Chapter 4

Commission Delegated Regulation (EU) 2020/1230

Article 20 Operational risk

(1) An application for registration as a securitisation repository shall contain:

(a) a detailed description of the resources available and procedures designed to identify and mitigate operational risk and any other material risk to which the applicant is exposed, including a copy of any relevant policies, methodologies, internal procedures and manuals drawn up for that purpose;

(b) a description of the liquid net assets funded by equity to cover potential general business losses in order to continue providing core securitisation services as a going concern;

(c) an assessment of the sufficiency of the applicant's financial resources to cover the operational costs of a wind-down or reorganisation of the critical operations and services over at least a nine-month period;

(d) the applicant's business continuity plan and a description of the policy for updating that plan, including:

(i) all business processes, resources, escalation procedures and related systems which are critical to ensuring the core securitisation services of the applicant, including any relevant outsourced service and including the applicant's strategy, policy and objectives for the continuity of those processes;

(ii) any arrangements in place with other financial market infrastructure providers including other securitisation repositories;

(iii) the arrangements to ensure a minimum service level of the critical functions and the expected timing of the full recovery of those functions;

(iv) the maximum acceptable recovery time for business processes and systems, taking into account the deadlines for reporting laid down in Article 7(1) of Regulation (EU) 2017/2402 and the volume of information that the applicant needs to process within the quarterly period;

(v) the procedures to deal with incident logging and reviews;

(vi) a periodic testing programme, ensuring that sufficient tests will be carried out to cover an adequate range of possible scenarios, in the short and medium term, including but not limited to system failures, natural disasters, communication disruptions, loss of key staff and inability to use the premises regularly used and providing for the tests to identify how hardware, software and communications respond to potential threats, together with the results and follow-up actions resulting from any tests and those systems that have been shown to be unable to cope with the specific scenarios being tested;

(vii) the number of alternative technical and operational sites available, their location, the resources of those sites when compared with the main site and the business continuity procedures in place in the event that alternate sites need to be used;

(viii) information on access to a secondary business site to enable staff to ensure continuity of core securitisation services if a main office location is not available;

(ix) plans, procedures and arrangements for handling emergencies and ensuring safety of staff;

(x) plans, procedures and arrangements to manage crises, to coordinate the overall business continuity efforts and to determine their timely (within the recovery time objective set by the applicant) and effective activation, mobilisation and escalation capabilities;

(xi) plans, procedures and arrangements to recover the applicant's system, application and infrastructure components within the recovery time objective set by the applicant;

(xii) details on staff training on the operation of the business continuity arrangements, and individuals' roles in that regard, including specific security operations staff ready to react immediately to a disruption of services;

(e) a description of the arrangements for ensuring the applicant's core securitisation services in case of disruption and the involvement of its users and other third parties in those arrangements;

(f) a description of the applicant's arrangements for publishing on its website and promptly informing the FCA and other users of any service interruptions or connection disruptions as well as the time estimated to be needed to resume regular service;

(g) a description of the applicant's arrangements permitting its staff to continuously monitor in real-time the performance of its information technology systems.

(2) An application for registration as a securitisation repository shall include a copy of policies and procedures to ensure the orderly transfer of information to other securitisation repositories and the redirection of reporting flows to other securitisation repositories.