A|M|S

People powered partnership

3rd Party Assurance Policy

Version 2 – May 2025

Data classification: Public

A|M|S

Contents

A|M|S

Definitions

- **3rd Party Assurance (3PA)** – part of AMS Risk & Compliance, responsible for managing the due diligence compliance standards and risk assessments for 3rd party suppliers.
- **ProcessUnity** – AMS's 3rd party risk management/due diligence platform provided by Process Unity Inc.
- **3rd party (parties) –** third-party suppliers/vendors engaged by AMS to support delivery of its services.
- **3rd party due diligence assessment (s)** – online questionnaire(s) released to all applicable 3rd parties via ProcessUnity according to their risk category and as defined in the AMS Supplier Risk Matrix.
- **Business Requestor/Business Owner (BO)** – A member of AMS staff intending to engage a new 3rd party.
- **Dow Jones** – provider of online portal used by 3PA Team for checking for any adverse findings relating to sanctions, watchlists or adverse media.
- **Exceptions** – list of approved exception categories and low risk 3rd parties.
- **AMS Supplier Risk Evaluation Process** – calculated method of supplier inherent and residual risk, and associated due diligence applied.
- **Risk Mitigation/Remedial Action Plan** – plans which are produced by AMS for 3rd parties to mitigate any risks identified following the 3rd party due diligence assessment review to reduce the residual risk.
- **AMS functional subject matter experts (SMEs)** – experts within AMS across Information Security, Data Protection, Business Continuity and Resilience, Compliance who may need to support from time to time in reviewing and approving supplier due diligence.

Introduction

AMS uses 3rd parties to provide products or services in support of our business operations and client solutions. Such outsourced relationships may benefit AMS by reducing costs, improved performance, staff augmentation, increased business competitiveness, access to specific expertise, etc. However, AMS recognises that AMS's reliance on 3rd party relationships presents various risks that must be identified, assessed, and appropriately managed. Failure to manage these risks can expose AMS and AMS's clients to financial loss, reputational damage, litigation, or other damages and may impair AMS's ability to service existing client relationships or establish new ones.

Policy Statement

Relationships with 3rd parties are fundamental to AMS's ability to maintain its operations and offer products and services to its employees and clients. AMS has a responsibility to ensure that products and services provided by 3rd parties do not expose its business to risk, and that 3rd parties comply with all applicable laws and regulations.

As such, AMS has established the 3rd Party Assurance Policy (hereinafter referred to as the 'policy') to formally define the framework, roles and responsibilities, scope, and components required for a fully functioning 3rd Party Assurance and 3rd Party Risk Management programmes. This policy sets out the requirements for the effective identification, assessment, and management of 3rd party risks.

The policy outlines the 3rd Party Assurance Framework which includes:

- assessing 3rd party inherent risk in line with the Supplier Risk Evaluation Process
- the requirement to complete 3rd party due diligence prior to contractual engagement/implementation of products and services provided by 3rd parties, and
- identification, evaluation, controlling, monitoring and mitigation of associated risks which may be present when engaging with 3rd parties

All AMS employees who intend to engage a 3rd party to support AMS or AMS's client solutions must be aware of and understand the requirements of this policy as any failure to comply may compromise both AMS and its clients and result in financial loss, reputational damage, litigation, or other damages.

As per this policy, AMS can only engage with a 3rd party upon successful completion of 3rd party due diligence assessment.

A|M|S

Scope and Applicability

This policy should be read in conjunction with AMS Procurement Policy available on myAMS and applies to all 3rd parties which AMS contracts with for products and services.

This policy applies to all AMS employees, i.e., employees, independent contractors and consultants who intend to engage a 3rd party, or extend existing relationship with a 3rd party, to support AMS or AMS's client solutions (the 'business owner').

3rd parties not in scope of this policy

The following 3rd parties / 3rd party due diligence are not subject to this policy:

- AMS's clients.
- AMS engaged contingent and temporary resources, including independent contractors.
- 4th parties.
- Approved exception categories and low risk 3rd parties as defined in the Supplier Risk Evaluation Process.

