ALYIANT
Consultancy Limited

Guide to Business Continuity Planning and Disaster Recovery Planning

Overview:

1. As the consequences of recent global events continue to reverberate and impact businesses big and small across the world, we consider in this paper the requirement for businesses to put in place a Business Continuity Plan ("**BCP**") and a Disaster Recovery Plan ("**DRP**") which is taking on an increasingly critical role. A BCP is essentially a comprehensive enterprise-wide process involved in creating a system of prevention and recovery from potential threats to a business and which defines how a business responds to and recovers from a business disruption, thereby enabling it to continue to function, service and protect customers, personnel, other stakeholders and assets. A DRP is in essence a plan for business continuity in the event of a disaster and is focused on restoring business operations following a disaster.

2. The requirement for businesses to put in place processes and BCP and DRP policies are a part of regulatory requirements in many jurisdictions for business activities - in particular for regulated financial services activities such as banking. Each jurisdiction may have its own specific regulatory requirements for matters which need to be covered by and included in a BCP and a DRP. By way of example, we later examine in this paper the Dubai International Financial Centre ("**DIFC**") which has in place a robust and effective legislative and regulatory framework.

3. Even where a jurisdiction does not have express regulatory requirements for a business in the financial services and non-financial services sectors to implement BCP and DRP policies, it is not uncommon for businesses in the financial services and non-financial services sectors to put in place BCP and DRP policies for the purposes of risk management, internal control, compliance and corporate governance requirements.

Basel Committee on Banking Supervision:

4. The Basel Committee on Banking Supervision ("Basel Committee") in 2011 issued "Principles for the Sound Management of Operational Risk" Principle 10 ("*Business Resiliency and Continuity*") thereof provides that *"Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption."* It provides that banks are exposed to disruptive events, some of which may be severe and result in an inability to fulfil some or all of their business obligations. Incidents that damage or render inaccessible a bank's facilities, telecommunication or information technology infrastructure, or a pandemic event that affects human resources, can result in significant financial losses to a bank as well as broader disruptions to the financial system. Accordingly, to provide resiliency against such risk, a bank should establish business continuity plans commensurate with the nature, size and complexity of their operations. Such plans should consider different types of likely or plausible scenarios to which the bank may be vulnerable. The Basel Committee further contemplates a number of matters to be considered with respect to continuity management, including the incorporation of business impact analysis, recovery strategies, testing, training and awareness programmes, communication and crisis management programmes, and review of its continuity plans. In present context, whilst the above pertains to banks, it may also serve as a useful guide for matters to be covered in the BCP and DRP of other financial services businesses (other than banking) as well as for businesses in the non-financial services sector.

BCP:

5. With respect to a BCP, broadly speaking the process would include a Business Impact Analysis (BIA), Risk Assessment, Risk Management, and Risk Monitoring and Testing. First, a BIA involves reviewing business function and processes and their interdependencies on each other; identifying the potential impact on the functions and processes of a business from uncontrolled or non-specific events; identifying the legal, regulatory, financial requirements and impact on business functions and processes of the business and the reputational impact in relation to the business; the estimate maximum allowable downtime as well as the acceptable level of losses associated with business functions and processes and;

estimated recovery time. Second, in terms of Risk Assessment, a business would evaluate the assumptions of the BIA using various threat scenarios; analyse threats based upon the impact to the business, its customers, personnel, other stakeholders and assets; prioritize potential business disruptions based on the severity of the disruption; and perform a "gap analysis" to compare existing the BCP (where already in place) or otherwise the existing position of the business to the procedures and policies to be implemented based on prioritized disruptions identified and their resulting impact on the business. Third, in terms of Risk Monitoring and Testing, this should ensure that the BCP process of a business remains viable through the: incorporation of the BIA and risk assessment into the BCP and testing program; development of an enterprise-wide testing program; assignment of roles and responsibilities for implementation of the testing program; completion of periodical testing of the BCP; evaluation of the testing program and the test results by senior management and the governing board (e.g. the board of directors in the case of a company); assessment of the testing program and test results by an independent party; and revision of the BCP and testing program based upon, amongst other matters, changes in business operations and test results. An entity should also participate in disaster recovery and business continuity testing with key service providers. The BCP and DRP should include provision for a crisis management team (comprising of for example various functionaries of a business).

