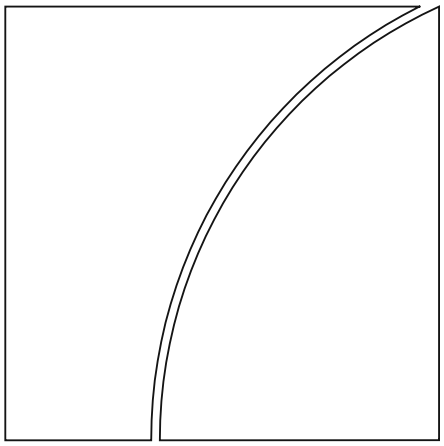
Consultative Group on Risk Management



Business continuity planning at central banks during and after the pandemic

April 2022

BIS Representative Office for the Americas

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-548-7 (online)

Contents

Foreword

This report, Business continuity planning during and after the pandemic, is the outcome of work conducted by BIS member central banks in the Americas within the recently established Consultative Group on Risk Management (CGRM).

The CGRM was launched in March 2021 to meet the demand by BIS member central banks in the Americas for greater cooperation in the area of central bank risk management, recognising the rapid shifts taking place in the risk landscape. These shifts include the intensification of cyber threats, rapidly evolving technology, growing reliance on third-party service providers and changes in central bank operations due to the Covid-19 pandemic.

The CGRM conducts its activities under the auspices of the Consultative Council for the Americas (CCA), an advisory body that comprises the Governors of BIS member central banks in the Americas. It meets regularly to discuss risk management issues and execute projects of common interest to strengthen risk management. One such project is the review of approaches to business continuity planning in light of the lessons learnt from central bank responses to the Covid-19 pandemic. To conduct this review, the CGRM created a task force led by Claudia Álvarez Toca from the Bank of Mexico. This report marks the successful completion of this project and is published for the benefit of the wider central bank community and the public.

Joshua Rosenberg

Chair, CGRM, Federal Reserve Bank of New York

Alexandre Tombini

BIS Chief Representative for the Americas

Executive summary

Business continuity planning (BCP) is the process that allows organisations to continue operating during a disruption, ensuring the protection of their processes, assets and human resources. BCP is a critical component of operational resilience, which is defined as the capacity of any institution to prevent, respond, adapt, recover and learn from any type of disruptive event.

Before the Covid-19 pandemic, institutions had been exposed to a variety of risks. The strategies they have developed to mitigate these risks have allowed them to successfully cope with various scenarios, including the unavailability of personnel and/or facilities as well as information technology failures, among others. The pandemic posed a severe real-world stress test for BCP at central banks. The strategies designed prior to the pandemic helped institutions to rapidly find new ways to perform their operations. Yet, the pandemic has also brought about new risk scenarios related to increased strain on resources and working from home, prompting central banks to adapt their BCP strategies. As a result, the adaptation of BCP strategies must include changes in the work environment in order to further strengthen operational resilience.

In August 2021 the Consultative Group on Risk Management (CGRM) set up a task force to examine the experiences of BIS member central banks in the Americas[1] during the Covid-19 pandemic. This report is the outcome of the work of the task force and describes changes in the business continuity frameworks that took place at participating institutions after the beginning of the pandemic. Its findings might help central banks in the region and beyond to adjust their BCP to the new risks that emerged from the pandemic and the new ways of working that might outlive the pandemic.[2]

Business continuity planning during the pandemic

Following the eruption of the pandemic, organisations have identified, or are in the process of identifying, key actions that will allow them to strengthen their operational continuity strategies and incorporate mechanisms to develop their operational resilience in a holistic way.

To this end, some members of the task force are considering adopting different time frames (eg immediate, short, medium and long term) in their operational continuity strategies, depending on the results of their business impact analysis (BIA) and the needs and resources of each institution. The operational continuity strategies must consider the new ways of working that have been implemented and the new risks that arose in this context, such as failures in the technological infrastructure for remote connection and other infrastructure that allows personnel to work from home. These strategies should be sufficiently flexible to easily adapt to unforeseen situations. Another relevant aspect is to consider key external dependencies in BCP. In addition, the implementation of schemes for flexible roles is important so that designated roles can be changed and adapted depending on the scenario or contingency that the institution faces.

Communication is one of the main factors underlying the success of operational continuity strategies. Hence, some organisations are considering the implementation of alert schemes and automated communication tools to inform their staff of the status of events that have the potential to cause an operational interruption. Similarly important is the application of drills, training and permanent

[1] BIS-member central banks in the Americas are listed in Annex 2. Governors of the central banks are members of the Consultative Council for the Americas (CCA), to which the Consultative Group on Risk Management (CGRM) reports.

[2] Useful references for BCP implementation include: Basel Committee on Banking Supervisions, *High-level principles for business continuity*, 2006, www.bis.org/publ/joint17.pdf, International Organization for Standardization, *ISO 22300:2021 Security and resilience – vocabulary*, 2021, www.iso.org/standard/77008.html.

monitoring of operational continuity strategies that allow for continuous improvement and boosting resilience.

New work schemes and "the future of work"

The report also reviews the work schemes that might define "the future of work", discussing the challenges that they entail for critical activities, meetings and the technological infrastructure, among others.

Following the pandemic most organisations have already changed the way they operate and will continue to shape their future working environment. Institutions currently lean toward adopting hybrid work schemes whereby staff will alternate between working at the institution's facilities and working from home. That said, in some organisations, some staff will not be entitled to hybrid working owing to the nature of their activities. Furthermore, whether staff will be considered for a hybrid work scheme will also depend on security policies, as well as the level of maturity of the security controls in place or being implemented for working from home.

A number of factors are highlighted in the report.

The first is the reliability and security of information technology services. These have ensured that operations could continue to be conducted remotely during the pandemic and will remain a critical factor behind the successful implementation of the hybrid working scheme. It is of the utmost importance to monitor and strengthen the IT infrastructure against cyber attacks and loss of information, among other threats. Additionally, it will be necessary to continue to carry out or strengthen the digitalisation of activities regarding the execution of processes, as well as to adapt or create guidelines for the use of electronic signatures.

The second is the potential for additional costs. Some institutions are considering schemes that limit the amount of time staff can work from home to avoid additional expenses such as covering the costs of internet or electricity services incurred by their staff when working from home. In some cases, covering such costs is a legal obligation (eg when staff work from home more than 40% of their time). Other organisations are, instead, considering a one-off grant to their staff to cover part of the cost of setting up their home offices.

