**L2 ~~or L3~~ or tests name:** IT-Operation Management

**Legal entities in scope:** DBAG, ExR, EFAG, ECAG, CBF, CBL, LuxCSD, CI, CS and CFCL

|  |
| --- |
| IT-Operations Governance |

**[+ including AU-121-11-CSDR CSDR IT-Operation Management]**

**Test(s) according to RCA:**

(TP1) Inquire with relevant personnel about the structure arranged in the context of governance around the IT Operations Area with focus on roles defined, responsibilities allocated and tasks to be performed in the context of monitoring and reporting regarding IT Operations per LE.

(TP2) Validate via a representative sample of Policies and Procedures, whether DORA Principles have been identified and translated into the available governance arrangements.

(TP3) Test the Future Notes identified as relevant to the respective L2s.

(TP4) During fieldwork, overall KPI reporting (Incl. Performance Monitoring, applicable) on in-scope processes will be assessed for completeness and appropriateness, especially if the reporting encompasses all product teams inside DBG. Also, assess why CFCL is not included in the IT Governance Committee KPIs.

(TP5) Understand the governance of IT Operations-related findings management, especially for non-severe findings (F1/F2 rated) and evaluate the monitoring controls pertaining to implementation of remediation actions and closure tracking of such findings.

(TP6) IA to check and validate with relevant personnel about the 2nd line (Risk/Compliance) activities in IT Operations area performed in the year under review

**Audit procedures/source:**

* Information directly requested from auditee (via e-mail or call) or extracted from provided documentation during preparation phase.

**Conclusion:**

Ok, no exception identified

Internal audit (YW, YG) has performed the following Audit procedures:

