ANNEX B

Measures to address and manage key risks for the resilience and security of DCs

Category	What does it cover?
• DC infrastructure (power, cooling, fire suppression, access control, etc.) • Governance (change management, incident management, etc.) • Cyber (malware attacks, ransomware, etc.)	Step 1 - The "Plan" step involves establishing the scope and policies of the Business Continuity Management System (BCMS), garnering top management support to be executive sponsors, and identifying the critical products and services that should be protected from business disruptions. Step 2 – The "Do" step entails implementing the business continuity policy, controls, processes and procedures. This includes steps to understand, plan and test for business continuity events. Step 3 – The "Check" step involves monitoring and reviewing performance against the established BCMS objectives. The results of the assessment should be presented to top management for review. Step 4 – The "Act" step ensures that operators maintain and improve the BCMS by taking preventive and corrective actions based on the results of management review, and updating it to align to management's expectations.
Additional cybersecurity measures	Additional measures to manage the risks and cyber threats in the DC's network and systems effectively.