The third factor is the preparedness of employees and their families. The ability of staff to work from home directly depends on how well they are prepared to address hazards at home (power/internet outages, safety amidst protest activity, etc).

Finally, for some organisations, working from home schemes open up the possibility to have staff working remotely from a location other than the city where the institution's headquarters or branches are located (including the possibility of staff being located outside the country, provided the institution's security policies are met).

Return to on-site operations

The report also highlights the importance of having a transition plan in place for staff to return to work in the office as well as embracing the new work schemes. Several issues are relevant for a successful transition. Given the priority placed on the health of their staff, all central banks have decided on a gradual return to their facilities, the speed and modalities of which depend on the evolution of the pandemic (percentage of population vaccinated, number of new cases, occupancy rates in hospitals, to name a few). During this process, all organisations would continue to follow the health measures determined by the health authorities of their respective countries, such as social distancing, use of face masks and limits on the occupation of buildings, among others. Furthermore, given the high degree of uncertainty regarding the evolution of the virus, all organisations have plans for a rollback – ie an immediate return to the

working from home scheme – in case of a significant increase in the number of infections among staff or the general population.

Regarding the vaccination of staff against Covid-19, all institutions follow the regulations or directives of their respective authorities. Some are making the vaccination mandatory for all staff, while others are considering some exceptions (eg on religious or medical grounds).

1. Introduction

Business continuity planning (BCP) is the process aimed at creating a system of prevention and recovery from potential threats. As part of this system, it is important to ensure that all processes, assets and human resources are protected, and that the institution is able to resume its functions quickly following a disruption. BCP is a critical component of operational resilience, which is defined as the ability of organisations to continue serving their clients and meeting expectations even in an abnormally constrained environment.

The pandemic represented a real world stress test for BCP in many institutions, including central banks. The latter have managed to shift the place in which operations are performed – going from executing them in an office to executing them from home – to a much greater extent than most people had anticipated. However, the pandemic has also revealed that many of the assumptions embedded in their BCP were questionable. Many assumptions underlying BCP therefore need to be revisited and new assumptions and scenarios considered.

At its August 2021 meeting, the Consultative Group on Risk Management (CGRM) set up a task force on post-pandemic business continuity planning to examine the experiences of BIS member central banks in the Americas[3] and of the BIS itself during the pandemic. The participating institutions identified the main lessons learned from the pandemic in business continuity planning and analysed how these lessons influence the assumptions behind business continuity plans and resilience arrangements (eg location and IT infrastructure, among others).

As a starting point, the group reviewed how the BCP had been implemented before the pandemic, the business continuity assumptions that proved inadequate during the pandemic and the way central banks reconfigured them. In this regard, the group took into consideration that work schemes are evolving (or will evolve) in order to strengthen operational resilience. They will mainly evolve into hybrid schemes which include both on-site and off-site operations. This reconfiguration of work modalities should be considered in the business continuity framework, along with new risks that have emerged from working from home (eg dependence on the electrical and internet services of personnel) and the strategies to ensure operational continuity in case of a future crisis. Specifically, each member of the task force shared the following aspects of their central bank's business continuity framework:

- time frame;
- identification of critical processes;
- risk scenarios;
- business continuity strategies;
- dependencies on external resources;
- staff roles;
- business continuity coordination and senior leadership;
- alert or warning scheme;
- communication; and
- testing and training.

In addition, each participant explained the challenges faced by their respective institutions in defining "the future of work" or new work schemes. The following issues were covered:

[3] BIS member central banks in the Americas are listed in Annex 2. Governors of the central banks are members of the Consultative Council for the Americas (CCA), to which the Consultative Group on Risk Management reports.

- working from home scope;
- critical activities;
- meetings;
- technological infrastructure;
- facilities;
- legal adjustments;
- expenses; and
- operational adjustments.

Finally, the task force also focused on the transition plan for returning to on-site operations, considering aspects such as:

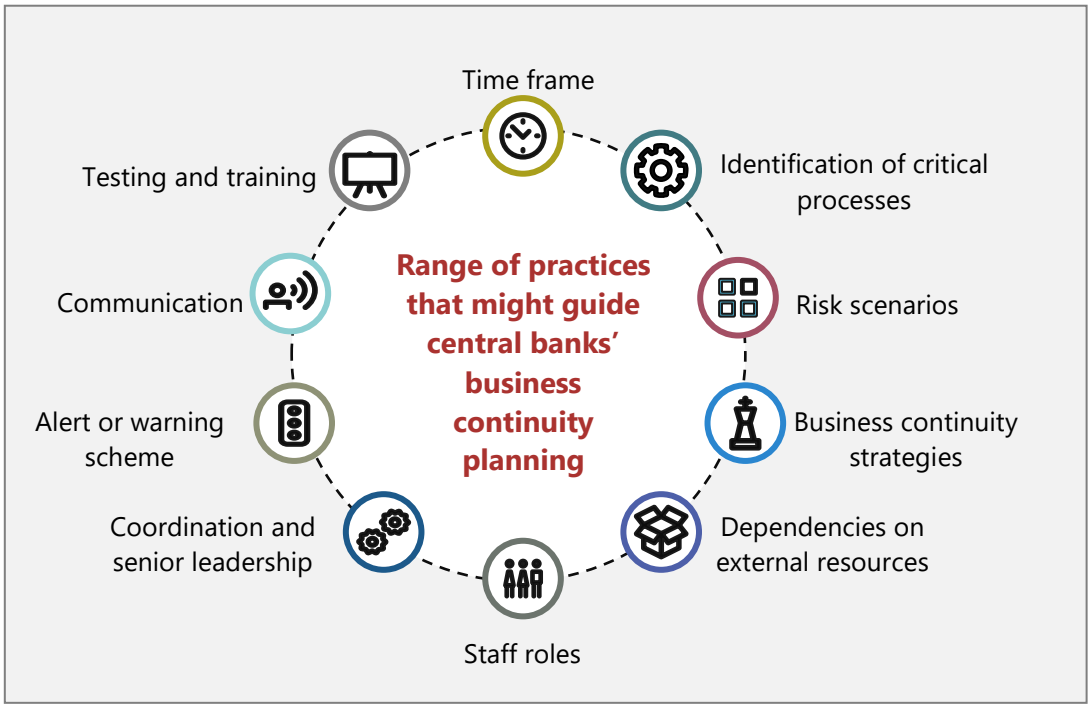
- transition plan (phases);
- eligibility of staff;
- staff organisation;
- trigger to execute the transition plan;
- vaccination policy; and
- rollback plan.

