FINANCE & TECHNOLOGY LUXEMBOURG

DUE DILIGENCE CHARTER

A Voluntary Industry Framework for the Luxembourg Financial and Insurance Ecosystem

PRINCIPLES GUIDANCE

Finance & Technology Luxembourg

Final Version - September 2026

1. Introduction

What this Charter is – and what it is not

This Charter is a code of conduct. It sets out the behaviours that adhering organisations undertake to apply when they request, provide or assess due diligence information. Adherence is open to any organisation, whether or not it is a member of FTL. It creates no contractual obligation between the parties, replaces no regulatory requirement, and confers on no organisation any certification, label or presumption of compliance.

The Charter is accompanied by a package with two components: a list of the documents and evidence a provider can make available, and a repository of the questions with the regular justification clients commonly ask. The repository is a tool that allows an ICT service provider to assemble, once, a complete package answering the questions its clients ask, instead of answering a differently worded questionnaire for every request.

The repository is not a standard, and it is not a template to be sent as it stands. Neither the Charter nor the repository entitles a client to require that every question be answered irrespective of the risk carried by the engagement, of the principle of proportionality, or of the type of service subscribed. The client remains responsible for scoping its own request; the provider remains responsible for the accuracy and completeness of its answers.

Finance and Technology Luxembourg encourages the signatories of this Charter to also make use of this package.

FTL's commitment, publication and adherence

This Charter is published on the FTL website. Adherence is voluntary: an organisation adheres by signing the Charter, and FTL may publish the list of adhering organisations.

FTL's commitment is limited to maintaining the Charter and its package and to making them available to adhering organisations and to the market. FTL is neither a party to, nor an arbitrator of, the due diligence exchanges conducted between adhering organisations and their clients.

FTL reserves the right to withdraw the adherence of any organisation that does not respect the principles of this Charter, and to remove it from the list of adhering organisations.

© 2026 Finance & Technology Luxembourg a.s.b.l. with registered office at 7, Rue Alcide de Gasperi, L-1468 Luxembourg, registered with RCS Luxembourg under number F7436. All rights reserved.

2. Due Diligence and Risk Assessment – Definitions

Due diligence

Due diligence is a formal process of collecting and verifying information to ensure compliance with legal, regulatory, and contractual obligations, particularly in the context of third-party engagements.

Under DORA (EU Regulation 2022/2554), it is required for pre-contractual assessments and ongoing monitoring of ICT third-party providers and supports obligations such as the Register of Information (Art. 28–30) and third-party risk management.

Risk assessment

Risk assessment is the subsequent evaluative process in which that information is analysed to identify, measure, and determine the acceptability of risks, including defining mitigation measures.

Under DORA and related frameworks (e.g., EBA Outsourcing Guidelines, NIS2, GDPR Art. 32), entities must perform risk-based assessments, including classification of Critical or Important Functions (CIFs) and evaluation of operational and ICT risks.

© 2026 Finance & Technology Luxembourg a.s.b.l. with registered office at 7, Rue Alcide de Gasperi, L-1468 Luxembourg, registered with RCS Luxembourg under number F7436. All rights reserved.

3. Principles

Principle 1: Voluntary Industry Framework

> ***This Charter establishes a voluntary, non-binding reference framework to standardize, streamline, and proportionately align ICT due diligence interactions between financial-sector clients and ICT service providers, preserving each party's regulatory accountability and contractual autonomy.***

This Charter, issued by Finance and Technology Luxembourg association and its members, establishes a voluntary, non-binding reference framework to standardise, streamline, and proportionately align ICT due diligence interactions between financial-sector clients and ICT service providers, preserving each party's regulatory accountability and contractual autonomy.

This Charter serves as a voluntary, non-binding reference framework to align and streamline ICT due diligence across the Luxembourg financial and insurance ecosystem (hereafter, "the ecosystem"). It does not replace regulatory obligations, contractual agreements, or institution-specific risk methodologies, nor does it assign or transfer regulatory accountability. Instead, it provides a common vocabulary and shared principles that committed organisations may voluntarily adopt to reduce friction, improve consistency, and foster more constructive client-provider dialogues.

