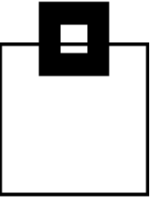

Audit your Db2 for z/OS Isn't she aDORAbLe!!

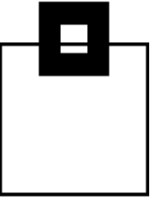
PSP05 Tuesday 29th Oct 2024

Roy Boxwell
Software Engineering GmbH



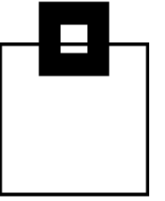
Agenda

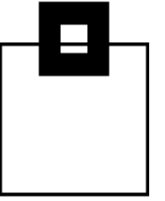
1. Audit – do you need it, do you care?!
2. DORA – What is it?
3. DORA - Highlights
4. Audit needs and musts
5. Solution overview and their Pros/Cons
6. The viable way – let Db2 do the magic!



Agenda

1. Audit – do you need it, do you care?!
2. DORA – What is it?
3. DORA - Highlights
4. Audit needs and musts
5. Solution overview and their Pros/Cons
6. The viable way – let Db2 do the magic!





YES!



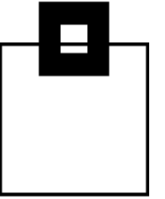
Audit – do you need it, do you care?!

GDPR is in force and companies are paying mega-bucks!






Just go here:

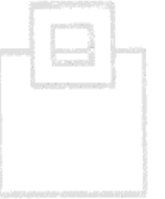
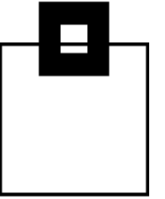
<https://www.enforcementtracker.com/>

And sort by “Fine” descending...



Audit – do you need it, do you care?!

Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type
<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>
 IRELAND	2023-05-12	1,200,000,000	Meta Platforms Ireland Limited	Art. 46 (1) GDPR	Insufficient legal basis for data processing
 LUXEMBOURG	2021-07-16	746,000,000	Amazon Europe Core S.à.r.l.	Unknown	Non-compliance with general data processing principles
 IRELAND	2022-09-05	405,000,000	Meta Platforms, Inc.	Art. 5 (1) a), c) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 24 GDPR, Art. 25 (1), (2) GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
 IRELAND	2023-01-04	390,000,000	Meta Platforms Ireland Limited	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR, Art. 12 GDPR, Art. 13 (1) c) GDPR	Non-compliance with general data processing principles
 IRELAND	2022-11-25	265,000,000	Meta Platforms Ireland Limited	Art. 25 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security

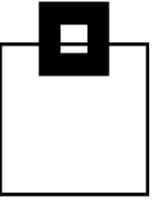


Audit – do you need it, do you care?!

Fresh off the press on the 26th August 2024:

The ride-hailing app Uber has been hit with a €290m (£246m; \$324m) fine for transferring the personal data of European drivers to US servers in violation of EU rules, the Dutch data protection regulator said on Monday.

The Dutch Data Protection Authority (DPA) said the transfers were a "serious violation" of the EU's General Data Protection Regulation (GDPR), as they failed to appropriately protect driver information.



Audit – do you need it, do you care?!

Art. 83 GDPR General conditions for imposing administrative fines

Each SA shall ensure that the imposition of administrative fines (...) be **effective, proportionate and dissuasive.**

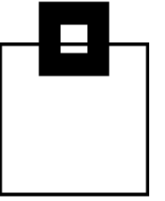
When deciding (...) due regard shall be given to the following:

the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

the intentional or negligent character of the infringement;

any action taken by the controller or processor to mitigate the damage suffered by data subjects;

the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;



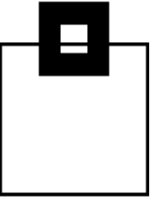
Audit – do you need it, do you care?!

Art. 83 GDPR General conditions for imposition of administrative fines

Each SA shall ensure that the administrative fine imposed (Article 83(1) GDPR) be **effective, proportionate and dissuasive.**

When deciding (...) due to the nature of the infringement given to the following factors:

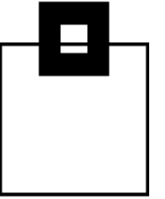
- the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing as well as the number of subjects affected and the level of damage suffered;
- the intentional or negligent character of the infringement;
- any action taken by the controller or processor to mitigate the damage suffered by data subjects;**
- the degree of responsibility of the controller or processor to account technical and organisational measures implemented by the controller or processor in accordance with Articles 25 and 32;**



Audit – do you need it, do you care?!

But GDPR is old hat these days!

Coming up on the 17th of January 2025 is DORA...

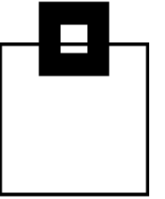


Audit – do you need it, do you care?!

But GDPR is old hat these days!

Coming up on the 17th of January 2025 is DORA...

Digital



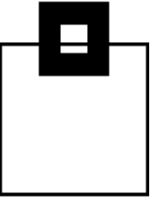
Audit – do you need it, do you care?!

But GDPR is old hat these days!

Coming up on the 17th of January 2025 is DORA...

Digital

Operational



Audit – do you need it, do you care?!

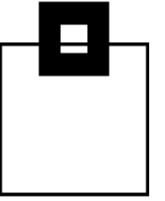
But GDPR is old hat these days!

Coming up on the 17th of January 2025 is DORA...

Digital

Operational

Resilience



Audit – do you need it, do you care?!

But GDPR is old hat these days!

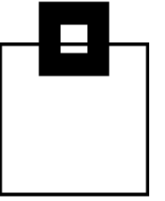
Coming up on the 17th of January 2025 is DORA...

Digital

Operational

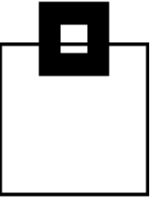
Resilience

Act



Agenda

1. Audit – do you need it, do you care?!
2. DORA – What is it?
3. DORA - Highlights
4. Audit needs and musts
5. Solution overview and their Pros/Cons
6. The viable way – let Db2 do the magic!



DORA – What is it?

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

It was formulated on the 14th December 2022.

It will come into force on the 17th January 2025. T-80 days and counting...

This is a massive change in FINTEC and **not for “just audit” as resilience is not really just about audit, is it?**

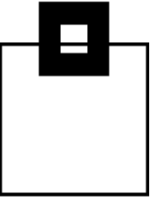
Resilience: noun

1. The capacity to withstand or to recover quickly from difficulties; toughness.

"the remarkable resilience of so many institutions"

2. The ability of a substance or object to spring back into shape; elasticity.

"nylon is excellent in wearability and resilience"



DORA – What is it?