This report provides the information collected by the task force and is intended to guide BCP at central banks and to assist in efforts to identify and address new risk scenarios and gaps that have emerged during the pandemic.

The report is organised as follows. Section 2 describes how BCP is conducted at central banks following the outbreak of the pandemic. Section 3 reviews the new work schemes, including off-site and on-site work as well as hybrid schemes. It also reviews some of the criteria that institutions might follow to adjust their operations to the new reality. Section 4 describes the new risks and challenges to operational continuity due to the pandemic, as well as how these could be addressed. Section 5 highlights some of the issues that institutions might consider implementing as part of the transition plan for returning to on-site operations (planning, staff eligibility, trigger of plan, etc). Section 6 concludes. Annex 1 provides definitions of the main concepts used in the report. Annex 2 lists the members of the task force.

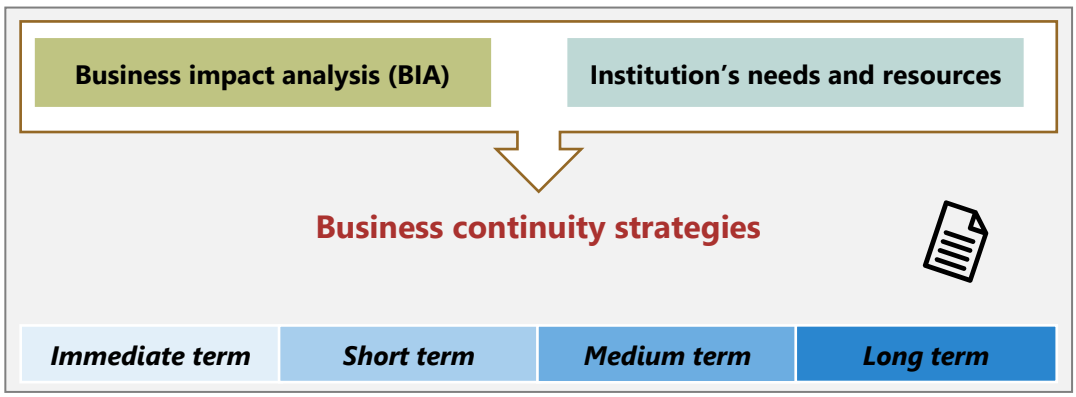
2. Business continuity planning at Consultative Council for the Americas central banks

The pandemic caused unprecedented disruption, prompting rapid change in the operations of all Consultative Council for the Americas (CCA) central banks. This has demonstrated the need to develop business continuity strategies that contribute to the organisation's resilience in the face of short- and long-term disruptions to operations, regardless of the causes. Members of the task force share the experiences of their own institutions with a view to identifying best practices in BCP. These practices are not meant to be standards to be followed. Instead, they should be regarded as general references that could help each organisation to identify those that best suit their needs. Regarding these practices, they considered the following topics:



2.1 Time frames

Before the pandemic, business continuity plans and strategies in most organisations were predicated on interruption periods ranging from a few hours to a week at most. As a result of the pandemic, however, it might be appropriate to develop business continuity strategies for longer lasting scenarios, in addition to short-lived ones. In particular, members of the task force have considered defining multiple time frames (eg immediate, short, medium and long term) for which to develop their continuity plans. These time frames might range from a couple of hours to more than six months.



A common practice to define time frames is based on the results of a business impact analysis (BIA). The BIA allows the identification and categorisation of the criticality of processes and provides valuable information to develop the institution's business continuity plans and strategies. It focuses on process needs and not on the contingency scenario. The BIA methodology should also be used to validate the criticality of any new processes that have been developed to face the pandemic.

Depending on the results of its BIA, operational needs and available resources, each institution may determine different operational continuity strategies for interruptions, considering different time periods. Some examples are the following:

	Immediate term	Short term	Medium term	Long term
Example 1	1 hour to 8 hours	24 hours	5 days	1 month
Example 2	24 hours	1 to 14 days	5 to 12 months	More than a year

2.2 Identification of critical processes

Following the pandemic and considering that this type of event can last for a long time, some institutions might need to redefine the criticality of their processes, bearing in mind that before the pandemic many processes which had not been considered critical may now fall into this category, or may do so eventually. One approach could be to sub-classify processes into those that are critical (ie requiring recovery within short time periods) and those that are semi-critical (ie recovery could occur over longer time periods).

In addition, given the new forms of work implemented during the pandemic, the institutions may establish additional variables in their BIA in order to identify which processes, or specific activities of each process, can be executed remotely and which ones must necessarily be executed on site.

2.3 Risk scenarios

It is evident that in a pandemic scenario the risk of a large number of staff becoming unavailable increases significantly. Apart from that, the new ways of working implemented during the pandemic generate new risks that need to be recognised and aligned in continuity plans.

Among these new risks are technological failures in the infrastructure for remote connections as well as in the infrastructure available in the homes of personnel. Additionally, working off site for extended periods increases exposure to information security risks owing both to less secure practices during remote working and the higher number of cyber attacks observed during the pandemic.

An organisational resilience approach should consider the probability of simultaneous contingencies which may have independent or correlated origins. The challenges faced during a pandemic may be compounded by the occurrence of other events such as earthquakes, terrorism and cyber attacks, among others. The simultaneous occurrence of disruptive events increases with the time frame. Furthermore, the probability of some scenarios such as a power outage, the unavailability of key personnel or cyber attacks occurring may in fact be higher due to circumstances brought about by the pandemic. For these reasons, it is essential that BCP is flexible enough to account not only for any specific scenario but also for any simultaneous combination of them.

2.4 Business continuity strategies

Before the pandemic, the business continuity strategies of most institutions focused on addressing short-term impact scenarios. These would normally require remote access and/or alternate site operations, and were based on the expectation of returning to the same work model which had been in place before the business continuity event. By contrast, since the start of the pandemic, institutions have been analysing the possibility of formulating appropriate, sufficiently flexible and easy to adapt BCP and strategies – these could also be useful for unforeseen situations. Furthermore, as the current pandemic has shown, these plans and strategies require consideration not only of the existence of new risk scenarios, but also the possible restoration of activities in different operational conditions to those existing before the contingency. As such, a review of BCP strategies cannot be conducted without reference to the new ways of working, as most organisations intend to retain working from home as a permanent feature of their arrangements (Box 1).

