Internal Audit Report

2025-045 Cyber and Information Security

September 05, 2025

- CONFIDENTIAL -

Audit scope period	April 2024 to March 2025
Legal entities in scope	DBAG/ExR/EFAG/ECAG/CBF/CBL/CH/CI/CS/LuxCSD/CFCL/ECC/EEX
IA function	DBAG/ECAG/CBF/CBL/CFCL/ECC
Location	Eschborn, Luxembourg, Leipzig

Results	S1	S2	S3	S4
Total Internal Audit findings: 8	1	7	-	-
Self-identified Issues: 0	-	-	-	-

1. Executive summary

Internal Audit (IA) conducted a review of Cyber and Information Security (IS) processes across Deutsche Börse Group (DBG) from April to September 2025.

Significant remediation efforts are underway through the **DORA and AMELI programs** until the end of 2025 or H1/2026, which IA is accompanying including separate validation activities. These initiatives address key areas such as Application Security documentation, IS Risk Management, SSH Key Inventory and Management, Security Information and Event Management (SIEM) data handling, and Advanced Persistent Threat (APT) protection.
Given their scope and progress, IA focused this audit on areas not directly targeted by these programs: cryptography and key management, continuous threat detection and response, threat-led penetration testing (TLPT), and threat intelligence.

Related to **Cryptography and Key Management**, IA identified four S2 findings across 6 of the 13 applications reviewed. Key issues include:

- Inadequate documentation and governance of cryptographic key management processes for multiple applications, including the three internal Certificate Authorities, which are critical for secure authentication and encryption.
- Gaps in cryptography related risk management, validation of implemented measures and key rotation, and incomplete key management processes, for individual applications.

These deficiencies reflect a need to strengthen governance and harmonization in the related control environment across Asset Owners, Shared IT, and Product IT teams.

Five of the eight findings were linked to **insufficient or unclear written rules** (policies, guidelines, and procedures). Examples include:

- Use of informal working instructions not subject to regular review.
- Missing or unclear procedures for key management and vulnerability handling.
- Inadequate guidance on asset classification (e.g., Partner Services in APMS).

These gaps likely contributed to the weaknesses observed in cryptography and key management, underscoring the impact of operational guidance on control effectiveness.

In terms of **Threat-Led Penetration Testing (TLPT)**, IA reviewed the design of DBG's TLPT framework and found no issues. However, as DORA restricts information sharing about planned or ongoing TLPT exercises to the "control team" that does not include IA, no conclusion was made regarding execution or DBG's overall preparedness.

2. Overview of audit findings and recommendations

Findings[1]																Recommendations[2]		
Title	Severity	Page	DBG Board Member	Relevant Legal Entity's Area Board Member												Owner	Entity (area)	Target Date
				DBAG	ExR	EFAG	ECAG	CBF	CBL	CH	CI	CS	LuxCSD	CFCL	ECC	EEX			
Deficiency in Cryptography Key Management documentation and Process Governance for multiple applications (2025-045_F01)	S2	6	Christoph Böhm	Christoph Böhm	Frank Gast	-	Manfred Matusza	Volker Riebesell	Yannick Goineau	-	-	Daniel Besse	Marco Caligaris	Kevin Hayes	Jens Rick	Jens Rick	Security IT - Digitise, Evolve & Innovate (SAO)	DBAG (Christoph Böhm)	Apr 24, 2026
Incomplete validation of implemented cryptography measures and key rotation in Account Master (AID031) (2025-045_F02)	S2	8	Christoph Böhm	-	-	-	-	Volker Riebesell	Yannick Goineau	-	Fabrice Tomenko	Daniel Besse	Marco Caligaris	Kevin Hayes	-	-	Instrument and Institution Data IT (ÖÖD)	DBAG (Christoph Böhm)	Apr 24, 2026
Incomplete process governance of cryptography and key management processes in CFS Portal (AID2151) (2025-045_F03)	S2	10	Christoph Böhm	-	-	-	-	-	-	-	-	-	-	Kevin Hayes	-	-	CFS Applications Support (CFT)	DBAG (Christoph Böhm)	Closed

[1] The Finding Owner is the relevant legal entity board member responsible for the area where the risk ultimately lies.
[2] The recommendation owner is the action plan owner and has accountability to implement remediation activities for a finding.