Procedures not in 3PA scope

The following procedures are excluded from this policy and 3PA scope:

- Procurement strategy and procedures.
- 3rd party contract negotiation, RFI/tenders, contract production, contract management.
- 3rd party credit checks (except AMS strategic partner credit monitoring).
- Insurance validation.
- Finance set up of a supplier and Purchase Order creation.
- Management of Preferred Supplier Lists.
- Ongoing operational management of 3rd parties and SLA monitoring.
- Exit management for 3rd parties.

Roles and Responsibilities

Business Owner (BO)

- Comply with AMS Procurement Policy and this policy in the engagement of any 3rd party.
- Notify Procurement and 3PA of intended new or changing 3rd parties as per the Procurement onboarding process and New Supplier Request form, and obtain Procurement approval.
- Validate accuracy and content of services provided by selected 3rd party.
- Support 3PA process.
- 3rd party contract negotiation and management.
- Manage ongoing relationship with the selected 3rd party.
- Record any risks into the risk register where gaps in expected standards/controls are identified for the selected 3rd party and gain Senior Management approval to proceed.

Procurement

- Set and drive compliance to the Procurement Policy.
- Support the business with the engagement of 3rd parties as appropriate in line with the Procurement Policy.
- Price/contract negotiations and renewals in line with the Procurement Policy.
- Communicate 3PA requirements to Business Owners.
- Contract management.
- Insurance validation (agency only).

3PA Team

- Management of 3rd Party Supplier Risk Evaluation Process.
- Risk-based due diligence assessment (High, Medium, Low): initiation, supervision, validation of 3PA assessment and checks.
- Identify, measure, report, monitor risks identified during 3rd party due diligence process
- Dow Jones check to identify adverse media, sanctions, PEPs, state owned company etc.
- Companies' House check (UK registered 3rd parties) to validate company details.
- Set risk mitigation (remedial) action plans for 3rd parties not meeting AMS standards and monitoring through to completion with relevant Business Owner.
- Flag risks to Business Owner and Senior Management for review to accept or reject 3rd parties.
- Status reporting and ongoing monitoring of critical 3rd parties, and high inherent risk 3rd parties.
- Record keeping and reporting.

Finance

- Act as a control point to ensure 3rd parties are not set up for payment without 3PA and Procurement prior approval.
- Set up new 3rd parties in Finance system once approved by 3PA and Procurement.
- Carry out credit checks on request.

Risk and Compliance Committee

- Point of escalation, review and acceptance for any 3rd parties presenting high residual risk following completion of their due diligence process where the business wishes to continue engagement.

Legal and Commercial

- Support the business and/or Procurement in 3rd party contract negotiations and management (where required).

Data Privacy Office

- Define 3rd party due diligence questions and scoring required for all assessment types, reviewing requirements annually.
- Review and validate any non-preferred answers related to data protection from the 3rd party due diligence assessment and provide approval to engage or flag risks of engagement.

Business Resilience & Continuity

- Define 3rd party due diligence questions and scoring required for all assessment types, reviewing requirements annually.
- Review and validate any non-preferred answers related to business resilience and continuity from the 3rd party due diligence assessment and provide approval to engage or flag risks of engagement.

Information Security Officer

- Define 3rd party due diligence questions and scoring required for all assessment types, reviewing requirements annually.
- Review and validate any non-preferred answers related to information security from the 3rd party due diligence assessment and provide approval to engage or flag risks of engagement.

3PA Senior Manager

- Approval of Dow Jones identified adverse findings, supplier dispensations, and exception process.
- Review/creation of supplier Risk Mitigation Plans.
- Risk acceptance and escalation of suppliers not meeting AMS standards.

Regional Compliance

- Support in defining 3rd Party due diligence questions and scoring requirements annually.
- Review and validate any region specific non-preferred answers from the 3rd party due diligence assessment and provide support to 3PA as and when required.

Supplier Risk Evaluation Process

Inherent Risk

Each prospective 3rd party engagement will initially be assessed for the inherent risk posed to AMS and/or AMS's clients based on the nature of products or services provided, and other factors, to determine whether a 3rd party is critical or non-critical.