**-------------------------------------------------------**

**Summary of work done:**

**-------------------------------------------------------**

|  |  |  |
| --- | --- | --- |
| **AP** | **Work done** | **Result** |
| **TP1** | IA had a meeting on 11 February 2025 with DBAG IT Governance Boris Link supported by Bartosz B. and Sean McTaggart to discuss the test point. The IT Governance Policy is in place since 24 May 2024 and covered in section “2.7. IT Governance Roles & Responsibilities” all elements of IT Governance.  DBAG IT Governance serves the CIO and CTO of LEs (except Clearstream) that have outsourced IT services to DBAG. The monthly reporting is to DBG CIO/COO. IA discussed with Boris Link (HoD, IT Governance) the IT related KPIs on group level and was informed there is an IT Governance Committee that presents an aggregated report on decentralised IT product reporting IT Governance Committee since September 2023 on a monthly basis and minutes of the meeting were prepared for takeaways and next actions.  Evidence: IT Governance Committee slides ([link](https://deutscheboerse.sharepoint.com/:f:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/IT%20Governance%20Committee?csf=1&web=1&e=m4rZPX))  IA had a meeting on 21 February 2025 with Clearstream IT Governance - Volker Henke and Hans-Joachim Fitzke to discuss the test point. Please see comments/updates regarding the notes:   * Post Trade IT (PTIT) Governance (U) is serving the CIO’s and CTO’s of PTIT. Key activities include Audit Management (2Lod – Risk/Compliance, IA. External), Regulatory reporting, ICS, IT Strategy etc. ([structure](https://deutscheboerse.sharepoint.com/:p:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/Post%20Trade%20IT%20Governance%202024.pptx?d=w55fcb3f3a743415a96d54c824b4c692d&csf=1&web=1&e=ROHI40)) * Caters to LEs CBF/CH/CBL/CS/LuxCSD/CFCL. CI is not in scope but sometimes supported in good will as colleague. LuxCSD is not supported directly by the unit, but Stephane Deschamps (CS) is supported who is acting as CTO of LuxCSD via SDS. * The monthly IT Board Member Update Meeting formally started in October 2023 and is supported by Minutes of the Meeting (MoM). * KPI reporting was performed. Basis IA findings from 2023, a new IT Strategy was prepared for LEs (CBF/CBL/LuxCSD/CFCL) and approved end of 2024. Accordingly, IT Strategy implementation is ongoing in Q1. KPI Report from Q1 regarding new IT Strategy will be prepared/published in Q2. * DORA topics to be discussed with DORA@Clearstream Project Managers – Dirk Hofmann, Karsten Schulze. Meeting to be planned in the coming week. Also, include discussion topic - DORA Incident Classification and Regulatory Reporting. More details in TP2.   Evidence:   * Monthly IT Governance – IT Board Member update meetings from July, September, November 2024 and for January 2025. Also, share respective MoM. ([link](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/Clearstream%20IT%20Governance%20(Post%20Trade%20IT)/IT%20BMUs.zip?csf=1&web=1&e=cGgqh0)) * New IT Strategy (2024) for CBF and CFCL – and approvals. ([link](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/Clearstream%20IT%20Governance%20(Post%20Trade%20IT)/IT%20Strategy.zip?csf=1&web=1&e=cGDp7P)) * Structure: Post Trade IT Governance 2024.pptx ([link](https://deutscheboerse.sharepoint.com/:p:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/Post%20Trade%20IT%20Governance%202024.pptx?d=w55fcb3f3a743415a96d54c824b4c692d&csf=1&web=1&e=7E2goE))   => OK  In the context of monitoring and reporting regarding IT Operations, the DBAG and Clearstream Governance bodies inform the DBG CIO/COO with group-wide status. The information is mainly received from Boris Link for DBAG and its outsourced entities and from Volker Riebesell for all Clearstream entities (incl. CFCL).  IT Strategy (S) was not in direct scope of this audit. In IT Operations – related to ‘Governance’ fieldwork, we assessed the need to include IT Strategy as quarterly IT reporting (Business update Technology) is performed at DBG level by Christoph B. (CIO/COO) to the Technology Committee of the Supervisory Board.  As discussed with Alexander Kuebler, IT Strategy, Culture and PMI (S), IA requested from 2024, the 4 Quarterly reports (incl. business updates Technology and supported by the subset - deep dive presentations on various IT programs/projects. Note: the documents are labelled ‘confidential’([link](https://deutscheboerse.sharepoint.com/:f:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/2024%20SVB%20Technology%20Committee%20Documents?csf=1&web=1&e=xBnGPL)).  No exceptions were noted for 2024.  => OK  Following items are for management attention from January 2025 [slides](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/DORA%20slides/20250131_DORA%20Implementation%20SteerCo.pdf?csf=1&web=1&e=xGIUoR)    => OK | Ok, no exception identified |
