



LUXEMBOURG
ALTERNATIVE
ADMINISTRATORS
ASSOCIATION

LPEA 

OUTSOURCING GUIDELINES

VERSION 2.0

BASED ON CSSF
CIRCULAR 25/883

Developed in Collaboration with
L3A Operations Committee
& LPEA Central Administration Committee





TABLE OF CONTENTS

1. Introduction
2. Practical Guidelines for Outsourcing
3. Regulatory Requirements and Monitoring Framework
4. Training and Communication
5. Audit, Reporting, and Continuous Improvement
6. Outsourcing Policy and Procedure
7. Managing Intra-Group Outsourcing Arrangements
8. Outsourcing Monitoring Centralized at Group Level

About L3A

The Luxembourg Alternative Administrators Association ("L3A") is the leading representative body for fund and corporate administrators of alternative assets in Luxembourg. Since its founding in 2004, the association has been dedicated to promoting the interests of alternative service providers and contributing to the development of Luxembourg as the investment hub and operations centre of choice for global alternative investment managers.

Our members deliver our mission through their work on our 5 permanent committees, being Operations, Tax, Regulatory, HR and Events & Communications, with output delivered to industry players, regulators and government bodies amongst others, and published through our website and social media channels, in particular LinkedIn. As the recognised voice of our profession, we engage with authorities through participation in commissions and working groups, and maintain strong ties with government bodies, professional organisations, and Chambers of Commerce.

Our membership is made up of over 60 members, including Full Members, being Luxembourg administration firms predominantly providing services to foreign investment managers of funds and related entities in the alternative management industry and Associate Members, being Luxembourg professional firms operating in the real asset environment and offering services to Full Members and/or their clients. Together, we form a trusted network committed to excellence.

About LPEA

The Luxembourg Private Equity and Venture Capital Association ("LPEA") aims at promoting and defending the interests of investors and professionals principally active in the field of Private Equity ("PE") and Venture Capital ("VC"). The Association is the trusted and relevant representative body of PE and VC practitioners with a presence in Luxembourg. Created in 2010 by a leading group of PE and VC players, with more than 600 members, LPEA plays a leading role locally, actively promoting PE and VC in Luxembourg. LPEA provides a dynamic and interactive platform, which helps investors and advisors to navigate through latest trends in the industry. International by nature, the association allows members to network, exchange experience, expand their knowledge and grow professionally by attending workshops and trainings held on a regular basis.

1

INTRODUCTION

PURPOSE OF THE POSITION PAPER

This white paper provides practical guidance on outsourcing arrangements for financial institutions operating in Luxembourg, aligned with CSSF Circular 22/806 (as amended by CSSF Circular 25/883) hereinafter referred to as CSSF Circular 25/883. It is intended as a market-oriented reference for administrators and service providers. The guidance aims to help organizations strengthen outsourcing governance and operational resilience while remaining consistent with applicable regulatory requirements.

SCOPE AND AUDIENCE

The white paper is aimed at fund and corporate administrators, in-house compliance and risk teams, and other stakeholders (hereinafter referred to as the 'In-Scope Entity', 'Entity', or 'Organization') involved in outsourcing decisions.

This White Paper applies to all arrangements relating to functions and activities that would normally be performed by the Organization, except those expressly excluded under the Circular, and that are subject to CSSF supervision.

It covers the lifecycle of outsourcing arrangements, including definitions, due diligence, risk assessment, contractual considerations, monitoring, intra-group arrangements, exit planning, and oversight. The guidance is non-binding and does not replace legal or regulatory advice.

This White Paper does not cover the delegation arrangements relating to UCI administration activities as specifically governed by CSSF Circular 22/811.

NON-BINDING NATURE

The recommendations in this white paper are intended to reflect prevailing market practice and to support compliance with CSSF Circular 25/883. They do not impose any new regulatory and legal obligations and should be adapted to each entity's size, complexity, and risk profile. In the event of any conflict or inconsistency, the provisions of the Circular shall take precedence over this White Paper.



GLOSSARY

OUTSOURCING ARRANGEMENT

An arrangement of any form between an entity and a service provider by which that provider performs a process, service or activity that would otherwise be undertaken by the entity (CSSF Circular 25/883, Point (13)).

