, the adequacy of this classification and of any relevant documentation.

3. Financial entities, other than microenterprises, shall perform a risk assessment upon **each major change** in the network and information system infrastructure, in the processes or procedures affecting their ICT supported business functions, information assets or ICT assets.

7. Financial entities, other than microenterprises, shall on **a regular basis**, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems and, in any case before and after connecting technologies, applications or systems.

DORA - Highlights (3|18)

Chapter 2 Section II Article 9 Protection and prevention

Paragraphs

1. …financial entities shall **continuously monitor** and control the security and functioning of ICT systems and tools and shall minimise the impact of ICT risk …through the deployment of appropriate ICT **security tools, policies and procedures.**

2. …and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of **availability, authenticity, integrity and confidentiality of data**, whether **at rest**, **in use** or **in transit.**

(This bit is scary!)

3. (c) Prevent the lack of availability, the **impairment of the authenticity and integrity**, the breaches of confidentiality and the loss of data; (d) ensure that data is protected from risks arising from data management, **including poor administration**, processing related risks and human error.

DORA - Highlights (4|18)

Chapter 2 Section II Article 9 Protection and prevention

Paragraphs

4. (d) implement policies and protocols for **strong authentication** mechanisms … and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes;

DORA - Highlights (5|18)

Chapter 2 Section II Article 10 Detection

Paragraphs

1. Financial entities shall have in place mechanisms to promptly **detect anomalous activities**, in accordance with Article 17, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure.

3. Financial entities shall devote sufficient resources and capabilities to **monitor user activity**, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.

DORA - Highlights (6|18)

Chapter 2 Section II Article 11 Response and recovery

Paragraphs

1. (b) Financial entities … quickly, appropriately and effectively respond to, and resolve, all ICT-related incidents in a way that limits damage and prioritises the **resumption of activities and recovery actions.**

3. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall implement associated ICT **response and recovery plans** which, in the case of financial entities other than microenterprises, shall be subject to **independent internal audit reviews**.

DORA - Highlights (7|18)

Chapter 2 Section II Article 12 Backup policies

Paragraphs

1. For the purpose of ensuring the restoration of ICT systems and data with **minimum downtime, limited disruption** and loss, as part of their ICT risk management framework, financial entities shall develop and document:

(a) backup policies and procedures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data;

(b) restoration and recovery procedures and methods

2. …Testing of the backup procedures and restoration and recovery procedures and methods shall be **undertaken periodically**.

DORA - Highlights (8|18)

Chapter 2 Section II Article 13 Learning and evolving

Paragraphs

1. Financial entities shall have in place capabilities and staff to gather information on **vulnerabilities and cyber threats**, ICT-related incidents, in particular cyber-attacks, and analyse the impact they are likely to have on their digital operational resilience.

6. Financial entities shall develop ICT **security awareness programmes** and digital operational resilience training as **compulsory modules** in their staff training schemes. Those programmes and training shall be applicable to all employees and to **senior management** staff, and shall have a level of complexity commensurate to the remit of their functions. Where appropriate, financial entities shall also **include ICT third-party service providers** in their relevant training schemes in accordance with Article 30(2), point (i).

DORA - Highlights (9|18)

Chapter 4 Article 24 Testing

Paragraphs

1. For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial entities, other than microenterprises, shall, taking into account the criteria set out in Article 4(2), **establish, maintain and review a sound and comprehensive digital operational resilience testing programme** as an integral part of the ICT risk-management framework referred to in Article 6.

2. The digital operational resilience testing programme shall include a **range of assessments, tests, methodologies, practices and tools** to be applied in accordance with Articles 25 and 26.

6. Financial entities, other than microenterprises, shall ensure, **at least yearly**, that appropriate tests are conducted on all ICT systems and applications supporting critical or important functions.

DORA - Highlights (10|18)

Chapter 4 Article 25 Testing of ICT tools and systems

Paragraphs

1. The digital operational resilience testing programme referred to in Article 24 shall provide, in accordance with the criteria set out in Article 4(2), for the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, **performance testing**, end-to-end testing and **penetration testing**.