Inherent risk represents the amount of risk existing in the activity/service in the absence of risk treatment, including appropriate controls. The inherent risk assessment identifies types of risk associated with the 3rd party's product or service and its significance to AMS. Once further evaluations and due diligence are complete, the validation of controls, practices, and assurances help determine the residual risk of the 3rd party engagement.

To assess the inherent risk category accurately so that the correct due diligence process can be applied, AMS's 3PA team review the following criteria as documented below:

- 3rd party category - based on the type of services/products provided to AMS
- Processing of/access to AMS's/AMS clients' personal, sensitive or confidential data
- Criticality of products/services provided to AMS or AMS's clients
- Estimated value of the contract with the 3rd party
- Degree of integration of services/technology
- Whether sub-contracted to a client solution

Risk Ratings

AMS risk ratings applied to inherent risks are as follows:

- Critical/Strategic
- High
- Medium
- Low/exceptions

High, Medium and Low ratings are utilised as residual risk ratings.

Critical/Strategic

A small subset of 3rd party engagements will be identified as critical/strategic. The distinct and separate classification of critical/strategic serves to identify the most essential and highest-risk business activities provided by 3rd parties to AMS or AMS's clients. 3rd parties deemed "critical/strategic" or "high risk" are subject to additional ongoing due diligence/monitoring or other internal controls as determined by AMS management.

Critical/strategic partners perform activities deemed crucial to AMS's operations, or to the solutions we provide to our clients as a sub-contractor, or where they could be the main/sole provider of an essential business function. Any interruption of that activity (or failure to perform it as required) can cause significant disruption to AMS or AMS clients' operations if not quickly and easily remedied.

High

3rd parties assessed as "high risk" are core suppliers to AMS or AMS's clients and have similar characteristics as "Critical / Strategic" partners.

Typically, they are deemed important to AMS operating as a business, or delivering services to our clients, however, could be replaced (with some impacts). They may have a high degree of technology integration, process large volumes of data on behalf of AMS or AMS's clients, or act as data controller in their own right.

"High Risk" and "Critical / Strategic" 3rd parties will receive the same comprehensive due diligence assessment and are subject to the ongoing due diligence and monitoring. The nature of services by such 3rd parties is deemed to present a significant risk to AMS that must be mitigated and requires frequent oversight through ongoing due diligence and monitoring activity.

Medium

3rd parties assessed as "medium risk" are important suppliers to AMS, however, would not be critical to AMS operating as a business, with limited impact should there be an interruption of a service (or failure to perform it as required). Services could easily be delivered by another 3rd party. "Medium risk" 3rd parties have limited access to, or interaction with, AMS data and no interaction with AMS's client data.

Low Risk/Exceptions

As each 3rd party engagement is risk-rated, some may be deemed low risk/exceptions based on the nature of service/category and therefore will not need to complete AMS due diligence assessment.

Such 3rd parties have no access to, or interaction with, AMS or AMS's client data or confidential information. All Suppliers however are required to follow AMS Supplier Code of Conduct and receive a copy as part of their onboarding.

Residual Risk

Once AMS has concluded their 3rd party due diligence assessment which includes evaluation, validation of controls, practices and assurances, a residual risk rating for a given 3rd party can be determined.

The residual risk rating is used solely to establish any remaining risk associated with engaging a given 3rd party, and whether such risk can be accepted by AMS, or whether additional risk mitigation actions are required before entering into a business relationship with such 3rd party.

The risks emanating from 3rd party engagements are evaluated using an online due diligence platform (ProcessUnity) which measures the inherent and residual risks of the product, service, and relationship.