Box 1

Business continuity strategies allowing the strengthening of operational resilience

Continuity strategies for disruptive events while operating with large-scale teleworking staff:

- Employee internet connectivity – review the need to extend continuity plans to consider employee internet service providers (ISP) to help ensure that critical employees are on different ISPs. Similar planning may also be used for mobile networks as well. For instance, a home office resilience programme that provides an iPhone and UPS battery to all staff involved in the extended incident management team and designated time-critical staff, could be implemented.
- Security considerations – review plans to help ensure working from home (WFH) protocols meet IT and information security policies.
- Tests and exercises – examine the need to test and document critical functions, using online collaboration tools for crisis communications.
- Cross-training – while already a part of the bank's continuity planning, cross-training efforts will need to be coordinated with the current WFH strategy

2.5 External dependencies management

In general, most organisations emphasise the importance of assessing the relevance of managing external dependencies in BCP, including third-party services such as data centres (eg hosting), telecommunications services providers, suppliers of technological inputs, etc.

Based on the experience of the pandemic, some institutions are considering the legal formalisation of agreements and contracts with third parties to ensure adequate provision of critical products and services in case of any operational interruption or contingency that affects the provisions, regardless of the duration of the event.

This strengthening of BCP strategies must consider the fact that some contingencies, such as the current pandemic, can have a significant widespread impact on the availability of services and resources at a national or even international level.[4] That is to say, the contingency may affect not only the institution itself but also a wide range of suppliers of goods and services, as their inventories, transportation channels and means of production are impacted. It is therefore not enough to have clauses or rules established with third parties. BCP should also consider scenarios in which certain critical goods or services will not be available, and establish plans relating to their scarcity or unavailability for long periods.

2.6 Business continuity staff roles

Institutions have defined roles for key or essential staff who are responsible, in the event of an interruption, for ensuring the continuity of processes according to business continuity strategies. Such roles commonly have a backup and alternate staff.

Following their experiences during the pandemic, many organisations are considering the possibility of defining schemes for flexible roles. Some have implemented those schemes in such a way that these roles can be modified and adapted, depending on the scenario or contingency that materialises.

[4] Prior analysis suggested that shocks to vendors, including contingency vendors (such as technology or core business related issues), could only have a low correlation with shocks to central banks. The pandemic has clearly shown that this might not be true in all circumstances.

In any case, it is also advisable to establish a support role – in addition to key and backup roles – for each critical process of the organisation.

Some institutions have procedures or methodologies for defining these roles aimed at ensuring that more than one person knows how to carry out the same activities in case key personnel are unavailable during a contingency (Box 2). That is, a person performing any role, might have to assume different responsibilities and cover for colleagues who are not available to execute their tasks.

Box 2

Business continuity strategies – identification of key roles

Continuity strategies for disruptive events while operating with large-scale teleworking staff:

The identification of key roles might consider:

1. The process and position in which staff participate, considering the criticality of both the process and the position.
2. Replacement cost – considering the estimated time for the backup person to autonomously execute the functions of the position with a key role, as well as the estimated time to get a replacement with the appropriate profile on the internal or external market.
3. Documentation and formalisation of the processes in which he or she participates throughout the process information system.
4. If a replacement with an official document is needed, in case of absence, and if the position has legal representation.
5. Mode in which the position can operate, considering if the functions can be performed remotely, occasionally in person or only in person at the bank's facilities.
6. If the position manages any sensitive assets (eg information, information systems, physical assets).
7. Relevance of the control activities carried out by the position of direct incidence in the process.
8. Ability for rapid problem solving or technical expertise in the activities of the process which are required in the position.

2.7 Business continuity coordination and senior leadership

Institutions have considered several organisational schemes for proper management of BCP. While most of the functions associated with developing and implementing business continuity plans and strategies are carried out – in most organisations – by the risk management area, some organisations have also established interdisciplinary teams. The latter, which include experts from different areas as well as the top management, are in charge of managing contingency or crisis situations, monitoring the event and making timely decisions. In some institutions, these interdisciplinary teams have been particularly active during the pandemic and have also been involved in the development of new business continuity strategies.

2.8 Alerts and warning schemes

Several central banks have implemented alert schemes to inform their staff of the status of an event that is causing, or could cause, an operational interruption. These schemes use different alert levels – for example, indicated by red, orange or yellow – to represent the severity of the actual or potential event.

This in turn depends on the number of processes, people or assets affected, as well as the estimated recovery time.

In some organisations, these alert schemes are implemented using technological tools that allow them to communicate during an operational interruption or contingency, and are associated with their respective communication trees.

Since the start of the pandemic, several organisations have considered updating their alert schemes to make them more flexible and functional for any type of scenario, integrating them, if necessary, into their business continuity strategies.

2.9 Communication

Several organisations have specific communication strategies for use during a contingency based on tools such as call trees. These are complemented with technological tools for notifying staff of a disruptive event rapidly and effectively. For instance, some organisations have specific sites on the intranet which staff can consult to monitor the evolution of the event. In addition, organisations have, in some cases, also provided telephones or satellite communication equipment to key personnel responsible for managing operational continuity.

The pandemic has also led some organisations to improve or adopt communication strategies for crisis management, particularly in the context of high-impact scenarios, such as cyber attacks (arising from remote work and external conditions), earthquakes, etc. These communication strategies may consider the identification of audiences, types of messages and communication channels. They may also consider procedures for the definition, review and publication of information, periods for updating published information, responsibilities, and predefined key formats and messages to react in a timely manner in a crisis situation.

2.10 Testing and training

In general, organisations have a plan in place for the periodic execution of drills to ensure that staff are trained and prepared, and to validate existing business continuity strategies. These drills mainly involve critical processes and key personnel. However, due to the pandemic, some organisations have considered extending these drills to include possibly unprepared/unaware personnel (considering a surprise factor), personnel with a low level of expertise, as well as personnel from areas which do not have a continuity plan in place. Likewise, they have considered it necessary to adjust the drills so that they reflect conditions prevailing in hybrid work schemes (with part of the staff working on site and part remotely).

