AI

AI & Partners

Amsterdam - London - Singapore

EU AI Act

Principles for the sound management of third-party AI risks

July 2024

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

This report was prepared by Sean Donald John Musch and Michael Charles Borrelli. For more information visit https://www.ai-and-partners.com/.

Contact: Michael Charles Borrelli | Chief Operating Officer | m.borrelli@ai-and-partners.com.

This report is an AI & Partners publication.

Contents

1. Introduction

Firms are able to rely on arrangements with artificial intelligence ("AI") third-party service providers ("AI TPSPs") for reasons such as to access specialised expertise, reduce costs, improve scalability, efficiency and operational resilience, and focus on core activities. Over the past few years, ongoing digitalisation has led to a rapid adoption of innovative approaches, which has increased firms' dependency on AI TPSPs for services that they had not previously undertaken. This expansion of reliance on AI TPSPs requires an evolution of the traditional concept of outsourcing to the broader scope of AI TPSP arrangements.

AI & Partners believes that appropriate risk management of firms' AI TPSP arrangements, supply chain (ie nth parties) and concentration risk arising therefrom can enhance firms' ability to withstand, adapt to and recover from operational disruption and thereby mitigate the impact of potentially severe disruptive events. Through the publication of this document, AI & Partners promotes a principles-based approach to improving firms' operational risk management and operational resilience through effective AI third-party risk management ("AI TPRM"). The approach builds on market-accepted Principles for operational resilience ("POR"), the revised Principles for the sound management of operational risk ("PSMOR") to reflect the life cycle of a AI TPSP arrangement.

The Principles focus on AI third-party risk management holistically and are technology-agnostic to keep pace with technological developments, such as under the European Union ("EU") AI Act (the "EU AI Act"). They aim to promote international engagement, greater collaboration and consistency, with a view to reducing regulatory fragmentation and strengthening the overall operational resilience of the global AI ecosystem.

The Principles seek to accommodate a diverse range of AI risk management practices and approaches. They are intended to be applied on a proportionate basis depending on the size, complexity and risk profile of the firm as well as the nature and duration of the AI TPSP arrangements and their contribution to the delivery of critical services. The Principles are primarily directed to all firms of all sizes across all sectors and their senior management staff.

2. Definitions

These Principles aim to build on the terms used in the EU AI Act. Additionally, certain terms that are necessary and relevant from an AI perspective are specifically defined in this document. To ensure a common understanding, as well as clarity and consistency, definitions for terms used in this document are provided below.

- **AI TPSP**: An entity or individual which performs services, activities, functions, processes or tasks relating to AI directly for a firm.
- **AI TPSP arrangement**: A formal arrangement between a firm and a **AI TPSP** for the provision of one or more services, activities, functions, processes or tasks relating to AI to a firm (which includes but is not limited to "outsourcing").
    - The term **AI TPSP** arrangement includes arrangements for the provision of services to a firm by an intragroup service provider.
    - The term **AI TPSP** arrangement excludes arrangements between a **AI TPSP** and any party in the supply chain (ie an nth party to the firm).
- **Critical AI TPSP arrangement**: A **AI TPSP** arrangement which supports or impacts one or more critical services provided to a firm.

- **Critical service**: A service provided to a firm, the failure or disruption of which could significantly impair a firm's viability, critical operations, or ability to meet legal and regulatory compliance obligations, such as those under EU AI Act.
- **Critical AI TPSP**: A **AI TPSP** that provides a critical service to a firm.
- **Intragroup AI TPSP**: A **AI TPSP** that is part of a firm's group and provides services predominantly to entities within the same group. Intragroup **AI TPSP** may include a firm's parent company, sister companies, subsidiaries, service companies or other entities that are under common ownership or control.
- **Supply chain**: The network of entities that provide infrastructure, physical goods, services and other inputs directly or indirectly utilised for the delivery of a service to a firm, limited to the services under a **AI TPSP** arrangement.
- **Concentration risk**:
  - Firm-level: Risk arising from a dependency of a firm on one or more services provided by a single **AI TPSP** (directly or indirectly through nth parties) or a limited number of **AI TPSPs** where the disruption or failure of such activities has potential implications for the firm's critical operations. Examples of situations in which concentration risk may arise include but are not limited to: (i) concentrations of multiple services provided by the same **AI TPSP**; (ii) concentration of services from one or multiple **AI TPSPs** in a single geographic region; or (iii) multiple **AI TPSPs** with a dependency on the same key nth party.
  - **Systemic**: Risk to the AI economy (and, in some cases, broader global economy) overall arising from a dependency on one or more services provided by a single **AI TPSP** or a limited number of **AI TPSPs** (directly or indirectly through nth parties), the disruption or failure of which may have systemic implications.
- **Nth party**: A service provider that is part of a **AI TPSP's** supply chain and supports the ultimate delivery of services to one or more firms. This term includes, but is not limited to, subcontractors of the **AI TPSP**.
- **Key nth party**: A service provider that is part of a **AI TPSP's** supply chain and supports the ultimate delivery of a critical service by a **AI TPSP** to a firm or that has the ability to access sensitive or confidential firm information (e.g. consumer data).