Due Diligence Assessments

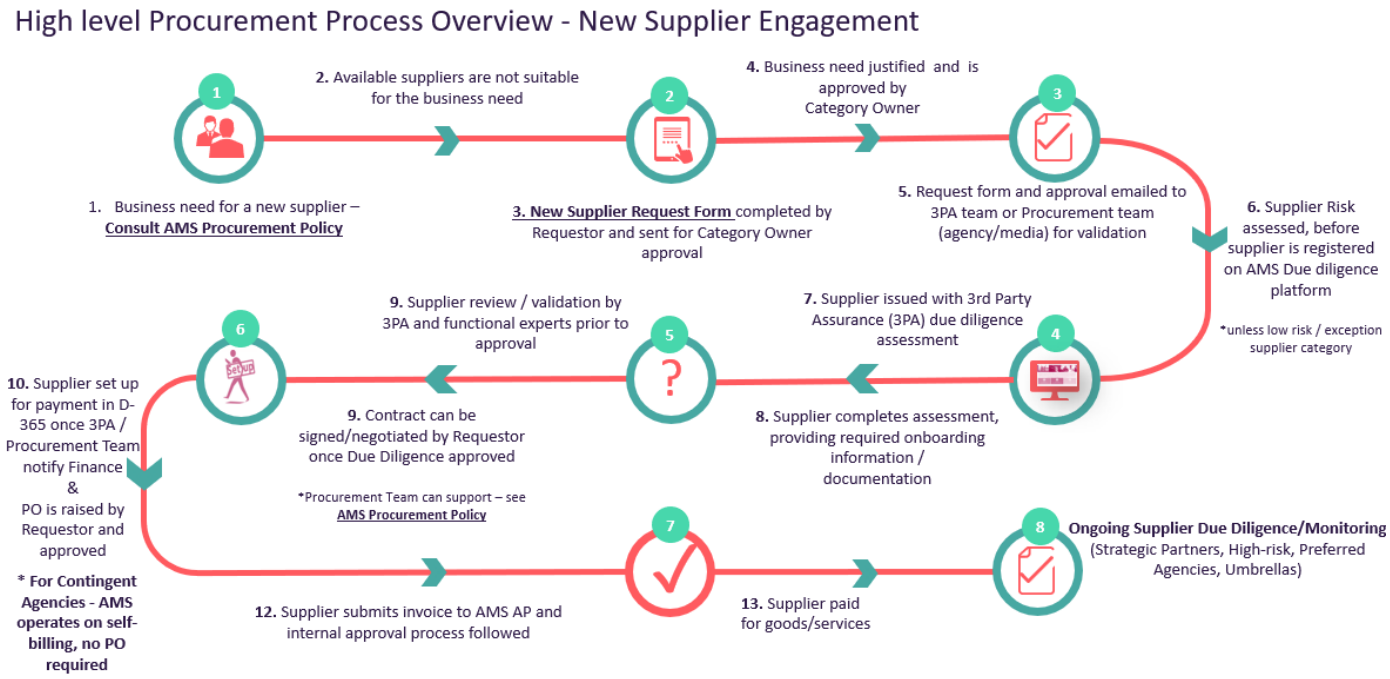
Overview

Comprehensive, risk-based due diligence assessments are appropriately scaled in line with the inherent risk to ensure that contracted engagements meet AMS's expected standards.

3PA forms part of the end-to-end process for engaging a 3rd party which involves several key functions as detailed in the "High-level New Supplier Engagement" diagram below. 3PA focusses on reviewing and evaluating 3rd party controls and standards across several key areas to understand and mitigate any risk to AMS and AMS's clients. These areas include:

- Information Security
- Data Privacy
- Business Continuity & Resilience
- Compliance to legislation
- Ethical standards/behaviours including attestation to AMS Supplier Code of Conduct
- Operational procedures
- Adverse media/sanctions/PEPs/state owned company checks via Dow Jones
- Companies' House check
- Credit Checks (Critical/Strategic partners)

3rd parties complete a due diligence assessment which is supported through AMS online due diligence platform (ProcessUnity). Only upon successful completion of the assessment and required checks can Business Owners engage a 3rd party for services either directly to AMS, or as part of a client solution. Specific due diligence requirements will vary depending on the risks associated with the scope of services or products delivered by a 3rd party.



The due diligence process must be completed and formally approved before AMS and the 3rd party enter a contract and begin providing services or products. Due diligence is then performed periodically during the contract lifecycle for "critical/strategic" and "high risk" 3rd parties as per the Supplier Risk Evaluation Process.

