**L2 >> L3 or tests name:** Cyber and IS Prevention >> Continuous Threat Detection & Response

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

|  |
| --- |
| Continuous Threat Detection & Response (+covers AU-121-04-CSDR Cyber & IS) |

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

Review the Continuous Threat & Response process with the focus on the following topics:

- (TP1) Setup of design of controls for CrowdStrike (monitoring and alerting, coordination, coverage, decommissioning of previous tool)

- (TP2) Setup of detection of advanced persistent threats and relevance to existing processes and tools (SIEM use cases, behavioral analysis)

(TP3) Review the Vulnerability Management process with the focus on the following topics:

- Setup and design of controls around Rapid 7 applications (e.g. different scanning types, assets covered (cloud), scanning failure management and reporting

- Oversight and reporting of outputs to relevant stakeholders (trend analysis, DSC reporting)

- Management of closure of vulnerabilities in VMT related projects (criteria, timelines, automation, re-scanning)

(TP4) Based on FuN 240410100556:

Review the usage of Microsoft Defender for malware scanning of cloud related assets.

Additionally follow up on Clearstream relevant Malware related incident not noted in the incident list.

(TP5) Perform General Controls tests related to the L3 Processes Continuous Threat & Response and Threat and Vulnerability Management based on risk-based assessment of applicability.

(TP6)

1.6.1. IT application lifecycle and documentation risks - Inspect the latest available IT application risk assessment and ensure it is timely performed and in accordance with IRM process. Verify if any high criticality risks have been identified (R3-R5) and remediation plans have been adequately defined.

1.6.2. IT availability and continuity risks - Obtain the Security Concept on the related IT Application and validate that dedicated controls regarding the functionality are formally defined, esp. regarding availability and continuity. Inspect the Security Concept and APMS whether RTO or RPOs are defined and in line with business needs. Inspect relevant documentation whether any incidents occurred during the test on the applications in scope and if they were handled adequately and timely.

1.6.3. IT change and data integrity risks - Take a sample of fields (e.g., classification, RTO/RPO) in the IT Application Inventory and check their adequacy, plausibility and consistency of classifications in the various inventories (CMS, CMT, APMS, RoPA, BCM/URP, etc...). IA to further check on technical interfaces for accurate / complete data transfer from TDP to ECP.

1.6.4. IT security operation risks - sensitive business access and segregation of duties controls. Inspect the access rights granted to the application and verify the access rights are granted on a need-to-know/need-to-have basis.

Applications to be covered for L3 Continuous Threat & Response:

AID2131 CrowdStrike Falcon Complete - as part of testing above

AID2146 PA CNAPP - general IT Controls according risk assessment (TP6)

AID737 MISP - general IT Controls according risk assessment (TP6)

CID3586 of AID551 Microsoft Defender for Endpoint - as part of testing above

Applications to be covered for L3 Threat and Vulnerability Management

AID953 RPE - general IT Controls according risk assessment (TP6)

AID986 Rapid7 Nexpose - as part of testing above

AID430 VMT & Risk Register- as part of testing above

**Audit procedures/source:**

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

**Conclusion:**

2 exceptions identified

Internal audit (MM - TP1 to TP5, ÖG/AW – TP6) has performed the following Audit procedures:

