Internal Audit Report

2025-001 IT Operation Management

7 April 2025

- CONFIDENTIAL -

Audit scope period	January 2024 to December 2024
Legal entities in scope	DBAG/ExR/EFAG/ECAG/CBF/CBL/CH/CI/CS/LuxCSD/CFCL
IA function	DBAG/ECAG/CBF/CBL/CFCL
Location	Eschborn & Luxembourg

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

1. Executive summary

Internal Audit performed an audit of the IT Operation Management processes implemented across Deutsche Börse Group (DBG). They maintain and improve the availability and performance of IT systems and services, which are essential for the smooth business operation and growth.

The audit is part of the standard audit cycle and was performed between January and March 2025.

Based on the testing defined and performed, and under consideration of the known gaps that are being addressed through the dedicated initiatives further detailed below, Internal Audit (IA) did not identify any further findings. The reviewed processes and established controls were found to be mature.

However, improvements are needed for new technologies, where one S3 self-identified issue (SII) on inadequate Cloud container governance and security was reported by Management, with steps pro-actively taken to address the risk, demonstrating good risk management practices:

- With regard to the Google and Microsoft Cloud platforms, the IT governance framework was lacking specific roles and responsibilities, as well as requirements around asset and change management, privileged access and security. This had already led to inconsistent containerisation practices, incomplete asset inventory, overprivileged accounts, vulnerabilities and misconfigurations related to Cloud containers not being addressed. The remediation actions initiated by Management aim to ensure the secure management and operations of containers as a new layer between operating systems and applications.

For more information on the SII, refer to Section 2 “Self-Identified Issues” of this report. In addition to the legal entities involved in this audit, the SII was also relevant for ECC, EEX and ISS STOXX.

IA is aware that several Group-wide initiatives are ongoing to address known gaps and the associated risks in the area under review, e.g. IT Amelioration program (AMELI), DORA-readiness (Digital Operational Resilience Act - European Union) Program and Hyperion Layer 2 Project. The initiatives are supported by regular reporting to management and continue with implementation by end of 2025 / first half of 2026. In particular:

- Although no additional findings were identified, many aspects such as IT asset management were still undergoing remediation, especially from AMELI, which is why a further duplicative examination of these aspects was not expedient. IA would like to strongly encourage the parties involved to keep the current focus to timely improve all the measures in the scope of AMELI, allowing the risks to be addressed.

- Additionally, the DORA Readiness Program equally impacted the whole area. Even though the program with the respective segments is tracking and monitoring implementation progress, it will require further ongoing effort in 2025 to achieve organisational readiness and sustain future BAU activities. Periodic alignment meetings between DBG and regulatory bodies (BaFin and CSSF) are arranged regarding DORA readiness reporting and the plan of remaining activities within the defined timelines.

2. Self-Identified Issues

Severity rating	**S3**
SII Identification number	2025-001_F01 (AMIT-1407, AMIT-1408, AMIT-1402)
SII related to	Control environment, control design and control operating effectiveness
Title	Inadequate Cloud container governance and security
Description of SII	Containers are an abstraction layer used in Cloud computing. They are lightweight packages of application code bundled with all its dependent elements, therefore allowing flexible deployment, shifting and running in any (Cloud or on-premises) environment. In contrast to virtual machines (VMs), containers do not encompass an underlying operating system and are therefore easier to manage in terms of size, portability and operations. As containers introduce a new layer between operating systems and applications, the IT governance framework would also need specific requirements and processes to ensure their secure management and operations. Chief Cloud Officer / Core Infrastructure (ZFJ) and IT Governance, Risk and Transformation (IRT) controls reviews in January 2025 noted a lack of defined and documented IT and IS Governance requirements for Cloud container asset types and container platforms (scope: OpenShift, Kubernetes). As a result, non-standardised and de-centralised heterogeneous container technologies and containerisation practices have evolved and led to several deficiencies across the control environment: ▪ Undefined roles and responsibilities ▪ Asset management: lack of clear ownership of each container, as well as missing linkage with applications and business processes ▪ Change management & Privileged Access Management: gaps and manual practices in the change processes resulting in the need for overprivileged developer access to production containers (particularly OpenShift) for infrastructure provisioning ▪ Security: OpenShift platforms not under governance of the “Secure Landing Zones” (SLZ), which were designed for cloud-native workloads in Google Cloud Platform (GCP) and Microsoft (MS) Azure; inability to perform software scans inside container images with DBG’s discovery solutions This impacted all legal entities using GCP and MS Azure and relying on OpenShift. Due to the thematic overlap, the aspects covered in this issue were merged from three separate SIIs on Cloud container governance.