"Critical/strategic" and "high risk" 3rd parties are subject to a rigorous due diligence review to assess their control environment's sufficiency, resilience, compliance with all applicable laws and regulations, and the ability to support AMS operations. This process requires 3rd party's provision of internal documents and evidence such as policies, procedures, business continuity/disaster recovery plans and testing results, and evidence of technical security controls applied.

The scope of due diligence documentation required for all 3rd parties is risk-based and calibrated to both the nature of the relationship and the evidence necessary to assess controls accurately.

Additionally, other required evidence may substantiate controls for "critical/strategic" 3rd parties where required by contract, including on-site Information Security visits and interviews with 3rd party key personnel.

Due Diligence Assessment Review and Supplier Risk Acceptance

Review Process

3PA team reviews and validates all responses and documentation provided by the 3rd party including any question scoring within the relevant sections. The online portal scoring enables 3PA team to follow up with questions and actions as well as set any Risk Mitigation Plans where 3rd parties do not meet AMS required standards.

AMS functional subject matter experts (SMEs) review and sign off against their relevant section, or where appropriate, highlight any gaps in controls and potential risks in engaging with the 3rd party.

Decision

The residual risk in engaging the 3rd party is calculated by 3PA team once all feedback has been collated from the functional SMEs. A decision is then passed to the Business Owner which details any failures/gaps in the 3rd party due diligence assessment and the residual risk.

The following decision may be rendered:

- **High Residual Risk - Reject –** 3rd party does not meet AMS minimum standards, with many critical controls not evidenced/not in place (or) has not/will not complete AMS due diligence. Instruction is Do Not Engage.
- **Medium Residual Risk –** 3rd party presents gaps across some controls or standards, or has only partially evidenced some controls, which taking into consideration their inherent risk (type of service or product offered), presents medium residual risk.

- Recommendation is Do Not Engage, unless supplier agrees to the Risk Mitigation Plan and risk is accepted as shown below.
- **Low Residual Risk/No Risk –** 3rd party has satisfactorily evidenced all required critical controls or meets AMS minimum standards, which taking into consideration services or products to be provided presents low residual risk and can therefore be engaged.

Supplier Risk Acceptance/Approval

Following the 3rd party due diligence assessment, if a 3rd party fails to meet AMS standards and presents "Medium Residual Risk", the **recommendation** is either for that 3rd party not to be engaged or to set a Remedial Action Plan. Where the 3rd party presents "High Residual Risk", the **instruction** is that the 3rd party must not be engaged.

In some instances, where the Business Owner/Requestor has a critical business reason to engage the 3rd party, appropriate risk acceptance and approval must be obtained. This will be facilitated by the 3PA Team in conjunction with the Business Owner, and approvals required will depend on the level of risk and impacted function or operational team:

Medium Risk with Remedial Action Plan:

- Functional Director **or** Career Level 6 +
- Client Operations Director / Account Director
- Other as appropriate

High Risk with Remedial Action Plan:

- Requesting function's ExCo Member
- MD of Legal, Risk & Compliance, Gordon Bull
- As appropriate, other ExCo member (e.g., Information Security, Regional Client MD, Functional MD, other)

AMS Business Owner / Supplier Relationship Owner is responsible for documenting the risk and mitigation actions on their own risk register and owning the completion or agreed actions with the relevant 3rd party, feeding into the 3PA team as required. Escalations and corrective actions are documented and tracked appropriately by 3PA team through to completion.

In some cases, if a 3rd party fails to deliver against the Risk Mitigation Plan or otherwise fails to address deficiencies within the agreed timeframes, this may result in AMS no longer using the services of the 3rd party, until the plan is satisfactorily completed. AMS evaluates all legal and contractual rights and remedies to avoid or mitigate continued exposure to 3rd party risk.

Contractual Standards

3rd party relationships must be documented by written agreements that appropriately and adequately consider the expected relationship and provide AMS with appropriate protections and controls, consistent with prudent business practices. AMS supplier relationship owner / supplier requestor must arrange appropriate contractual terms, in conjunction with Procurement (where applicable to the Procurement Policy) and AMS Legal, and ensure any client specific flow downs are incorporated. All Suppliers are contractually required to follow AMS Supplier Code of Conduct.

