ADB

July 2016

Organizational Resilience

Asian Development Bank

ABBREVIATIONS

ADB	–	Asian Development Bank
BCF	–	business continuity facility
BCM	–	business continuity management
BIA-RA	–	business impact analysis and risk assessment
ISO	–	International Organization for Standardization
IT	–	information technology
MDB	–	multilateral development bank
OGC	–	Office of the General Counsel
OIST	–	Office of Information Systems and Technology
ORM	–	Office of Risk Management
OSFMD	–	Operations Services and Financial Management Department

NOTE

In this report, “$” refers to US dollars.

Vice-President and Steering Group Chair	D. Stokes, Administration and Corporate Management
Principal Director	R. Z. Teng, Principal Director, Office of Administrative Services (OAS)
Steering Group	T. Oya, Director General, Bud get, Personnel, and Management Systems Department (BPMSD)
	C. Kim, Controller, Controller's Department
	S. O'Sullivan, Director General, Central and West Asia Department (CWRD)
	S. Bindra, Principal Director, Department of External Relations (DER)
	H. C. Ong, Auditor General, Office of the Auditor General (OAG)
	C. Stephens, General Counsel, Office of the General Counsel (OGC)
	S. Hamid, Principal Director, Office of Information Systems and Technology (OIST)
	M. Yamawaki, Head, Office of Risk Management (ORM)
	R. Subramaniam, Director General, Operations Service s and Financial Management Department (OSFMD)
	M. Barrow, Deputy Director General, Private Sector Operations Department (PSOD)
	J. Nugent, Director General, Southeast Asia Department (SERD)
	I. Bhushan, Director General, Strategy and Policy Department (SPD)
	P. Van Peteghem, Treasurer, Treasury Department

Team Leader	A. Clinton, Unit Head, Security and Emergency Services, OAS
Team Members	F. Vargas, Senior Organizational Resilience Officer, OAS
	G. Cruz, Organizational Resilience Administrator, OAS
Working Group	E. Zhukov, V. Tan, S. Hung, BPMSD
	B. Reid, N. Wallace, Controller's Department
	M. Samson, R. dela Cruz, DER
	P. Gadpaille, OAG
	M. Ojiro, Q. Zhang, S. Nanwani, OAS
	C. Gautrot, OGC
	A. Duminy, P. Passin, G. Maggiorre, OIST
	M. Kroll, E. Chen, E. Adisoebrata, ORM
	M. Parkash, OSFMD
	S. Pu, PSOD
	C. N. Chong, A. Head, SERD
	S. Jarvenpaa, A. Hussain, SPD
	S. Phanachet, J. Morales, Treasury Department

GLOSSARY

Adaptive capacity – The extent to which an organization or individual can adjust to a range of conditions that deviate from normal expectations, and provide an effective and sustainable response to deal with changing circumstances.

Awareness – The state of individual and/or collective knowledge relating to past and current events, their implications, and potential future development.

Business continuity – The process and management systems designed to prepare, respond, and return to a stable operating condition for any disruptive events.

Business continuity management – The holistic management process that identifies potential threats to an organization and the impacts to business operations these threats, if realized, might cause, and that provides a framework for building organizational resilience to safeguard the interests of its key stakeholders, reputation, brand, and value-creating activities.

Capacity – The combination of all strengths and resources available within an organization, community, or society that can reduce the level of risk or the effects of a crisis.

Culture – The collective beliefs, values, attitudes, and behaviors of an organization that contribute to the unique social and psychological environment in which it operates.

Disruption – An expected or unexpected event causing an unplanned and negative deviation from the usual delivery of outputs.

Networks – An organization, or series of interconnected people and organizations, that works together to achieve a shared vision or objective.

Organizational resilience – The outcome of an organization's capability to anticipate and respond to disruptions related risks and its capacity to adapt to complex or changing circumstances under conditions of uncertainty.

Organizational resilience framework – The set of components that link principles, attributes, and strategies for design, development, implementation, and continuous improvement of organizational resilience.

Resources – All assets, people, skills, information, technology (including facility and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, to operate and meet its objective.

Risk – A possible event that could cause harm or loss, or affect the ability of an organization to achieve its objectives. A risk is measured by the probability of a threat, the vulnerability of the organization to that threat, and the impact it would have if it occurred.

Risk appetite – The amount and type of risk that an organization is willing to pursue or retain.

CONTENTS

EXECUTIVE SUMMARY

The headquarters of the Asian Development Bank (ADB) is broadly exposed to potential business disruptions if a large disaster—either natural or human-made—were to occur in Metro Manila. Exacerbating this vulnerability is ADB's highly centralized operations. Most of the bank's core and support functions, as well as all of its critical data and production, are located in the headquarters complex.

To maintain continuity of operations and protect shareholder value in the event of a disaster, and to ensure long-term viability despite changes in the operating environment, ADB plans to shift to an organizational resilience model to strengthen its business continuity posture. The organizational resilience framework proposed in this paper will enable ADB to prepare for and respond to disruption-related risks and strengthen its capacity to adapt to complex and changing circumstances without compromising its ability to fulfill its core mission.

The framework will safeguard ADB's reputation and the interests of its stakeholders by ensuring the ability to manage its contractual obligations, cash flow, revenue and solvency, and delivery of its mission to developing member countries without interruption. It will enable ADB to maintain operations throughout a disruptive event and to meet instances of uncertainty and change with coherence and appropriate resources. This will be achieved by optimizing the use of key resources—people, premises, information technology, business data and processes, and supply chain—to increase availability and ensure that adequate redundancies in operational procedures are in place.

The framework outlines a set of actions from 2016–2021 to make ADB a more resilient organization. It addresses both the traditional or technical (hard) elements and the behavioral (soft) elements that are essential in creating adaptability and flexibility. The implementation plan will have the following phases:

(i) **Immediate actions (2016).** Enhancing current business continuity arrangements to support key financial processes of the Controller's Department, Treasury Department, and the Office of Risk Management.

(ii) **Short-term actions (2016–2018).** Extending protection to ADB's operations departments, as well as the Office of Cofinancing Operations, Office of the General Counsel, and Operations Services and Financial Management Department.

(iii) **Medium-term actions (2016–2021).** Embedding resilience across ADB.

(iv) **Monitoring phase (2021–2031).** Monitoring and measuring ADB's resilience.

The framework establishes the governance and organizational structure to provide guidance and management direction and to ensure efficient administration of ADB's resilience efforts. In March 2016, an Organizational Resilience Unit was created in the Office of Administrative Services to lead and manage resilience at ADB. It will coordinate the implementation of action items for all ADB offices and locations within the framework. The timelines for completing the actions, as well as the lead and support departments and offices responsible for executing the actions, are also identified. The unit will be responsible for coordinating with the departments concerned and will report to Management on the progress of each implementation phase, as provided in the implementation plan. The Organizational Resilience Unit will conduct an annual review of the framework and will report the outcome to Management.

I. INTRODUCTION

1. Asian Development Bank (ADB) headquarters is located in Manila, Philippines, the capital city of one of the most disaster-prone countries in the world. ADB headquarters is particularly vulnerable to disruptions caused by natural disasters such as flooding, large storms, and/or seismic events, including earthquakes or volcanic activity. Exacerbating this vulnerability is ADB's highly centralized operations. Most of ADB's core and support functions, as well as all of its critical data and production, are in Manila. In their operational risk self-assessments, ADB departments and offices have consistently rated the potential for a business disruption because of a large natural disaster or human-made event *very high*.[1]

2. Since 2005, ADB has worked to improve its business continuity readiness. However, ADB's current business continuity posture is inadequate to meet the challenges of a major disruption. As a result, ADB is shifting to an organizational resilience model to increase its preparedness and response capacity, and to ensure that it is agile and adaptable to a wide range of disruptive events regardless of the nature and duration.[2] ADB's organizational resilience framework[3] is the product of collaboration among members of the Business Continuity Management Steering Group, chaired by the vice-president for administration and corporate management.[4] Appendix 1 provides the current state and gap analysis of ADB's business continuity management (BCM).

3. In 2015, ADB conducted a comprehensive business impact analysis and risk assessment (BIA-RA) to (i) revalidate its business continuity objectives and priorities, (ii) identify threats that could disrupt its operations, and (iii) identify mitigation measures to reduce the likelihood or impact of a disruptive incident. The BIA-RA, which is performed annually, forms the basis for developing prevention and mitigation procedures that will enable ADB to become and remain resilient. Appendix 2 discusses the results of the 2015 BIA-RA.

II. RISK APPETITE

4. ADB's reputation in the capital markets is closely linked to ADB's competitiveness and ability to serve its developing member countries (DMCs). This reputation is attributed to ADB's sound governance and conservative financial management, supported by a robust balance sheet and strong sovereign shareholder support from its 67 members. These provide the greatest levels of confidence to its creditors and financing partners. Having committed to invest in ADB, sovereign shareholders are primarily concerned with the efficient utilization and security of the bank's financial resources to meet its development agenda. In recent years, the Board of Directors has been continually and increasingly interested in improving ADB's disaster preparedness and response capability.

5. ADB regards staff safety as its primary concern. ADB is a conservative organization that adheres to sound banking principles in order to retain its reputation as a premiere financial institution. With respect to financial liabilities, ADB is committed to meeting its financial obligations when they are due, avoiding default, and maintaining its financial standing. ADB also complies with its contractual obligations, to the extent possible, in order to remain viable and

[1] Quarterly Risk Management Reports in 2015.

[2] ADB's current BCM capability can reasonably withstand potential disruptions that would last for less than 7 days.

[3] The term "framework" refers to the set of components linking principles, attributes and action plans for the design, development, implementation, and continuous improvement of ADB's organizational resilience.

[4] The President approved the creation of the Business Continuity Management Steering Group in April 2015.

able to fulfill its mission to its DMCs. A discussion on ADB's risk appetite is in Appendix 3.

III. SHIFT TOWARDS RESILIENCE

6. Activities are ongoing and/or planned to strengthen ADB's BCM, which is currently reactive and lacks measures to address the impacts of an area-wide and/or prolonged disruption. ADB has also compared the BCM approaches of other multilateral development banks (Appendix 4). ADB has an opportunity to transform the way it operates in order to improve preparedness for a disruptive incident that could deprive the organization of any of the five key resources identified in the BIA-RA: people, premises, information technology (IT), data and information, and the supply chain.

7. **Organizational resilience**. ADB needs to develop the capability to deal with unexpected disruptions to business-as-usual activity. The International Organization for Standardization (ISO) defines this as the "outcome of an organization's capability to adapt to complex or changing circumstances under conditions of uncertainty."[5] From the disaster risk perspective, this would provide ADB the ability to resist, absorb, recover, respond, and reorganize after a disruptive event in a measured and coherent manner. Achieving resilience requires actions and contributions from a wide range of disciplines and actors at various levels, working together with a shared responsibility and a broad mix of tools and methods to balance their needs and resources.[6]

8. By adopting organizational resilience, the following are envisioned for ADB:

(i) The organization continuously considers expected and unforeseen crises and identifies what plans are in place, what preparations need to be made, and what resources are available.
(ii) Buildings and facilities are designed for durability and robustness in the face of an increasing number of catastrophic events.
(iii) Crisis management teams are established and rehearsed, are distinct from normal management chains, and have defined roles and responsibilities.
(iv) Emergency communication systems are established and tested regularly.
(v) Support is provided to staff and dependents in an emergency, to the extent possible.
(vi) All staff members are aware of their responsibilities in case of an emergency.
(vii) Business processes are clearly documented, and concerned staff have the capacity to perform these processes.
(viii) Information and systems are secured and available anytime from anywhere.
(ix) Business processes are designed to operate from anywhere and from multiple locations, and transactions can be processed with flexibility either manually or electronically.
(x) The supply chain is involved in planning and sharing of information.

9. The framework set out in this paper will enable ADB to shift from the current reactive focus on the recovery and continuation of a small number of priority business processes to more proactive threat anticipation, risk mitigation, and adaptation to changing conditions. This will enable ADB to continue operations throughout a disruptive event. The framework provides a methodology that allows ADB to rationalize its business processes and resource utilization to

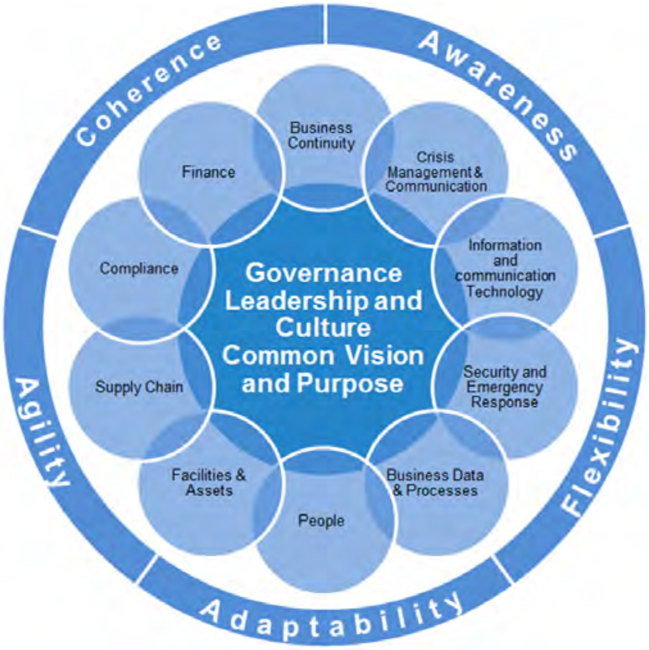
[5] ISO 22316 (under development) Guidelines for Organizational Resilience.
[6] ADB. 2013. *Investing in Resilience: Ensuring a Disaster-Resistant Future*. Manila.

ensure the continuation of operations during a disruption. This will be achieved in a practical, scalable, and cost-effective manner, taking into consideration ADB's risk appetite and an analysis of alternatives and options.

IV. ADB ORGANIZATIONAL RESILIENCE FRAMEWORK

10. The development of the framework[7] has drawn upon recognized international standards and best practices, and adopts those principles and concepts best suited to ADB. Figure 1 illustrates the key components of ADB organizational resilience framework. The framework and ADB's actions to enhance organizational resilience are in Appendix 5. Detailed discussions on the framework's components relating to business continuity, crisis management and communication, information and communication technology, security and emergency response, facilities and assets, business data and processes, people, finance, supply chain, and compliance are in Appendixes 6–15.

Figure 1: ADB Organizational Resilience Framework


Coherence
Awareness
Flexibility
Adaptability
Agility
Business Continuity
Crisis Management & Communication
Information and communication Technology
Security and Emergency Response
Business Data & Processes
People
Facilities & Assets
Supply Chain
Compliance
Finance
Governance Leadership and Culture Common Vision and Purpose

Source: Asian Development Bank.

A. Mission Statement

11. ADB's organizational resilience framework will improve ADB's ability to anticipate and respond to disruption-related risks to ensure the delivery of its core mission without disruption. The framework enables ADB to maintain operations throughout any disruption and meet instances of uncertainty and change with clarity, coherence, and appropriate resourcing.

[7] ADB's organizational resilience framework is based on international best practices and standards, including (i) British Standards BS 65000:2014 Guidance on Organizational Resilience, and (ii) International Standards ISO 22316 (under development) Guidelines for Organizational Resilience.

12. The framework's priority is to safeguard ADB's reputation and the interests of its stakeholders by ensuring the ability to manage its contractual obligations, cash flow, revenue, and solvency without interruption. This will be achieved by proactively reducing risk exposure and the potential impacts of threats through the optimization of key resources—people, premises, information technology (IT), data and information, and the supply chain—to allow greater availability and adequate redundancies in operational procedures.

13. The framework will be implemented in phases that will (i) maximize the use of resources, (ii) align with ADB's current and future long-term strategies, (iii) adhere to ADB's business imperatives and risk appetite, and (iv) be cost-effective.

B. Governance and Leadership

14. ADB's governance and organizational structure provides direction and ensures that efforts in establishing and maintaining organizational resilience remain consistent with ADB's objectives and requirements. Effective governance enables ADB to take advantage of opportunities and mitigate risks, and to ensure that appropriate teams are accountable for decisions. The Board, Management, and the Organizational Resilience Steering Group[8] are accountable for ensuring that an appropriate level of resilience is achieved, together with other outcomes such as development effectiveness, compliance, and sustainability. When necessary, they are obligated to define the balance to be achieved between such outcomes. Transparency is important, and the framework requires this information be proactively shared. Details on the governance and organizational structure for ADB's organizational resilience are in Appendix 16.

15. In March 2016, an Organizational Resilience Unit was established in the Office of Administrative Services to lead and manage resilience at ADB. The unit will coordinate the implementation of plans and action items within the framework components.

C. Scope

16. The scope of the organizational resilience framework includes all ADB personnel and business and operational processes at all ADB offices and locations.

D. Focus Areas

17. As reflected in the 2015 BIA-RA (Appendix 2), ADB's greatest vulnerability is the concentration of key resources—people, processes, and information technology (IT)—at headquarters. Addressing this key issue is the primary focus of the framework. Beginning with priority business processes supporting key products and services identified in the BIA-RA report, the framework will eventually enable the continuation of all ADB operations by ensuring the availability and accessibility of personnel, data, and systems.

1. People

18. ADB's paramount concern is the safety, security, and well-being of its people. This concern is derived from the organization's inherent duty of care. As people are also the key resource in responding to disruptive events, maintaining resilient personnel is imperative to ADB. ADB must ensure that appropriate policies and practices are in place to guarantee the

[8] Upon approval of this paper, the Business Continuity Management Steering Group will be changed to the Organizational Resilience Steering Group to oversee organizational resilience in ADB.

availability of qualified and motivated personnel to support the organization.

19. Data availability alone is insufficient for the continuity of business operations. A significant disruption event will affect the availability of staff to perform key business functions. In addition to protecting staff to the extent possible, the framework will establish procedures that provide appropriate levels of assistance to staff and dependents.

2. Information Technology and Data Availability

20. IT systems are indispensable enablers of ADB's operations. Therefore, the availability of IT services must be ensured, which requires redundancies in the IT architecture and enhanced disaster-recovery capabilities, while maintaining the necessary level of security and providing service support to users.[9]

21. ADB's reliance on documents in hard copy presents a risk including in the event that access into the building is denied. As IT systems and electronic data become more available and accessible externally, business processes will shift to digitized transactions and paperless processing. Aside from achieving resilience, outcomes such as improved productivity and efficiency can be realized.

22. The evolving global technology landscape presents opportunities for ADB to continually strengthen its ability to maintain its operations throughout a disruption.

3. Efficient and Adaptive Processes

23. To achieve resilience:

(i) ADB's operational processes will be aligned with the organization's strategic objectives. These processes will be made as efficient and easily replicable as possible with all necessary safeguards.
(ii) ADB's processes will be agile and adaptable to address challenges of a business disruption in a resourceful manner.
(iii) All processes will be reviewed regularly to identify unnecessary redundancies as well as potential single points of failure that need to be addressed.
(iv) Contingency plans[10] will be developed, maintained, updated, tested, and rehearsed regularly to enable the continuation or quick recovery of processes.
(v) All ADB processes will be examined during the regular BIA-RA to identify the most critical ones to ADB so that resources can be allocated accordingly.

