Internal Audit Report

2025-039 CFCL IT, Information & Physical Security

December 12, 2025

- CONFIDENTIAL -

Audit scope period	January 2024 to May 2025
Legal entities in scope	CFCL
IA function	CFCL
Location	Luxembourg

Results	**S1**	**S2**	**S3**	**S4**
Total Internal Audit findings: 6	2	4	-	-
Self-identified Issues: -	-	-	-	-

1. Executive summary

CFCL Internal Audit performed an audit of CFCL's governance, risk management, and internal controls around IT Governance, IT and Information Security, and Physical Security processes.

Internal Audit acknowledges the collaboration of CFCL IT's 1LoD governance services and the centralized Post Trade IT Governance (GPC) unit to create synergies across Clearstream legal entities. However, the audit found that implementation of this operating model and the overall control environment required improvement to ensure full effectiveness and demonstrate compliance with regulatory expectations.

The audit revealed overarching weaknesses in both CFCL and GPC IT governance frameworks. The synergized operating model was not supported by formalized documentation or a robust oversight structure. This resulted in fragmented accountability and inconsistent management of internal written rules. Internal Audit also noted a lack of dedicated legal entity-level reporting of CFCL's IT security posture and insufficient oversight of outsourced services, particularly for cloud arrangements. Deficiencies were also identified in physical access controls to secure areas, and the accuracy of Internal Control System documentation.

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

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	CEU	CBL	CH	CS	LuxCSD	CFCL			
Governance and accountability documentation gaps in CFCL IT's operating model (2025-039_F01)	S2	5	Christoph Böhm	-	Volker Riebesell	Yannick Goineau	Daniel Besse	Daniel Besse	Marco Caligaris	Kevin Hayes	Post Trade IT Governance (GPC) (2025-039_F01-A01)	Daniel Besse (CS)	Dec 15, 2026
											CFS IT (ZJL) (2025-039_F01-A02)	CFCL (Kevin Hayes)	Dec 15, 2026
Inconsistent management and governance of CFCL 1LoD IT Written Rules (2025-039_F02)	S2	7	Christoph Böhm	-	-	-	-	-	-	Kevin Hayes	CFS IT (ZJL)	CFCL (Kevin Hayes)	Dec 15, 2026
Deficiencies in CFCL IT governance and oversight framework (2025-039_F03)	S2	10	Christoph Böhm	-	-	-	-	-	-	Kevin Hayes	CFS IT (ZJL) (2025-039_F03-A01)	CFCL (Kevin Hayes)	Dec 15, 2026
											Post Trade IT Governance (GPC) (2025-039_F03-A02)	Daniel Besse (CS)	Dec 15, 2026
											IS Risk Management (IGI) (2025-039_F03-A03)	Christoph Böhm (DBAG)	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	CEU	CBL	CH	CS	LuxCSD	CFCL			
Incomplete governance and oversight of CFCL cloud outsourcing arrangements (2025-039_F04)	S2	16	Christoph Böhm	-	-	-	-	-	-	Kevin Hayes	CFS IT (ZJL)	CFCL (Kevin Hayes)	Dec 15, 2026
Inadequate CFCL secure area physical access controls (2025-039_F05)	S1	18	Stephanie Eckermann	-	-	-	-	-	-	Philippe Seyll	Clearstream Fund Services (MIF)	Philippe Seyll	Apr 30, 2026
Inaccurate CFCL Internal Control System (ICS) process maps and Risk Control Matrices (2025-039_F06)	S1	20	Christoph Böhm	-	-	-	-	-	-	Kevin Hayes	CFS IT (ZJL)	CFCL (Kevin Hayes)	Mar 31, 2026

3. Finding details

Severity rating	**S2**
Finding number	2025-039_F01
Finding related to	Control environment and design effectiveness
Title	Governance and accountability documentation gaps in CFCL IT's operating model
Description of finding	Internal Audit (IA) review of CFCL's First Line of Defense (1LoD) governance and operating model, and identified gaps in the formalization, documentation, and role delineation within CFCL IT: ▪ <u>No formal operating model documentation</u> While CFCL IT's 1LoD governance services integrated into Post Trade IT Governance (GPC) in January 2024, no documentation was maintained to describe the new organizational design, synergy concept, legal entity independence or compliance with regulatory requirements. The model was not submitted to the CFCL Executive Board for approval or acknowledgment. ▪ <u>No formalized IT Governance Framework</u> Despite GPC being operational, there was no documented IT governance framework illustrating its structure, legal entity coverage, roles and responsibilities, RACI matrix for accountability, and alignment with the Group-level IT Governance System led by IT Governance, Risk and Transformation (WRT). ▪ <u>Inconsistent strategy and role representation</u> CFCL IT's legal entity responsibilities were inconsistently represented in strategic documents. E.g., the CFS IT organizational chart was incorrectly labeled as CFCL IT, and terminology such as "Clearstream IT" or "CFS IT" was used interchangeably leading to misrepresentation of actual CFCL IT activities. ▪ <u>Potential Conflict of Interest in dual roles</u> The Head of CFS IT (ZJL) also served as CFCL Chief Information Officer (CIO), creating an inherent conflict of interest risk. In case of KPI breaches or poor service delivery, escalation would be directed to ZJL, who also oversaw the insourcer teams. This may impair independent CFCL decision-making without appropriate mitigants. The conflict risk was not reported to CFCL Compliance or Group Compliance and mitigating measures not documented.
Root cause	Inadequate Process
Risk	Governance and accountability documentation gaps in CFCL IT's operating model may lead to inadequate CFCL governance, potentially resulting in regulatory non-compliance, or strategic misalignment with synergized IT initiatives not supporting legal entity interests. Unclear roles and responsibilities may result in a lack of accountability and transparency including inefficient resource allocation. Overall, this represents a material gap against internal and external provisions and could lead to minor financial loss and potential breach of regulatory requirements.
Criteria	▪ DORA, Article 6 ▪ CSSF Circular 12/552 ▪ CSSF Circular 22/806 ▪ *ICT Risk Management Policy V1.0*