OUTSOURCED FUNCTION

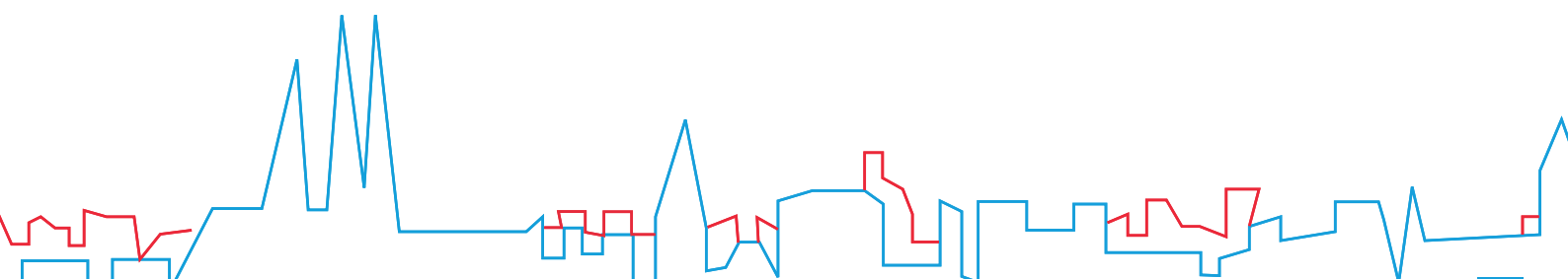
A specific process, activity or service performed by a service provider under an outsourcing arrangement.

CRITICAL OR IMPORTANT FUNCTION

A function whose disruption would materially impair the entity's operations, regulatory compliance, financial position or reputation (CSSF Circular 25/883, Chapter 4 (Section 4.1.2(18))).

SERVICE PROVIDER

Any third party, including intra-group entities, that performs an outsourced function.



2

PRACTICAL GUIDELINES FOR OUTSOURCING



2.1. DEFINING AN EXHAUSTIVE AND ACCURATE OUTSOURCING INVENTORY

ACTION ITEMS

→ **Define Outsourcing:** Document the organization's interpretation of the regulatory outsourcing definition, including activities excluded (e.g., statutory audit, market information services, legal advice, gardening and maintenance of premises, utilities services). While CSSF Circular 25/883 and EBA guidelines provide the baseline, the implementation should consider the relevant internal context. Entities outside DORA should apply the same definition and ICT/cloud service list as in DORA.

→ **Identify Outsourced Functions:** Create a comprehensive list of outsourced functions with appropriate granularity. This should include both business driven and support functions such as Human Resources, Procurement, and Finance where relevant.

→ **Define Criticality:** Define and document the criteria used by the organization to assess the criticality of the intended outsourced functions and processes. As an example, in addition to the impact on the core services provided by the organization, this assessment should also consider, amongst other, the operational, regulatory and technology related impacts as well as the sensitivity of data involved in the course of the outsourcing arrangements lifecycle. We have frequently observed that certain aspects (i.e. operational continuity, sensitivity of data) tend to dominate the assessment process, systematically leading to the classification of the arrangement as critical.

→ **Assess Criticality of Outsourced Functions:** Evaluate each Outsourced function against the criticality criteria and document the outcome. Define validation rules and approval steps for the assessment. This assessment should be completed at an early stage of the outsourcing lifecycle, prior to entering the intended arran-

gement, as it determines whether a prior notification to the Regulator is required. Reassess periodically and upon trigger events that could materially change the assessment.

→ **Classify Outsourced Functions:** Categorize Outsourced functions as Critical or Important, or as non-critical where appropriate. Ensure classifications feed into monitoring cadence, contractual requirements and exit planning.

These assessments should not be limited to the function, activity or process level. Where a single provider supports multiple functions or where several entities rely on the same provider, the organization should perform an **entity-level assessment** to capture concentration and systemic risk across the legal entity. Entity-level assessments should:

→ Identify all services and subsidiaries entities that depend on the Service provider.

→ Assess the degree of ICT interconnectedness and potential single points of failure across systems, upstream and downstream processes.

→ Quantify concentration exposure (for example, percentage of Critical or Important Functions, supported non-critical activities and processes, number of entities affected, transaction volume or other value metrics).

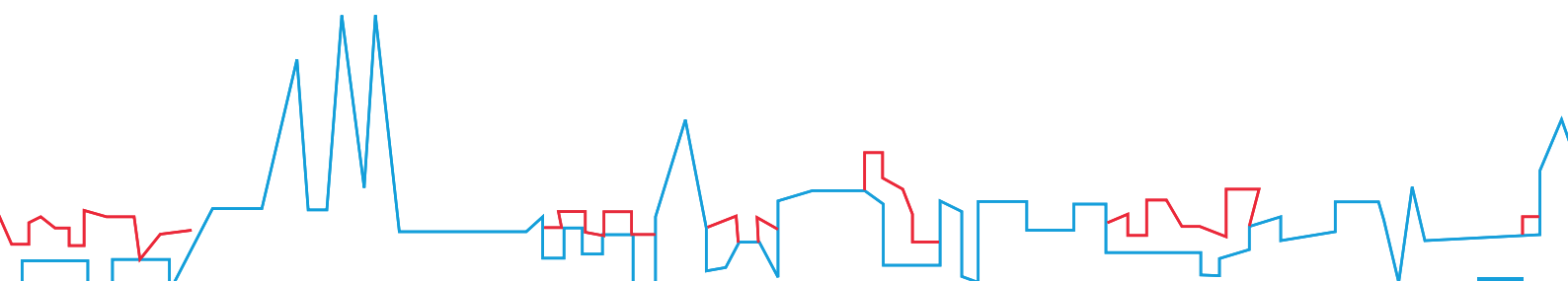
→ Evaluate cross-entity contagion scenarios (operational, ICT, financial, regulatory and reputational impacts arising from service disruption or failure).