Prospective 3rd Party Due Diligence

New Client Solution

From time-to-time AMS teams may look to incorporate new technologies/services as part of the overall solution scope for a prospective client, or as part of an enhanced solution for an existing client or re-bid. Where AMS looks to incorporate a new 3rd party to deliver part (s) of that solution, the relevant teams must engage 3PA as soon as practicable in order to initiate the 3rd party due diligence assessment. This process should be completed **before** proposing or documenting the solution, so that AMS is able to assess any risk to AMS/AMS's clients in working with/proposing to work with such 3rd party. The process must be initiated in sufficient timescale (c. 8 weeks in advance) so that 3PA team is able to fully assess the prospective 3rd party and provide findings.

The 3rd party must not be awarded contract or confirmed as a 3rd party within the client solution until they have completed and passed the 3rd party due diligence process, as it may impact the implementation if the supplier does not meet AMS standards and is not approved for use.

Note some AMS clients will also require AMS sub-contractors to complete their own due diligence process before implementing their services – this must also be factored into the overall solution design and implementation timeline.

New AMS Service

From time-to-time AMS Business/Procurement may look to engage a 3rd party as a replacement for an existing 3rd party who supplies services or products to AMS. This may be part of an RFI/bid process, and consequently the relevant Business Owner/Procurement should engage 3PA team at the point they have produced a 3rd party shortlist. Relevant RFI's/selection criteria for 3rd party(s)

should include the necessity to complete 3rd party due diligence assessment and the requirement to provide relevant evidence where requested. The 3rd party must not be awarded contract with AMS until they have completed the 3rd party due diligence assessment so that AMS is able to assess risk in working with such 3rd party.

Ongoing 3rd Party Due Diligence

A 3rd party's risk profile may change over time, and overall risk can increase or decrease due to numerous factors, therefore in line with best business practices enhanced oversight rules apply to any 3rd party relationship deemed "critical/strategic" and "high risk".

As appropriate, outcomes of such reviews together with findings are reported to the relevant stakeholders, including Senior Management, with any risks escalated as per AMS Risk Management Policy. As minimum, "critical/strategic" 3rd parties undergo a periodic due diligence assessment within one calendar year of completing the initial or previous due diligence assessment, and other inherently "high risk" 3rd parties within two years of completing the initial or previous due diligence assessment, unless client contract stipulates sooner or as otherwise agreed with AMS Business.

These evaluations require 3rd parties to provide updated responses and evidence as necessary.

Additional periodic assessments are considered under the following circumstances:

- Material changes in a 3rd party's business practices, financial position, reputation
- Increased AMS's or AMS clients' reliance on the 3rd party and its services or products
- Expansion of 3rd party geographical scope, or expansion of services
- Changes in applicable law or regulations impacting the 3rd party's product or service
- Increased media attention, negative publicity, or industry scrutiny related to the 3rd party
- Regulatory enforcement actions or industry-related guidance impacting the 3rd party relationship.

Records and Reporting

3PA maintains records of all 3rd party due diligence assessments, functional approvals and Risk Mitigation (remedial) Action Plans and reports on its 3rd party assurance process and any risks identified. Regular reporting is provided to the appropriate stakeholders and include:

- Monthly, bi-annual and annual reporting on 3rd party due diligence assessments completed, risks identified, action plans and continuous improvement plans presented to the Global Head of Risk & Compliance.
- An inventory of all 3rd parties, identifying services and the relationships that involve critical activities and status of ongoing due diligence assessments in line with the Supplier Risk Evaluation Process.

Governance

This framework is governed by:

- AMS Risk & Compliance will maintain and develop the Policy in line with direction from GMD Legal, Risk & Compliance.
- It shall be stored and accessed through a central Share-point location AMS Policies.
- For any questions related to this Policy, contact 3rdpartyassurance@weareams.com

Document Control

This document was last reviewed and updated in May 2025. In line with AMS's Quality Management System (QMS) the next review is scheduled for no later than May 2026. Document Version Control is managed centrally and access is restricted, please request if required.

A|M|S

Document Control