The DORA paperwork covers ***everything*** to do with being resilient in data processing (ICT in the lingo) and covers these major points:

- Security
- Operations
- Recoverability
- Test

Here's a link, directly to the English pdf: [Publications Office \(europa.eu\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554)

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

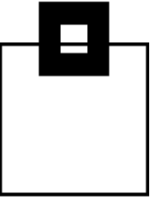
Opening Paragraphs

26: Mandates vulnerability testing

48: Maintained systems (Current Release/PTF/APAR etc.)

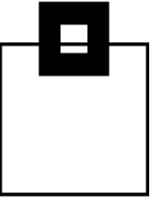
49 & 50: Recovery and RTO

56: Performance, Testing and Scanning



Agenda

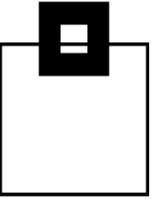
1. Audit – do you need it, do you care?!
2. DORA – What is it?
3. DORA - Highlights
4. Audit needs and musts
5. Solution overview and their Pros/Cons
6. The viable way – let Db2 do the magic!



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.



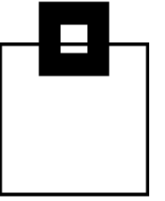
Chapter 2 Section II Article 8 Identification

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.

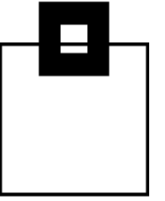


Chapter 2 Section II Article 9 Protection and prevention

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. Financial entities shall design, procure and implement ICT security policies, procedures, protocols 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.
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;

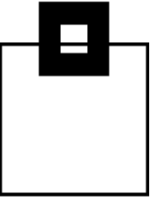


Chapter 2 Section II Article 10 Detection

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.

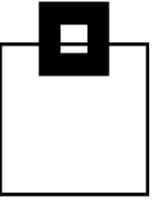
3. Financial entities shall devote sufficient resources and capabilities to **monitor user activity**, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.



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**.



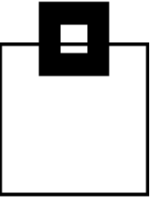
Chapter 2 Section II Article 12 Backup policies

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

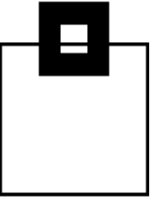
2. ...Testing of the backup procedures and restoration and recovery procedures and methods shall be **undertaken periodically**.



Chapter 2 Section II Article 13 Learning and evolving

Paragraphs

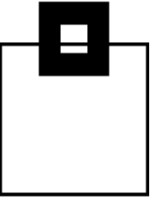
1. Financial entities shall have in place capabilities and staff to gather information on **vulnerabilities and cyber threats**, ICT-related incidents, in particular cyber-attacks, and analyse the impact they are likely to have on their digital operational resilience.
6. Financial entities shall develop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



Chapter 4 Article 24 Testing

Paragraphs

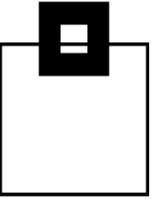
1. For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial entities, other than microenterprises, shall, taking into account the criteria 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.



Chapter 4 Article 25 Testing of ICT tools and systems

Paragraphs

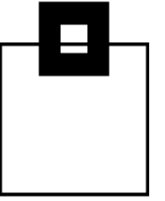
1. The digital operational resilience testing programme referred to in Article 24 shall provide, in accordance with the criteria set out in Article 4(2), for the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, 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.



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 **threat-led penetration test** 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.



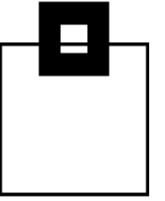
Chapter 5 Section II Article 35 Powers of the Lead Overseer – Part 1

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...

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.



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

Paragraphs

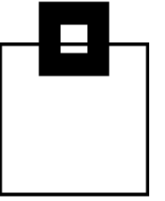
7. The periodic penalty payment referred to in paragraph 6 shall be imposed on **a daily basis** until compliance is achieved and for no more than a **period of six months** following the notification of the decision to impose a periodic penalty payment to the critical ICT third-party service provider.

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** of the critical ICT third-party service provider 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 ICT third-party service provider with the Lead Overseer

Ouch!



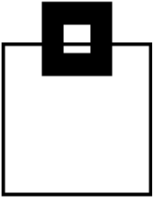
DORA – Highlights

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/)

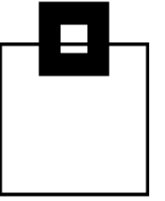
<https://www.statista.com/statistics/938425/leading-banks-in-europe-by-revenue/>



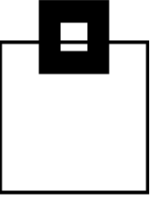
DORA - Highlights

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:

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



DORA - Highlights



Encryption at rest – You should all have this now, all data at rest on disk must be encrypted.

Encryption in transit – More and more work is “flying over the wire” and today 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.

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

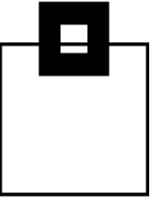
Audit checks – This is the rest of this presentation!

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



Agenda

1. Audit – do you need it, do you care?!
2. DORA – What is it?
3. DORA - Highlights
4. Audit needs and musts
5. Solution overview and their Pros/Cons
6. The viable way – let Db2 do the magic!

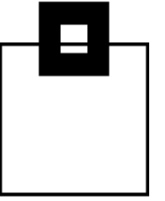


Audit needs and musts

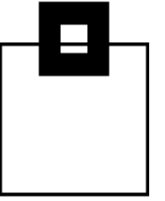
Critical activities that enterprises should be auditing:

- Privileged Users
 - Access/changes/deletion to critical data
 - Access using inappropriate channels
 - Schema modifications
 - Unauthorized addition of user accounts

Who is the privileged user?



Audit needs and musts

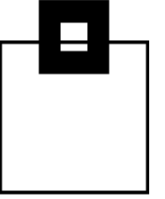


Critical activities that enterprises should be auditing:

- End Users
 - Unusual access to excessive amounts of data
 - Access to data outside standard working hours
 - Access to data through inappropriate channels
- Developers, Analysts and System Administrators
 - Access to live production systems
- IT Operations
 - Inappropriate changes to DB/DB applications



Audit needs and musts



Collect as much data as you can, because you probably don't know today what you'll need tomorrow

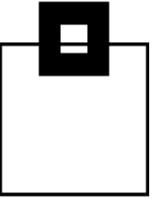
→ Breach patterns do change!!!