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

**Summary of work done:**

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

|  |  |  |
| --- | --- | --- |
| **AP** | **Work done** | **Result** |
| **TP1** | IA performed a walkthrough of the process with head of unit Detect & Prevent Rui Mendes on 11.6.2025.  **The relevant controls are mentioned as part of ICT Operations guideline.**  **Evidence:**    **Relevant requirements:**    **The operational manual for CS is located on confluence** [**link**](https://confluence.deutsche-boerse.com/spaces/SECCUR/pages/105522036/1.1+Crowdstrike+Falcon) **:**    **The scope of the tool as any other security tools is defined in the Security Tool Matrix file.**  **Obtained the latest available version during fieldwork.**  **Evidence:**  **Status and scope:**    **The previous tool has been decommissioned:**    **CrowdStrike is onboarded in SIEM. Relevant alerts are forwarded to the SIEM for assessment and potential investigation (IS incident management).**  **The current coverage is approximately 94% of the servers are onboarded in CrowdStrike.**  **Onboarding part of regular reporting.**  **Conclusion: No issues noted for close out list** |  |
| **TP2** | IA performed a walkthrough of the process with head of unit Detect & Prevent Rui Mendes on 11.6.2025.  According to auditee there is currently no advanced persistent threats functionality enabled for the devices. The so called Crowdstrike UEBA service is not in use.  However part of the existing services is already certain ML capability of the platform.  Evidence of sample alert raised detected by ML:    Further setup of these additional functionalities potentially to be checked in next audit preparation phase.  Conclusion: no issues noted. | **OK** |
| **TP3** | IA performed a walkthrough of the process with head of unit VM – Plan and Design Rahul Choubey on 11.6.2025.  Relevant documents:    Noted that the level 4 document has not been yet updated to change in the 2025 version of ICT Patch – this is in progress according to auditee and has been also highlighted by 2nd LoD (IO\_ICT-PVM\_03)  For Rapid 7 there are 2 types of scans – deep scan with user created on local machine. Also called an authenticated scan.  If a user cannot be created on the appliance, parameter scanning is performed, e.g. through open ports.  For scan failures, or issues with the scanner – a BAU it ticket with assignment to Security IT as IT owner of the tool would be created.  The scan results are fed into a Datawarehouse (based on R7).  This is a middleware from which afterwards reporting to VMT tool, ISPIRI tool for KPIs related to SDSs and DSC meetings slides are taken.  IA noted lack of awareness of the ICS controls in place by the respective team. However this point has been raised during our fieldwork in dedicated Special Audit on General Controls as S3 finding 2025-024\_F01 – one of the reco owners is IT Governance, Risk and Transformation (IRT) which would be responsible, therefore no need to duplicate the point.  Regarding the reporting, there is no specific trend analysis in place. However overdue vulnerabilities is a defined KPI for the DSC meetings.  This KPI is  DSC: April 2025:    DSC: May 2025:    DSC June 2025:    Auditee mentioned that there has been a working group setup in February.  This has been closed as topic in DCS and moved to the CP forum    IA obtained two sample of latest CP forum slidedecks:    The vulnerabilities are broken down, status is also shown in advance (example of upcoming exceptions expirations) to highlight to teams potential increase to be worked on, but no further actions to address the still large number of overdues.  Auditee mentioned also a setup of VMTfix project – which would be moving out of the current JIRA VMT tool environment. Led by Corporate IT developers.  According to the DBG TISO role description. Details:    It is the TISOs responsibility to:  *Oversees the Information Security DSC KPIs, relevant product line metrics and informs the responsible stakeholders in the IT product line about missing measures to improve the overall security posture and thereby the KPI level.*  Regarding the closure of the vulnerabilities in the tool. The impacted teams can claim False positive or Fix Claim, which need either interaction of the VM team member for final closing, or the weekly retest is closing the ticket automatically when the issue is remediated on the same asset.  IA has checked the status of the tickets with Fix Claim in the VMT tool related to the in-scope Rapid 7 scans (project NXP within VMT) and noted the following    Also there was lack of documentation on the statuses of these tickets in any of the process documents. However this has been already raised during our fieldwork by 2nd LoD which performed overarching VM process review at the same time. Meeting held with Sourabh Shrivastava to confirm these points to be included in the ICT Risk assurance report. (  2025-01\_05)  Conclusion: Noted the following for the close out point:   * Significant number of overdue vulnerabilities in status Fix Claim not treated * Overall high and critical overdue vulnerabilities reported to DSC 3 months in row significantly over the defined threshold – without attention on the impacted product side by TISOs (confirmed during fieldwork/col stage) | **NOK** |