3. Third-Party Risk Management Principles

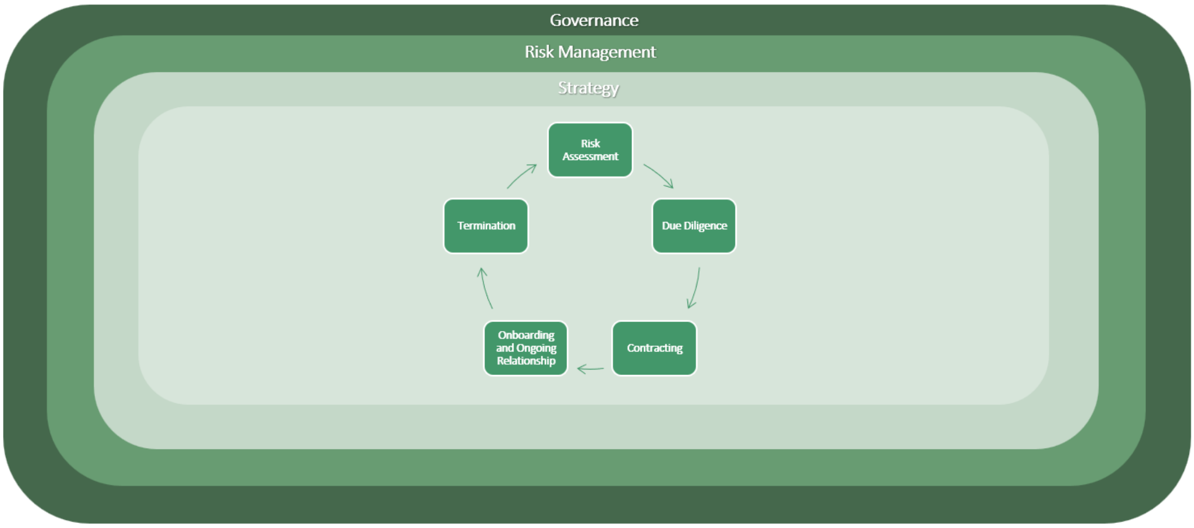
This section presents AI & Partners' proposed Principles for the sound management of AI risks emanating from AI TPSP arrangements, organised across the following categories:

- governance, risk management and strategy;
- the life cycle of AI TPSP arrangements; and
- the role of executive management. These Principles should be applied on a consolidated and on an individual firm basis.

Whether activities are performed internally or by a AI TPSP, firms are required to operate in a safe and sound manner and in compliance with applicable laws and regulations, such as the EU AI Act. While the use of AI TPSPs can reduce firms' direct control over their activities and may introduce new risks or increase existing risks, the use of AI TPSPs should neither diminish firms' responsibility to fulfil their obligations to stakeholders (e.g. customers, supervisors, other legal authorities) nor impede regulatory oversight. As with all business processes, documentation evidencing key decisions (e.g. third-party strategy, board minutes reflecting decision to enter into a critical AI TPSP arrangement) should be maintained in firms' records.

Effective AI TPRM generally follows the stages of the life cycle for AI TPSP arrangements. Controls should be designed proportionally to the risks of each AI TPSP arrangement. A framework for monitoring and managing risks associated with AI TPSP arrangements benefits from identifying the criticality of firm operations supported by AI TPSP services at inception and periodically throughout the life cycle of a AI TPSP arrangement. The stages of the life cycle typically include risk assessment, due diligence, contracting, onboarding and ongoing monitoring, and termination. The firm's governance, risk management and strategy are integral to each stage of the life cycle. The stages of the life cycle are shown in **Figure 1**, with detailed descriptions given in the respective subsections.

Figure 1: AI Third-Party Life Cycle



The stages of the life cycle do not necessarily reflect a linear progression. Rather, the output of each stage should serve as factors to consider in the subsequent and prior stages. For example, a firm may leverage information gained in response to an incident during the onboarding and ongoing monitoring stage for updating the risk assessment and due diligence processes.

Not all AI TPSP arrangements present the same level of risk and therefore not all arrangements require the same level or type of oversight or risk management. The following key concepts are embedded in all stages of the life cycle and apply to all Principles:

Criticality: The Principles emphasise additional areas to focus on when AI TPSP arrangements cover critical services. Critical services typically warrant a greater level of risk management consideration. Firms' processes should enable services and AI TPSP arrangements which are designated as critical to receive more comprehensive oversight and more rigorous risk management (e.g. robust business continuity management ("BCM")).

Concentration: Concentration risk in AI TPSP arrangements may emerge either at the individual firm level or at the systemic level. Monitoring and managing concentration at the individual firm level is the responsibility of the individual firm. While executive management are best placed to monitor systemic concentrations, it is important for firms to understand the relative systemic importance of a AI TPSP, based on available information (e.g. from the public domain, directly from the AI TPSP), so that they may consider the implications of entering into an arrangement with the AI TPSP.

