LUXEMBOURG ALTERNATIVE ADMINISTRATORS ASSOCIATION

LPEA

OUTSOURCING GUIDELINES

BASED ON CSSF CIRCULAR 22/806

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

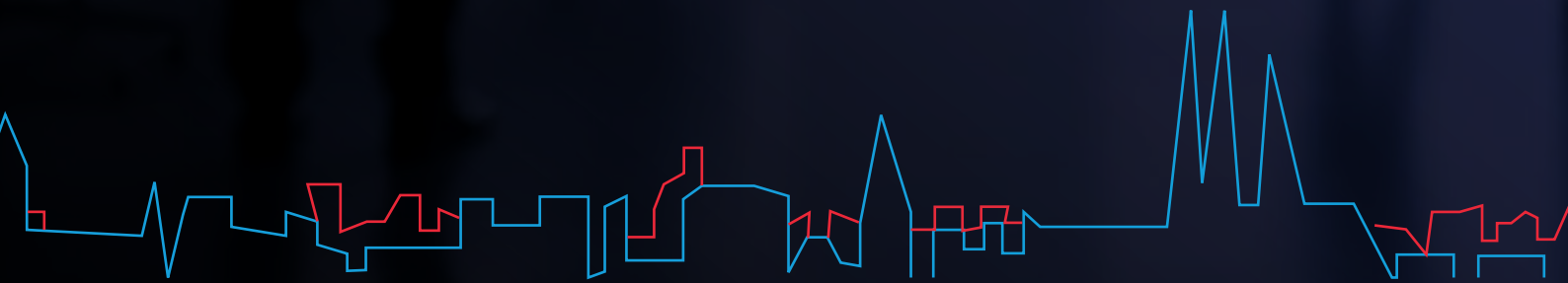


TABLE OF CONTENT

About L3A

The Luxembourg Alternative Administrators Association ("L3A") is the leading representative body for fund and corporate administrators of alternative assets in Luxembourg. Founded in June 2004 by 15 pioneering members, the association is dedicated to promoting Luxembourg's alternative investment industry and advancing the professional interests of its members.

Our members deliver our mission through their work on our 5 so-called 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 recognized voice of our profession, we engage with authorities through participation in commissions and working groups, and maintain strong ties with government bodies, professional organizations, and Chambers of Commerce.

Our membership is made up of 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 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 Circular CSSF 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 involved in outsourcing decisions. 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.

NON BINDING NATURE

The recommendations in this white paper are intended to reflect prevailing market practice and to support compliance with CSSF Circular 22/806. They do not create new legal obligations and should be adapted to each entity's size, complexity, and risk profile.

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.

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.

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., audit, travel, network infrastructure). While CSSF Circular 22/806 and EBA guidelines provide the baseline, add any 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. Include functions that are not business driven or not subject to direct regulation such as human resources, procurement and finance where applicable.

➔ **Define Criticality:** Define the organization's assessment of what the criteria are to determine the criticality of the outsourced 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. 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 institution should perform an **entity level assessment** to capture concentration and systemic risk across the legal entity. Entity level assessments should:

➔ identify all services and legal entities that depend on the Service provider;