Make sure you include:

- SELECTs (against sensitive data)
- DDL
- DML
- DCL
- Utilities (online + offline)
- Commands
- Assignment, or change of a user ID/authorization – especially privileged users



Audit needs and musts



Be mindful of what happens outside of a table:

- Consider clones
- Consider backups
- Consider extended statistics in catalog tables, like SYSCOLDIST + SYSKEYTGTDIST
- Consider utility output (REORG, RUNSTATs)
- Consider UNLOADs
- Consider replication
- Consider access to the underlying VSAM cluster

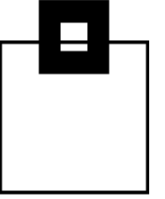


Also consider your INSTALL SYSADM/SYSOPR

→ Sorry DBAs, but auditing requires a separation of duties



Audit needs and musts



The Db2 Audit Trace is a great starting point:

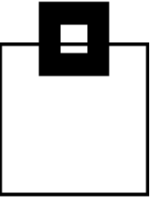
- Classes 1, 2, 7, 8 have very little overhead
 - Access violations (Class 1 IFCID 140)
 - GRANTs/REVOKEs (Class 2 IFCID 141)
 - Assignment, or modification of a user ID/authorization (Class 7 IFCIDs 55, 83, 87, 169, 319)
 - Db2 utility (Class 8 IFCIDs 23, 24, 25, 219, 220)
- Class 3 (IFCID 142) has very little overhead
 - DDL (only for TB having the AUDIT ALL attribute)



Audit needs and musts

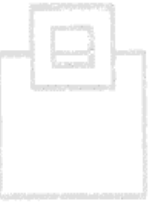
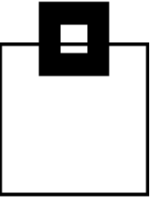
The Db2 Audit Trace:

- Classes 4, 5 (IFCIDs 143, 144) have up to 5% overhead
 - 1st INSERT/UPDATE/DELETE, SELECT in a UOR
- Class 10 (IFCIDs 269, 270) has low overhead
 - Trusted context DDL and Usage
- IFCIDs 90, 91 have very little overhead
 - Db2 Commands

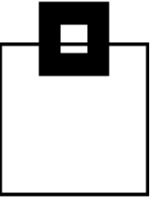


Agenda

1. Audit – do you need it, do you care?!
2. DORA – What is it?
3. DORA - Highlights
4. Audit needs and musts
5. Solution overview and their Pros/Cons
6. The viable way – let Db2 do the magic!



Solution overview and their Pros/Cons



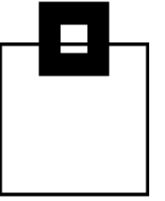
There are a variety of existing resources Db2 already provides/comes with:

- Db2 Log
- Db2 Trace
- Db2 Memory (DSC/EDM)
- Db2 Exits



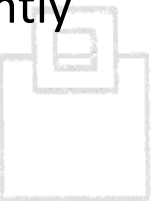
IBM Db2

Solution overview and their Pros/Cons

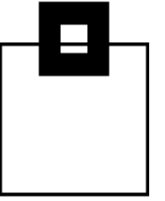


Db2 Log:

- Pros:
 - Comes with Db2 and supports all versions
 - No additional overhead
 - No additional costs (except you want to keep logs for a longer period of time than currently and, of course, your analysis)
 - Most companies have log analysis tools they're already familiar with
- Cons:
 - Not all required data is logged
 - SELECTs are especially lacking

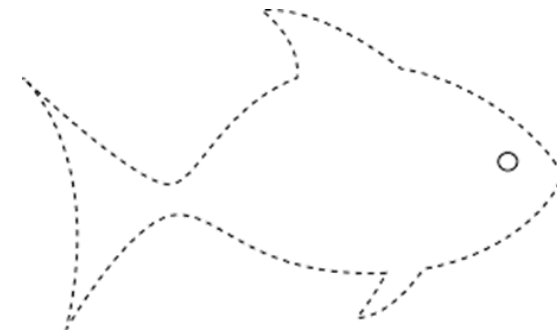


Solution overview and their Pros/Cons

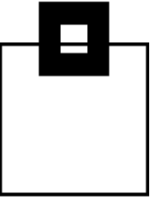


Db2 Trace:

- Pros:
 - Comes with Db2 and supports all versions
 - No additional costs (except for storing and processing the collected data)
 - Most companies have trace data analysis tools they're already familiar with
- Cons:
 - Depending on the scope (number of IFCIDs/classes), and the type (SMF, OPX, GTF, SRV), the overhead may be significant
 - You need to build your own repository
 - If not using OPX you lose time!



Solution overview and their Pros/Cons



Db2 Trace:

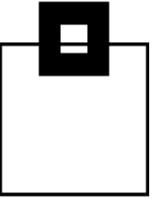
- What are the differences:
 - There are different types of traces:
 - Statistics, Accounting, Audit, Monitor, Performance, Global
 - There are different classes
 - There are hundreds of individual IFCIDs

- Depending on your choice, the overhead is unmeasurable to significant

- A key difference in cost is the trace destination!
 - SMF, OPX, GTF, SRV



Solution overview and their Pros/Cons



Db2 Trace: What are the differences:

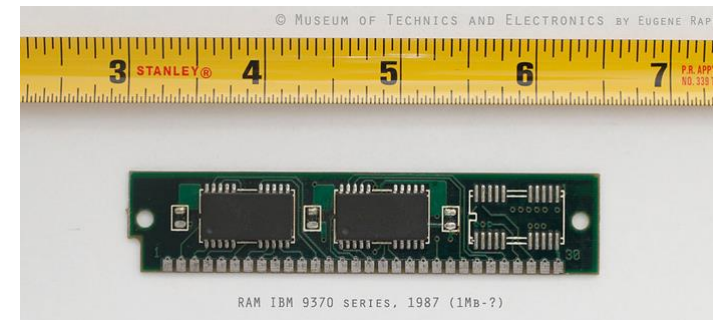
- Processing the data requires simple to more sophisticated knowledge:
 - SMF: System Management Facility:
Most commonly used, easy to process (use DSN1SMFP) – Once a day “cuts” cost 24 hours
 - OPn/OPX: Buffer Destination Trace
Very efficient, but Assembler needed to process (DSN1SDMP is pretty poor)
 - GTF: Generalized Trace Facility:
Used for detailed monitoring
 - SRV: Serviceability Routine:
I have never seen it used
 - ZAI: Db2 13 FL505 - New trace for IBM Db2 AI for z/OS users only!