	▪ *Outsourcing & Third-Party Risk Policy V7.0* ▪ *DBG Policy On Conflict of Interest V5* ▪ *Clearstream Fund Centre S.A. - IT Strategy 2024-2026 V2.0* ▪ *Clearstream Fund Centre S.A. - Outsourcing Business Surveillance Procedure*
Relevant entity	CFCL, CBL, CEU, CH, CS, LuxCSD
Recommendation number	2025-039_F01-A01
Recommendation	Define and implement Post Trade IT Governance (GPC) Operating Model, including role delineation, and regulatory alignment (e.g., CSSF 22/806 and 12/552 circulars) ▪ Establish and formalize appropriate control mechanisms and documentation, including RACI matrix and reporting lines ▪ Collect any required formal approval(s).
Management response	Post Trade IT Governance (GPC) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Post Trade IT Governance (GPC)
Target date	December 15, 2026

Recommendation number	2025-039_F01-A02
Recommendation	▪ Reinforce the legal entity view within the CFCL IT Strategy including dedicated CFCL IT (1LoD) organization chart showing legal entity roles and responsibilities, and reporting lines. ▪ Enforce consistent organizational units' naming in the IT Strategy i.e., "CFCL IT" for legal entity oversight/governance responsibility, "CFS IT" exclusively while referring to the department in Post Trade IT. Avoid using unspecific "Clearstream IT". ▪ Define and implement a CFCL IT Governance Framework model including scope, roles/responsibilities, RACI matrix, reporting lines and regulatory alignment (e.g. CSSF 22/806 and 12/552 circulars) - Describe how CFCL IT Governance is embedded within the DBG matrix organization (e.g., GPC) - Collect any required formal approval(s). ▪ Notify CFCL Compliance of any situation potentially leading to conflicts of interest (e.g., acting as providers in outsourcing arrangements) for further assessment and formalization of mitigating measures.
Management response	CFS IT (ZJL) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	CFS IT (ZJL)
Target date	December 15, 2026

Severity rating	**S2**
Finding number	2025-039_F02
Finding related to	Design and Operating Effectiveness
Title	Inconsistent management and governance of CFCL 1LoD IT Written Rules
Description of finding	Internal Audit (IA) identified inconsistencies in the management and governance of CFCL IT Written Rules, which undermine the effectiveness of existing written rules and contractual arrangements between CFCL and DBAG: ▪ Unaligned Repositories and Governance Structures - GPC maintained on SharePoint a separate "Clearstream IT Written Rules Repository" which contained CFCL IT Written rules and further indicated unfamiliarity with the Group "Written Rules" database. - The "*Clearstream IT Written Rules Repository Procedure v.1.0*" (dated 12 Feb 2025) outlining lifecycle management of CFCL IT Written Rules, lacked formal administrative delegation to GPC, consideration of existing DBAG-CFCL contractual frameworks and a formalized adoption process of the Group Written Rules. ▪ Gaps noted within the CFCL IT Handbook - The CFCL IT Handbook was positioned as an official reference source, yet IA found outdated, incomplete, or inconsistent documentation across key process bundles: ○ Process Bundle: CFCL Run – Incident Management The Incident Management Process document: ➢ Incorrectly listed IRT as owner and CS as process operator, omitting CFCL's accountability for outsourced risk. ➢ Lacked CFCL review/adoption evidence and failed to align with DORA Articles 18–19 and CSSF Circular 25/893. ➢ Referenced decommissioned Group guidelines (e.g., *Incident & Crisis Management Guideline)* and missing supporting documents (e.g., ICT Incident Management Procedure, Incident Statement Template). ○ Process Bundle: CFCL Run – Continuity Management: ➢ Missing DBG ICT Operations Guideline within CFCL IT Repository ➢ The Clearstream IT Resilience Management Procedure duplicated DBAG's IT Resilience Management Procedure in terms of chapters, methodology, and regulatory alignment with DORA. The only observed differences were superficial terminology changes: • Replacement of "DBAG" with "Clearstream" • Reassignment of Process Operator responsibility from DBAG IT Governance Team to CFCL IT Process Operator ➢ No evidence of formal adoption or gap assessment by CFCL to reflect consideration of CFCL-specific requirements of the DBAG IT Resilience Testing procedure. To add CFCL owned IT assets were also in the scope of the DBAG IT Resilience testing. ➢ Misassigned Governance roles within the RACI Matrix: IRT (Group Coordinator) and GPC (Legal Entity Coordinator) roles were omitted, and the CFCL Process Operator was incorrectly designated as Legal Entity Coordinator, despite not participating in DBAG governance forums. ➢ Reporting was directed at the Process Operator Committee, which GPC confirmed does not exist and for which the Clearstream procedure had to be updated.