Risk	Inadequate Cloud container governance and security may lead to major operational and financial impact and high potential for extra reporting requirements and/or regulatory examinations as a result of: ▪ high variety of container technologies potentially without sufficient operational and tools support ▪ incomplete software inventory in the asset inventory CMS (Configuration Management System), unauthorised software usage, increased risk of unknown vulnerabilities. ▪ misconfiguration of Cloud Service Provider (CSP) services based on OpenShift solution; overprivileged service principals. Further, it might lead to serious violation of internal and/or external provisions, such as a major breach of regulatory requirements, e.g. non-existent description/documentation of processes and/or control environment.
Root cause	Lack of governance and inadequate controls
Relevant entity	DBAG/ExR/EFAG/ECAG/CBF/CBL/CH/CI/CS/LuxCSD/CFCL/ECC/EEX/ISS STOXX
Intended actions	In alignment with the different parties involved, the responsible action owners have proactively started to address and continue the implementation around the Cloud and Secure Landing Zones across the DBG LEs. High-level responsibilities are as follows with owners taking the lead to complete: ▪ Supported by CTO and in coordination with Group Security (GS), IT Governance, Risk and Transformation (IRT) to: - review and improve the governance around container asset type, reflected in the ICT Asset and Change Management framework. - enhance the baselines for approved container technologies and configurations. Resolution due date: 31 January 2026 ▪ IRT in coordination with GS, - perform a proof of concept using PA CNAPP - Palo Alto's Cloud-Native Application Protection Platform (AID2146) - sourced discovery data to enrich container asset information in DBG's CMS system. - depending on the implementation of the IT Governance requirements, assess and implement a discovery tool supporting DBG container technologies. Resolution due date: 15 April 2026 ▪ Chief Cloud Officer / Core Infrastructure (ZFJ) to adapt the Azure and GCP landing zone for OpenShift workloads i.e. by: - designing and documenting the desired target state. - implementing automated controls for OpenShift platforms on SLZs. - mitigating risks of high privileges required for installation and

	configuration. Resolution due date: 15 July 2026 The progress of above-mentioned actions is regularly tracked by the IT Governance Council and the Secure Landing Zone Steering Committee.
Owners	IT Governance, Risk and Transformation (IRT) Chief Cloud Officer / Core Infrastructure (ZFJ)
Target date for resolution	15 July 2026
Rationale for long due date:	To note, the remediation measures for the above-mentioned activities are subject to multiple team coordination and availability. Interdependencies between the actions to be taken by responsible and involved action owners. Also, the technical feasibility analysis is to be performed. Accordingly, a solution must be designed, developed and implemented to mitigate the current situation.

3. Finding severity definition[1]

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

[1] 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.

4. Distribution list

Executive Management	Stephan Leitner	CEO of DBAG Executive Board
	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
	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
	David Brosnan	Member of CFCL Executive Board
	Neil Wise	Member of CFCL Executive Board
	Sonia Dribek-Pfleger	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	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, General Manager of ExR
	Frank Gast	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
	Tobias Paulun	CEO of ECC Executive Board