4. Enhanced Business Continuity Management

24. A key component of building resilience is strengthening ADB's organizational capability to respond to or resist the impacts of disruptive events. Shifting to a more proactive approach will enable ADB to anticipate, prepare for, and respond to unexpected events more quickly and more cost effectively. BCM will be enhanced to achieve the following:

[9] ADB. 2013. *Information Systems and Technology Strategy III.* Manila.

[10] Contingency plans encompasses plans related to physical security, emergency response, crisis management, IT disaster recovery, business continuity, and other disciplines that need to be exercised and tested regularly to ensure that these remain consistent with the organizational resilience initiative.

(i) Mitigate the risks of disruptive events and protect ADB’s reputation, assets, and resources by employing existing operational disciplines enabling resistance to disruption.

(ii) Take timely and informed actions to anticipate and mitigate impacts of adverse events, including unforeseen overwhelming crises.

(iii) Identify single points of failure and establish a response capability to react quickly so that core functions are maintained at an acceptable and predetermined level.

(iv) Sustain operations following a disruption and transition from a crisis response state to business resumption at a predetermined level within agreed timelines and with enhanced resilience capabilities.

(v) Restore ADB to normal business operations and/or adapt to a changed business environment after a disruption.

V. IMPLEMENTATION ARRANGEMENTS

25. The 2015 BIA-RA determined that ADB has significant risk exposure and that the business impacts may be severe if ADB is not prepared.

26. The framework will be supported by an implementation plan (Appendix 17). The plan will focus on both the traditional and technical (hard) elements and behavioral (soft) elements that are important in creating an adaptable and flexible capability. This will enable ADB to deal successfully with unpredicted, disruptive, and sometimes catastrophic events.

27. The implementation plan will be a living document. It will be reviewed and updated periodically in line with changing business requirements and implementation experience.

28. The implementation plan will build on the immediate actions that are already underway. These actions will enhance business continuity capabilities for key financial processes from disruption-related risks, as identified through the 2015 BIA-RA.

29. Figure 2 shows the phases of the implementation plan.

Figure 2: Implementation Plan

Enhanced Business Continuity		Full Organizational Resilience	
Immediate Actions	**Short-Term Actions**	**Medium-Term Actions**	**Monitoring Phase**
• Establishment of governance and oversight • Offshore warm site • Online data replication of IT financial systems with minimal data loss (less than 12 hours) • Prepare and finalize short-term outposting of staff • Protection of key financial processes • Off siting of nonfinancial systems backup	• Implement Cloud technologies • Short-term outposting of OIST and TD staff • Set up of SDPC and long-term outposting of CTL International Staff for SDPC operation • Business continuity plans for operations departments, OCO, OGC, and OSFMD • Review of policies, processes, and procedures • Establishment of interim spending arrangements during a disruption • Design of organizational resilience communication plan details • General awareness and training programs	• Extend Cloud technologies • Long-term resilience plan for critical business processes (CTL, TD, ORM) including decentralization and setup of new processing hubs • Digitization of financial transaction processing and other essential files • Business continuity plans for all ADB departments and offices • Ongoing staff awareness and training	• Testing • Monitoring • Review and/or assessment • Top level review and/or assessment of organizational resilience framework
Year **2016**	**2018**	**2021**	**2031**

ADB = Asian Development Bank, CTL = Controller's Department, DR = disaster-recovery, IT= information technology, OCO = Office of Cofinancing Operations, OGC = Office of the General Counsel, OIST = Office of Information Systems and Technology, ORM = Office of Risk Management, OSFMD = Operations Services and Financial Management Department, SDPC = secondary disbursement processing center, TD = Treasury Department.

Source: ADB.

A. Immediate Actions (2016)

30. Approved by the President in January 2016, these immediate actions will increase ADB's capacity to maintain sufficient financial processes of the Controller's Department, Office of Risk Management, and Treasury Department throughout a prolonged disruption before the full implementation of the organizational resilience framework. Data protection of critical financial systems[11] will be enhanced by moving from tape backups to data replication technology, reducing potential data loss from a number of days to hours. This will be accomplished by establishing a warm data center[12] enabling data replication outside of the

[11] Critical financial systems include SWIFT, Mainframe, Oracle ERP, iFIRST, CLASS and TRMS.

[12] A warm site is a facility containing active data links and pre-configured equipment and requires restoration of current data to commence operations.

Philippines.[13] The data center will be managed by the Office of Information Systems and Technology (OIST) or outsourced.

31. Plans will also be available to ensure that key staff of the Controller's Department and Treasury Department are deployed outside of the Philippines to access and utilize critical financial systems and data if headquarters is offline. This will reduce the staff concentration risk to an acceptable level. In addition, a review of the functionality of the business continuity facility will be undertaken and the backup of other IT systems will be moved outside headquarters.

32. The Organizational Resilience Unit will align, integrate, and coordinate the activities under business continuity, crisis management, security and emergency management, IT disaster recovery, and other resilience disciplines. ADB's crisis management system will be strengthened, clearly defining roles and responsibilities and decision-making processes. Training and drills will be conducted regularly.

B. Short-Term Actions (2016–2018)

33. One of the key objectives of the short-term action plan to extend protection to ADB operations and selected other departments is to lay the groundwork for institutionalizing resilience throughout ADB. These actions will establish key organizational resilience structures, including determining the appropriate IT architecture concept (cloud, virtual data centers, stand-alone data center, or hybrid options).

34. Remote access to main operational and financial systems will be strengthened to enable usage from anywhere by staff supporting priority processes as identified in the BIA-RA. Communication services such as email will also be accessible to all ADB staff in the event of a disruption.

35. The Controller's Department and Treasury Department will finalize and implement arrangements to ensure that staff are assigned outside of the Philippines to perform key financial transactions. OIST will ensure the availability of adequate IT resources to perform these processes.

36. Business continuity capability will be extended to the Central and West Asia Department, East Asia Department, Office of Cofinancing Operations, Operations Services and Financial Management Department, Office of the General Counsel, Pacific Department, Private Sector Operations Department, South Asia Department, and Southeast Asia Department. Business continuity plans will be developed and tested. Resource requirements will be identified and provided for. Consequently, the backup strategy and IT disaster recovery procedures will be expanded to include the recovery of IT systems and shared drives of these departments and offices to ensure the continuous flow of transactions to the financial business processes. Access to cloud storage or the equivalent will be provided to these departments and offices.

37. Options for alternate workspace in Metro Manila will be assessed, including the use of the in-country business continuity facility. This could provide ADB additional workspace in the event of a prolonged disruption to complement the work-from-home option.

38. General awareness and training programs will be designed and delivered, with an

[13] The Office of Information Systems and Technology estimates that the online data replication will reduce the data loss during a major business disruption from more than 1 day to less than 12 hours.

emphasis on those that will improve individual and family preparedness and raise awareness of roles and responsibilities during a disruption.

39. The supporting human resources policies and related guidelines will be established and processes, and procedures will be reviewed.

40. An institutional arrangement to secure funding for relief and recovery operations, as well as other regular expenses during extended emergency situations in headquarters, will be established. In 2016, BPMSD and OAS will request Board approval for special spending authority for Management to use in the event of an extended emergency situation affecting headquarters operations. This would authorize Management to incur costs to cover (i) relief operations for staff; (ii) establishment of an alternate or temporary office facility, logistics, and other costs necessary to sustain operations; (iii) capital expenditures needed to restore office facilities, equipment, IT infrastructure and systems, and others as necessary; and (iv) regular internal administrative expenses using the current or previous year's approved budget, as appropriate.

C. Medium-Term Actions (2016–2021)

41. The medium-term actions to embed resilience across ADB will build on the short-term actions and address key policy areas such as those directly affecting personnel. These actions will also address the people and process dimensions in alignment with the Midterm Review[14] Action Plan of empowering field offices.

42. A cost-effective staffing strategy will be developed to support the decentralization of key staff positions away from headquarters. Options may include (i) outposting or rotating headquarters staff to field offices, (ii) cross-training of headquarters and field office staff, (iii) training field office staff on headquarters functions, (iv) creating distributed functions in field offices or other processing hubs and centers; or (v) delegating functions to field offices. A welfare preparedness program will also be implemented to teach staff, families, and associates to best ways to manage their own risks and be able to access help and support when needed.

43. The medium-term actions will implement the shift to a more robust IT infrastructure covering requirements of all ADB business processes, including field offices. All ADB IT systems and production processes, financial and nonfinancial, will be available and accessible from anywhere. Access to cloud storage or an equivalent IT solution to store critical files, reports, and other documentation will be made available to all staff. Processes will be continually assessed to make them more efficient, sustainable, and replicable. All processes will be digitized to the extent possible.

44. The medium-term actions should effectively and adequately prepare ADB to survive low-probability, high-impact disruptive events. They will also provide resilience strategies for the remaining business processes and communication programs not covered by the short-term arrangements.

D. Monitoring Phase (2021–2031)

45. The monitoring phase will begin after 5 years, or earlier as required. The primary goal of this phase is to analyze the effectiveness of the framework implementation and measure if an

[14] ADB. 2014. *Midterm Review of Strategy 2020*. Manila.

acceptable level of resilience has been achieved. By this time, an ongoing system for organizational resilience would have been established, implemented, and maintained.

46. The monitoring phase will continually evaluate the level of resilience achieved and the adequacy of the organizational resilience framework in addressing ADB's internal and external business requirements, and will recommend changes as necessary.

VI. INDICATIVE BUDGETARY RESOURCE REQUIREMENTS

47. Appendix 18 provides an initial analysis identifying the options to achieve the desired level of resilience. To lay the foundation for achieving an acceptable level of resilience, the major investments required for implementing the organizational resilience framework are focused on improving ADB's IT disaster recovery capability and outposting key staff from the Controller's Department, Office of Information Systems and Technology, and the Treasury Department.

48. It is estimated that the budgetary resource requirements to support the 2016 immediate action plans is about $4.2 million comprising of $3.1 million for capital expenditures and $1.1 million for administrative expenses. The requirements for capital expenditures will be met through reallocating the remaining balance of the 2005 Business Continuity Facility Special Capital Budget and utilizing the earmarked budget for business continuity improvement under Information Systems and Technology Strategy (ISTS) III, while the requirements for administrative expenses will be met through reallocation from within the 2016 internal administrative expenses budget.

49. Indicative estimates for the implementation of short-term actions (2017–2018) is around $2.4 million to $3 million for capital expenditures, while indicative estimates for administrative expenses is $6 million to $8 million. For the implementation of medium-term action plans (2019–2021), the requirements for administrative expenses is estimated about $9 million, while there may be no requirements for capital expenditures for this period. These are indicative estimates which will be firmed up through further review and consultations with the relevant stakeholders. The requirements for capital expenditures for 2017–2021 will be processed for Board approval through a separate Board paper, while the requirements for administrative expenses will be requested through the regular annual budget approval process.

VII. REPORTING TO MANAGEMENT

50. The project milestones in each implementation phase under the framework will be assigned to the departments and offices concerned for monitoring, as provided in the recommended action plans (Appendixes 6–15). The Organizational Resilience Unit will be responsible for coordinating with the departments concerned and will report to Management on the progress of each implementation phase, as provided in the framework and their related action plans. The Organizational Resilience Unit will review the framework annually, including assessing residual risks and level of resilience achieved, and will report the outcome to Management.

Current State and Gap Analysis of ADB's Business Continuity Management

1. Since 2005, significant effort has been expended, involving many departments within ADB, to support business continuity. Business vulnerabilities have been identified, risks assessed, potential impacts to operations measured and business continuity plans developed. ADB has a business continuity management (BCM) structure in place. Business impact analyses and supporting risk assessments are undertaken on a regular basis. Business continuity plans (BCP) have been prepared and are regularly tested. And each test serves to improve the degree to which ADB can reasonably expect to withstand the vast majority of potential disruptions, those that would last for less than seven days. The Office of the Auditor General (OAG) conducts regular audits of ADB's business continuity planning, business impact analysis (BIA) processes and emergency drills.

2. ADB currently maintains an owned warm in-country business continuity facility (BCF) at Clark and a leased cold offshore site in Singapore.[1] Both sites have a seating capacity for 40 staff. The offshore site is a contracted facility on a "first come, first served" basis and there is no assurance that ADB would be given priority use of the facility during a disaster.

3. The activation of either site is triggered by a decision of the Crisis Management Team. Depending on the degree of disruption, three business continuity plans are invoked, i.e. BCP A, B or C. BCP A is activated when headquarters is still accessible and building support facilities and information technology (IT) infrastructure for priority business applications are still in place. Priority business processes are continued in ADB headquarters while normal business operation is suspended in such incidents as typhoon, pandemic, etc. BCP B is activated when priority IT applications are unavailable in headquarters and/or working from headquarters is unsafe. Events such as IT failure, earthquake, biochemical and bomb threats preventing normal operations call for BCP B activation. This plan covers the relocation of a number of key staff to and the continuation of priority business functions at the BCF. BCP C is activated when both the headquarters and the BCF are inaccessible. The plan covers the relocation of a number of key staff to resume and continue priority business functions at the offshore recovery site.

4. Assuming circumstances allow the provision of a full resource complement, ADB is capable of recovering critical IT systems and applications within 24–48 hours.[2] To stand up any of the recovery sites, a contingent of fifteen (15) IT staff would need to be deployed from the headquarters to recover critical systems and applications. Another thirty five (35) staff from the financial departments would also be required to be transferred from headquarters to the recovery site to resume priority business functions. This is assuming that key personnel are available and able to relocate to the recovery site during a major disruption.

5. Data recovery of critical applications relies primarily on backup media tapes being transmitted to the recovery sites on a daily basis.[3] Due to cost and the closure of customs offices on the weekends, no tapes are received at the offshore site on weekends. Data restoration at the recovery sites requires restoring the entire datasets, including test and

[1] A warm site contains active data links and pre-configured equipment and requires restoration of current data to commence operations. While a cold site is a standby site containing power and air conditioning facilities which can house data processing activities. The site requires full system configuration and data restoration of equipment and communication links.

[2] Memo on OIST Analysis of Recovery Time Achieved and Recovery Point Achieved dated 6 July 2015.

[3] Backups of SWIFT, iFIRST, Mainframe, Oracle-ERP, CLASS and TRMS are currently being performed daily on tapes and sent offsite to both the BCF in Clark and the offshore recovery site in Singapore. Backup tapes of other non-critical IT systems are maintained in headquarters.

development environments as ADB's backup systems does not allow extraction and restoration of specific transactions.

6. The business continuity management system has been designed to support the processing of urgent pending transactions only; new business is suspended while ADB is in business continuity mode. Furthermore, it depends on a number of assumptions. First, it is assumed that knowledgeable and trained personnel are available and able to execute the recovery plans. Second, it is assumed that ADB could access either the BCF or get to Singapore and that the Singapore facility is available.[4] It is also assumed that with parallel IT support from the headquarters, the recovery site will operate fully for partial recovery and that critical IT applications, systems, and data would be transmitted to the recovery site in a timely manner. Depending upon when the disruption would occur, there is a risk that all transactions generated over a two day period could be lost (if backup had not been created and/or sent to the recovery sites). It is also assumed that public telecommunication infrastructure will still be functioning and allow communication with staff.

7. ADB's International Organization for Standardization (ISO) certification, business impact analysis and business continuity planning is based on a disruption scenario lasting for less than seven days. Any event causing a disruption of more than six days, falls outside the business continuity planning window and will, therefore, be treated as a crisis and will fall under the purview of crisis management.[5]

8. In most organizations, BCM, security and disaster or crisis management are no longer viewed as simple administration functions, but rather as strategic functions. To improve ADB's business continuity ability to a resilient culture, the reporting function has to be changed.

9. In spite of considerable efforts to date to strengthen its business continuity, ADB may not be ready to handle a significant disruption to normal operations. The OAG audit on the BIA and BCP in July 2014 supported this view, noting the lack of business continuity planning for disruptions of more than six days and weaknesses in the BIA methodology. OAG further recommended that Management and the Crisis Management Committee be more actively engaged in business continuity decisions.

[4] The Singapore facility is a leased facility and operates on a first come first serve basis. Furthermore, the in-country facility at Clark is located in Pampanga. This province has been identified first amongst the top ten provinces susceptible to flooding.

[5] By reverting to a Crisis Management construct, risk events will be dealt with as they materialize rather than being managed or mitigate in advance. Administrative Order 4.18 authorizes the Crisis Management Committee to oversee ADB's response once a crisis is declared.

2015 Business Impact Analysis and Risk Assessment

1. As a first step in developing an Organizational Resilience Strategy, PricewaterhouseCoopers was engaged to assist ADB in completing a comprehensive Business Impact Analysis and Risk Assessment (BIA-RA).[1] The ADB-wide activity was performed from January to December 2015 with the final report[2] signed off and accepted in January 2016. The primary objectives of the BIA-RA are to:

(i) identify ADB's recovery and continuity priorities, objectives and targets;

(ii) identify, analyze and evaluate potential threats that could disrupt prioritized functions and supporting resources and ADB's exposure to those threats.

(iii) propose strategic and tactical measures that would:

(a) reduce the likelihood of a disruption,
(b) shorten the period of disruption,
(c) limit the impact of a disruption on ADB's key products and services, and
(d) allow key business functions to continue in a disruption.

A. Results of the Business Impact Analysis

2. The Business Impact Analysis (BIA) established an understanding of the adverse impact that a disruption may cause to ADB's reputation and credibility. ADB, which has been rated AAA since 1990, has provided the greatest level of security to its shareholders. Its strong business profile appeals to major borrowers making ADB a preferred creditor. Reputational damage could mean a decline or loss of shareholders' trust and confidence. Eventually, this could severely affect its financing and lending operations for the purpose of achieving its mission.

3. From a strategic perspective, the key products and services listed in Table A2.1 below are the business recovery priorities in maintaining ADB's sustainability in the event of a disruption. From the operational level, business processes supporting the continuous provision of these priorities were then identified and prioritized.

[1] The priorities and requirements identified in the BIA-RA are optimal objectives set by the departments and will be refined further based on the risk appetite and cost-benefit analysis.

[2] The BIA-RA is regularly reviewed and updated. Please refer to OAS for the 2015 BIA-RA results/report.