→ Include governance and escalation arrangements specific to multi-entity dependencies.

→ Analyze the potential cascading effects of ICT disruption across interconnected systems and services chains.

→ Feed into the Outsourcing inventory, risk rating and monitoring cadence; and

→ Inform contractual requirements, exit planning and capital/contingency provisioning.



If the entity-level assessment indicates high concentration risk, the organization should consider strengthening its oversight, conducting enhanced due diligence, performing targeted stress tests and accelerating exit-plan readiness. Document the rationale for chosen mitigation measures. In addition, the substitutability and reliance on the provider should be reassessed periodically, with appropriate measures taken to diversify where feasibility and proportionate.

RESULT: OUTSOURCING INVENTORY / REGISTER

Maintain a centralized and continuously updated outsourcing inventory (also referred to as an outsourcing register) capturing all outsourcing arrangements in accordance with CSSF Circular 25/883, Point (53).

The register should:

- Include all outsourcing arrangements, irrespective of criticality
- Clearly distinguish between the arrangements supporting Critical or important functions and those relating to non-critical functions and activities
- Be maintained at entity and, where applicable, consolidated level
- Be readily available to the CSSF upon request, (CSSF Circular 25/883, point (56)).

MINIMUM INFORMATION REQUIREMENTS

In line with the CSSF Circular 25/883, point (54) each outsourcing entry should include at least:

- Unique identifier/reference
- Description of the outsourced function
- Classification (critical/important vs non-critical) and justification
- Service provider details (name, legal identifier, group affiliation)
- Location of service provision and data
- Personal data indicator (if applicable)

- Key contractual dates (start, renewal, termination and notice period)
- Date of last criticality assessment

ADDITIONAL REQUIREMENTS FOR CRITICAL OR IMPORTANT FUNCTIONS

For Critical or Important Outsourcing arrangements, the register should also include, in accordance with the CSSF Circular 25/883, point (55):

- Risk assessment outcomes
- Approval body
- Audit details
- Sub-outsourcing details
- Substitutability assessment
- Exit options or alternatives
- Estimates cost
- Notification date to the competent authority

GOVERNANCE AND RISK MANAGEMENT ROLE

The outsourcing register constitutes a key governance and supervisory tool, enabling:

- A consolidated overview of outsourcing arrangements
- Monitoring of concentration and dependency risks
- Support with management decision-making
- Transparency towards supervisory authorities

It should be periodically reconciled with contractual repositories, vendor/accounting records and ICT inventories to ensure completeness and accuracy.

2.2. DUE DILIGENCE AND SERVICE RISK ASSESSMENT

Entities should perform a documented due diligence and service level risk assessment prior to entering into an outsourcing arrangement and an ongoing basis, in line with CSSF requirements in the CSSF Circular 25/883, points (65-70).

ACTION ITEMS

→ **Providers Due Diligence:** Conduct proportionate due diligence on potential Service providers aligned with the inherent risk profile of the Outsourcing arrangement. For intra-group arrangements, assess capacity, expertise and any change in scope.

→ **Evaluate Reputation:** Consider preliminary research (i.e. digital footprint, public information), sanctions and adverse media screening, client references, financial stability indicators, legal and compliance history, certifications (for example, ISO, SOC 2), industry reputation and operational site reviews.

→ **Perform Risk Assessment:** Entities should consider performing a comprehensive and documented risk assessment before entering an Outsourcing arrangement. The assessment should be proportionate to the nature, scale and complexity of the arrangement, integrated into the entity's risk framework and reviewed regularly or upon material change. The assessment shall reflect the inherent risk level, mitigations actions and residual risk level,

the use methodology should be in line with the entity's enterprise risk management principles.

KEY RISK CATEGORIES TO ASSESS, NOT LIMITED TO

Operational Risk – Potential disruptions to business continuity or service delivery.

Compliance Risk – Risk of failing to comply with applicable laws, regulations, regulatory requirements, or internal policies.

Legal Risk – Uncertainties arising from contractual terms or jurisdictional issues.