| **TP2** | From Boris L.: A massive source of basic info is of course DBG intranet announcement and microsite:  <https://deutscheboerse.sharepoint.com/SitePages/DORA--the-Digital-Operational-Resilience-Act-applies.aspx>  <https://deutscheboerse.sharepoint.com/sites/IN-ChiefRiskOfficer/SitePages/DORA.aspx>  Regarding Definition of Operations, see breakdown of our DORA/procedure roll-out in the ICT finding CAP (2024-063\_F01). Procedure roll-out includes governance arrangements, hence the long timelines.  DORA has done new guidelines and CIF identification in dedicated workstreams, but outside of GRT. Certain parts of IT Operations (as defined by the Guideline) 1st Line “Governance Arrangements” is only planned for 2026.  With DORA effective January 2025, IT GRT are already changing/expanding the central governance remit of IT GRT in 2025 as follows:   * Establishing Cloud Governance: A dedicated team will be established through the respective Hyperion workstream and join IT GRT for BAU * Establishing DORA Governance: As part of the TOM definition for digital operational resilience a dedicated team will take care of resilience and incident aspects (details in definition) * Expanding the core process governance to other IT operations aspects, piloting with patch management (extension of finding 2023-027-F01-A02) * the three items above, respective 1st line procedures are planned to be created (through 2025 – S3 CAP 2024-063\_F01) valid across IT teams, and required controls/topics will be governed and reported accordingly (through existing ITGC structure/approach)   Evidence:  Last 3 DORA Program Monthly decks (2024: Nov, Dec. 2025: Jan) ([link](https://deutscheboerse.sharepoint.com/:f:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/DORA%20slides?csf=1&web=1&e=MXWic3))  Mandatory DORA training rolled out to all Executives – status completed.  => OK  Current progress status:    Individual statuses for DBAG (green), T&C (amber) and Post Trade (amber) – [Refer slides 18-20](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/DORA%20slides/20250131_DORA%20Implementation%20SteerCo.pdf?csf=1&web=1&e=s83iJI)  => OK  From January 2025 – following are key achievements from high priority deliverables    => OK  From December2024:  DORA meetings with BaFin held on 13 December. Productive exchange on ICT risk management and third-party risk management.  DORA @CIO – Project focus:  Module 4 – Digital Resilience Coordination & Testing   * Digital Resilience comparison current posture vs. DORA requirements completed. Overall ~65% ready * Focus topics identified and planning for 2025 has started, esp. creation of supporting docs and support by new IT Resilience Governance Team   Module 5 – ICT Incident Mgmt. & Reporting (High priority Topic 2024)   * ICT Incident Management has been designed according to the DORA requirements and codified in a new procedure * The underlying ICT incident processes will be operationally ready by January 17th, 2025. Tabletop exercises will be performed to provide awareness and training end-to-end. The preparation and execution of test exercises with LE, IT and Business (SPOCS) is in progress.   Both procedures for IT Incident & Resilience completed and going through final Alfresco approvals.  => OK  IA had a meeting on 26 February 2025 with Clearstream IT Governance - Volker Henke and Hans-Joachim Fitzke and Clearstream DORA Project Managers Dirk Hoffman and Karsten Schulze to discuss the test point. Please see comments/updates regarding the notes taken during the meeting.  Evidence:   * 20250221\_DORA@Clearstream SteerCo [slides](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/Clearstream%20IT%20Governance%20(Post%20Trade%20IT)/20250221_DORA@Clearstream%20SteerCo_v1.1.pdf?csf=1&web=1&e=g8DZAG) * Clearstream CIFs and CIF relevant applications ([link](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/Clearstream%20IT%20Governance%20(Post%20Trade%20IT)/Clearstream%20CIFs%20and%20CIF%20relevant%20applications.xlsx?d=w1438bc8ee9be40ad8fe4d0930419d72c&csf=1&web=1&e=vD80g4)) for CBF, CBL, LuxCSD and CFCL. * Completion of Mandatory DORA training for Executives ([email](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/Clearstream%20IT%20Governance%20(Post%20Trade%20IT)/FW%20Board%20training%20attendance%20-%2021%20November.msg?csf=1&web=1&e=47j4Mb)) * Meeting with CSSF on DORA progress held on 23 January 2025 ([link](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/Clearstream%20IT%20Governance%20(Post%20Trade%20IT)/20250123_CSSF_WS_DORA_1.0.pdf?csf=1&web=1&e=YNIrSE))   => OK  On January 23, 2025, a CBL&LuxCSD DORA workshop was held with CSSF&BCL. The workshop presented the DORA readiness status and the plan for the remaining activities in 2025, receiving positive feedback. CSSF&BCL expressed interest in key work products. Following the European Commission's publication, CSSF supported CBL&LuxCSD view that regulated financial services are not considered ICT services. ([source](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/DORA%20slides/20250131_DORA%20Implementation%20SteerCo.pdf?csf=1&web=1&e=idwLxl))  For CC3 3 ICT Risk Methodology & Framework and CC6 6 Information Register on Third Parties, the group program status meets the anticipated ambition level with two minor deviations. This was informed to CSSF and scheduled for completion by latest end of March. This would be verified by CSSF in its tentative schedule meeting on 11 April 2025.  => OK  IA reviewed all documentation provided and discussed with Dirk Hoffman and Karsten Schulze (Post-Trade - CSS DORA project main contacts), and DBAG DORA slides from Boris Link/ Andreas Reilich (DORA Program Managers), and reached to the below understanding/conclusion:  DBG DORA Activities Timeline    CSS Specific:    Organization  DBG Program Structure    Specific LEs Projects Structure  DBG    Post-Trade – CSS      T&C    In addition, an alignment project within the Trading & Clearing division and Clearstream was set up in 2024 to ensure compliance by the legal entities.    => OK  DORA Program/Projects Progress  22 entities across DBG are in scope of DORA:    In 2023 a DORA analysis project was finalized that end up with the identification/definition of 17 areas of development clusters (AoD) to drive solution-oriented implementation planning (*note: AoD were updated and prioritization in 2024 as you can see below*):   * + 2023:     Also, solution leads per area of development were identified to coordinate implementation planning:     * + 2024:     DBAG DORA Program Sponsor Meeting  A DORA deep dive gap analysis on ECAG, ECC, and CBF was conducted between February and March 2024 by Severn. Other Legal Entities were invited to participate in the workshops as listeners. Colleagues from DBAG were involved when necessary:    More than 360 gaps were identified (on different levels of granularity). They were aggregated in 163 deliverables, mapped to 18 capability clusters and 7 overarching modules developed by the DBAG project:    In addition, a Gap analysis at CBL/CFCL was also performed by Deloitte to consider Luxembourg specifics in July 2024.  Priority clusters were defined, and, currently, working groups are addressing the respective gaps, responsibilities were assigned, and solutions aligned between the legal entities.    PwC raised the following concern on 09/08 Regular Meeting PwC / Group IT Audit: “*Meetings have taken place with project leads from LEs/clusters, key output (the work product matrix) has now been received but still raises a lot of questions: not filled out correctly, missing LE view. An issue is that they expect DBAG to define CIF, but LE had to start doing this on their own as DBAG is taking so long. Their concern is late due dates for most items in the plan, and inconsistencies in dependencies.”*  However, IA after reviewing the below deliverables (work product matrix, steercos decks) do not share the same view. For example, column Q – W in the work product matrix define the lead for the different work products to be created.  In April the different projects were organized by segments (DBAG, T&C, Post Trade), and in June assignment of activities/responsibilities started: work product matrix (define the lead for the different work products)  DBAG have been monitoring the progress via steerco (e.g. 21.08, 19.07) including all the different segments (DBAG, T&C, Post Trade).  Post-Trade - CSS also have been monitoring their own segment progress via steerco (e.g. 20/08 -> slide 6-10 show the detail progress for the 18 clusters and the overall overview in slide 2).  => OK | Ok, no exception identified |
| **TP3** | None identified for this L2  => OK | Ok, no exception identified |
| **TP4** | From Boris, Current KPI-reporting is based on SDS with LEs. Additional data is shown in ITGC, and further developments were planned in 2025 due to DORA priorities, including LE views. Current split is based on product groups aligned to LEs.  IT Governance metrics (KPIs) follow the rules described in the IT Governance Policy section 2.4, and are defined and reported in the IT Governance Committee:    The data sourcing and tool-based management reporting of IT Governance metrics (KPIs) was deprioritised for the moment; however, this is not a mandatory aspect:    As reported by 2 LoD over IT and IS metrics, all metrics are green, safely above the breach thresholds.  => OK  IA also covered certain aspects of Incident Management-related process documentation (non-cyber related) to validate whether it is in line with the DORA requirements (including timeliness and criticality).  In this context, IA discussed with Sean McTaggart (evidence received via [email](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/FW_%202025-001_IT%20Operation%20Management_Incident%20Management.msg?csf=1&web=1&e=kg9v1y)) -  (1) to check and confirm if the DORA related requirements have already been embedded into the process documentation  (2) that the ICT Incident management framework has been updated to reflect requirements from DORA.  (3) If yes, are those applicable centrally to all IT product teams across DBG and is documentation available within the IT Written Rules repository.  The procedure is published in the [Written Rules repository](https://deutscheboerse.sharepoint.com/sites/WrittenRulesDatabase/Shared%20Documents/Forms/AllItems.aspx).  