Proportionality: Proportionality focuses primarily on how firms' management of risks related to AI TPSP arrangements might vary based on a firm's business model, complexity, cross-border presence, function, risk profile, scale, structure and size. When applying proportionality, a service or arrangement for one firm might not reflect the same risks or same level of risks as compared to another firm. For example, one firm with operations in one jurisdiction and another that operates in multiple jurisdictions may differ in their approach to applying these Principles regarding a service arrangement with the same AI TPSP. Application of proportionality does not mean that arrangements should be exempt from the application of appropriate risk management.

Intragroup TPSP arrangements: Firms should not treat intragroup arrangements as if they are less risky than other arrangements. Firms' risk management processes should be proportionate to the unique characteristics of intragroup arrangements (e.g. the firm's level of control and influence on the intragroup entity, complexities from cross-border operations, prioritisation of the firm's requirements) and the criticality of the arrangements. Some of the important considerations include: carrying out due diligence to align with the firm's understanding of governance and risk management of the intragroup AI TPSP; having an appropriate formal, written arrangement with appropriate provisions and escalation mechanisms; managing risk of intragroup nth parties akin to external third parties; tailoring BCPs to maintain the firm's operations; and having exit strategies for planned and unplanned terminations of the intragroup AI TPSP arrangements reflecting the firm's position, while recognising that the possible range of exit options may be limited.

Nth parties and supply chains: Firms' AI TPSP arrangements often involve dependencies on nth parties in the supply chain for delivery of services because of a variety of factors (e.g. specialisation, different types of innovation). Such chains may be lengthy and complex, resulting in additional or increased risks to firms. Firms should have appropriate risk management processes to identify and manage the supply chain risks, proportionate to the criticality of the services being provided. Firms' risk assessment, due diligence, contracting and onboarding and ongoing monitoring processes should evaluate the AI TPSP's ability to manage its nth parties and meet equivalent contractual obligations (e.g. level of service, risk management, compliance, operational resilience standards). Further, contracts should reflect the right of firms to obtain information (including incident notifications) about key nth parties on an ongoing basis. As determined by the risk, such information should be captured in the registers and factored into ongoing risk assessments, including assessment of the firm-level concentration risk.

New and advanced technologies: Rapid adoption of new and advanced technologies, such as emerging forms of AI, has increased firms' dependency on AI TPSPs. This has the potential to magnify existing risks (including intellectual property disputes) and introduce new risks to firms. In certain cases, because of a lack of staff experience, it may be more challenging for firms to identify or evaluate risks associated with a new technology that is provided through a AI TPSP arrangement.

Audits and assurance: There are various types of audits and multiple sources of assurance that firms can use in their due diligence and onboarding and ongoing monitoring of AI TPSPs. Audits include those by independent parties engaged by either a single firm, a collection of firms working collaboratively (e.g. pooled audits), or the AI TPSPs themselves (to be provided to and critically reviewed by firms). Additional sources of assurance may include industry-recognised certifications or standards (e.g. ISO certification). These certifications and standards can help provide a comparable, baseline level of assurance about AI TPSPs' controls, but they may not, by themselves, provide all the assurance firms need with regard to the resilience of critical services. These certifications and standards should therefore not be seen as eliminating the need for audits and other forms of assurance where appropriate (refer to the sections on Contracting and Onboarding and ongoing monitoring below).

3.1 Governance, Risk Management, and Strategy

Principle 1*: The board of directors has ultimate responsibility for the oversight of all AI TPSP arrangements and should approve a clear strategy for AI TPSP arrangements within the firm's risk appetite and tolerance for disruption.*

Principle 2*: The board of directors should ensure that senior management implements the policies and processes of the AI third-party risk management framework ("AI TPRMF") in line with the firm's AI third-party strategy, including reporting of AI TPSP performance and risks related to AI TPSP arrangements, and mitigating actions.*

Firms should implement a AI TPRMF defined by a board-approved policy, supported by a strong governance structure led by the board of directors and effective risk management, and aligned with the firms' business strategy (e.g. business needs, overall strategic goals and objectives), AI risk management strategy and AI third-party strategy (refer to section on **3.1.3 Strategy** below).

3.1.1 Governance

The board of directors has ultimate responsibility for the oversight of all AI TPSP arrangements and for holding senior management accountable for the AI TPRMF's implementation. Senior management should ensure communication of the firm's AI third-party strategy and policy to all relevant stakeholders, including firm personnel and intragroup entities, and should establish policies and procedures that include clearly defined roles and responsibilities to manage AI TPSP arrangements throughout the third-party life cycle.

The firm's AI third-party life cycle and services under AI TPSP arrangements should be integrated into the three lines of defence. Roles and responsibilities of all staff should be appropriately defined. Based on risk and complexity, firms may establish a central function to monitor all AI TPSP arrangements.

There are certain arrangements with AI TPSPs which entail "shared responsibility" between the firm and the AI TPSP (e.g. cloud-hosting services). The concept of "shared responsibility" does not abrogate the board of directors' ultimate responsibility for the oversight of risk management associated with AI TPSP arrangements and for firms to meet their legal and regulatory compliance obligations.

3.1.2 Risk management

Firms should establish a comprehensive AI TPRMF, integrated within their broader AI operational risk management framework ("AI ORMF") to manage AI arrangements.