In addition to drills, several organisations are also considering developing courses for staff, focused on business continuity, operational risks and crisis management.

3. Strengthening operational resilience in the face of new work schemes

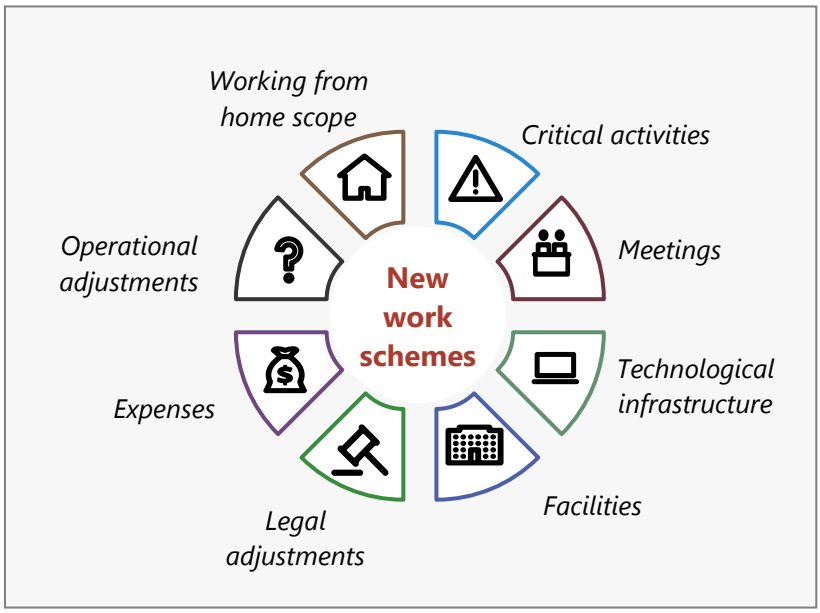
Not only have organisations had to adapt and strengthen their operational continuity strategies during the pandemic, they also had to start thinking about how to adapt them to the new work schemes to boost and strengthen operational resilience.[5] When physical distancing restrictions are no longer a relevant factor, working from home will continue to be an effective work scheme. For this reason, and in response to staff and operational needs, pre-pandemic work schemes involving – in most cases – 100% in-person

[5] Basel Committee on Banking Supervision, *Principles for operational resilience*, March 2021, www.bis.org/bcbs/publ/d516.pdf.

interaction will likely be replaced by hybrid operating schemes. These allow both for working on site and from home. For some activities or specific positions, new work schemes could even involve up to 100% remote work.

Although hybrid work schemes might become permanent features, in practice their details may vary significantly depending on: the institutions' experience and needs, especially for roles concerned with time- and information-sensitive processes; the adaptability and resilience of staff; and the possibility of enhancing and adapting technological tools. As to the latter, ensuring sufficient levels of information security is key.

The task force analysed the impact of these new work schemes based on the factors shown in the image below.



3.1 Working from home scope

As a result of the pandemic, institutions have adopted remote work schemes for the execution of their operations. Once social distancing restrictions are no longer the norm, most institutions will adopt hybrid work schemes, depending on the needs of processes and information security considerations.

In general, all participating institutions expect to establish hybrid work schemes, in which part of the staff alternate between working on site and remotely. For most employees, the proportion of time working on site and remotely is expected to be well balanced (50% each). However, this proportion might vary across jobs according to the nature of the processes involved. Some processes require that they be performed entirely on site (eg due to physical security requirements), while others might be entirely executed remotely, especially those that have functioned adequately and safely during the pandemic.

Hybrid work scheme examples
Three days on site and two days at home on a weekly basis.
50% on site and 50% at home during a two-week period.

In some organisations, some staff members are identified as being unsuitable for a hybrid working scheme, due to the nature of their activities. This is the case when their activities must be executed on site, such as security, general services and cash distribution, to cite a few examples. Additionally, some

processes may have to be executed both on site and off site, in order to preserve a sufficient level of security. For this reason, in defining the scope of work schemes, institutions will have to identify which critical activities will have to be executed at the premises – eg the exchange of highly confidential information.

The balance between on site and remote work will depend not only on the nature of the activities but also on factors such as political decisions and national legislation. For example, some countries have enacted laws that oblige employers to cover part of the expenses which employees incur when working from home.

Another important factor to consider is the impact on organisational culture. Examples of organisational culture include the way of communicating, collaborating, participating and integrating into work teams. Because of its nature, culture needs to be experienced so that it can be properly and more easily transmitted to newcomers joining the organisation. This might be difficult or even impossible without a common physical space where staff can bond and interact in person. The problem is particularly severe for new hires. To address these issues, several organisations are considering implementing fixed days for working on site for all staff and will have to develop strategies to ensure that newly hired employees can absorb and blend into the organisational culture.

In addition, organisations have to adapt their management of human resources practices, in order to effectively monitor the productivity of more dispersed teams, as well as to provide equal opportunities for employees working on site and those working from home.

3.2 Critical activities

Based on the identification of critical activities, some central banks consider that the security controls implemented at their facilities – such as call recording, confined spaces, isolated communication networks, closed circuit television, etc – cannot be applied in a similar way in a home environment. Thus, they have determined that activities that require these types of controls, as well as those that involve managing confidential information, must be performed within the organisation's facilities.

Other central banks indicate that they have adapted some controls for remote working to guarantee a safe working environment, regardless of where the activities are carried out. These controls are considered to be part of stricter security principles known as the "four eyes" (sometimes "six eyes") principles such as the segregation of duties, the principle of least privilege and the application of systematic risk reviews, to name a few.

3.3 Meetings

Once social distancing restrictions are no longer in place, most organisations expect to implement mixed meeting schemes – ie some participants in person and others using virtual means of communication. This would require the adaptation of meeting rooms, for example enabling remote access, installing microphones and cameras, etc. These organisations also consider developing practices or guidelines to minimise the potential disadvantages faced by remote participants such as preventing staff present in the same room from discussing meeting-related issues when remote participants are offline.

Additionally, based on the sensitivity of the information involved, some organisations have determined that meetings involving sensitive information can only be conducted in person at a common safe location. Some institutions have also pointed out that meetings considered to be of strategic importance would be more productive if held in person, but they have refrained from preventing them from being held in hybrid or remote modes.

