

# Internal Audit Report

## 2025-064 Risk Management

### December 23, 2025

- CONFIDENTIAL -

Audit scope period	January 2023 to July 2025
Legal entities in scope	DBAG/ExR/EFAG/ECAG/CEU/CBL/CH/CI/CS/LuxCSD
IA function	DBAG/ECAG/CEU/CBL
Location	Eschborn, Luxembourg

Results	S1	S2	S3	S4
<i>Total Internal Audit findings: 11</i>	5	6	0	0
<i>Self-identified Issues: 1</i>	0	1	0	0

## 1. Executive summary

Internal Audit performed an audit of the Risk Management framework from August to October 2025 across ten legal entities, including DBAG, Eurex Repo, EFAG, ECAG, CEU, CBL, CH, CI, CS and LuxCSD. The audit assessed the design and operating effectiveness of the Group's risk management processes, governance, and controls.

While foundational elements of the risk management framework are established, the audit identified several deficiencies in governance, documentation, and control execution. A key takeaway from the audit is the need to address the reliance on manual data processing. While other governance and documentation issues also require attention, the potential for operational errors and data integrity issues stemming from manual controls is an important consideration for the Group's risk posture.

A notable point for concern is the extensive reliance on manual processes and insufficient controls over user-developed applications, which elevates the risk of data integrity issues and operational errors. A self-identified issue also highlighted that reporting tools were losing their controlled status due to their manual setup.

The audit also noted weaknesses in the governance framework. Material changes to a key risk acceptance guideline were made without the required approvals. Additionally, the documentation for the Clearstream Risk Strategy and Risk Appetite Framework was lacking clear integration of key components and stakeholder roles. The operational risk management processes in DBAG and EFAG were also identified as being weaker compared to other entities within the Group.

Internal Audit positively acknowledges that one issue in this report was already self-identified by Management, with steps pro-actively taken to address the risk, demonstrating good risk management practices.

Details of these observations are disclosed separately in Section 3 and 4 of this report.

## 2. Overview of audit findings and recommendations

Findings <sup>1</sup>														Recommendations <sup>2</sup>		
Title	Severity	Page	DBG Board Member	Relevant Legal Entity's Area Board Member										Owner	Entity (area)	Target Date
				DBAG	ExR	EFAG	ECAG	CEU	CBL	CH	CI	CS	LuxCSD			
Inadequate governance for material changes to risk acceptance guideline (2025-064_F01)	S2	8	Heike Eckert	Heike Eckert	Frank Odendall	-	-	-	-	-	-	-	-	Group Risk Framework & Quantification (ZIN) (2025-064_F01-A01)	DBAG (Heike Eckert)	Jan 16, 2026
														Group Risk Framework & Quantification (ZIN) (2025-064_F01-A02)	DBAG (Heike Eckert)	May 15, 2026
Excessive write access to RITA import directories (2025-064_F02)	S2	10	Heike Eckert	Heike Eckert	-	-	Dmitrij Senko	Udo Henkelmann	Jean-Marc Di Cato	-	-	-	-	Group Risk Models (ZHD)	DBAG (Heike Eckert)	June 12, 2026

<sup>1</sup> The Finding Owner is the relevant legal entity board member responsible for the area where the risk ultimately lies.

<sup>2</sup> The recommendation owner is the action plan owner and has accountability to implement remediation activities for a finding.

Findings <sup>1</sup>														Recommendations <sup>2</sup>		
Title	Severity	Page	DBG Board Member	Relevant Legal Entity's Area Board Member										Owner	Entity (area)	Target Date
				DBAG	ExR	EFAG	ECAG	CEU	CBL	CH	CI	CS	LuxCSD			
Deficient governance of IDPs (2025-064_F03)	S2	12	Heike Eckert	Heike Eckert	Frank Odendall	Melanie Dannheimer	-	-	-	-	-	-	-	Group Risk Framework & Quantification (ZIN) (2025-064_F03-A01)	DBAG (Heike Eckert)	May 15, 2026
														Group Risk Framework & Quantification (ZIN) (2025-064_F03-A02)	DBAG (Heike Eckert)	June 19, 2026
Deficiencies in Clearstream Risk Strategy and Risk Appetite Framework documentation (2025-064_F04)	S2	14	Stephanie Eckermann	-	-	-	-	Udo Henkelmann	Jean-Marc Di Cato	Anne-Pascale Malrechauffe	Fabrice Tomenko	Boglarka Bartha	-	Risk Framework & Governance (RFG)	CBL (Jean-Marc Di Cato)	Closed

Findings <sup>1</sup>														Recommendations <sup>2</sup>		
Title	Severity	Page	DBG Board Member	Relevant Legal Entity's Area Board Member										Owner	Entity (area)	Target Date
				DBAG	ExR	EFAG	ECAG	CEU	CBL	CH	CI	CS	LuxCSD			
Lack of process and repository for capturing material non-financial operational risk incidents in Eurex Repo (2025-064_F05)	S2	16	Heike Eckert	Heike Eckert	Frank Odendall	-	-	-	-	-	-	-	-	Group Risk Framework & Quantification (ZIN)	DBAG (Heike Eckert)	Nov 20, 2026
Weak operational risk management processes in DBAG and EFAG (2025-064_F06)	S2	17	Heike Eckert	Heike Eckert	-	Melanie Dannheimer	-	-	-	-	-	-	-	Group Risk Framework & Quantification (ZIN)	DBAG (Heike Eckert)	May 15, 2026
Deficiency in documentation management for SAP GRC (2025-064_F07)	S1	19	Christoph Böhm	Christoph Böhm	Frank Gast	Quinten Koekenbier	Manfred Matusza	Volker Riebesell	Yannick Goineau	-	Fabrice Tomenko	Daniel Besse	Marco Caligaris	SAP Operations (RTA)	DBAG (Christoph Böhm)	Mar 13, 2026