The initiative recognises that market participants operate under varying maturity levels, service criticalities, and internal governance structures. Accordingly, this Charter is intentionally non-prescriptive, allowing organisations to apply its principles proportionately while retaining full autonomy over their decision-making processes, risk appetites, and contractual arrangements. Its value lies in creating a predictable, transparent baseline that both the ecosystem clients and ICT service providers can reference to navigate increasingly complex regulatory and operational landscapes.

Principle 2: Proportionality & Risk-Based Scoping

> ***Parties shall tailor the depth, breadth, and frequency of due diligence requests to the criticality of the supported function, service context, and actual risk exposure, and avoid uniform or maximalist approaches.***

Effective due diligence must be calibrated to the actual criticality, complexity, and risk exposure of the service relationship, rather than applying uniform or maximalist expectations across all engagements. This principle aligns with the proportionality framework embedded in DORA and supervisory expectations, recognising that services supporting CIFs warrant deeper scrutiny, while lower-risk or non-CIF arrangements require proportionate, targeted assessments. Both clients and service providers are expected to explicitly consider factors such as service materiality, data sensitivity, subcontracting complexity and historical performance when determining the scope and intensity of due diligence exercises.

Clients are encouraged to avoid generic, blanket questionnaires and instead anchor requests to clearly defined service boundaries and risk rationales. Service providers, in turn, should structure their due diligence packages to accommodate tiered expectations, enabling efficient responses that scale with the relationship's criticality. By jointly embracing risk-based scoping, both parties reduce operational fatigue,

© 2026 Finance & Technology Luxembourg a.s.b.l. with registered office at 7, Rue Alcide de Gasperi, L-1468 Luxembourg, registered with RCS Luxembourg under number F7436. All rights reserved.

improve the relevance of the information exchanged, and ensure rigorous oversight is reserved for where it matters most.

Principle 3: Precision & Mutual Transparency

> ***All requests and responses shall be explicitly scoped, purpose-driven, and limited to information material to the contractual and regulatory objective, with a clear distinction between mandatory regulatory requirements, contractual obligations, and internal policies.***

Clear articulation of purpose, scope and regulatory or contractual basis is essential for efficient and trustworthy due diligence exchanges. Clients are expected to clearly state the objective of each exercise (e.g., pre-contractual assessment, ongoing review), define the precise service perimeter and indicate whether requests stem from binding regulatory requirements, contractual rights or internal policies. This transparency enables service providers to accurately prioritise responses, mobilise the right internal stakeholders and avoid unnecessary duplication or overly engineered disclosures.

Service providers, in turn, should respond with structured, accurate and verifiable information, explicitly flagging any limitations, assumptions or areas where disclosure is restricted. Both parties should distinguish between corporate-level and service-specific information, avoid speculative or forward-looking assertions presented as fact and maintain open channels for clarification without resorting to adversarial or iterative back-and-forth. Precision and transparency reduce ambiguity, accelerate decision-making and strengthen mutual confidence in the due diligence process.

Principle 4: Recognition & Reuse of Evidence

> ***Parties should prioritise the reuse of existing documentation, independent assurance reports, and recognised certifications, minimise redundant requests, and support delta-based updates over full resubmissions.***

The efficient reuse of existing documentation, independent assurance reports and recognised certifications is a cornerstone of sustainable due diligence practices. Both parties should prioritise accepting valid, in-scope evidence – such as ISO 27001, SOC reports, or prior due diligence responses – rather than repeatedly requesting information that has already been assessed or validated by reputable third parties. Service providers are expected to maintain structured, up-to-date evidence repositories with clear metadata indicating scope, validity periods and disclosure conditions, while clients should establish internal processes to validate and appropriately leverage such documented evidence.

