Finalto Operational Resilience

Overview

Finalto is a dynamic and innovative prime brokerage that provides bespoke and powerful fintech and liquidity solutions to a broad range of clients. Our award-winning proprietary technology stack and in-house expertise allow us to deliver excellence to our customers, so we understand the importance of providing uninterrupted delivery of products and services through our technology solutions.

This operational resilience notification ("Notification") provides an overview of our approach and a summary of the plans and processes we have in place to resist, absorb, and recover from or adapt to an unexpected event that may cause harm, destruction, or loss of ability to perform operational functions.

Summary

We understand the significance of preparing for various uncontrollable events that could disrupt our ability to operate as usual and have implemented robust measures to provide for business continuity under a range of potential scenarios. Operational resilience is at the heart of our business strategy, ensuring that we remain prepared to protect our clients, assets, and reputation in the face of any disruption.

We are committed to delivering continuous uninterrupted service to our clients and continuously evaluate and enhance our Business Continuity and Disaster Recovery Plans to ensure they are up to date and robust.

We are committed to adhering to best practice standards and the evolving regulatory landscapes in which we operate.

We conduct continuity training and exercises to familiarise personnel with their responsibilities and to ensure that essential staff can access the necessary equipment, permissions, and connectivity to function effectively from recovery sites and remote locations. Testing and training are essential for assessing, demonstrating, and improving our ability to maintain essential functions and services.

We review all plans at least annually to evaluate their effectiveness, ensure they are accurate and remain aligned with the business, and to ensure awareness across the business.

For more information please contact:

Client Services on +44 203 455 8750 or cs@finalto.com.

Commitment & Compliance

Finalto recognise the importance of operational resilience to our clients and stakeholders and are committed to delivering a continuous service. The ability to withstand and recover from disruptions is a necessity, our approach is based on three key objectives:

- **Prevent Disruptions:** Through investment in technology, people and processes combined with proactive risk management and ongoing monitoring of our systems and processes.
- **Respond Effectively to Disruptions:** By ensuring that we can rapidly and effectively respond to unforeseen events and rely on back-up services wherever possible to ensure continued service and minimum downtime.
- **Recover and Learn from Disruptions:** We continue to report and review, minimising downtime and improving our systems based on lessons learned from incidents.

Finalto ensure this is delivered effectively and compliant by adopting the "three lines of defence" approach to provide clear roles and responsibilities for managing and overseeing risks across different functions, ensuring that risks are properly identified, managed, and mitigated.

Finalto also recognise that focus on Operational resilience is subject to increasing regulatory expectations, especially in financial services and technology providers. Regulators globally are continuously refining frameworks to ensure that organisations not only manage risks but also ensure continuity in the face of operational shocks. We actively develop our frameworks, policies, and processes in order to meet these requirements and seek assurance via audit against guidance and regulation to include:

- **ICT -** EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)
- **DORA** – The Digital Operational Resilience Act (Regulation (EU) 2022/2554)
- **MAS -** Monetary Authority of Singapore (MAS) Operational Resilience Guidelines
- **TRM** - MAS Technology Risk Management (TRM) Guidelines
- **FCA** - Operational Resilience Policy (PS21/3)
- **PRA** - Supervisory Statement on Outsourcing and Third-Party Risk Management (SS2/21)

Note that this is not an extensive list as we consider guidance and regulatory material from numerous sources and thematic reviews from time to time. These referenced materials are also updated regularly or may be superseded but are current at the time of writing.

Contractual Supplement

This Notification operates to supplement the Finalto Standard Terms of Business ("STB") in place between clients of any Finalto entity set out at Appendix I of this Notification. This Notification, unless otherwise specified, relates solely to Information and Communication Technology ("ICT") services provided by Finalto to you. Descriptions of all critical or important ICT functions provided by Finalto, directly or indirectly, are included in this Notification (such functions are referred to in this Notification, whether provided by Finalto or a subcontractor of Finalto, as "Critical Functions") as set out at Appendix II of this Notification.

The Finalto entity with which you have a contractual relationship provides further information on its protection of certain categories of data in its respective Privacy Policy (links to which are set out at Appendix I of this Notification). Such Privacy Policies set out, amongst other things, your rights in relation to such data. Finalto, further to the STB in place with you, also owes obligations to you in relation to confidential information.

The following provisions apply to the STB and operate alongside, and are subject to, the provisions contained therein:

(i) Service level descriptions are set out at Appendix II of this Notification.