Solution overview and their Pros/Cons

Db2 Memory (DSC/EDM):

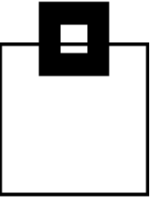
- Pros:
 - Comes with Db2 and supports all versions
 - No additional overhead
 - No additional costs (except for storing and processing)
- Cons:
 - Not all required data is there
 - Usually you can't access it yourself, unless you hook into it
 - The information is volatile and can get lost quickly



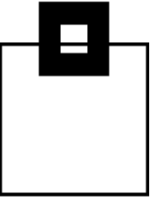
Solution overview and their Pros/Cons

Db2 Exits:

- Pros:
 - Partially comes with Db2 and supports all versions
 - No additional costs (except for storing and processing)
- Cons:
 - Not all required data is there
 - Lots of coding necessary to catch and process the data
 - The overhead may be significant



Solution overview and their Pros/Cons

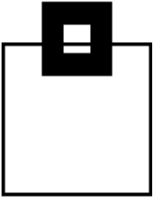


Additional Tools:

- Pros:
 - There are various solutions to choose from
 - Usually easy to use and more powerful than native Db2 options
- Cons:
 - Vendors charge for it
 - Implementation and processing overhead may be significant
 - Additional appliances lead to more vulnerability and administration overhead



Solution overview and their Pros/Cons



Additional Tools:

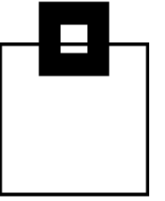
- What are the differences?
 - Good solutions have efficient data collectors and share repositories for Audit, Performance Management, Accounting, Analytics ...
 - Some solutions use hooks into the Db2 address space to capture SQL activity – errors can bring down Db2, or the entire LPAR, thus they try to protect Db2 by encapsulating the “foreign” code
 - Some solutions need additional appliances (easily up to 100+ virtual appliances) → all SQL captured is sent (unencrypted!) through the network. If the connection gets lost they try to cache it. Keep in mind that attackers do DDoS attacks! Archive.org for example...

https://en.wikipedia.org/wiki/Internet_Archive_cyberattack



Agenda

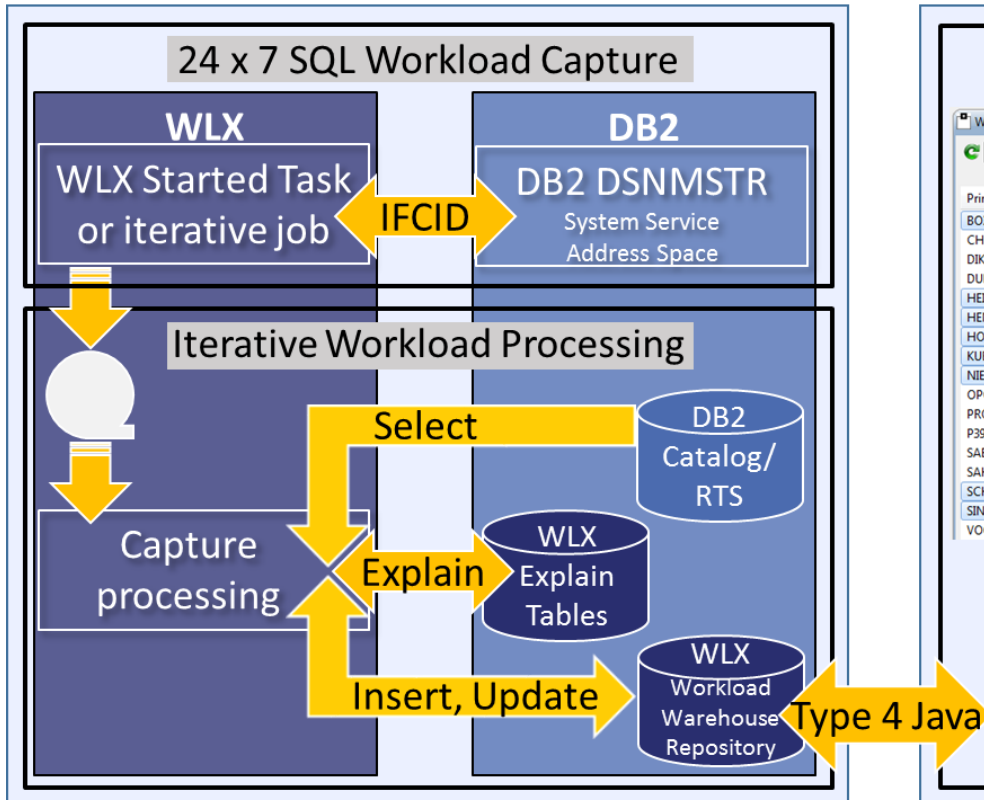
1. Audit – do you need it, do you care?!
2. Audit needs and musts
3. Solution overview and their Pros/Cons
4. The viable way – let Db2 do the magic!
5. A special announcement!



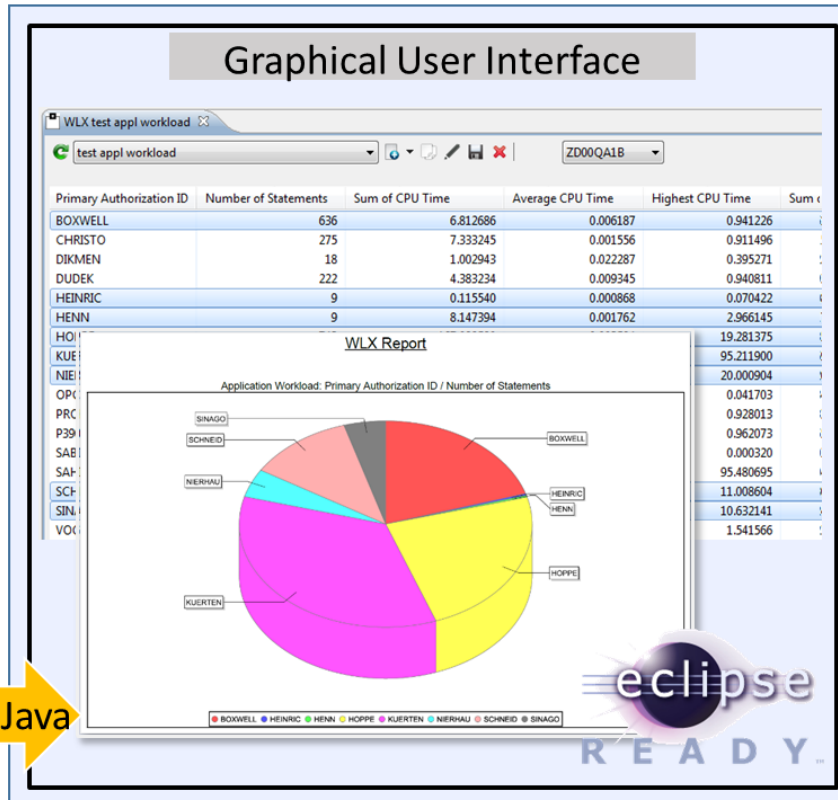
The viable way – let Db2 do the magic

Efficient data collector for your desired scope of Audit

Mainframe Engine



Workstation Engine

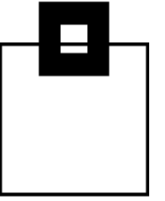


The viable way – let Db2 do the magic

The most reliable/efficient solution is based on those reliable and robust Db2 key functions we've been using for ages. Exploiting them results in the most powerful solution:

- You benefit from rock solid features, like:
 - Security
 - Compression
 - Native Db2 functions
 - Extended Client Identification Registers, `sqleseti()`

The only question is: What key Db2 functions are needed?