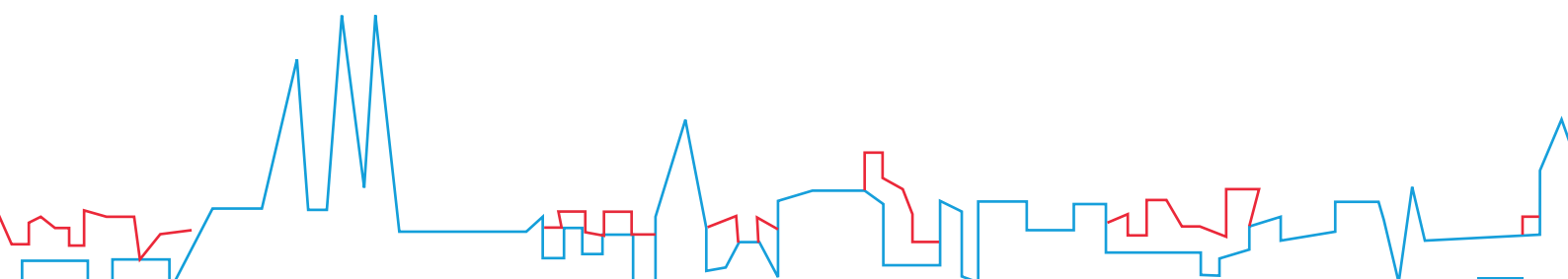
Reputational Risk – Potential damage to the organization's public image or stakeholder trust.

Concentration Risk – Over-reliance on a single provider or geographic region.

Information Security and ICT Risk – Risks affecting the confidentiality, integrity, availability, authenticity, security, and resilience of information assets, ICT systems, applications, infrastructure, and technology-enabled processes, including cyber-attacks, system outages, data breaches, and failures of supporting ICT services.

Exit Strategy Risk – Challenges in transitioning services back in-house or to another provider or back in-house (i.e. in-scope migration assistance, knowledge transfer, data migration constraints).

Organisation should also assess the **service provider's risk profile**, including its financial health, resilience, and ability to comply with applicable laws and standards.



Stress Testing: Pursuant to CSSF Circular 25/883, point (67), the pre-outsourcing risk analysis must, where appropriate, incorporate scenario-based assessments of possible risk events — including high-severity operational risk events — with particular emphasis on arrangements supporting a critical or important function. This scenario analysis should evaluate the potential impact of failed or inadequate service delivery across the standard operational risk failure categories, namely process, systems, people, and external events, and must be fully documented together with its results. The circular applies to a proportionality

standard: small entities may rely on qualitative scenario assessments, whereas other in-scope entities are expected to adopt a more sophisticated methodology, incorporating internal and external loss data where available to calibrate the scenarios. In all cases, the analysis must culminate in a reasoned estimate of the extent to which the outsourcing arrangement increases or decreases the entity's overall operational risk profile and should inform the design and adequacy of the corresponding business continuity and exit plans for the arrangement in question.

2.3. CONTRACTUAL REQUIREMENTS AND SERVICE LEVEL AGREEMENT (SLA)

Outsourcing arrangements must be formalized through a written agreement clearly defining the rights and obligations of both parties in the CSSF Circular 25/883, points (65-70).

ACTION ITEMS

a. Draft Contracts: Ensure contracts include at least:

- Function Description: Clear outline of the outsourced function.
- Duration & Notice: Start and end dates, plus notice periods.
- Governing Law: Specification of applicable law.
- Financial Obligations: Details of financial responsibilities.
- Sub-Outsourcing Conditions: Rules for sub-outsourcing, especially for critical functions.

- Service Locations: Regions for service provision and data processing, with change notification requirements.
- Data Provisions: Accessibility, integrity, privacy, and safety of data.
- Performance Monitoring: Right to continuously monitor service provider performance.
- Service Levels: Specific performance targets for monitoring (such as availability, response times, error rates, reporting timeliness etc.).
- Reporting Obligations: Requirements for the service provider to report significant developments.
- Insurance Requirements: Mandatory insurance against certain risks.
- Contingency Plans: Requirements for business continuity plans.
- Data Access in Insolvency: Access to data if the service provider becomes insolvent.
- Cooperation with Authorities: Obligation to cooperate with relevant authorities.
- Audit Rights: Unrestricted Rights to inspect and audit the service provider.
- Termination Rights: Clearly defined rights for termination.



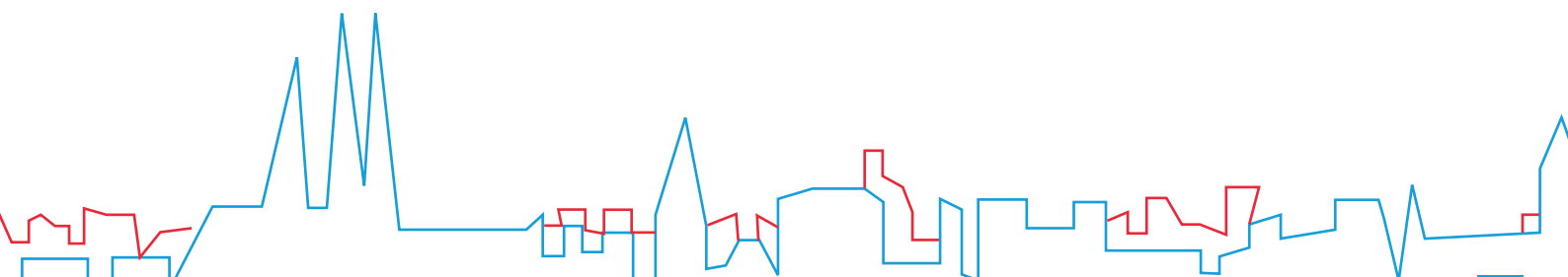
When contracts are drafted at group or consolidated level, organizations should consider maintaining adequate back-to-back provisions to help preserve local regulatory compliance.