Findings[1]																Recommendations[2]		
Title	Severity	Page	DBG Board Member	Relevant Legal Entity's Area Board Member												Owner	Entity (area)	Target Date
				DBAG	ExR	EFAG	ECAG	CBF	CBL	CH	CI	CS	LuxCSD	CFCL	ECC	EEX			
Partially insufficient management and tracking of cryptography risks in SCILA (AID797) (2025-045_F04)	S2	12	Christoph Böhm	Christoph Böhm	-	-	-	-	-	-	-	-	-	-	-	-	Functionality & Partner Exchanges (CMD)	DBAG (Christoph Böhm)	Apr 24, 2026
Inadequate guidelines on Partner Services as asset type in DBG's APMS (2025-045_F05)	S2	14	Gregor Pottmeyer	Gregor Pottmeyer	Frank Odendall	Jonas Ullmann	Dmitrij Senko	Udo Henkelmann	Jean-Marc Di Cato	Philip Brown	Fabrice Tomenko	Boglarka Bartha	Marco Caligaris	Sonia Dribek-Pfleger	Ralf Prinzler	Jens Rick	ICT Risk Framework (KJU) (2025-045_F05-A01)	DBAG (Gregor Pottmeyer)	Nov 17, 2025
																	IT Core Process Design & Operations (ÜPÜ) (2025-045_F05-A02)	DBAG (Christoph Böhm)	Apr 03, 2026
Incomplete inventory in DBG`s APMS supporting Threat Intelligence process (2025-045_F06)	S2	16	Christoph Böhm	Christoph Böhm	Frank Gast	Quinten Koekenbier	Manfred Matusza	Volker Riebesell	Yannick Goineau	Daniel Besse	Fabrice Tomenko	Daniel Besse	Marco Caligaris	Kevin Hayes	Jens Rick	Jens Rick	Cyber Defense (CBD)	DBAG (Christoph Böhm)	Apr 30, 2026

Findings[1]																Recommendations[2]		
Title	Severity	Page	DBG Board Member	Relevant Legal Entity's Area Board Member												Owner	Entity (area)	Target Date
				DBAG	ExR	EFAG	ECAG	CBF	CBL	CH	CI	CS	LuxCSD	CFCL	ECC	EEX			
Deficiency in SoD controls implementation and outdated application documentation for MISP (AID737) (2025-045_F07)	S2	17	Christoph Böhm	Christoph Böhm	Frank Gast	Quinten Koekenbier	Manfred Matusza	Volker Riebesell	Yannick Goineau	-	-	Daniel Besse	Marco Caligaris	Kevin Hayes	-	-	Security IT – Engineering Build and Improve (CUR)	DBAG (Christoph Böhm)	Closed
Lack of details in vulnerability management procedures in respect to timelines of involved teams (2025-045_F08)	S1	19	Christoph Böhm	Christoph Böhm	Frank Gast	Quinten Koekenbier	Manfred Matusza	Volker Riebesell	Yannick Goineau	Daniel Besse	Fabrice Tomenko	Daniel Besse	Marco Caligaris	Kevin Hayes	Jens Rick	Jens Rick	Plan & Design Services (VLM)	DBAG (Christoph Böhm)	Feb 18, 2026

3. Finding details

Severity rating	S2
Finding number	2025-045_F01
Finding related to	Control design effectiveness and control operating effectiveness
Title	Deficiency in Cryptography Key Management documentation and Process Governance for multiple applications
Description of finding	The PKI DBAG (AID1064) and PKI Clearstream (1066) applications are internal Certificate Authorities used to digitally sign certificates for internal applications and servers that are requested by other teams within DBAG and Clearstream legal entities. PKI MSCA (AID1065) is a Certificate Authority used to digitally sign certificates that are requested regarding Skype and Outlook S/MIME[3] certificates and Microsoft Windows Hello for Business. During an inspection of the PKI DBAG, PKI Clearstream and PKI MSCA cryptography key management processes primarily managed by Security IT's - Digitise, Evolve & Innovate (SAO) unit, they referenced an internal operational procedure as "Audit Document" instead of a formally approved procedure. The document didn't include essential elements (i.e., purpose, scope, management approval) as defined by the overarching *Written Rules Framework Guideline*. Despite its informal nature and not being published in the central written rules repository, SAO acknowledged the Audit Document was possibly used by multiple IT Operations/Production Support teams as a key reference for the structure of their own key management procedures, to support and further operationalize the requirements laid down in the primary document, the *Encryption and Key Management Guideline* published centrally by the Chief Risk Officer (FOC) area. Further inspection of the SAO SharePoint site revealed that 19 out of 37 cryptography-related operating procedures and work instructions had not been reviewed and approved in several years (between 2020-2023) and did not state whether they were active or decommissioned. While a yearly review control exists in a JIRA task (SECPKII-1063), it lacked detailed execution steps, as well as evidence of its performance. European, German, and Luxembourg regulations require precise and clear procedures manual which is accessible and up to date must be maintained. Business activities are conducted based on organizational guidelines. Related business, control and monitoring documentation should be written in a manner that is readily comprehensible to expert third parties.

[3] S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard used to encrypt and digitally sign email messages.