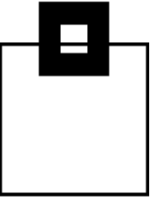
The viable way – let Db2 do the magic

Using IFCIDs along with OPX buffers delivers in-depth information without the overhead and delay of SMF processing.

The absolute minimum requirement is to get the SQL that is running in the enterprise, so at least:

316/318 Dynamic SQL (SELECT, INSERT, etc.)
(+317 for the full SQL statement)

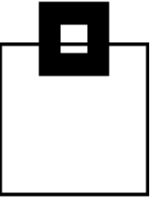
400/401 Static SQL (SELECT, INSERT, etc.)
(+SYSPACKSTMT for the full SQL statement)



The viable way – let Db2 do the magic

Using IFCIDs along with OPX buffers delivers in-depth information without the overhead and delay of SMF processing.

23/24/25	Utility start, phase change, and stop
219/220	Utility Listdef and Template
55/83/87/ 169/319	SQLID setting
62/142	DDL and CREATE/ALTER/DROP for tables with AUDIT changes or all
90/91	Commands and their completion status

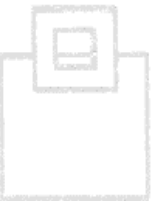
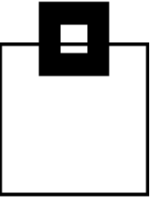


The viable way – let Db2 do the magic

Using IFCIDs along with OPX buffers delivers in-depth information without the overhead and delay of SMF processing:

140	Authorization failures
141	Authorization changes
143/144	AUDIT Table access
197	Console messages
269/270/271	Trusted Context DDL/Usage and Column Masks/Row Permissions
361	Administrative Authority usage
404	LOAD Authority usage

Add the correlation headers to get detailed authentication data.

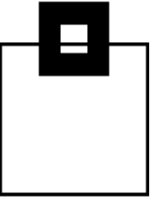


The viable way – let Db2 do the magic

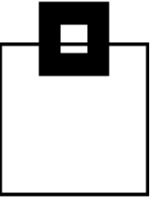
So now you have all that data for Audit. But also now think about what else you could do with all of it...

Just imagine the performance data contained within...or the usage analysis possible...

The possibilities are endless! This is a fantastic data source created for Audit but available for performance DBAs and even developers! (and also for DORA!!!)



The viable way – let Db2 do the magic



All IFCIDs listed have a much smaller footprint than a blanket AUDIT CHANGES/ALL.

This is integrated, reliable Db2 technology, OPX is the right target for efficient capturing. Store it in a repository and protect it using proven technology (e.g. RACF, ACF2, Top Secret)

Using Db2 compression reduces storage requirements by exploiting proven, integrated technology.



→ No new vulnerabilities like:

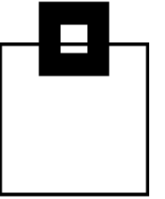
- Black Box appliance
- Massive sensitive data transmissions over the network



The viable way – let Db2 do the magic

Do your (automated) reporting/alerting/analytics as needed:

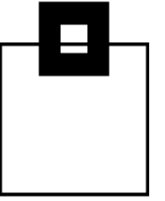
- SPUFI
- Batch Job
- Enterprise-wide reporting system
- GUI (DRDA based queries are fully zIIP eligible)
 - Eclipse based
 - Zowe based



The viable way – let Db2 do the magic

DSC and EDM provide detailed workload insights, including flushed statements:

- SQL text
- Statement ID
- Date/time
- Current status
- Resource consumption
- Identification/environmental data

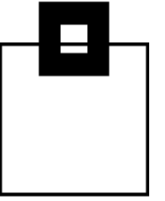


The viable way – let Db2 do the magic

Use a GUI front end:

Exploit and integrate into Eclipse based GUI front ends

- GUIs can come as a Plug-in for
 - IBM Rational
 - IBM Data Studio
 - Eclipse native
- Use Zowe – It rocks!
- Existing Db2 connections are used to connect to the mainframe
- Interactive dialogs allow complex and powerful analysis
- Export features can create PDF reports and allow MS Excel handover



The viable way – let Db2 do the magic

The screenshot shows the SQL WorkloadExpert GUI. The top toolbar contains several icons with callout boxes: 'New', 'Select query', 'Execute query', 'Edit', 'Delete', 'Copy', 'Save', 'SQL', 'MS Excel export', and 'Import/Export'. A dropdown menu on the right shows 'QA1B' and 'Selected database connection'. The main window displays the 'SQL WorkloadExpert for Db2 z/OS' title and a table of application workload data.

GUI features – button overview

Zowe overview

Statement Origin	Package	Primary Authorization ID	Collection ID	Number of Statements	Sum of CPU Time	Average CPU Time	Highest CPU Time
D	n/a		n/a	324	5	0.00009	1.85644
D	n/a		n/a	20	0	0.000379	0.003515
D	n/a		n/a	34	0	0.000516	0.016252