(ii) Data storage and processing locations are set out at Appendix III of this Notification.

(iii) Finalto shall provide to you reasonable assistance in relation to any incident which negatively impacts your access to Finalto's ICT services.

(iv) Finalto shall cooperate with any competent authority or resolution authority in relation to services falling under the STB.

(v) Finalto shall use reasonable efforts to participate and cooperate with threat-led penetration testing you carry out in relation to services provided by Finalto to you but you acknowledge that the costs to carry out such testing, unless otherwise agreed by Finalto, shall be borne by you.

(vi) Finalto warrants that it:

  (A) provides compliance (including but not limited to data protection) training and ICT security awareness training to its staff; and

  (B) takes reasonable precautions and has in place all reasonable measures and policies in place to provide an appropriate level of security for the provision of ICT services to you.

(vii) Finalto shall grant:

  (A) as far as reasonably possible and on reasonable written notice from you, rights of access, inspection and audit by an independent third party appointed by you in relation Critical Functions. Such rights shall be granted remotely or by way of assurance provided by Finalto wherever possible but relevant documentation, if related to Critical Functions, may be provided on-site if required and if there is no competing confidentiality, or other legal, obligation restricting on-site disclosure. In relation to any inspection or audit carried out in this Notification, Finalto shall

cooperate, as far as reasonably possible, with all requests unless such requests are, in the reasonable opinion of Finalto, vexatious or designed to burden Finalto in bad faith;

(B) rights of access, inspection and audit to any competent authority in relation to, amongst other things, questions arising from the Critical Functions shall be granted on request by a competent authority.

(viii) Any on-site right of access, inspection, or audit shall be carried out within the working hours of the relevant Finalto entity with which there is an STB in place with you. Any right of access, inspection, or audit shall not occur more than once per year (commencing from the date of this Notification and, subsequently, a year being calculated from the date any right of access, inspection, or audit is concluded). The cost of any right of access, inspection, or audit shall be borne by you.

(ix) All records and documentation ("Records") which are the subject to rights of access, inspection, and audit under this Notification, may be limited:

(A) to regulatory time periods and will only be shared insofar as such records have not otherwise been disposed or deleted in accordance with such time periods;

(B) to such Records required for the Critical Functions;

(C) by confidentiality obligations, pertaining to Finalto or any of its counterparties, to which Finalto must adhere whether through limited or redacted disclosure, or a reasonable omission from disclosure;

(D) to methods other than an on-site visit if such Records retrieval requires access to confidential systems which Finalto cannot, in its reasonable opinion, protect or redact satisfactorily to protect confidential information.

(x) The STB contains a termination for convenience notice period or the parties may agree such other notice period for termination ("Transition Period"). During the Transition Period, Finalto agrees to continue providing the ICT services as provided by the STB and will endeavour to assist, wherever reasonably possible, with any transition to a new provider of the ICT services if such assistance does not: (i) breach any terms of confidentiality, (ii) compromise any intellectual property of Finalto, or (iii) unduly burden Finalto.

Key Controls for Operational Resilience

We have summarised our key controls in this section to provide an overview of the controls in place to prevent disruptions and to respond and recover if a disruptive event occurs.

1. **Governance and Oversight**
    - Governance The Risk & Compliance Committee is a board level committee which approves the operational resilience framework which is designed to identify, assess, and manage risks across all functions.
    - We operate a three lines of defence model, with the business providing disruption prevention, resilience and incident management controls, oversight provided by risk and compliance and supplemented by an Operational Risk Committee. Assurance is provided by internal and external audit.
    - Clear Accountability: Senior management has clear accountability for understanding their risk environment, for resilience, and ensuring that all employees understand their roles and responsibilities in maintaining operational stability. This is recorded and assessed via the Risk and Control Self-Assessment (RCSA) process.

2. **Business Continuity Planning (BCP)**
    - We have established comprehensive business continuity plans that outline specific procedures for managing various types of disruptions, whether operational, technical, or environmental.
    - Business Continuity Plans are in place at various levels, for all operational departments, for each physical location in which we operate, and for the overall company. This provides for a comprehensive and co-ordinated approach.
    - Cross-jurisdiction Coordination: In line with global operations, our BCP is designed to function seamlessly across the UK, Europe, and Singapore, enabling cross-border support in the event of regional disruptions.