Root cause	Insufficient policies, procedures and guidelines
Risk	Deficiency in Cryptography Key Management documentation and Process Governance for multiple applications may expose the organization to inconsistent implementation of key management practices and outdated documentation. This could lead to minor regulatory non-compliance and reputational impact, resulting from inadequate governance, lack of traceability, and misrepresentation of control effectiveness in internal and external audits.
Criteria	▪ EU Regulation 2022/2554 (DORA), article 5 ▪ CSSF Circular 20/750, chapter 3, article 3.5 ▪ MaRisk (Minimum Requirements for Risk Management) – BaFin Circular 06/2024, AT 7.2 ▪ *DBG Written Rules Framework Guideline* V1.0, Section 3 ▪ *DBG Encryption and Key Management Guideline*, v1.0
Relevant entity	DBAG/ExR/ECAG/CBF/CBL/LuxCSD/CS/CFCL/ECC/EEX
Recommendation	Internal Audit recommends that Security IT – Digitise, Evolve & Innovate (SAO): ▪ classify and update the "Audit Document" and the contents of the SAO SharePoint site according to the DBG Written Rules Framework Guideline ▪ determine the key relevance of the internal documentation (working instructions, procedures) and its possible shared usage, to consider transferring them into DBG's official IT written rules database in coordination with IT Governance, Risk and Transformation (IRT)
Management response	Security IT – Digitise, Evolve & Innovate (SAO) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Security IT – Digitise, Evolve & Innovate team (SAO)
Target date	April 24, 2026

Severity rating	S2
Finding number	2025-045_F02
Finding related to	Control design effectiveness and control operating effectiveness
Title	Incomplete validation of implemented cryptography measures and key rotation in Account Master
Description of finding	The Account Master (AM) (AID031) platform manages account-related reference data for ICSD (International Central Securities Depository) business needs. The application supports the setup of descriptive account data, critical settlement-related data (e.g., risk limits, collateral details), and currency-related information (e.g. rates and deadlines). As part of the AM application risk assessments, the application owner performs an annual review/re-assessment of the implemented cryptography measures. However, Internal Audit (IA) could not obtain evidence of the annual review/re-assessment of cryptography measures performed in the most recent risk assessment period. Additionally, upon further inspection of the cryptography key management processes performed by the supporting IT Operations team, IA observed a lack of established key rotation procedures for AM. While both issues were known to the application owner, the risks were not reflected in the application's Risk Assessment Tool (RAT). At the time of the audit, the RAT controls for cryptography (ID no. 188) were erroneously marked as fully compliant. European, German, and Luxembourg regulations require financial institutions to apply and manage cryptography keys throughout its lifecycle, implement controls to protect keys, maintain a register of certificates and ensure timely renewal.
Root cause	Lack of Awareness
Risk	Incomplete validation of implemented cryptography measures and key rotation in Account Master (AID031) application may expose the company to outdated cryptography measures, expired keys, and data breaches. This could lead to minor breach of regulatory requirements and reputational impact resulting from inadequate protection of sensitive data and misrepresentation of control effectiveness in risk assessments.
Criteria	▪ EU Regulation 2022/2554 (DORA), articles 5 and 7 ▪ CSSF Circular 20/750, chapter 3, article 3.4.4 ▪ MaRisk (Minimum Requirements for Risk Management) – BaFin Circular 06/2024, AT 7.2
Relevant entity	CBF/CBL/LuxCSD/CS/CI/CFCL

Recommendation	Internal Audit recommends that Instrument and Institution Data IT (ÖÖD): ▪ reassess the relevant RAT control compliance status for encryption and cryptography measures in place, particularly in line with the non-compliant provision of key rotation processes and raise risks accordingly ▪ establish a regular review/verification of cryptography measures in place within the application, whilst providing adequate documentation for the performance of this control ▪ adequately define roles/responsibilities for the provision of the key management process in conjunction with the supporting IT operations teams
Management response	Instrument and Institution Data IT (ÖÖD) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Instrument and Institution Data IT (ÖÖD)
Target date	April 24, 2026

Severity rating	**S2**
Finding number	2025-045_F03
Finding related to	Control design effectiveness and control operating effectiveness
Title	Incomplete process governance of cryptography and key management processes in CFS Portal (AID2151)
Description of finding	CFS Portal (AID2151) is a web-based platform serving as a single access point for internal and external users to connect to Clearstream Fund Services (CFCL and CFCS) customer-facing applications through single sign-on. During an inspection of the CFS Portal application's cryptography key management processes, Internal Audit (IA) observed that CFS Production Support (PRD) unit was unable to provide dedicated PRD procedure documentation for certificate installation and monitoring workflows within the application's documentation. PRD referenced a work instruction for cryptography key management ("*AS_WS_Cryptographic_key_management (IFS)*"). However, in the section for the installation and monitoring workflows, there were no defined procedures. After IA mentioned the gap, these procedures were proactively added into the operational documentation of *CFC Portal Operational Documentation* v2.1. Moreover, IA noted that PRD used asset's Security Documentation as a working instruction, despite not corresponding to a "written rule" as defined by the overarching *Written Rules Framework Guideline*. European, German, and Luxembourg regulations require that systems implement a combination of technical, physical, and administrative controls to ensure adequate protection levels, proportionate to the sensitivity of the system and data.
Root cause	Lack of Awareness
Risk	Incomplete process governance of cryptography and key management processes in CFS Portal (AID2151) may expose the company to an absence of formally structured, updated and approved key management procedures, lack of accountability and inconsistent cryptography practices. This could lead to minor breach of regulatory requirements resulting from ineffective governance over key lifecycle management and misalignment with internal Written Rules Framework requirements.
Criteria	▪ EU Regulation 2022/2554 (DORA), article 5 ▪ CSSF Circular 20/750, chapter 3, article 3.5 ▪ MaRisk (Minimum Requirements for Risk Management) – BaFin Circular 06/2024, AT 7.2 ▪ *DBG Written Rules Framework Guideline* V1.0, Section 3
Relevant entity	CFCL