A firm's AI TPRMF should consider the business model, nature, size, complexity, cross-border presence, scale, structure and risk profile of its AI TPSP portfolio. The AI TPRMF should clearly outline criteria, processes and frequency for:

- risk identification and assessment;
- monitoring and reporting; and
- application of controls.

Controls supported by competent personnel across all three lines of defence should be implemented in each stage of the third-party life cycle. Firms may engage external support to supplement the qualifications and technical expertise of in-house staff. .

Firms should maintain a complete and up-to-date register of all AI TPSP arrangements (and nth parties, as appropriate to the criticality of the service and associated risks).

Firms should include key elements of each arrangement in the register (e.g. criticality of the arrangement, substitutability of the AI TPSP's services, contingent providers, whether proprietary or confidential information is shared, location(s)of service and data). Registers should be updated periodically or when there are relevant changes (e.g. entering into another arrangement with the AI TPSP, change in contractual terms, changes in criticality, changes to the service location, availability of an alternative service provider, a new subcontract, mergers and acquisitions). Firms should use the information in the registers to map dependencies and interconnections related to arrangements, particularly those associated with higher risks and those supporting critical services. Firms should be prepared to share the register with supervisors when requested (as per jurisdictional requirements).

Firms should assess the firm-level concentration risk initially at the time of due diligence, and periodically throughout the life cycle of the AI TPSP based on changes in the AI TPSP portfolio. Up-to-date third-party registers and mapping of dependencies and interconnections facilitate the identification of concentration risk of AI TPSPs. Where concentration risk is not avoidable, firms should enhance monitoring and other measures (e.g. testing at more frequent intervals) to mitigate the risk of critical AI TPSP arrangements, including concentrations in their supply chains. Firms should also explore multiple options (e.g. provision of critical services from multiple availability zones or geographic regions by a single provider, ensuring that AI TPSPs adequately manage the resilience of their supply chains, combining the use of firms' on-premises infrastructure with AI TPSPs' services, backup or alternative AI TPSPs, retaining capability to bring the service back in-house) to manage risk within their risk appetite and tolerance for disruption.

3.1.3 Strategy

The board of directors should approve a third-party AI strategy (which could also be part of the firm's overall AI risk management strategy). It should be consistent with the firm's overall business strategy, risk appetite and tolerance for disruption. It should cover the following:

- whether and to what extent the firm should enter into AI TPSP arrangements;
- which services should or should not be performed by a AI TPSP;
- standards for the ongoing evaluation of risks, costs and benefits associated with reliance on one or more AI TPSPs; and
- what conditions, if any, should trigger an exit from AI TPSP arrangements.

Firms' tolerances for disruption should reflect the risks from AI TPSP arrangements, be forward-looking and, where applicable, subject to scenario and stress testing to ensure that firms evaluate whether risks relating to AI TPSP arrangements remain within their risk appetites. This includes consideration of the risks and benefits posed by new and advanced technologies, such as emerging forms of AI (including, but not limited to, artificial general intelligence ("AGI")), when developing their third-party AI strategy, and as part of the implementation of their AI TPRMF. Firms should maintain adequate in-house knowledge, experience, and training and awareness programmes to identify, assess, manage and monitor the risks posed by AI TPSP arrangements.

3.2 Risk Assessment

***Principle 3**: Firms should perform a comprehensive risk assessment under the AI TPRMF to evaluate and manage identified and potential risks both before entering into and throughout an AI TPSP arrangement.*

The risk assessment stage of the life cycle is where firms identify and assess the criticality of potential services and the risks before entering into a proposed arrangement with a AI TPSP, in alignment with the firm's AI third-party strategy, policies and AI TPRMF. Moreover, risk assessment is an iterative process throughout the life cycle of a AI TPSP arrangement.

When assessing criticality firms should consider factors such as the financial, operational or strategic importance of the arrangement; their tolerance for disruption; the nature of any data or information shared with the AI TPSP; or the substitutability of the service..

Firms should assess the potential impacts of entering into any TPSP arrangement on their operations (eg activities, functions, systems, data), including the criticality of the operations, considering risks and assessment results in order to:

- assess adequacy of the current control environment to incorporate the AI TPSP's activities;
- plan appropriate risk monitoring, reporting and escalation;
- plan mitigation measures;
- communicate expectations of the proposed AI TPSP arrangement to stakeholders; and
- develop related proposed contractual terms and conditions.

Firms should consider known risks that may be reduced or better managed and potential risks that may arise from the proposed arrangement, such as risks posed by new and advanced technologies, such as AGI. They should consider all types of risks related to AI TPSP arrangements, including but not limited to strategic risk, reputational risk, compliance risk, operational risk (e.g. information and communication technologies ("ICT"), cyber), concentration risk and the risk stemming from a long supply chain. Firms should document the process and results of the analysis performed.

In their risk assessments, firms should consider how any arrangement would align with their business strategy, third-party strategy, risk appetite and tolerance for disruption, and consider the expected benefits and costs of the proposed AI TPSP arrangement. The outcome of the initial risk assessment should enable a firm to make an informed decision on whether to engage a AI TPSP. This risk assessment would be complemented by a AI TPSP-specific risk assessment (e.g. AI TPSP's size, complexity).