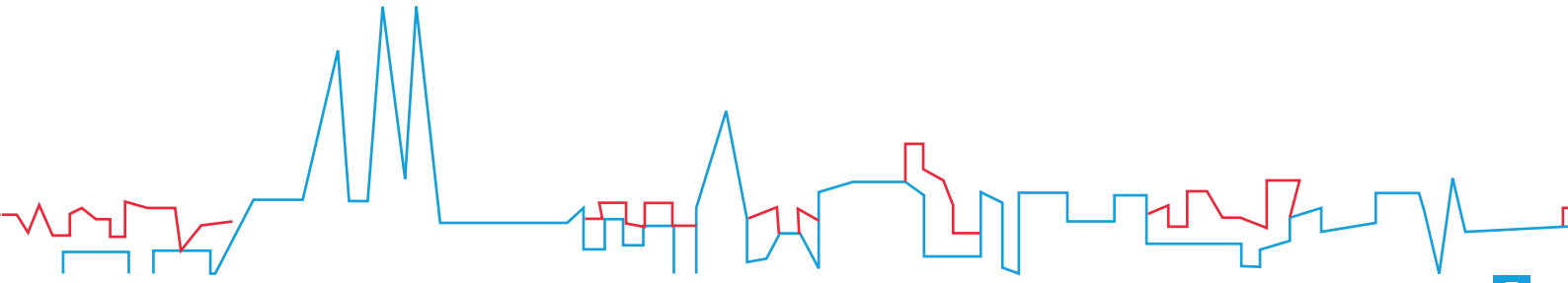
➔ quantify concentration exposure (for example, percentage of Critical or Important Functions, number of entities, volume or value metrics);

➔ evaluate cross entity contagion scenarios (operational, financial, regulatory and reputational);

➔ include governance and escalation arrangements specific to multi entity dependencies;

➔ 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 institution should consider increasing oversight, conducting deeper due diligence, running targeted stress tests and accelerating exit-plan readiness. Document the rationale for chosen mitigation measures.

RESULT: OUTSOURCING INVENTORY

Maintain a living Outsourcing inventory that lists all Outsourcing arrangements, their classification, owners, key contractual terms and monitoring cadence. The inventory should clearly delineate between delegation and Outsourcing arrangement and highlight functions that are neither business driven nor regulatory in nature.

2.2. DUE DILIGENCE AND SERVICE RISK ASSESSMENT

ACTION ITEMS

→ **Research Providers:** 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 (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.

KEY RISK CATEGORIES TO ASSESS

Operational Risk – Potential disruptions to business continuity or service delivery.
Compliance Risk – Risk of breaching legal or regulatory obligations.
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 – Threats to data confidentiality, integrity, and availability.
Exit Strategy Risk – Challenges in transitioning services back in-house or to another provider.
Entities 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:** 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.

2.3. CONTRACTUAL REQUIREMENTS AND SERVICE LEVEL AGREEMENT (SLA)

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.
➔ nsurance 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: 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

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.

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.

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.

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. 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 are 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 for non-critical arrangements and additional oversight elements for Critical or Important Functions to enable standardized reporting.

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.

3.7. Audit Review: Audit reviews should be practical, evidence-based and scheduled proportionately to risk. 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.

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.

3.9. Review-cycle specific to Specialized PSFs: Specialized PSFs often combine regulatory sensitivity, low transaction volumes and high legal/technical complexity. 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 (focus on SLA attainment, incidents, open remediations items), quarterly 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.

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.

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 tabletop 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 22/806 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 22/806, 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.

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

Document procedures that operationalize the policy, including 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

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.

7 MANAGING INTRA-GROUP OUTSOURCING ARRANGEMENTS

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 22/806 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 intra-group 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 standards[1] 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.

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

---

1. 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.

KPIs[2], and service review schedules. Proper documentation serves as a reference point and ensures that all parties are aligned to expectations and obligations.

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.

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 specificities of the processes that are outsourced.

7.6. EXIT STRATEGY

Develop and maintain an exit strategy for critical intragroup outsourcing arrangements. The strategy should outline the preferred exit option[3] 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.

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.

---

2. When defining KPIs, they should be measurables 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.

3. To alternate service provider, repatriation or discontinuation.

8 CASE OF OUTSOURCING MONITORING IS CENTRALIZED AT GROUP LEVEL

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.

9 CONCLUSION

This white paper shares best practices and practical guidance to help support compliance with CSSF Circular 22/806. It is intended as a reference to help organizations strengthen Outsourcing governance and operational resilience. The guidance is non binding and does not replace, override or amend the Circular or any regulatory requirement.

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.

LUXEMBOURG
ALTERNATIVE
ADMINISTRATORS
ASSOCIATION

LPEA