Recommendation	Internal Audit recommends that CFS Applications Support (CFT): ▪ update the dedicated procedure documentation to include the activities used in the management of encryption measures and under the responsibility of the team (completed during the audit) ▪ enhance awareness of the fixed written rules / procedure documentation within the production support team The recommendation was adequately addressed before the issuance of the report.
Management response	CFS Applications Support (CFT) agrees with the finding and recommendation and has implemented the recommendation.
Recommendation owner	CFS Applications Support (CFT)
Target date	Closed

Severity rating	S2
Finding number	2025-045_F04
Finding related to	Control design effectiveness and control operating effectiveness
Title	Partially insufficient management and tracking of cryptography risks in SCILA (AID797)
Description of finding	The SCILA Partner Exchanges (SCILA) (AID797) is a trading surveillance application software which is operated by Deutsche Börse in its role as a service provider for the German Regional Exchanges (Boerse Berlin AG and BÖRSEN AG) supporting trading behavior monitoring of their exchange participants to fulfill these two exchange partners' regulatory obligations. During an examination of the cryptography measures for the SCILA application, Internal Audit observed the use of weak, non-compliant cryptography algorithms. These were known to the application owner and had been planned for decommissioning as part of a planned upgrade to RedHat Linux 8. This known weakness was not found in the application's last performed Risk Assessment Tool (RAT). During the audit, an IT Change Request to update the underlying infrastructure's compliance status regarding the cryptography policy was initiated. Lastly, IA's review of the application's Security Documentation noted minor inaccuracies regarding the communication interfaces. Specifically: ▪ the type and version of cryptography technology securing connection I-01 ▪ the present status or obsolescence of connection I-04 European, German, and Luxembourg regulations require that systems implement a combination of technical, physical, and administrative controls to ensure adequate protection levels, proportionate to the sensitivity of the system and data.
Root cause	Human Error/Omission
Risk	Partially insufficient management and tracking of cryptography risks in SCILA (AID797) may expose the company to outdated encryption standards and misinformed security configurations. The use of weak, non-compliant cryptographic algorithms and inaccurate documentation of communication interfaces in the SCILA application (AID797) could lead to minor breach of regulatory requirements resulting from insufficient identification and mitigation of ICT risks.
Criteria	▪ EU Regulation 2022/2554 (DORA), articles 6 and 9
Relevant entity	DBAG

Recommendation	Internal Audit recommends that Functionality and Partner Exchanges (CMD): ▪ ensure the implementation of the outstanding IT Change Request to activate the measures required by the cryptography policy for SCILA application (AID797) ▪ update the security documentation, particularly the communication interfaces, to reflect the current state The first bullet was adequately addressed before the issuance of the report.
Management response	Functionality & Partner Exchanges (CMD) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Functionality & Partner Exchanges (CMD)
Target date	April 24, 2026

Severity rating	S2
Finding number	2025-045_F05
Finding related to	Control design effectiveness and control operating effectiveness
Title	Inadequate guidelines on Partner Services as asset type in DBG's APMS
Description of finding	An audit comment 5.3 raised in 2024-063 Technology Governance noted Deutsche Börse Group's (DBG) Application Portfolio Management System (APMS) was incomplete regarding external web assets/services, which IA provisionally designated as "Partner Services". A feasibility assessment about introducing Partner Services as a new asset type was to be completed by December 2024, its definition included within the *ICT Asset Management Guideline* v1.0 and control requirements established in the Mandatory Control Framework (MCF). IA noted that DBG's APMS inventory did not yet include Partner Services. 2nd LoD - ICT Risk Framework (KJU) and 1st LoD - IT Core Process Design & Operations (ÜPÜ) were still developing clear definition, control requirements and process descriptions. KJU plans to put in force a fully revised *ICT Asset Management Guideline* v1.1, including the definition of Partner Services, by end of Q3 2025. German and Luxembourg regulations require financial institutions to maintain accurate and complete inventories of IT assets, including third-party related assets.
Root cause	Insufficient policies, procedures and guidelines
Risk	Inadequate guidelines on Partner Services as asset type in DBG's APMS may expose the company to inaccurate IT asset tracking, reduced visibility over regulatory-relevant tools, and weakened governance over application ownership and accountability. This could lead to minor financial losses and material reputational, regulatory and internal provisions, resulting from compliance gaps, operational inefficiencies, and auditability issues.
Criteria	▪ EU Regulation 2022/2554 (DORA), article 8 ▪ CSSF Circular 20/750, chapter 3, article 3.5 ▪ *DBG ICT Asset Management Guideline*, v1.0, section 4 ▪ *DBG Software License Management (SwLM) Process*, v2.1
Relevant entity	DBAG/ExR/EFAG/ECAG/CBF/CBL/CH/CI/CS/LuxCSD/CFCL/ECC/EEX
Recommendation number	2025-045_F05-A01
Recommendation	Internal Audit recommends that ICT Risk Framework (KJU): ▪ complete the review, approval and publishing of the *ICT Asset Management Guideline*, v1.1