Risks may change throughout the life cycle of the AI TPSP arrangement. Therefore, firms should perform risk assessments on an ongoing basis.

3.3 Due Diligence

Principle 4*: Firms should conduct appropriate due diligence on a prospective AI TPSP prior to entering into an arrangement.*

The due diligence stage of the life cycle is where firms gather and analyse the information needed to determine how well an arrangement with a specific AI TPSP would support their AI third-party strategy. Firms should also perform due diligence to evaluate whether they would be able to appropriately identify, monitor and manage risks associated with the specific arrangement with a prospective AI TPSP.

Firms should have an appropriate and proportionate process for selecting and assessing the prospective AI TPSP before entering into a AI TPSP arrangement. The risk associated with a specific AI TPSP could affect the overall risk assessment of a firm's existing AI TPSP arrangements.

Firms should perform due diligence to mitigate risks as outlined in the risk assessment stage. Firms' due diligence, including inputs from monitoring of any prior arrangements, should support the analysis of:

- the AI TPSP's capacity and ability to perform;
- known and potential risks related to the AI TPSP arrangement;
- relative benefits and costs of the arrangement.

Aspects that should be considered under each of these dimensions are outlined below.

3.3.1 Capacity and ability

As part of the assessment of a AI TPSP's capacity and ability to deliver the services under the arrangement, firms should consider the AI TPSP's:

- operational and technical capability;
- ability to support the firm's objectives for innovation, expansion and third-party AI strategy;
- ability to support the firm's legal and regulatory compliance obligations;
- ability to maintain qualified and adequate staff for ongoing service delivery as well as during disruption;
- effectiveness of internal controls and risk management, including its ability to manage ICT, cyber and other operational risks;
- ability to manage supply chain risks; and
- ability to maintain BCPs, disaster recovery plans ("DRPs") and other relevant plans (e.g. crisis communication plans) consistent with or benchmarked to the firm's tolerance for disruption of critical services.

Risks

As part of the assessment of known and potential risks associated with the AI TPSP arrangement, firms should consider:

- how the responsibility for security, resilience and other technical configurations (e.g. access management controls) will be allocated between firms and AI TPSPs with respect to the delivery of services, and the associated risks;
- financial soundness insofar as it can affect the delivery of the relevant services;
- geographic dependencies and management of related risks (e.g. risks related to the economic, financial, political, legal and regulatory environment in the jurisdiction(s) where the relevant service will be provided);
- potential conflicts of interest (including those from intragroup and nth parties);
- recent or pending relevant complaints, investigations or litigation including (if relevant) at AI TPSPs' nth parties;
- availability of potential alternative AI TPSPs and assessment of related risks; and
- whether the arrangement under consideration may result in unacceptable concentration risk.

Relative benefits and costs

As part of the assessment of relative benefits and costs associated with the AI TPSP arrangement, firms should consider:

- the potential risks of not entering into a AI TPSP arrangement against the risks that the new AI TPSP arrangement may introduce or amplify known risks (e.g. replacing obsolete legacy system, difficulty in hiring and maintaining qualified staff);
- the firm's ability (including cost, timing, contractual restrictions) to exit the AI TPSP arrangement and either transition to another AI TPSP or bring the activity back in-house; and
- the firm's ability to adopt new and advanced technologies and the potential risks thereof.

3.4 Contracting

Principle 5*: AI TPSP arrangements should be governed by legally binding written contracts that clearly describe rights and obligations, responsibilities and expectations of all parties in the arrangement.*

The contracting stage of the life cycle is when negotiations between a firm and a AI TPSP occur, and where terms and conditions of the delivery of services are agreed. Contract provisions should facilitate effective risk management and oversight and specify the expectations and obligations of both firms and AI TPSPs. The firm should negotiate a contract that meets its business goals and risk management needs.

AI TPSP arrangements should be governed by clearly written, legally binding contracts[1]. The nature and details of these contracts should be appropriate to the firms and to the criticality of the services provided by the AI TPSPs and should reflect legal and regulatory obligations of the jurisdictions where the firms and AI TPSPs operate.

Firms' contracts governing AI TPSP arrangements should consider:

- key performance benchmarks;
- rights for firms to receive accurate, comprehensive and timely information (including regarding incidents impacting the services they are receiving);
- rights of the AI TPSPs related to provision of the services outlined in the SLAs (e.g. technical requirements, facility access);
- rights of firms to access (including premises), audit and obtain relevant information from the AI TPSPs;
- rights of supervisory authorities to access (including premises), audit and obtain relevant information from AI TPSPs as permitted under applicable laws and regulations within the respective jurisdictions or bi-/multilateral agreements amongst supervisors;
- obligations and responsibilities relating to business continuity and disaster recovery for the services provided and to support firms' BCP and DRP testing as appropriate;
- costs, including (if applicable) flexibility and scalability based on the firms' use of the service and the payment arrangements;
- ownership, access to and use of logical assets (e.g. data, applications, application programming interfaces ("APIs"), models, intellectual property rights) and physical assets (e.g. hardware, records, premises) as well as how easily these can be transferred in a timely manner and appropriate format, including in the case of termination;
- obligations and responsibilities relating to security, resilience and other technical configurations;
- the location(s) (i.e. regions or countries) where the activity will be performed and where relevant data will be processed and stored;
- confidentiality of firms' proprietary and strategic information and the use of non-disclosure agreements ("NDAs");
- addressing the risk of co-mingling of firms' information with that of other clients of the AI TPSPs;
- rights of firms to indemnification in specific circumstances (including any limitations on the AI TPSPs' liability);
- customer complaints handling and dispute resolution mechanisms;
- choice of law and jurisdiction in case of dispute (where possible, with a preference to apply the laws of the jurisdiction where the firm is incorporated or operating);
- default and termination, including conditions to terminate, roles and responsibilities, notification, and minimum periods to execute termination provisions;