Table A2.1: Priority Products and Services

Key Products and Services	Minimum Business Continuity Objective (MBCO)[a]	Maximum Tolerable Period of Disruption (MTPD)[b]
1. New Bond Issuance and Debt Service	Debt service payments and coupon payments	24 hours
2. Trade Settlements (Investment)	Settlement of existing trades and contracts	24 hours
3. Derivatives Collateral Management	Validation of derivatives valuations and monitoring collateral calls	24 hours
4. Cash Management	Maintaining cash requirements	24 hours
5. Guarantees	Guarantee issuance	48 hours
6. Investments	Initiate new investment placements	7 days
7. Non Sovereign Loans	Servicing existing loans	10 days
8. Sovereign Loans and Grants	Servicing existing loans and grants	10 days
9. Equity Investment	Servicing existing investment commitments	10 days
10. Technical Assistance	Servicing existing technical assistance	15 days
11. Cofinancing Operations	Receipt of donor funds	1 month

Notes:

[a] Minimum Business Continuity Objective is the minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption.

[b] Maximum Tolerable Period of Disruption is the time it would take for adverse impacts, which might arise as a result of not providing a product and/or service or performing an activity, to become unacceptable. The MTPD column represents the duration of completing the entire process cycle from end to end. For example, the MTPD of 10 days for sovereign loans and grants disbursement processing covers receipt of withdrawal applications to payment processing of Treasury Department. These values were arbitrarily defined by Business Continuity Management Steering Group.

Source: *Business Impact Analysis and Risk Assessment Final Report,* January 2016

4. An assessment of potential impacts to these priorities reveals that the impact of a disruption on loans (sovereign and non-sovereign) and grants is high as they make up about 60% of ADB's financial operations and 62% of its revenue. Debt servicing and investment trade settlements are rated moderate to high impact largely due to the exposure of ADB's reputation in the capital market. For both investments and cofinancing operations, the moderate to high ratings reflect their financial positions between 30 to 40% of revenue and financial operations respectively. Since guarantees and equity investments make up less than 10% of the annual approvals but contribute significantly to ADB's net income, it is assessed with a moderate impact.[3]

5. The results of this BIA remain consistent with those of past BIAs. The resumption of time sensitive financial activities focusing on business processes related to debt servicing, trade settlements and cash management remain to be top recovery priorities for ADB following a disaster. The resumption of mission critical activities relating to the delivery of development projects and supporting activities closely follows to ensure ADB's ability to fulfill its mission of

[3] ADB Annual Report 2014

providing financial assistance to its developing member countries (DMCs). Table A2.2 illustrates the recovery of business processes supporting the delivery of key products and services.

Table A2.2: Recovery Timelines of Business Processes Supporting Key Products and Services

Recovery Time Objective (RTO)	Business Processes
Within 4 hours	• People, Health, Safety and Security • Communication to Internal and External Stakeholders
Within 1 day	• Cash Management • Trade Settlements (Investments) • Debt Servicing • Derivatives Collateral Management • SWIFT Processing • Emergency Procurement • Emergency Travel and Land Transport Requests
Within 3 days	• Sovereign Loans and Grants Disbursements • Non-sovereign Loans and Equity Investment Disbursements • Guarantee Issuance • Request Donor Funds • Payments Processing • Payroll & Pension Processing • Staff Consultant Claims Processing • Vendor Payments
Within 7 days	• Investments • Limits & Compliance Monitoring • Institutional Procurement • Loan Service Payments and Other Collections • Operation support • Loan, Guarantee, Equity Investment Accounting
Within 2 weeks	• Technical Assistance Disbursements • Other accounting operations including preparation of financial reports
Within 1 month	• Loan Billing and Capitalization • Project Administration • Private Sector Operations • Public-Private Partnership Operations • Co-financing Operations • Independent Evaluations
Within 3 months	• Knowledge Products • Project Preparation and Processing
Within 6 months	• Country Partnership Strategy

Support Functions: Information Technology and Communication Systems; Facilities, Building and Utilities; Security and Emergency Services, Human Resource

Source: *Business Impact Analysis and Risk Assessment Final Report,* January 2016

6. Resources for business recovery were assessed and are summarized below. While these aspirations are ambitious, these are workable given Management support and financial resources.

(i) People – Approximately 5% (or 100 staff) of the workforce needs be deployed within the 24 hours following a disruption to resume essential processes. After which, the staff requirement will increase to 11% within the first one week, 25% within 1 month and 50% within 6 months. This does not account for additional staffing requirements that would perform damage assessment and prepare the permanent site for eventual restoration.

(ii) Premises – The design and size of the alternate office is dependent on the number of staff required to be onsite. Based on department consultations, approximately 60% of the business processes could potentially be performed remotely while the remaining processes would need to be performed at the recovery site. Business processes requiring inter-business unit workflows should be given priority for workspaces to increase the effectiveness of the recovery process.

(iii) Information Technology (IT) – Some IT systems are required to be recovered within 8 hours following a disaster. These are communications systems, which ensure continuous connection with ADB's stakeholders, such as email, website and telephone systems; and SWIFT which allows payment of ADB's urgent financial obligations. Financial related IT systems crucial in supporting the resumption of ADB's recovery priorities such as iFIRST, Mainframe and Oracle-ERP need to be recovered in no more than 24 hours.

(iv) Data and information – The departments/offices' dependence on documents in hardcopy, zero data loss for SWIFT, iFIRST, Oracle-ERP and Mainframe as well as data loss of no more than 24 hours for TRMS and CLASS are critical to resuming priority business processes. This requires employing a backup technology capable of real time data replication in an alternate location and the automation of the business processes.

(v) Supply Chain – An improved contract and service agreement with external parties to include business continuity arrangements should be in place. Many of ADB's processes are highly dependent on consultants, contractors and service providers in the delivery of services which also include operating the headquarters facilities and IT systems. A disruption of services provided by these external partners will have adverse impact to ADB.

B. Results of the Risk Assessment

7. The Risk Assessment (RA) was conducted concurrently with the BIA to identify the risk of the unavailability of five (5) essential resources for business processes to continuously function. These resources are people, premise, information technology, information, and supply chain.

8. Based on the assessment, while mitigating controls and plans are in place, there are still inherent risks in the availability of resources that would hinder the continuity of business processes in the event of a disruption. Natural calamities and IT failure are top threats perceived by departments that would likely disrupt their processes.

9. From a business continuity risk perspective, ADB's greatest vulnerability is attributed to the following.

(i) **Centralized business operations.** The majority of ADB's business processes including IT services, treasury and accounting functions are performed at the headquarters. Though the headquarters building has been designed to withstand natural disasters, it does not guarantee that its contents, particularly the data center and telecommunications systems will be left undamaged. Additionally, dependencies on public infrastructure such as power, communication, water and sanitation highlight the vulnerabilities to the availability of ADB's premises.

(ii) **Concentration of staff force including Management in ADB headquarters.** A geographical disaster could potentially impact on the availability of key personnel and decision makers. The current recovery plan is highly dependent on the availability of key staff in headquarters and, in an extreme event, these same people may be injured or severely affected hindering their ability to respond and support the recovery of ADB's business processes for a substantial period of time.

(iii) **Centralized data and IT resources in the headquarters.** Currently, the data center in the headquarters houses all IT production systems. Only electronic backups of critical IT systems are sent offsite. Backups of noncritical IT systems remain in the headquarters and are not stored offsite. Existing recovery sites have downscaled data centers that can only recover critical applications and selected shared folders which need to be brought up by headquarters staff. Therefore, a disaster affecting ADB's primary IT data center or the IT infrastructure may severely disrupt the continuity of ADB's operations. The current arrangement assumes that people and data will be able to get to the alternate site on a timely basis. It will, however, be difficult to locate and transfer staff to the recovery site in the event of a major disaster.

10. Details on the risk areas, current and proposed mitigation controls are summarized in Table A2.2.

C. Moving Forward

11. The 2015 BIA-RA report recommends the following next steps for ADB:

(i) Update ADB's current business continuity management (BCM) strategy to reflect the business and IT recovery time objectives identified during the BIA-RA exercise.

(ii) During the strategy selection and development phase, determine indicative costs of options and undertake a cost benefit analysis which may require a subsequent revision of the BIA-RA results. Indicative costing should include the following:

(a) upgrading of facilities and resources (e.g. IT equipment, workstations, etc.) at the alternate site,

(b) upgrading of IT disaster recovery capability, and

(c) improving offsite storage and recovery capability of all electronic data and hardcopy documents.

(iii) Assess the feasibility of decentralizing some of its operations to the field offices (FO). The assessment should include staffing, IT requirements and development of business continuity plans (BCP) at the FO level.

(iv) Upon finalization of the organizational resilience strategy, develop the following:

(a) crisis management plans including a corporate communications plan,

(b) BCPs documenting response, recovery and return to normal activities for all departments; and

(c) IT disaster recovery plans documenting the recovery of IT systems as per the IT recovery time objective and recovery point objective requirements.

(v) Upon finalization and approval of the BCPs, conduct regular exercises and testing of plans to ensure their adequacy and effectiveness, and promote ADB staff awareness. The exercise should include the following:

(a) notification tree exercise,

(b) tabletop walkthrough exercise,

(c) crisis simulation exercise, and

(d) IT disaster recovery testing

(vi) Provide continuous awareness to staff on ADB's BCM strategies, recovery priorities and their roles and responsibilities in the event of a disaster. It is also recommended that BCM be included as part of ADB's employee orientation program and performance appraisal.

(vii) Establish change management procedures and programs to set the standard operating protocols for any changes and revision to the BCM recovery objectives and strategy that will impact the BCM plans. The BIA-RA is a work-in-process, thus, validation should be conducted regularly.

Table A2.3: BCM Risk Register

Risk Category	Risk Description	Current Controls	Net Risks	Potential Mitigating Controls
People	Unavailability of key personnel to support BCM action plans during disaster	• Business continuity plans are in place to: ➢ Identify alternate staff in case primary staff is unavailable, and ➢ Invoke shortened approval processes (for CTL, ORM, and TD). • Key staff participate in business continuity training and exercises. • Some degree of multifunctional, cross trained staff exists due to job promotion opportunities within departments.	• Essential business functions are concentrated in headquarters. Consequently, key staff for decision making, approval, verification and processing are concentrated in headquarters. • Fragmentation of skills and the perceived "silos" in the organization are not only business recovery issues but also organizational performance issues. "Furthermore, the increase in the staff size of ADB resident missions has not been accompanied by a corresponding transfer of decision-making authority.[a] • There is a high potential of personnel or staff turnover due to early retirements and resignations.	• Decentralization of business processes through the following: ➢ Increasing field offices' decision making authority ➢ Outposting key staff to a field office or an alternate offshore office • Formal cross-training programs to increase layer of redundancy or alternates for key job roles • Documentation of operational procedures and work instructions including manual workarounds • Agreements with third party agencies for temporary staffing requirements or for executing payments (reciprocal agreements) • Work-from-home through remote connectivity and use of alternative communication channels
Premise	i. Unavailability of ADB headquarters ii. Loss of power iii. Loss of communication lines v. Loss of water and sanitation services	• Structural integrity of the headquarters can withstand seismic activities measuring up to 8 Richter scale • The headquarters is situated at a location which is not prone to flood • Typhoon precautions and warning mechanisms are in place • The headquarters is connected to 2 main electrical lines (ADB Avenue and EDSA sectors) operated by sole power distributor (MERALCO). • The headquarters has 6 x 1050 kW power generators which can be activated if power lines go down. The generators	• Majority of headquarters' power requirements depends on MERALCO, exclusive power distributor to Metro Manila. • There is a disconnection in the provision of utilities that would enable support of essential functions - electricity for 15 days while water supply for 5 days. This seems to indicate that building operation is sustainable only for 5 days. • Majority of ADB's telecommunication requirements is dependent on the Philippines telecommunication infrastructure. • Transferring of telephone lines/connections to the recovery site to respond to calls from stakeholders seems unclear	• Establish a fully functional business continuity facility based on requirements of the business impact analysis and risk assessment • Ensure sufficient space for staff at the business continuity facility based on the minimum staff requirement in a disaster • Provide VSAT units and trainings for key personnel • Avoiding dependency on single power distributor through: ➢ Assess or re-assess the sustainability of headquarters' building services to support essential business functions over longer periods of disruption

[a] *Inclusion, Resilience, Change: ADB's Strategy 2020 at Mid-Term*, IED Special Evaluation Report, February 2014.

Risk Category	Risk Description	Current Controls	Net Risks	Potential Mitigating Controls
		have a diesel fuel endurance of 330,000 liters which is good for 15 days. • A 743 MWh Solar Power Plant was recently installed to supply about 3.5% of the headquarters' total energy requirements. • The headquarters contracts 3 telecommunication and mobile service providers. ADB have radios, VSAT, BGAN and satellite phones as communication backups • Domestic water supply comes from two pipes, one on EDSA and the other from ADB Avenue. Water supply is stored in 2 x 260,000 gallons domestic tank which would be sufficient for 5 days. • A rainwater harvesting facility provides water for general cleaning of grounds, façade, and irrigation	• ADB is dependent on a single water concessionaire to supply domestic water. Metro Manila depends solely on Angat Dam for water supply. • Water supply and wastewater system can be incapacitated for an extended period of time in the event of a major disaster	➢ Operating a dedicated alternate site or multiple offices outside Metro Manila ➢ Avoiding dependency on Philippines' telecommunication infrastructure by operating a dedicated alternate site or multiple offices outside the Philippines • Formal training on the use of alternative communication devices • Distribute or disperse business functions across multiple operating sites (decentralized operations) outside Metro Manila or the Philippines
Information Technology/ System	Unavailability of IT systems and platforms	• Redundant or secondary servers for critical applications are available in headquarters. • Comprehensive IT governance (e.g., anti-virus deployment across production systems, real-time network IDS to monitor and detect suspicious activities, daily monitoring of system logs, firewall and router logs, penetration testing of Internet-facing applications, etc.) is in place. • In-country and offshore sites established to recover critical IT system and applications.	• The primary data center and production systems are centralized in headquarters. Its risk exposure is the same as the headquarters premises, Management, staff and business processes. • The existing recovery sites need to be brought up by staff coming from headquarters. It will be difficult to locate and transfer staff to the recovery site in the event of a major disaster like an earthquake. • Recovery sites have downscaled data centers that can recover critical applications only and selected shared folders. • Development banks in the Asia Pacific Region have high exposure to cyber-attacks. • Outsourced system development projects may leak sensitive information.	• Review and upgrades of redundant systems at headquarters • Availability and timeliness of IT systems at the recovery sites that meet ADB's business recovery timelines • Depending on ADB's risk tolerance, consider alternative continuity strategies and recovery options such as: ➢ Dual data center ➢ Offshoring of primary data center ➢ Owned or outsourced hot recovery site ➢ Cloud computing

Risk Category	Risk Description	Current Controls	Net Risks	Potential Mitigating Controls
Data and Information	Loss of information – hardcopy active files are kept onsite and copies of inactive files are kept offsite	• Backup of the entire ADB headquarters IT systems is performed daily. • Backup tapes of some critical IT systems (SWIFT, Mainframe, iFIRST, ERP) are transmitted daily to the in-country and offshore site while backup tapes of selected shared drives are transmitted weekly. • Backup of Lotus Notes email and databases are performed daily. Backup tapes of emails for selected staff and selected Notes databases are transmitted weekly to the offshore recovery sites. • Guide to Classifying Records and Applying Appropriate Records Retention and Disposal Schedule is in place. Archived files are stored off site through a service provider.	• Backups for "non-priority" IT systems including eSTAR and shared drives are stored only in the headquarters. No duplicate copies are stored outside the headquarters premises. • There are no backups for personal drives. • There is no clear guidance on the security of storing documents within a non-ADB, net based email domain. • A number of these high level processes are dependent on supporting documents in hard copies. These documents reside in the departments' office area. Only inactive files are archived.	• Enhance data backup strategy by considering the following: ➢ Level of criticality of data to be backed up and corresponding frequency ➢ Business recovery requirements and dependency to electronic data by various stakeholders ➢ Interdependency and interfaces of IT applications • Depending on ADB's risk tolerance, consider alternative continuity strategies and recovery options that may meet recovery point objective requirements such as: ➢ Increase frequency of transmittal of backup tapes to the recovery site ➢ Virtual tape back up ➢ Asynchronous and synchronous data replication • Strengthen guides, procedures and arrangements on document retention and disposal and protection of active hard copy documents. Promote electronic document submission and processing
Supply Chain	Dependency on consultants, contractors and service providers including public utilities	• Service Level Agreement or Work Performance Statement for each contract is in place • Documented and tested business continuity plans for key vendor/contractors (e.g., building maintenance, security, logistics, etc.)	• ADB remains dependent on a large number of contractors including utilities to provide operational services. Most contractors have not adequately prepared their employees to perform immediately in a post disaster environment. • Local government units do not have adequate firefighting, search and rescue, and communication capabilities to aid ADB in the event of major disaster.	• Distribute or disperse business functions across multiple operating sites (decentralized operations) outside Metro Manila or the Philippines • Documentation of operational procedures and work instructions including manual workarounds

ADB = Asian Development Bank, BGAN = Broadband Global Area Network, CTL = Controller's Department, ERP = enterprise resource planning, eSTAR = electronic Storage and Retrieval, IDS = intrusion detection system, iFIRST = integrated Funding, Investment, Risk and Settlements in Treasury, IT = information technology, ORM = Office of Risk Management, SWIFT = Society for Worldwide Interbank Financial Telecommunication, TD = Treasury Department, VSAT = very small aperture terminal.

Source: *Business Impact Analysis and Risk Assessment Final Report,* January 2016

ADB Risk Appetite

A. Background

1. Risk appetite can be defined as the amount and type of risk that an organization is prepared to accept in pursuit of its strategic objectives. The risk appetite statement reflected in this paper is limited to disruption related risks. The results of the 2015 BIA-RA have been considered in defining the risk appetite which in turn was used as one of the guiding principles in developing the OR framework.

2. The established risk appetite is a result of consolidating the inputs from the Business Continuity Management Steering Group (BCM-SG). By having an articulated risk appetite, ADB will be able to:

(i) identify threats and evaluate ADB's exposure to those threats,
(ii) define clearly acceptable and unacceptable risks,
(iii) strengthen controls and enhance business continuity capabilities, and
(iv) identify and streamline existing processes to make them more efficient, resilient, and operational while avoiding single points of failure

3. It is recognized that risk appetite may change over time as the OR program develops and matures. The Organizational Resilience Unit will initiate the periodic review of the risk appetite for adequacy and suitability. Any changes will be endorsed by the Steering Group prior to management approval.

B. ADB's Risk Appetite Statement

4. Risk appetite defines the boundary of acceptable risk and outlines which risk is not tolerable to ADB. It establishes ADB's risk tolerance. It could be originated by aligning real business disruption exposures with the management of critical activities. In establishing the Risk Appetite statement, ADB considers the worst plausible scenario such as a high magnitude earthquake or severe typhoon. ADB defines its risk appetite as follows:

"ADB regards staff safety as its primary concern. ADB is a conservative organization that adheres to sound banking principles in order to retain its reputation as a premiere financial institution. With respect to financial liabilities, ADB is committed to meeting its financial obligations when they are due, avoiding default, and maintaining its financial standing. ADB also complies with its contractual obligations, to the extent possible, in order to remain viable and able to fulfill its mission to its developing member countries (DMCs)."

