UBS

Global Supplier Policy

Business Continuity and Operational Resilience (BCOR) Policy

WHY

To help safeguard global financial systems and avoid systemic impact on other market participants, as required by our Regulators.

WHEN

Whenever you supply BCM-Critical Services/Products, or support an Important Business Service.

WHAT to know about HOW to comply

1. BCOR Framework

- You must maintain a BCOR Framework, setting out your approach to identifying and managing business continuity and operational resilience risk. Your BCOR Framework at a minimum must include:
  - an owner within your organization who has overall responsibility to ensure adherence with the BCOR Framework;
  - the governance of the BCOR Framework;
  - the methodology for identifying critical products and services, and the risks inherent in providing them;
  - minimum standards covering:
    - i) business impact analysis as it relates to relevant risks;
    - ii) the creation and maintenance of BCOR Recovery Plans to address any risks identified; and
    - iii) testing of BCOR Recovery Plans ;
  - an annual review process to ensure the BCOR Framework remains up to date; and
  - a version control log.

2. Crisis Management Plans

- You must maintain a Crisis Management Plan to assist in effectively and efficiently managing the effects of a crisis and recovery from it.

3. BCOR Recovery Plans

- You must create and maintain BCOR Recovery Plans to ensure critical products and services can be recovered within a Recovery Time Objective and an Impact Tolerance Limit (where applicable) specified by us in the case of an Operational Event.
- The BCOR Recovery Plans must include:
  - recovery solutions to address, where applicable, loss of your premises, loss of technology, loss of Staff, or loss of Subcontractors, to ensure our Recovery Time Objectives are met;
  - enhanced recovery solutions to address specific scenarios to ensure our Impact Tolerance Limits are not breached;
  - procedures for invocation of the BCOR Recovery Plans;
  - ownership of the BCOR Recovery Plans; and
  - a version control log.
- BCOR Recovery Plans must be reviewed and updated on an annual basis, and in the event of any material changes to your organization or infrastructure, or any material changes to the scope of Products or Services provided under the Agreement.

4. Testing of BCOR Recovery Plans

- You must test BCOR Recovery Plans at least annually to demonstrate that each solution can meet the Recovery Time Objective and Impact Tolerance Limit (where applicable). Testing should include, where applicable:
  - Staff relocation to secondary sites to validate connectivity, capacity, technology provision and any other assets required to provide the Products or Services following a local or wide-area disruption;
  - work transfer to alternative sites to validate capability, capacity, technology provision and any other asset required to provide the impacted Products or Services following a local or wide-area disruption or if a high volume of Staff are unavailable;
  - technology fail-over from production to secondary datacenters or applications to demonstrate capability, connectivity and capacity of technology required to provide the Products or Services;
  - reconstruction of technology assets to validate that the Services can be restored following a data corruption, loss of information or technology disruption which renders existing primary and back-up capabilities as compromised;
  - component testing of cloud functionality;
  - recovery testing with Subcontractors that are critical to the Products or Services, to validate that they can support the specified Recovery Time Objective or Impact Tolerance Limit (where applicable); and
  - testing of any other solutions which enables the recovery of, or provides resilience to, the Products or Services.
- You'll document any issues identified in the testing and ensure they're assigned ownership and a timeframe for resolution.
- You'll provide reasonable notice to us of your testing

and, when requested by us, allow us to participate in the testing of your BCOR Recovery Plans.

- You'll participate in business continuity and operational resilience testing undertaken by us at no additional cost up to once per year.

5. Activation of BCOR Recovery Plans

- You'll notify us as soon as possible and in any event within 30 minutes of the actual or likely occurrence of an Operational Event.
- Where an Operational Event has occurred or is likely to occur, we may require immediate activation of your BCOR Recovery Plans applicable to the impacted Products or Services.
- Where circumstances prevent you from notifying us prior to activation of the BCOR Recovery Plans, you'll activate the required plan and notify us of this as soon as possible afterwards.
- As far as possible you'll involve us in key decisions concerning restoration of the Products and/or Services.
- Upon invocation of the BCOR Recovery Plans, you must complete implementation of the relevant processes documented in the plans to recover the Products and/or Services within the specified Recovery Time Objective and Impact Tolerance Limit (where applicable)
- At all times during the occurrence of an Operational Event, you'll make available to us such access, resources, personnel, facilities, and assistance as we may require and will cooperate fully with us.
- In the event of any failure or default by you or any Subcontractor in connection with the invocation of the recovery plans, we'll be immediately entitled to remedy such failure or default ourselves (or by a third party on our behalf) and you'll pay our reasonable costs and expenses incurred in doing so.
- You can't charge, or increase the Charges, for

implementing and invoking the BCOR Recovery Plans.

6. Reporting

- Unless we notify you otherwise, we require you to provide the following on an annual basis:
  - details of the BCOR Recovery Plans which must include an overview of all applicable scenarios and solutions for recovery and resilience used to mitigate relevant risks and the Recovery Time Objective and Impact Tolerance Limits (where applicable) for the overall products or services provided;
  - testing results of the BCOR Recovery Plans for each solution documented including the recovery time achieved and any issues identified during the test, with a time frame for resolution of each; and
  - where applicable, a summary of the due diligence and recovery testing performed for all critical Subcontractors to demonstrate that they can meet the Recovery Time Objective and Impact Tolerance Limit (where applicable) for the overall product or service.

7. Additional Requirements

- You must appoint a BCOR Coordinator and, in each case, identify a reserve individual to each such role, and notify us of such appointments.
- You must provide annual business continuity and operational resilience awareness training to Staff, which must include the approach to managing relevant risks as documented in your BCOR Framework and the specific processes and procedures set out in the BCOR Recovery Plans . Upon our request, you must provide details of the training program to us. If the Security Exhibit is applicable, you must ensure that its requirements continue to be met in the event of an Operational Event, unless otherwise agreed with us.