[1] In cases where a legally binding contract may not be possible, for example where the AI TPSP is a branch of the firm and thus not a legally distinct entity, it may be useful to have a service level agreement ("SLA") to formally document the services required by the branch, the roles and responsibilities of the involved parties including service standards, and the consequences of not meeting these standards. This may be particularly useful in cases where the branch needs to meet local regulatory requirements, for instance with respect to operational resilience, for the services it provides locally.

- the framework to amend existing arrangements, including when there are changes in regulatory requirements in relation to the AI third-party activities; and
- provisions to support firms' exit strategies for eventual termination.

Firms' contracts governing critical AI TPSP arrangements should at a minimum include the provisions listed below:

- conditions governing key nth parties (e.g. prior notification of use or change, incident reporting);
- additional indicators and metrics for key performance benchmarks including the methodology for measurement (e.g. SLA and standards, BCM testing results, control effectiveness test results, customer complaint information);
- rights for firms to receive accurate, comprehensive and timely information as outlined in the SLA, including but not limited to information on incidents and material changes to the services of AI TPSPs or their supply chains;
- rights of firms to access, audit and obtain relevant information from key nth parties;
- rights of supervisory authorities to access, audit and obtain relevant information from key nth parties as permitted under applicable laws and regulations within the respective jurisdictions or bi-/multilateral agreements amongst supervisors;
- obligations and responsibilities for BCPs and DRPs should include minimum service uptime and/or maximum service downtime commitments, recovery time objectives ("RTOs") and recovery point objectives ("RPOs"); and
- AI TPSPs' obligation to take out insurance against insurable risks.

In exceptional cases where a legally binding contract does not exist, firms remain responsible for appropriate AI risk management and oversight of their AI TPSP arrangements as outlined in this document.

3.5 Onboarding and Ongoing Monitoring

Principle 6*: Firms should dedicate sufficient resources to support a smooth transition of a new AI TPSP arrangement in order to prioritise the resolution of any issues identified during due diligence or interpretation of contractual provisions.*

Firms should maintain levels of staffing and competency (including education, certifications or qualifications, skillsets, language proficiency, experience and training) to meet the needs of the AI TPSP arrangement within their AI TPSP portfolios.

When a AI TPSP is onboarded, firms need to ensure it has adequate understanding of the firm's policies, people, processes, technology, facilities and the interconnections that are needed to provide the contracted service, in compliance with laws and regulations. Each time firms onboard a new AI TPSP they should update their register and map interdependencies. Tools like an initial checklist may help firms in their onboarding process. Specific checklist items might vary depending on the type of arrangement, its associated risks and other context-dependent elements.

3.5.1 Ongoing monitoring

Principle 7*: Firms should, on an ongoing basis, assess and monitor the performance and changes in the risks and criticality of AI TPSP arrangements and report accordingly to board and senior management. Firms should respond to issues as appropriate.*

The ongoing monitoring stage is where firms should:

- confirm the quality and sustainability of a AI TPSP's controls and ability to meet contractual obligations;
- report the performance status of AI TPSPs and significant issues or concerns (e.g. material or repeat audit findings, deterioration in financial condition, security breaches, data loss, service interruptions, compliance lapses or other indicators of increased risk);
- escalate as specified in firms' policies and procedures;
- respond to issues; and
- confirm the quality and sustainability of the firms' and AI TPSPs' BCM.

Ongoing monitoring should be aligned with firms' governance, risk management and strategy, the risks considered when the AI TPSP was selected, any new risks that have emerged since selection, and contractual obligations of the AI TPSPs. It should include key nth parties.

All AI TPSP arrangements should be reviewed and assessed on a regular basis and whenever there are major changes in a firm's internal environment (e.g. organisation, conflict of interest), the AI TPSP (e.g. organisation, location of services, introduction of new or advanced technologies) or the external environment (e.g. political, economic, social, legal and financial landscape, any potential impediments to the delivery of activities). Critical AI TPSP arrangements should be assessed more frequently.

Monitoring should include performance-related metrics, such as ongoing key performance indicators and scorecards in line with firms' policies and procedures used to check compliance with SLAs, contractual provisions, regulatory expectations and legal requirements. Firms should keep an updated register of all AI TPSP arrangements, reflecting any changes in criticality. Firms should also maintain an up-to-date mapping of their interdependencies or interconnections for critical AI TPSP arrangements. Firms should leverage this information to identify and monitor firm-level concentration risk at a frequency commensurate with the changes to the operating environment.