5. Using the results of the 2015 BIA-RA, the desired risk appetite is "not to exceed the maximum tolerable period of disruption (MTPD)". Achieving this in the event of a business disruption lasting for one month would mean:

(i) SWIFT and other financial systems are operational within 1 day with minimal data loss.
(ii) debt service payments, priced bonds and swap transactions are settled within 1 day.
(iii) trade investments with same day value settlement are processed within 1 day.
(iv) monitoring of derivative exposures and collateral are completed within 2 days.
(v) guarantee issuances are processed within 3 days.

(vi) sovereign loans and grants other urgent claims are processed within 3 days.
(vii) cash management functions such as cash positioning, emergency cash disbursement, and payment processing are performed within 3 days.
(viii) payroll and pension are processed within 3 days.
(ix) non-sovereign loans and equity disbursements are processed within 7 days.
(x) servicing of existing technical assistance grants are processed within 15 days.
(xi) receipt of donor funds under the cofinancing operations are processed within 1 month.

6. The articulation of ADB's risk appetite also considered the impacts of a disruption on resources necessary to continue the delivery of the organization's key products and services.

(i) **People.** The safety and security of ADB personnel is a top priority. ADB will mitigate risks that may compromise people's safety and security. It will accept impacts of a disruption to its operation to protect its people.

(ii) **Premises and/or facility loss or denial of access to office space, equipment, and materials.** In a disruptive event affecting any of ADB's buildings or sites, staff may experience displacement, downtime or a decreased capability to operate. ADB recognizes that there is the possibility to lose access to or use of buildings, including its equipment and materials within the buildings due to a wide range of possible events. ADB will accept a level of unavailability of building and/or facility that that will not compromise its ability to resume its essential business processes in a timely manner.

(iii) **Technology processing.** In the event of a disruption, ADB will accept a level of technology downtime that that will not compromise its ability to resume its essential business processes in a timely manner.

(iv) **Technology data loss.** ADB has zero tolerance to data loss.[1] Business processes will recover by any means any lost transactions, records and documentation to keep ADB's reputation and financial records intact.

(v) **Processes.** ADB accepts a level of operational downtime that will not compromise the organization's viability. It will mitigate risks that may disrupt its ability to fulfill its mission. It is also recognized that some processes are sensitive and confidential and are required to be performed in a controlled environment. If the controlled environment is compromised, ADB is willing to accept delays rather than exposing itself to more risks.

(vi) **Supply chain (consultants, contractors, and all key vendors).** Inherent in all third party business relationships is the risk of non-performance, including non-performance due to impacts to the supplier's operational capabilities. ADB has low tolerance to the non-performance of agreed service levels.

[1] For the immediate and short-term actions, OIST will aim to reduce the data loss during a major business disruption from more than one day to less than twelve (12) hours. Zero data loss through real time data replication may be achieved over time and not in the immediate or short term.

Matrix of Multilateral Development Banks' Business Continuity Management Approaches

The matrix provides a comparison of multilateral development banks' approaches to business continuity management, as well as budget information, where applicable.

Organization	Resilient Infrastructure (e.g. Recovery Sites, Alternate work spaces)
World Bank Group	• Has effectively decentralized its activities and has the ability to operate most of its critical processes offshore. • Has the ability to secure alternate work spaces for some staff and management as the organization operates in multiple buildings in Washington DC. Other alternate arrangements include: readily available office and a third-party agreement office space provision for management • Operates two data centers with varying redundancy levels. Each data center is capable of supporting the entire operations: – Primary data center (hot site[a]) is located about 35 miles (56 km) from Washington DC. – Primary back-up site (also a hot site) is located in headquarters. – Currently, no out-of-region data center solutions.
International Finance Corporation	
European Bank for Reconstruction and Development	• Has two (2) disaster recovery sites, one on edge of financial district in London with dedicated full treasury operations. The other is 10 miles (16km) from headquarters on outskirts of London. Both are syndicated, contracted out recovery sites – except for the treasury operation which is a contracted but dedicated site.
International Monetary Fund	• IT Recovery Center contains a small portion of the organization's IT systems. • Operational recovery relies highly on remote work. • Recovery site (hot site) is 30 miles (48 km) from Washington including 30 work stations managed through a contractual arrangement
European Investment Bank	• Has outsourced its IT production in two (2) redundant datacenters (hot sites) with data mirroring capability • Contracted an external site with shared and dedicated recovery positions
African Development Bank	• Contracted a commercial alternate site based in Europe (both for the datacenter and office spaces of 100 seating capacity) to run the critical functions until at least 2015 • Implemented an owned alternate facility site (datacenter and 450 offices space capacity) co-located in a business park in Pretoria, South Africa. The site is permanently manned by 5 full time IT staff. Additional space to accommodate 450 staff was also leased. • The Pretoria site has a complete, on-line functional data center replicating the Tunis data center.

Organization	Resilient Infrastructure (e.g. Recovery Sites, Alternate work spaces)
	• With the transfer to Abidjan headquarters completed end 2014, Tunis was also retained as the second external business continuity facility with a full data center and 400 office space capacity.
Asian Development Bank	• Operates own in-country recovery site (warm site[b]) with 40- to 80-work station capacity located 100 km (62 miles) from the headquarters • Contracted a shared (on a first-come-first-serve basis) offshore recovery site (cold site[c]) located in Singapore

[a] A hot site is a fully equipped and configured recovery facility ready to take over data processing operations at short notice; data replication is continuous.

[b] A warm site is a facility containing active data links and pre-configured equipment and requires restoration of current data to commence operations.

[c] A cold site is a standby site containing power and air conditioning facilities which can house data processing activities. It requires full system configuration and data restoration of equipment and communication links to commence operations.

CTL = Controller's Department, DER = Department of External Relations, IT = information technology, OAS = Office of Administrative Services, OIST = Office of Information Systems and Technology, ORM = Office of Risk Management, TD = Treasury Department.

Source: Asian Development Bank.

ADB Organization Resilience Framework

1. Organizational resilience is an organization's capability to anticipate and respond to disruption related risks and its capacity to adapt to complex or changing circumstances under conditions of uncertainty. Organizational resilience is a mixture of both continuity and adaptability; it is maintaining continuity in the face of disruptive challenges, and sustaining long-term viability in the face of strategic change and a changing external environment.

2. ADB identifies the following key attributes in enhancing its resilience:

(i) **Governance.** Policies, structures and processes that promote coherent decision making within acceptable parameters of cost, risk and speed contribute to resilience. Effective governance enables ADB to take advantage of opportunities and mitigate risks, and ensure that appropriate entities are accountable for decisions. It also provides an environment in which innovation is supported and resources are provided and efficiently utilized.
(ii) **Leadership and culture.** Effective leadership creates a culture that drives resilience. Leadership both at the strategic and operational levels across ADB departments seeks to foster a culture where people are encouraged to take ownership of key decision making processes. Knowledge and information is accessible and shared proactively across internal boundaries to support the achievement of organizational objectives. As a result, a work environment is created that empowers a culture of trust, openness and innovation.
(iii) **Common vision and purpose.** By clearly communicating ADB's mission, goals, strategies and objectives, this will allow its staff to act in a manner consistent with the core purpose and values of the organization.

3. The following actions will support organizational resilience:

(i) develop awareness to anticipate, plan for, and respond to potential disruptive events,
(ii) bring coherence among ADB's business processes and resources,
(iii) develop adaptability into ADB's business processes to respond to changes in a resourceful and innovative manner,
(iv) strengthen ADB's capability to address disruptions, emergent risks and changes to its operating environment, and
(v) review effectiveness and continually improve.

Business Continuity (BPMSD, DER, OAS, OIST)

A. Purpose

1. The Business Continuity (BC) component manages the recovery or continuity of ADB's operations in the event of a disaster with minimal or no interruption. It identifies potential impacts and provides a capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

2. ADB recognizes that its current business continuity capability is limited to the recovery of some of key financial processes for disruptive events that may last for six days. The integration and alignment of business continuity to the organizational resilience framework will allow rationalization of key resources for a more effective response that will maintain ADB's core operations throughout a disruptive event. While the initiative aims to substantially decrease the impact of a disruptive event, it will not absolutely eliminate the risk. Thus, business continuity management (BCM) will play a major role in ADB's resilience.

B. Involved Departments and Offices

3. The Office of Administrative Services (OAS) will lead the development of this component. OAS will also provide support such as procurement, facilities and building, physical security, crisis response, logistics, travel, etc. in the implementation of BC initiatives.

4. The Budget, Personnel, and Management Systems Department (BPMSD) will provide advice on medical related emergencies, emergency budget requirements and development of business continuity related training programs.

5. The Department of External Relations (DER) will provide the resources and strategies to assist ADB communicate with internal and external audiences.

6. The Office of Information Systems and Technology (OIST) will document and maintain IT disaster recovery plans that ensures availability of technology during a disruption when practical.

7. All department and offices will develop, document and maintain their business continuity plans (BCP). All departments will participate in the regular exercising and assessment of business continuity arrangements.

C. Scope

8. The Business Continuity component covers all aspect of maintaining ADB's BCM program including:

(i) business impact analysis and risk assessment (BIA-RA);
(ii) business continuity strategy and plan development;
(iii) training, awareness, testing and exercising;
(iv) risk monitoring and reporting;
(v) review, assessment, performance monitoring;
(vi) maintenance of the International Organization for Standardization (ISO) 22301 certification; and
(vii) reporting to Management of ADB's BCM performance

D. Core Focus

9. In the immediate and short-term action plans, the component will focus on the following areas:

(i) align the existing program to support the organizational resilience framework which includes providing assistance to the operations departments, Office of Cofinancing Operations, Office of the General Counsel, and Operations Services and Financial Management Department in developing their business continuity plans;

(ii) work with the Office of Information Systems and Technology in implementing improvements to IT disaster recovery capabilities;

(iii) work with the Budget, Personnel, and Management Department, Controller's Department, Department of External Relations, Office of Risk Management, and Treasury Department in improving their existing business continuity arrangements; and

(iv) monitor the implementation of risk mitigating measures and assess the residual business disruption risks.

E. Key Action Items

10. Based on the high level implementation plan, a detailed action plan has been developed by the lead department or office. The succeeding table lists the action items to align this component to the overall organizational resilience initiative.

Table A6.1: Action Plan for the Business Continuity Component

Focus Area(s)

- To develop and institutionalize business continuity planning and management in all ADB departments and offices, including field office
- To validate and align business continuity requirement and recovery timeline of ADB departments and offices in consideration of ADB's risk appetite and cost-benefit analysis
- To coordinate the testing of business continuity plans and arrangement to ensure that they remain up-to-date and adequate to respond in the event of a disaster

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
A.	**Short-term Actions (0-2 years)**			
1	Update the business continuity strategy to reflect improvements in business continuity and IT DR capabilities	OAS	Q1 2016	Q2 2016
2	Review, update and obtain Management approval on relevant Administrative Orders, policies and procedures related to security, crisis management and business continuity.	OAS, BPMSD	Q2 2016	Q1 2017
3	Provide support for the interim to short-term staffing strategies	BPMSD, OAS	Q2 2016	Q4 2016
4	Identify additional resource requirements to support the updated or revised BCPs including IT requirements	OAS, OIST	Q2 2016	Q3 2016
5	Coordinate backup and IT DR procedures to support changes in BCPs	OIST, OAS	Q2 2016	Q3 2016
6	Validate if the business processes supporting the key products and services can be resumed within the recovery timelines set in the 2015 BIA-RA in consideration of ADB's risk appetite and cost-benefit analysis	OAS	Q2 2016	Q4 2017
7	Develop CMPs	OAS, BPMSD	Q2 2016	Q2 2017
8	Develop guidelines and/or criteria to include organizational resilience in the annual performance review process	BPMSD, OAS	Q3 2016	Q4 2016
9	Implement the organizational resilience communication plan	OAS, DER	Q3 2016	Continuing activity
10	Engage departments on the feasibility of decentralizing functions to the field offices in line with the Midterm Review Action Plans	OAS	Q3 2016	Q2 2017
11	Improve BCM awareness and training programs and coordinate and develop content on BCM and organizational resilience for the ADB employee orientation program	OAS	Q3 2016	Q2 2017
12	Enhance or update existing BCPs in line with IT immediate actions and include restoration to normal operations at a permanent facility after a disruption	OAS, CTL, ORM, TD	Q3 2016	Q2 2017

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
13	Develop and enhance BCPs for operations departments, OCO, OSFMD, and OGC	OAS, OIST, OGC, OSFMD, RDs, PSOD	Q4 2016	Q4 2017
14	If applicable, outsource selected business continuity and organizational resilience functions as an interim to support the organizational resilience implementation plan	OAS	Q4 2016	Q4 2017
15	Review re-purposing alternatives or options of the business continuity facility	OAS, OIST	Q1 2017	Q2 2017
16	Develop and implement organizational resilience performance metrics	OAS	Q1 2017	Q1 2017
17	Establish the organizational resilience reporting schedule, content and requirements	OAS	Q1 2017	Q1 2017
18	Establish a schedule for exercises for the immediate, short-term, medium-term, and monitoring phases of the organizational resilience framework including IT DR testing	OAS, OIST	Q1 2017	Continuing activity
19	Establish change management procedures for the BCM and organizational resilience framework	OAS	Q1 2017	Q2 2017
20	Revalidate the BIA-RA including recovery timeline and achieved residual risk post-organizational resilience implementation based on risk appetite and cost-benefit analysis	OAS	Q1 2017	Q2 2017
21	Coordinate and conduct crisis management exercises to occur in conjunction with the BC and IT DR exercises	OAS, OIST	Q3 2017	Q4 2017
B.	**Medium-term Actions (0-5 years)**			
22	Validate the staffing requirement, recovery timelines and resource requirements of all ADB departments and offices	OAS, OIST, BPMSD	Q2 2016	Q4 2018
23	Review and update the business continuity strategy to reflect improvements as a result of implementing the organizational resilience framework	OAS, OIST	Q3 2016	Q4 2016
24	Develop BCPs for remaining headquarters departments and offices, as well as field offices	OAS, OIST, All departments and offices	Q1 2018	Q4 2021
25	Develop a knowledge transfer capability to share organizational resilience concepts with developing member countries with the intent to develop an enhanced resilient community capabilities	OAS, RDs	Q1 2020	Q4 2020
C.	**Monitoring Phase (5-15 years)**			
26	Sustain and improve existing BCM program including BCP maintenance, exercises, drills, training and ISO certification	OAS	Q1 2018	Continuing activity

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
27	Continue the review and update BC strategy to reflect improvements in business and IT capabilities for the BC and IT DR program	OAS	Q1 2019	Continuing activity
28	Maintain BCM program including regular BIA-RA, testing, BCP reviews and assessments, management reporting	OAS	Q1 2019	Continuing activity

BPMSD = Budget, Personnel, and Management Systems Department, BCM = business continuity management, BCP = business continuity plan, BIA-RA = business impact analysis and risk assessment, CTL = Controller's Department, CMP = crisis management plan, DER = Department of External Relations, DR = disaster recovery, ISO = International Organization for Standardization, IT = information technology, OAS = Office of Administrative Services, OCO = Office of Cofinancing Operations, OIST = Office of Information Systems and Technology, ORM = Office of Risk Management, OSFMD = Operations Services and Financial Management Department, PSOD = Private Sector Operations Department, RD = Regional Departments, TD = Treasury Department.

Source: Asian Development Bank.

Crisis Management and Communication (BPMSD, DER, OAS, OIST)

A. Purpose

1. The Crisis Management and Communication establishes how ADB will effectively coordinate its actions to mitigate adverse outcomes of a business disruption. It focuses on understanding the situation, having communication strategies, and delivering key messages to the correct audience.

B. Involved Departments and Offices

2. The Office of Administrative Services (OAS) will lead the development of this component.

3. The Department of External Relations (DER) will provide advice and support in disseminating messages and information to internal and external audiences.

4. The Budget, Personnel, and Management Systems Department (BPMSD) will provide advice and support on medical related emergencies such as pandemic, biochemical attack, etc., provision of budget requirements, and development of training and awareness programs.

5. The Office of Information Systems and Technology (OIST) will provide the technology and support to disseminate messages and information to key stakeholders.

6. All department and offices will be aware of actions related to crisis management and communication.

C. Scope

7. Crisis management and communication covers the following aspects:

(i) crisis prevention – crisis preparation through planning and development of crisis management structure and plans, training and exercising;
(ii) incident command and control capability and the role of leadership before, during and after a crisis;
(iii) crisis response; and
(iv) reputation management, communications with key stakeholders and recovery of operations

D. Core Focus for the Immediate and Short Term

8. In the immediate and short-term, the component will focus on the following areas:

(i) improve the crisis management and communication structure and develop crisis management and crisis communications plans, and
(ii) improve the safe haven program and other crisis management support systems.

E. Key Action Items

9. Departments and/or offices involved will assess ADB's current disaster preparedness and response capabilities. Crisis management structure, plans and actions will be reviewed and improved based on ADB's requirements. If necessary, Management endorsement and approval will be sought.

10. Based on the high level implementation plan, a detailed action plan has been developed by the lead department or office. The succeeding table lists the action items to align this component to the overall organizational resilience initiative.

Table A7.1: Action Plan for the Crisis Management and Communication Component

Focus Area(s)

- To establish a functional crisis management structure and plans to respond to an emergency or crisis
- To enhance crisis management and communication capability
- To coordinate the testing of crisis management and emergency response plans to ensure that they remain up-to-date and adequate to address impacts of an emergency or crisis

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
A.	**Short-term Actions (0-2 years)**			
1	Review, update and obtain Management approval on relevant Administrative Orders, policies and procedures related to security, crisis management and business continuity	OAS, BPMSD	Q2 2016	Q1 2017
2	Review the CMP developed by the consultant and recommend modifications as necessary in line with the organizational resilience framework	OAS	Q2 2016	Q1 2017
3	Develop a crisis management structure with primary and alternate positions aligned with the organizational resilience framework	OAS	Q2 2016	Q4 2016
4	Oversee the development of a detailed earthquake preparedness and response plan under the Security and Emergency Response component	OAS	Q2 2016	Q2 2017
5	Select representatives from the appropriate areas or departments to review and refine the crisis management structure and plan	OAS	Q3 2016	Q4 2016
6	Finalize the CMP and circulate to concerned departments for comments and seek endorsement from Business Continuity Management Steering Group and/or Management, as applicable	OAS	Q4 2016	Q2 2017
7	Develop and schedule CMP exercising sessions and send out advance notice to participants, as necessary	OAS	Q1 2017	Q2 2017
8	Develop content for CMP training sessions	OAS	Q2 2017	Q3 2017
9	Complete post-training “After-Action” review and identify “Lessons Learned” and distribute these for comment	OAS	Q2 2017	Q2 2017
10	Update and revise the CMP, as necessary	OAS	Q2 2017	Q2 2017
11	Determine resource requirements and tools for effective crisis management capabilities and plan for a phased implementation	OAS	Q2 2017	Q2 2017
12	Implement project plan to improve emergency communication capability	OAS	Q3 2017	Q3 2021

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
13	Request approval, procure resources and tools and implement crisis management capacity building	OAS	Q3 2017	Q3 2021
14	Participate in the planning of long term exercising schedule in coordination with business continuity and IT disaster recovery exercises to enhance command, control and communication	OAS	Q3 2017	Q4 2017
15	Conduct briefing to the Business Continuity Management Steering Group and Management, if necessary.	OAS	Q1 2018	Q1 2018
B.	**Medium-term Actions (0-5 years)**			
16	Conduct regular CMP awareness and training sessions	OAS	Q3 2017	Continuing activity
17	Assess adequacy of the CMP and update or revise, as necessary	OAS	Q3 2017	Continuing activity
18	Establish a program maintenance for crisis management	OAS	Q1 2018	Continuing activity
19	Schedule and conduct exercises at least twice a year	OAS	Q1 2018	Continuing activity
20	Report the performance of the crisis management program to Management and the Business Continuity Management Steering Group	OAS	Q1 2019	Continuing activity
21	Expand coordination and working relationships external to ADB and with developing member countries	OAS	TBD	TBD
22	Expand coordination and working relationships with local government agencies	OAS	TBD	TBD

BPMSD = Budget, Personnel, and Management Systems Department, CMP = crisis management plan, OAS = Office of Administrative Services

Source: Asian Development Bank.