DRP:

6. With respect to a DRP, broadly speaking the process would, in addition to contemplating matters under the BCP section above, include: first, identifying and addressing various types of contingency scenarios, which may be caused by, inter alia, system faults, hardware malfunction, operating errors or security incidents and total or partial incapacitation of the primary datacentre of a business; second, evaluating the recovery plan and incident response procedures periodically and update them as and when changes to business operations, systems and networks occur, implement replication, rapid backup and recovery capabilities at the individual system or application cluster level; third, consider inter-dependencies between critical systems in drawing up a recovery plan and conducting contingency tests; fourth, define system recovery, business resumption priorities and establish specific recovery objectives for IT systems and applications; and fifth, establish a recovery site that is geographically separated from the primary site to enable the restoration of critical systems and resumption of business operations in case of disruption at the primary site. In the context of disaster recovery testing, these would broadly include: adopting tested and rehearsed recovery measures; testing and validating periodically, the effectiveness of recovery requirements and the ability of personnel to execute the necessary emergency and recovery procedures; covering various scenarios in disaster recovery tests including total shutdown and/or complete switchover of the primary site as well as the component failure at an individual system or application cluster level; and testing the recovery dependencies between systems.

The DIFC:

7. As mentioned earlier, different jurisdictions may each have their own regulatory requirements for BCP and DRP matters and in this regard, we briefly take the example of regulatory requirements for businesses in the DIFC licensed by the Dubai Financial Services Authority ("**DFSA**") to undertake financial services activities.

8. The General Module of The DFSA Rulebook ("**GEN Module**") which applies to every Authorised Person (as defined in the relevant DIFC/DFSA legislation) other than the exceptions specified in the GEN Module, essentially provides in relation to "Business continuity and disaster recovery" that an Authorised Person must have in place adequate arrangements to ensure that it can continue to function and meet its obligations under the legislation applicable in the DIFC in the event of an unforeseen interruption and that such arrangements are to be kept up to date and regularly tested to ensure their effectiveness. The DFSA has provided guidance in the GEN Module regarding the arrangements and matters which an Authorised Person is expected to have in place and considered in connection with business continuity and disaster recovery.

9. The Prudential-Investment, Insurance Intermediation and Banking Module of The DFSA Rulebook ("**PIB Module**") also contains Operational Risk provisions requiring an Authorised Firm (as defined in the relevant DIFC/DFSA legislation) in the categories and types specified in the PIB Module, to have business continuity and disaster recovery as part of their Operational Risk

management framework and by way of guidance provides, amongst other matters, that an Authorised Firm's Operational Risk policy should, amongst other things, include consideration of Principles for the Sound Management of Operational Risk, issued by the Basel Committee on Banking Supervision (please see above discussion) and the Guidelines on the management of Operational Risk in market-related activities issued by the European Banking Authority which are useful in relation to activities other than banking. Further, in the context of the DIFC, the Prudential-Insurance Business Module of The DFSA Rulebook ("**PIN Module**") which applies to every Insurer (as defined in the relevant DIFC/DFSA legislation) except as otherwise provided in the PIN Module, requires an Insurer to develop, implement and maintain a risk management system to identify and address the non-financial or operational risk of the Insurer, including but not limited to business continuity planning risk. The guidance by the DFSA in the PIN Module provides for matters which the Insurer's risk management system should contain with respect to a disruption in business continuity and the matters and procedures which are required to be described in the business continuity plan.

Conclusion:

10. In these unprecedented times, it is likely that businesses globally which have put in place BCP and DRP policies will be tested to the extreme under the current circumstances and should consider reviewing and updating their BCP and DRP policies. Those businesses that do not have BCP and DRP policies in place, should consider putting BCP and DRP policies in place as a matter of priority. Having in place robust BCP and DRP policies could go a long way to mitigate serious financial loss and adverse impact on a business as systems, processes and a framework on which to build a road map towards recovery will be in place at the outset in case of an event which disrupts business operations.

11. As each entity will vary in size and complexity, there is no one size fits all approach for BCP and DRP policies. Whether for an existing business or a new business, our Compliance and Risk Management services are able to assist businesses in the financial services and non-financial services sectors in multiple jurisdictions with their overall compliance and risk management requirements and in present context, to assist in the review and update or development and implementation of BCP and DRP policies. Please contact us at aly@alyiantconsultancy.com for further details.

Aly Shah
Managing Director
Date: 15 April 2020