Findings <sup>1</sup>														Recommendations <sup>2</sup>		
Title	Severity	Page	DBG Board Member	Relevant Legal Entity's Area Board Member										Owner	Entity (area)	Target Date
				DBAG	ExR	EFAG	ECAG	CEU	CBL	CH	CI	CS	LuxCSD			
Insufficient and unreliable documentation of control execution (2025-064_F08)	S1	20	Heike Eckert	Heike Eckert	-	Melanie Dannheimer	-	-	-	-	-	-	-	Group Risk Framework & Quantification (ZIN) (2025-064_F08-A01)	DBAG (Heike Eckert)	Mar 13, 2026
														Group Risk Models (ZHD) (2025-064_F08-A02)	DBAG (Heike Eckert)	Mar 13, 2026
Lack of executive board approval for group level risk framework (2025-064_F09)	S1	22	Heike Eckert	Heike Eckert	-	-	-	-	-	-	-	-	-	Group Risk Framework & Quantification (ZIN)	DBAG (Heike Eckert)	Mar 13, 2026
Lack of ownership and documentation for RITA model parameter review (2025-064_F10)	S1	23	Heike Eckert	Heike Eckert	-	-	-	-	-	-	-	-	-	Group Risk Models (ZHD)	DBAG (Heike Eckert)	Sep 25, 2026

Findings <sup>1</sup>														Recommendations <sup>2</sup>		
Title	Severity	Page	DBG Board Member	Relevant Legal Entity's Area Board Member										Owner	Entity (area)	Target Date
				DBAG	ExR	EFAG	ECAG	CEU	CBL	CH	CI	CS	LuxCSD			
Lack of review and approval for financial and market risk handbooks (2025-064 F11)	S1	24	Heike Eckert	Heike Eckert	Frank Odendall	-	Dmitrij Senko	-	-	-	-	-	-	Group Risk Models (ZHD)	DBAG (Heike Eckert)	Feb 13, 2026

### 3. Finding details

Severity rating	S2
Finding number	2025-064_F01
Finding related to	Control design effectiveness
Title	Inadequate governance for material changes to risk acceptance guideline
Description of finding	<p>Internal Audit (IA) noted that material changes to the <i>DBG Guideline for Dedicated Risk Governance Components</i> (Version 1.1, July 2025) (the Guideline) were introduced without following the required governance and approval process. The Guideline was created to address weaknesses and inconsistencies in the Group's risk-acceptance framework identified in the Internal Audit finding 2023-008_F02 Weaknesses in the Risk Acceptance framework. However, these material changes scaled back the main requirements of the Guideline once the finding was closed.</p> <p>For DBAG and Eurex Repo, no review or approval at the appropriate level was requested, i.e. by a director-level employee or above. For Eurex Repo, the same vice president-level individual initiated and approved the amendments, indicating a lack of segregation of duties. Further no review or approval was requested neither from the DBAG CRO, the responsible board member nor the Eurex Repo General Managers.</p> <p>At the time of report publication, the Guideline had not yet been transitioned to the Written Rules Framework, despite this framework taking effect in August 2024 and despite the Guideline being updated in July 2025. This framework introduced new templates for guidelines and a much more stringent governance process for material changes thereto.</p> <p>As a result, material changes were implemented without adhering to even the much lower governance standards in place prior to the introduction of the Written Rules Framework, reducing transparency and weakening oversight of Group-wide risk acceptance practices.</p> <p>In line with internal requirements, guidelines must be approved by area or section management and the responsible board member. International best practices call for risk management policies and guidelines to be approved by appropriate authorized senior management to ensure accountability, consistency and effective oversight.</p>
Root cause	Lack of Awareness
Risk	Inadequate governance for material changes to risk acceptance guideline may lead to inconsistencies in the Group's risk-acceptance framework, reduced transparency and lack of accountability. This can undermine



	previous remediation efforts and represents a material violation of internal provisions and best practices.
<b>Criteria</b>	<ul style="list-style-type: none"> <li>▪ German Corporate Governance Code, Principle 4</li> <li>▪ Coso Framework (2017), Governance and Oversight Components</li> <li>▪ ISO 31000:2018, Risk Management Principles and Guidelines</li> <li>▪ DBG <i>Written Rules Framework Guideline</i>, Version 1.1</li> <li>▪ DBG <i>Policies Lifecycle Management</i>, Version 2.8, Definitions Annex</li> </ul>
<b>Relevant entity</b>	DBAG/ExR
<b>Recommendation number</b>	2025-064_F01-A01
<b>Recommendation</b>	Obtain approval for the DBG <i>Guideline for Dedicated Risk Governance Components</i> (Version 1.1) from the Chief Risk Officer of DBAG and from the Eurex Repo General Managers, highlighting the material changes made since Version 1.0.
<b>Management response</b>	Group Risk Framework & Quantification (ZIN) agrees with the finding and recommendation, and will implement the recommendation.
<b>Recommendation owner</b>	Group Risk Framework & Quantification (ZIN)
<b>Target date</b>	January 16, 2026