3. **Disaster Recovery Planning (DRP)**
    - Disaster Recovery Planning incorporates our Disaster Recovery policy and processes. DRP is a critical component of our overall resilience strategy and focuses specifically on the recovery of our IT systems and data following a significant disruption.
    - DRP is designed to ensure rapid restoration of services and data integrity, minimizing business disruptions and financial losses.
    - Continuous and secure backups of critical data are stored offsite and, in the cloud, to ensure data is always recoverable, even in the event of physical damage of systems.
    - Key operational systems are duplicated and designed to switch to backup servers in the event of a primary system failure. This ensures continuity of service with minimal downtime.
    - Data centres are geographically distributed across multiple regions, including the UK, New York, and Singapore, allowing us to leverage regional redundancy in the event of localised disruptions.

4. **Interconnected approach**

Our BCP and DRP are interconnected, ensuring clear objectives and recoverable services.

- Clear Recovery Time Objectives (RTOs), Maximum Acceptable Outage (MAO), and Recovery Point Objectives (RPOs) are in place for each critical operation and system:
- RTO refers to the maximum acceptable time that a system or function can be offline before recovery.
- MAO refers to the maximum period during which a critical function or system can be unavailable.
- RPO refers to the maximum acceptable amount of data that can be lost in a disaster, measured by the time between data backups.
- These objectives record the disruption which could be incurred without causing significant disruption to firm, its clients, or the broader financial system. They ensure that recovery processes are prioritised and aligned with business needs, with more critical systems having shorter RTOs, MAOs and RPOs.

5. IT and Cybersecurity Risk Management

- Our technology infrastructure is designed to support high availability, scalability, and redundancy. We employ failover systems to minimize the impact of system outages.
- We have implemented comprehensive cybersecurity protocols, including encryption, multi-factor authentication, and 24/7 monitoring to safeguard sensitive financial data from cyber threats. These measures align with industry standards and local regulatory requirements, including GDPR (Europe) and the Personal Data Protection Act (Singapore).
- We carefully assess and monitor the resilience capabilities of our third-party service providers to ensure that any risks from external dependencies are mitigated.

6. Incident Management

- Rapid Response Protocols: In the event of an operational disruption, our Incident Response Team (IRT) is activated immediately to mitigate impact and restore services.
- Communication Strategy: We ensure timely, clear, and transparent communication with stakeholders, regulators, and customers during and after any disruption, ensuring that all parties are well-informed about the status and progress of recovery efforts.
- Post-Incident Reviews: After every incident, we conduct a comprehensive review to identify the root causes, assess the response effectiveness, and implement improvements where necessary.

7. Resilience & Recovery Testing

- We conduct regular disaster recovery tests to ensure that our systems, processes, and personnel are prepared to respond swiftly in the event of a disaster. These tests include simulations of various disaster scenarios, from natural events like earthquakes or floods to technical failures and cybersecurity breaches.
- Testing results are analysed to identify areas for improvement, and we update our plans based on lessons learned.
- Regular stress tests, simulations, and drills are conducted to ensure that our business continuity plans remain effective under a variety of scenarios.

8. **Regulatory Compliance and Reporting**
    - We comply with the regulatory standards set by the FCA, PRA, EBA, and MAS to ensure operational resilience. Our compliance team works closely with regulators to meet reporting obligations and maintain transparency.
    - We have specific processes in place to ensure we can provide timely and accurate reports to regulators, ensuring we meet our obligations across all jurisdictions.

9. **Continuous Improvement and Innovation**
    - We continuously assess operational risks through the Risk and Control Self-Assessment process which incorporates ongoing monitoring and audits, ensuring that our controls evolve in response to business changes and emerging risks.

Cyber Security - Controls & Standards

Finalto Technology Security is an expansive area which covers the vulnerabilities of systems and networks and aims to ensure the business is protected from incidents and failure of services.

This section provides a summary of the key controls in place;

Network Configuration

- ✓ Network segmentation to separate the user's subnets from the servers subnets, DMZ and other untrusted networks.
- ✓ Firewalls between untrusted, demilitarized zone and internal network zones.
- ✓ Intrusion/Detection and prevention systems at the perimeter and critical points of the sensitive data environment.

Vendor defaults

- ✓ vendor default settings and credentials are changed at installation.
- ✓ unnecessary default accounts are removed or disabled before installing a system on the network.
- ✓ only necessary services, protocols, daemons, etc., as required for the function of a system.
- ✓ configuration standards are developed for system components consistent with industry accepted system hardening standards based on CIS benchmarks.