2. Central securities depositories and central counterparties shall **perform vulnerability assessments** before any deployment or redeployment of new or existing applications and infrastructure components, and ICT services supporting critical or important functions of the financial entity.

DORA - Highlights (11|18)

Chapter 4 Article 26 Advanced testing of ICT tools and systems / TLPT

Paragraphs

1. Financial entities … shall carry out **at least every 3 years** advanced testing by means of TLPT. Based on the risk profile of the financial entity and taking into account operational circumstances, the competent authority may, where necessary, request the financial entity to **reduce or increase** this frequency.

2. Each **t**hreat-**l**ed **p**enetration **t**est shall cover several or all critical or important functions of a financial entity, and shall be performed **on live production systems** supporting such functions.

6. At the end of the testing, after reports and remediation plans have been agreed, the financial entity and, where applicable, the external testers shall provide to the authority, … a summary of the relevant findings, the remediation plans and the documentation demonstrating that the TLPT has been conducted in accordance with the requirements.

DORA - Highlights (12|18)

Chapter 5 Section II Article 35 Powers of the Lead Overseer – Part 1

Paragraphs

1. For the purposes of carrying out the duties laid down in this Section, the Lead Overseer shall have the following powers in respect of the critical ICT third-party service providers:

(a) to request **all relevant information and documentation** in accordance with Article 37;

(b) to conduct **general investigations and inspections** in accordance with Articles 38 and 39, respectively;

(c) to request, after the completion of the oversight activities, **reports specifying the actions that have been taken** or the remedies that have been implemented by the critical ICT third-party service providers…

DORA - Highlights (13|18)

Chapter 5 Section II Article 35 Powers of the Lead Overseer – Part 2

Paragraphs

6. In the event of whole or partial non-compliance with the measures required to be taken … and after the expiry of a period of at **least 30 calendar** days from the date on which the critical ICT third-party service provider received notification of the respective measures, the Lead Overseer shall adopt a decision imposing **a periodic penalty payment** to compel the critical ICT third-party service provider to comply with those measures.

DORA - Highlights (14|18)

Chapter 5 Section II Article 35 Powers of the Lead Overseer – Part 4

Paragraphs

7. The periodic penalty payment referred to in paragraph 6 shall be imposed on **a daily basis** until compliance is achieved and for no more than a **period of six months** following the notification of the decision to impose a periodic penalty payment to the critical ICT third-party service provider.

DORA - Highlights (15|18)

Chapter 5 Section II Article 35 Powers of the Lead Overseer – Part 5

Paragraphs

8. The amount of the periodic penalty payment, calculated from the date stipulated in the decision imposing the periodic penalty payment, shall be up to **1 %** of the **average daily worldwide turnover …** in the preceding business year. When determining the amount of the penalty payment, the Lead Overseer shall take into account the following criteria regarding non-compliance with the measures referred to in paragraph 6:

(a) the gravity and the duration of non-compliance;

(b) whether non-compliance has been committed intentionally or negligently;

(c) the level of cooperation of the … provider with the Lead Overseer

Ouch!

DORA - Highlights (16|18)

Just for fun!

Name	Revenue 2023	Per day	1 % of Per day	After 182 days
HSBC Holdings	€59.85 Billion	€163.9 Million	€1.64 Million	€298.5 Million
BNP Paribas	€45.87 Billion	€125.6 Million	€1.26 Million	€229.3 Million
Lloyds Banking	€21.48 Billion	€58.8 Million	€0.59 Million	€107.4 Million

Source: Europe: leading banks by revenue 2023 | Statista

https://www.statista.com/statistics/938425/leading-banks-in-europe-by-revenue/

DORA - Highlights (17|18)

At a minimum you then need everything in your enterprise! Joking aside, you must be able to show that you have applied "Due Diligence" to at least the following areas when talking about Db2 for z/OS:

- Vulnerability checks
- Encryption at rest
- Encryption in transit
- Audit checks
- Recovery checks

DORA - Highlights (18|18)

Encryption:

At rest – All data at rest on disk must be encrypted.