| **TP4** | The underlying Future note 240410100556:  *During the 2024-017 Data Resiliency Audit we have observed that malware protections services are not in production for Microsoft Azure Cloud. Microsoft Defender is activated for sensitive data discovery but MS launched the new service called "Malware Scanning" for storages and it looks like that it has some special capabilities for scanning. It is advised to control the current state of malware scanning for cloud storages in upcoming Cyber audit.*  IA noted in the currently published Azure platform security baseline v1.2 from March 2024 ( Evidence link: [2024\_DBG\_Azure\_Security\_Baseline\_1.2.pdf](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0823/400_Publication/IS%20IT%20Services/IS%20baselines/2024_DBG_Azure_Security_Baseline_1.2.pdf?csf=1&web=1&e=gKUrhn) )  That the function of Microsoft Defender for Storage is required to be set to ‘On’:    Inquiry of SME on the topic Vibhor Goel on 2.6.2025 noted the following:  The service of Microsoft of Defender is enabled.    The service is enabled at the subscription level. DBG does not exclude any account from it.  There are various cases in terms of licensing. The service started to be used on the classic licensing, however any new landing zones are automatically on v2. As the cost would be cca 3.5x if all would switch on v2 – for now the previous ones stay on v1.  V2 has real-time malware scanning, however only enabled for now for cca 10 cases out of 1000-1100.  Capping is enabled only on the v2 as it relates to these advanced per transactions scanning vs per storage.  The advanced functionality like sensitive data discovery is not turned on:    Alerts from the tool are available and dedicated emails are being sent to the asset owner and the cloud platform engineering team.    Example:    The access to the settings are following the access right concept for the cloud platform as described [here](https://knowledge.deutsche-boerse.de/spaces/CLOUD/pages/395414325/02+-+Cloud+User+Role+Model).  The discrepancy in the provided incidents list [here](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/CTDR%26VM/14%20Incidents%20records%202025-045%20Audit.xlsx?d=w25303589de56494f8b9a35d5faee34d8&csf=1&web=1&e=10pl6s) and the incident [here](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/CTDR%26VM/Re%20(CUTT-52669)%20IS%20Incident%20detected%20CFCS%20Director%20Endpoint%20Involved%20in%20Botnet%20.msg?csf=1&web=1&e=Phq9Ib) has been investigated and noted, that this was due to date difference, the incident has been noted after the extraction for our audit was performed.  Ticket details:    Extraction performed:    *Conclusion: No issues noted for close out list.* | **OK** |
| **TP5** | One of the selected General Controls based on risk based approach:  Review capturing of relevant regulatory requirements in legal inventories (DORA focused)  CBL  IA reviewed the RegMon application and noted the following:   * for CBL only one line (LIE-945) and that regarding BCM (which is only one aspect of the DORA regulation) * no line for other Luxembourg entities at all     Conclusion: Incomplete capturing of DORA in the RegMon application for Clearstream Luxembourg entities. | **NOK** |
| **TP6.1** | 1. **Palo Alto Networks Prisma Cloud (PA CNAPP) – AID2146 is rated Major, Risk Assessment must be carried out every 24 months, according to Information Security Management Standard**     JQL query:  project = "Risk Assessment Planning" and "Asset Name" = AID2146 order by due desc  [Execute query](https://vmt.deutsche-boerse.de/browse/RAP-5756?jql=project%20%3D%20RAP%20AND%20text%20~%20%22AID2146%22)  These were identified:  Link for The most recent risk assessment that was resolved in December 2023 >>[**RAT\_Dec 2023**](https://vmt.deutsche-boerse.de/browse/RAP-5712)  IA noted that the next risk assessment is due in December, 2026> [RAP-5756](https://vmt.deutsche-boerse.de/browse/RAP-5756) and hence that the risk assessment is not planned to be performed at least ones in 24 months.    Considering the application criticality was changed according to APMS from minor to major on the date 24/02/2025, IA concluded that the due date should have been changed by IS risk team. IA contacted the application owners, and the due date has been corrected as 19/12/2025. (See the screenshot below). As the minor issue was already addressed during the fieldwork phase, IA didn’t raise a finding.    [DBG\_IS\_RAT\_AID2146\_PA CNAPP\_v1.6\_2023-12-07\_1548.xlsm](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/CTDR%26VM/DBG_IS_RAT_AID2146_PA%20CNAPP_v1.6_2023-12-07_1548.xlsm?d=w0043cfa74f42407cbdc01b9338f7eadb&csf=1&web=1&e=Bp5pPy)  IA assessed the sheets “Asset Profile”, “SSD Control Requirements”, “Risk Assessment” and “RR Risk & Measures” and reviewed that all relevant fields are filled.  Plausibility check: [RAP-5712\_AID2146\_PA CNAPP\_PlausibilityChecks\_v1.4\_2023-12-07\_1608.xlsx](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/CTDR%26VM/RAP-5712_AID2146_PA%20CNAPP_PlausibilityChecks_v1.4_2023-12-07_1608.xlsx?d=w1c848fd792874d4c80dd7f221be64cad&csf=1&web=1&e=eAN2qx)  Formal plausibility check is available, and all relevant fields are filled. Plausibility check is described in sheet “Checklist”.  