	▪ update the Mandatory Control Framework (MCF) for new asset-type and its control requirements
Management response	ICT Risk Framework (KJU) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	ICT Risk Framework (KJU)
Target date	November 17, 2025

Recommendation number	2025-045_F05-A02
Recommendation	Internal Audit recommends that IT Core Process Design & Operations (ÜPÜ) - ▪ update the '*APMS_User Manual*' and '*APMS Process Description*' documents with detailed criteria / guidance and their rollout ▪ update APMS application functionality to include new asset type ▪ impart awareness across DBG on the new asset type
Management response	IT Core Process Design & Operations (ÜPÜ) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	IT Core Process Design & Operations (ÜPÜ)
Target date	April 3, 2026

Severity rating	S2
Finding number	2025-045_F06
Finding related to	Control operating effectiveness
Title	Incomplete inventory in DBG's APMS supporting Threat Intelligence process
Description of finding	Deutsche Börse Group's (DBG) Application Portfolio Management System (APMS) is designed to serve as a central inventory of all relevant applications used across DBG and its subsidiaries. Internal Audit noted that 'Dataminr', a subscription-based external web portal used for collecting 'Physical Security related Threat Intelligence' details for DBG entities, was not captured in the APMS inventory. German and Luxembourg regulations require financial institutions to maintain accurate and complete inventories of IT assets, including third-party related assets.
Root cause	Lack of awareness
Risk	Incomplete inventory in DBG's APMS supporting Threat Intelligence process may result in non-compliance with both internal and external provisions, such as minor breach of regulatory requirements, posing risks of incomplete or inaccurate inventory information and auditability issues.
Criteria	▪ EU Regulation 2022/2554 (DORA), article 8 ▪ CSSF Circular 20/750, chapter 3, article 3.5 ▪ *DBG ICT Asset Management Guideline*, v1.0, section 4 ▪ *DBG Software License Management (SwLM) Process*, v2.1
Relevant entity	DBAG/ExR/EFAG/ECAG/CBF/CBL/CH/CI/CS/LuxCSD/CFCL/ECC/EEX
Recommendation	Internal Audit recommends that Cyber Defense (CBD) include Dataminr in the APMS inventory.
Management response	Cyber Defense (CBD) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Cyber Defense (CBD)
Target date	April 30, 2026

Severity rating	S2
Finding number	2025-045_F07
Finding related to	Control design effectiveness and control operating effectiveness
Title	Deficiency in SoD controls implementation and outdated application documentation for MISP (AID737)
Description of finding	The MISP (AID737) Threat Intelligence Platform implemented for SOC/CERT operations is used to implement new use-cases based on Threat Intelligence data from third parties, enhancing detection and investigation of cyber events and security incidents. Internal Audit (IA) identified missing MISP access rights management controls. For the three role types – user, admin and publisher – the application owner had neither defined nor implemented segregation of duties (SoD) principles and rules in the Authorization Concept and in the ruleset in the SailPoint IIQ (AID760) identity and access management tool. As a result, the effectiveness of use-cases in MISP may be impacted, leading to malicious actions going undetected, affecting the reliability of threat intelligence and SOC/CERT operations. The risk rating of this finding considers that IA's review of MISP access rights currently granted to users did not identify any SoD toxic combinations. German and Luxembourg regulation requires that organization shall manage access rights to information assets and their supporting systems on a "need-to-know" basis and under the least privileged model. Internal policies, procedures and standards require that a SoD lifecycle change process be documented, and SoD conflicts be handled. Additionally, application owners are responsible for defining, implementing, and maintaining adequate application security controls and documentation.
Root cause	Insufficient policies, procedures and guidelines
Risk	Deficiency in segregation of duty controls implementation and outdated application documentation for MISP (AID737) represents a violation of internal and external provisions with users being granted access without any valid business need. As a result, critical threat intelligence operations could be executed without appropriate oversight, increasing the risk of unauthorized data manipulation and the dissemination of false or malicious information in the operational environment. This may lead to material reputational damage, minor financial loss, and potential breach of regulatory requirements.
Criteria	▪ EU Regulation 2022/2554 (DORA), articles 20 and 21 ▪ EMIR article 9 ▪ EBA/GL/2019/04 sections 3.3.2, 3.5 – 31

