HSBC

Business Continuity & Incident Management (BCIM)

Client Continuity Statement

Revised August 2024

General Statement Regarding HSBC's BCIM Position

HSBC regards the ability to continue to provide banking and other financial services to our customers as fundamental to our business. HSBC has a well-established Business Continuity & Incident management (BCIM) programme in place designed to protect our staff, assets, processes, and customers in the event of an interruption to our normal business activities. Additionally, regulators have been rolling out Operational Resilience frameworks to select markets, looking at a holistic end-to-end service view focused on preventing, detecting, and remediating operational disruptions.

1. Management and Governance

HSBC have a global BCIM team supported by regional and market-level teams, with qualified and experienced business continuity and risk management professionals. The BCIM team, supports the compliance of our businesses and function with HSBC's Business Continuity Management (BCM) and Major Incident Management (MIM) Operation Instructions.

A global Monitoring and Support Services (MASS) team provides support to teams for their management of BCIM controls. Status updates are reported through relevance global and regional business Non-Financial Risk (NFR) committees to ensure the appropriate levels of governance around BCIM risks and controls.

2. Business Continuity Planning and Maintenance

Business Continuity (BC) has evolved and matured to leverage different recovery strategies that work together to optimize resilience and protect the bank's operations. BC Planning includes an impact analysis, strategy and response development, and a robust exercise program.

2.1 Business Impact Analysis

Each business or function within HSBC undertakes a Business Impact Analysis (BIA) which determines the criticality and the Maximum Disruption Time (MDT) that the business can tolerate. The BIA identifies dependencies that the business or

function deems to be important to support their efforts in continuing critical operations during an incident.

2.2 Business Continuity Plan

Each Business Continuity Plan (BCP) reflects the requirements and criticality of their operations and helps HSBC respond effectively to different interruption scenarios, including but not limited to;

- Loss of staff
- Loss of premises
- Loss of IT services
- Loss of key third party services

2.3 Response Strategies

With ongoing improvements in technology and constant optimization of strategies, it means that BCIM responses also evolve to reflect the latest ways of working.

- Technology advances enable the use of secure and proprietary networks to support remote working capabilities through corporate laptops or thin-client solutions.
- Premise strategies ensure the optimisation of office spaces to support BAU working, dual-site resilience, and BCP activation.
- Work area recovery sites utilize dedicated or displacement strategies, depending on the criticality of the teams and the hardware requirements they need.
- Offshore support from the HSBC Global Services Centres (GSC) is subject to a robust continuity framework whereby critical tasks are distributed between two locations to mitigate concentration risk. HSBC onshore management are kept informed of the incidents and risk landscape that impact the GSCs.

2.4 Exercises

Regular testing of the BCM responses is conducted at least annually by each business and support function to validate that the BCP remains relevant, effective and fit for purpose. The BCIM testing programme includes, but is not limited to, staff relocation exercises, workload-shifting to another bank location, remote working, loss of technology, desktop awareness and emergency notification exercises.

2.5 Maintenance

Each BIA and BCP are updated at least annually, or more frequently if there are material changes or as per local regulations. The plan owner must review and approved the BIA and BCP to ensure the appropriate level(s) of management awareness as well as confirm the completeness and accuracy of BCIM artefacts and exercise outcomes. Staff undertake annual training to ensure they are aware of their business continuity roles and responsibilities.

3. Major Incident Management

Depending on the nature of an incident, HSBC can leverage one of two effective management structures to manage the response to any significant event that many have an adverse effect on the bank, which exist at the global / regional / market levels:

i. Major incident group (MIG): A MIG is called when there is an incident that may impact different business lines across the bank.

ii. Incident Management team (IMT): the IMT is a business-specific construct that supports incidents impacting one specific line of business

Regulators take a keen interest in incident management. Clearly defined roles and responsibilities, combined with a programme of ongoing training and exercises, ensure the banks's capability to provide a timely and effective response to manage any major incident.

3.1 Communicable Disease

In the case of a serious outbreak of a communicable disease, HSBC would implement appropriate measures designed to continue services and support to our clients with minimal disruption. HSBC have a Group Communicable Disease Plan at the global level which leverages guidelines from leading global health organizations. All planning and response activity is coordinate globally through an integrated incident management command and control structure. Regular incident management meetings are called to assess and respond as the situation evolves.

From the Group Plan, markets may have their own local version of a Communicable Disease plan or Pandemic Plan that is managed by the MIG. The market-level Plan would support local responses to a metro-wide outbreak and many cater for scenarios such as mass absenteeism, with guidelines on communications, hygiene, travel, etc. Monitoring of announcements by government and health authorities, plus local epidemiological status reports, are conducted and factored into decision-making processes.

3.2 Cyber Security

HSBC has a robust suite of cybersecurity policies, procedures and key controls designed to help ensure that the organization is well managed, with effective oversight and control. This includes but is not limited to defined information security responsibilities for employees, contractors and third parties, as well as standard procedures for cyber incident identification, investigation, mitigation and reporting. The Cyber Security Operations function leverages multiple security solutions to provide proactive 24/7x365 monitoring, technical analysis support and threat response. Business and functions partner with Cyber teams to assess, manage and respond to cyber incidents with appropriate remedial activities. HSBC also operation a cybersecurity education and awareness programme using various channels to engage staff on key messages and target high-risk personal groups with tailored content. These channels include at least annual mandatory training of all staff.

4. Systems and Disaster Recovery

Where possible, HSBC ensures that its critical business systems are not co-located with business system users, thereby reducing concentration risk. HSBC has several major

dedicated data centres around the world, which support technology resilience locally and regionally.

Technology teams have IT Disaster Recovery Plans and procedures in place to support incident management responses to unavailability of IT services. These plans include established escalation procedures and communication channels to ensure the right levels of management are involved, and to enable effective issue assessment and solutioning.

Regular testing demonstrates that business systems and IT services are contingent and that recovery processes are effective. Results from these tests are regularly communicated to business owners via a well-established IT Service Continuity Certification process.

5. Operational Resilience

HSBC has a Group Operational Resilience (OpRes) Strategy that supports the increasing rollout of OpRes in different markets. The OpRes teams review the Important Business Services that HSBC offer externally and consider whether, if they are disrupted, they would cause harm to our customers, HSBC itself, or the broader financial market. The programme includes end-to-end mappings of services, testing of the ability to remain within defined impact tolerances levels, and a maturing journey to further improve the resilience of individual services, legal entities and the Group as a whole

6. Communications

During an incident, the dissemination of factual and timely information is critical. HSBC has procedures in place to manage the communications with internal staff and external stakeholders. Internally, there are tools in place to send important information to staff at local / regional / global levels via different channels on short notice. There are escalation and reporting protocols to ensure the client, regulatory, and media communications are appropriately coordinated and managed by the designated teams to ensure alignment of accurate information.

7. Audit

HSBC undergo regular internal and external audits, as well as regulatory reviews of internal processes and procedures, to assess the Group’s compliance with our internal guidelines

and standards, external regulatory guidance and regulations, plus industry standards and best practices.

8. Additional Points

It should be noted that no BCIM programme can eliminate all risks or be able to assure an interruption to our business operations would not occur. This is largely due to the unpredictable and varied nature of any incident. However, we believe that our planning for such events is robust and consistent with many best practices established in the financial services industry, to enable HSBC to be resilient and prepared.