In transit – With remote access (DDF) you cannot access the mainframe using a technical user id and a clear text password anymore…You *have* to move to TLS/SSL with MFA and/or certificates, possibly moving to Trusted Contexts.

Checks:

Vulnerability – How does your system look? Known problems? Dodgy GRANTs?

Audit – You must run, and archive, internal and external audits of everything on your machine.

Recovery – The absolute minimum here is that all data can be recovered. The icing on the cake is when you can meet your RTOs!

AGENDA

1. DORA/PCI DSS v4.0.1 – What are they?
2. DORA – Highlights
3. PCI DSS – Highlights
4. Vulnerability checks
5. Summary

PCI DSS - Highlights (1|24)

Business-as-Usual

- Entities should make PCI DSS Business-as-Usual (BAU)
- Assign overall responsibility for compliance
- Develop performance metrics and continuous monitoring of security controls including intrusion detection, change detection, access controls etc.
- Review of logging data more frequently to gain insights and trends

PCI DSS - Highlights (2|24)

Business-as-Usual

- Ensure that all failures in security are detected and responded to promptly
- Review changes that could introduce security risks
- Review any 3rd Party Software vendors periodically for compliance and vendor software and security support
- Periodic reviews to confirm PCI DSS requirements are being met
- All of these are “due diligence”

PCI DSS - Highlights (3|24)

The Assessor

- Sampling is an option that should not be taken!
- However, if the population to be reviewed is large then sampling of “same type” is acceptable, but must be documented and explained

PCI DSS - Highlights (4|24)

Testing Methods

- Examine: Critically evaluate data evidence including documents (electronic or physical), screenshots, config files, audit logs, and data files.
- Observe: Watch an action in the environment. For example, personnel performing a task or process, system components performing a function or responding to input, environmental conditions, and physical controls.
- Interview: Talk with individual personnel. Interview objectives may include confirmation of whether an activity is performed, descriptions of how an activity is performed, and whether personnel have particular knowledge or understanding.

PCI DSS - Highlights (5|24)

Definitions:

ASC	Approved Scanning Vendor
BIN	Bank Identification Number
CDE	Cardholder Data Environment
CHD	CardHolder Data
IRP	Incident Response Plan
PAN	Primary Account Number
POI	Point Of Interaction
SAD	Sensitive Authentication Data

PCI DSS - Highlights (6|24)

Definitions:

Significant change is:

- New hardware, software or networking equipment added to the CDE
- Any replacement or major upgrades of hard and/or software in the CDE
- Any changes in the flow or storage of account data.
- Any changes to the boundary of the CDE and/or to the scope of the PCI DSS assessment.
- Any changes to the underlying supporting infrastructure of the CDE
- Any changes to 3rd party vendors/service providers that support the CDE or meet PCI DSS requirements on behalf of the entity.

PCI DSS - Highlights (7|24)

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls. 2. Apply Secure Configurations to All System Components.
Protect Account Data	3. Protect Stored Account Data. 4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	5. Protect All Systems and Networks from Malicious Software. 6. Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	7. Restrict Access to System Components and Cardholder Data by Business Need to Know. 8. Identify Users and Authenticate Access to System Components. 9. Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	10. Log and Monitor All Access to System Components and Cardholder Data. 11. Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	12. Support Information Security with Organizational Policies and Programs.

PCI DSS - Highlights (8|24)

1: Install and maintain Network Security Controls (NSC)

- All security policies to be documented, kept up to date and in use
- Roles and responsibilities are documented, assigned and known
- Configuration standards for NSC are defined, implemented and maintained
- All networks are diagrammed and all services, protocols and ports are identified, approved and have known business yes
- All configurations are reviewed at least every six months
- In and outbound traffic to/from the CDE is restricted
- System components that store CHD are not accessible from untrusted networks
- Security controls are in place and not alterable by users

PCI DSS - Highlights (9|24)

2: Apply Secure Configurations to All System Components

- All security policies to be documented, kept up to date and in use
- Roles and responsibilities are documented, assigned and known
- Configuration standards are developed, implemented and maintained to address all known security vulnerabilities
- Vendor default account passwords changed or disabled
- Primary security across systems isolated if possible
- All unnecessary functionality removed/disabled
- Any unsecure services, protocols or daemons must be documented
- System security parameters are correctly configured
- All data encrypted in-flight