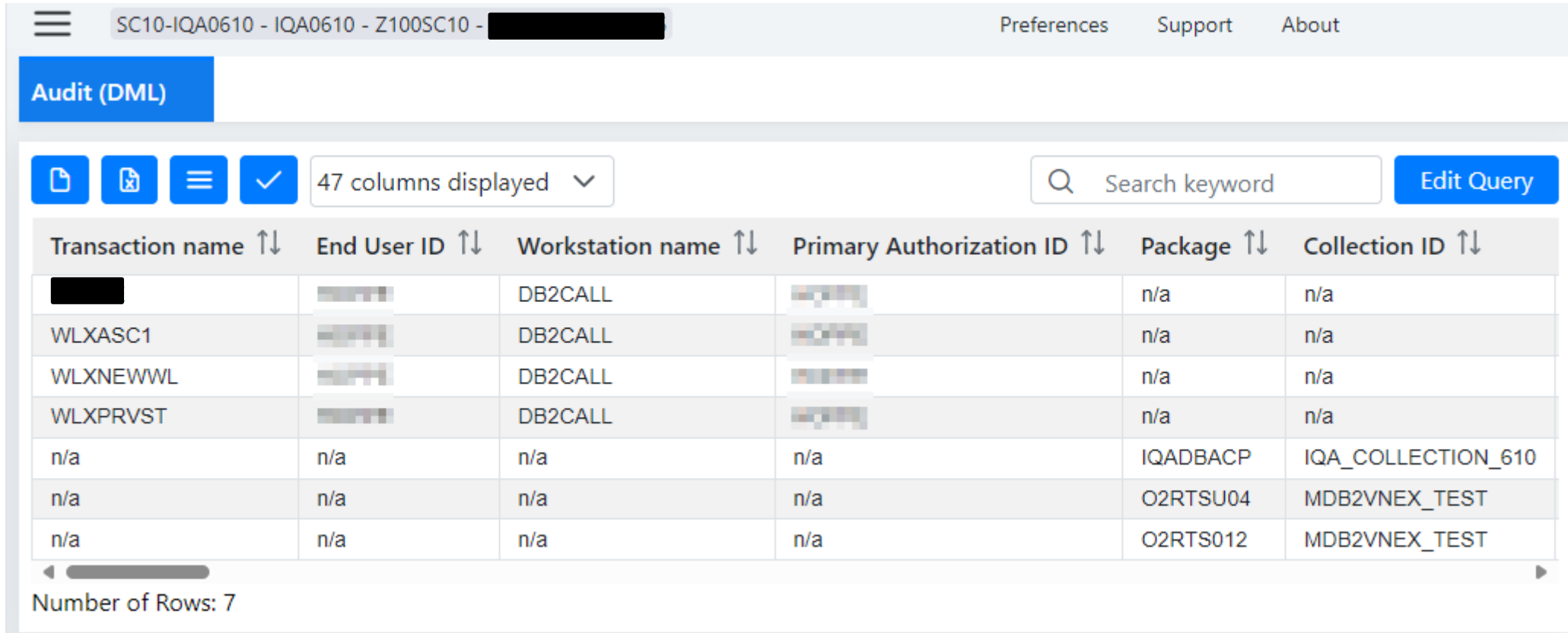
The viable way – let Db2 do the magic

Choose how you'd like to find out who did what and when...

The screenshot displays the 'WLX Audit for Db2 z/OS' application window. The interface is organized into a tree view with three main columns of categories. The first column contains categories like 'Access to audited tables', 'Administrative authorities', 'Audit (DML)', 'Authorization compatibility settings', 'Authorization failures', 'CREATE, ALTER, DROP (DDL)', and 'CREATE, ALTER, DROP (DDL) audited tables'. The second column includes 'Db2 commands', 'Db2 console messages - Details', 'Db2 console messages - Overview', 'Delay deltas', 'Distributed translation', 'DBADM data updates', 'DBADM object update', 'End of identify', 'End of signon in IMS/CICS', and 'GRANTs and REVOKEs (DCL)'. The third column lists 'Object Update Dynamic', 'PUBLIC access to tables', 'Row permission', 'Security Processing', 'Set current SQLID', 'Show Primary Authorization IDs', 'System DBADM data update', and 'System DBADM object update'. To the right of these columns is a vertical scroll bar with a slider. On the far right, there is a vertical stack of icons: a black square at the top, followed by three document icons, and a fourth document icon at the bottom. A vertical scroll bar is also present next to these icons.

The viable way – let Db2 do the magic

Choose how you'd like to find out who did what and when...



The screenshot shows the Db2 Audit (DML) interface. At the top, there is a header with a menu icon, the text "SC10-IQA0610 - IQA0610 - Z100SC10 - [REDACTED]", and links for "Preferences", "Support", and "About". Below the header is a blue button labeled "Audit (DML)".

The main area contains a toolbar with icons for document, refresh, menu, and checkmark, followed by a dropdown menu showing "47 columns displayed". To the right is a search box labeled "Search keyword" and a blue "Edit Query" button.

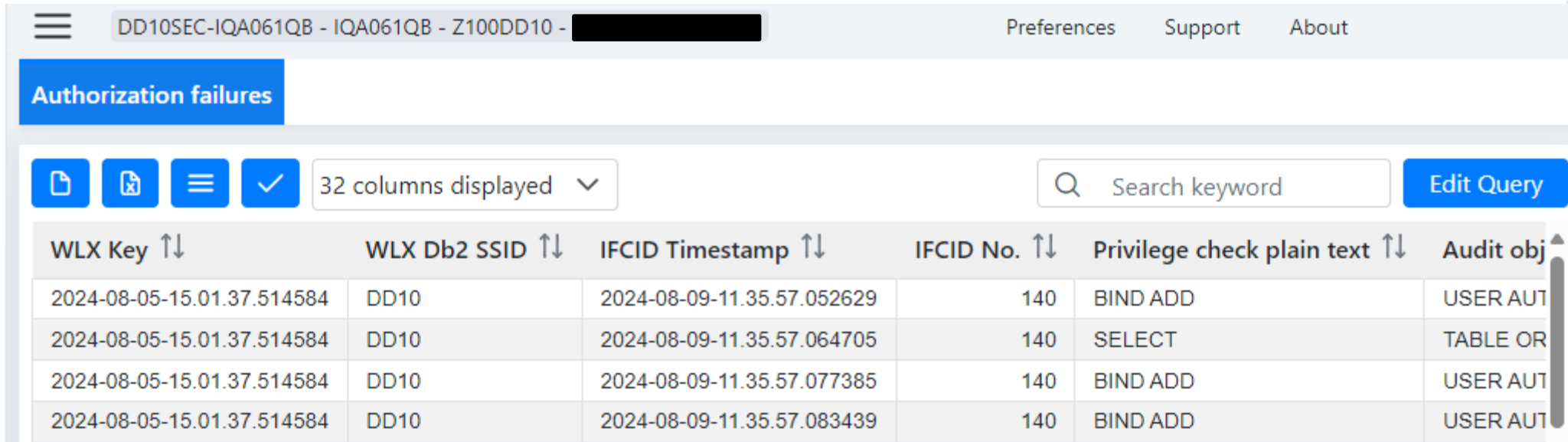
Below the toolbar is a table with the following columns: "Transaction name", "End User ID", "Workstation name", "Primary Authorization ID", "Package", and "Collection ID". Each column has a sort icon (up/down arrows). The table contains 7 rows of data:

Transaction name	End User ID	Workstation name	Primary Authorization ID	Package	Collection ID
[REDACTED]	[REDACTED]	DB2CALL	[REDACTED]	n/a	n/a
WLXASC1	[REDACTED]	DB2CALL	[REDACTED]	n/a	n/a
WLXNEWWL	[REDACTED]	DB2CALL	[REDACTED]	n/a	n/a
WLXPRVST	[REDACTED]	DB2CALL	[REDACTED]	n/a	n/a
n/a	n/a	n/a	n/a	IQADBACP	IQA_COLLECTION_610
n/a	n/a	n/a	n/a	O2RTSU04	MDB2VNEX_TEST
n/a	n/a	n/a	n/a	O2RTS012	MDB2VNEX_TEST

At the bottom left of the table area, it says "Number of Rows: 7".