Reuse does not imply reduced oversight; rather, it shifts focus from repetitive collection to meaningful verification. Where existing evidence is outdated, narrowly scoped, or misaligned with the service in question, parties should pursue targeted delta reviews or supplementary clarifications rather than full resubmissions. By systematically favouring evidence reuse and version-controlled updates, the ecosystem reduces administrative burden, accelerates onboarding and renewal cycles, and preserves analytical capacity for higher-value risk assessment.

© 2026 Finance & Technology Luxembourg a.s.b.l. with registered office at 7, Rue Alcide de Gasperi, L-1468 Luxembourg, registered with RCS Luxembourg under number F7436. All rights reserved.

Principle 5: Controlled Transparency & Data Protection

> ***Information sharing shall employ tiered disclosure mechanisms (e.g., executive summaries, redacted documents, controlled-access reviews, NDAs) to balance legitimate information needs with the protection of intellectual property, security configurations and commercial confidentiality.***

Balanced information sharing must reconcile clients' legitimate need for oversight with providers' obligations to protect intellectual property, security configurations and commercially sensitive data. The Charter promotes a controlled transparency model that utilises tiered disclosure mechanisms – including executive summaries, redacted documents, controlled-access portals, NDAs and on-site or virtual review environments – rather than demanding full document handovers by default. Clients are expected to justify the depth of access required, while service providers should clearly articulate the rationale for any restrictions and propose proportionate alternative verification methods where feasible.

This approach mitigates security and confidentiality risks without compromising regulatory or contractual oversight rights. Both parties should maintain clear internal access controls, limit circulation to authorised stakeholders and document the agreed disclosure mode for each item of documented evidence. Controlled transparency fosters trust, reduces friction around sensitive information, and ensures that security and Intellectual Property protections do not become obstacles to legitimate due diligence objectives.

Principle 6: Internal Alignment & Single-Point Coordination

> ***Both clients and providers shall establish internal coordination mechanisms to consolidate requests, ensure consistency across functions (procurement, ICT, security, legal, compliance) and designate accountable owners for due diligence exchanges.***

Ineffective due diligence is often rooted in internal fragmentation, where multiple client functions issue overlapping or uncoordinated requests, and service providers lack a central point of accountability for responses. To address this, both parties should establish clear internal coordination mechanisms, designating responsible owners who consolidate inputs, align terminology and ensure consistency across procurement, ICT, security, compliance, legal and risk teams. Clients are encouraged to eliminate parallel questionnaires and route all due diligence communications through a single coordinating function, while service providers should maintain a centralised due diligence package with explicit ownership and validation processes.

Internal alignment reduces duplication, accelerates response times and prevents contradictory positions from emerging during assessment. When both sides operate through coordinated channels, due diligence becomes a structured dialogue rather than a scatter-shot exercise. This principle does not impose specific organisational structures but emphasises that efficiency and consistency depend on clear internal governance before external exchanges begin.

© 2026 Finance & Technology Luxembourg a.s.b.l. with registered office at 7, Rue Alcide de Gasperi, L-1468 Luxembourg, registered with RCS Luxembourg under number F7436. All rights reserved.

Principle 7: Constructive Engagement & Timely Execution

> ***Parties shall maintain professional, solution-oriented dialogue, provide reasonable timelines calibrated to the complexity of the request and proactively communicate any material changes, limitations or delays that affect due diligence outcomes.***

The quality of due diligence is directly influenced by the professionalism, responsiveness and constructive posture of both parties. Clients should provide reasonable lead times, avoid systematic last-minute requests and allow adequate windows for complex assessments, particularly when multiple functions or evidence categories are involved. Service providers are expected to acknowledge requests promptly, mobilise internally without undue delay and proactively communicate any anticipated challenges, scope limitations or timeline constraints. Where disagreements or ambiguities arise, both sides should prioritise clarification and solution-oriented dialogue over rigid positional stances.

Timely execution does not mean accelerating assessments to the point of compromising quality or accuracy. Instead, it reflects mutual respect for each party's operational capacity and the strategic importance of timely vendor decisions. By embedding responsiveness and professional courtesy into their due diligence culture, the ecosystem entities and ICT providers can transform a traditionally transactional process into a collaborative governance practice that supports long-term partnership stability.