PCI DSS - Highlights (10|24)

3: Protect Stored Account Data

- All security policies to be documented, kept up to date and in use
- Roles and responsibilities are documented, assigned and known
- Account data storage is kept to a minimum by using data retention and disposal policies including a process for verifying at least every three months that stored account data has been securely deleted
- No SAD/PIN is kept after authorization – Check logs, trace, history etc.
- PAN is never displayed in full (Just BIN and last four digits are allowed) unless personnel have a legitimate business need
- PAN should be rendered unreadable anywhere it is stored
- If disk/partition level encryption is used it is only on removable media or another mechanism is *also* used directly on the PAN data
- Good crypto key management in place

PCI DSS - Highlights (11|24)

4: Protect Cardholder Data

- All security policies to be documented, kept up to date and in use
- Roles and responsibilities are documented, assigned and known
- PAN is protected with strong encryption in-flight

PCI DSS - Highlights (12|24)

5: Protect All Systems and Networks from Malicious Software

- All security policies to be documented, kept up to date and in use
- Roles and responsibilities are documented, assigned and known
- An anti-malware solution is deployed on all system components apart from those that are "not at risk from malware"
- All "not at risk from malware" components will be evaluated periodically and documented and confirmed as so
- Periodically is defined in section 12.3.1 and is now, as of 2025, **yearly**!
- The anti-malware shall run periodic scans and active/real-time scans or run continuously, all logs will be retained for analysis as per 10.5.1 (At least one year and the last three years for immediate review)
- Anti-malware cannot be altered/disabled by users
- Anti-phishing training for personnel and use of DMARC, SPF and DKIM to reduce spoofing

PCI DSS - Highlights (13|24)

6: Develop and Maintain Secure Systems and Software

- All security policies to be documented, kept up to date and in use
- Roles and responsibilities are documented, assigned and known
- Bespoke and custom software are developed using industry standards and/or best practices for secure development
- All personnel are trained at least once every year on software security relative to their job
- Bespoke and custom software is reviewed prior to production that it is developed according to secure coding and looks for existing and emerging vulnerabilities including non-author code reviews and management approval
- Injection attacks, buffer over runs etc.

PCI DSS - Highlights (14|24)

6: Develop and Maintain Secure Systems and Software

- Security vulnerabilities are identified and managed
- Bespoke and customer software patch management
- Public facing web apps should continually check for threats and detect attacks
- All changes to system components have a documented reason and have been tested and approved
- Pre-production is separated from production
- Roles and functions separated
- No pre-production data on production
- No live data on pre-production unless also in CDE and protected

PCI DSS - Highlights (15|24)

7: Restrict Access to System Components and CHD by Business Need to Know

- All security policies to be documented, kept up to date and in use
- Roles and responsibilities are documented, assigned and known
- An access model is defined with appropriate access based on the entities needs, the “least privileges required”
- Required privileges are approved by authorized personnel
- All users accounts and related access privileges are reviewed every three months
- All access by application and system accounts are reviewed periodically (every year)
- The access control system(s) is/are set to “deny all” by default
  - GRANT xxxxx on yyyyy TO PUBLIC is not good!

PCI DSS - Highlights (16|24)

8: Identify Users and Authenticate Access to System Components

- All security policies to be documented, kept up to date and in use
- Roles and responsibilities are documented, assigned and known
- All users have a unique ID
- Group/generic only on an exception basis with explicit management approval
- Addition, deletion and modification of user IDs only authorized and approved
- Access to terminated users is immediately revoked
- Inactive accounts disabled within 90 days of inactivity
- 3rd party accounts only enabled for the period required
- User session idle time out 15 minutes
- User session lock out after 10 attempts with duration before retry minimum 30 minutes
- No password/passphrase reuse of any of the last four

PCI DSS - Highlights (17|24)

8: Identify Users and Authenticate Access to System Components

- Training of users to be aware of strong passwords, password reuse etc.
- Passwords/passphrases change at least once every 90 days ***unless*** security posture is dynamic or MFA is in use
- MFA is required for all non-console access into the CDE
- Any system accounts that allow interactive login (online) are managed very carefully indeed! (Surrogate userid, SYSADM for batch etc.)