The viable way – let Db2 do the magic

Choose how you'd like to find out who did what and when...



DD10SEC-IQA061QB - IQA061QB - Z100DD10 - [REDACTED] Preferences Support About

Authorization failures

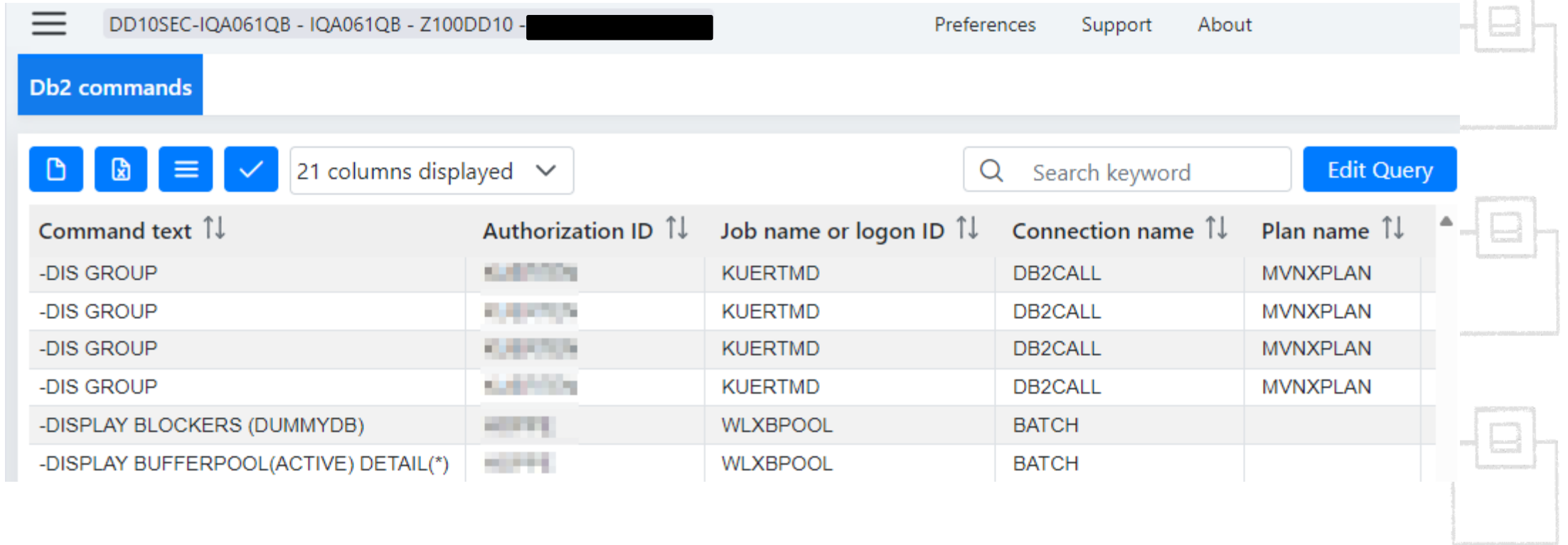
32 columns displayed

Search keyword Edit Query

WLX Key ↑↓	WLX Db2 SSID ↑↓	IFCID Timestamp ↑↓	IFCID No. ↑↓	Privilege check plain text ↑↓	Audit obj ↑↓
2024-08-05-15.01.37.514584	DD10	2024-08-09-11.35.57.052629	140	BIND ADD	USER AUT
2024-08-05-15.01.37.514584	DD10	2024-08-09-11.35.57.064705	140	SELECT	TABLE OR
2024-08-05-15.01.37.514584	DD10	2024-08-09-11.35.57.077385	140	BIND ADD	USER AUT
2024-08-05-15.01.37.514584	DD10	2024-08-09-11.35.57.083439	140	BIND ADD	USER AUT

The viable way – let Db2 do the magic

Choose how you'd like to find out who did what and when...



The screenshot shows the Db2 command interface. At the top, there is a header bar with a menu icon, the session ID 'DD10SEC-IQA061QB - IQA061QB - Z100DD10 - [REDACTED]', and links for 'Preferences', 'Support', and 'About'. Below the header is a blue 'Db2 commands' button. The main area contains a toolbar with icons for file operations and a '21 columns displayed' dropdown. A search bar with the text 'Search keyword' and an 'Edit Query' button is also present. The central part of the interface is a table with the following columns: 'Command text', 'Authorization ID', 'Job name or logon ID', 'Connection name', and 'Plan name'. The table contains six rows of data.

Command text ↑↓	Authorization ID ↑↓	Job name or logon ID ↑↓	Connection name ↑↓	Plan name ↑↓
-DIS GROUP	[REDACTED]	KUERTMD	DB2CALL	MVNXPLAN
-DIS GROUP	[REDACTED]	KUERTMD	DB2CALL	MVNXPLAN
-DIS GROUP	[REDACTED]	KUERTMD	DB2CALL	MVNXPLAN
-DIS GROUP	[REDACTED]	KUERTMD	DB2CALL	MVNXPLAN
-DISPLAY BLOCKERS (DUMMYDB)	[REDACTED]	WLXBPOOL	BATCH	
-DISPLAY BUFFERPOOL(ACTIVE) DETAIL(*)	[REDACTED]	WLXBPOOL	BATCH	

The viable way – let Db2 do the magic

Optionally, use our LEEF (Log Event Extended Format) or sysloger support for the SIEM system of your choice!

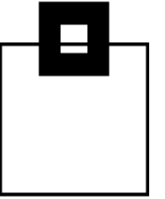


```
LEEF:1.0|Software Engineering GmbH|WorkLoadExpert Audit|6.1|
IFCID 090|cat=success|devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSZ|
devTime=2018-03-09T09:57:33.886+0100|Sev=01|usrName=GABELMA|
name=|usrPriv=|usrGroups=|src=|subsys=DC10|dsn=|plan=MVNXPLAN|
objtyp=|obj=|intent=|SQLid=GABELMA|poe=|submitby=|job=Z100 DC10|
cmd=-DIS GROUP|checkid=|conn=DC10 location Z100DC10 LU DESWEG01.Z100DC10
group DC10 member DC10 connector DB2CALL GABELMA operator GABELMA
workstation DB2CALL tx GABELMA enduser GABELMA|sum=DB2 DC10 GABELMA
Command Issued by id GABELMA:-DIS GROUP
```

The viable way – let Db2 do the magic

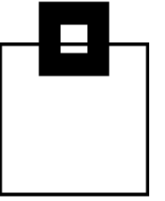
These days most z/OS Audit systems collect data and transfer to a Data Lake of your choice for post processing every one or two hours, e.g. WorkLoadExpert, zSecure etc.