In arrangements involving shared responsibility, firms should monitor AI TPSP performance and operational implementation to ensure that obligations and responsibilities are clearly understood and fulfilled by the AI TPSP. Firms should also monitor their internal control environment and processes to meet their obligations and responsibilities.

Firms should review BCPs and DRPs of critical AI TPSPs and ensure that periodic testing is performed (refer to section on Business continuity management).

3.5.2 Reporting

The outcome of the risk assessments (e.g. portfolio level, critical services level) should be reported to senior management and boards of directors periodically and as needed according to firms' policies and procedures. Reporting should encompass:

(i) reports on the results/performance of AI TPSPs;
(ii) significant changes in the AI TPSP portfolio and its risk profile;
(iii) breach of established triggers and thresholds; and
(iv) items in need of prompt attention (e.g. a major disruption resulting from an incident at a AI TPSP, concentration risk).

Effective risk management includes monitoring, reporting and responding to incidents, including those originating from AI TPSPs contracted to provide services to firms. Where applicable, firms must comply with all reporting obligations to authorities regarding incidents and contract provisions should provide firm management with the ability to monitor incidents related to AI TPSPs. For critical services, firms should consider incorporating requirements related to incident reporting in the contracts, including minimum information to be reported.

Contracts may require AI TPSPs to have clearly defined processes for identifying, investigating and remediating incidents related to contracted services and notifying firms in a timely manner of incidents that impact the AI TPSP's ability to meet contractual obligations. Firms' ongoing monitoring processes should include monitoring of incident response at AI TPSPs. Firms should integrate the remediation and reporting of incidents related to AI TPSPs into their broader risk management processes (e.g. cyber security, threat and intelligence gathering, BCM).

Firms should also analyse updates on remediation of reported incidents and use this information to update their risk assessments of AI TPSPs.

Firms may utilise the results of independent audits and other forms of assurance on the services contracted to AI TPSPs. However, for critical services, they should use multiple forms of assurance and not rely solely on one. Standardised assurances (e.g. ISO certificates) need to be critically assessed and fully understood to allow firms to identify their relevance compared to the firms' internal standards and requirements.

3.5.3 Response

In case of a disruption, firms' monitoring should provide:

(i) oversight of remediation actions by AI TPSPs to restore service delivery to contractual levels;
(ii) identification of risks associated with the continuation of the AI TPSP arrangement; and
(iii) feedback to AI TPSPs' senior management of firms' expectations.

When monitoring determines that a given AI TPSP is no longer a viable option, firms need to initiate steps for the least disruptive termination of the arrangement.

When firms decide to renew a AI TPSP arrangement, they should leverage the information obtained from the onboarding and ongoing monitoring stage in performing due diligence prior to renewing the arrangement.

When firms decide to not renew a TPSP arrangement, they should ensure continuity of their operations and manage termination in the least disruptive manner (refer to section on Termination).

3.6 Business continuity management

Principle 8*: Firms should maintain robust business continuity management to ensure their ability to operate in case of a AI TPSP service disruption.*

Firms should manage their dependencies on TPSP arrangements within their BCM. A firm's BCM should consider:

- development, periodic review and updating of the firm's internal BCPs and DRPs with respect to AI TPSP arrangements;
- periodic testing of the firm's BCPs and DRPs, considering a range of possible recovery strategies or compensating controls (e.g. switching to another AI TPSP, using multiple AI TPSPs, bringing the service in-house, employing a combination of on-premises and external data centres across different geographical regions) that can deliver a level of resilience consistent with the firm's risk appetite and tolerance for disruption;
- lessons learned from incidents (if any) and result of the periodic testing; and

- periodic updating of identified alternative providers.

A firm's BCM governing critical AI TPSP arrangements should at a minimum include the provisions listed below:

- assurance that AI TPSPs develop and periodically review and update BCPs that set out clear and measurable RTOs and RPOs that support firms' tolerance for disruption; and
- assurance testing (e.g. walkthroughs, tabletops and simulations) that the AI TPSP's BCP methodologies are robust.

Firms should also consider joint design and testing of BCPs with AI TPSPs, or utilise independent parties to do the same.

In cases where alternative AI TPSPs do not exist for critical services, firms' BCM should address actions to be taken to ensure the continuity of the service.

3.7 Termination

Principle 9*: Firms should maintain exit plans for planned termination and exit strategies for unplanned termination of AI TPSP arrangements.*

The termination stage is where firms manage planned or unplanned terminations of arrangements for reasons such as expiration or breach of the contract, the AI TPSP's failure to comply with applicable laws or regulations, or a desire to seek an alternate AI TPSP, bring the activity in-house or discontinue the activity. When this occurs, it is important for firms to terminate the arrangement in a safe and sound manner.

Firms should maintain appropriate and proportionate exit plans for planned terminations within their exit strategies. Exit plans need to be regularly updated and tested for availability of budget, human resources, technical infrastructure, transfer of knowledge, access to data and other factors. The level of detail in the plans should be commensurate with the criticality and substitutability of the services provided. Firms' plans for the termination of AI TPSP arrangements should consider:

- transitional periods;
- perfection of rights contained in contract provisions (e.g. preservation and availability of audit trails, archiving and destruction of data, system access revocation);
- adequate budget allocation; and
- clear identification of responsibilities to coordinate and manage the exit.