The check was carried out by Alexis Fernandez,IS Risk Management (U).  Identified risk ISRM-120392 2Lack of, or incomplete, operating procedures” is open and the resolution is due on the date 12/06/2025.  IA contacted the application owner and was informed that a 3-month extension has been requested for the due date and the approval for the request is in review.  Next risk assessment is due in December 2025 >>[RAP-5756](https://vmt.deutsche-boerse.de/browse/RAP-5756?jql=project%20%3D%20RAP%20AND%20text%20~%20%22AID2146%22)  OK   1. **MISP Internal Threat Intelligence Sharing platform – AID737 is rated Minor, Risk Assessment must be carried out once per 36 months according to Information Security Management Standard.**   **JQL query:**  **project = "Risk Assessment Planning" and "Asset Name" = AID737 order by due desc**  [**Execute Query**](https://vmt.deutsche-boerse.de/issues/?jql=project%20%3D%20RAP%20AND%20summary%20~%20AID737%20ORDER%20BY%20priority%20DESC%2C%20updated%20DESC)  **These were identified:**      **Link for the most recent risk assessment >>:** [**Link**](https://vmt.deutsche-boerse.de/browse/RAP-4768) **, the one resolved on the date 24/02/2025**  **Link for the previous risk assessment >>:** [**Link**](https://vmt.deutsche-boerse.de/browse/RAP-3318?jql=project%20%3D%20RAP%20AND%20summary%20~%20AID737%20ORDER%20BY%20priority%20DESC%2C%20updated%20DESC) **, the one resolved on the date 06/01/2023**  **IA verified that the risk assessment was performed at least ones in 36 months.**  [DBG\_IS\_RAT\_AID737\_MISP\_v3.8\_2024-10-08\_0742.xlsm](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/CTDR%26VM/DBG_IS_RAT_AID737_MISP_v3.8_2024-10-08_0742.xlsm?d=w07cbbff054f143ae8d2b4faed5edc9e9&csf=1&web=1&e=XObPjB)  IA assessed the sheets “Asset Profile”, “SSD Control Requirements”, “Risk Assessment” and “RR Risk & Measures” and reviewed that all relevant fields are filled.  Plausibility check: [RAP-4768\_AID737\_MISP\_PlausibilityChecks\_v1.8\_2024-10-09\_1609.xlsx](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/CTDR%26VM/RAP-4768_AID737_MISP_PlausibilityChecks_v1.8_2024-10-09_1609.xlsx?d=w6c4e3490725c462e847dd31082d4c417&csf=1&web=1&e=tKyLAL)  Formal plausibility check is available, and all relevant fields are filled. Plausibility check is described in sheet “Checklist”.  Check was carried out by Debmalya Chatterjee, IS Risk Management (U).  IA noted that also in the plausibility check, it is identified that the actual IC is not aligned with the IC in the APMS. (Refer to line 8 in the worksheet “Checklist”.), however IC is not updated in the APMS. However, IA was informed by the IT application owner that criticality is automatically calculated based on CIAA values and Core Application Flag entered. According to calculation embedded in APMS, for non-core applications, maximum criticality is calculated as max CIAAA value-1. See below the explanation:    Identified risks were followed up in Jira and the risks were accepted:    Next Risk Assessment due in October 2025 >[RAP-6403](https://vmt.deutsche-boerse.de/browse/RAP-6403)  OK   1. **Remote Penetration Test Environment** **RPE – AID953 is rated Major, Risk Assessment must be carried out every 24 months, according to Information Security Management Standard**   JQL query:  project = "Risk Assessment Planning" and "Asset Name" = AID953 order by due desc  [Execute query](https://vmt.deutsche-boerse.de/issues/?jql=project%20%3D%20RAP%20AND%20resolution%20in%20(Unresolved%2C%20Resolved%2C%20%22Cannot%20Reproduce%22%2C%20%22Review%20needed%22%2C%20%22False%20Positive%22%2C%20%22Feedback%20IS%20Eng%22%2C%20Imported%2C%20Done%2C%20%22Escalation%20needed%22%2C%20%22Won%27t%20Do%22%2C%20Rejected%2C%20Duplicate%2C%20%22To%20Mitigate%22%2C%20Accepted%2C%20%22Not%20Decided%22%2C%20Avoided%2C%20Mitigated%2C%20%22No%20Impact%22%2C%20Invalid%2C%20%22Measure%20Not%20Implemented%22%2C%20%22No%20Risks%20Identified%22%2C%20Decommissioned%2C%20Rolledback%2C%20%22Was%20informed%22%2C%20Reassessed%2C%20Approved%2C%20Acknowledged%2C%20Cancelled%2C%20%22Risk%20Identified%22%2C%20%22Risk%20Created%22%2C%20Expired)%20AND%20text%20~%20%22AID953%22%20ORDER%20BY%20priority%20DESC%2C%20updated%20DESC)  These were identified:      **Link for the most recent risk assessment >>:** [**Link**](https://vmt.deutsche-boerse.de/browse/RAP-3899?jql=project%20%3D%20RAP%20AND%20text%20~%20%22AID953%22%20ORDER%20BY%20created%20DESC) **, the one resolved on the date 06/12/2024**  **IA noted that the current risk assessment will be due on the date 02/06/2025, however the assessment has not been attached yet for review. IA contacted the application owner and was informed that the RPE infrastructure is getting updated with the latest architectural components. Queuing this constant update also within the Risk Assessment deliverables is taking significant time. Hence, together with Management, it has been decided to request an extension for risk assessment. IA noted that the due date has been extended to 15/07/2025. (See below the screenshot**    **IA verified that the risk assessment was planned to be performed at least ones in 24 months. However, the due date for the assessment was extended due to the latest architectural changes in RPE architecture. As the most recent risk assessment is not finalized by fieldwork time, IA couldn’t perform an evaluation. While the delay had been caused by the latest architectural changes in RPE architecture, IA didn’t raise a finding.**  **As the most recent risk assessment hasn’t been approved by the fieldwork time period, IA couldn’t evaluate the plausibility check.**  Conclusion: Ok. No issues for the Close-out list. |  |