3.4 Technological infrastructure

Information technology was a major factor that allowed organisations to transfer their operations to a remote work scheme.

As part of the future of work – and taking into consideration the constant cyber attacks that institutions have suffered during this pandemic – central banks are planning to use new security tools or upgrade existing ones to improve information protection, detect threats and prevent data loss. Among these tools are endpoints, network firewalls, web/proxy protection, anti-spam, web application firewall (WAF), hardware security module (HSM), privileged access management (PAM) and data loss prevention (DLP) tools.

To strengthen their remote working schemes, several organisations have provided, or are in the process of providing, portable computer equipment (laptops) to their staff, and to acquire licences for the use of the required communication and coordination tools. Additionally, they are considering adopting two-factor authentication mechanisms as well as monitoring remote connections. Some organisations have even been evaluating the possibility of assigning smartphones to all their staff.

3.5 Facilities

In general, around three quarters of the institutions participating in the task force are considering taking advantage of changes in ways of working brought about by the pandemic to optimise space in their facilities. The options considered include hoteling schemes (sharing and reserving spaces), increased open spaces, non-dedicated desks and modification of the premises to promote teamwork. Some organisations already have docking stations available to provide staff with the flexibility to use their portable computing equipment wherever they need. Also, one institution pointed out that it is exploring the alternative of creating decentralised offices in areas where a significant number of its employees are located, in order to reduce commuting.

3.6 Legal adjustments

A few organisations foresee possible adjustments to labour contracts, depending on the work scheme that will eventually be implemented. This is to comply with the legal framework of their respective countries.

Some institutions also foresee that remote working agreements could specify the expected work deliverables during a given period, how staff will be supervised and their performance measure. Some organisations are even considering including policies that allow their staff to work remotely from a location other than the city where the institution's headquarters or branches are located, or even the possibility of having staff working outside the country as long as they meet security policies.

3.7 Expenses

For two of the participating institutions, the law establishes that employers must provide economic support to their staff if remote work exceeds 40% of their working time over the week. This support normally consists of covering, at least partially, the costs of internet and electricity services and even furniture. For this reason, both organisations have put a cap of 40% on the time that could be spent working from home. By contrast, the rest of the participating institutions are not subject to such legal provisions. Hence, these expenses are not a factor in their decisions regarding the maximum time employees are allowed to work remotely. That said, some of these institutions are considering a one-off grant to staff towards setting up their home offices as it best suits their needs.

3.8 Operational adjustments

Although many processes had already been digitalised or are in the process of being digitalised, the pandemic has provided a strong incentive for further digitalisation. Changes were implemented, as far as possible, to processes that involved a lot of person-to-person interaction, including cash handling (increasing the use of electronic transfers), recruitment (through greater use of online evaluations) and procedures that involved dealing with the public. In general, institutions are adjusting their operations so that they can be executed more easily or efficiently by employees working remotely. Adjustments include a greater use of digital information (less need for paper documents), the use of electronic signatures, automated monitoring of controls and implementation of virtual sessions, among others.

4. New risks to operational continuity in the future of work

In an unprecedented situation like the Covid-19 pandemic, where new challenges and risks have emerged, it is important to be prepared to deal with them, given that they might strike institutions in a swift and broad manner. Furthermore, it is important to understand how these risks can impact the institutions' current risk profiles. The pandemic-related disruptions have affected information systems, personnel, facilities and relationships with external service providers. Besides, cyber security threats experienced during the pandemic –ransomware attacks, phishing, etc – have increased the concern that there could be more operational risk events resulting from greater dependency on remote working schemes (Box 3).

Thus, it is important to reflect on whether the risks that have emerged can be managed, and whether there are procedures which have already been implemented to identify, analyse and aggregate these risks while the new work schemes evolve. Furthermore, institutions must have the certainty that key operational risks brought about by the pandemic have been identified and that proper strategies have been developed to mitigate them (for example, if implemented technology tools can be leveraged to manage pandemic risks).

One of the risk scenarios that some institutions are currently experiencing, or are about to experience, is the transition of their current pandemic-related operational continuity scheme to a state of operation without physical distancing restrictions. In order to ensure operational continuity, institutions are executing actions to avoid possible massive contagion of their staff, and consequently the possible inoperability of their activities. Thus, they are considering a gradual reinstatement of staff to in-person work.

Box 3

Cyber security risks

Due to the lockdown and the need to maintain business continuity, organisations extended their remote access capabilities for most staff, allowing them to conduct their work remotely. As a consequence, employees had access to critical information, conducted private meetings and discussed sensitive subjects from home, with the possibility of being heard by neighbours or family members. These activities were performed using a technological infrastructure that was shared with family, friends or roommates, and which was not monitored or controlled by the organisation. These remote operation schemes using residential internet connections and, in some cases, personal devices, generated important cyber security risks by themselves. Both physical and digital control normally used to protect the organisations' information and infrastructure were bypassed for the sake of maintaining social distancing. On top of that, during the pandemic, hackers took advantage of remote connections and operations to intensify social engineering schemes to gather information. They also launched aggressive phishing campaigns to install malware to steal credentials and conduct ransomware attacks.

As a result, organisations were forced to swiftly review and strengthen their remote access capabilities, provide secure IT solutions for most employees, launch cyber security awareness campaigns and make adjustments to their processes to avoid the use of documents in physical format. Most of these schemes came to stay and will still be used once operations resume as normal. Depending on the future of work defined by each organisation, further cyber security protections might be needed, but the operational and technological basis is already available and has been extensively tested during the pandemic.

As preserving information security is one of the concerns that institutions have today, they have made efforts to identify the information assets they manage, which means to determine the category or classification that the information has and the applicable security standards. In addition, along with these efforts, organisations have considered the implementation of data loss prevention (DLP) tools that allow them to identify, classify and protect documents, using the application of content labels.

Finally, it might be necessary to consider the implementation of new and available tools such as cloud storage and processing, which can support the implementation of continuity strategies throughout organisations.

The hybrid working scheme (part-time on site and part-time off site) will eventually be implemented in all organisations. This scheme requires increased resilience for the organisation as it ensures the continuity of operations, especially in scenarios that affect the availability of facilities (eg social unrest, earthquakes, among others) or the availability of staff on site (eg extreme weather, failures in transportation services etc). In fact, geographical dispersion of operations has historically been considered to be part of BCP, in order to prevent interruptions derived from extreme weather, power failures or terrorism. A new rationale for geographical dispersion includes health threat scenarios, since these may affect geographical regions differently (including their impact on the need for quarantines, on transit etc).