Root cause	Inadequate controls
Risk	Inconsistent management and governance of CFCL 1LoD IT Written Rules may compromise written rules transparency, accountability, and redundancy, due to misaligned documentation and inconsistent implementation across the legal entity leading to control failures. Also, given CFCL's reliance on outsourced Group IT services, the absence of a formal written rule adoption process increases the likelihood that CFCL-specific (internal and external) requirements be overlooked, impairing oversight of and alignment with service providers or insourcer. Overall, this represents a material gap in internal and external provisions and could lead to minor financial loss and potential breach of regulatory requirements.
Criteria	▪ DORA, Article 6 ▪ Circular CSSF 12/552 ▪ CSSF Circular 24/847 ▪ CSSF Circular 25/893 ▪ *ICT Risk Management Policy V1.0* ▪ *Written Rules Framework Procedure V1.1* ▪ *Clearstream IT Written Rules Repository Procedure V1.0* ▪ *Clearstream IT Resilience Management Procedure V1.0* ▪ *IT Resilience Management Procedure V1.0* ▪ *ICT Incident Management Procedure V1.0* ▪ *Written Rules Framework Guidelines V1.0* ▪ *ToR Written Rules Committee V1.3*
Relevant entity	CFCL
Recommendation	▪ Review the *Clearstream IT Written Rules Repository Procedure* to address the identified gaps, specifically: - Formalize the delegation of responsibilities to GPC for CFCL IT Written Rules maintenance through SDS, if required. - Document the rationale of CFCL IT Written Rules scope (1LoD) in relation to DBAG Written Rules DB (in line with section 4.2.6 of the *Written Rule Framework Guideline*) - Describe a CFCL IT review and approval process to adopt DBG procedures, including adoption criteria, tailoring to add CFCL IT-specific requirements and CFCL IT Written Rule owner annual review - Formalize the prioritization of Group documents over individual/ local documents to achieve synchronization across DBG (in line with section 4.2.6 of the *Written Rule Framework Guideline*) - Ensure CFCL IT 1LoD procedures are aligned with 2LoD ICT Risk Management documents (e.g., *ICT Risk Guidelines*). ▪ Conduct a comprehensive review and cleanup of the "CFCL IT Handbook" (Clearstream IT Written Rules Repository) following the updated CFCL IT Written Rules Procedure (1LoD), especially: - Ensure the CFCL IT Written Rules set's completeness and accuracy, to include all CFCL IT-required documents aligned with applicable *ICT Risk Guidelines* and update or decommission outdated documentation - Maintain CFCL IT Handbook as the central register of all CFCL IT Written Rules (adopted and own) including adoption dates, ownership, roles and responsibilities tailored to CFCL, and review cycles to support transparency, governance, and ongoing compliance. ▪ *Clearstream IT Resilience Management procedure*: - Review and confirm the need to maintain a standalone *Clearstream IT Resilience Management Procedure* given its structural duplication of DBAG's. Alternatively, in line with the updated *CFCL IT Written Rules*

	Procedure and in the absence of CFCL-specific requirements, consider formally adopting the DBAG procedure and decommissioning the CFCL version to avoid redundancy and maintenance overhead - If required, update the standalone *Clearstream IT Resilience Management Procedure* regarding the reporting channel for KPI and status updates - Align with GPC to define and document roles and responsibilities for *IT Resilience Procedure* operationalization. Alternatively, consider performing CFCL IT Assets resilience testing internally within CFCL, or establishing an outsourcing arrangement with the DBAG Written Rule owner (IRT).
Management response	CFS IT (ZJL) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	CFS IT (ZJL)
Target date	December 15, 2026