PCI DSS - Highlights (18|24)

9: Restrict Physical Access to CHD

- All security policies to be documented, kept up to date and in use
- Roles and responsibilities are documented, assigned and known
- Appropriate facility controls are in place to restrict access including video or physical access control monitors at entry/exit points and stored for three months, if not restricted by local law
- Consoles are locked when not in use
- Any visitors must be approved and escorted at all times
- All media with CHD is securely stored and the locations are reviewed every year
- All media with CHD that is sent is logged and by secure courier
- Hard copies are cross-cut shredded, incinerated or pulped
- Electronic media is physically destroyed
- POI records, inventories, inspections, training and checks

PCI DSS - Highlights (19|24)

10: Log and Monitor All Access to System Components and CHD

- All security policies to be documented, kept up to date and in use
- Roles and responsibilities are documented, assigned and known
- Audit logs are enabled and active for all access to CHD
- Audit logs for all actions taken by privileged users
- Audit logs of all access to audit logs
- Audit logs capture all invalid logical access (Brute force login attempts)
- Audit logs capture creation of new accounts, elevation or change of privilege
- Audit logs capture init of new log, start/stop/pause of logging
- Audit logs capture creation and deletion of system level objects
- Audit logs Read access limited & protected against modification

PCI DSS - Highlights (20|24)

10: Log and Monitor All Access to System Components and CHD

- Audit logs daily review:
  - All security events
  - All system components that work with CHD
  - Critical system components
  - Servers that perform security functions
- Automated Audit log review implemented
- After review, all anomalies must be investigated
- Audit logs to be held for 12 months, last three months available immediately
- Failures of critical security control systems are detected, alerted and addressed promptly

PCI DSS - Highlights (21|24)

11: Test Security of Systems and Networks Regularly

- All security policies to be documented, kept up to date and in use
- Roles and responsibilities are documented, assigned and known
- Wi-Fi checks
- Internal vulnerability checks every three months or after any “significant” change
- External vulnerability checks every three months by an ASV or after any “significant” change
- Penetration testing from inside and outside retention period of results 12 months
- Internal/External penetration testing at least once every year or after any “significant” change

PCI DSS - Highlights (22|24)

11: Test Security of Systems and Networks Regularly

- Intrusion detection and prevention techniques
- Change detection of critical files

PCI DSS - Highlights (23|24)

12: Support Information Security with Organizational Policies and Programs

- An overall information security policy is to be established, published, maintained and disseminated
- Reviewed at least once every year and updated as needed
- Responsibility is assigned to the Chief Information Security Officer
- Risks to the CHD are formally identified, evaluated and managed and also reviewed at least once every year
- A targeted risk analysis for each of the PCI DSS elements must be done
- Crypto cipher suites and protocols documented and reviewed at least once a year
- Hardware and software technology reviews at least once a year
- PCI DSS inventory and scope maintained and kept current at least once a year
- Formal security awareness training – ongoing at least yearly

PCI DSS - Highlights (24|24)

12: Support Information Security with Organizational Policies and Programs

- Employee screening for all who have access to CDE
- Written agreements with all 3rd party vendors including monitoring their compliance
- IRP – exists and ready to be used. Reviewed at least yearly and tested
- 24/7 Personnel availability when an incident occurs
- The IRP contains procedures if PAN data is found stored anywhere where it should not be (Outside the CDE)

AGENDA

1. DORA/PCI DSS v4.0.1 – What are they?
2. DORA – Highlights
3. PCI DSS – Highlights
4. Vulnerability checks
5. Summary

Vulnerability checks (1|9)

These are a new part of the kit required for DORA and PCI DSS checks!

Vulnerability checks (2|9)

The Center for Internet Security (CIS) have released a document for Db2 13 on z/OS:

CIS IBM Z System Benchmarks (cisecurity.org)

https://www.cisecurity.org/benchmark/ibm_z

Lists all you can do on the Db2 z/OS side of the road!