<b>Recommendation number</b>	2025-064_F01-A02
<b>Recommendation</b>	Transition the DBG <i>Guideline for Dedicated Risk Governance Components</i> (Version 1.1) to the Written Rules Framework and submit the resulting document through the formal governance channels defined in the DBG <i>Written Rules Framework Guideline</i> .
<b>Management response</b>	Group Risk Framework & Quantification (ZIN) agrees with the finding and recommendation, and will implement the recommendation.
<b>Recommendation owner</b>	Group Risk Framework & Quantification (ZIN)
<b>Target date</b>	May 15, 2026

Severity rating	S2
Finding number	2025-064_F02
Finding related to	Control design effectiveness and control operating effectiveness
Title	Excessive write access to RITA import directories
Description of finding	<p>RITA (AID239) is used to calculate Value at Risk (VaR) using the Monte-Carlo method. For this calculation, it imports several kinds of data, e.g., relevant master data for risk calculation and various types of credit risk exposure.</p> <p>RITA relies on data imports from files located in specific directories. While write access to all directories except one was appropriately restricted, typically limited to three individuals from the Risk team, the directory GRM_FINRISK used for importing various types of data (e.g., market data and exposure data) was found to have significantly broader access permissions. A total of 27 individuals had write access to this directory, including:</p> <ul style="list-style-type: none"> <li>▪ Enterprise Risk Management (ECAG)</li> <li>▪ Group Risk Framework, Models &amp; Tools (DBAG)</li> <li>▪ Clearstream Securities Services</li> </ul>
Root cause	Inefficient/Inadequate Controls
Risk	Excessive write access to RITA import directories might impair the integrity of import data. As the data import included manual processes, data could be changed, on purpose or by accident, which would result in wrong risk calculation results. A change could go unnoticed. This can result in a material violation of external provisions.
Criteria	<ul style="list-style-type: none"> <li>▪ CSSF 20/750 Information and communication technology (ICT) and security risk management</li> <li>▪ MaRisk, AT 7.2 (2)</li> <li>▪ DORA, Article 9 Protection and prevention</li> <li>▪ EMIR, Article 26 (6)</li> <li>▪ EMIR RTS 153/203, Article 9 (3) and (4)</li> <li>▪ DBG <i>Identity and Access Management Guideline</i>, Version 1.1</li> </ul>
Relevant entity	DBAG/ECAG/CEU/CBL
Recommendation	Review the access permissions for the GRM_FINRISK directory. Update them as needed to ensure compliance with the principles of need-to-know and segregation of duties. To resolve this finding, also provide a mapping that shows which team is responsible for each data type within the GRM_FINRISK directory.
Management response	Group Risk Models (ZHD) agrees with the finding and recommendation, and will implement the recommendation.

<b>Recommendation owner</b>	Group Risk Models (ZHD)
<b>Target date</b>	June 12, 2026

Severity rating	S2
Finding number	2025-064_F03
Finding related to	Control design effectiveness and control operating effectiveness
Title	Deficient governance of IDPs
Description of finding	<p>Internal Audit (IA) identified that the Pension Risk Materiality Assessment IDP used to assess pension-related risks is not recorded in the official IDP tracker, and thus there is no documented evidence of ownership. No documented assessment, approval, or testing evidence was available. Additionally, test and production versions were stored in the same location, the file was not password protected, and no documented environment segregation existed. As a result, the security, integrity, and governance over this IDP could not be verified.</p> <p>Additionally, IA identified access control weaknesses related to the management of the IDP used to assess Business Risk. Specifically, the IDP file was stored at the parent folder level within the project drive structure. This configuration granted access to 57 Risk Management team members, 47 with read access and 10 with write access, across the sections Group Risk Framework, Models &amp; Tools (GRM), and Group Risk Controlling (GRG). However, only two individuals had a valid business need for a write access to this IDP file.</p> <p>In line with internal requirements and international best practices, entities should maintain complete IDP inventories, apply documented governance over IDP lifecycle management, and ensure adequate access controls and environment segregation to safeguard data integrity.</p>
Root cause	Inefficient/Inadequate controls
Risk	Deficient governance of IDPs may result in unauthorized changes, incomplete or inaccurate risk assessments, and potential data integrity issues leading to incorrect management reporting of risk exposure. This represents a material violation of internal provisions and international best practices.
Criteria	<ul style="list-style-type: none"> <li>▪ German Corporate Governance Code, Principle 4</li> <li>▪ COSO Framework 2017</li> <li>▪ ISO 27001:2022, A.5.32, A.8.32 and A.5.7</li> <li>▪ DBG IDP Guideline, Sections 4.1 and 6.6</li> </ul>
Relevant entity	DBAG/ExR/EFAG
Recommendation number	2025-064_F03-A01

<b>Recommendation</b>	<ul style="list-style-type: none"> <li>▪ record the Pension Risk Materiality Assessment IDP in the official IDP tracker, ensuring complete lifecycle documentation (ownership, assessment, approval, testing, and IDP protection)</li> <li>▪ implement access controls based on the principle of least privilege by restricting read and write access to individuals with a valid business need</li> <li>▪ implement environment segregation by separating test and production versions and applying proper version control and governance evidence</li> </ul>
<b>Management response</b>	Group Risk Framework & Quantification (ZIN) agrees with the finding and recommendation, and will, together with Group Risk Models (ZHD), implement the recommendation.
<b>Recommendation owner</b>	Group Risk Framework & Quantification (ZIN)
<b>Target date</b>	May 15, 2026

