IGUAKO CAPITAL · Group policy

Operational Resilience

This policy sets how IGUAKO Capital identifies the services whose interruption would harm clients, counterparties or the markets it trades in, how much interruption it will tolerate for each, and how it proves in advance that the tolerance holds. It covers the 11 important business services the group has mapped, the people, technology, premises, data and third parties each depends on, and the scenario testing that the Chief Operating Officer reports to the Board twice a year. It binds every entity, every one of the 36 offices and every supplier that supports a mapped service.

CODE	CATEGORY	VERSION
IGC-GR-003	Governance and risk	2.1
EFFECTIVE	**REVIEW**	**OWNER**
2024-04-01	Annual. Last reviewed March 2026. Next review due March 2027.	Chief Operating Officer

1. Purpose and scope

Business continuity asks how the firm recovers. Operational resilience asks what the firm must keep doing while it recovers. The two questions have different answers, and this policy exists for the second. It requires the group to name the services that matter most, to state how long each may be interrupted before the harm becomes intolerable, and to hold itself to that statement whatever the cause of the disruption.

The policy applies to all six divisions and to every legal entity in the 28 jurisdictions of domicile or registration. It reaches beyond the group perimeter to the custodians, administrators, data providers and technology suppliers that sit in the delivery chain of a mapped service. Where a supplier supports a service, the resilience of that supplier is treated as the firm's own concern and is tested as such.

It sits alongside three other documents. The Business Continuity and Disaster Recovery policy governs the recovery plans themselves. The Information Security policy governs the protection of systems from deliberate attack. The Third-Party Risk and Outsourcing policy governs the contracts under which suppliers are engaged. This policy draws on all three and adds the client-facing test that none of them asks on its own.

2. Important business services

An important business service is a service the group delivers to an external party, client, counterparty or fund, whose interruption would cause intolerable harm to that party, threaten the viability of the group or disturb the orderly functioning of a market in which the group is active. Internal processes, however critical to the firm, are not services in this sense. They are resources that services depend on.

As at 30 June 2026 the group has mapped 11 important business services. They include the execution and settlement of client orders, the payment of client money and the release of client assets, the daily valuation of managed portfolios, the drawdown of committed facilities for Commercial Finance borrowers, the treasury and liquidity operations of the group itself, and the reporting of positions to clients and to the supervisors of the licensed entities.

The list is reviewed by the Executive Committee every six months and whenever a division launches a product, opens an office or changes a material supplier. A service is added when the harm test is met and removed only when the Board accepts a written case that the harm test is no longer met. Programme Latitude adds services as new offices come to full capacity, and the Head of Expansion is required to propose the additions before an office opens.

- Execution and settlement of client orders across the Quantitative Strategies and Private Wealth & UHNW desks.
- Payment of client money and release of client assets on a valid instruction.
- Daily valuation and reporting of managed portfolios and fund positions.
- Drawdown of committed facilities for Commercial Finance borrowers within the contractual notice period.
- Group treasury and liquidity operations, including intra-group funding.
- Periodic and event-driven reporting to the supervisors of the licensed entities.

3. Impact tolerances

For every important business service the Board sets an impact tolerance: the maximum length of interruption, and where relevant the maximum volume of affected transactions, beyond which the harm becomes intolerable. The tolerance is stated as a fixed figure, not a range, and it is set with the client in mind, not the firm. A tolerance the firm cannot yet meet is still recorded, with a dated plan to close the gap.

The tolerances in force from 1 April 2026 are: four hours for the payment of client money and the release of client assets; the same business day for the execution and settlement of client orders in open markets; 24 hours for the daily valuation of managed portfolios; two business days for facility drawdowns; and 48 hours for regulatory reporting, save where a shorter deadline applies in the jurisdiction concerned.

Tolerances are approved by the Board on the recommendation of the Risk & Valuation Committee. They are recorded in the group resilience register alongside the resources each service depends on. The Chief Operating Officer may not relax a tolerance. Only the Board may do so, and only on a written case that records the harm the relaxation would permit.

4. Mapping and dependencies

Each important business service is mapped end to end. The map records the people who deliver it, the systems that process it, the premises from which it is run, the data it consumes and produces, and the third parties in the chain. The map names a primary and a secondary location for each step, so that the loss of one office never removes a service outright.

Mapping is a living record. Each service has a named service owner at Executive Committee level and a service manager who maintains the map. The map is refreshed every quarter and after every material change. The hub offices carry most primary roles: George Town, Luxembourg, Singapore and Panama City between them host the primary processing for nine of the 11 services, with Palm Beach and Brisbane as the principal secondaries.

The mapping exercise is where concentration shows. When the same supplier, data centre or team appears in the chain of several services, the concentration is recorded as a resilience risk and escalated to the Risk & Valuation Committee. Concentrations found in the 2025 mapping cycle led to the introduction of a second market-data feed and a second settlement agent in the Asia-Pacific region.

5. Scenario testing

The firm tests whether it can stay within each tolerance under severe but plausible scenarios. Severe means a scenario that has not been ruled out by the firm's own controls. Plausible means a scenario that has happened to a comparable institution or could happen given the firm's dependencies. Scenarios include the loss of a hub office, the failure of a critical supplier, a cyber incident that corrupts data, and the departure at short notice of a key team.

Testing runs on a fixed calendar. Each important business service is tested against at least two scenarios a year, one of which is run without notice to the operational teams. Tests are designed by the Group Resilience function, observed by Internal Audit and reported to the Risk & Valuation Committee with the elapsed time, the point at which the service was restored and the tolerance it was measured against.

A test that breaches a tolerance is a finding, not a failure of the test. Every breach receives a remediation plan with a named owner and a date. The 2025 cycle ran 24 tests across the 11 services and recorded three breaches, all of which were closed by March 2026. The results, in aggregate, form part of the annual resilience self-assessment the Board approves.

6. Governance and reporting

The Board owns the policy and approves the important business services, the impact tolerances and the annual self-assessment. The Chief Operating Officer is accountable for the resilience of the services. The Risk & Valuation Committee reviews testing and concentration risk each quarter. The Audit Committee receives Internal Audit's opinion on the programme once a year.

The annual self-assessment is a written document. It lists the services and their tolerances, describes the mapping and testing carried out, records every breach and its remediation, and states the Board's conclusion on whether the firm can remain within tolerance. The document is retained for six years under the Records Management and Retention policy and is available to the supervisors of each licensed entity on request.

Communication during an actual disruption follows the incident protocol in the Business Continuity and Disaster Recovery policy. This policy adds one requirement: when an important business service is interrupted beyond half its tolerance, the service owner informs the Chief Operating Officer and the Chief Risk Officer at once, and affected clients are told what has happened and when the service is expected to resume.

Key controls

- A register of important business services, refreshed every six months and approved by the Board.
- A Board-approved impact tolerance for each service, expressed as a fixed figure and never relaxed below Board level.
- End-to-end dependency maps for each service, with named primary and secondary locations and a quarterly refresh.
- At least two scenario tests per service each year, one unannounced, observed by Internal Audit.
- A remediation plan with a named owner and a date for every tolerance breach recorded in testing.
- Quarterly reporting of testing results and concentration risk to the Risk & Valuation Committee.
- An annual resilience self-assessment approved by the Board and retained for six years.

- Notification to the Chief Operating Officer and Chief Risk Officer when any live interruption passes half its tolerance.

Related policies

- Business Continuity and Disaster Recovery (IGC-DT-007)
- Information Security (IGC-DT-002)
- Third-Party Risk and Outsourcing (IGC-DT-006)
- Risk Appetite Framework (IGC-GR-001)