Information and Communication Technology (OIST, OAS, BPMSD)

A. Purpose

1. ADB's business processes rely extensively on information technology (IT). This requires a high availability of IT services and enhanced disaster recovery capabilities while maintaining the necessary level of security and providing service support to users.

2. This component is to ensure the required IT systems and data are available when they are needed and that information vital to ADB's operations are protected and recoverable according to the desired levels agreed with the business users.

B. Involved Departments and Offices

3. The Office of Information Systems and Technology (OIST) will lead the effort to build resilience in ADB's technical infrastructure including data availability and IT disaster recovery capability. OIST will develop capabilities that are diverse, redundant and designed for high availability supporting ADB's operations, business requirements and risk appetite.

4. The Office of Administrative Services (OAS) and the Budget, Personnel, and Management Systems Department (BPMSD) will provide support in the provision of budget requirements, procurement and implementation of selected technical solutions including, but not limited to, facilities engineering, space planning, and development of training and awareness programs.

C. Scope

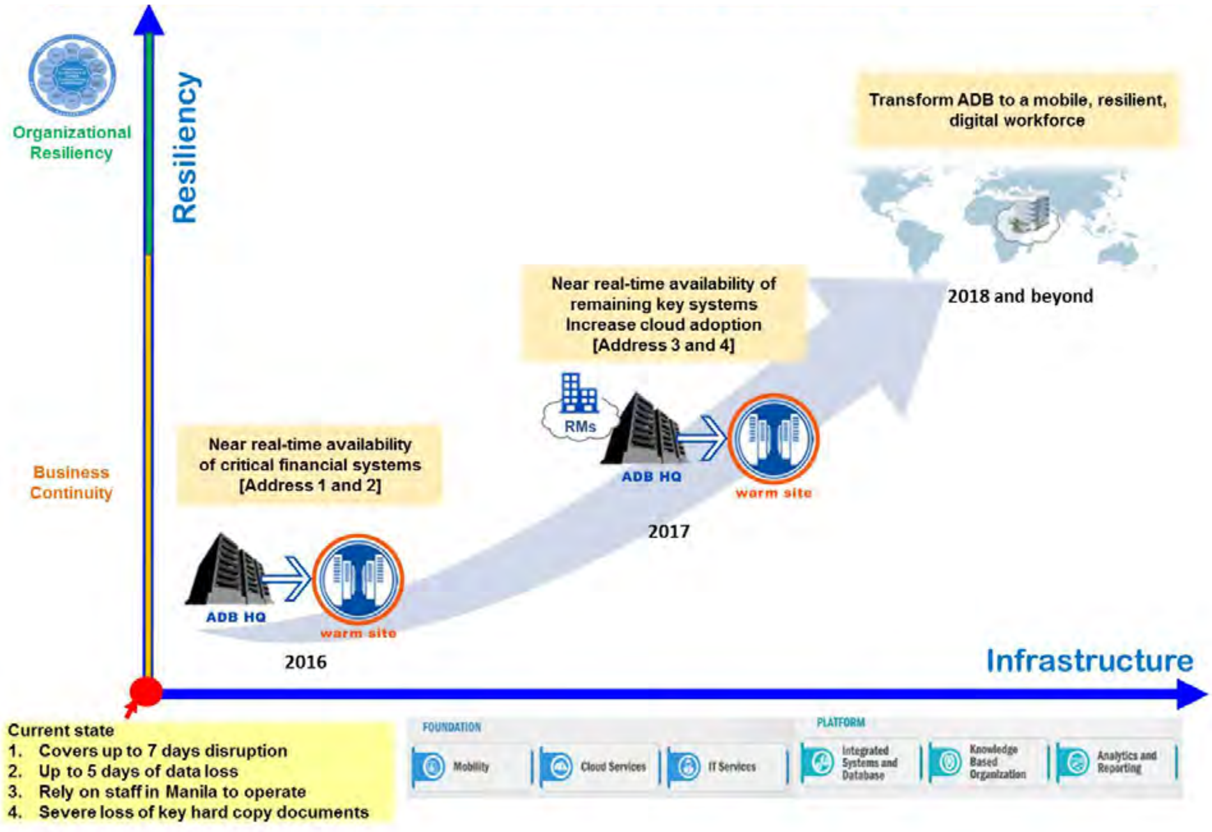
5. The ICT component covers the following aspects:

(i) information systems security;
(ii) network security;
(iii) systems analysis and design;
(iv) IT system data management;
(v) data creation and use;
(vi) active and inactive records systems;
(vii) data backup and protection including appraisal, retention and disposition; and
(viii) data center management and operations.

C. Core Focus: Information Technology Organizational Resilience Enabling Capabilities

6. Figure A8.1 illustrates the roadmap and timelines for achieving resilience in ADB's IT infrastructure. OIST will focus on improving the organization business continuity capability and IT disaster recovery capability, as well as transforming ADB into a mobile and resilient workplace.

Figure A8.1: ADB's Information Technology Organizational Resilience Roadmap


Organizational Resiliency
Resiliency
Business Continuity
Transform ADB to a mobile, resilient, digital workforce
2018 and beyond
Near real-time availability of remaining key systems Increase cloud adoption [Address 3 and 4]
RMs
ADB HQ
warm site
2017
Near real-time availability of critical financial systems [Address 1 and 2]
ADB HQ
warm site
2016
Infrastructure
FOUNDATION
Mobility
Cloud Services
IT Services
PLATFORM
Integrated Systems and Database
Knowledge Based Organization
Analytics and Reporting

Current state
1. Covers up to 7 days disruption
2. Up to 5 days of data loss
3. Rely on staff in Manila to operate
4. Severe loss of key hard copy documents

Source: ADB Office of Information Systems and Technology

D1: Significantly Improve ADB's Business Continuity Capabilities (0-2 years)

7. In 2016–2017, OIST will focus on improving the levels of recovery speed and increase data protection of ADB's key systems. By end of 2016, ADB's greatest vulnerability of having all its IT resources and data centralized in its headquarters in Manila will be addressed through establishment of a warm data center with data link to replicate critical financial systems in near real time, specifically for Controller's Department, Office of Risk Management, and Treasury Department. A secure cloud storage solution will also be provided for ADB data and documents.

8. Focus of 2017 is ensuring near-real time availability of remaining key systems. Managed services will also be engaged in order to reduce dependency on staff in the headquarters in recovering systems. Cloud adoption will also be increased enabling digitization and allowing anyone access to key data and documents remotely.

9. The outcome will reduce potential data loss and deliver faster recovery of critical financial systems to meet the desired levels of the business.

D2: Transform ADB to a mobile, resilient and digital workplace (0–3 years)

10. OIST has embarked on creating a comprehensive IT Plan for ADB covering the next three years. Labeled as “Real Time ADB”, it consolidates IT initiatives under Information System and Technology Strategy (ISTS) III, the Midterm Action Plan and current business needs into one strategic framework. As ADB's business landscape grows, it has become imperative for a modernized IT to help drive efficiency, resilience, and collaboration in response to increasing expectations and demand from the business.

11. Real Time ADB comprises of six pillars from which various initiatives will be implemented for a stronger, better, faster ADB:

(i) Integrated Systems and Databases (Financial, Human Resource, and Operations),
(ii) Knowledge-based Organization,
(iii) Analytics and Reporting,
(iv) Mobility,
(v) Cloud Services, and
(vi) IT Services.

12. As the business world is moving faster and is becoming more global and mobile, ADB workforce need to be able to communicate, collaborate and share resources from anywhere, anytime. Ultimately, ADB’s workplace in the future must seamlessly have the right devices, appropriate communication infrastructure, necessary mobile business applications and a workplace environment which is team-oriented. The ‘Real Time ADB’, through the Cloud Services and Mobility pillars, supports ADB’s shift towards organizational resilience and shall enable an agile and mobile workforce to work effectively despite any disruption.

13. The Real Time ADB was endorsed by the President on 2 March 2016 and by the IT Committee on 3 March 2016.

E. Key Action Items

14. OIST will leverage on the existing IT capabilities in implementing the immediate/interim IT solutions with a more advanced and robust technical infrastructure as a desired future state in mind.

15. In designing a long term IT solution, OIST will have to review and validate the business continuity requirements of each department taking into account ADB’s risk appetite, and the most practical and cost effective IT phased approach toward organizational resilience.

16. Based on the high level implementation plan, a detailed action plan has been developed by the lead department or office. The succeeding table lists the action items to align this component to the overall organizational resilience initiative.

Table A8.1: Action Plan for the Information and Communication Technology Component

Focus Area(s)

- To significantly improve ADB's business continuity capability and information technology disaster recovery
- To transform ADB into a mobile, resilient, and digital workplace

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
A.	**Immediate Actions (within 6 to 12 months)**			
Significantly Improve ADB's Business Continuity Capabilities				
1	Establish an offshore warm site	OIST	Q1 2016	Q3 2016
2	Establish data link between headquarters and the offshore site to replicate critical financial systems	OIST	Q1 2016	Q3 2016
3	Regular offsiting of tape backup of non-financial systems[a]	OIST	Q1 2016	Q3 2016
4	Infrastructure management and system administration managed by service provider (for offshore data center)	OIST	Q1 2016	Q3 2016
5	Provide cloud storage solution for ADB data and documents	OIST	Q2 2016	Q4 2016
B.	**Short-term / Medium-term Actions (0-3 years)**			
Transform ADB to a mobile, resilient, and digital workplace				
6	Extend warm site to replicate other key systems	OIST	Q1 2017	Q4 2017
7	Develop IT Blueprint[b] and implementation roadmap for Real Time ADB	OIST	Q1 2016	Q4 2016
8	Initial initiatives in the IT Blueprint relevant to organizational resilience are, but not limited to, the following: (i) Cloud Services (e.g. cloud storage solution, cloud email solution) (ii) Mobility (e.g. remote access, mobile devices, mobile applications) (iii) Consolidation of financial systems (iv) Decommissioning of Mainframe	OIST	Q1 2016	Q4 2018

[a] Yearend backups of nonfinancial systems will be offsited to BCF Clark.

[b] As of this writing, different teams in OIST are working together to create the IT Blueprint which will outline the projects and initiatives for each of the pillars of the Real Time ADB. Detailed action plans will be updated once the IT Blueprint is finalized.

IT = information technology, OIST = Office of Information Systems and Technology.

Source: Asian Development Bank

Security and Emergency Response (BPMSD, OAS, OIST)

A. Purpose

1. The Security and Emergency Response component refers to the management of proactive efforts to reduce the physical risk to ADB and the established responses to the consequences/impacts of a crisis or disaster to protect personnel and property. This would include operations, logistics, planning, finance, administration, safety, and information flow of selected emergency responses.

B. Involved Departments and Offices

2. The Office of Administrative Services (OAS) will lead the development of this component.

3. The Budget, Personnel, and Management Systems Department (BPMSD) will provide advice and support on medical related emergencies such as pandemic, biochemical attack, etc. provision of budget requirements, and development of training and awareness programs.

4. The Office of Information Systems and Technology (OIST) will provide support for any new technologies required to enhance this component and identify methods to protect IT assets and data in the event of a disaster.

5. Staff in all departments and offices will be aware of their responsibilities in an emergency or security situation.

C. Scope

6. The Security and Emergency Response component covers the following aspects:

(i) safety and security of all personnel at all ADB locations or all locations where ADB businesses are conducted;
(ii) crisis management support – preparation through planning and development of security and emergency management programs including team structures, plans and providing awareness and training;
(iii) management of daily operational incidents, incident escalation and communication before, during and after an incident;
(iv) incident prevention and immediate response capabilities;
(v) coordination and interoperability of external responses;
(vi) protection of ADB premises and assets; and
(vii) individual and family preparedness (earthquake, fire, severe weather, etc.).

D. Core Focus

7. In the immediate and short-term, the component will focus on the following areas:

(i) improve the security and emergency management structure, programs, capabilities and communications capabilities;
(ii) design and manage the safe haven program; and
(iii) support and integrate with the crisis management plan through existing and developed support systems.

E. Key Action Items

8. Departments and/or offices involved will need to assess the current security and emergency response capabilities and improve these capabilities significantly over time. This includes the review and enhancement of the safe haven program, earthquake preparedness, emergency communications capabilities and emergency evacuation and shelter in place program for a variety of disruptive scenarios.

9. Based on the high level implementation plan, a detailed action plan has been developed by the lead department or office. The succeeding table lists the action items to align this component to the overall organizational resilience initiative.

Table A9.1: Action Plan for the Security and Emergency Response Component

Focus Area(s)

- To establish a functional emergency response and communication structure and plans
- To enhance ADB headquarters' emergency response and physical security capability
- To increase staff awareness on personal and family disaster preparedness

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
A.	**Short-term Actions (0-2 years)**			
General				
1	Review, update and obtain Management approval on relevant Administrative Orders, policies and procedures related to security, crisis management and business continuity	OAS, BPMSD	Q2 2016	Q1 2017
2	Review and update plans and procedures for monitoring expected and unforeseen events or situations that could become a crisis	OAS	Q2 2016	Q2 2017
3	Review, update or develop security and emergency response plans to align with the 2015 business impact analysis and risk assessment and identify available resources and additional preparations needed	OAS	Q2 2016	Q3 2016
4	Work with other functional areas (facilities, logistics, medical, etc.) to ensure emergency response teams are established and rehearsed, are distinct from normal management chains, and have defined roles and responsibilities	OAS	Q2 2016	Q2 2017
5	Engage external entities e.g. key service providers, emergency responders in the planning and sharing of information	OAS	Q2 2016	Continuing activity
6	Develop implementation timelines and resource requirements for improving security and emergency response to support the organizational resilience framework	OAS	Q3 2016	Q4 2016
7	Upgrade of the electronic access control system	OAS, OIST	Q1 2017	Q4 2018
8	Develop content for crisis management training and awareness sessions	OAS	Q2 2017	Q3 2017
9	Attend organizational resilience awareness and education training	OAS, BPMSD	Q3 2017	Q4 2017
10	Participate in the planning of long term exercising schedule in coordination with business continuity and IT disaster recovery exercises to enhance command, control and communication	OAS	Q3 2017	Q4 2017
11	Conduct or deliver an initial run of crisis management training sessions	OAS	Q3 2017	Q4 2017

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
Supporting Project: Emergency Communication Program				
12	Establish an emergency communication plan which will be incorporated as a component of the crisis management plan	OAS, DER, OIST	Q2 2016	Q2 2017
13	Scope the emergency communication plan to be two-way i.e. communications can be issued by ADB and ADB can receive responses from staff and stakeholders during an emergency	OAS	Q2 2016	Q2 2017
14	Develop the emergency communication plan which includes a review of current ADB capabilities, identification of necessary tools and equipment. Initiate consultant recruitment, as necessary	OAS, OSFMD	Q2 2016	Q2 2017
15	Review and test elements of the established emergency communication systems for effectiveness.	OAS	Q1 2017	Q2 2017
16	Develop a detailed project plan and resource requirements on building emergency communication capacity for endorsement by the Business Continuity Management Steering Group and/or Management, as necessary. Plan for a phased implementation approach.	OAS	Q2 2017	Q2 2017
17	If necessary, modify the existing crisis management area to accommodate an emergency operations center and have redundant facilities in a separate location	OAS	Q3 2017	Q4 2018
18	Implement project plan to improve emergency communication capability	OAS	Q3 2017	Q3 2021
Supporting Project: Develop and Implement Earthquake Preparedness Program for Staff and Dependents				
19	Formulate and test an earthquake evacuation plan for staff and dependents	OAS, BPMSD	Q2 2016	Q3 2017
20	Develop and test earthquake response operational plan	OAS	Q3 2016	Q2 2018
21	Enhance the Security Operations Center	OAS, OIST	Q1 2016	Q4 2016
22	Enhance the emergency communication system	OAS, OIST	Q1 2017	Q4 2017
23	Undertake bracing of equipment and furniture to protect against seismic damage	OAS	Q3 2016	Q1 2017
24	Procure safety and emergency response equipment	OAS	Q1 2016	Q4 2017
25	Replace or rehabilitate the fire management and alarm system and upgrade the headquarters building seismic sensors	OAS	Q4 2016	Q4 2018
26	Enhance safe haven facilities	OAS	Q2 2017	Q4 2018
27	Purchase trauma bags (handling of mass casualty medical incidents)	OAS, BPMSD	Q2 2017	Q4 2017
28	Establish procedures for building assessment after a major earthquake event	OAS	Q1 2017	Q3 2017

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
29	Purchase of manual alarm system (as redundancy to the existing public address system)	OAS	Q1 2017	Q4 2017
30	Enhance evacuation signage and procedures	OAS	Q2 2017	Q4 2017
31	Conduct specialized trainings for Incident Response Team	OAS	Q3 2016	Continuing activity (once a year)
32	Conduct awareness raising activities (town hall meetings, emergency supplies fair, workshops/trainings on personal and family preparedness, articles on disaster preparedness, flyers, drills, etc.)	OAS	Q2 2016	Continuing activity
33	Conduct basic and advanced first aid and basic life support training for ADB Staff (including refresher sessions)	OAS, BPMSD	Q1 2016	Continuing activity
34	Conduct training on Incident Command System	OAS	Q2 2017	Q2 2017
35	Provide staff subsidy for 72 hour emergency kits	OAS, BPMSD	Q3 2016	Continuing activity (for incoming new staff)
36	Develop staff neighborhood response plan	OAS, BPMSD	Q4 2017	Q2 2019
B.	**Medium-term Actions (0-5 years)**			
37	Establish regular testing and update of the earthquake evacuation plan	OAS	Q1 2018	Continuing activity (at least once every two years)
38	Establish regular testing and update of the emergency communication plan	OAS, DER	Q1 2018	Continuing activity (at least once every two years)
39	Conduct table top exercises to management and/or senior staff to assess adequacy of the earthquake response operational plan	OAS	Q2 2018	Continuing activity (at least once every two years)
40	Conduct table top exercise to ADB departments and offices to assess the adequacy of the earthquake response operational plan	OAS	Q3 2018	Continuing activity (at least once every two years)
41	Conduct ADB wide simulated earthquake exercises	OAS	Q3 2018	Q4 2018
42	Conduct refresher session on first aid for staff	OAS	Q1 2018	Continuing activity
43	Conduct trainings for search and rescue for Incident Response Team members	OAS	Q1 2018	Continuing activity

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
44	Participate in business continuity and IT disaster recovery testing activities	OAS	Q1 2018	Continuing activity
45	Attend organizational resilience awareness and education training	OAS	Q1 2018	Continuing activity
46	Report the performance of the emergency management program to the Business Continuity Management Steering Group and/or Management, as applicable	OAS	Q1 2018	Continuing activity
47	Establish program maintenance for emergency management	OAS	Q1 2018	Continuing activity
48	Expand working relationships external to ADB and with developing member countries	OAS	TBD	TBD
49	Expand working relationship with local government agencies	OAS	TBD	TBD
50	Support for staff and their families in the case of emergency to the extent possible as directed	OAS	TBD	TBD

BPMSD = Budget, Personnel, and Management Systems Department, DER = Department of External Relations, IT = information technology, OAS = Office of Administrative Services, OIST = Office of Information Systems and Technology.