|  | A) IA inspected the supplied Palo Alto Networks Prisma Cloud Security Documentation v1.3 from April 2024. IA validated that dedicated controls regarding the functionality are formally defined, esp. regarding availability and continuity. In the Security Concept and APMS, RTO or RPOs are defined and in line with business needs.  RTO is defined between 2 hours to 1 day in the security documentation which is aligned with APMS. As the application’s max availability is “major” (RPO is defined as 1 hours to 4 hours), IA noted that the application is not relevant to CSDR regulation, hence it was not covered as part of the annual DR test in 2024.  [SharingWExt - 19-25 Information Technology - All Documents](https://deutscheboerse.sharepoint.com/sites/GIA/ext/2025%20Auditee%20Accessible%20Library/Forms/AllItems.aspx?id=%2Fsites%2FGIA%2Fext%2F2025%20Auditee%20Accessible%20Library%2F2025%2D045%20Cyber%20and%20Information%20Security%20%28DBAG%2C%20ECAG%2C%20CBF%2C%20CBL%2C%20CFCL%29%2F1LoD%2FDBAG%2FGroup%20Security%20%282nd%20try%29%2FDocuments%20provided%20by%20GS%2F19%2D25%20Information%20Technology&viewid=3d0f3181%2Dcb01%2D4e4e%2D8583%2D701067a8a767&csf=1&web=1&e=fdH9G7&ovuser=e00ddcdf%2D1e0f%2D4be5%2Da37a%2D894a4731986a%2Cal284%40deutsche%2Dboerse%2Ecom&OR=Teams%2DHL&CT=1747146970025&clickparams=eyJBcHBOYW1lIjoiVGVhbXMtRGVza3RvcCIsIkFwcFZlcnNpb24iOiI0OS8yNTA0MTcxOTMwOSIsIkhhc0ZlZGVyYXRlZFVzZXIiOmZhbHNlfQ%3D%3D&CID=f4e82f20%2D7241%2D4494%2Db509%2D60d3db5b0e79&cidOR=SPO&FolderCTID=0x0120007A37F1A072D10D41911CA464DCFF758A)  The application is a cloud-based SaaS cloud-native application protection platform from Palo Alto Networks. It has multiple modules to secure cloud-based computing, we will be using the following:   * Cloud Security Posture Management (CSPM) * Cloud Workload Protection (CWP) * Cloud Code Security (CCS) * Data Security (DS) * Cloud Infrastructure Entitlement Management (CIEM)   Prisma Cloud’s computer security features are integrated into Prisma Cloud and use the same user interface. DBG Prisma Cloud is hosted on GCP. The responsibility of operating, managing, and maintaining the software and the underlying infrastructure lies with the vendor.  Availability of information processing facilities  RTO: 2 hours < RTO <= 1 day  Part of yearly DRP: Not applicable as the application criticality is major and as the application is not CSDR relevant. IA noted that the application was not part of the annual DR test performed in 2024. DBG Prisma Cloud tenant is hosted in app.eu.prismacloud.io which is located in Frankfurt and Ireland data centers.  Information backup:  Recovery Point Objective (RPO): 1 hours <= RPO < 4 hours  Mirroring: no mirroring in place  Backup interval: SaaS, defined by Palo Alto Networks  Backup recovery test regularly (at least yearly) performed: Applicable (Availability requirements for the application are rated as ‘Major’. However, due to the SOC 2 criteria A1.3, C5 criteria OPS-08, controls 37, 38, 39. The application is SOC2 ).  The screenshot of the daily backup performed on the date 17/06/2025, weekly backup performed on the dare 16/06/2025 and monthly backup performed on the date 18/05/2025 by Palo Alto:      Cloud service providers define guidelines for classification, prioritization, and escalation of security incidents and create interfaces to incident management. The Cloud Service Provider has set up a CERT team, which contributes to the coordinated resolution of occurring security incidents. After a security incident has been processed, the solution is documented, and the report is sent to DBG for final acknowledgement and/or for confirmation.  Backup recovery tests regularly (at least yearly) are performed. See the screenshot below showing that the last backup restore test was performed on the date 17/06/2025:        For more detailed information please refer to the application’s [security document](https://deutscheboerse.sharepoint.com/:w:/r/sites/GIA/ext/2025%20Auditee%20Accessible%20Library/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/1LoD/DBAG/Group%20Security%20(2nd%20try)/Documents%20provided%20by%20GS/19-25%20Information%20Technology/Security%20Documentation%20-%20Prisma%20Cloud%20-%20AID2146%20-%20v1.3%20(2024.04.24)%20(Template%20v1.3).docx?d=w50b2c7064e0d41a38969684f4da7709a&csf=1&web=1&e=uP42yp) that has been comprehensively prepared and were referenced during fieldwork interviews.  **OK**  **B) IA inspected the supplied MISP (AID737) security documentation v 1.7 from October, 2024.** IA validated that dedicated controls regarding the functionality are formally defined, esp. regarding availability and continuity. In the Security Concept and APMS, RTO or RPOs are defined and in line with business needs. In the Security Concept and APMS, RTO or RPOs are defined and in line with business needs. No relevant incidents occurred during the test on the application.  [SharingWExt - 19-25 Information Technology - All Documents](https://deutscheboerse.sharepoint.com/sites/GIA/ext/2025%20Auditee%20Accessible%20Library/Forms/AllItems.aspx?id=%2Fsites%2FGIA%2Fext%2F2025%20Auditee%20Accessible%20Library%2F2025%2D045%20Cyber%20and%20Information%20Security%20%28DBAG%2C%20ECAG%2C%20CBF%2C%20CBL%2C%20CFCL%29%2F1LoD%2FDBAG%2FGroup%20Security%20%282nd%20try%29%2FDocuments%20provided%20by%20GS%2F19%2D25%20Information%20Technology&viewid=3d0f3181%2Dcb01%2D4e4e%2D8583%2D701067a8a767&csf=1&web=1&e=fdH9G7&ovuser=e00ddcdf%2D1e0f%2D4be5%2Da37a%2D894a4731986a%2Cal284%40deutsche%2Dboerse%2Ecom&OR=Teams%2DHL&CT=1747146970025&clickparams=eyJBcHBOYW1lIjoiVGVhbXMtRGVza3RvcCIsIkFwcFZlcnNpb24iOiI0OS8yNTA0MTcxOTMwOSIsIkhhc0ZlZGVyYXRlZFVzZXIiOmZhbHNlfQ%3D%3D&CID=f4e82f20%2D7241%2D4494%2Db509%2D60d3db5b0e79&cidOR=SPO&FolderCTID=0x0120007A37F1A072D10D41911CA464DCFF758A)  MISP is DBG’s Intern**al Threat Intelligence Sharing platform application which is not developed internally and instead a commercial-off-the-shelf solution.**  Availability of information processing facilities  RTO: 2 hours < RTO <= 1 day  Part of yearly DRP: Not applicable as the application criticality is major and as the application is not CSDR relevant. IA noted that the application was part of the annual DR test performed in 2024. Refer to [IT DR Execution Report 2024](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-024%20SA%20General%20Controls%20%5BDBAG,%20ECAG,%20CBF,%20CBL,%20CFCL%5D/06%20Fieldwork/IT%20availability%20and%20continuity%20controls/Evidence/Test_Execution_Report_Systems_2024_FINAL.pdf?csf=1&web=1&e=uQ1ghI)  Data is hosted on premises.  Information backup  Recovery Point Objective (RPO): 4 hours <= RPO < 1 day  Mirroring: no mirroring in place  Backup interval: Once a week full backup, daily incremental, retention approx. 4 weeks.  Virtual Machines have five incremental backups throughout the week, and a full back up over the weekend. Please see screenshots showing the backup schedules below for each virtual machine.  For misptipas01      For misptipas02    The CSV file shows the backup status of two VMs since the beginning of the month. >>[Backup\_Status\_misptipas\_June.csv](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/CTDR%26VM/Backup_Status_misptipas_June.csv?d=w16900f4c7dc24449844546d46f91c38c&csf=1&web=1&e=hR02x2) . IA noted that for each server, there are two jobs for every day which are a snapshot; and backups which were successfully taken apart from the three failed backups of misptipas01 which are seen in lines 70, 81, 82 (status 129 - “disk storage unit is full”). IA was informed that the backup failures derived from the lack of disk space on the storage, but they run cleanups manually to ensure that subsequent backups were successfully completed.  Backup recovery tests are not performed at least annually. Not Applicable (Availability requirements for the application are rated as ‘Major’.)    Standard DBG incident management process is followed in case of an incident. If an incident owner detects a security breach, the CERT team must be informed immediately by calling the CERT hotline (can be reached under - 3 35 55) or sending an email ([cert@deutsche-boerse.com](mailto:cert@deutsche-boerse.com)). This obligation to report incidents to CERT is described in the Incident Management Process document.  DBG Data retention policy followed: Yes – retained for 4 weeks.  For more detailed information please refer to the application’s [security document](https://deutscheboerse.sharepoint.com/:w:/r/sites/GIA/ext/2025%20Auditee%20Accessible%20Library/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/1LoD/DBAG/Group%20Security%20(2nd%20try)/Documents%20provided%20by%20GS/19-25%20Information%20Technology/Security_Documentation_MISP_v1.7.docx?d=w9b11b839b9bd48169752e26fb2dc9270&csf=1&web=1&e=Ss27l5) that has been comprehensively prepared and was referenced to during fieldwork interviews.  **OK**   1. **IA couldn't inspect RPE (AID953) Security Documentation of Remote Penetration Test environment application as the most recent risk assessment is not finalized by fieldwork time, IA couldn’t perform an evaluation. While the delay had been caused by the latest architectural changes in RPE architecture, IA didn’t raise a finding.**   **OK**  Conclusion: Ok. No issues for the Close-out list. |  |
|  | 1. Information in APMS is correspondent to the information in the Security Documentation v1.3 from April 2024. Internal Audit received the current extract for the application Palo Alto Networks Prisma Cloud – AID2146 from the application repository [see [APMS](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/CTDR%26VM/CNAPP%20application%20APMS%20extract.pdf?csf=1&web=1&e=i6wVlg)]. The classification of the application is consistent in the provided documents as ‘major’. The RTO is 2 hours < RTO <= 1 day and RPO is 1 hour <= RPO < 4 hours. No material changes were identified since the previous review. Internal Audit reviewed the extract for Palo Alto Networks Prisma Cloud – AID2146 to conclude: 2. Application is entered in APMS. All relevant fields for the applications have been filled in the repository. Internal Audit sampled the below listed fields:  * Onboarded to IIQ * Cloud Application * Internet Facing * External Facing * Max Criticality * Max Integrity * Max Availability * Max Confidentiality * Max Authenticity * RTO (Recovery Time Objective) * RPO (Recovery Point Objective) * Relevant LEs (owning/using)  1. The application is deployed to cloud, Google Cloud Platform (GCP) being the cloud service provider (CSP). The service model is Software-as-a-Service (SaaS). GCP provides protection for hosts, containers, and serverless infrastructure in the cloud and on-premises. 