The future ways of working might imply risks that need to be recognised in an organisation's risk profile. The main risks identified by the task force are described below.

4.1 Increased risks that may affect staff availability

The risk of personnel unavailability has increased significantly during the pandemic. Not only does this risk refer to current key personnel becoming ill at any given time but also includes the ability to retain and recruit talent. This problem is expected to continue post-pandemic due to changes in work schemes. Hence, it is necessary to consider strategies for a more efficient recruitment process, without diminishing its quality. One of these strategies is fostering and strengthening organisational culture among new employees in order to generate the appropriate bond, ties and commitments with the organisation. It is important to notice that new working schemes could also offer the opportunity to recruit talent residing in different domestic regions or abroad.

Risks related to the physical and psychological health of personnel arising from the pandemic have increased. Thus, in addition to deploying preventive actions and medical support in case of contagion amongst personnel, organisations have also regarded the implementation of psychological support programmes for staff to be necessary. The change in work schemes, prolonged isolation, information related to the evolution of the pandemic, the loss of physical contact with other people, as well as the possible loss of friends and relatives have generated fear, anxiety and anguish in many people. Therefore, it is necessary to monitor the mental health of staff, establish support networks and provide professional psychological advice, among other actions.

4.2 Dependency on physical and technological infrastructure external to the organisation

Prior to the pandemic, practically all the activities and processes of an organisation were executed inside their facilities, where there are logical and physical access control schemes in place and absolute control on the computing and communication infrastructure and primary services such as electricity, running water, etc. However, in a generalised scheme of remote or hybrid working, staff could use their own computer equipment as well as their residential internet and electricity services to access the technological infrastructure of the organisation.

During the pandemic, organisations had to accept new risks that would not be considered if all activities were carried out within its facilities. However, they have also considered some practices to mitigate these risks. One was providing staff with computers and telephony equipment, which can be supervised and managed by the organisations. Another was to assign uninterruptible power supply systems (UPS), mobile broadband internet and satellite telephony devices for strategic roles. Besides, institutions have implemented connection schemes, with a robust access control, and other additional tools for monitoring and detecting vulnerabilities in the technological infrastructure.

4.3 Possible relaxation in information security controls and personnel management

Organisations quickly moved to remote working schemes due to the need to maintain the continuity of their operations during the pandemic while prioritising the health of their staff. Yet, by doing so they also allowed working practices that would not be appropriate under regular circumstances such as operating critical systems from the home of staff and using personal (non-institutional) email or meeting tools, among others. As part of the future of work, institutions should therefore define which of these practices will be allowed and how they could be executed (eg using institutional hardware and software tools). For that purpose, they should consider the risk and criticality of their processes.

An additional challenge that organisations have faced in the pandemic is adequately managing and supervising staff who work from home or in a hybrid scheme. In many cases, organisations have strengthened performance assessment schemes focusing on deliverables. They have also established more flexible schedules and focused less on the number of working hours.

4.4 Increased risks that affect information security

Much of the information that had been handled exclusively inside the organisation's facilities before the pandemic is currently being used by staff in their homes. This increases information security risk as this information travels over the internet using private connections belonging to staff and is used in physical spaces unknown to the organisation, such as the homes of staff. Furthermore, staff members often live in the same space as family or friends, who are outside the organisation's surveillance. Without adequate guidelines – or sufficient training to ensure compliance with these guidelines – staff members could adopt unsafe practices in the handling of information. Unsafe practices include connecting through public

networks, handling files or documents in an unsafe manner, sharing laptops and computers for activities other than working, etc. Indeed, in order to exploit this greater vulnerability, hackers and other types of criminal groups have increased their attacks during the pandemic.

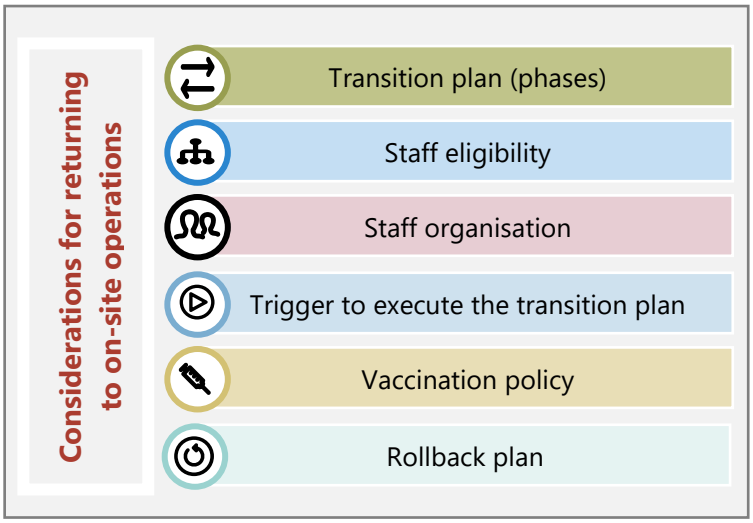
To properly manage information security risk, organisations need to define secure working guidelines, promote them and train staff in their application. They should also invest in technological tools for secure access, communication and coordination as well as for the use of connections in a virtual private network. At a minimum, organisations should implement a double authentication scheme and secure password rules for access control, and should avoid, to the extent possible, conducting monetary transactions outside the premises of the organisation.

The risk of staff mishandling information should be mitigated by strengthening the information security culture throughout the organisation, by alerting staff about potential risks and training them on safe information management practices and the proper use of tools and equipment for remote work. Since new work schemes may prevail, this information security culture must be aligned with the implementation of technological advances in remote working.

In general, the experience that organisations went through in this pandemic showed that they must be prepared to face any kind of disruptive event, regardless of its origin. That is, their plans and personnel must be prepared to act and react to any type of incident and not be limited to a list of probable events. Risks from climate change, or other phenomena (natural or caused by human beings) leading to shortages of basic resources such as water or electricity should also be considered. Today these risks appear distant but they might increase in the future.