Source: Asian Development Bank.

Facilities and Assets (BPMSD, OAS, OIST)

A. Purpose

1. The Facilities and Assets component aims to provide safe, secure and reliable work spaces in headquarters and field offices. This component also includes provision of safe haven and alternate work spaces in the event of a disruption.

2. The headquarters building has been designed, engineered and operated to be a safe and secure working environment. It houses Management and the majority of ADB staff, the current data center and offices of core and support functions. The possibility exists that a disruptive event may occur that damages, destroys or denies access to the headquarters. This is a recognized single point of failure.

B. Involved Departments and Offices

3. The Office of Administrative Services (OAS) will lead the development of this component.

4. The Office of Information Systems and Technology (OIST) will provide facility requirements to support the required IT infrastructure.

5. The Budget, Personnel, and Management Systems Department (BPMSD) will contribute to establishing ADB's safe haven program.

6. All departments and offices will provide the minimum workspace requirements to resume their business processes based on agreed timelines.

C. Scope

7. The Facilities and Assets component covers the physical building design and operations; office site selection criteria, assessment and recommendations; safety and security design, operations and maintenance; construction and engineering documents, technical bidding specifications, real estate; asset protection; data center and critical environments construction, maintenance, and management; and, environmental and sustainability programs such as certifications to Leadership in Energy and Environmental Design, International Organization for Standardization (ISO) 14001, Occupational Health and Safety 18001, Energy Management ISO 50001.

D. Core Focus

8. The initial focus in the immediate and short term timeframes is to assess and implement actions related to improving headquarters' capability to support operation in the event of a prolonged disruption including provision for safe haven and a backup workspace arrangement in country or offshore. This will include assessing the utility of the in-country business continuity facility.

E. Key Action Items

9. Departments and offices involved will perform a feasibility and market analysis of available options including alternate work spaces and will review the space requirements of business processes that will be outposted.

10. Based on the high level implementation plan, a detailed action plan has been developed by the lead department or office. The succeeding table lists the action items to align this component to the overall organizational resilience initiative.

Table A10.1: Action Plan for the Facilities and Assets Component

Focus Area(s)

- To assess and improve ADB headquarters building and facilities' capability to support business processes in the event of a disruption
- To design and implement a workplace recovery arrangement in the event that the ADB headquarters cannot be accessed
- To provide office space requirements for ADB departments and offices that will setup functions offshore

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
A.	**Short-term Actions (0-2 years)**			
1	Review ADB policies and guidelines on safe haven. Identify requirements and reach an agreement on safe haven specifications. Establish exclusions as appropriate	OAS, BPMSD	Q3 2016	Q2 2017
2	Assess the work space availability of the field offices to accommodate short-term outposting of TD staff and long-term outposting of CTL staff	OAS, OIST	Q3 2016	Q3 2016
3	Provide support to OIST's technology implementation, as applicable	OAS	Q3 2016	Q1 2017
4	Determine if outposting TD and CTL impacts operations at existing field office and provide suggestions, recommendations and alternatives	OAS, TD, CTL	Q3 2016	Q4 2016
5	Assess ADB headquarters building and facilities to support operations in a disruption and identify enhancements and align availability of utilities, as necessary	OAS	Q3 2016	Q4 2016
6	Establish the approval and authority to activate crisis management arrangements during emergencies	OAS	Q3 2016	Q1 2017
7	Request for representatives from appropriate departments to assess workspace requirements	OAS	Q4 2016	Q3 2017
8	Take a leadership role in the assessment, feasibility study and recommendations on a headquarters based alternate workplace strategy	OAS, OIST, BPMSD	Q4 2016	Q3 2017
9	Establish criteria for the market assessment of available office space including accessibility, security, existing high speed network connection, access to food, parking and transportation	OAS, OIST, BPMSD	Q4 2016	Q1 2017
10	Perform feasibility study of leasing readily available office space for 250 staff within 1 week, 500 within one month inside and outside the Philippines. Further, study the feasibility of purchasing or leasing temporary office facilities (modular or mobile solutions) for 1,000 staff within 3 months and 2,300 staff within 12 months at a site of choice (inside or outside the Philippines) at the time of disruption	OAS, OIST	Q4 2016	Q1 2017
11	Determine when full staffing (or staff levels as directed) can be in place, if necessary, based on the various events or scenarios	OAS, OIST, BPMSD	Q4 2016	Q1 2017

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
12	Setup of offices for outposted staff and/or expand selected field office, as applicable	OAS	Q4 2016	Q1 2019
13	Establish a plan for damage assessment and restoration activities at headquarters	OAS	Q1 2017	Q3 2017
14	Develop initial scope, resources, funding related issues	OAS, BPMSD	Q1 2017	Q1 2017
15	Review re-purposing alternatives and options for the business continuity facility and determine any reasonable alternative within the same location	OAS, OIST	Q2 2017	Q3 2017
16	Develop alternate workplace recovery arrangements and seek endorsement, as necessary	OAS , OIST	Q2 2017	Q2 2017
17	Develop a detailed project plan and resource requirements to improve safe haven program. Plan for phased implementation approach	OAS, BPMSD	Q2 2017	Q3 2017
18	Implement actions to establish and/or improve the safe haven program	OAS, BPMSD	Q3 2017	Q4 2018
19	Brief the Business Continuity Management Steering Group and Management and/or Management, as applicable, on the safe haven program	OAS, BPMSD	Q1 2018	Q1 2018
20	Establish and implement safe haven program maintenance	OAS, BPMSD	Q4 2018	Continuing activity
B.	**Medium-term Actions (0-5 years)**			
21	Implement the alternate work place strategy	OAS, OIST	Q2 2017	Q3 2017
22	Implement recommendations to fortify headquarters building against prolonged disruptions with improved safe haven provisions for affected personnel	OAS, OIST, BPMSD	Q2 2017	Q1 2019
23	Establish program maintenance for facilities and building preventive maintenance and safety inspection	OAS	Q2 2018	Continuing activity
24	Assess any data center and/or server facilities requirements in country and/or offshore	OAS, OIST	Q2 2018	Continuing activity
25	Assess additional in-country and/or offshore workspace requirements	OAS, BPMSD, OIST	Q3 2018	Continuing activity
26	Implement headquarters long-term disruption strategy	OAS, OIST	Q1 2019	Q4 2021

BPMSD = Budget, Personnel, and Management Systems Department, CTL = Controller’s Department, OAS = Office of Administrative Services, OIST = Office of Information Systems and Technology, TD = Treasury Department.

Source: Asian Development Bank.

Business Data and Processes (DER, OAS, OIST, and involved Departments/Offices)

A. Purpose

1. The Business Data and Processes component refers to all ADB business processes that contribute to the sustainability of the organization and the information that flows into each process.

2. As higher IT and data availability are realized, all departments are expected to take advantage and streamline their processes, integrate automation and minimize manual processes, where feasible. The intent is to have consistent and practical methods across ADB to review and improve the flexibility of all data and processes over time in a deliberate manner.

B. Involved Departments and Offices

3. All departments and offices will refine their processes, manage business data in a more efficient manner and identify areas for improvement across ADB. Information sharing on best practices adopted by respective departments will be made available throughout the organization.

4. The Office of Administrative Services (OAS) will lead the development of the organizational resilience framework. OAS will also provide support such as procurement, facilities engineering, space planning, business continuity, etc. in the implementation of process improvement and data protection initiatives.

5. The Department of External Relations (DER) will provide advice and support in disseminating messages and information to internal and external audiences.

6. The Office of Information Systems and Technology (OIST) will lead the effort to build resilience in ADB's technical infrastructure including data availability and IT disaster recovery capability. OIST will develop capabilities that are diverse, redundant and designed for high availability supporting ADB's operations, business requirements and risk appetite.

C. Scope

7. Business Process and Data covers all processes and data in all departments and offices and all locations where ADB is operating.

D. Core Focus

8. In the immediate and short-term, the component will focus on the following areas:

(i) improve access to business data,
(ii) review business processes and identify improvement opportunities, and
(iii) identify means to minimize impacts of a disruption to business operations and expedite a return to business as usual.

E. Key Action Items

9. All departments and offices will assess their current processes and data access needs and identify areas for improvement to eliminate inefficiencies and to enable access to data when needed.

10. Based on the high level implementation plan, a detailed action plan has been developed by the lead department or office. The succeeding table lists the action items to align this component to the overall organizational resilience initiative.

Table A11.1: Action Plan for the Business Data and Processes Component

Focus Area(s)

- To engage ADB departments and offices in further rationalizing and digitization of their processes
- To develop and institutionalize business continuity planning in all ADB departments and offices, including field offices

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
A.	**Short-term Actions (0-2 years)**			
1	Communicate throughout the organization the concept of the organizational resilience framework and the intent to enhance all ADB operations	OAS, BPMSD	Q2 2016	Q4 2016
2	Provide regular and ongoing communication, awareness, training, and exercise and encourage participation from all departments including contractors, consultants	OAS, BPMSD, DER	Q3 2016	Continuing activity
3	Establish focus groups in all ADB departments and offices to look into process gaps, improvement and streamlining opportunities in line with the organizational resilience framework objectives	All departments and offices	Q4 2016	TBD
4	Develop business continuity plans	All departments and offices	Q1 2017	Q4 2017
5	Establish focus groups in all departments to look into how the departments and offices can accomplish their work if the headquarters is unavailable	All departments and offices	Q1 2017	Q4 2017
6	Establish focus groups in all departments and offices to assess the temporary remote working opportunities using existing field offices and identify potential areas or functions, where this is feasible	All departments and offices	Q1 2017	Q4 2017
7	Establish focus groups in all departments and offices to document required resources to support the temporary transfer of work to the field offices they have identified	All departments and offices	Q1 2017	Q4 2017
8	Establish focus groups in all departments and offices to annually review more effective methods to complete their processes	All departments and offices	Q1 2017	Q4 2017
10	Encourage all ADB staff, consultants, and service providers to be alert on potential risks that may face their business operations and escalate these through their reporting structures	All departments and offices	Q1 2017	Continuing activity
11	Review the departments/offices' business continuity requirement as identified in the 2015 business impact analysis and risk assessment and determine whether these are documented at a level where these can be continued by a temporary resource as a short-term alternative	All departments and offices	Q1 2017	Continuing activity

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
12	Review the reliance of processes to hard copy documents. This review should consider the impacts if these records are no longer available. The departments and offices should determine if it is better to save and store these records away from the workplace or if it is more effective to digitize these records.	All departments and offices	Q1 2017	Q4 2018
13	Encourage discussion within departments on the issue of personal and family preparedness	All departments and offices	Q1 2017	Continuing activity
14	Review business processes and determine the implications of not recovering any of these within 2 weeks. This review should consider whether this process is a business imperative and why it is being done. - If this process is not a business imperative, then perhaps this should be considered for discontinuing this process. - If this process is required, can it be done in other ways to make this process available? - If this process remains with the current recovery time, are there staff members that are idled or have no work to do? - Can this process be done at another location or by other areas as a workaround? - If the technology and systems are available in a short timeframe in the future, can these processes be operational in a shorter period of time?	All departments and offices	Q1 2017	Continuing activity
15	Review the department's business continuity requirement as identified in the 2015 business impact analysis and risk assessment to determine any restriction other than data availability to shorten their recovery timelines inconsideration of the risk appetite and cost-benefit analysis	All departments and offices	Q1 2017	Q2 2017
16	Encourage interested staff to participate in safety and security programs	OAS	Q3 2017	Continuing activity
17	Provide awareness to all ADB staff on their roles and action in the event of an emergency, including updates to safety and security procedures	OAS, BPMSD	Q3 2017	Continuing activity
B.	**Medium-term Actions (0-5 years)**			
18	Include previous actions in the regular work plan of all departments and build upon accomplishments	All departments and offices	Q1 2017	Continuing activity
19	Review and modify recovery time objectives as technology improvements are made at ADB	All departments and offices	Q1 2017	Continuing activity
20	Review the business impact analysis and risk assessment results to determine any restriction other than data availability to shorten the recovery time objective	All departments and offices	Q1 2018	Continuing activity
21	Review and update the business continuity plans	All departments and offices	Q1 2019	Continuing activity

Source: Asian Development Bank.

People (BPMSD, OAS, SPD)

A. Purpose

1. The People component refers to the human aspects of the OR framework. It covers the Board of Director, Management, ADB staff and their dependents, consultants and contractors engaged in ADB's operations.

2. People are the key resource in responding to disruptive events to keep ADB operational and essential contributors in making the organization the premier development institution in the region. As much as they are essential, ADB's people are also the most vulnerable. The safety, security and well-being of its people are important to ADB.

3. ADB recognizes that appropriate measures must be in place to support staff dependents in the event of a crisis to enable staff to be available to support ADB.

B. Involved Departments and Offices

4. The Budget, Personnel, and Management Systems Department (BPMSD) will lead the development of this component.

5. The Office of Administrative Services (OAS) will provide staff welfare services such as first aid treatment, safe haven, advisories etc., as practical and possible.

6. The Strategy and Policy Department (SPD) will provide guidance on the development of appropriate policies.

7. All department and offices will be aware of the benefits and support available to staff during a disaster.

C. Scope

8. The People component covers the following aspects:

(i) budget allocation,
(ii) staffing requirements,
(iii) separation of duties to avoid personnel single points of failure,
(iv) geographic diversity of skills,
(v) training and awareness programs, including multi-skill training, and
(vi) support to dependents during a crisis.

D. Core Focus

9. The component will focus on the following areas in the immediate and short-term:

(i) work with departments and offices for staffing requirements and budget allocation for implementing respective action items,
(ii) provide guidance in developing training programs related to disaster preparedness and organizational resilience, and
(iii) establish policies and guidelines to provide support for dependents in the event of a crisis to include repatriation to home countries, if necessary.

E. Key Action Items

10. Departments and offices involved will provide guidance in developing training programs on general organizational resilience awareness, cross-training staff to perform critical processes, and individual and family disaster preparedness for headquarters staff which will then be cascaded to existing field offices and future business hubs when applicable in the medium term. These departments and offices will develop policies on staff welfare and support services for affected individuals.

11. Based on the high level implementation plan, a detailed action plan has been developed by the lead department or office. The succeeding table lists the action items to align this component to the overall organizational resilience initiative.

Table A12.1: Action Plan for the People Component

Focus Area(s)

- To increase ADB staff awareness on their roles and responsibilities in the organizational resilience initiative, including awareness on personal and family disaster preparedness and available support to staff and their dependents in the event of a crisis
- To reduce business disruption risk due to concentration of staff at the headquarters by distributing key functions at the field office

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
A.	**Short-term Actions (0-2 years)**			
1	Discuss budget impact issues of the organizational resilience framework implementation	BPMSD	Q1 2016	Q2 2016
2	Provide guidance on and support to the approved TD and CTL outposting and/or decentralization actions	BPMSD	Q2 2016	Q4 2016
3	Identify and provide guidance on human resources policies required to support the immediate, short- , and medium-term action plans of the organizational resilience framework	BPMSD	Q2 2016	Q4 2018
4	Provide guidance on and support to the approved information technology infrastructure solution	BPMSD	Q2 2016	Q4 2018
5	Participate in the review and improvement of the crisis management plan particularly emergency issues impacting staff	BPMSD	Q2 2016	Q2 2017
6	Review and update staff compensation policies for an extended outage where staff are not able to work due to the lack of ADB capabilities including available support when required	BPMSD, OAS	Q3 2016	Q3 2018
7	Assess the feasibility of incorporating organizational resilience aspects in job descriptions, individual work plans and annual performance evaluation	BPMSD, SPD	Q3 2016	Q4 2016
8	Participate in the development and delivery of awareness, training and exercise programs on organizational resilience	BPMSD, OAS	Q3 2016	Q2 2017
B.	**Medium-term Actions (0-5 years)**.			
9	Provide guidance on and support to the approved alternate workspace arrangements	BPMSD, OAS	Q2 2017	Q3 2017
10	Continue participation in organizational resilience awareness, training and exercise programs related to People	BPMSD	Q3 2017	Continuing activity
11	Develop long term staffing strategy including outposting guidelines, decentralization, etc. in consultation with concerned departments	BPMSD, CTL, TD, PSOD, OSFMD, SPD	Q4 2017	Q4 2018

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
12	Participate in the continual improvement of staffing strategies, budget review, training programs, etc. supporting the organizational resilience framework	BPMSD	Q4 2018	Continuing activity

BPMSD = Budget, Personnel, and Management Systems Department, CTL = Controller’s Department, OAS = Office of Administrative Services, OSFMD = Operations Services and Financial Management Department, PSOD = Private Sector Operations Department, SPD = Strategy and Policy Department, TD = Treasury Department.

Source: Asian Development Bank.

Finance (BPMSD, CTL, DER, OAS, OIST, ORM, TD)

A. Purpose

1. ADB's business model is built on its recognized reputation, sound financial principles, and credibility among its stakeholders, including shareholders and creditors. Reputational damage caused by untimely or failed settlements of any financial obligation may affect established trust and confidence. This component refers to the financial management aspects of ADB.

2. This component also details the establishment and maintenance of financial controls throughout a business disruption. This includes availability of funds for emergency purchases required for response and recovery, and recording of expenses during an incident.

B. Involved Departments and Offices

3. The Controller's Department (CTL), Office of Risk Management (ORM), and Treasury Department (TD) will lead the development of this component.