B. DEFINE RESPONSIBILITIES

Outline clear responsibilities of both parties. This should include data treatment and protection measures and a clear description of responsibilities in the event of termination of the services.

C. REVIEW CONTRACTS

Where applicable, review and update contracts to reflect changes in regulatory requirements and business needs.



3

REGULATORY REQUIREMENTS AND MONITORING FRAMEWORK



Entities are required to monitor outsourcing arrangements on an ongoing basis, applying a risk-based approach with particular focus critical or important functions in the CSSF Circular 25/883, point (104).

ACTION ITEMS

3.1. Designate a Senior Management representative responsible for Outsourcing Governance:

Organizations should consider appointing a Senior Management member or team as the Outsourcing Governance Lead. This role should be explicitly tasked with oversight of the Outsourcing governance framework and with maintaining up-to-date documentation, **(CSSF Circular 25/883, points (33-36))**. The evidence of approval, for new critical arrangements, should be documented and retained.

3.2. Set up a Cross-Functional team: Given the multifaceted impact of Outsourcing arrangements, assemble representatives from operations, legal, compliance, IT, risk and procurement. These teams may operate as committees or working groups depending on entity size, **(CSSF Circular 25/883, point (30))**.

3.3. Outsourcing Guidelines Summary:

Develop summarized guidelines for business owners that outline key lifecycle steps, KPI reporting expectations, incident escalation triggers and considerations that may lead to termination. Keep this summary concise and practical, **(CSSF Circular 25/883, points (39-40))**.

3.4. Subcontracting Chain Monitoring:

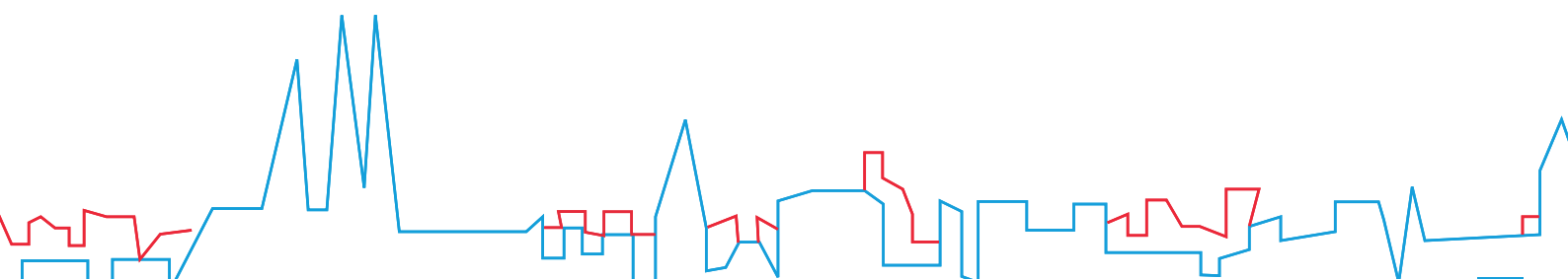
Financial institutions should consider monitoring the subcontracting chain on a continuous, risk-based basis to help ensure delegated activities remain compliant and resilient, **(CSSF Circular 25/883, point (70))**. Monitoring should cover direct Service providers and material sub-processors or affiliates that perform Critical or Important Functions, Integrate monitoring into the Outsourcing inventory and

entity-level assessments. A non-exhaustive list of monitoring requirements is sub-supplier register updates, change notifications, concentration metrics, operational KPIs from sub-processors, targeted control testing etc.

3.5. Implement Monitoring Tools: Leverage automated tools for KPI tracking and performance dashboards. Define a KPI catalog and additional oversight elements for Critical or Important Functions to enable standardized reporting **(CSSF Circular 25/883, point (108))**.

3.6. Conduct Periodic Reviews: Schedule regular performance reviews with Service providers focusing on trends, incidents and remediation progress. Adjust monitoring cadence based on risk and concentration metrics. The review conclusion shall be formally documented and retained as evidence of the assessment performed and the decisions taken where applicable.

3.7. Audit Review: Audit reviews should be practical, evidence-based and scheduled proportionately to risk, **(CSSF Circular 25/883, points (51-52))**. Define scope, frequency and evidence requirements in contracts and ensure providers can operationally support audits. Document and report findings to senior management and track remediation actions to closure, **(CSSF Circular 25/883, points (88-90))**.



