IGUAKO CAPITAL · Group policy

# Third-Party Risk and Outsourcing

This policy governs every relationship in which a person or firm outside the group provides a service, a system, data or an introduction on which the group relies. It classifies each of the 231 active relationships as critical, important or standard, fixes the due diligence performed before and during each, prescribes the contract terms every provider must accept, limits concentration on any single provider, requires a tested exit plan for every critical service and extends the Ethical Technology Charter to every vendor that handles group data or supplies a learning system. Oversight is run from Luxembourg by the third-party risk function under the Chief Operating Officer.

| CODE | CATEGORY | VERSION |
|---|---|---|
| IGC-DT-006 | Data and technology | 2.5 |
| **EFFECTIVE** | **REVIEW** | **OWNER** |
| 2023-01-01 | Annual. Last reviewed January 2026. Next review due January 2027. | Chief Operating Officer |

## 1. Purpose and scope

The group performs its core judgements itself: origination, underwriting, allocation, advice and the decision to move capital. Around those judgements it relies on custodians, administrators, depositaries, correspondent banks, hosted infrastructure, market data, screening services, professional advisers and introducers. A failure in any of these can harm a client as surely as a failure of the group's own staff. This policy exists so that the group knows what it depends on, has examined each dependency and can replace it.

A third party is any person or firm outside the group that provides a service, a system, data or an introduction to the group or to its clients on the group's behalf. An outsourcing is a third-party arrangement under which the provider performs a function the group would otherwise perform itself on a continuing basis. Arrangements between group entities are treated as outsourcings for the purposes of the entity that receives the service, so that a local board knows what it depends on elsewhere in the group.

The register held 231 active relationships at 30 June 2026. The Chief Operating Officer owns the policy. The third-party risk function, four people in Luxembourg, maintains the register, runs the assessment calendar and reports to the Risk & Valuation Committee. Each relationship has a named relationship owner in the business who answers for its performance and for the accuracy of its register entry.

## 2. Classification

Every relationship is classified before contract and reviewed annually. A critical relationship is one whose failure would stop a Tier 1 or Tier 2 service under the Business Continuity and Disaster Recovery policy within 24 hours, would expose Confidential or Restricted information, or would cause direct loss to a client.

Thirty-one relationships were critical at 30 June 2026: the custodians, fund administrators and depositaries, the correspondent banks on the approved panel, the two hosted infrastructure providers, the market data and screening providers and the recorded-line service.

An important relationship is one whose failure would degrade a service for more than five business days, would affect a regulatory obligation or would require a change of provider under time pressure. There were 68, including professional advisers on retainer, specialist valuation agents, payroll and benefits providers, and the introducers through whom the Private Wealth & UHNW division accepts new relationships. Every other relationship is standard; there were 132.

The classification is proposed by the relationship owner and confirmed by the third-party risk function. Where the two disagree, the higher classification applies until the Chief Operating Officer decides. A relationship is reclassified upward immediately when its use changes, and downward only at the annual review.

- Critical: failure stops a Tier 1 or Tier 2 service within 24 hours, exposes protected data or causes direct client loss. Thirty-one.
- Important: failure degrades a service beyond five business days or affects a regulatory obligation. Sixty-eight.
- Standard: every other relationship. One hundred and thirty-two.

## 3. Due diligence before and during the relationship

Before a contract is signed, the third-party risk function assesses the provider's financial standing, ownership and control, sanctions and adverse-media screening, regulatory status where the service is regulated, information security, data protection practice including the provenance of any data supplied and the identity of every sub-processor, business continuity capability measured against the group's own recovery objectives, and conflicts of interest. For a provider of a learning system, adherence to the Ethical Technology Charter is assessed as a separate item.

A critical provider is assessed on site or by a structured remote review that examines evidence, not questionnaire answers, and the assessment is renewed every year. An important provider is assessed by questionnaire with evidence sampled, renewed every two years. A standard provider is assessed at onboarding and at each contract renewal. Findings are graded on the scale used in the Information Security policy. A critical provider with an open grade one finding cannot go live and, if already live, is placed on the exit path.