	▪ ISO/IEC 27001:2022 A.5.15 ▪ *DBG Identity and Access Management Standard*, v4.0, chapter 3 ▪ *DBG Identity & Access Management Guideline*, v1.0, chapters 3 and 12.1
Relevant entity	DBAG/ExR/EFAG/ECAG/CBF/CBL/CS/LuxCSD/CFCL
Recommendation	Internal Audit recommends that Security IT – Engineering Build and Improve (CUR) clearly define and implement the missing segregation of duties (SoD) controls in IIQ and update the outdated information in the MISP (AID737) Authorization Concept. This should include: ▪ defining and updating the role concept, including segregation of duties requirements, such as the correlation of user roles, the toxic role combination assessment, potentially creating new roles in alignment with changing technology needs and evolving security risks, as well as ensuring the technical IIQ implementation of the respective rulesets ▪ any remaining gaps or limitations resulting in excessive access rights should be documented in the risk register ▪ finalizing the above activities related to applying SoD principles and ensuring updated information within the application's Authorization Concept The recommendation was adequately addressed before the issuance of the report.
Management response	Security IT – Engineering Build and Improve (CUR) agrees with the finding and recommendation and has implemented the recommendation.
Recommendation owner	Security IT – Engineering Build and Improve (CUR)
Target date	Closed

Severity rating	S1
Finding number	2025-045_F08
Finding related to	Control design effectiveness and control operating effectiveness
Title	Lack of details in vulnerability management procedures in respect to timelines of involved teams
Description of finding	When assessing DBG's vulnerability management solution Rapid7 Nexpose (NXP), Internal Audit (IA) identified around 2500 NXP tickets with status 'Fix Claimed' that were overdue, out of which 45 were critical or high. Addressing vulnerabilities until closure is the IT Asset Owner's/Application Owner's (IT teams) responsibility, and the vulnerability management team – Plan & Design Services (VLM) – acts as a control function, by confirming/rejecting the IT teams 'Fix claimed' and 'False Positive' status claims. Such tickets statuses are being reported as part of the Digital Security Committee (DSC) KPIs, however these should have been treated and set to 'close' by the VLM team or by the automated re-test. Deadlines for treatment of vulnerabilities are set in the ICT Patch and Vulnerabilities Management Guideline, however multiple teams need to be involved – teams treating the fix (IT teams) and validating the fix (VLM), who all need a certain time to perform their tasks. The underlying procedures were not detailed enough to be able to respect jointly the timelines set by the guidelines. In case the IT team submitted the ticket as 'Fix Claimed' just before the overall deadline, the ticket was already in 'overdue' status when treated by VLM. European, German and Luxembourg regulation requires organizations to establish a structured process for identifying, assessing, remediating, and reporting vulnerabilities.
Root cause	Insufficient policies, procedures and guidelines
Risk	Lack of details in vulnerability management procedures in respect to timelines of involved teams may lead to delays or overdue in reporting. This could lead to negligible breach of regulatory and internal requirements.
Criteria	▪ EU Regulation 2022/2554 (DORA), Article 25 ▪ CSSF Circular 20/750, Section 3.4 ▪ MAS TRM 13.1.1 ▪ *DBG ICT Patch and Vulnerability Management Guideline*, v1.0
Relevant entity	DBAG/ExR/EFAG/ECAG/CBF/CBL/CH/CI/CS/LuxCSD/CFCL/ECC/EEX
Recommendation	Internal Audit recommends that Plan & Design Services (VLM) propose an adequate solution agreed between relevant stakeholders and implemented in related procedures.

Management response	Plan & Design Services (VLM) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Plan & Design Services (VLM)
Target date	February 18, 2026

4. Finding severity definition[4]

For details on finding severity definition, please refer to Group Audit - Findings severity definitions

[4] 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.