> *Note: Regional Departments (RDs) and the Private Sector Operations Department (PSOD) will identify transactions that need to be prioritized by CTL and TD in the event of a disruption.*

4. The Budget, Personnel, and Management Systems Department (BPMSD) will provide advice on personnel arrangements for outposting staff, medical related emergencies, emergency budget requirements, and development of training programs to support OR.

5. The Department External Relations (DER) will provide advice and support in disseminating messages and information to internal and external audiences.

6. The Office of Administrative Services (OAS) will provide the necessary support and resources such as facilities, assets, emergency response, business continuity, transport, etc. to ensure continuity of key financial processes.

7. The Office of Information Systems and Technology (OIST) will provide the systems, applications, and facility requirements to support the required IT infrastructure and communication tools.

C. Scope

8. The Finance component covers key financial processes of CTL, ORM, and TD related to maintaining ADB's reputation, debt servicing, and continuing the delivery of financial products. Below are those processes identified as the most critical:

(i) funding, debt service and derivatives management,
(ii) investment trade settlements,
(iii) SWIFT[1] and system management,

[1] Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a provider of secure financial messaging services.

(iv) cash transactions including cash positioning management, emergency cash disbursement and administrative expense payments,
(v) derivatives collateral management,
(vi) guarantee servicing, and
(vii) loan administration and loan accounting processing.

D. Core Focus

9. In the immediate and short-term, the component will focus on the following areas:

(i) strengthening of business continuity plans and arrangements of key CTL, TD and ORM deliverables including rationalization of key business processes, as applicable; and
(ii) developing, with OAS coordination, business continuity plans for upstream dependencies such as the Office of Cofinancing Operations, Office of the General Counsel, Operations Services and Financial Management Department, Private Sector Operations Department, and the Regional Departments to ensure the continuous processing of urgent transactions through a prolonged disruption.

E. Key Action Items

10. Departments and offices involved will validate the accuracy of their business continuity requirements identified in the 2015 business impact analysis and risk assessment (BIA-RA) to support the immediate, short-, and medium-term organizational resilience framework implementation plan.

11. In the medium term, departments and offices involved will expand their business continuity plans to all processes, as appropriate, and with costs justified with the intent to resume at a reduced timeline.

12. Based on the high level implementation plan, a detailed action plan has been developed by the lead department or office. The succeeding table lists the action items to align this component to the overall organizational resilience initiative.

Table A13.1: Action Plan for the Finance Component

Focus Area(s)

- To strengthen disaster preparedness and business continuity arrangements of Controller's Department, Office of Risk Management, and Treasury Department, including rationalization and decentralization of processes, to ensure continuity of key financial functions

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
A.	**Short-term Actions (0-2 years)**			
1	Confirm immediate or interim staffing arrangements	TD, CTL, ORM	Q1 2016	Q2 2016
2	Provide timing and resource requirements for the immediate or interim actions	TD, CTL, ORM	Q1 2016	Q2 2016
3	If outposting staff is an option, finalize selection of field office in coordination with OIST and BPMSD	TD, CTL, ORM, OIST, BPMSD	Q1 2016	Q4 2016
4	Test and validate changes in the BCP	TD, CTL, ORM	Q1 2016	Q4 2016
5	Design and implement changes in the BCP to meet the new requirements requested from the 2015 BIA-RA, as necessary	TD, CTL, ORM	Q1 2016	Q4 2017
6	Involve the supply chain (external parties) in planning and the sharing of information	TD, CTL, ORM	Q1 2016	Continuing activity
7	Develop and implement work-from-home programs to assess remote worker effectiveness	TD, CTL, ORM	Q2 2016	Q4 2017
8	Work with BPMSD to review and comply with policies that would affect staff outposting	TD, CTL, BPMSD	Q2 2016	Q4 2017
9	Review business processes for opportunities to digitize records and documents and minimize the use hard copy documents subject to the availability of adequate IT infrastructure. Review processes to establish streamlined and alternative processes to cope with business disruptions	TD, CTL, ORM	Q2 2016	Q4 2018
10	Work with OAS and OIST to confirm if the selected field office has capacity to accommodate outposted staff	TD, CTL, OIST, OAS	Q2 2016	Q4 2017
11	Develop cross-training programs.	TD, CTL, ORM	TD: Q2 2016 CTL/ORM: Q1 2018	Continuing activity
12	Provide briefings to staff in the departments on their roles and responsibilities in an emergency.	TD, CTL, ORM	Q3 2016	Continuing activity
13	Setup of offices for outposted staff and/or expand selected field office in consultation with relevant departments and/or offices	OAS, OIST	TD: Q3 2016 CTL: Q2 2017	Q4 2016 Q4 2017
14	Attend organizational resilience awareness and education training	TD, CTL, ORM	Q4 2016	Q4 2017

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
15	Deploy staff in selected field office once the enhanced technical infrastructure is available	TD CTL	Q1 2017 Q1 2018	Q4 2018
16	Establish departmental teams to document all business processes so that multiple staff can perform these processes	TD, CTL, ORM	Q1 2017	Q4 2017
17	Participate in business continuity and IT disaster recovery testing activities	TD, CTL, ORM	Q1 2017	Continuing activity
18	In line with the business process rationalization, work with OIST to ensure data security and integrity	TD, CTL, ORM, OIST	Q1 2017	Continuing activity
19	Review and report on the immediate outposting plan efforts	TD, OIST	Q2 2017	Q4 2018
20	Design long term staffing strategy (local hiring or outposting, offshore offices, etc.) for CTL, ORM, TD and OIST based on business unit requirements	TD, CTL, OIST, ORM	Q4 2017	Q4 2018
B.	**Medium-term Actions (0-5 years)**			
21	Promote electronic document submission and processing subject to availability of IT infrastructure	TD, CTL	Q1 2016	Continuing activity
22	Deliver cross-training programs	TD, CTL, ORM	TD: Q1 2018 CTL/ORM: Q1 2018	Continuing activity
23	Strengthen guides, procedures, and arrangements on document retention and disposal and protection of active hard copy documents	CTL	Q1 2017	Continuing activity
24	Review and report on the outposting progress and improved business continuity capabilities supporting the organizational resilience framework	TD, CTL, ORM	Q3 2017	Continuing activity
25	Implement the long term offsite staffing plan	TD, CTL, ORM	Q1 2018	Continuing activity
26	Participate in the annual BIA-RA	TD, CTL, ORM	Q1 2018	Q4 2018

BPMSD = Budget, Personnel, and Management Systems Department, BCP = business continuity plan, BIA-RA = business impact analysis and risk assessment, CTL = Controller's Department, IT = information technology, OAS = Office of Administrative Services, OIST = Office of Information Systems and Technology, ORM = Office of Risk Management, TD = Treasury Department.

Source: Asian Development Bank.

Supply Chain (BPMSD, OAS, OSFMD)

A. Purpose

1. The Supply Chain component refers to entities engaged in the delivery of services and products including outsourcing and offshoring that are not under ADB's direct management and control. With some of ADB's processes being outsourced and its supply chains becoming increasingly complex and extended, ADB is exposed to new and additional risk of supply chain interruption. Therefore, to ensure continuous operation, organizational resilience is extended to ADB's supply chains.

2. The purpose of the Supply Chain component is to coordinate the roles and actions of external resources such as consultants, contractors and vendors to mitigate adverse outcomes of a business disruption. Effective supply chain partnership and management during a business disruption creates value and protects brand and reputation.

B. Involved Departments and Offices

3. The Office in Administrative Services (OAS) will lead the development of this component in relation to service providers, contractors, contract management and insurance related activities.

4. The Operations Services and Financial Management Department (OSFMD) will co-lead the development of this component in relation to consultant management and other activities such as planning, monitoring, and coordinating project processing and administration work programs, procurement reviews, and consultant recruitment related guidance.

5. The Budget, Personnel, and Management Systems Department (BPMSD) will provide advice and support on the provision of budget requirements and development of training and awareness programs.

6. All departments and offices will identify their essential third party resources and ensure business continuity arrangements are in place.

C. Scope

7. Supply Chain covers the following aspects:

(i) vendor relations and management
(ii) contractor and supplier management
(iii) support of work programs and projects
(iv) insurance management

D. Core Focus

8. In the immediate and short-term, the component will focus on the following areas:

(i) strengthening relationships and capabilities with external resources,
(ii) addressing weaknesses in the system,
(iii) providing support for existing consultant needs and projects, and

(iv) reviewing and establishing robust insurance strategies and ensuring coverage programs are in place for disruptive events.

E. Key Action Items

9. Departments and offices involved will assess the current capabilities and develop methods to enhance relationships across the supply chain. Best practices will be adopted to manage disruptive events throughout the supply chain.

10. Based on the high level implementation plan, a detailed action plan has been developed by the lead department or office. The succeeding table lists the action items to align this component to the overall organizational resilience initiative.

Table A14.1: Action Plan for the Supply Chain Component

Focus Area(s)

- To engage ADB's third party partners—service providers, consultants, counterparties, etc.— in the planning, information sharing, and establishing redundancies within the supply chain.

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
A.	**Short-term Actions (0-2 years)**			
1	Design supply chain to be redundant	OAS, OSFMD	Q2 2016	Q4 2019
2	Ensure that business processes of key service providers are clearly documented so that multiple staff can perform these processes	OAS	Q2 2016	Q4 2019
3	Involve external parties in the development and/or review of policies, contracts and Service Level Agreements to support the organizational resilience framework	OAS	Q2 2016	Q4 2019
4	Involve external parties in the development and review of the crisis management plans	OAS	Q2 2016	Q1 2017
5	Survey critical vendors to determine if they have business continuity plans in place	OAS	Q3 2016	Q4 2017
6	Perform a supply chain impact analysis and develop a detailed project plan to address identified gaps. Seek endorsement from Business Continuity Management Steering Group and/or Management, as applicable	OAS, OIST	Q3 2016	Q4 2017
7	Conduct an insurance coverage review for alignment with 2015 business impact analysis and risk assessment, and the organizational resilience framework and propose improvement opportunities	OAS	Q3 2016	Q4 2016
8	Implement changes in the insurance coverage, as applicable	OAS	Q1 2017	Q4 2018
9	Implement changes necessary to meet the requirements identified in the 2015 business impact analysis and risk assessment in consideration of the risk appetite and cost-benefit analysis	OAS, OIST	Q1 2017	Q2 2017
10	Implement organizational resilience training and awareness for all ADB staff and service providers	OAS, BPMSD	Q2 2017	Q4 2017
B.	**Medium-term Actions (0-5 years)**			
11	Engage external parties in planning, sharing of information, and establishing service level agreements during a business disruption	OAS, OSFMD, OGC	Q1 2017	Q4 2021
12	If applicable, consider decentralized or dispersed business functions of potential service	OAS	Q1 2017	Q4 2019

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
	providers in the selection criteria			
13	Engage service providers to document operational procedures and work instructions including manual workarounds	OAS	Q1 2017	Continuing activity
14	Engage service providers to strengthen guides, procedures, and arrangements on document retention and disposal and protection of active hard copy documents	OAS	Q1 2017	Continuing activity
15	Promote electronic document submission and processing	OAS	Q1 2017	Continuing activity
16	Involve or include service providers in business continuity and IT disaster recovery testing activities	OAS, OIST	Q3 2017	Continuing activity
17	Encourage service providers to attend organizational resilience awareness and education training	OAS	Q1 2018	Continuing activity

BPMSD = Budget, Personnel, and Management Systems Department, IT = information technology, OAS = Office of Administrative Services, OGC = Office of the General Counsel, OIST = Office of Information Systems and Technology, OSFMD = Operations Services and Financial Management Department.

Source: Asian Development Bank.

Compliance (OGC)

A. Purpose

1. The Compliance component refers to ADB's adherence to legal and other internal and external requirements to which it subscribes and maintaining adequate compliance throughout a disruption.

B. Involved Departments

2. The Office of the Auditor General (OAG) will continue to provide audit and advisory service on the organizational resilience implementation but the approach and review will depend on the risks attached to the organizational resilience framework implementation.

3. The Office of the General Counsel (OGC) will provide advice and support on legal and regulatory related issues.

4. All departments and offices will identify applicable legal requirements and other internal and external requirements that relate to the continuity of their processes and their interested parties.

C. Scope

5. Compliance covers the following aspects:

(i) audit and compliance to the requirements of the organizational resilience framework.
(ii) compliance of the organizational resilience planning and development of crisis management structure, plan development, training and exercising programs.
(iii) legal, regulatory, and communication content and guidance on all communications by Management before, during and after a crisis.
(iv) compliance and guidance on reputation management issues and communications with key stakeholders.

D. Core Focus

6. In the immediate and short-term, the component will focus on providing legal guidance and exposure management to departments and offices related to the organizational resilience framework implementation.

E. Key Action Items

7. Based on the high level implementation plan, a detailed action plan has been developed by the lead department or office. The succeeding table lists the action items to align this component to the overall organizational resilience initiative.

Table A15.1: Action Plan for the Compliance Component[1]

Focus Area(s)

- To provide legal guidance and exposure management to departments and offices related to the organizational resilience framework implementation

Item	Actions	Responsible Unit(s)	Start Date	Target Completion Date
A.	**Short term Actions (0-2 years)**			
1	Assess ADB staff awareness level as baseline information for developing training and awareness programs	OAS, BPMSD	Q3 2016	Q2 2017
2	Priority review of all contracts or legal documents in the immediate actions category	OGC	Q3 2016	Q4 2017
3	Review of force majeure and material adverse change clauses in existing contracts	OGC	Q3 2016	Q4 2017
4	Nominate a representative to the crisis management structure	OGC	Q3 2016	Q4 2016
5	Identify legal, regulatory and other requirements related to ADB's conduct of business that may be significant in times of business disruption	OGC, ORM, TD, CTL	Q3 2016	Q2 2017
6	Develop a business continuity plan to ensure availability of support/process during a business disruption (e.g., involvement in new global bond issuances)	OGC	Q4 2016	Q4 2017
B.	**Medium-term Actions (0-5 Years)**			
7	Engage external parties in planning, sharing of information and establishing service level agreements during a business disruption	OGC, OAS, OSFMD	Q1 2017	Q4 2021
8	Participate in business continuity and IT disaster recovery testing activities, as necessary	OGC	Q1 2017	Continuing activity
9	Participate in the organizational resilience awareness and education training	OGC	Q2 2017	Continuing activity

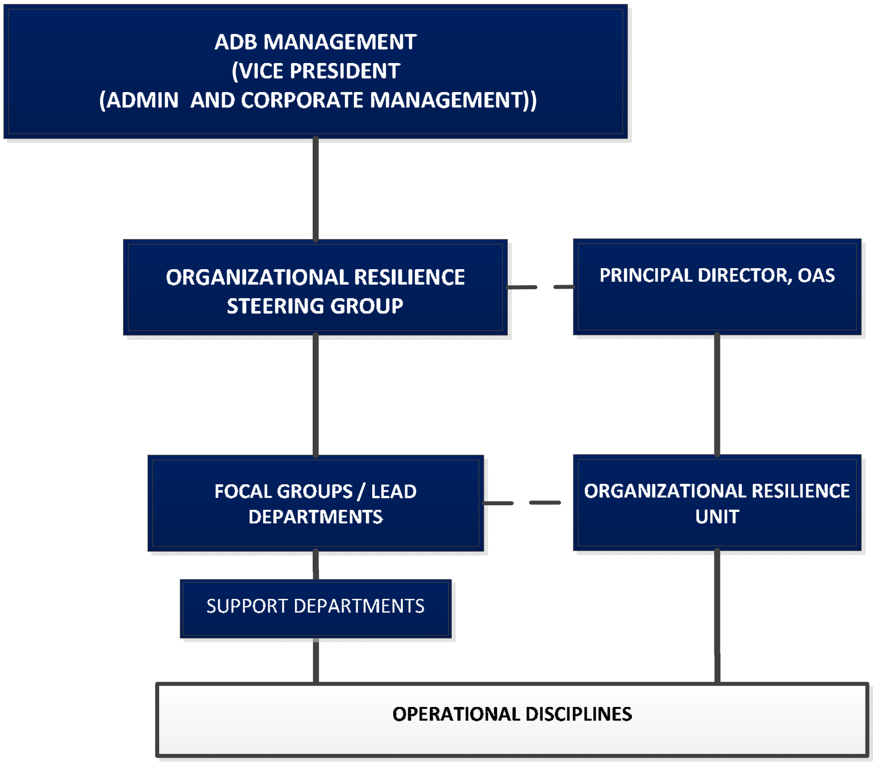
BPMSD = Budget, Personnel, and Management Systems Department, CTL = Controller's Department, IT = information technology, OAS = Office of Administrative Services, ORM = Office of Risk Management, OSFMD = Operations Services and Financial Management Department.

Source: Asian Development Bank.

[1] OAG will continue to audit and provide advisory service to OR implementation.

Governance and Organizational Structure for ADB Organizational Resilience

Figure A16.1: Organizational Chart


ADB MANAGEMENT
(VICE PRESIDENT
(ADMIN AND CORPORATE MANAGEMENT))
ORGANIZATIONAL RESILIENCE STEERING GROUP
PRINCIPAL DIRECTOR, OAS
FOCAL GROUPS / LEAD DEPARTMENTS
ORGANIZATIONAL RESILIENCE UNIT
SUPPORT DEPARTMENTS
OPERATIONAL DISCIPLINES

Source: Asian Development Bank

1. Recognizing the strategic significance of organizational resilience, the role of ADB Management is to set the priority and broad direction and commit the necessary resources for the delivery of the organizational resilience framework.

2. The Vice President (Administration and Corporate Management) (VPAC) is delegated with the authority to provide leadership and guidance in achieving an appropriate level of resilience for ADB. VPAC is the primary sponsor of the initiative from the management level.

3. The Organizational Resilience Steering Group (OR-SG) is chaired by VPAC and consists of Heads of Departments and Offices. The steering group has a key role in leading ADB towards increased resilience. Its main priority functions will be to provide oversight and guidance and to monitor the implementation of the framework.

4. Principal Director, Office of Administrative Services (PD, OAS) is responsible for the overall implementation of the initiative at the operational level. PD, OAS is a core member of the OR-SG.

5. A dedicated Organizational Resilience Unit in OAS (OAOR) has been created. Its main task is to lead the transition of ADB from business continuity to an organizational resilience model and institutionalize and mainstream the concept of organizational resilience throughout ADB, embedding it into the culture of the organization and ensuring the organizational resilience principles are adopted into ADB's operations and business processes.

6. Focal groups and lead departments are responsible for integrating and aligning assigned components to the framework by developing and implementing action plans to ensure each component contributes to enhancing ADB's resilience. Other departments will provide the necessary expertise, support and cooperation in meeting the initiative's objectives.

7. Where applicable, an organizational structure to oversee a specific framework component is established with defined roles and responsibilities. For example, the organizational structure for the business continuity and crisis management component of the framework is governed by OAS as the lead department. The performance of these components in relation to enhancing organizational resilience will flow back to the governance structure. Similarly, guidance to further improve resilience will flow from the governance structure to the framework components through the OR-SG.