Severity rating	**S2**
Finding number	2025-039_F03
Finding related to	Control environment, control design and control operating effectiveness
Title	Deficiencies in CFCL IT governance and oversight framework
Description of finding	Internal Audit (IA) review of CFCL IT's governance principles, oversight, and reporting mechanisms identified several gaps that may undermine CFCL's ability to demonstrate effective control over IT risks and compliance with regulatory expectations: ▪ <u>No Centralized Governance Documentation</u> - No central repository defining internal CFCL IT roles/responsibilities. - Key oversight roles e.g., CFCL Change Manager were described as "constantly evolving" without formal documentation. - The Information Security (IS) specialist with a CFCL contract had a restricted scope to the CFS IT Product Line under the Technical Information Security Officer (TISO) remit, leading to ambiguity over IS subject matter responsibility at CFCL legal entity-level. - All CFCL IT-related SDSs were assigned to a single Business Owner (BO) under the Service Delivery Manager (SDM) remit rather than distributed based on domain-specific expertise. ▪ <u>No Legal Entity-Level Reporting</u> - No dedicated legal entity-level reporting (e.g., Owning/Using IS; incident; change management) demonstrating CFCL's ICT controls. - CFCL BO oversight was limited to reviewing granular service delivery KPIs. This did not constitute a comprehensive oversight framework. ▪ <u>Gaps in IT Product Line and Support Group Reporting</u> - CFCL IT assets spread across multiple product lines/support groups. - Deficiencies in reporting mechanisms e.g., the Digital Security Committee (DSC), DBAG IT Governance Committee, and Clearstream Information Security Committee (CISC): a) <u>Digital Security Committee (DSC)</u> • No IFS TISO deliverables to evidence continuous monitoring of the full IS DSC KPIs. • IFS TISO, responsible for the IFS Product Line, stated not using the DSC reports due to data quality/non real-time issues, with unclear escalation of reporting issues to Group Security. • IFS TISO was using an internal "CFS IS Dashboard" for their oversight function. However, no formal documentation or tracker existed to monitor remediation progress ("path to green") for overdue security metrics. • Also, several critical controls (e.g., PAM, Access Control, SIEM, Malware Defenses) were not in TISO's monitoring scope. b) <u>DBAG IT Governance Committee</u> • CFCL lacked direct representation: oversight was delegated to GPC without clear evidence of effective information cascading to CFCL management. • CFCL-specific KPI reporting was missing in early 2025 and only initiated post-IA intervention. c) <u>Clearstream Information Security Committee (CISC)</u> • CFCL representatives (e.g., IFS TISO, BO, CIO) were not involved in 2025 CISC meetings.

- Inability to demonstrate the 2024 Post Trade IT restructuring with the CISC reporting. E.g., the CISC slides offered limited legal-entity level reporting, mainly covering SDS finalization. Also, the split by business segment (CFS/CSS) and product line-level visibility were missing. As such, the current CISC structure did not clearly assign ownership, responsibility and accountability to either the relevant TISO (e.g., IFS TISO) or business segment Heads of units.
- Missing visibility of the Product line Vulnerability Assessment Coordinator (VAC)'s involvement and key deliverables within the CISC reporting (further details are in *Appendix*).
- Since 2024, CFCL lacked KPI reporting on IT Asset & Configuration Management (reporting only started March 2025). The gap was not flagged in prior CISC sessions for CFCL management, and the SDS was still not live during fieldwork.
- Some IFS assets were mapped under the "IT IFS" support group in the CMS extract, but this classification was missing in the April 2025 PAM Coverage report. The Identity Access Management team (ICA), responsible for the Privileged Accounts Inventory, did not provide clarification. Also, CISC reporting currently only covered AST and SET support groups, leaving the IT IFS group's coverage unclear.
- Incomplete monitoring and reporting of the Post Trade IT assets onboarding to various DBG security tools, including but not limited to Security Information and Event Management (SIEM), Database Activity Monitoring (DAM), vulnerability scanners and CyberArk (further details are in *Appendix*).
- Exclusion of CFCL from the risk register (AID430) due to an automated workflow triggered by a legal entity name change in April 2024 (further details are in *Appendix*).

▪ <u>Deficiencies in CFCL IT Strategy KPI Monitoring</u>

CFCL's IT Strategy KPI monitoring was conducted jointly with GPC under a harmonized governance model across Clearstream entities (CBL, CEU, CS). No intragroup SDS existed between CFCL and GPC, and no other document clarified the governance model, while CFCL retained full responsibility and accountability. The Q1 2025 review identified several reporting gaps in this setup:

- The revised "CFCL IT Strategy Process" manual, although it had CFCL CIO's final sign-off, lacked evidence of CFCL's initial involvement as creator or reviewer. Instead, the document was created and reviewed by CBL and CEU. Also, the role of "IT Governance Specialist", tasked with implementing the strategy (e.g., KPI collection, monitoring, alignment), was not a CFCL job title. This designation was currently assigned to CEU and CS legal entity representatives under GPC. Overall, no SDS formalized the task delegation to GPC or CEU and no document clarified how the model worked if not through formal delegation. This could undermine CFCL's accountability and ownership.
- KPI milestones did not reflect CFCL's actual risk landscape e.g., non-CFCL applications were included (CMAX [AID034]) while CFCL-owned assets (FCBS [AID2010]) were missing.
- In all instances reviewed, the collection of Q1 2025 CFCL IT Strategy KPIs was conducted by CEU rather than CFCL.
- Lack of evidence of CFCL's active review or approval of KPI reports before final submission to CFCL CIO.