<b>Recommendation number</b>	2025-064_F03-A02
<b>Recommendation</b>	Implement access controls to the folder where the business risk IDP is residing based on the principle of least privilege by restricting read and write access to individuals with a valid business need and apply folder or IDP file-level segregation.
<b>Management response</b>	Group Risk Framework & Quantification (ZIN) agrees with the finding and recommendation, and will implement the recommendation.
<b>Recommendation owner</b>	Group Risk Framework & Quantification (ZIN)
<b>Target date</b>	June 19, 2026

Severity rating	S2
Finding number	2025-064_F04
Finding related to	Control design effectiveness
Title	Deficiencies in Clearstream Risk Strategy and Risk Appetite Framework documentation
Description of finding	<p>Internal Audit (IA) noted that the procedures governing the development of the Clearstream Risk Strategy and the Clearstream Risk Appetite Framework were not sufficiently comprehensive to ensure consistency, clarity, and effective governance. The current documentation did not fully articulate the end-to-end process, roles, and integration points required for robust risk management oversight.</p> <p>The existing procedures lacked clarity in the following areas:</p> <ul style="list-style-type: none"> <li>▪ Integration of key components: The documentation did not specify how the Business Strategy, Material Change Process, and Risk Taxonomy/Risk Inventory are incorporated into the Risk Strategy and Risk Appetite Framework cycle.</li> <li>▪ Stakeholder roles and interactions: Roles, inputs, and interactions of key stakeholders during the annual review were not clearly defined.</li> <li>▪ Process flow: The sequence of activities, including reviews and approvals, was not documented in a structured process flow.</li> <li>▪ Second line committees: The roles and timing of second line committees, including the Supervisory Board Risk Committee, were not explicitly described.</li> <li>▪ Ad-hoc review triggers: Conditions that would necessitate an ad-hoc review of the Risk Strategy and Risk Appetite Framework were not documented.</li> </ul> <p>IA noted that the newly established (end of Q1 2025) Committees had not been incorporated into the process documentation. Procedures should be reviewed and updated to ensure that any new stakeholders, such as the Clearstream Non-Financial Risk Committee and Financial Risk Committee – are appropriately reflected, ensuring their roles and responsibilities are clearly defined within the process flow.</p> <p>The gaps appear to result from an absence of a formalized governance framework and detailed procedural documentation for the development and review of these key risk management components.</p> <p>The observed gaps conflict with supervisory expectations and regulatory standards that emphasize robust governance and comprehensive documentation of risk frameworks.</p>
Root cause	Insufficient policies, procedures and guidelines

<b>Risk</b>	Deficiencies in Clearstream Risk Strategy and Risk Appetite Framework documentation is a material violation of external requirements. This bears the risk of inconsistent integration of strategic and risk considerations that may undermine decision making. Furthermore, ambiguity in stakeholder responsibilities could lead to delays, ineffective oversight, and gaps in accountability. In addition, insufficient governance and limited responsiveness to material changes in the risk profile or external environment could expose the company to operational inefficiencies and increased vulnerability to emerging risks.
<b>Criteria</b>	<ul style="list-style-type: none"> <li>▪ Directive 2013/36/EU (CRD IV), Article 76</li> <li>▪ EBA Guidelines on Internal Governance under Directive 2013/36/EU</li> <li>▪ MaRisk, AT 4.2 and AT 5</li> <li>▪ CSSF Circular 12/552</li> <li>▪ CSSF Circular 20/758</li> </ul>
<b>Relevant entity</b>	CEU/CBL/CH/CI/CS
<b>Recommendation</b>	<p>Enhance the governance and procedural framework for the development and review of the Clearstream Risk Strategy and Risk Appetite Framework by:</p> <ul style="list-style-type: none"> <li>▪ Formalizing governance: Establish a comprehensive governance framework and detailed documentation covering the full lifecycle of these processes.</li> <li>▪ Clarifying roles and interactions: Define stakeholder responsibilities, inputs, and interaction points, including second-line committees and newly established risk committees.</li> <li>▪ Integrating key components: Document how Business Strategy, Material Change Process, and Risk Taxonomy/Risk Inventory are incorporated into the cycle.</li> <li>▪ Structuring process flow: Include a comprehensive visual representation of all sequences of activities, reviews, and approvals.</li> <li>▪ Defining ad-hoc review triggers: Specify conditions for initiating ad-hoc reviews and escalation paths.</li> <li>▪ Periodic updates: Implement a mechanism to review and update procedures whenever new stakeholders or committees are introduced.</li> </ul> <p>The recommendation was adequately addressed before the issuance of the audit report.</p>
<b>Management response</b>	Risk Framework & Governance (RFG) agrees with the finding and implemented the recommendation.
<b>Recommendation owner</b>	Risk Framework & Governance (RFG)
<b>Target date</b>	Closed