Direct link to the procedure [ICT Incident Management Procedure.pdf](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/ICT%20Incident%20Management%20Procedure.pdf?csf=1&web=1&e=R298Ya)  Updated [ICT Incident Emergency Procedure\_v 2.9\_DORA-published.pdf](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/ICT%20Incident%20Emergency%20Procedure_v%202.9_DORA-published.pdf?csf=1&web=1&e=OPxYCA)  Updated Template [Incident Statement v1.9 after DORA RTS JULY 24 adjusted.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/Template%20Incident%20Statement%20v1.9%20after%20DORA%20RTS%20JULY%2024%20adjusted.docx?d=w577ee8d5f0dc44ce83e4e80e1646b6cb&csf=1&web=1&e=xUDurs)  For more details, refer the working papers of [WP - IT Operations Management.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Management/WP%20-%20IT%20Operations%20Management.docx?d=w34e374e66c104c66b0251edfe98c3ac2&csf=1&web=1&e=N3vHT8) and [WP - Cloud operations.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/Cloud%20operations/WP%20-%20Cloud%20operations.docx?d=w9c5547f175d04680946a67260e5871b6&csf=1&web=1&e=EbLeLf) regarding this point.  Further, IA discussed how DBG Incident Classification alert-levels are mapped to the DORA Incident Classification and Regulatory Reporting with Boris L./Sean M. As per definition, DBG Incident Management classification based on colour-schema is as shown in snapshot below -    The Incident Management template holds the DORA Criteria & Thresholds:  Every Incident is quantitatively validated across the criteria to be sure if it must be reported in line with DORA requirements.  Ein Bild, das Text, Screenshot, Zahl, Schrift enthält.  Automatisch generierte Beschreibung    [ICT Incident Management Procedure.pdf](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/ICT%20Incident%20Management%20Procedure.pdf?csf=1&web=1&e=R298Ya)  IA in parallel validated the using and awareness of this Incident Management Classification with Clearstream colleagues Laurent K. and Anna C. A meeting planned on 4 March 2025 indicated that Clearstream entities are aligned and using the new [template](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/Template%20Incident%20Statement%20v1.9%20after%20DORA%20RTS%20JULY%2024%20adjusted.docx?d=w577ee8d5f0dc44ce83e4e80e1646b6cb&csf=1&web=1&e=xUDurs) to indicate DORA relevance and act.  => OK  Regulatory reporting: From [ICT Incident Management Procedure.pdf](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/ICT%20Incident%20Management%20Procedure.pdf?csf=1&web=1&e=R298Ya) page 25 section 5.5.2    => OK  Upon ask, it was brought to IA knowledge by Sean McTaggart (see [email](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/FW_%202025-001_IT%20Operation%20Management_Incident%20Management.msg?csf=1&web=1&e=4VgyLk)); 1 incident has been reported relevant in 2025 as part of the ICT Incident Management process. Incident Statement is [attached](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/20250203_Eurex%20T7%20Partition%208%20%26%2010%20unavailability_Incident%20Statement_not%20distributed.pdf?csf=1&web=1&e=f1bpMJ). Incident was regarding - 20250203\_Eurex T7 Partition 8 & 10 unavailability.  “A single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity”  The same procedure requirements (Page 17/18 of [Procedure](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/ICT%20Incident%20Management%20Procedure.pdf?csf=1&web=1&e=oWN6X0)) apply to anything falling into this definition, regardless of hosting.      => OK  **TS - T2S Incident:**  On 27 February 2025, IA was informed that T2S is currently facing an incident impacting Application-to-Application (A2A) outbound and inbound communication and T2 is facing an incident impacting processing of the Application-to-Application (A2A) transactions and User-to-Application (U2A) access. The incident management has classified the incidents as ‘yellow. Later, IMM summary from BDM IMMs indicates downgrade from Yellow to Purple to Blue.  On 5 March, IA discussed with Clearstream colleagues - Stephane Deschamps, Damian O'Connell, Laurent Kaiser, Didier Lenges, Nathalie Rouilleaux, Nathalie Adam, Lisa Holland on proper documented risk assessment of the incident, incident classification levels as this has had adverse international media outlets with Clearstream explicitly named over multiple days, Regulatory Communication, communication to DBG Board level and Internal Minutes ([link to email comms](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/TS%20-%20T2S%20Incident/TST2S%20Incident%20Communication.zip?csf=1&web=1&e=i4AFKh)). At the time of audit fieldwork, it was noted that the incident was handled as per DBG process, Incident remediation measures were ongoing, and the Incident Management Statement would be published/circulated in next days. Problem Report is linked [here](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/TS%20-%20T2S%20Incident/WG_%20TS_T2S%20Incident%20.msg?csf=1&web=1&e=UrzPOU). Key takeaway from the meeting:   * This is not considered an IT incident because it had “only business impact” * It was only classified as yellow, therefore not reported to DBG Board (to be involved from orange and above) * It was communicated to Compliance and CISOs of the affected LEs. * It was not reported under DORA as T2 and T2S were explicitly excluded from DORA. IA checked the exact exemption. Ok. * It was however reported to regulators under the CSDR requirements. * Near miss – actual impact was limited as Clearstream was able to catch up with the backlog overnight and only delayed opening on the next morning by 20 minutes.   