▪ <u>Weaknesses in CFCL Change Management Oversight</u>

- The CFCL Change Manager was not involved in the CFCL IT Strategy KPI monitoring/reporting process in Q1 2025, while a CS representative was

	incorrectly listed as the release delivery KPIs SPOC. The CS SPOC lacked engagement in the Service Acceptance Certificate (SAC) sign-off process, against the SME role expectations, which include active contribution to KPI implementation and tracking. - No documented written rules to evidence the IT change management oversight process. - For 2 randomly selected CFCL releases, no change management oversight evidence was provided. The CFCL Change Manager claimed to review insourcer's SACs and Business Acceptance Test (BAT)s, but this overlapped with BO KPI monitoring under the SDS (MA-002366-2022). There was also no active IT Change Manager involvement in the SAC/BAT execution process and no further supporting oversight evidence (e.g., SAC/BAT reviews, release trackers, test validations) was provided. - IA was informed that a new SDS (CO81459) replaced the previous one effective December 1, 2024, with new KPIs only focused on Staff Availability, omitting IT change management oversight KPIs.
Root cause	Inadequate controls
Risk	Deficiencies in CFCL IT governance and oversight framework can result in fragmented accountability due to unclear organizational structure and absence of formally defined roles and responsibilities. Also, the lack of dedicated legal entity reporting on the oversight of ICT risks might undermine CFCL's ability to exercise effective control over outsourced IT functions. Overall, this represents a material gap in internal and external provisions and could lead to minor financial loss and potential breach of regulatory requirements.
Criteria	▪ CSSF Circular 22/806 ▪ CSSF Circular 12/552 ▪ *ICT Risk Management Policy V1.0* ▪ *Outsourcing & Third Party Risk Policy* ▪ *DBG TISO Role Description V10.2* ▪ *CPMO Governance Guideline V11.0* ▪ *DBG GS IRM Guideline V1.4* ▪ *DORA ICT Risk Management Policy V1.0* ▪ *DBG GS Penetration Test Guideline V2.0* ▪ *Clearstream SDLC Testing and Acceptance Procedure V4.1*
Relevant entity	CFCL
Recommendation number	2025-039_F03-A01
Recommendation	▪ Review and update required 1LoD CFCL IT governance roles and responsibilities (e.g., IT Written Rules maintenance, IT Resilience Management, Cloud officer, IT Change Management, IT Strategy, Information Security Subject Matter expert). ▪ Reallocate SDS responsibilities based on domain expertise or establish a process to foster collaboration between SDM and technical experts (e.g., CFCL IS Specialists) for SDS review/drafting. ▪ Formalize the IFS TISO's oversight responsibilities and deliverables, including maintaining a centralized tracker to document all DSC KPIs and CFS IS metrics relevant to the IFS Product Line, including breached or overdue metrics, assigned remediation actions and responsible parties and Target dates and progress updates ("path to green"). Escalate and follow up on anomalies (e.g., missing or inaccurate data) to DBG insourcer (e.g., Group Security).

	▪ As the IFS Product line responsible party, together with ICA, ensure full coverage of IFS-related support by following up on missing coverage of the "IT IFS" support group in the PAM coverage report. ▪ Include CFCL IT stakeholders (e.g., CFCL Business Owner) into the DBAG IT Governance Committee and establish a documented process to cascade key take-aways. Follow up on CFCL-specific or impacted concerns. ▪ Finalize the IT Asset & Configuration Management SDS and escalate any potential blocker to CFCL management. ▪ Address identified gaps in the "CFCL IT strategy exercise", promoting adequate consideration of legal entity-specific risks within the CFCL IT Governance Framework. This can be demonstrated by: - Update the "CFCL IT Strategy process", especially 2.2 "Description of Roles & Responsibilities", to reflect CFCL IT Governance roles and the correct CFCL SPOCs as defined in 2025-039_F03-A01. Changes in this chapter must be applied throughout the document. - Review of IT Strategy deliverables should include a traceable and auditable review trail to ensure CFCL's active involvement and accountability prior to CFCL CIO's approval to address the gaps identified in the audit (e.g., documented review logs with CFCL feedback and comments, formal sign-offs including supporting artifacts from CFCL representatives). ▪ Formalize the IT Change Management oversight responsibilities and deliverables, including: - Document CFCL IT 1LoD oversight responsibilities for IT Change Management risks in line with DBG's IT Change Management Written Rules. - Maintain a centralized CFCL release oversight to monitor CFCL Owned and Impacted releases. - Release scope review/approval (e.g., release charter confirmation) - Continuous oversight controls on key IT change management deliverables (SAC, BAT, Technical Acceptance Test (TAT)) to validate content completeness and accuracy. Evidence should also be retained.
Management response	CFS IT (ZJL) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	CFS IT (ZJL)
Target date	December 15, 2026