Firms' exit plans for the termination of critical AI TPSP arrangements should at a minimum include the provisions listed below:

- processes for transferring logical assets (e.g. data, application, API, models, intellectual property rights) in an appropriate format, physical assets (e.g. hardware, records, premises) and human resources (e.g. consultants, contract employees) in a timely manner; and
- actions necessary to enable alignment between all internal (e.g. human resources, legal and compliance function, IT teams) and external stakeholders (e.g. new AI TPSP, supervisor).

Firms should maintain appropriate and proportionate exit strategies for unplanned terminations for all AI TPSP arrangements taking into consideration factors such as the size, complexity and risk profile of the firm and whether the AI TPSP arrangements cover critical services. Although unplanned terminations may occur less frequently than planned terminations, they potentially pose more risks and firms should prepare for such events.

Firms' exit strategies for the unplanned termination of critical AI TPSP arrangements should at a minimum include:

- processes for transferring logical and physical assets in a timely manner and an appropriate format;
- periodic updating of identified members of an escalation or emergency group (with appropriate control functions represented); and
- a process for budget approval to cover additional costs associated with the event and to source necessary expertise (e.g. consultants, temporary workers) to transition the services.

3.8 Role of Executive Management

Principle 10*: Supervisors should consider third-party AI risk management as an integral part of ongoing assessment of firms.*

Executive management recognise that firms' dependencies on AI TPSPs, if not managed appropriately, may impede their ability to fulfil their regulatory requirements. Executive management should, therefore, assess firms' AI TPRMF and consider how they align to their AI ORMF to support their operational resilience. Executive management evaluations should cover the entire third-party AI life cycle. Emphasis should be placed on how firms' integrate AI TPSP arrangements within their overall risk management processes (e.g. incident management, cyber security controls, BCM). As certain AI TPSP arrangements require highly technical skills, executive management should periodically evaluate the knowledge and skills of executive management staff.

Principle 11*: Supervisors should analyse the available information to identify potential systemic risks posed by the concentration of one or multiple AI TPSPs in the AI economy.*

Concentration of services provided by AI TPSPs combined with lack of substitutability of AI TPSPs is relevant to the identification of systemic risks. To assess and monitor such risks across the AI economy, supervisors should be able to obtain from firms information reflecting their arrangements with AI TPSPs (including those involving shared responsibilities). The types of information supervisors could leverage include registers of AI TPSP arrangements; maps of interconnections and interdependencies; recovery and resolution plans; and reports on incidents involving AI TPSPs. To analyse systemic concentration risk, executive management may assess firms' aggregate AI TPRM capabilities using common supervisory tools (e.g. scenario analysis, data analytics, other data-driven models).

Principle 12*: Executive management should promote coordination and dialogue across sectors and borders to monitor systemic risks posed by critical AI TPSPs that provide services to firms.*

Firm executive management should promote coordination and dialogue among themselves, executive management of other sectors and relevant stakeholders to monitor systemic risk. Such collaboration may include a variety of efforts to support the resiliency of critical infrastructure (eg industry- and/or supervisory-led business continuity exercises). Additionally, collaboration may comprise:

(i) appropriate cross-border coordination and collaboration mechanisms (e.g. enhancement of bilateral and multilateral memoranda of understanding ("MoUs"), leveraging supervisory forums) fostering direct collaboration with critical TPSPs providing services to firms in multiple jurisdictions (e.g. use of bilateral or multilateral platforms for promoting information-sharing and building collective competencies); and

(ii) exploring efforts to enhance cross-border resilience of critical, internationally active service providers (e.g. information-sharing, tabletop exercises, coordinated responses and recovery exercises, joint examinations).

About AI & Partners

AI & Partners – 'AI That You Can Trust'

Your trusted advisor for EU AI Act Compliance. Unlock the full potential of artificial intelligence while ensuring compliance with the EU AI Act by partnering with AI & Partners, a leading professional services firm. We specialise in providing comprehensive and tailored software solutions for companies subject to the EU AI Act, guiding them through the intricacies of regulatory requirements and enabling responsible and accountable AI practices. At AI & Partners, we understand the challenges and opportunities that the EU AI Act presents for organisations leveraging AI technologies. Our team of seasoned experts combines in-depth knowledge of AI systems, regulatory frameworks, and industry specific requirements to deliver strategic guidance and practical solutions that align with your business objectives.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Contacts

Sean Donald John Musch, CEO, s.musch@ai-and-partners.com

Michael Charles Borrelli, Director, m.borrelli@ai-and-partners.com

Authors

Sean Donald John Musch, CEO

Michael Charles Borrelli, Director

Important notice

Opinions in this document reflect the opinions of the authors, and are not intended to be relied upon. The authors do not accept any responsibility for any reliance placed on this document. It is important to obtain professional guidance as appropriate when seeking to deal with the matters raised in this report.

AI & Partners B.V. is the Dutch headquarters of AI & Partners, a global professional services firm. Please see https://www.ai-and-partners.com/ to learn more about us.

Designed and produced by AI & Partners B.V