GUIDELINES FOR THE TEMPLATE OF BUSINESS CONTINUITY PLAN

Business Continuity Plan ('BCP') is a comprehensive written plan of action that sets out the procedures and systems necessary to continue or restore the operation of a firm in the event of a disruption.

The purpose of these guidelines is to assist firms intending to carry on Regulated or Market Activities in the AIFC with developing effective BCPs. It must be noted that a firm's BCP should be proportionate to its business risks arising from both internal and external sources and tailored to the scale and scope of its operations. Consequently, there is no "one-size-fits-all" approach in the way firms should establish and maintain systems and controls. Therefore, these Guidelines are an indication of AFSA's minimum expectations and does not constitute an exhaustive list of requirements that might be applicable to the firm's business.

BCP should be developed in compliance with relevant requirements stipulated in AIFC Financial Services Framework Regulations ("FSFR"), AIFC General Rules ("GEN"), AIFC Conduct of Business Rules ('COB'). Firms should also take into account other relevant AIFC Rules and Regulations depending on the proposed business of a firm.

In compliance with AIFC GEN 5.8.4. an Authorised Person must have a BCP, which is subject to periodic review and scenario testing, that addresses events posing a significant risk of disrupting operations, including events that could cause a widespread or major disruption.

Whilst this is not exhaustive, the key elements of a BCP will often include:

- *An executive abstract* of the substantive elements of the BCP, most notably, the trigger framework and available recovery strategies. The purpose of the executive abstract is to serve as a roadmap of the recovery plan to enable Board and Senior Management of a firm to quickly understand and assess the governance, trigger framework, recovery options and communication strategies for effectively responding to a severe stress situation. It may be helpful to use tables and flow charts to summarise these operational details.
- *A trigger framework* that allows a firm to identify in a timely manner any emerging risks that may have the potential to threaten its viability. The trigger framework should identify a set of pre-defined criteria, which may trigger the activation of the recovery plan so as to allow the firm to successfully monitor, escalate and activate the appropriate range of responses for an emerging stress event. The trigger framework should reflect the fact that different levels of response will be required, depending on the circumstances and severity of the stress event. For instance, the firm may choose to use certain criteria as 'early warning indicators' to alert it to emerging risks and determine that these criteria require heightened monitoring. Other criteria may be used

as ‘trigger points’ for informing more intensified responses such as activation of the recovery plan. The framework may consider market conditions, macro-economic conditions, weather-related events, biological incidents, local protests, terrorism, cyber-attacks and anything with the potential to have a broad impact on the firm's operations.

- A description of *recovery strategies* for those business functions and operations that are to be recovered on a priority basis, with expected recovery levels and recovery timeframe. Recovery strategies for Information technology (IT) systems, applications and data is essential for continued operation of the business. The plan should include regularly scheduled backups from wireless devices, laptop computers and desktop computers to a network server. The frequency of backups, security of the backups and secure off-site storage should be addressed in the plan.
- A description of its *governance* for recovery planning. This includes a description of the processes for monitoring, escalating and activating the recovery plan, and a description of the key roles and responsibilities of the firm’s Board, Senior Management and other key personnel. The plan should outline circumstances in which the firm would consider an increased level of monitoring and reporting to the Board and Senior Management. Forming necessary monitoring and governing committees, such as crisis management team can be useful.
- A comprehensive emergency *communication* protocols and procedures, including crisis management. A firm would need to consider the external parties with whom it should communicate, such as AFSA, Clients, and other stakeholders, as well as how best to communicate with them and within its own organisation.
- A set of *stress scenarios* to assist in assessing the credibility and feasibility of the recovery plan, notably of the trigger framework and recovery strategies.
- Timetable for BCP testing and frequency, including how results of such tests are recorded and lessons learned are communicated.

Subject to the type of business activity, firms may refer to the following documents that can be useful in developing their own BCPs:

1. High-level principles for business continuity https://www.bis.org/publ/joint17.pdf
2. Market Intermediary Business Continuity and Recovery Planning https://www.iosco.org/library/pubdocs/pdf/IOSCOPD523.pdf
3. Application Paper on Recovery Planning https://www.iaisweb.org/file/87228/application-paper-on-recovery-planning