Recommendation number	2025-039_F03-A02
Recommendation	▪ Update the Clearstream Information Security Committee (CISC) Terms of Reference (ToR) to: - highlight legal entity (i.e., CFCL IT) Information Security reporting requirements to cover both "owning" and "using" IT Assets - include review and escalation of DBG insourcer (e.g., Group Security) outsourcing performance. <u>Legal Entity Reporting</u> ▪ Review, describe and update CISC reports to: - Together with the appointed CFCL Information Security Specialists, introduce legal entity reporting to demonstrate full oversight/control on

	outsourced activities (e.g., CFCL-relevant IT infrastructure, IT Assets security and Processes [owning and using]) - Escalate anomalies to DBG insourcer (e.g., Group Security). <u>Product Line Reporting</u> ▪ Define and implement 1LoD roles and responsibilities in Post Trade for Information Security ensuring alignment with the Group-defined technical interface roles (e.g., TISO) ▪ Define and implement Post Trade IT 1LoD Information Security reporting, follow-up and escalation mechanisms, including reporting mechanisms from and to the CISC and DSC ▪ Include Product Line VACs and deliverables to address the gaps identified (further details are in *Appendix*) ▪ Review the security tool onboarding slide within CISC reporting to address the gaps identified (further details are in *Appendix*) ▪ Complete GCP Cloud Simulation Platform (AID111) APMS LE onboarding, enabling risk treatment and acknowledgement, thus addressing the gap identified (*further details are in Appendix*) ▪ Reflect Post Trade IT product perspective including all product line departments (e.g., Full PAM coverage report for the IFS Product Line) within CISC reporting.
Management response	Post Trade IT Governance (GPC) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Post Trade IT Governance (GPC)
Target date	December 15, 2026

Recommendation number	2025-039_F03-A03
Recommendation	Investigate the risk register mapping issue due to legal entity renaming and ensure CFCL is correctly reflected on VMT & Risk Register (AID430). This was adequately addressed at time of audit report issuance.
Management response	IS Risk Management (IGI) agrees with the finding and recommendation, and implemented the recommendation.
Recommendation owner	IS Risk Management (IGI)
Target date	Closed

Severity rating	**S2**
Finding number	2025-039_F04
Finding related to	Control design effectiveness
Title	Incomplete governance and oversight of CFCL cloud outsourcing arrangements
Description of finding	Internal Audit (IA) identified CFCL cloud outsourcing governance and compliance gaps, particularly regarding CFCL's use of DBG's Google Cloud Platform (GCP) (AID414), fully operated by DBAG and CS: ▪ Shared Resource Operator model without direct agreement While the MA-005463-2021 SDS governed the provision of Cloud Infrastructure Services between DBAG (supplier) and CS (customer), with both entities acting as shared resource operators, there was no direct written SLA between CFCL and the shared resource operators. This impaired CFCL's ability to demonstrate oversight and control of its cloud infrastructure. ▪ Incomplete delegation and oversight of CFCL's Cloud Officer (CO) role - Delayed Formal Delegation A shared CO function was in place within CS ("Resource operator"), covering CFCL. From January 2024, a staff member was assigned to CFCL-related activities. SDS CO213276 formalized the delegation only in May 2025 due to resource constraints. - Oversight and Reporting Deficiencies ○ Within SDS-CO213276, CO reporting was limited to the CFCL Outsourcing Governance Committee (2LoD); no direct CFCL IT (1LoD) reporting, thereby weakening CFCL operational oversight. ○ Defined KPIs were tracked ad hoc (3) and quarterly (1), undermining continuous monitoring of outsourcing arrangements. ○ Missing CFCL cloud oversight metrics (e.g., C4C SAC review, CSSF compliance, CFCL officer training records, security incidents, cloud infrastructure and data monitoring metrics).
Root cause	Inadequate controls
Risk	Incomplete governance and oversight of CFCL cloud outsourcing arrangements will lead to CFCL's inability to assess service performance, risk exposure, and compliance status resulting in ineffective monitoring of outsourced cloud services. Overall, this represents a material gap in internal and external provisions and could lead to minor financial loss and potential breach of regulatory requirements.
Criteria	▪ DORA, Article 5 ▪ CSSF Circular 22/806 on Outsourcing, as amended ▪ *DBG Cloud Center of Excellence (COE)- Cloud Operations Handbook V2.0* ▪ *DBG Cloud Usage Policy V1.5* ▪ *MM-51104 Cloud for Clearstream (C4C)- Project Charter*
Relevant entity	CFCL
Recommendation	▪ Review and formalize all outsourcing arrangements leveraging cloud infrastructure, including service level description thereof with precise quantitative and qualitative performance targets within the agreed service levels in line with CSSF Circular 22/806. ▪ Enhance CFCL 1LoD cloud governance and reporting mechanisms for adequate oversight of the complete cloud outsourcing chain.