Severity rating	S2
Finding number	2025-064_F05
Finding related to	Control design effectiveness
Title	Lack of process and repository for capturing material non-financial operational risk incidents in Eurex Repo
Description of finding	<p>Internal Audit (IA) observed that there was no established process or centralized repository in place for capturing material operational risk incidents that do not have a clearly identifiable financial impact.</p> <p>IA noted that certain incidents lacking a direct financial consequence—such as inaccurate regulatory reporting caused by data errors—had been considered in some operational risk scenario analyses. However, there was no central system to record these types of incidents in order to provide a comprehensive overview and historical record.</p> <p>In line with German regulation, an entity should maintain a comprehensive operational risk management framework that captures all relevant incidents and ensure proper documentation and oversight through a centralized repository.</p>
Root cause	Inadequate processes
Risk	Lack of process and repository for capturing material non-financial operational risk incidents in Eurex Repo may expose the company to incomplete operational risk assessments and an incomplete risk profile. This represents a material breach of external provisions.
Criteria	<ul style="list-style-type: none"> <li>▪ MaRisk, AT 4.3.2 and BTR 4</li> <li>▪ German Securities Trading Act (WpHG), Section 80(1)</li> <li>▪ German Banking Act (KWG), Section 25(a)</li> <li>▪ Delegated Regulation (EU) 2017/565, Article 23</li> </ul>
Relevant entity	DBAG/ExR
Recommendation	Introduce a definition of “material” incidents in the <i>Incident Notification Guideline</i> and establish a formal process for capturing and evaluating material operational risk incidents in SAP GRC (e.g. via a new category or broader scope the category “near miss”) to maintain historical records for material operational risk incidents not already collected and processed as internal operational risk events.
Management response	Group Risk Framework & Quantification (ZIN) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Group Risk Framework & Quantification (ZIN)
Target date	November 20, 2026



Severity rating	S2
Finding number	2025-064_F06
Finding related to	Control design effectiveness
Title	Weak operational risk management processes in DBAG and EFAG
Description of finding	<p>Internal Audit identified that DBAG and EFAG have significantly weaker controls for operational risk management compared with other entities, like Eurex Repo, ECAG and Clearstream entities. Specifically:</p> <ul style="list-style-type: none"> <li>Operational risk scenario workshops and documentation of meeting minutes were not mandatory for DBAG and EFAG.</li> <li>Quality assurance (QA) of operational risk scenarios in SAP GRC followed a fast-track approach without formal QA records, and only a single-step QA approval was performed directly in the system by Group Risk Monitoring &amp; Reporting (ZIO) with no four-eyes-principle check.</li> <li>There was no defined process for the Risk Management function to review high-severity Internal Audit findings and initiate ad-hoc operational risk scenario reviews when necessary for DBAG and EFAG.</li> <li>For EFAG the definition and monitoring of Key Risk Indicators/Risk Indicators are not mandatory for operational risk scenarios.</li> </ul> <p>In line with German regulation, an entity should establish and maintain robust processes for operational risk management, including ad-hoc reviews, workshops, and quality assurance controls.</p>
Root cause	Inadequate Processes
Risk	Weak operational risk management processes in DBAG and EFAG may lead to an inability to effectively identify, assess, and mitigate significant operational risks. This could expose the organization to minor financial impact, material regulatory impact and material reputational damage.
Criteria	<ul style="list-style-type: none"> <li>Börsengesetz, Section 5(4), Point 2</li> <li>Kreditwesengesetz, Section 25a (3)</li> <li>MaRisk, AT 4.5</li> <li>Aktiengesetz, Section 91 (2) and (3)</li> <li>German Corporate Governance Code (DCGK), Principles 4 and 5</li> </ul>
Relevant entity	DBAG/EFAG
Recommendation	Group Risk Framework & Quantification (ZIN) should confirm if the weaker approach to operational risk management is acceptable with the Chief Risk Officers of DBAG and EFAG. If not, ZIN should implement the additional controls that exist for other entities.
Management response	Group Risk Framework & Quantification (ZIN) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Group Risk Framework & Quantification (ZIN)

Target date	May 15, 2026
-------------	--------------

Severity rating	S1
Finding number	2025-064_F07
Finding related to	Control design effectiveness and control operating effectiveness
Title	Deficiency in documentation management for SAP GRC
Description of finding	<p>SAP GRC Risk Management &amp; Process Control application (AID490) supports comprehensive enterprise risk management by facilitating the administration of Internal Control System (ICS) procedures and addressing Operational Risk scenarios.</p> <p>Although SAP GRC includes various interfaces, these were only briefly mentioned in the Security Documentation. During the audit, detailed documentation for these interfaces was not provided.</p> <p>SAP Operations (RTA) explained that the absence of documentation was attributable to the recent implementation of a Jira tracker tool and accompanying process for tracking team activities. However, because this process was still developing, the audit request was not recorded in the tracking tool.</p>
Root cause	Human Error/Omission
Risk	Deficiency in documentation management for SAP GRC poses a risk to the IT continuity. In the case of an incident, relevant documentation might not be available in time. This could result in a limited violation of external provisions.
Criteria	<ul style="list-style-type: none"> <li>▪ MaRisk, AT 7.2 (1)</li> <li>▪ CSSF 20/750 Information and communication technology (ICT) and security risk management</li> <li>▪ DORA, Article 7</li> <li>▪ EMIR, Article 26 (6)</li> <li>▪ EMIR RTS 153/2013, Article 9 (3) and (4)</li> </ul>
Relevant entity	DBAG/ExR/EFAG/ECAG/CEU/CBL/CI/CS/LuxCSD
Recommendation	Create a formal process documentation for the usage of the Jira tracker to ensure a comprehensive tracking of team activities.
Management response	SAP Operations (RTA) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	SAP Operations (RTA)
Target date	March 13, 2026