image  [T2: Incident and cut-off extension](https://www.clearstream.com/clearstream-en/newsroom/ops250227-2-4308678)  [T2S: Settlement feed interrupted - Update](https://www.clearstream.com/clearstream-en/newsroom/ops250227-3-4308816)  [T2S: Settlement feed interrupted](https://www.clearstream.com/clearstream-en/newsroom/ops250227-4308370)  For hint: [IA Internal communication](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/TS%20-%20T2S%20Incident/RE_%20IT%20Ops_%20Incident%20mgt.msg?csf=1&web=1&e=3QsLja)  => OK | Ok, no exception identified |
| **TP5** | IA had a meeting on 03 March 2025 with DBAG IT Governance Boris Link supported by Bartosz B. and Sean McTaggart to discuss the test point.  Findings management is agnostic of any specific IT-area or rating. The ITAFM Unit covers the CIO/COO division. Based on review of findings from External Audits, no findings relevant for this audit and the applicable L2 processes in scope were identified. During the review, IA observed that some of the IT findings are directly mapped to Boris Link who is identified as the ‘FAR Responsible Finding Owner’. IA asked to understand the IT-related findings management and governance processes of non-severe findings (F1/F2 rated) to evaluate the effectiveness of monitoring of implementation steps and subsequent closure.  Internal Audit (IA) performed a walkthrough of the process regarding IT related audit findings management together with Boris Link (Head of IT Governance & Audit Management) and Bartosz Baczynski (Head of IT Audit & Findings Management) to validate a process regarding the management of IT related audit findings [internal (if similarly to the external findings) and external IT findings] is established and noted that the described process is linked to the FAR Tool process, which is used group-wide, allowing the tracking and follow-up of the findings, with measures / timelines set. IA furthermore inquired about the non-severe findings (rated as F1/F2) which we identified as mapped to Boris Link as ‘FAR Responsible Finding owner’ and were informed the following:  Additionally, it was mentioned, that in case there are external findings, the solution coordination team (SCT) in FAR for IT is ITAFM. All external IT findings are assigned to that SCT and then distributed/assigned to the finding owners.  Furthermore, an ongoing feasibility check is undertaken by FPM and PWC together to fine tune the external findings assignment process regarding identification of correct owner from different coordinator groups (LE specific, Functional, etc). This if agreed as working model, will then be incorporated into the procedure through annual revision tentatively planned for Q2 2025 (May/June).  Regarding monitoring controls pertaining to implementation of remediation actions and closure tracking of such findings a monthly meeting is planned with IT Product Lines/ Finding owners and statuses are discussed. Reporting / ITGC forum – [Dec’24](https://deutscheboerse.sharepoint.com/:p:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/IT%20Audit%20Forum%20Dec%202024.pptx?d=w65e4a738c2574033b217ebe949af9458&csf=1&web=1&e=fQ9knP), [Jan’25](https://deutscheboerse.sharepoint.com/:p:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/IT%20Audit%20Forum%20Jan%202025.pptx?d=wbd9ba04e164f48a2acbd9b69fb36993e&csf=1&web=1&e=mj2o9J), [Feb’25](https://deutscheboerse.sharepoint.com/:p:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/IT%20Audit%20Forum%20Feb%202025.pptx?d=w174621247475462289d51c0e309940c5&csf=1&web=1&e=Uy5dcA).  => OK | Ok, no exception identified |
| **TP6** | IA had a meeting on 19 February 2025 with Petr Strnad Head of ICT Risk Controlling (S) and Sourabh Srivastav, Head of ICT Risk Assurance to check and validate with relevant personnel about the 2nd line Risk responsibilities for assessments / activities in IT Operations area performed in the year under review 1 Jan to 31 Dec 2024:   * IT operation processes (IT run) such as Incident Management, Problem Management, Software license management, IT Change Management, etc. * Assessments of IT operation processes (IT run) and how this is part of the ICT framework.   