Management response	CFS IT (ZJL) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	CFS IT (ZJL)
Target date	December 15, 2026

Severity rating	**S1**
Finding number	2025-039_F05
Finding related to	Control design effectiveness and control operating effectiveness
Title	Inadequate CFCL secure area physical access controls
Description of finding	Internal Audit (IA)'s review of a list of people with access to the CFCL secure area within the Clearstream Luxembourg premises noted inappropriate access permissions as the following control requirements were not established: ▪ Formal Access Requests: Access to CFCL/CFS perimeters and security zones not consistently requested and approved based on necessity. ▪ Access Profile Management: Access right profiles not systematically created, reviewed, or revoked when no longer required. External service personnel's access not always restricted and their access not consistently authorized and monitored. ▪ Annual Review: No evidence of annual review and documentation of physical access rights to ensure plausibility and ongoing need. European and Luxembourg regulation require institutions define and implement documented physical security measures to protect their premises, data centres and sensitive areas from unauthorized access.
Root cause	Inefficient/Inadequate Controls
Risk	Inadequate CFCL secure area physical access controls is a minor violation of internal and external provisions which could result in unauthorized access to the CFCL secure area, and could lead to minor financial loss and potential breach of regulatory requirements.
Criteria	▪ DORA Article 9, Point 4c ▪ CSSF Circular 12/552, Chapter 2, Section 6; Chapter 5, Section 5.3.3; Chapter 6, Section 6.1.3 ▪ Law of 5 April 1993 on the financial sector, Article 41 ▪ DBG *Physical Security Policy* v3.2, Chapter 2.3 ▪ DBG *Physical Security Standard* v3.2, Chapter 4.1, 4.2
Relevant entity	CFCL
Recommendation	Implement a periodic CFCL secure area access control review.
Management response	Clearstream Fund Services (MIF) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	Clearstream Fund Services (MIF)
Target date	April 30, 2026

Severity rating	**S1**
Finding number	2025-039_F06
Finding related to	Control design and control operating effectiveness
Title	Inaccurate CFCL Internal Control System (ICS) process maps and Risk Control Matrices
Description of finding	Internal Audit (IA) identified that CFCL's ICS process maps and Risk Control Matrices related to the below processes/sub-processes contained inaccurate control descriptions and requirements: ▪ "*P_CFCL_SU_8_IT Run*" / "*SP_CFCL_SU_8.1_IT Run Outsourced*" / Control "*C_CFCL_SU_8.1_Op. Effectiveness*" ▪ "*P_CFCL_SU_10_IT Governance*" / "*SP_CFCL_SU_10.2_IT Strategy Management*" / Control "*C_CFCL_SU_10.2_Op. Effectiveness*" European and Luxembourg regulations, as well as internal standards, policies and guidelines, a financial institution should maintain adequate safeguards and controls to ensure an effective internal control system.
Root cause	Human Error/ Omission
Risk	Inaccurate CFCL Internal Control System (ICS) Risk Control Matrices and process maps may expose the company to operational risk due to minor gaps in internal and external provisions.
Criteria	▪ DORA Article 5, 6 ▪ CSSF Circular 12/552, Chapter 6 ▪ DBG *Internal Control System (ICS) Policy* v6.4, Chapter 6.5 ▪ *ICT Risk Management Guideline* v1.1, Chapter 9.1
Relevant entity	CFCL
Recommendation	Update CFCL ICS process maps and Risk Control Matrices related to the IT Governance and IT Run processes to reflect the current setup.
Management response	CFS IT (ZJL) agrees with the finding and recommendation, and will implement the recommendation.
Recommendation owner	CFS IT (ZJL)
Target date	March 31, 2026

4. Finding severity definition[3]

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

[3] 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	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
	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
Business Line	Volker Henke	Head of Unit, Post-Trade IT Governance, (GPC)
	Anna Cutilli	VP, Post Trade IT Governance (GPC)
	Bishwamitra Thakur	VP, Infrastructure Development and Continuous Delivery (GNE)
	Laurence Gillet	VP, Clearstream Fund Services (MIF)
	Branislav Rajcani	Head of IS Risk Management (IGI)
Risk Management	Clemens Völkert	Chief Risk Officer DBAG
	cfclriskmgt@clearstream.com	CFCL Risk Management Inbox
Compliance	Marc Peter Klein	Group Chief Compliance Officer
	GC_Audit_Coord@deutsche-boerse.com	Group Compliance Audit Coordination
	Christian Heyne	Chief Compliance Officer CBL
	Jan Kobbach	Chief Compliance Officer CEU and CH
	Sabine Guip	Chief Compliance Officer CFCL
	cfclcompliance@clearstream.com	CFCL Compliance Coordination
ICT	Sebastian Wedeniwski	CTO, DBAG
	Christian Gorke	Chief ICT Risk Officer/CISO