Vulnerability checks (3|9)

What you must check and review:

1) All security-relevant ZPARMs including defaults that should not be left at their default value! As well as DDF settings for TLS.
2) The Communication Database (CDB).
3) All GRANTs to objects in the Db2 Catalog, Directory, XML , AI.
4) All GRANTs to PUBLIC or GRANTs “WITH GRANT” option.
5) Trusted Contexts, Row Permissions, Column Masks, Audit Policies and Roles.
6) Privileged user Ids (SYSADM, SYSOPR, SQLADM etc.)

Vulnerability checks (4|9)

All security-relevant ZPARMs:

AUDITST	AUTH
AUTH_COMPATIBILITY	AUTHEXIT_CACHEREFRESH
AUTHEXIT_CHECK	
BINDNV	
DBACRVW	DISALLOW_SSARAUTH
ENCRYPTION_KEYLABEL	EXTSEC
REVOKE_DEP_PRIVILEGES	
SECADM1	SECADM2
SEPARATE_SECURITY	
SYSADM	SYSADM2
SYSOPR1	SYSOPR2
TCPALVER	

Vulnerability checks (5|9)

Defaults that should not be left at their default value:

Catalog Alias	Group Name
Member Name	SSID
Command prefix	Unknown User Id
Db2 Location Name	Db2 LU Name
DRDA Port	SECURE Port

Any one of these still being at its default value is leaving your system a little bit more open than it should be!

For Ports check that SSL is active and **all** ALIAS usage is also correct!

Vulnerability checks (6|9)

The Communication Database (CDB):

Use of SNA (VTAM is deprecated!)

Use of SYSIBM.IPLIST (Not recommended any more)

Any rows in SYSIBM.IPNAMES with a SECURITY_OUT value not = ‘R’

Any rows in SYSIBM.LOCATIONS with SECURE = ‘N’

Any rows in SYSIBM.LUNAMES with a SECURITY_OUT value not = ‘R’ or a SECURITY_IN value not = ‘V’

Any rows in SYSIBM.USERNAMES with spaces in AUTHID, LINKNAME or NEWAUTHID

Vulnerability checks (7|9)

Use of GRANTs to PUBLIC:

All SYSIBM.SYSxxxxxAUTH tables must be checked for any GRANTs to PUBLIC.

With, possibly, the exception of SYSIBM.SYSDUMMY1 there should be no GRANTs to PUBLIC found.

Even the SYSIBM.SYSDUMMY1 should not really be done anymore!

All usage of **WITH GRANT OPTION** must be checked and fixed as this does **not** conform to modern security practices.

Vulnerability checks (8|9)

For Trusted Contexts, Row Permissions, Column Masks, Audit Policies and Roles:

All of their definitions and usage must be validated and checked.

Audit Policy Usage must be also checked that, if present, they are started and are defined as tamper-proof.

Vulnerability checks (9|9)

All Privileged Ids must be discovered. Here is a listed of all privileges:

ACCESSCTRL	CREATE SECURE OBJECT
DATAACCESS	MONITOR1*
MONITOR2	SQLADM
SYSADM	SYSCTRL
SYSOPR	System DBADM

Any User ID with one of these must be validated!

* This is not *really* privileged as no sensitive (SQL Text & Audit) data is there but it can still receive and process TRACE data which is important.

AGENDA

1. DORA/PCI DSS v4.0.1 – What are they?
2. DORA – Highlights
3. PCI DSS – Highlights
4. Vulnerability checks
5. Summary

Summary

- DORA and PCI DSS are “new” kids on the block!
  - V4.0.1 changed a bunch of options to be requirements
- We must learn to live with them and the way they will affect our work.
- Are you up to speed on all of this for your firm?
- What about all your 3rd Party Vendor Software?
- Do you want to be the first firm to pay out mega-bucks?