IA had a meeting on 20 February 2025 with Marco Popp Head of Group Compliance Strategy, Group Compliance Strategy (U) to check and validate with relevant personnel about the 2nd line Compliance responsibilities for assessments / activities in IT Operations area performed in the year under review 1 Jan to 31 Dec 2024:   * Compliance Control Plan 2024 and results (LEs covered by Group Compliance Strategy) * Compliance Control Plan 2025 (LEs covered by Group Compliance Strategy – any new outsourcing service agreement finalised) – S3 finding progress has been satisfactory   Evidence:   * IT Control Plan 2024 (CBF and ExR) - [link](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/2LoD%20ICT%20Compliance/IT-Compliance%20Control%20Plan%202024_DBAG%20-%20ExR-%20CBF.xlsx?d=w213d35a5d67b480d897cf1d9dbec8194&csf=1&web=1&e=13zkHn) * DBAG-DORA mapping table to the existing ICT-Guidelines - [link](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/2LoD%20ICT%20Compliance/DBAG_DORA%20Mapping%20-%2022012025.xlsx?d=wca812ac6651944cb863953d15e35c803&csf=1&web=1&e=eGxqAn) * Monthly Status-Alignment Presentation with CBF, provided by Group Compliance - [link](https://deutscheboerse.sharepoint.com/:p:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/2LoD%20ICT%20Compliance/Monthly%20reporting%20meeting%20(CBF%20IT%20compliance%20from%20slide%2014-15)%20.pptx?d=wcab67809d68841b88f083c10168af58c&csf=1&web=1&e=VIwP9t) slides 14/15.   Background from Q4 Technology Governance audit:  According to the new IT Compliance & ICT target operating model valid from Q4 2024 (refer to [ITcomplianceICT.pptx](https://deutscheboerse.sharepoint.com/:p:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/ITcomplianceICT.pptx?d=w8baeab2cfa59476286db24a12805a342&csf=1&web=1&e=oiO4Vj)), in 2025, IT Compliance will review design effectiveness and ICT Risk 2LoD/IT 1LoD will review implementation effectiveness – as also confirmed this includes standards and procedures/processes for both IT Operation and IT Security).  Also, regarding testing of 1 LoD IS implementation effectiveness, it was confirmed by Sourabh S., Head of ICT Risk Assurance unit within 2LoD shall validate / perform test of 1LoD implementation.  Sourabh further stated that the review implementation effectiveness - this includes standards and procedures/processes for both IT Operation and IT Security, if you refer that we inspect these documents for testing the 1LoD control, then we are aligned with this statement.”  Refer to [RE\_ 2024-063 Technology Governance - ICT framework and 2LoD assessments.msg](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2024%20Audits/2024-063%20Technology%20Governance%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/IS%20Risk%20Management/FuN%20240529183149%20and%20240529142019/RE_%202024-063%20Technology%20Governance%20-%20%20ICT%20framework%20and%202LoD%20assessments.msg?csf=1&web=1&e=QqBW6U)  Also, in the meeting it was confirmed that Compliance screens the regulations and informs ICT if new standards are required, and that also existing standards are screened against regulation and if process documentation is in line with the standards.  A screen shot of a computer  Description automatically generated  Fieldwork:  Revised ICS mapping from Alexandru L. and status of annual recertification. Export the latest PM/RCM from SAP GRC. Sign-off on working level was performed by all POPs / RRs except Carsten Kreuz. Now, the sign-off on PO/RO is running till the month end.  IA obtained the IT Compliance Control plan for 2024 (DBAG, ExR, CBF). The audit timeframe under review is from 01 January 2024 to 31 December 2024. The IT compliance function was only installed during 2023, refer to [Compliance Control Plan 2024 - IT Compliance.xlsx](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2024%20Audits/2024-063%20Technology%20Governance%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/IS%20Risk%20Management/FuN%20240529183149%20and%20240529142019/Compliance%20Control%20Plan%202024%20-%20IT%20Compliance.xlsx?d=w117398caa97c4ac0bf4ab0749611cccb&csf=1&web=1&e=JkoQfL). The results of the controls can be seen in Columns “BW” onwards in the provided control plan excel.  According to the IT [Control Plan 2024](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/2LoD%20ICT%20Compliance/IT-Compliance%20Control%20Plan%202024_DBAG%20-%20ExR-%20CBF.xlsx?d=w213d35a5d67b480d897cf1d9dbec8194&csf=1&web=1&e=iZhHqa) e.g., controls in scope are -  IT Asset Management, IT Incident Management, IT Change, Project Management, IT Operations Management, Application Development, IT Change, Solution Identification, Development and Testing, IT Change, Availability and Capacity, etc. Controls for IT Operation processes were in scope for 2024, and results were noted, this includes Joint audits with legal entities CBF and ECAG.  => OK  Available result reports for IT Operation topic have been provided by Peter Dikow and Joern Ogiermann (Group Compliance Strategy (U)), this includes reports for Availability and Capacity Management; IT Infrastructure Change Management, IT Problem Management refer to folder [DBAG ExR](https://deutscheboerse.sharepoint.com/:f:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/2LoD%20ICT%20Compliance/DBAG%20EXR?csf=1&web=1&e=3qceOj)  => OK  IA checked the available control plans and reports for further legal entities using a risk-based approach with focus on the regulated entities ECAG, CBF, CBL and ExR  Note: According to information provided by Marco Popp:   * ExR has outsourced IT Compliance to DBAG * Contacts for IT Compliance are   EFAG, ECAG = Bianca Sahrholz – Joint outsourcing with DBAG  CBF, CH = Jan Kobbach/Franziska Fleckenstein – outsourced to DBAG and executing all 2024 controls for them.  