Introducers and intermediaries are a specific case. No introduction is accepted from an intermediary that has not passed the review, and the review examines the intermediary's own client due diligence, its remuneration arrangements and whether it has ever been refused by another institution. Forty-two intermediaries had passed the review at 30 June 2026 and three had been declined during the year.

## 4. Contract standards

Every contract with a critical or important provider contains the group standard clauses, and a departure from any of them requires the written approval of the General Counsel. The clauses set measurable service levels with remedies; give the group, its auditors and any regulator of a group entity rights of audit and access; require notification of any security or data incident within 24 hours; require sub-outsourcing to be disclosed and consented to in writing before it begins; and require the provider to maintain business continuity arrangements that meet the group's recovery objectives.

Data clauses apply the Charter. A provider that receives group or client data may use it only for the contracted service, may not sell it, aggregate it, or use it to train any system, and must state the origin of any data it supplies to the group. A provider of a learning system must accept that group prompts and outputs are not retained, that no training on group data occurs, that prohibited inferences are excluded by design and that the group may test for them.

Every critical contract provides for exit assistance of at least twelve months on termination for any reason, for the return or certified destruction of group data at exit, and for termination by the group on a change of control of the provider, on a sanctions event or on an unremedied breach. No provider is authorised to bind the group or to hold itself out as acting for the group beyond the contracted service.

- Measurable service levels with remedies.
- Audit and access rights for the group, its auditors and regulators.
- Incident notification within 24 hours and written consent before any sub-outsourcing.
- No sale, aggregation or training use of group or client data; origin stated for any data supplied.
- Twelve months of exit assistance and certified destruction of group data at exit.

## 5. Concentration and exit

No single provider may support more than two critical services without the approval of the Executive Committee, and every such approval is recorded with the reason and the mitigation. Five approvals were in force at 30 June 2026, the largest covering the primary hosted infrastructure provider, which supports three critical services and is mirrored by the second provider for each of them. A substitute provider or an in-house fallback is identified for every critical service before the contract is signed.

Every critical service has a written exit plan stating the substitute, the data to be transferred, the sequence of steps, the people responsible and the time the exit would take. Exit plans are tested on a desk basis every two years, and the test confirms that the substitute remains willing and able. Fourteen exit plans were tested in 2025; two were revised because the substitute had withdrawn from the market.

Where the group is the provider, in an intra-group arrangement, the receiving entity holds the same exit plan and the same substitute analysis, so that a local regulator can see that the entity could continue if the group service failed. The Programme Latitude expansion phases each include a third-party plan for the new offices before they open.

## 6. Ongoing oversight and reporting

The relationship owner holds a service review with each critical provider every quarter and with each important provider every six months. The review covers service levels, incidents, changes to the provider's ownership, sub-processors or control environment, and the status of assessment findings. Minutes are filed in the archive. Provider incidents are logged in the register and, where they affect a group service, follow the incident process in the Information Security policy.

Each provider confirms annually in writing that it remains in compliance with the contract and this policy. The third-party risk function reports to the Risk & Valuation Committee each quarter on the register, the assessment calendar, open findings, concentration approvals and exit tests, and to the Board annually. Internal Audit reviews the function and a sample of critical relationships every two years under the Internal Audit Charter.

## Key controls

- Register of 231 relationships with class, relationship owner, assessment dates and findings, maintained in Luxembourg.
- Three-class scheme confirmed by the third-party risk function, with the higher class applying in any dispute.
- Evidence-based assessment of every critical provider annually and of important providers every two years.
- Charter adherence assessed as a separate item for every provider of a learning system or of data.
- Standard contract clauses with General Counsel approval required for any departure.
- Executive Committee approval for any provider supporting more than two critical services.
- Written exit plan and identified substitute for every critical service, tested every two years.
- Quarterly service reviews for critical providers and quarterly reporting to the Risk & Valuation Committee.

## Related policies

- Information Security (IGC-DT-002)
- Business Continuity and Disaster Recovery (IGC-DT-007)
- Data Protection and Privacy (IGC-DT-001)
- Operational Resilience (IGC-GR-003)

### Colophon