IGUAKO CAPITAL · Group policy

Business Continuity and Disaster Recovery

This policy keeps the services on which clients and counterparties depend running through the loss of people, premises, technology or a third party, in any of the 36 offices. It maps 38 services into three tiers with fixed recovery time and recovery point objectives, sets the architecture that replicates every Tier 1 system between George Town and Luxembourg, pairs every regional hub with an alternate site, fixes who may invoke the plan and how clients are told, and requires an annual full failover test and two exercises a year. Technology recovery is owned by the Head of Technology and Ethics under the overall ownership of the Chief Operating Officer.

CODE	CATEGORY	VERSION
IGC-DT-007	Data and technology	3.1
EFFECTIVE	**REVIEW**	**OWNER**
2022-08-01	Annual, and after any invocation. Last reviewed August 2026. Next review due August 2027.	Chief Operating Officer

1. Purpose and ownership

A payment that does not settle, an order that cannot be transmitted or a client who cannot reach their reporting is a harm the group has undertaken to prevent. This policy defines which services matter most, how quickly each must be restored, how much data the group is prepared to lose in restoring it, and who decides. It applies to every office, every hosted platform and every third party that supports a tiered service.

The Chief Operating Officer owns the policy and chairs the Crisis Management Team. The Head of Technology and Ethics owns technology recovery and the failover architecture. Each regional hub head owns the regional plan and each office head owns the local plan, including staff safety and premises. A new office may not open under Programme Latitude until its local plan has been approved and its staff have completed the call-tree test.

The policy is distinct from the Operational Resilience policy, which sets the tolerances for disruption the Board will accept and the mapping of services to the resources they depend on. This policy is the recovery mechanism that keeps the group inside those tolerances.

2. Business impact analysis and service tiers

A business impact analysis is completed for every service each year and on any material change. It states what the service does, who depends on it, what happens at one hour, four hours, one day and three days of outage, which systems, people, premises and third parties it relies on and which tier it belongs to. The analysis covered 38 services at 30 June 2026 and was signed by each service owner and the Chief

Operating Officer.

Tier 1 services must be restored within four hours with no more than fifteen minutes of data lost. There are nine: payments and settlement, order transmission and execution, treasury and liquidity management, client access to reporting, client instruction channels, custody reconciliation, sanctions screening, counterparty communications and security monitoring. Tier 2 services must be restored within 24 hours with no more than four hours of data lost. There are fourteen, including client onboarding, valuation production, regulatory reporting, model monitoring, complaints handling and payroll.

Tier 3 services must be restored within 72 hours with no more than 24 hours of data lost. There are fifteen, covering research production, marketing, training, internal reporting and similar functions. A service is placed in a tier by the Chief Operating Officer on the recommendation of the analysis, and a service owner who wants a lower tier must show that a client or counterparty would not be harmed by the longer outage.

- Tier 1: nine services; recovery time objective four hours; recovery point objective fifteen minutes.
- Tier 2: fourteen services; recovery time objective 24 hours; recovery point objective four hours.
- Tier 3: fifteen services; recovery time objective 72 hours; recovery point objective 24 hours.

3. Technology recovery

The group's primary systems run in George Town and Luxembourg, and each site replicates to the other. Tier 1 data is replicated every fifteen minutes, which is the source of the Tier 1 recovery point objective. Tier 2 data is replicated every four hours. Each regional hub holds a copy of its own region's client records so that the region can continue on local systems if both primary sites are unreachable. The two hosted infrastructure providers named in the third-party register each serve both sites, and neither is a single point of failure for any Tier 1 service.

Failover of a Tier 1 service is automated to the point of readiness and is executed on the authorisation of the Head of Technology and Ethics or the duty technology lead. The authorisation step is deliberate: the second Charter principle, proportionate automation, applies to recovery as it does to any other action, and an unnecessary failover carries a cost the group has chosen to have a person weigh. Failback to the primary site follows the same rule.

Backups are taken daily, are stored separately from the replicated systems, are encrypted and are tested for restoration monthly on rotation. The annual full failover test in May 2026 moved every Tier 1 service to the Luxembourg site in three hours and twenty minutes and every Tier 2 service within nineteen hours, both inside objective. Restoration of a single Tier 1 service is additionally tested every quarter, with each service tested at least once in three years.

4. Premises and people

Every regional hub has a designated alternate site from which the hub's Tier 1 and Tier 2 services can be run. George Town is paired with Palm Beach, with Luxembourg as the second alternate for treasury; Luxembourg with London; Singapore with Hong Kong; Dubai with Port Louis; Panama City with Miami; and Brisbane with Sydney. Each alternate holds the access, the seats and the recorded lines needed to carry the paired hub's critical work for a period of at least thirty days.