CBL, CS, CI, LuxCSD = Alexandre Bauermeister – outsourced to DBAG in 2025  CFCL = Sabine Guip – under final discussion  **ECAG:**  Compliance control plan for year 2024 ([link](https://deutscheboerse.sharepoint.com/:f:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/2LoD%20ICT%20Compliance/ECAG?csf=1&web=1&e=FEk7TX))  The control plan contained the monitored process areas and state the relevant regulatory framework.  Relevant IT Operation processes were scoped in the Compliance control plans for ECAG in 2024: Software Change Management, Solutions Identification, Development & Testing, Acceptance & Transition Management  => ECAG Compliance Control Plan 2024 covered IT Operation processes IT Asset Management (including a test for license management), Incident Management and Change Management and these topics are also addressed in the compliance reports.  => OK  No control was planned for process IT Problem Management for ECAG and EFAG  This was confirmed by Bianca Sahrholz, Head of CCP Compliance, CCP Compliance (U). As ECAG / EFAG have their own LE Compliance Function in place, which is not only covering Business and Tax topics but also IT and IS topics. ECAG/EFAG Compliance are already covering IT and IS topics in its Annual Compliance Control Plans.  **CBF:**  According to information provided by Franziska Fleckenstein, Compliance Officer, Regulatory Compliance, IT Operation processes have been tested by CBF Compliance as pointed out, that the execution of planned controls for 2024 is with Group Compliance due to IT Compliance in the meantime being outsourced to Group colleagues (contacts: Marco Popp, Joern Ogiermann).  => OK  **CBL:**  According to information provided by Thomas Zanelli, IT Compliance Officer, Control Assurance (U), about 2024, a waiver approved by CBL ExBO on the non -performance of a 2024 risk assessment and control planning was provided. Therefore, no control was executed in 2024.  Waiver for 2024: [IT-Compliance Waiver 2024 CRAF.pdf](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences/2LoD%20ICT%20Compliance/CBL/IT-Compliance%20Waiver%202024%20CRAF.pdf?csf=1&web=1&e=78fuFl)  “The Executive Board of CBL approves the CBL IT-Compliance’s waiver request, granting a formal exemption to not perform the IT-Compliance risk assessment 2023, based on Group Compliance CRAF methodology.”  => As evidence, that the waiver request has been approved by CBL ExBO, the confirmation received from Boards & Committees via email.  **Note:** CBL Compliance enhanced the Compliance Risk Assessment Framework (CRAF) owned by Group Compliance, to achieve a risk assessment and control planning approach alignment on a broader basis. Consequently, upon CBL Compliance’s decision to review the methodology and work on the legal inventory, the CBL Executive Board had approved on 5 March 2024 a waiver request on a formal exemption from the Group’s Compliance CRAF methodology for the 2024 IT Compliance risk assessment.  => OK  Also, it was confirmed by Thomas Zanelli, Control Assurance (U), that Group Compliance completed working on a new risk assessment model that would fit IT-Compliance specifics. CBL Compliance assessed the opportunities of outsourcing IT-Compliance activities to Group Compliance. Control planning and testing planned to resume in 2025 and targeting more outsourced activities to Group Compliance (DBAG).  Additional information was provided by Thomas Zanelli, Control Assurance (U), IT-Compliance controls are derived from a risk-based assessment that will consider the domains identified in the future IT-Compliance universe that was developed with Group Compliance. The approach did not define a “multi-annual review cycle is not part of the IT-Compliance methodology and is also absent from Luxembourg regulations when it comes to Compliance control function - refer to Circulars CSSF 12/552 and 20/750”. The target operation model to have an outsourcing arrangement to DBAG for 2025 was implemented.  => OK  **DBAG and ExR:**  IT Compliance for ExR has been outsourced to DBAG. For 2024, following a risk-based approach, Incident Management testing was performed for DBAG and ExR and that IT Problem Management testing was performed for ExR only.  => OK | Ok, no exception identified |

**Procedures / Criteria / documents used:**

[Links](https://deutscheboerse.sharepoint.com/:f:/r/sites/sp0281/internal/2025%20Audits/2025-001%20IT%20Operation%20Management%20(DBAG,%20ECAG,%20CBL,%20CBF,%20CFCL)/06%20Fieldwork/IT%20Operations%20Governance/Evidences?csf=1&web=1&e=KK8bAR)

Caveat: All notes in this document do not represent a protocolary transcript or quotations of the meetings. They rather provide an overview over the content of the meeting. Further the notes may be arranged according to the topics discussed and not based on the chronological course of the meeting.