UBS

Global Supplier Policy

Audit Policy

WHY

To provide us with the information and oversight to help us meet our legal and regulatory obligations.

WHEN

Whenever you provide Outsourcing Services or BCM-Critical Services, or whenever the provision of the Services is regulated by a Regulator of UBS.

WHAT to know about HOW to comply

1. Scope of audit

- You must grant (or, in the case of your Subcontractors, procure for) the Auditors the right to access any of your, your agents' or your Subcontractors' premises, personnel and relevant records as may be reasonably required in order to:
  - fulfil any legally enforceable request by a Regulator; or
  - verify that you're complying with the terms of the Agreement (including any applicable Policies).
- You must provide Auditors with reasonable co-operation and access in relation to each audit.
- The Auditors' review rights will include, among other things, the right to review:
  - your risk management processes;
  - your information security and your physical, technical and administrative controls;
  - your disaster recovery and Business Continuity Plans,
  - any interdependencies in your supply chain and the operational resilience of your supply chain;
  - internal or external audit reports (e.g. ISO 27001, SOC 2 type 2, PCI DSS, etc.) and penetration test reports which have been completed by any independent bodies (these may be edited to restrict our access to your Confidential Information relating to other clients); and
  - if you use Subcontractors, your Subcontractors' compliance with the Subcontractor Policy.
- You acknowledge that our regulated financial services clients may also be required to audit you in accordance with Applicable Laws, and that the rights in this Audit Policy extend to those clients (or their regulators or appointed auditors).

2. On-site audits

- On-site audits will be performed in accordance with accepted national and international audit standards.
- When performing audits in multi-client environments, we understand that care should be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated, and we will endeavor to work with you in that regard.
- We will, where appropriate, consider performing pooled audits organized jointly with your other clients, to use audit resources more efficiently and to decrease the organizational burden on you and your clients.
- Before a planned on-site visit, we or the Auditors will provide reasonable notice to you. However, this may not be possible where:
  - the audit arises from an emergency or crisis situation, or a suspected act of fraud;
  - the audit is required by a Regulator and its timing or scope are beyond our control; or
  - for any other reason the audit would no longer be effective.
- You'll bear your own costs and expenses incurred in respect or any audit, as we will bear our own costs.

3. Remediation activities

- If an audit finds that you haven't complied with the terms of the Agreement (including any applicable Policies), you must promptly take all necessary steps to remediate the non-compliance.
- You must also implement any other reasonable recommendations made by the Auditor within the timeframe specified by the Auditor (or where no such timeframe is specified, within a reasonable timeframe).

4. Survival

- This Audit Policy will survive termination or expiration of the Agreement.