Cyber Minimum Requirements

The Supplier must ensure that it has in place appropriate cybersecurity controls to satisfy the following requirements:

1. Information and Cybersecurity Program

1.1 The Supplier must be able to demonstrate they have established an information security and cybersecurity framework that includes policies, standards, controls and processes with an organisational structure that supports effective implementation of security risk management in accordance with industry best practice (e.g. NIST, ISO/IEC 27001, ITIL, COBIT)

2. Access Control

2.1 The Supplier must maintain a documented and secure user access management process, adhering to the principles of least privilege and segregation of duties for the creation, distribution, management of authentication credentials and remote access including:

(a) Remote login access to The Supplier network must be encrypted and always use multi-factor authentication.

(b) Access to the HSBC network must use industry standard technology approved by HSBC.

3. Vulnerability Assessment

3.1 The Supplier must establish and maintain an up-to-date vulnerability management process designed for effective monitoring, timely detection to identify, investigate, and remediate any cybersecurity vulnerability within the Supplier-owned or managed applications, infrastructure network and system components.

4. Information Technology asset management

4.1 The Supplier must have a solution to detect and categorise hardware and software used to store, process and transmit HSBC information.

4.2 Technology assets and their associated configuration must be identified, named, classified, documented, and recorded in an authorised inventory. Access to records in the inventory must be authorised, periodically reviewed and maintained.

5. Logging & Monitoring

5.1 The Supplier must ensure that it's IT systems (e.g. applications, networking equipment, security devices and servers) used for the provision of service(s) to HSBC have the mechanism for logging, monitoring, and alerting of event data (i.e. physical and logical access logs, application logs, systems logs, network logs and alerts).

5.2 The Supplier must restrict audit logs access to authorised personnel and maintain records that provide unique access accountability.

5.3 The Supplier must monitor audit logs to detect suspicious activities from all parties, including trusted parties and 4th parties (e.g. CSP's).

6. Network Security

6.1 The Supplier must ensure that all the systems, applications and network devices used in the provision or support of services to HSBC are protected from inbound and outbound network threats. The Supplier must maintain an up-to-date network diagram that shows the infrastructure, security controls and the data flow for the service being provided to HSBC.

7. Configuration Baseline Management

7.1 The Supplier must have an established framework to ensure that all configurable systems/ networking equipment in scope of the service provided are securely configured. Only approved baselines with configurations must be deployed to IT assets and must be monitored and maintained on a continuous basis for any remedial action.