2. The application is not KRITIS relevant – no explicit requirement. 3. Part of yearly DRP: not applicable (as DR is conducted for applications RTO <= 2).     APMS shows the following entries:    Relevant fields are filled, are plausible and are consistent with the [CNAPP application APMS extract.pdf](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/CTDR%26VM/CNAPP%20application%20APMS%20extract.pdf?csf=1&web=1&e=6gglvt)    The network architecture diagram shows the connections between the relevant systems/components and the respective zone(s).    The interfaces and their security parameters are listed in the interfaces table below.     1. Information in APMS is correspondent to the information in the Security Documentation **1.7 from October 2024.** Internal Audit received the current extract for the application MISP – AID737 from the application repository [see [APMS](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/CTDR%26VM/MISP%20Application%20APMS%20extract.pdf?csf=1&web=1&e=whctsG)]. The classification of the application is consistent in the provided documents as ‘major’. The RTO is 2 hours < RTO < 24 hours and RPO is 4 hours <= RPO < 1 day. No material changes were identified since the previous review. Internal Audit reviewed the extract for MISP – AID737 to conclude: 2. Application is entered in APMS. All relevant fields for the applications have been filled in the repository. Internal Audit sampled the below listed fields:  * Onboarded to IIQ * Cloud Application * Internet Facing * External Facing * Max Criticality * Max Integrity * Max Availability * Max Confidentiality * Max Authenticity * RTO (Recovery Time Objective) * RPO (Recovery Point Objective) * Relevant LEs (owning/using)  1. The application is an on-premises application which is a Commercial-off-the-shelf Solution. 2. The application is not KRITIS relevant – no explicit requirement. 3. Part of yearly DRP: not applicable (as DR is conducted for applications RTO <= 2).     APMS shows the following entries:    Relevant fields are filled, are plausible and are consistent with the [Security\_Documentation\_MISP\_v1.7.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/GIA/ext/2025%20Auditee%20Accessible%20Library/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/1LoD/DBAG/Group%20Security%20(2nd%20try)/Documents%20provided%20by%20GS/19-25%20Information%20Technology/Security_Documentation_MISP_v1.7.docx?d=w9b11b839b9bd48169752e26fb2dc9270&csf=1&web=1&e=yOv1B5)    The network architecture diagram shows the connections between the relevant systems/components and the respective zone(s).    The interfaces and their security parameters are listed in the interfaces table below:  I   1. **IA couldn't inspect if** Information in APMS is correspondent to the information in the **RPE (AID953) Security Documentation for Remote Penetration Test environment application as the most recent risk assessment is not finalized by fieldwork time. Since the delay had been caused by the latest architectural changes in RPE architecture, IA didn’t raise a finding.**   **OK** |  |
|  | * Palo Alto Networks Prisma Cloud – AID2146 Identity & Access Management   Authorisation Concept was received during preparation phase.  IA inspected the application [Authorisation Concept](https://deutscheboerse.sharepoint.com/:w:/r/sites/GIA/ext/2025%20Auditee%20Accessible%20Library/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/1LoD/DBAG/Group%20Security%20(2nd%20try)/Documents%20provided%20by%20GS/19-25%20Information%20Technology/Authorization%20Concept%20-%20Prisma%20Cloud%20-%20AID2146%20-%20v1.1%20(2023.11.30.a)%20(Template%20v1.3).docx?d=w94d0d1b6f2f54422a4342d66f439e74c&csf=1&web=1&e=lCK4Rd) and the [extract from IIQ (dated 16 June 2025)](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/IIQ%20Roles%20(16June%202025).xlsx?d=wccc4a4a145cb4f4f99cc646108d77f3e&csf=1&web=1&e=vGwdiU) and performed analysis. The entitlements/roles were not in sync from the description in AC and the implementation in IIQ:   * There are 48 IT Roles/ Entitlements that are existing in Sailpoint IIQ but not in the Authorization Document. * There are 15 IT Roles/Entitlements that are existing in Authorization document but not in Sailpoint IIQ   Additionally, the SoD analysis was not prepared as per matrix template and implemented within IIQ.  Internal Audit (IA) identified missing access rights management controls for the Palo Alto Networks Prisma Cloud – AID2146 application. The application owner had neither defined nor implemented segregation of duty (SoD) principles and rules between its Authorisation Concept and the ruleset in identity and access management tool SailPoint IIQ (AID2146).  German and Luxembourg regulation circulars require that the organisation shall manage access rights to information assets and their supporting systems on a “need to know” basis and under the least privilege model. Segregation of Duties (SoD) and the handling of SoD conflicts must be documented and implemented.   * MISP – AID737 Identity & Access Management   Authorisation Concept was received during preparation phase.  IA inspected the application [Authorisation Concept](https://deutscheboerse.sharepoint.com/:w:/r/sites/GIA/ext/2025%20Auditee%20Accessible%20Library/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/1LoD/DBAG/Group%20Security%20(2nd%20try)/Documents%20provided%20by%20GS/19-25%20Information%20Technology/Authorization%20Concept%20_MISP_IT%20Asset_v1.4_final.docx?d=w5eefccaa4cac436fb94d3a740a449562&csf=1&web=1&e=WVt9M6) and the extract from IIQ (dated 16 June 2025) and performed analysis. The entitlements/roles were in sync from the description in AC and the implementation in IIQ. However, the SoD analysis was not prepared as per matrix template and implemented within IIQ.  There are 3 type roles (user, admin and publisher) with no SoD defined that might cause the:   * Threat Intelligence Platform to be configured to manipulate data, * Events to be created and modified and published by the same user that might spread false or malicious information. * distribution rules might be configured and content to be pushed bypassing an oversight.   Internal Audit (IA) identified missing access rights management controls for the MISP – AID737 application. The application owner had neither defined nor implemented segregation of duty (SoD) principles and rules between its Authorisation Concept and the ruleset in identity and access management tool SailPoint IIQ (AID737).  German and Luxembourg regulation circulars require that the organisation shall manage access rights to information assets and their supporting systems on a “need to know” basis and under the least privilege model. Segregation of Duties (SoD) and the handling of SoD conflicts must be documented and implemented.  Note: IA provided the user/role list for MISP application users and verified that none of the application users are assigned to the roles with toxic combinations. Refer to [test-Aid737.xlsx](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/CTDR%26VM/test-Aid737.xlsx?d=w4c688afe6bf3495ca2d9bc8bcd23336c&csf=1&web=1&e=n3FTdM)  Close-out list sent to auditee regarding the observation on 2nd June 2025 (Refer to [RE Close-out List 2025-045 Audit.msg](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/CTDR%26VM/RE%20Close-out%20List%202025-045%20Audit.msg?csf=1&web=1&e=iopbNV))   * Remote Penetration Test Environment – AID953 Identity & Access Management   Authorisation Concept was received during preparation phase.  IA inspected the application [Authorisation Concept](https://deutscheboerse.sharepoint.com/:w:/r/sites/GIA/ext/2025%20Auditee%20Accessible%20Library/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/1LoD/DBAG/Group%20Security%20(2nd%20try)/Documents%20provided%20by%20GS/19-25%20Information%20Technology/Authorization%20Concept%20Template_IT%20Asset_AID953_RPE_v1.3%20(1).docx?d=w981840b2a0ad42e98c547199ea73c1ba&csf=1&web=1&e=GpdDyx) and the extract from IIQ (dated 16 June 2025) and performed analysis. The entitlements/roles were not in sync from the description in AC and the implementation in IIQ. However, IA was informed that Authorization Concept has been finalized on 13-June 2025. Due to architectural changes that are currently in progress, roles will be set up for RPE and some roles will be deleted accordingly. Hence, IA didn’t raise a concern.  The SoD analysis was not prepared as per matrix template and implemented within IIQ. Internal Audit (IA) identified missing access rights management controls for the RPE– AID953 application.    Conclusion: Not Ok. Issues for the Close-out list for MISP application missing definition of SoD principles in the Authorization Concept. |  |

Follow up on the close out points noted above:

Lack of Dora in legal inventories.

Point already raised in audit ongoing in parallel as highlighted by auditee.



IA team, provided the information to the respective auditors and auditor in charge of 2025-033 outsourcing audit and issue will be raised as finding 2025-033\_F10 there.

Therefore issues considered as closed for this audit.

For the outstanding status of overdue vulnerabilities reported to DSC

IA contacted 4 most impacted TISOs on their actions.

Received the following responses:









All acknowledgement actions undertaken on their behalf, attentions to the issues. IA did not identify reason or actions not taken by them, therefore no reason for a finding to be raised.

DORA mapping:

Dora act level 1. Art 25.1:

Even though the requirement is related to the testing programme, the specific vulnerability management process is in place always. The process has dedicated mandatory guideline, tools, teams involved and reporting in place.

No gap noted.

Dora act level 1. Art 25.2:

Not specifically testing as part of this audit. However the requirements are part of the guidelines and procedures. And there the currently running scans do not distinguish between the environments:

A white background with black text

AI-generated content may be incorrect.

Therefore the scanning would be performed already on testing/acceptance/simulation servers before production.