3.8. Report Findings: Document and report findings to Senior management and ensure appropriate remediation is in place. Track the action items to ensure timely closure. **(CSSF Circular 25/883, points (33-34) and (106)).**

3.9. Risk-based and proportionate monitoring cadence: Outsourcing arrangements often combine regulatory sensitivity, low transaction volumes and high legal/technical complexity, particularly for Specialized PSFs. Monitoring cycles should therefore be risk-based, proportionate and include both

frequent operational checks and deeper periodic assurance activities such as, but not limited to: monthly operational dashboard (i.e. Focus on SLA attainment, incidents, open remediations items), quarterly¹ performance and compliance review (review KPI trends, regulatory filing timeliness and control failures), trigger-based deep dive (ad-hoc on incidents, provider financial events or regulatory changes), annual independent assurance, on-site or virtual due diligence or thematic reviews and resilience tests.

¹. As a common practice.

4

TRAINING AND COMMUNICATION



TRAINING TOPICS AND AUDIENCE

Provide targeted training for Business owners, Procurement, Compliance, IT and Senior management. Topics should include Outsourcing lifecycle governance, risk assessment, incident escalation, data protection and exit planning. Tailor content to role responsibilities, **(CSSF Circular 25/883 points (33-35) and (36))**.

CADENCE AND DELIVERY

Offer onboarding training for new staff, annual refresher sessions and ad-hoc briefings after significant incidents or regulatory updates. Use a mix of formats such as workshops, e-learning modules and table-top exercises.

COMMUNICATION CHANNELS

Maintain clear internal communication channels for reporting incidents and escalation. Provide concise guidance documents and quick reference checklists for business owners and operational teams.



5

AUDIT, REPORTING, AND CONTINUOUS IMPROVEMENT



Effective management of outsourcing arrangements in compliance with CSSF Circular 25/883 requires robust audit, reporting, and continuous improvement practices. This section outlines the key strategies and examples for integrating these practices into the organizational framework.

5.1. INTEGRATE OUTSOURCING REVIEWS

To ensure ongoing compliance with **CSSF Circular 25/883**, it is essential to integrate outsourcing reviews into the internal audit cycle and compliance monitoring plan. This integration helps in systematically assessing the effectiveness and adherence to regulatory requirements of outsourcing arrangements, (**CSSF Circular 25/883**, points (51-52)).

5.2. IMPLEMENTATION STRATEGIES

Leverage existing audit frameworks to streamline reviews. Use dedicated checklists for Outsourcing compliance and combine provider self-assessments with independent assurance reports and targeted testing.



6 OUTSOURCING POLICY AND PROCEDURE



OUTSOURCING POLICY (THE “WHAT”)

The Outsourcing policy should define the strategic framework, governance principles and approval thresholds for Outsourcing arrangements. The policy should be approved by the management body and reviewed periodically.

PROCEDURES (THE “HOW”)

Document procedures that operationalize the policy include steps for initiating Outsourcing, due diligence checklists, contract approval workflows, monitoring requirements and exit planning. Ensure procedures are accessible to Business owners and relevant support functions.

ROLES AND RESPONSIBILITIES (THE “WHO”)

Define clear roles for Business owners, Procurement, Compliance, IT and the Outsourcing Governance Lead. Ensure responsibilities for monitoring, reporting and escalation are documented and understood.



OUTSOURCING

7

MANAGING INTRA-GROUP OUTSOURCING ARRANGEMENTS



Intragroup outsourcing arrangements are subject to the same regulatory framework and requirements as outsourcing to external providers (CSSF Circular 25/883, point (11)).

Intra-group outsourcing arrangements, while often perceived as less risky due to the internal nature of the relationship, require the same level of diligence and oversight as external outsourcing arrangements. The CSSF circular 25/883 emphasizes the importance of managing these arrangements effectively to ensure compliance and operational efficiency. Below are key practices for managing intra-group outsourcing arrangements:

7.1. MAINTAIN A CLEAR OPERATING MODEL

Document the intra-group operating model at legal entity level, identifying affiliates involved in the supply chain and any chain Outsourcing. Record intra-group arrangements in the Outsourcing inventory and consider group-level concentration risk.

7.2. ENHANCE TRANSPARENCY AND DEFINE REPORTING LINES IN THE CONTEXT OF OVERSIGHT AND ESCALATION

Transparency is crucial in intra-group outsourcing. Clearly document the roles and performance expectations for all intragroup services. This includes defining reporting lines to ensure accountability and effective communication. Regular updates and transparent reporting mechanisms help in maintaining clarity and trust between the entities involved.

7.3. APPLY EQUAL STANDARDS

Intragroup arrangements should be subject to the same contractual, oversight and standards² as external outsourcing arrangements. This ensures consistency in service quality and risk management. Applying equal standards helps in identifying and mitigating risks that might otherwise be overlooked due to the internal nature of the relationship. It also ensures that the operating model remains in compliance with regulatory and risk management expectations at all time (CSSF Circular 25/883, point (7)).