5. Distribution list

Executive Management	Gregor Pottmeyer	Member of DBAG Executive Board
	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 CBF Executive Board
	Martina Gruber	Member of CBF Executive Board
	Udo Henkelmann	Member of CBF Executive Board
	Volker Riebesell	Member of CBF 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
	Jens Hachmeister	Member of CI Board of Directors
	Fabrice Tomenko	CEO of CI Board of Directors
	Armin Borries	Member of CS Executive Board
	Boglarka Bartha	Member of CS Executive Board
	Daniel Besse	CEO of CS Executive Board and Member of CH Executive Board
	Marco Caligaris	CEO of LuxCSD
	Philippe Seyll	CEO of CFCL Executive Board
	Neil Wise	Member of CFCL Executive Board
	Sonia Dribek-Pfleger	Member of CFCL Executive Board
	David Brosnan	Member of CFCL Executive Board
	Marco Steeg	Member of CFCL Executive Board
	Bernard Tancré	Member of CFCL Executive Board
	Kevin Hayes	Member of CFCL Executive Board
	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	Interim CEO of ECAG Executive Board and Member of EFAG Executive Board
	Frank Gast	General Manager of ExR
	Frank Odendall	General Manager of ExR
	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
	Tobias Paulun	CEO of ECC Executive Board
	Götz Dittrich	COO ECC
	Peter Reitz	CEO EEX
Business Line	Christian Gorke	Chief ICT Risk Officer/CISO
	Christian Goetz	HoU ICT Risk Strategy and Methodology (KLM)
	Petr Strnad	HoS ICT Risk Controlling (MRI)
	Alexandru Lupan	HoU ICT Internal Controls Monitoring (IIM)
	Sarah Ahmad Jahn	HoU ICT Risk Framework (KJU)
	Sourabh Shrivastava	HoU ICT Risk Assurance (KIU)
	Marco Popp	HoS Group Compliance Strategy (SCG)
	Hinrich Völcker	CSO DBAG, HoD Group Security (ZZA)
	Florian Rodeit	HoS IS Governance & Risk (RGI)
	Sibylle Hick	HoS Cyber Protection & Automation (IFB), ad-interim: HoU Plan & Control (WAR)
	Mario Sema	HoU Penetration Testing and Red Teaming (DLP)
	Rahul Choubey	HoU Plan and Design Services (VLM)
	Rui Mendes	HoU Detect & Prevent (DTP)
	Olga Wenge	HoS Cyber Defense (CBD), ad-interim: HoU Threat Intelligence & Threat Hunting (TIT)
	Jeremy Lucas Mendiola	HoU SOC/CERT (IFD)
	Baptiste Sichere	HoU Cyber Analytics (CAN)
	Lydia Ricarda Kretschmer	HoU Cyber Defense Framework (CDF)
	Julian Wiegmann	HoU Strategy & Architecture (ZZX)
	Anke Dannenberg	HoU Group Security LE Governance (GLE)
	Branislav Rajcani	HoU IS Risk Management (IGI)
	Sean Mc Taggart	HoU IT Core Process Design and Operations (ÜPÜ)
	Bartosz Baczynski	HoU IT Audit & Findings Management (IFM)
	Volker Henke	HoU Post Trade IT Governance Unit (GPC)
	Steffen Thomas Gremm	HoS Post Trade IT PaaS Delivery (IZC)
	Stephane Deschamps	HoS Monitoring and Application Support (ZEV)
	Joel Scherrer	HoS Connectivity & CFS Applications Support (CFT)
	Christophe Jacob	CFS Production Support (PRD)
	Francois Leveling	HoD Corporate IT Cloud Operations (GAL)
	Nataliia Iskra	HoS Security IT (BHY)
	Geoffrey Saint-Alary	Security IT – Digitise, Evolve and Innovate (SAO)
	Ana-Simona Pop	Audit Coordination and Support, Security IT (BHY)
	Michal Rudolf	Security IT – Engineering, Build and Improve (CUR)
	Helge Harren	HoD Xetra/Eurex Operations (ZJK)
	Thomas Reich	HoS Xetra/Eurex Infrastructure Operations (IIA)
	Maja Sdrakas	HoD Data-aaS (ITI)
	Frantisek Hradil	HoS Reference Data as a Service (IZM)
	Pavlina Valentova	HoU Instrument and Institution Data IT (ÖÖD)
	Frank Hoba	HoD Cash Market Design and Delivery (XAT)
	Alexej Roytburg	HoU Functionality & Partner Exchanges (CMD)
	Jens Hoffmann	HoU Trading IT Support (ZFX)
	Stefan Wenske	HoS Xetra/Eurex Delivery & Support (XED)
	GS_Findings-Management@deutsche-boerse.com	Group Security Findings Management

	CRP-Audit@deutsche-boerse.com	CRP-Audit coordination, Corporate IT
	LuxCSD_Audit_Control@LuxCSD.com	LuxCSD Audit Control
Risk Management	Dominik Schmidt-Kiefer	Chief Risk Officer DBAG
	cfclriskmgt@clearstream.com	CFCL Risk Management Inbox
	Ralf Prinzler	CRO ECC
Group Legal	Bettina Kramer-Braun	Managing Director of Group Legal
Compliance	Marc Peter Klein	Group Chief Compliance Officer
	GC_Audit_Coord@deutsche-boerse.com	Group Compliance Audit Coordination
	Christian Heyne	Chief Compliance Officer CBL
	Oliver Haderup	Chief Compliance Officer ECAG
	Jan Kobbach	Chief Compliance Officer CBF and CH
	Katja Röhle	Chief Compliance Officer ExR
	Sabine Guip	Chief Compliance Officer CFCL
	Bianca Sahrholz	Head of Unit CCP Compliance
	Stefan Gebauer	Director Compliance ECC
	tvr-audit-monitoring-eurex@eurex.com	EFAG TVR Inbox
	cfclcompliance@clearstream.com	CFCL Compliance Inbox
ICT	Sebastian Wedeniwski	CTO, DBAG
	Boris Link	HoD IT Governance, Risk and Transformation (IRT)
	Neslihan Meinert	CTO ExR
	Ulf Wollenweber	CISO ExR
	Jörg Pfeffer	CISO EFAG
	Karthik Ramamurthy	CISO CFCL
	Jan Patrick Drehwald	CISO CBF
	Henning Volz	CISO ECAG
	Yannik Goineau	CIO CBL
	Nejib Zaouali	CISO CBL
	Jens Rick	CIO ECC/EEX
	Marc Schlösser	LE CISO ECC/EEX
	crit-is-office@deutsche-boerse.com	CRIT IS Office ECAG
Internal Audit	Andrea Bracht	Group Audit
	Dietmar Hinkel	Group IT Audit
Audit Manager(s)	Tatjana-Janine Tollkühn	Internal Audit DBAG
	Mirweiss Inayt	Internal Audit CBF
	Valerie Aubert	Internal Audit CBL
	Thomas S. Musgrave	Internal Audit ECAG
	Bertrand Thiault	Internal Audit CFCL
	Runa Eichler	Internal Audit ECC
Auditor(s)	Yezad Wadia	Internal Audit DBAG
	Anvay Walavalkar	Group IT Audit
	Özge Gueltekin Arslan	Internal Audit ECAG
	Yigit Gullu	Internal Audit CBF