This data is typically RACF, SMF and Master Log data on its way to e.g. QRadar, Splunk, AlienVault et al.



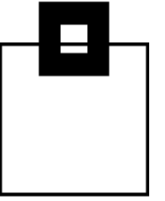
Agenda

1. Audit – do you need it, do you care?!
2. DORA – What is it?
3. DORA - Highlights
4. Audit needs and musts
5. Solution overview and their Pros/Cons
6. The viable way – let Db2 do the magic!
7. Something new...



Agenda

1. Audit – do you need it, do you care?!
2. DORA – What is it?
3. DORA - Highlights
4. Audit needs and musts
5. Solution overview and their Pros/Cons
6. The viable way – let Db2 do the magic!
7. A **free** SecurityAudit HealthCheck for Db2 z/OS

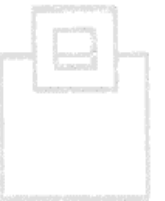
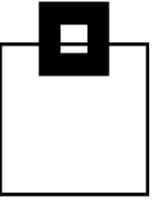


SecurityAudit HealthCheck for Db2 z/OS

This year's SEG Christmas give-away will be a SecurityAudit HealthCheck for Db2 z/OS – Short form: SAC2.

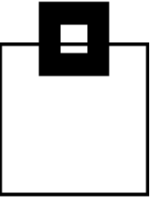
It audits six “classes” of things:

- 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.)



SecurityAudit HealthCheck for Db2 z/OS

If you remember how we started, you can tell that this covers a lot of the same ground as a traditional audit, but with the extra boost of being a full vulnerability check at the same time!



SecurityAudit HealthCheck for Db2 z/OS

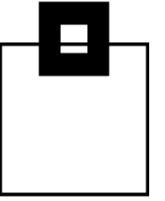
If you remember how we started, you can tell that this covers a lot of the same ground as a traditional audit, but with the extra boost of being a full vulnerability check at the same time!

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

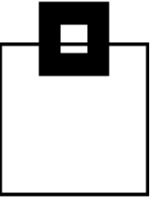
[CIS IBM Z System Benchmarks \(cisecurity.org\)](https://www.cisecurity.org/benchmark/ibm_z)

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

SAC2 covers all of the benchmark checks apart from External Security exits and SMP/E –
Some things remain manual!



SecurityAudit HealthCheck for Db2 z/OS



All security-relevant ZPARMs:

AUDITST
AUTH_COMPATIBILITY
AUTHEXIT_CHECK
BINDNV
DBACRVW
ENCRYPTION_KEYLABEL
REVOKE_DEP_PRIVILEGES
SECADM1
SEPARATE_SECURITY
SYSADM
SYSOPR1
TCPALVER

AUTH
AUTHEXIT_CACHEREFRESH

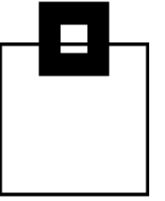
DISALLOW_SSARAUTH
EXTSEC

SECADM2

SYSADM2
SYSOPR2



SecurityAudit HealthCheck for Db2 z/OS



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 it also checks that SSL is active and **all** ALIAS usage is also correct.



SecurityAudit HealthCheck for Db2 z/OS

The Communication Database (CDB). Reporting any problems found and recommendations:

Use of SNA (VTAM is deprecated!)

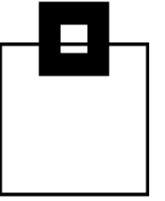
Use of SYSIBM.IPLIST (Not recommended any more)

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'

USERNAMES listing out those with spaces in AUTHID, LINKNAME or NEWAUTHID



SecurityAudit HealthCheck for Db2 z/OS

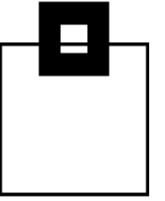
Use of GRANTs to PUBLIC:

All SYSIBM.SYSxxxxAUTH tables will be checked for any GRANTs to PUBLIC.

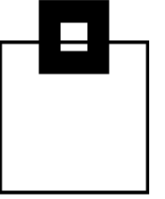
With, possibly, the exception of SYSIBM.SYSDUMMY1 there should be no GRANTs to PUBLIC found.

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

All usage of WITH GRANT OPTION will be listed as this does not conform to modern security practices.



SecurityAudit HealthCheck for Db2 z/OS



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

All Trusted Contexts will be listed with Auth Ids and Attributes.

All Row Permissions will be listed.

All Column Masks will be listed.

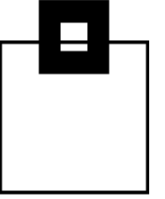
All Audit Policy Usage will be decoded, listed and verified as being started and/or tamper-proof.

All Roles will be listed.

All of these must be individually validated that they are all 100% correct!



SecurityAudit HealthCheck for Db2 z/OS



All Privileged Ids will be listed with their respective Privilege(s):

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

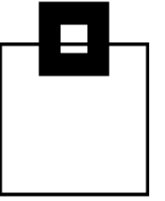


All of these must be individually validated that they are all 100% correct!

SecurityAudit HealthCheck for Db2 z/OS

All of this data as well as a Recovery Report, available in our RealTimeDatabaseExpert (RTDX) product, and the usage of our WorkLoadExpert (WLX) Audit Use Case will arm you to be able to deliver the reports that the Lead Overseer will be requesting.

Running these Audits, Vulnerability checks and Audit Use Cases on a regular basis will prove “Due Diligence” has been done and can be used to mitigate any fines issued against your firm.

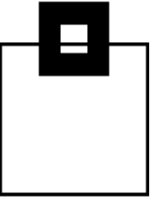


SecurityAudit HealthCheck for Db2 z/OS

All of this data as well as a Recovery Report, available in our RealTimeDatabaseExpert (RTDX) product, and the usage of our WorkLoadExpert (WLX) Audit Use Case will arm you to be able to deliver the reports that the Lead Overseer will be requesting.

Running these Audits, Vulnerability checks and Audit Use Cases on a regular basis will prove “Due Diligence” has been done and can be used to mitigate any fines issued against your firm.

Do **not** try and be the first company fined 1% of their gross daily earnings!



Questions???

Many thanks for your attention and now....