2. Including but not limited to appropriate expertise and sufficient human and technical resources as well as the implementation of controls measures and practices which enable to meet the local entity's risk and regulatory requirements as well as the market standards.

7.4. CONTRACTUAL ARRANGEMENTS

Create comprehensive contractual agreement for all intragroup outsourcing arrangements. This should include an intra-group master agreement including the appropriate terms and conditions applicable to outsourcing, as well as a memorandum of understanding or a service agreement detailing the roles, responsibilities, service level agreements (SLAs) including appropriately defined KPIs³, and service review schedules.

This aligns with the requirement that outsourcing arrangements must be formalized in a written agreement clearly allocating rights and obligations, (CSSF Circular 25/883, Chapter 4, point (76)).

Proper documentation also supports compliance with the documentation and record-keeping requirements, (CSSF Circular 25/883, points (53-58)).

7.5. CONDUCT PERIODIC REVIEWS

OVERSIGHT REVIEW

Schedule periodic oversight activities for the purpose of monitoring and tracking performance, addressing and escalating identified issues and agreeing upon the required remediation actions which should be tracked afterwards.

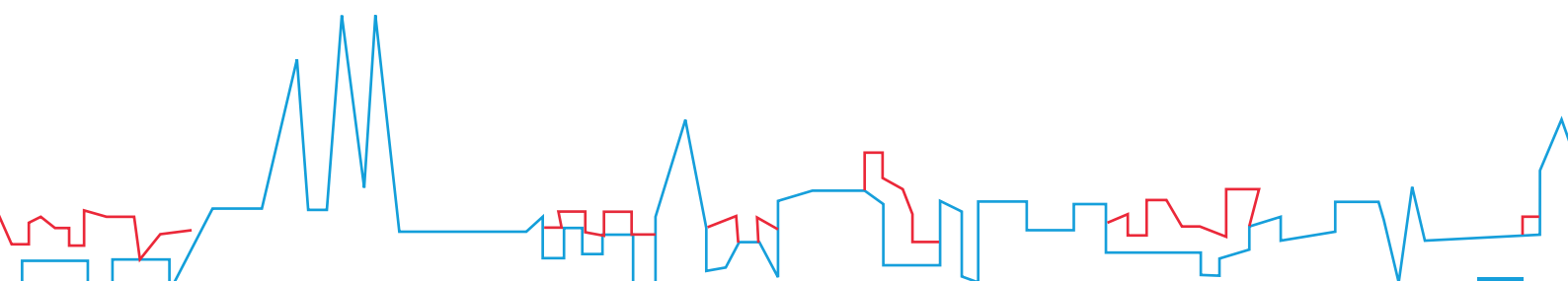
This reflects the requirement to monitor outsourcing arrangements on an ongoing basis using a risk-based approach, (CSSF Circular 25/883, point (104)).

INDEPENDENT REVIEWS

Schedule periodic reviews of intragroup outsourcing arrangements by an internal audit team or an external consultant. Independent reviews provide an objective assessment of the arrangement's effectiveness and compliance with regulatory requirements. They also help in identifying areas for improvement and ensuring continuous enhancement of the outsourcing practices.

The organization should ensure that the on-site due diligence questionnaire covers the specifics of the processes that are outsourced. In line with CSSF Circular 25/883, points (51-52).

³. When defining KPIs, they should be measurable by using a combination of quantitative or qualitative criteria when relevant. Some services may not be subject to KPIs, nevertheless the entity should define quality or success metrics in order to ascertain the services are provided according to the agreed standards alternatively.



7.6. EXIT STRATEGY

Develop and maintain an exit strategy for critical intragroup outsourcing arrangements. The strategy should outline the preferred exit option⁴ and the associated steps to be taken in the event of termination or failure of the arrangement. An effective exit strategy ensures operational resilience and minimizes disruption to operations in the context of termination, in line with CSSF Circular 25/883, point (14) and points (111-112).

KEY ELEMENTS

Owner and triggers: Assign a named exit owner and define clear exit triggers such as repeated SLA breaches, insolvency, material regulatory action or unacceptable concentration risk.

Operational runbooks: Maintain step-by-step playbooks for data extraction, secure transfer, system access revocation, knowledge transfer and interim manual processes.

Data inventory and access: Keep an up-to-date inventory of data types, locations,

backups and access credentials; define secure extraction and verification methods.

Fallback options: Identify alternate providers or in-house options and confirm basic onboarding readiness or pre-contract terms where feasible.

Contractual safeguards: Include transition assistance, insolvency data access, data escrow and back-to-back flow-down clauses in contracts.

Testing and cadence: Test the plan regularly: tabletop exercises (biannual), partial simulations (annual) and full-dress rehearsals every 2–3 years; require remediation closure within a defined timeframe after each test.

Acceptance criteria: Define simple success metrics such as data completeness, RTO/RPO targets, reconciliation tolerances and timely regulatory filings.

Evidence and governance: Maintain versioned exit plans, test reports and an action log; escalate failures to senior management per defined timelines.