Severity rating	S1
Finding number	2025-064_F08
Finding related to	Control operating effectiveness
Title	Insufficient and unreliable documentation of control execution
Description of finding	<p>Internal Audit found that across several risk-related processes managed by two distinct units, Group Risk Framework &amp; Quantification (ZIN) and Group Risk Models (ZHD), evidence documenting control performance was incomplete, difficult to trace, and not adequately protected, raising concerns about the reliability of control execution documentation.</p> <p>Specifically, for the business risk quantification process, documentation of the four-eyes principle was maintained in an unprotected Excel task list. This list lacked version control and access restrictions, making it susceptible to unauthorized modifications.</p> <p>Comparable issues were identified in the Financial Risk Task List, which is used to track key monthly and quarterly activities. Sample reviews revealed blank fields, overdue tasks, manual overrides of completion dates, and an absence of formal sign-offs and a secured audit trail.</p> <p>Additionally, the task list used to evidence control execution for Eurex Repo risk reporting was unreliable and untraceable. The task list lacked formal sign-offs, timestamps, and an audit trail, and could be altered at any time without version tracking. As a result, it could not provide verifiable evidence that required review and validation steps had been properly performed or approved.</p> <p>In line with German regulation and internal requirements, an entity should maintain reliable, durable and traceable evidence of control performance to ensure accountability, auditability and protection from unauthorized modifications.</p>
Root cause	Inefficient/Inadequate controls
Risk	Insufficient and unreliable documentation of control execution may lead to unreliable, incomplete or unverifiable proof of controls. This increases the risk of control failure and represents a minor breach of internal and external provisions.
Criteria	<ul style="list-style-type: none"> <li>▪ MaRisk, AT 6</li> <li>▪ ISO 27001:2022, Annex A.12.4 and A.8.2</li> <li>▪ COSO Internal Controls – Integrated Framework, Principles 10 &amp; 11</li> <li>▪ DBG <i>ICS Policy</i>, Section 5.5</li> </ul>
Relevant entity	DBAG/EFAG

<b>Recommendation number</b>	2025-064_F08-A01
<b>Recommendation</b>	Implement a standardized, protected, and traceable method for documenting control activities in the task lists for business risk quantification and Eurex Repo risk reporting. Evidence should be maintained in a controlled format that ensures review and approval steps are reliably recorded and cannot be modified without authorization.
<b>Management response</b>	Group Risk Framework & Quantification (ZIN) agrees with the finding and recommendation, and will implement the recommendation.
<b>Recommendation owner</b>	Group Risk Framework & Quantification (ZIN)
<b>Target date</b>	March 13, 2026

<b>Recommendation number</b>	2025-064_F08-A02
<b>Recommendation</b>	Implement a standardized method for documenting control activities for the Financial Risk Task List. Evidence should be maintained in a controlled format that ensures review and approval is reliably recorded and cannot be modified later without authorization.
<b>Management response</b>	Group Risk Models (ZHD) agrees with the finding and recommendation, and will implement the recommendation.
<b>Recommendation owner</b>	Group Risk Models (ZHD)
<b>Target date</b>	March 13, 2026

Severity rating	S1
Finding number	2025-064_F09
Finding related to	Control design effectiveness
Title	Lack of executive board approval for group level risk framework
Description of finding	<p>Internal Audit (IA) noted that the <i>2024 DBG Group Risk Framework</i> included approval evidence from the DBAG CFO and DBAG CRO. However, no DBAG Executive Board approval was requested, and the Group documentation did not specify who held ultimate accountability for this approval. The approach to limit the approval to the Chief Financial Officer (CFO) was implemented by a former CFO.</p> <p>In contrast, at the legal entity level, risk strategy documents were formally approved by their respective executive boards, specifically the 2025 DBAG Risk Strategy as operator of the FWB Exchange and the 2025 EFAG risk strategy. This inconsistency in approval levels weakens governance alignment and accountability. As a result, group-level risk strategy documents may lack clear accountability and may not meet expectations for oversight of risk matters at the group level.</p> <p>In line with external regulations and internal governance expectations, risk strategy documents at group level should be formally approved by the Executive Board to ensure clear accountability.</p>
Root cause	Inadequate roles and responsibilities
Risk	Lack of executive board approval for group level risk framework may result in unclear accountability for risk oversight and incomplete governance documentation. This conflicts with internal governance expectations and represents a minor violation of external provisions.
Criteria	<ul style="list-style-type: none"> <li>▪ German Corporate Governance Code, Sections A.1 and A.2</li> <li>▪ EBA Guidelines on Internal Governance (2021/05), Sections 16 and 25</li> <li>▪ <i>DBG Group Risk Management Policy</i>, Section 1.2</li> </ul>
Relevant entity	DBAG
Recommendation	The Group Risk Framework should be formally submitted for Executive Board approval to establish clear top-level accountability.
Management response	Group Risk Framework & Quantification (ZIN) and the DBAG Chief Risk Officer agree with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Group Risk Framework & Quantification (ZIN)
Target date	March 13, 2026

Severity rating	S1
Finding number	2025-064_F10
Finding related to	Control design effectiveness
Title	Lack of ownership and documentation for RITA model parameter review
Description of finding	<p>Internal Audit (IA) identified weaknesses in the governance of key activities related to the RITA tool.</p> <p>While risk model parameters in RITA were reviewed annually, the process lacked defined ownership, governance arrangements and documentation of responsibilities for conducting or approving these reviews. These parameters support credit and market risk quantification, economic capital, and Group level risk-reporting.</p> <p>In line with external regulations and guidelines, an entity should define clear roles and responsibilities, review steps and documentation requirements to ensure traceability and consistent application.</p>
Root cause	Inadequate roles and responsibilities
Risk	Lack of ownership and documentation for RITA model parameter review at DBAG level may result in inconsistent or undocumented updates to key model assumptions. This could lead to governance weaknesses in credit and market risk calculations at group level, reduce model transparency and impair traceability of changes.
Criteria	<ul style="list-style-type: none"> <li>▪ German Corporate Governance Code, Sections A.1 and A.2</li> <li>▪ EBA Guidelines on Internal Governance (2021/ 05), Sections 16 and 25</li> </ul>
Relevant entity	DBAG
Recommendation	Define clear roles and responsibilities, review steps, and documentation requirements for the periodic review of key model parameters.
Management response	Group Risk Models (ZHD) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Group Risk Models (ZHD)
Target date	September 25, 2026