Data Protection

- ✓ Data storage amount and retention time is limited to that required for legal, regulatory, and/or business requirements.
- ✓ Defined processes in place for informing, accessing, securely deleting, rectifying, and restricting processing as per GDPR requirements.

Cryptographic Keys & Encryption

- ✓ Access to cryptographic keys is restricted to the fewest number of custodians necessary and stored in the fewest possible locations.
- ✓ Generation of strong cryptographic keys as based on industry best practices.
- ✓ Secure storage of cryptographic keys.
- ✓ Only trusted keys and/or certificates are accepted.
- ✓ TLS v1.2 or above for any required services, protocols or daemons whenever sensitive data is transmitted or received.

Device security

- ✓ Centrally managed Anti-malware software deployed on systems.
- ✓ Automatic updates enabled and anti-virus software and definitions kept current.
- ✓ Periodic scans are enabled and being performed.
- ✓ Anti-virus mechanisms are generating audit logs and unable to be disabled or altered by users.
- ✓ Extended Detection and Response (XDR) is implemented to enhance and unify threat detection, investigation, and response across various security layers within the company.
- ✓ Data encrypted at rest on end-user workstations.
- ✓ Data encrypted at rest on databases and servers.

Vulnerability and Patch Management

- ✓ All system components have critical security patches installed.
- ✓ Internal and external network vulnerability scans run at least quarterly and after any significant change in the network.
- ✓ Authenticated vulnerability scans implemented.
- ✓ Internal and external penetration test at least annually or after any significant change.
- ✓ Exploitable vulnerabilities found during penetration testing fixed, followed by repeated testing to verify the corrections.

System Acquisition, Development & Maintenance

- ✓ Development/test environments are separated from production environments.
- ✓ Development, test, and/or custom application accounts, test data, user IDs, and passwords are removed before system goes to production.
- ✓ Change-control procedures are documented.

- ✓ Functionality testing in place to verify that the change does not adversely impact the security of the system.
- ✓ We have back-out/roll-back procedures for all changes.
- ✓ Software-development processes address common coding vulnerabilities and are developed based on OWASP secure coding guidelines.
- ✓ We perform static analysis (Static Application Security Testing (SAST)) on source code to identify security vulnerabilities.
- ✓ We perform dependency checking on source code to identify security vulnerabilities third-parties libraries.

Maintaining secure systems and applications

- ✓ Third-Party vendor management in place.
- ✓ Security reviews and continuous third-party monitoring on critical third-party vendors.
- ✓ All third-party software is under vendor support.
- ✓ All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, software and unnecessary web servers is removed from servers.
- ✓ Limited access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users.
- ✓ Only authorised software can be loaded into a system process.
- ✓ Only authorised, digitally signed scripts are allowed to run on a system.

Access Control and Authentication Measures

- ✓ All generic user IDs and accounts are disabled or removed.
- ✓ Access for all terminated users is immediately deactivated.
- ✓ Accounts used by third parties via remote access are enabled only during the time period needed and disabled when not in use.
- ✓ Users accounts are locked after 6 repeated unsuccessful login attempts.
- ✓ Users re-authenticated after a session has been idle for more than 15 minutes.
- ✓ User password parameters configured to meet specific requirements and must be changed at least annually.
- ✓ Multi-factor authentication incorporated for all administrative access.
- ✓ Multi-factor authentication incorporated for all remote network access (user, administrator and third party) originating from outside the entity's network.
- ✓ Access to data provided to users based on least privilege and need-to-know basis.

Restricting physical access

- ✓ CCTV and access-control mechanisms in place to monitor physical access to sensitive areas and protected from tampering.
- ✓ Physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is restricted.
- ✓ All media is destroyed when it is no longer needed for business or legal reasons.
- ✓ Sensitive hard-copy materials crosscut shredded.
- ✓ Sensitive data on electronic rendered unrecoverable during disposal.

Logging and Monitoring

- ✓ Audit trails enabled and active for system components.
- ✓ Audit trail files promptly backed up to a centralized log server.
- ✓ Security Information and Event Management (SIEM) system in place that generates alerts for critical security incidents.
- ✓ All critical system clocks and times synchronized through use of time synchronization technology, and is the technology kept current (NTP).

Wireless Access Points

- ✓ Strong encryption is enabled for authentication and transmission for wireless networks transmitting sensitive data.
- ✓ We have separate wireless networks for corporate and guest users.