⁴. To alternate service provider, repatriation or discontinuation.

8

OUTSOURCING MONITORING CENTRALIZED AT GROUP LEVEL

(CSSF Circular 25/883, point (13-14))



CENTRALIZED MONITORING APPROACH

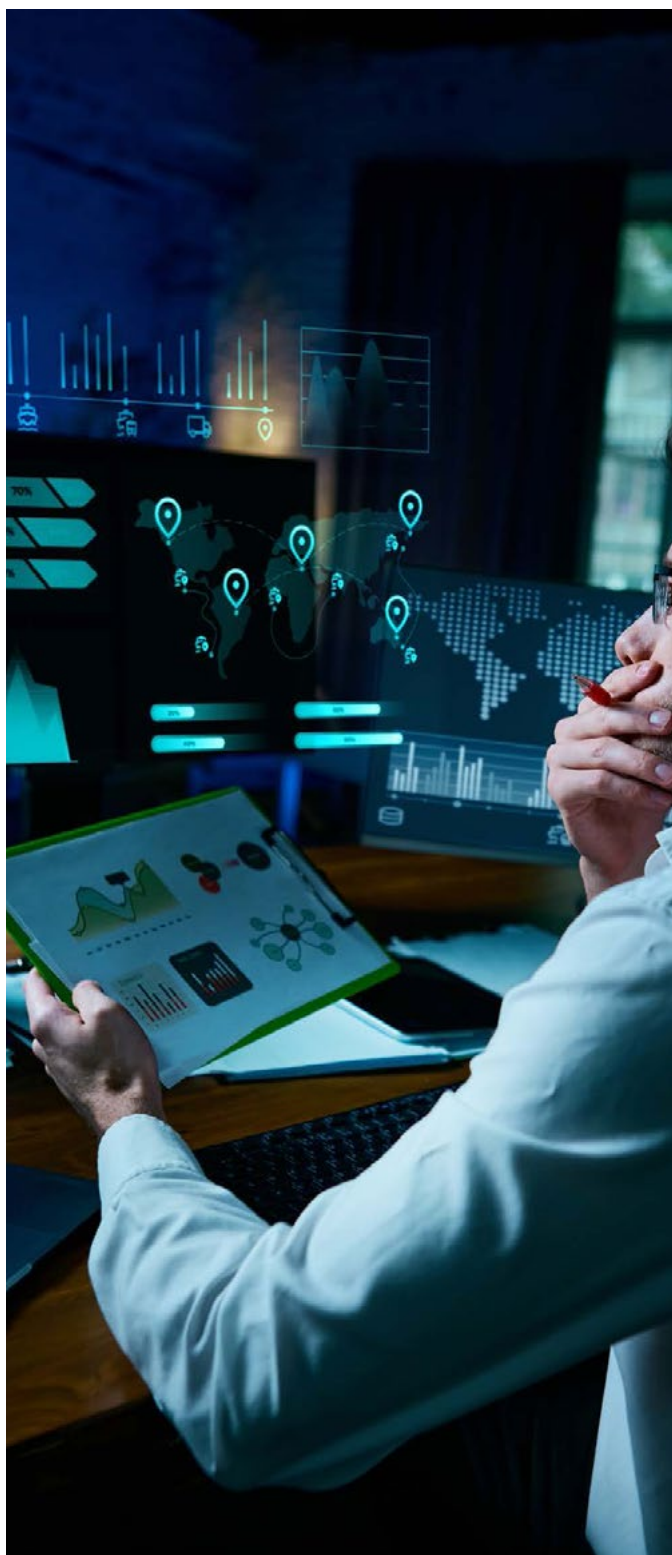
Where oversight is centralized at group level, ensure local entities receive sufficient information to assess local compliance and risk. Centralized monitoring can promote harmonization but local review against local regulatory expectations remains important.

REPORTING AND LOCAL REVIEW

Organizations may receive annual reports summarizing risk assessments, performance monitoring and audit findings. Local entities should review these reports against their local risk and regulatory expectations and address any identified gaps.

MANAGEMENT BODY ASSESSMENT

The management body of the local entity should assess the adequacy of group-level reports for governance and risk management purposes and request additional information or local controls where necessary.



DISCLAIMER

These guidelines are provided for informational purposes and are intended to offer a general overview of key principles and prevailing market practices.

They do not constitute, and should not be construed as, legal, regulatory, or compliance advice. The content herein does not create any rights or obligations and is not intended to replace, amend, or interpret any applicable laws, regulations, or binding requirements.

Under all circumstances, the provisions of the ESAs⁵ Guidelines on Outsourcing Arrangements and the relevant CSSF Circulars shall take precedence and remain fully applicable.

⁵. European Supervisory Authorities including EBA – European Banking Authority, ESMA – European Securities and Markets Authority, EIOPA – European Insurance and Occupational Pensions Authority.



LPEA 