	Boris Link	IT Governance, Risk and Transformation DBAG
	Hinrich Völcker	CSO DBAG
	Karthik Ramamurthy	CISO CFCL
	Jan Patrick Drehwald	CISO CEU
	Nejib Zaouali	CISO CBL
Internal Audit	Andrea Bracht	Group Audit
	Dietmar Hinkel	Group IT Audit
Audit Manager	Bertrand Thiault	Internal Audit CFCL
Auditors	Fabrice Moreira	Internal Audit CFCL
	Urvashi Emrith	Internal Audit CFCL

6. Appendix

- **Missing visibility of the Product line Vulnerability Assessment Coordinator (VAC)'s involvement and key deliverables within the CISC reporting.**

  Penetration testing of CFCL IT assets is fully outsourced to Group Security. Also at product line level, the designated VAC is responsible for coordinating penetration test planning and execution, validating scope, and receiving and reviewing penetration test reports within Penetration Testing Request Management System (PeTeR). VACs are also responsible for initiating re-tests for previously identified high and critical marked as "Fix Claimed" within VMT and escalating potential critical vulnerabilities to CERT.

  IA identified the following gaps:
  - No "Fix Claimed" status vulnerabilities and re-testing tracking. E.g., the FCBS (AID2010) 2024 penetration test report (PETER-11379) issued in January 2025 identified five vulnerabilities, including one critical. The latter was marked as "Fix Claimed" with a due date of 04 March 2025 (VMT ticket PT-7237). However, the VMT ticket remained overdue at the time of the audit, indicating that the required re-test had not been performed. This was not flagged in the Clearstream Information Security Committee (CISC) material, which was only showing "Exception Claimed" i.e., Vulnerability not fixed, and formally risk accepted.
  - No reporting of potential critical vulnerabilities escalated to CERT by VAC.
  - No review of penetration test reports, including scope, limitations, and vulnerability overview.
  - Potential overlap and inconsistency with the Digital Security Committee (DSC) reporting: Both DSC and CISC reported on completed pen tests by IT Product Line and overdue vulnerabilities. However, a new KPI was added to the DSC slide deck from August 2025 to monitor IT assets with a valid "Compliant" penetration test. This new KPI was not added to the CISC reporting, leading to oversight gaps.

- **Incomplete monitoring and reporting of the onboarding of Post Trade IT assets to various DBG security tools including but not limited to Security Information and Event Management (SIEM), Database Activity Monitoring (DAM), vulnerability scanners and CyberArk as detailed below:**
  - IFS Product line (Environment: Production) was initially omitted from the CISC reporting out of oversight. GPC remediated the gap during audit fieldwork.
  - Current CISC reporting's onboarding classifications for both production and simulation environments showed only as "Onboarded" or "To-Onboard". However, IA identified that "Onboarded" applications also included accepted deviations i.e., "Exceptions", which were not explicitly mentioned in the slides resulting in inaccurate management reporting.
  - Instances identified whereby, in simulation environment, CFCL applications (owned/used) were not onboarded to DAM. While this was categorized as "Exception Covered" with a VMT risk entry, IA identified Monitoring & Application Support (ZEV) only raised a single DAM exception ticket (EMP-92017) (approved by Cloud Services [CNS] as CBL GCP Cloud Simulation Platform [AID111] asset owner) to exempt all Post Trade IT assets, including CFCL assets. Also, the risk was only accepted by Clearstream Services, as owning and using legal entity. Also, IA's spot check review of onerandomly selected server (ID:1177537- OBLADE12) impacting the IFS, AST and GSF product lines, identified no linkage to AID111 on CMS. Also, the IT asset owner was recorded as PaaS OS& VM (ZEX) instead of CNS. Ultimately, the above-mentioned assets were also used by different Clearstream legal entities e.g., CFCL, CBL, CEU, all currently excluded from the risk acknowledgement process.
  - CFCL used and owned applications utilized the Rapid7 compliance scanning tool. Due to Rapid7 weaknesses, the insourcer (Group Security-GS) triggered an ad hoc risk request:
    - IA identified the ISRM ticket (158916) in VMT & Risk Register (AID430) was not assigned to CFCL (an impacted legal entity) to trigger the risk acknowledgement process.
    - IFS TISO confirmed not having the legal entity view within AID430and GPC not being responsible for investigating this gap.
    - IA's inquiries of IS Risk Management (IGI) identified that when GS assigned the risk to CFCL, the risk register workflow automatically transitioned the risk to "LE removed from AID" resulting in excluding CFCL.

- IGI further clarified that the root cause was the renaming of the legal entity from “CFCL – Clearstream Fund Centre Luxembourg” to “CFCL – Clearstream Fund Centre S.A” in the tool in April 2024. The reconciliation process failed to correctly map the risks to the updated legal entity.
- As a consequence, certain IS risks were transitioned to the status “LE removed from AID” as per the workflow design. This resulted in incomplete visualization and acknowledgement of CFCL’s IS risks either as an owning or affected legal entity within the risk register. This was adequately addressed during the audit.