Backup

- ✓ We automatically backup all systems on a regular basis.
- ✓ We perform a complete system backup on all critical systems through processes such as imaging, to enable the quick recovery of an entire system.

Maintain an Information Security Policy System

- ✓ Security policies are established, published, maintained, distributed to all relevant personnel, and reviewed at least annually.
- ✓ Acceptable usage policies for critical technologies developed to define proper use of these

technologies such as but not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.

- ✓ Security policy and procedures clearly define information security responsibilities for all personnel.
- ✓ Risk assessment process is implemented on an annual basis and upon any significant changes.
- ✓ Security awareness training program is implemented for all employees for raising awareness of the importance of sensitive data security and the information security policies and procedures.
- ✓ Potential personnel is screened prior to hire to minimize the risk of attacks from internal sources.

Incident Response

- ✓ The incident response plan is in place to respond to a system breach.
- ✓ The plan addresses the following:
  - Roles, responsibilities, and contact information.
  - Specific incident response procedures
- ✓ The plan is reviewed and tested at least annually.
- ✓ Designated personnel available on a 24/7 to respond to incidents.
- ✓ Appropriate trainings are provided to staff with security breach response responsibilities.
- ✓ Critical systems set up in High Availability.
- ✓ All critical service departments are supported in multi-locations and all staff able to work remotely. Business Continuity and Disaster Recovery Plans include procedures to transfer services to alternate locations.

APPENDIX I

List of Finalto entities and associated Privacy Policies

Finalto Entity	**Privacy Policy**
Finalto Financial Services Limited, 11th Floor, Broadgate Tower, 20 Primrose Street, London, EC2A 2EW, United Kingdom, company number: 6557752, LEI: 549300FSY1BKNGVUOR59	FS Privacy Policy
Finalto Asia Pte Ltd, 79 Anson Road, #16-03/06, UE BizHub, Singapore 079906, company number: 201923501E, LEI: 549300I2JZKYNQ1VF157	Finalto Asia Privacy Policy
Finalto EU Ltd, 148 Strovolos Avenue, 4th floor, 2048 Strovolos, Nicosia, Cyprus, company number: 332334, LEI: 549300M2TA4XMO4UUZ22	Finalto EU Privacy Policy
Any other entity specified by Finalto from to time.	

APPENDIX II

Critical Functions

Please note the below are illustrative only. All service level agreements ("**SLAs**") are provided as objectives/aims and do not reflect a guarantee of performance. Each issue will be context-specific and will require investigation however, the below SLAs provide indicative objectives within Finalto's Business Continuity Plan.

		Recovery Time Objective (RTO)[1]	Maximum Acceptable Outage (MAO)[2]
Critical Systems	ClearVision – Trading platform	< 45 mins	1 hour
	Trading platform (external provider 1)	< 45 mins	1 hour
	Trading platform (external provider 2)	< 45 mins	1 hour
	Trading platform (external provider 3)	< 45 mins	1 hour
	Clear (Risk/Control/Portal) Trading Platform	< 45 mins	1 hour
Critical Services	Client Support & Funding	< 5 mins	45 mins
	Client & Firm Trading	< 5 mins	45 mins
	IT Support - Trading Platforms	< 5 mins	45 mins

[1] Recovery Time Objective (RTO) is the time within which we aim to restore a critical system, process, or service after a disruption caused by a reasonably foreseeable event. This helps prioritise resources and efforts to recover essential operations.

[2] Maximum Acceptable Outage (MAO) is the projected maximum time a critical business system or function should be unavailable during reasonably foreseeable events. The MAO acts as a threshold in the operational resilience strategy, providing a target we can test against to ensure we can continue to operate even under significant stress.

APPENDIX III

Location of Data Storage

Please note, in addition to the jurisdiction of the Finalto counterparty with which you have a contractual relationship, your data will be stored in the following locations (in accordance with contractual data protection and confidentiality provisions as well as data protection laws in the relevant jurisdiction):

Service	**Location**
ClearVision and Internal Market Risk Tool	United Kingdom, Denmark, Ireland
Finalto Data Centres (Trading)	United Kingdom, United States of America (New York), Singapore, and Japan
External Technology Provider	United Kingdom
External Back-Office Provider 1	Sweden
External Back-Office Provider 2	In EU Model Clause compliant Data Centres
Any other data storage locations specified by Finalto from to time.	