	Jens Rick	Member of ECC Executive Board
	Götz Dittrich	Member of ECC Executive Board
	Marc Robert-Nicoud	Managing Director of ISS-STOXX
	Frank Prasse	Managing Director of ISS-STOXX
	Gary Retelny	CEO of ISS-STOXX
Business Line	Boris Link	HoD IT Governance, Risk and Transformation (IRT)
	Sean Mc Taggart	HoU IT Core Process Design and Operations (ÜPÜ)
	Bartosz Baczynski	HoU IT Audit & Findings Management (IFM)
	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)
	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)
	Francois Leveling	HoD Corporate IT Cloud Operations (GAL)
	Sriram Mani	HoS Cloud Application Operations (CAO)
	Nataliia Iskra	HoS Security IT (BHY)
	Benedicte Clotuche	HoU PaaS Storage and Backup (GAA)
	Rajesh Srinivasan	HoS StatistiX IT (ZJM)
	Helge Harren	HoD Xetra/Eurex Operations (ZJK)
	Thomas Reich	HoS Xetra/Eurex Infrastructure Operations (IIA)
	Michael Beckmann	HoU Xetra/Eurex Server Administration (XES)
	Juergen Schilp	HoU Xetra/Eurex Server Engineering (XEE)
	Joerg Schaetzlein	HoS Xetra/Eurex Clearing & Risk Applications (IRC)
	Peter Rommel	HoU Xetra/Eurex Database Operations (GAD)
	Martin Casper	HoS XE Trading Applications & Operations (XEA)
	Rasmus Kullanek	HoU Xetra/Eurex Operations Germany (IIB)
	Maja Sdrakas	HoD Data-aaS (ITI)
	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
	Udo Henkelmann	Chief Risk Officer CBF
	Tobias Büchel	Head of Risk Controlling & Governance
	Jean-Marc Di Cato	Chief Risk Officer CH and CBL
	Dmitrij Senko	Chief Risk Officer ECAG
	Sonia Dribek-Pfleger	Chief Risk Officer CFCL
	Ralf Prinzler	Director Risk Management ECC
	Victorine Oemus	Director Enterprise Risk & Outsourcing Management ECC
	Eva Stumpfova	Risk Management ISS-STOXX
	cfclriskmgt@clearstream.com	CFCL Risk Management Inbox
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
	Michael Hyzik	Compliance ISS-STOXX
	tvr-audit-monitoring-eurex@eurex.com	EFAG TVR Inbox
	cfclcompliance@clearstream.com	CFCL Compliance Inbox
ICT	Sebastian Wedeniwski	CTO, DBAG
	Christian Gorke	Chief ICT Risk Officer/CISO
	Boris Link	HoD IT Governance, Risk and Transformation (IRT)
	Marcus Lehmann	HoD IT Strategy / Chief of Staff (ZJV)
	Hinrich Völcker	CSO DBAG
	Neslihan Meinert	CTO ExR
	Ulf Wollenweber	CISO ExR
	Quinten Koekenbier	CTO EFAG
	Jörg Pfeffer	CISO EFAG
	Kevin Hayes	CIO CFCL
	Volker Riebesell	CTO CBF
	Jan Patrick Drehwald	CISO CBF
	Manfred Matusza	CTO ECAG
	Henning Volz	CISO ECAG
	Yannik Goineau	CIO CBL
	Nejib Zaouali	CISO CBL and acting CISO CFCL
	Daniel Besse	CIO CS
	Marco Caligaris	CEO LuxCSD
	Marc Schloesser	CISO ECC/EEX
	Ludwig Heinzelmann	HoS Central Post Trade IT Office (PTI)
	Stephen Holden	HoS Cloud Transformation (CUT)
	Kevin O'Leary	Chief Information Officer ISS-STOXX
	crit-is-office@deutsche-boerse.com	CRIT IS Office ECAG
Internal Audit	Andrea Bracht	Group Audit
	Dietmar Hinkel	Group IT Audit
	Runa Eichler	Internal Audit ECC
	John Genello	Internal Audit ISS-STOXX
Audit Managers	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
Auditors	Daniel Hart	Internal Audit CBL
	Yezad Wadia	Internal Audit DBAG
	Viswanath Palakkad Swaminathan	Internal Audit ECAG
	Yigit Gullu	Internal Audit CBF
	Fabrice Moreira	Internal Audit CFCL
	Gil Strahl	Internal Audit CBL

5. Appendices

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 IT Operations Management processes:

- IT-Operations Governance
- IT Asset Management, Configuration Management and Licence Management[2]
- IT Operations Management
- Capacity Management and Storage Management
- Cloud operations

Limitations of scope: As indicated in the Executive Summary, the processes under review were highly impacted by currently ongoing internal projects. Limitations were set not to impact these projects and activities were aligned with the auditee.

[2] Basis a risk-based approach, Licence Management was outside the scope of this audit, considering the exhaustive review performed in the prior year and an open finding with ongoing remediation measures due in March 2025.