Every office with more than ten people maintains a remote-working arrangement that can carry its Tier 1 and Tier 2 work within four hours, using group-managed devices under the Information Security policy. Staff safety comes before any service objective. Each office holds a call tree that is tested twice a year; the test is passed when 95 per cent of staff are reached within two hours, and the 2026 spring test reached 97 per cent across the 36 offices.

The Caribbean and Florida offices follow a seasonal protocol from June to November. Each May the regional plan is reviewed, generator fuel and communications equipment are checked, and the Crisis Management Team confirms the relocation triggers. When a storm warning is issued for George Town, treasury operations transfer to Luxembourg before the office closes, so that the treasury hub is never run from a site in the path of a storm.

5. Third parties

A third party supporting a tiered service must demonstrate, before contract and at each assessment under the Third-Party Risk and Outsourcing policy, that its own recovery objectives are at least as demanding as the tier it supports. Where they are not, the group holds a substitute that can be brought in within the objective, and the substitute is named in the exit plan.

Payment routes are the most exercised dependency. Each correspondent bank on the approved panel is paired with another that can carry its full payment load for at least a week, and every pair is tested quarterly by routing live low-value payments through the alternate. Custodians and administrators are tested annually by reconciling positions through their recovery channel. Market data has a second source for every Tier 1 instrument set.

6. Invocation and crisis management

The plan may be invoked by the Chief Operating Officer, by the Chief Executive, or by any regional hub head for an event confined to that region. Invocation does not wait for certainty; the person invoking records the facts known and the plan is stood down later if the event proves minor. The Crisis Management Team assembles within one hour of invocation and comprises the Chief Operating Officer as chair, the Head of Technology and Ethics, the Chief Risk Officer, the General Counsel, the Chief Financial Officer and the head of each affected hub.

The team keeps a decision log from the moment of invocation. Every decision is timed, attributed and reasoned, and the log is filed as a governance record. Clients whose Tier 1 service is affected are told within two hours of invocation what has happened, what the group is doing and when the next update will come. Counterparties and correspondent banks are told through the counterparty communications channel, and regulators are informed under the Regulatory Reporting and Engagement policy.

Communications with the press are handled only through press@iguako.tech and the Chief Executive. Staff are informed through the call tree and the group messaging channel. No member of staff other than the Chief Executive or a person the Chief Executive names may speak publicly about an invocation while it is in progress.

7. Exercises, review and reporting

The Crisis Management Team exercises twice a year on a scenario it has not seen in advance. The 2026 exercises covered the loss of the Luxembourg site during a European settlement day and a ransomware event affecting the client reporting platform. Each regional hub exercises its own plan once a year. Every exercise and every invocation is followed by a written review within 20 business days that records what worked, what did not and the actions taken.

The Chief Operating Officer reports to the Risk & Valuation Committee each quarter on tests, exercises, invocations and open actions, and to the Board annually with the business impact analysis and the failover test result. Internal Audit reviews the programme every two years. The plan was invoked once in the twelve months to 30 June 2026, for a regional storm affecting Nassau, and the Nassau office's Tier 1 work ran from

George Town for three days without a missed objective.

Key controls

- Annual business impact analysis of 38 services signed by each service owner and the Chief Operating Officer.
- Three service tiers with recovery time objectives of four, 24 and 72 hours and matching recovery point objectives.
- Replication of every Tier 1 system between George Town and Luxembourg at fifteen-minute intervals.
- Human authorisation of every failover and failback by the Head of Technology and Ethics or the duty technology lead.
- Annual full failover test and quarterly single-service restoration tests, with results reported to the Board.
- Designated alternate site for every regional hub and a call tree tested twice a year to a 95 per cent standard.
- Quarterly live testing of every correspondent bank pair and annual recovery-channel testing of custodians.
- Crisis Management Team decision log and client notification within two hours of any Tier 1 invocation.

Related policies

- Operational Resilience (IGC-GR-003)
- Information Security (IGC-DT-002)
- Third-Party Risk and Outsourcing (IGC-DT-006)
- Liquidity and Funding (IGC-GR-002)

Colophon

IGUAKO Capital is a work of institutional fiction by the Iguako Institute for Applied Unreality (iguako.tech). This document is part of that work. It creates no rights or obligations, describes no licensed entity and is not an offer, a contract, a client record or advice.