



External Supplier Control Obligations Business Continuity Management (BCM)

Control Title	Control Description	Why this is important
1. Threat Assessment	The supplier must monitor threat intelligence on an ongoing basis to identify potential risks that could result in losses and or significant disruptions to business activities.	Consistent monitoring of threat intelligence enables suppliers to proactively identify potential Business Continuity risks. These risks have the potential to lead to financial losses and significant disruptions in business activities. Therefore, by staying vigilant and informed, the supplier can take timely preventive measures, implement effective risk mitigation strategies, and ensure business continuity.
2. Plan Development	The supplier must establish its readiness to respond to disruptive events from potential disruptors by formulating business continuity plans that include but are not limited to the Maximum Tolerable Period of Disruption (MTPD), the Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), the Recovery Team, Backup Locations, Communication Protocols, Review, and Testing frequency.	Establishing comprehensive business continuity plans, covering critical aspects such as MTPD, RTOs, RPOs, recovery teams, backup locations, communication protocols, and regular testing, is essential for suppliers. These plans ensure swift recovery from disruptions, minimizing downtime, financial losses, and reputational damage. They also demonstrate proactive risk management, enhance stakeholder confidence, and ensure long-term business viability in today's volatile business environment.
3. Plan Testing	The supplier must test through simulated exercises, the business continuity plans on a recurring basis as per the defined testing frequency or on the back of event triggers	Testing business continuity plans through simulated exercises, either at predefined intervals or in response to event triggers, is vital. These exercises serve as a proactive measure to validate the effectiveness of the plans in real-world scenarios. They help identify weaknesses, refine response procedures, and ensure that the organization can swiftly and effectively recover from disruptions.
4. Plan Refinement	The supplier will update and refine the business continuity plans in line with results from the testing of the plans and as when the attributes of the risks being mitigated change.	Refinement of business continuity plans in response to test results and evolving risk attributes is essential as this dynamic approach ensures that the plans remain effective and adaptable to changing circumstances.
5. Plan Activation	The supplier invokes its business continuity plans with due consideration of the attributes of the associated risk, noting that the plan may be invoked as the occurrence of risk becomes imminent or after the disruption has occurred. In responding to the disruptive event the Group adjusts its plan in accordance with the actual attributes of the disruptive event. Under the circumstance that the Group encounters an unforeseen event or one that it had not specifically planned for, it will adapt existing plans or speedily develop an appropriate plan to address its business continuity objectives.	Adjustment of business continuity plans to match the specific attributes of the disruptive event demonstrates adaptability and resilience. Moreover, in the face of unforeseen or unanticipated events, the ability to swiftly adapt existing plans or create new ones reinforces the Supplier's commitment to maintaining business continuity objectives. This proactive and flexible approach ensures the Supplier's ability to continue delivering services, even in challenging and unexpected circumstances.

6. Situational recovery	The supplier must aim to restore its people, processes, systems, and infrastructure to resume delivery of services to ABSA customers expediently, albeit this may be an altered state when compared to before the disruptive event.	The supplier's commitment to quickly restore people, processes, systems, and infrastructure, even if it results in an altered state compared to pre-disruption, is paramount. This approach ensures that essential services are resumed promptly, minimizing the impact on the organization's customers.
7. Post incident review	The supplier must evaluate and record the damage sustained from a disruptive event. Action plans are developed to mitigate the effects of similar events in the future	Evaluating and documenting the impact of disruptive events is a fundamental component of Business Continuity Management. This process not only provides a clear understanding of the damage incurred but also serves as a learning opportunity. By developing action plans to mitigate the effects of similar events in the future, the Supplier demonstrates a commitment to continuous improvement and resilience. This proactive approach helps minimize the risk of recurrence and reinforces the Supplier's ability to maintain consistent service delivery, ultimately enhancing customer confidence and business sustainability.

Definitions

"Recovery Point Objective"	means the target status for the availability of data at the start of the recovery process. It is a measurement of the maximum data loss that is tolerable in a recovery situation.
"Recovery Time Objective"	means the targeted duration of time between an unexpected failure or interruption and the resumption of operations at agreed service levels.
"Maximum Tolerable Period of Disruption"	the maximum amount of time an organization can endure a disruption or outage of its critical functions, processes, systems, or services before it faces unacceptable consequences

Business Continuity Requirements Matrix

Process Criticality Assessment	Optional*	Critical	Major	Moderate	Limited
Resilience Category	0	1	2	3	4
Application Criticality Assessment Availability Rating	A0	A1	A2	A3	A4
Risk Profile (Suppliers)	High Risk	High Risk	Medium Risk	Medium-Lite Risk	Low Risk
Resilience/Business Recovery Type	Continuous	Highly Resilient	Recover	Recover	No Planned Recovery / Suspend / Backup Only
RTO	Five (5) minutes	0- four (4) hours	0-eight (8) hours	0-24 hours	Best Effort
* RPO: Transactional	Five (5) minutes	30 minutes	30 minutes	24 hours	Best Effort
* RPO: Non-Transactional	Five (5) minutes	0-four (4) hours	0-eight (8) hours	0-24 hours	Best Effort
Validation Frequency	Minimum every 12 months	Minimum every 12 months	Minimum every 12 months	Minimum every 24 months	No Planned Recovery