Severity rating	S1
Finding number	2025-064_F11
Finding related to	Control design effectiveness
Title	Lack of review and approval for financial and market risk handbooks
Description of finding	<p>The DBG <i>Financial Risk Handbook</i> (last updated March 2024) and the DBAG <i>Risk Model Handbook - Market Risk</i> (last updated April 2024) had not undergone their required annual review and formal approval at the time of audit testing (September/October 2025).</p> <p>In both documents, version-history records did not contain evidence of management review or sign-off within the preceding 12 months.</p> <p>In line with internal requirements and governance standards, key risk handbooks and policy documents must undergo periodic review and formal approval to ensure accuracy, accountability and consistent application.</p>
Root cause	Insufficient Policies, Procedures and Guidelines
Risk	Lack of review and approval for handbooks may result in outdated or inconsistent guidance being applied. This may reduce accountability, impair effective risk management practices and represents a minor violation of internal and external requirements.
Criteria	<ul style="list-style-type: none"> <li>▪ MaRisk, AT 4.3.1 and 5</li> <li>▪ German Corporate Governance Code, Sections A.1 and A.2</li> <li>▪ EBA Guidelines on Internal Governance (2021/ 05), Sections 16 and 25</li> <li>▪ DBG <i>Written Rules Framework Guideline</i>, Version 1.1</li> </ul>
Relevant entity	DBAG/ExR/ECAG
Recommendation	Update the <i>Financial Risk Handbook</i> and the DBAG <i>Risk Model Handbook - Market Risk</i> and obtain formal senior-management approval. Evidence of the completed review and approval should be recorded in the version history.
Management response	Group Risk Models (ZHD) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Group Risk Models (ZHD)
Target date	February 13, 2026



## 4. Self-Identified Issues

Severity rating	S2
SII Identification number	FH_0000023871
SII related to	Control design effectiveness
Title	Reporting tools with unstable IDP status
Description of SII	<p>In 2025, many tools used for the Group Risk Models (ZHD) reporting process were migrated from Excel to Python-based Jupyter notebooks. These new tools were registered as IDPs using the FileTracker IDV Suite. The tools were used to generate a group consolidated view, with the data being reported to group and legal entity management.</p> <p>However, each time the tools were used, they lost their IDP status due to changes in input data (such as the run date) and intermediate outputs. Although a ticket (APPOPS-22705) was submitted to IT to address this issue, IT determined that a change to the FileTracker IDV Suite would be too costly.</p>
Risk	Reporting tools with unstable IDP status increases the risk of data integrity issues and non-compliance within the Group Risk Models (ZHD) reporting process.
Root cause	Inadequate IT Infrastructure
Relevant entity	DBAG/ExR/EFAG/ECAG/CEU/CBL/CH
Intended actions	Group Risk Models (ZHD) is migrating all tools to native Python to prevent future loss of IDP status. This migration, including testing and IDP documentation, is expected to be completed in the first quarter of 2026.
Owner	Group Risk Models (ZHD)
Target date for resolution	March 31, 2026

## 5. Finding severity definition<sup>3</sup>

For details on finding severity definition, please refer to [Group Audit - Findings severity definitions](#)

---

<sup>3</sup> Identified findings are graded in terms of their (potential) risk significance, having assessed the overall effectiveness and efficiency of implemented controls (residual risk). The risk potentials and the potential estimated damages are determined by expert judgement. The highest severity of deficiencies noted, determines the minimum severity ranking.

## 6. Distribution list

Executive Management	Christoph Böhm	Member of DBAG Executive Board
	Heike Eckert	Member of DBAG Executive Board
	Thomas Book	Member of DBAG Executive Board
	Stephanie Eckermann	Member of DBAG Executive Board
	Christian Kromann	Member of DBAG Executive Board
	Jens Schulte	Member of DBAG Executive Board
	Samuel Riley	CEO of CH Executive Board
	Berthold Kracke	Member of CH Executive Board
	Dirk Loscher	CEO of CEU Executive Board
	Martina Gruber	Member of CEU Executive Board
	Udo Henkelmann	Member of CEU Executive Board
	Volker Riebesell	Member of CEU Executive Board
	Philip Brown	CEO of CBL Executive Board and Member of CH Executive Board
	Guido Wille	Member of CBL Executive Board
	Yannick Goineau	Member of CBL Executive Board
	Anne-Pascale Malréchauffé	Member of CBL Executive Board and CH Executive Board
	Denis Schloremberg	Member of CBL Executive Board and CI Board of Directors
	Jean-Marc Di Cato	Member of CBL Executive Board
	Marton Szigeti	Chairman of CI Board of Directors
	Mark Gem	Vice-Chairman of CI Board of Directors
	Fabrice Tomenko	CEO of CI Board of Directors
	Armin Borries	Member of CS Executive Board
	Boglarka Barthá	Member of CS Executive Board
	Daniel Besse	CEO of CS Executive Board and Member of CH Executive Board
	Marco Caligaris	CEO of LuxCSD
	Jens Janka	Interim CEO and Member of ECAG Executive Board
	Dmitrij Senko	Member of ECAG Executive Board
	Manfred Matusza	Member of ECAG Executive Board
	Matthias Graulich	Member of ECAG Executive Board and Member of EFAG Executive Board