IDUG

2025

Atlanta, GA | June 8-12

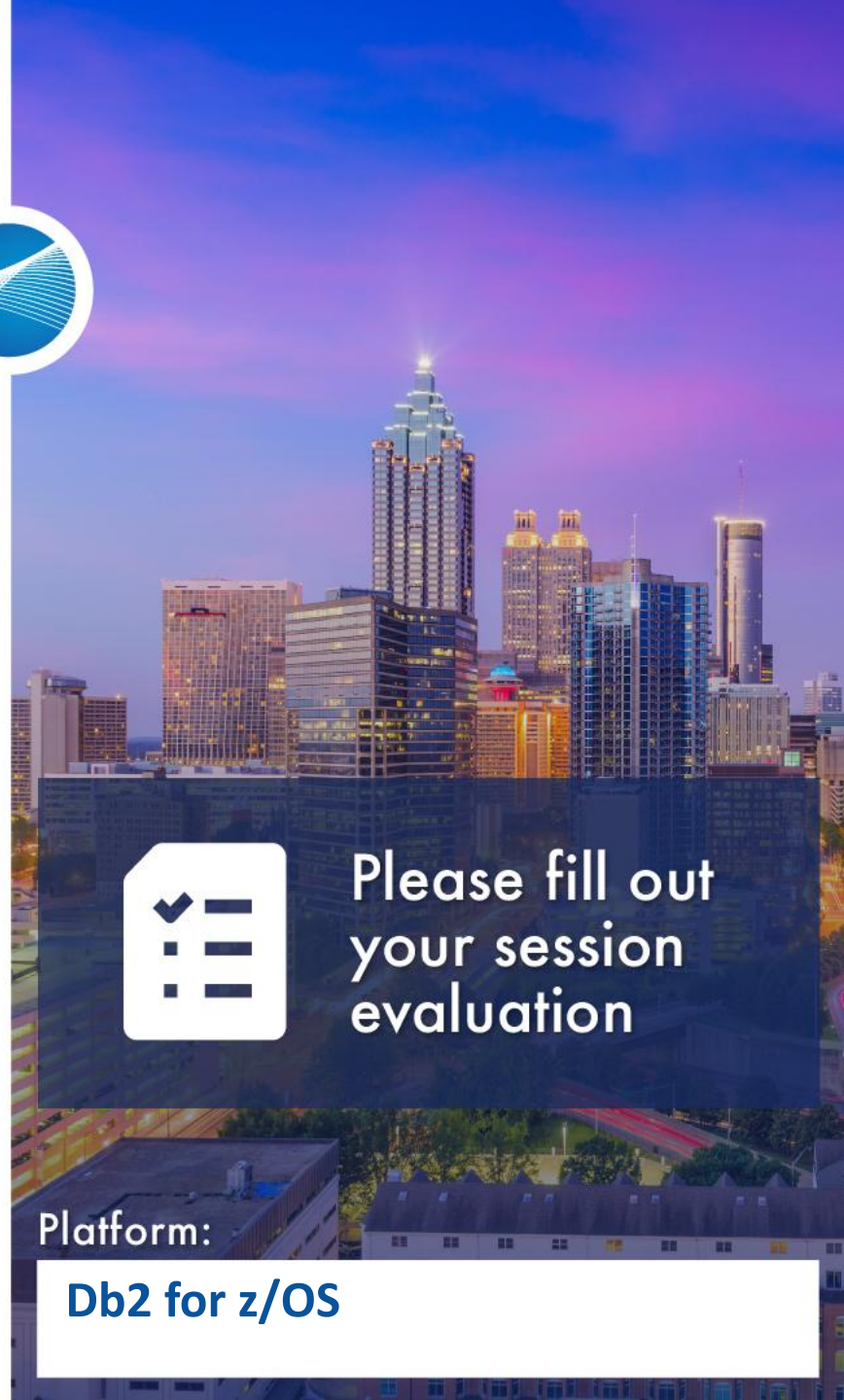
NA Db2 TECH CONFERENCE

Isn't she aDORAble? A DBAs guide to DORA, PCI DSS V4.0.1 and how to survive an audit!

Roy Boxwell, SEGUS Inc.

Contact: r.boxwell@segus.com

Session Code: D11




IDUG
2025 NA Db2 Tech Conference