	Milos Medrik	Internal Audit CBL
	Urvashi Emrith	Internal Audit CFCL
	Kevin Gregory Floro	Internal Audit ECC
	Predrag Adamovic	Internal Audit DBAG

6. Appendix A

Detailed scope

Cyber and Information Security (IS) processes implemented across Deutsche Börse Group (DBG) protect the organization's information assets from unauthorized users, disruption, alteration, or destruction, and strengthen the overall control environment to reduce risk.

The objective of this audit was to assess:
- DBG's Cyber and Information Security - governance framework
- the overall operating setup and posture i.e. evaluate security measures, as well as identifying weak links, vulnerabilities and potential risks
- whether processes and controls operated in compliance with Laws and Regulations.

The audit scope was determined on a risk basis and covered the following key aspects of the Cyber and Information Security processes:
- Cyber & IS Strategy and Design
- ICT Incident Management
- Cyber & IS Prevention
- Cyber & IS Detection
- Cyber & IS Control functions (2nd LoD)
- Threat Intelligence

As a specific focus area, the audit included a risk-based review of cryptography and key management controls. IA examined known cryptography risks, their assessment and mitigation (e.g., SSH Key Inventory/Management, PKI Structures), and performed a deep dive into the operationalization for sampled applications.

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 approach included the following steps:
- initial assessment of the organization's framework of Cyber and IS management, control and governance processes supplemented by walkthroughs of the key processes/areas/domains
- assessment of risks, issues and key controls identified during walkthroughs
- considering fraud risks in the assessment of the internal control design
- evaluation of the key risk areas for further testing
- sample testing of the key risk areas

Further ongoing remediation activity: IA is aware that several ongoing Group-wide programs are addressing known gaps and the associated risks in the area under review, e.g. IT Amelioration (AMELI) and DORA Readiness, with implementation by end of 2025/H1 2026. In particular:

- Many aspects, such as digitalization of Application Security Document, IS Risk Management, SSH Key Inventory and Management (SKI/SKM), Database Activity Monitoring (DAM), management of Security Information and Event Management (SIEM) data, Advanced Persistent Threat (APT) protection, etc. were still undergoing remediation/implementation. IA is accompanying significant external findings remediation with separate validation activities. So, a further duplicative examination of these aspects was not expedient.

- As part of the DORA Readiness program, First Line of Defense (1st LoD) – Group Security (ZZA) is working to streamline the Cyber and Information Security (IS) processes and control requirements. It was agreed to keep the yearly update cycle for ZZA-managed procedures, which consequently results in a time gap in the "operationalization" of updated Second Line of Defense (2nd LoD) policies and guidelines into 1st LoD procedures and operations. Until then, the previous 1st LoD IS operational documents and procedures are still valid.

- Additionally, the DORA Readiness Program implements further Cyber and IS related DORA requirements, such as security operations incl. cryptography, Threat-Led Penetration Testing (TLPT), and ICT[5] incident management. Management is aware that further ongoing effort is needed in 2025 to achieve organizational readiness and sustain future BAU activities.

Threat-Led Penetration Testing (TLPT): Information sharing about planned or ongoing TLPT exercises is restricted to the "control team", the management body, the testers, the threat intelligence provider and the regulator (TLPT authority) according to DORA RTS on TLPT, Article 4 (2) a. Since composition of the control team under DORA is limited to stakeholders managing the TLPT test, and governed by a validation process by the regulator, IA has so far been excluded. Therefore, information pertaining to any potentially ongoing first TLPT exercise under DORA could not be shared with IA to avoid compromising the secrecy of the test. This situation limited IA's ability to conclude on DBG's overall preparedness for the TLPT exercise. For the scope of this audit, IA has reviewed only the design effectiveness of the test (i.e. the Target Operating Model and related documents).

Cyber & IS Control functions (2nd LoD): Following the 2024 Technology Governance audit (2024-063) and its open S3/S2 findings, several key initiatives/remediations are underway. Led by CICTRO/CISO[6] (ICT), a new 2nd LoD target operating model (TOM) was rolled out by end-2024. Also, ICT Risk Assurance (KIU) launched its updated methodology in October 2024 and is executing the 2025 cycle, with follow-ups due by January 2026. Group Compliance Strategy (SCG) and the CISO also introduced a new IT Compliance and ICT Risk TOM aligned with DORA, now in implementation. An open item remains on finalizing the outsourcing SDS and 2025 control plan, targeted for January 2026. Given these developments, the topic was deferred to the next regular Cyber and Information Security audit.

[5] ICT being a term used by regulators for all Information and Communication Technology, including information technology (IT) and information security (IS).

[6] CICTRO/CISO – Chief Information and Communication Technology Risk Officer/Chief Information Security Officer.