Principle 8: Regulatory Complementarity

> ***The Charter is designed to complement, not replace, applicable regulations (e.g., DORA), supporting consistent mapping to supervisory expectations, the Register of Information, and third-party risk management obligations.***

This Charter is explicitly designed to complement, not supplant, applicable regulatory and supervisory frameworks, including DORA, CSSF and CAA circulars, NIS2, GDPR and sectoral outsourcing expectations. It does not provide regulatory interpretation, legal advice or compliance certification, nor does it modify contractual rights or obligations. This Charter shall in no case take precedence over binding regulations, supervisory guidance or specific contractual terms; where any tension arises, those requirements prevail. The Charter's role is to translate regulatory expectations into a coherent, operational reference that supports consistent implementation across the ecosystem.

By mapping due diligence activities to shared regulatory objectives – such as the DORA Register of Information, ex-ante risk assessments and ongoing oversight requirements – the Charter helps ecosystem entities and ICT providers avoid parallel, redundant exercises driven by overlapping compliance lenses. Parties are encouraged to align internal tracking mechanisms, cross-reference common topics and leverage shared evidence repositories to efficiently satisfy multiple regulatory mandates. This complementary positioning ensures the Charter remains agile, legally sound and practically useful across evolving supervisory landscapes.

© 2026 Finance & Technology Luxembourg a.s.b.l. with registered office at 7, Rue Alcide de Gasperi, L-1468 Luxembourg, registered with RCS Luxembourg under number F7436. All rights reserved.

Principle 9: Responsible Technology & AI Use

> ***Parties may leverage digital platforms and AI tools to enhance efficiency, provided they maintain human oversight, ensure data confidentiality, comply with applicable security standards and retain full accountability for accuracy and integrity.***

Digital platforms, automated workflows and artificial intelligence increasingly support due diligence activities by streamlining information requests, evidence mapping and consistency checks. While technology can enhance efficiency and traceability, its use must be governed by clear principles of security, transparency and human oversight. Parties are expected to employ enterprise-grade, access-controlled platforms that comply with confidentiality and data protection requirements, avoid exposing sensitive information to uncontrolled public tools and maintain strict retention and disposal protocols for due diligence data.

When Generative AI or automated systems assist in drafting, synthesising or analysing due diligence content, both clients and providers retain full accountability for accuracy, completeness and regulatory alignment. Automated outputs must be reviewed, validated and signed off by qualified personnel before reliance and material use of AI should be disclosed to the counterparty to maintain trust and transparency. By adopting technology responsibly, the ecosystem can scale due diligence practices without compromising integrity, security or human judgment.

Principle 10: Continuous Ecosystem Improvement

> ***Participants are encouraged to adopt this Charter pragmatically, contribute to its evolution through structured feedback and support its operational deliverables (standardised packages, evidence repositories, Register of Information mappings) to foster industry-wide maturity.***

Sustainable due diligence practices require continuous refinement driven by market feedback, regulatory evolution, and operational experience. This Charter is intended as a living framework that will be periodically reviewed, updated and aligned with emerging best practices, implementation guidance deliverables and shifting supervisory expectations. Organisations are encouraged to adopt its principles pragmatically, integrate them into internal frameworks where appropriate and contribute constructive feedback through established industry channels.

Long-term success depends on collective stewardship. The ecosystem entities, ICT providers and supporting professionals are invited to test the Charter in real engagements, identify friction points and support the development of standardised evidence repositories, RoI mapping templates and proportionality matrices under the implementation guidance. By treating this initiative as an evolving industry compact rather than a static document, the ecosystem can progressively reduce duplication, elevate assessment quality and build a more resilient, collaborative third-party governance culture.

© 2026 Finance & Technology Luxembourg a.s.b.l. with registered office at 7, Rue Alcide de Gasperi, L-1468 Luxembourg, registered with RCS Luxembourg under number F7436. All rights reserved.