	Robbert Booij	CEO of EFAG Executive Board
	Quinten Koekenbier	Member of EFAG Executive Board
	Jonas Ullmann	Member of EFAG Executive Board
	Melanie Dannheimer	Member of EFAG Executive Board
	Frank Gast	General Manager of ExR
	Frank Odendall	General Manager of ExR
<b>Business Line</b>	Michele D'Inca	Head of Section, Group Risk Controlling (GRG)
	Thomas Heinze	Head of Unit, Group Risk Governance & ICS (ZHE)
	Ivan de Wit	Head of Unit, Group Risk Monitoring & Reporting (ZIO)
	Agnieszka Chelminska	Head of Section, Group Risk Framework, Models & Tools (GRM)
	Franz Seidel	Head of Unit, Group Risk Framework & Quantification (ZIN)
	Nathalie Oebel-Karmoussi	Head of Unit, Group Risk Models (ZHD)
	Jacopo Corbetta	Vice President, Group Risk Models (ZHD)
	Petr Vecerek	Head of Unit, Risk Tools & Analytics (ZHF)
	Aleksandra Golon	Head of Unit, Regulatory Framework & Implementation (RGL)
	Raimund Brühl	Regulatory Framework & Implementation (RGL)
	Tobias Büchel	Head of Section, Risk Controlling & Governance (RCG)
	Stefan Bergmann	Head of Unit, Non-Financial Risk (NFR)
	Alexios Toptsoglou	Head of Unit, Risk Framework & Governance (RFG)
	Olivier Dekeme	Head of Unit, Financial Risk (FNR)
	Bernhard Milla	Head of Unit, Quantitative Models & Analytics (AMC)
	César Matos	Head of Section, Enterprise Risk Management (UIY)
	Ivan Madaras	Head of Unit, Financial Risk (FRM)
	Oussama Fakih	Head of Unit, Non-Financial Risk, ICS & BCM (FRB)

	Kristyna Gasperak	Head of Section, Analytical Services (PKJ)
	Neil Ryan	Head of Unit, SAP Operations (RTA)
	Suhas Kulkarni	SAP Operations (RTA)
	<a href="mailto:CRP-Audit@deutsche-boerse.com">CRP-Audit@deutsche-boerse.com</a>	Risk Management, Control, Governance
<b>Risk Management</b>	Dominik Schmidt-Kiefer	Chief Risk Officer DBAG
	<a href="mailto:LuxCSD_Audit_Control@LuxCSD.com">LuxCSD_Audit_Control@LuxCSD.com</a>	LuxCSD Audit Coordination
<b>Group Legal</b>	Bettina Kramer-Braun	Managing Director of Group Legal
<b>Compliance</b>	Marc Peter Klein	Group Chief Compliance Officer
	<a href="mailto:GC_Audit_Coord@deutsche-boerse.com">GC_Audit_Coord@deutsche-boerse.com</a>	Group Compliance Audit Coordination
	Christian Heyne	Chief Compliance Officer CBL
	Oliver Haderup	Chief Compliance Officer ECAG
	Jan Kobbach	Chief Compliance Officer CEU and CH
	Katja Röhle	Chief Compliance Officer ExR
	Bianca Sahrholz	Head of Unit CCP Compliance
<b>ICT</b>	Sebastian Wedeniwski	CTO, DBAG
	Boris Link	IT Governance, Risk and Transformation DBAG
	Neslihan Meinert	CTO ExR
	CRIT-IS-Office	CRIT IS Office ECAG
<b>Internal Audit</b>	Andrea Bracht	Group Audit
	Dietmar Hinkel	Group IT Audit
<b>Audit Managers</b>	Tatjana-Janine Tollkühn	Internal Audit DBAG
	Mirweiss Inayt	Internal Audit CEU
	Valerie Aubert	Internal Audit CBL
	Thomas S. Musgrave	Internal Audit ECAG
<b>Auditors</b>	Alba Kajtazi	Internal Audit CEU
	Ourania Androulaki	Internal Audit DBAG
	Robert Pardikes	Internal Audit ECAG
	Simona Gaffarelli	Internal Audit CBL
	Trupti Thakur	Internal Audit DBAG
	Volker Scheer	Internal Audit ECAG

## 8.1 Appendix A

### Detailed scope

The examination included procedures and tests to obtain reasonable assurance whether the control environment is adequate, the control design is effective and designed controls operate effectively.

The audit scope was determined on a risk basis, and covered the following key aspects of Risk Management processes:

- Risk Strategy Framework
- Risk Management System
- Assurance Heatmap Reporting
- Review of IDP applications
- Review of RITA (AID239) and SAP GRC (AID490) IT applications

Limitations of scope: None

Key aspects of the Risk Governance and ICS process were covered in the audit 2025-024 Special Audit on General Controls.

The Model Validation and Stress Testing processes were covered in the following audits:

- 2025-036 AMA, ICAAP (CEU, CBL)
- 2025-052 ILAAP (CEU, CBL)
- 2025-053 ICAAP and ILAAP (DBAG, ExR, ECAG)
- 2025-061 Stress Testing (ECAG)
- 2025-062 Model Validation (ECAG)