ADB Organizational Resilience Framework Implementation Plan

A. Immediate Actions

1. The inadequacy of the current business continuity capability combined with the time required to implement the organizational resilience framework leaves ADB vulnerable to unexpected or unpredictable events that may severely disrupt its operation. Prior to the full implementation of the organizational resilience framework, immediate actions will be taken beginning January 2016 to provide an enhanced business continuity capability and protection for the key financial processes of Controller's Department (CTL), Office of Risk Management (ORM), and Treasury Department (TD) as identified by the recent business impact analysis and risk assessment. These actions should provide a level of protection in the event of a disruptive event where ADB headquarters systems fail and the building is inaccessible but some staff remains safe and able to resume essential processes remotely or at an alternate office, not limited to the offshore data center or recovery site.

2. The objective is to resume key financial operations within several hours[1] and survive the disruption past the seven days regardless of the length of disruption. It intends to provide the capability to maintain minimum processing of transactions throughout a disruption until such a time as operations return to normal. It will allow staff from the headquarters and field offices to access the system from anywhere at any time. Borrowers, executing agencies, and consultants will be able to continue submitting claims.

3. Key components of the immediate actions are as follows:

(i) refining departments' business continuity priorities and objectives based on the risk appetite and cost-benefit analysis,
(ii) establishing an offshore warm data center,
(iii) establishing a data link between the headquarters and the offshore site to replicate critical financial systems online,
(iv) maintaining the offshore site operation through outsourced managed services or outposted staff,
(v) regular offsiting of tape backup of nonfinancial systems,
(vi) implementing cloud storage or equivalent solution for document backups,
(vii) strengthening headquarters building and facilities to support key business processes during a prolonged calamity,
(viii) building capacity on the use of remote access, formal cross-training and awareness programs,
(ix) strengthening third party arrangements through contracts or service level agreements,
(x) providing information technology and communication equipment including internet connectivity tokens to staff of CTL, ORM, and TD,
(xi) preparing a holding statement on business continuity, targeted at internal and external stakeholders, and
(xii) maintaining the in-country business continuity facility as backup workspace in the event of a prolonged disruption.

[1] Current IT disaster recovery capability recovers critical IT systems in 24-48 hours. The proposed interim solution will be able to reduce IT system recovery from 2 days to several hours.

B. Timelines and Responsibility

4. Figure A17.1 illustrates the transition towards resilience in ADB's operations in the event of a disruption. Table A17.1 lists the action items and the estimated timelines for completing them. It also identifies the lead and support departments and offices responsible for executing the actions. More details of the action items will be prepared during the project management stage.

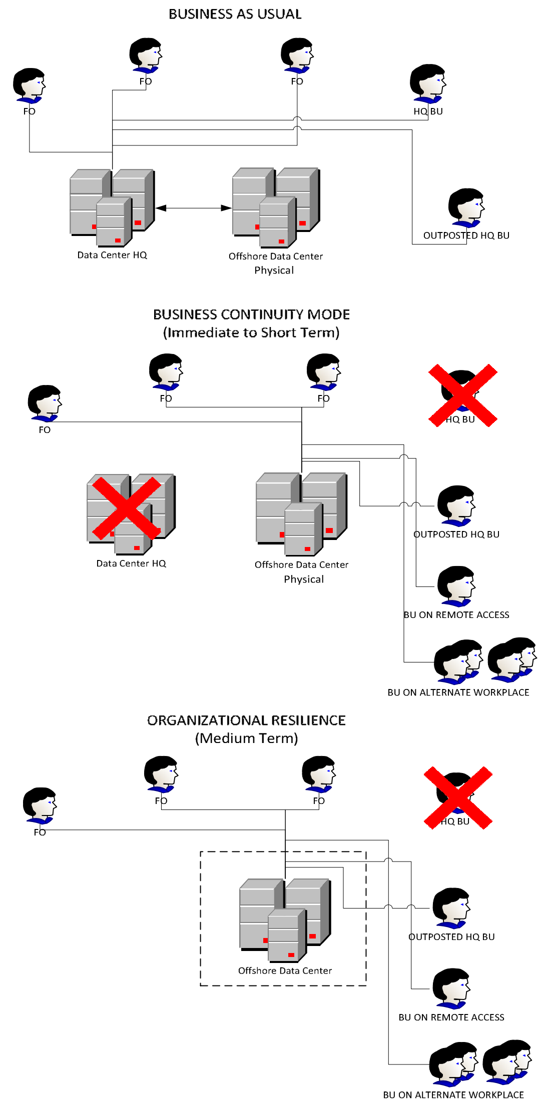
C. Budget

5. A number of proposed actions have budget requirements. The initial estimation of special capital and administrative expense budget is to be presented to the Board for approval (or for information). Some requirements may be covered through reprioritization and reallocation of approved annual budget across and with departments involved in this initiative. The possibility of additional budget, as required, will be further explored. Prioritization of the planned actions may be needed in line with budget availability.

D. Monitoring of the Implementation Process

6. The OR Steering Group will provide guidance and oversight of the implementation. The Head, Organizational Resilience Unit or designated staff will be responsible for the overall coordination and monitoring of the Implementation Plan and for communication within the organization. The Head will also be responsible for periodic reporting to ADB Management and the Board on the progress of the implementation. The OR Focal Group and Lead departments will work with the Organizational Resilience Unit to follow up on the implementation of action items for their assigned framework components. Any changes will be endorsed by OR Steering Group for management approval.

Figure A17.1: Organizational Resilience Concept during a Disruption


BUSINESS AS USUAL
FO
FO
FO
HQ BU
Data Center HQ
Offshore Data Center Physical
OUTPOSTED HQ BU
BUSINESS CONTINUITY MODE (Immediate to Short Term)
FO
FO
FO
HQ BU
Data Center HQ
Offshore Data Center Physical
OUTPOSTED HQ BU
BU ON REMOTE ACCESS
BU ON ALTERNATE WORKPLACE
ORGANIZATIONAL RESILIENCE (Medium Term)
FO
FO
FO
HQ BU
Offshore Data Center
OUTPOSTED HQ BU
BU ON REMOTE ACCESS
BU ON ALTERNATE WORKPLACE

- In the immediate to short-term, ADB will operate a warm offshore data center with online data replication of critical financial systems. During normal operations, IT systems and data are accessible by headquarters and field offices through a secured network. However, if the data center at the headquarters is offline, data processing will switch to the offshore data center and majority of the business units at the headquarters will be disconnected from the network.
- Since some staff of CTL and TD will be outposted outside of the Philippines, this will ensure faster resumption of financial processes with minimal data loss. The outposted staff will take over the headquarters workload which is primarily continuing processing of financial transactions for more than a week.
- If public telecommunication systems are available, other business units at the headquarters can support the unaffected processes by remote access. This will allow sustained continuity of processes for the next 2–3 weeks.
- To ensure continuity for more than a month, standby workplace arrangements will be in place. The temporary workplace will have a seating capacity of at least 300 staff. The remaining headquarters population will remain working from home.
- Additional workspaces will be in place on an ad hoc basis. There will be at least a month lead time to set up temporary workspaces until the entire headquarters business processes are resumed.
- In the medium- to long-term, ADB will operate on an IT infrastructure that will allow access to systems from anywhere, anytime. This can be achieved by operating a physical data center outside the Philippines, employing virtual data centers or cloud.
- Long-term staffing strategy for CTL, ORM, and TD will be implemented. OSFMD, PSOD, and RDs (through the field offices) will have business functions outside the Philippines. Unaffected staff can access IT systems and data from anywhere at any time. Residual risk on staff concentration will be significantly reduced.

ADB = Asian Development Bank, BU = business unit, CTL = Controller's Department, HQ = headquarters, IT= information technology, ORM = Office of Risk Management, OSFMD = Operations Services and Financial Management Department, PSOD = Private Sector Operations Department, TD = Treasury Department.

Source: ADB.

Table A17.1: Organizational Resilience Framework Implementation Plan Action Items

Actions	Responsible Unit(s)	Indicative Time Frame[a]	Status
A. Short term Actions			
1. Policies and Governance			
1.1 Establish organizational resilience governance structure and functional unit	OAS, BPMSD	March 2016	Completed.
1.2 Approval of Administrative Orders and Policy Statements for business continuity, crisis management, and emergency response	OAS	March 2017	
1.3 Review, update, and implement crisis management structure and procedures	OAS, BPMSD	March 2017	
2. Premises			
2.1 Assess building and facilities' capability of ADB headquarters to support business process in the event of disruption and identify improvement areas with budget requirements indicated	OAS	September 2016	
2.2 Design workplace recovery arrangements to accommodate additional staff seating, including provision for information technology (IT) equipment and connectivity	OAS, OIST	June 2017	
2.3 Reassess the purpose of the in-country business continuity facility	OAS, OIST	June 2017	
2.4 Setup of offices for outposted staff and/or expand selected field offices	OAS, OIST	June 2017	
3. Information Technology and Data			
3.1 Design a more permanent IT disaster recovery infrastructure suitable for ADB	OIST	December 2016	
3.2 Include operational departments, OCO, OSFMD, and OGC in the backup and IT disaster recovery procedures	OIST	June 2017	
3.3 Provision of IT and communication equipment for key staff in the operations departments	OIST	December 2018	
3.4 Develop and implement off siting schedule for nonfinancial system in tape backup	OIST	December 2018	
4. People			
4.1 Develop detailed organizational resilience communication plan including organizational resilience related training	OAS, BPMSD, DER	September 2016	
4.2 Engage operations departments on the feasibility of decentralizing and/or delegating function to the field offices in line with the Midterm Review Action Plans	OAS	June 2017	

[a] The indicative time frame is presented either as (a) month/year for those actions that have to be done one time, or (b) effectivity month/year, for those actions that will be of continuing nature and will start in certain months.

Actions	Responsible Unit(s)	Indicative Time Frame[a]	Status
4.3 Design long term staffing strategy (local hiring or outposting, offshore offices, etc.) for CTL, ORM, TD, and OIST based on business units requirements	BPMSD	December 2018	
4.4 Design of a comprehensive welfare preparedness program	BPMSD, OAS	December 2018	
5. Processes			
5.1 Develop business continuity plans for the operations departments, OCO, OSFMD, and OGC	OCO, OGC, OSFMD, PSOD, RDs	December 2017	
5.2 Engage departments on further rationalizing and digitizing processes and use of standard software platforms	OAS, CTL, ORM, OSFMD, PSOD, RDs, TD	December 2018	
6. Supply Chain			
6.1 Review and update of third party contracts to include provisions in the event of a disruption	OAS, OGC, OIST, OSFMD	December 2019	
6.2 Engage third party partners in establishing redundancies within the supply chain	OAS	December 2019	
B. Medium term Actions			
1. Premises			
1.1 Implement workplace recovery arrangements may include procurement of services	OAS	September 2017	
1.2 Implement identified solutions to fortify headquarters building against prolonged disruptions with improved safe haven provisions for affected personnel	OAS, OIST	March 2019	
2. Information Technology and Data			
2.1 Implement and commission improvements and agreed IT and IT disaster recovery infrastructure	OIST	December 2018	
2.2 Complete the provision of emergency IT and communication equipment to key staff of concerned department	OIST, OAS	December 2020	
3. People			
3.1 Deliver mandatory organizational resilience general awareness training ADB wide including field offices	BPMSD, OAS	December 2018	
3.2 Implement long-term staffing strategy (local hiring or outposting, offshore offices, etc.)	BPMSD	December 2020	
3.3 Review, improve, as necessary, and implement staff welfare programs in the event of a disruption	BPMSD	December 2021	

Actions	Responsible Unit(s)	Indicative Time Frame[a]	Status
4. Processes			
4.1 Develop business continuity plans for the rest of the headquarters departments and offices	All departments and offices	December 2018	
4.2 Conduct business impact analysis and risk assessment for fields offices and develop business continuity plans aligned with the organizational resilience framework	All field offices	December 2021	
4.3 Implement action plans related to process rationalization and digitization	CTL, OAS, ORM, OSFMD, PSOD, RDs, TD	December 2021	
5. Supply Chain			
5.1 Engage third party partners in planning and information sharing related to enhancing organizational resilience further	OAS, OIST, OSFMD	December 2021	
C. Monitoring Phase			
1. Ongoing information dissemination and training and awareness for critical staff, business continuity teams 2. Testing, review and update of business continuity arrangements 3. Periodic reporting to Management and the Board on the organizational resilience framework 4. Sharing experiences with developing member countries (DMCs)			

BPMSD = Budget, Personnel, and Management Systems Department, CTL = Controller's Department, DER = Department of External Relations, OAS = Office of Administrative Services, OCO = Office of Cofinancing Operations, OIST = Office of Information Systems and Technology, ORM = Office of Risk Management, OSFMD = Operations Services and Financial Management Department, PSOD = Private Sector Operations Department, RD = Regional Departments, TD = Treasury Department.

Source: Asian Development Bank.

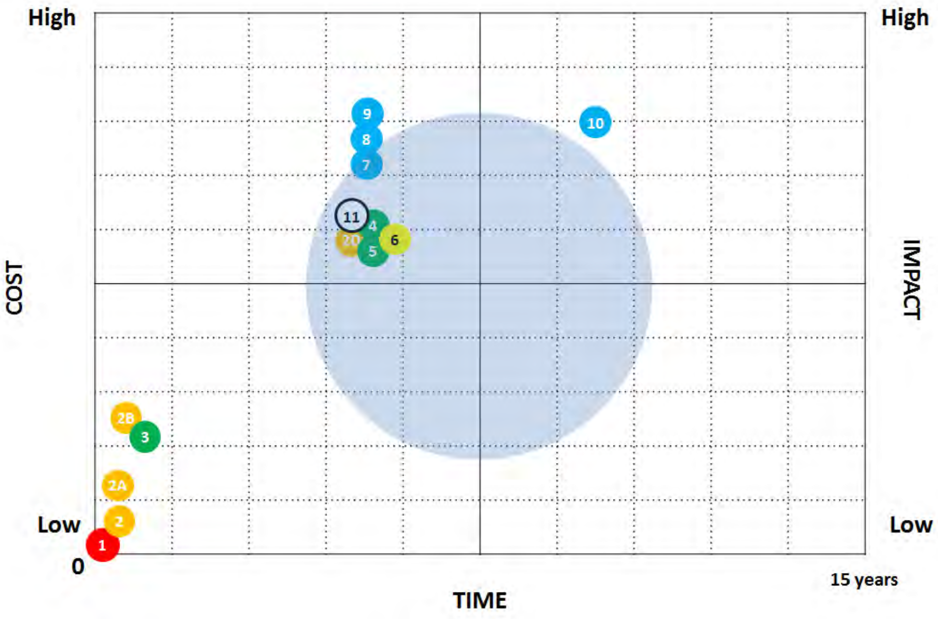
Initial Analysis of Alternatives and Options for Achieving Organizational Resilience

1. In 2015, an organizational resilience expert was engaged to provide technical advice and support to the Business Continuity Management Steering Group in developing this framework. Part of the project deliverable is the identification of options or alternatives in achieving a desired level of resilience and the corresponding the advantages and disadvantages in implementing these options. The options listed in Table A18.1 can be broadly categorized as follows:

(i) do nothing or status quo,
(ii) utilize existing capability of or enhance the in-country Business Continuity Facility,
(iii) utilize existing field offices to set up a data center and/or to decentralize business processes,
(iv) establish an offshore data center and/or offices not in a resident office, and
(v) outsource the management of ADB's data center.

2. The options were assessed based on the level of resilience that can be achieved against the time and cost to implement them as illustrated in Figure A18.1.

Figure A18.1: Analysis of Alternatives and Options for Achieving Organizational Resilience



Source: Asian Development Bank.

3. Locating the data center in a field office (option 4) or in any Asia-Pacific country (option 5), outsourcing the data center operations (options 6), upgrading the existing in-country facility (option 2d) and establishing a business hub outside the Asia-Pacific region (option 11) were found to be viable solutions that may potentially increase ADB headquarters' resilience against a major disruption with reasonable time and cost to implement. This initial analysis became one of the bases in formulating the framework's action plans.

Table A18.1: Working List of Alternatives and Options for Achieving Organizational Resilience

Option	Description	Estimated Time to Implement	Estimated Cost Implications	Transformation Impact on ADB's Resilience
1	Status Quo. Retain the existing in-country warm BCF and leased offshore cold site	Immediate	None	None
2	Utilize the existing capabilities of the in-country BCF. This could also include conducting regular business operations that are less time sensitive	Immediate	Low	Low
2A	Utilize the existing capabilities of the in-country BCF by positioning staff of priority business processes on a business as usual basis	Immediate	Low	Low to moderate
2B	Enhance the capabilities (i.e. additional office spaces) of the existing in-country BCF	Immediately	Low to moderate	Low to moderate
2C	Upgrade the technical capabilities of the existing in-country BCF to approach an active-active environment between the data centers at headquarters and BCF	Immediate	Low to moderate	Low to moderate
2D	Upgrade the capabilities of the existing in-country BCF, including increasing seating capacity, and distribute business areas including those that are not time sensitive and production data dependent (e.g. IT application development, production system backup)	Short to moderate	Moderate to high	Moderate to high
3	Distribute business operations to existing ADB field offices with available workspaces.	Immediate to short	Low to moderate	Low to Moderate
4	Establish production data center operations in an existing ADB field office	Moderate	Moderate to High	Moderate to high
5	Establish a new production data center facility in an existing and appropriate DMC and then move regional or country offices operations to this same location.	Moderate	Moderate to High	Moderate to high
6	Expand existing relationships with third party providers to support the BCM program and the organizational resilience strategy	Moderate	Moderate to High	Moderate to high
7	Establish a new ADB managed offshore facility, including an operational production data processing capability and operational business unit work areas.	Short to Moderate	Moderate to High	Moderate to high
8	Setup an ADB managed offshore replicated data center only. This can be a leased or owned facility. This would be an Active-Passive design where the currency of data is behind the primary active data center. Workspaces can be available through existing field offices.	Short to Moderate	Moderate to High	Moderate to high
9	Setup an ADB managed offshore data center and implement cloud architecture for data replication. Access to the data center is through remote access	Short to Moderate	Moderate to High	Moderate to high
10	Establish ADB managed multiple load balanced production data center with automatic failover systems in several locations within and outside the Asia-Pacific Region	Moderate to Long	High	High
11	Open a financial business focused office in a major financial location outside of Asia	Short to Moderate	Moderate to High	Moderate to high

Legend:

🟥 Status Quo

🟧 Options to use the BCF

🟩 Options to use an ADB field office

🟨 Option to outsource

🟦 Options to establish a new recovery site or data center in the Asia-Pacific region

⬜ Option to establish a new office outside Asia

BCF = business continuity facility, BCM = business continuity management, DMC = developing member countries, IT = information technology

Source: Asian Development Bank