5. Considerations for returning to on-site operations

In addition to the best practices mentioned in the previous section, this document has been elaborated on while the pandemic is still in force and many organisations are in the process of planning or executing their transition to their new normal. As a result, the task force analysed how their organisations could move from the current contingent operation scheme to one in which restrictions on in-person interactions are lifted. The analysis revolved around the following factors:



5.1 Transition plan (phases)

As all institutions prioritise the health of their staff in this pandemic, they have opted for a gradual return to face-to-face work. This transition will be carried out in different phases according to the guidelines determined by each organisation. In the first phase various institutions will consider the return of their staff on a voluntary basis, provided they meet the health requirements defined by the organisation itself, including being vaccinated and not having Covid-related symptoms. The return of staff to bank facilities will be gradually increased as the evolution of the pandemic allows it.

Another factor that some institutions consider in their plans is the criticality of the operations carried out by personnel and the need for, or relevance of, these operations being executed at the organisation's premises.

During the staff reinstatement process, all institutions will continue to adhere to the health measures determined by their country's health authorities (social distancing, use of face masks, limited occupation rates in buildings, etc). Regarding vaccination, institutions will also adhere to the regulations of their respective authorities and apply any relevant exceptions for religious or medical reasons.

5.2 Staff Eligibility

In general, institutions determine the eligibility of staff to return to on-site work by considering the following criteria: the vaccination status against Covid-19 of employees; the guidelines determined by the health authorities of their respective countries; and local contagion trends. Regarding this last point, it should be noted that some organisations have facilities in different locations and would therefore have to pay attention to different contagion trends.

Some organisations will also consider whether the employee participates in critical activities along with the employee's personal situation, including whether the person has the role of caregiver of school-age children who cannot attend school or full-time caregiver of close relatives who are ill.

5.3 Staff organisation

In general, organisations will gradually incorporate staff into groups or crews, and these groups will take turns to work at the facilities. Alternating shifts and flexible schedules would be considered. Furthermore, in some institutions, staff will be organised according to the space capacity available at the facilities, according to recommended health measures.

When organising staff, the transition plan should take into consideration the criticality of the processes in which they are involved, establishing strict measures for their healthcare at home, during commuting and transfers and within the facilities of the organisation. This is in addition to providing adequate medical support.

5.4 Trigger to execute the transition plan

In general, organisations have defined a trigger or a set of conditions to start returning to offices based on the current state of the pandemic. These conditions include criteria such as the percentage of vaccinated people in the population, the number of new cases of Covid-19 among staff and in the cities where facilities are located, occupancy rates in hospitals, operational needs, etc. It is expected that the new way of working will be implemented once pandemic restrictions are lifted.

5.5 Vaccination policy

Regarding vaccination against Covid-19, the institutions are following the regulations or directions of their respective governments. They are also considering exceptions (eg for those who cannot be vaccinated due to religious or medical reasons).

The actions to be carried out with respect to unvaccinated staff differ across organisations and depend on the internal rules applicable in each case. In some organisations, staff who have decided not to be vaccinated will be reinstated for on-site work based on the same criteria as the rest of the staff members. In some other organisations, they will be provided with training related to the immunisation process. And in others, vaccination will be mandatory for all staff.

5.6 Rollback plan

In general, institutions have considered a process of immediately returning to working from home in circumstances in which there is a sufficiently large increment in the number of new cases among their staff or in the population of their country. Compliance with official provisions would also need to be taken into consideration.

5.7 Suggested guidelines to prepare the transition to the future of work

The following questionnaire can be used as guidance to assess the preparedness of an organisation when considering its transition to a new, operationally resilient way of working.[6]

Questions		Ready?	Comments
1. Transition plan			
1.1	Has a decision been made to transition gradually (in phases) or in one go?		
1.2	Has a date to start the transition been agreed and communicated?		
1.3	Is the transition initiated voluntarily or mandated by management?		
1.4	Are health requirements required to transition out of the crisis?		If yes, list requirements:
1.5	Has a decision been made on how long the transition should last?		
1.6	Is the transition applicable to critical activities only?		If yes, list activities:
2. Staff eligibility			
2.1	Have staff eligibility criteria been defined and agreed?		If yes, list criteria:
2.2	Are criteria in line with the country's requirements?		If not, list differences:
2.3	Are eligible staff only those supporting critical activities?		
2.4	Are personal constraints part of the eligibility requirements (such as care giver requirements, schools…)?		
2.5	Is vaccination a mandatory requirement to return to office work?		
3. Staff organisation			
3.1	Are staff returning to the office in specific groups or as each individual decides?		If groups, list defined groups:
3.2	Are staff returning to the office in alternating shifts?		
3.3	Are staff returning to the office alternating desks (so that two people do not sit next to each other)?		
3.4	Is return to the office constrained by building capacity limits?		
3.5	Are managers following the same guidelines as individual contributors?		
4. Trigger to execute transition plan			
4.1	Has a trigger to start returning to the office been defined and agreed?		
4.2	Is the trigger data-driven (stats, vaccination rate, etc)?		
4.3	Will return to the office only happen once all measures are lifted by the government?		
4.4	Is the same trigger used across office sites (if there are multiple offices)?		

[6] Additional questions could be added to further refine the transition plan for a particular organisation.

Questions		Ready?	Comments
5. Vaccination policy			
5.1	Are exceptions from local government guidelines considered?		If yes, list exceptions (eg religious, cultural…):
5.2	Are actions to be carried out in respect of unvaccinated staff defined and agreed?		
5.3	Have both HR and Legal been involved in any personnel-related decisions?		
6. Rollback plan			
6.1	Has a rollback plan been defined and agreed?		
6.2	Has any option other than full home office been considered as a rollback plan?		
6.2	Is the trigger to rollback defined?		
6.4	Have the decision and communication processes to rollback been defined and documented?		

6. Conclusions

Due to the Covid-19 pandemic, there could be long-lasting changes to work patterns in organisations. Remote work was implemented as an alternative strategy for a contingency to ensure staff distancing and protect them against possible contagion. Not only did remote work prove possible, it also proved to be efficient. Hence, working from home is expected to remain part of the daily work schemes of central banks.

Another lesson from the pandemic is the relevance of developing operational resilience in institutions, and being prepared for unprecedented or very unlikely risk scenarios. Very few organisations could have foreseen the magnitude of this pandemic. Even when a pandemic was contemplated, the duration of such a pandemic was expected to be so short, or its probability assessed as so low, that little reference was made to it in business continuity plans. Nevertheless, the strategies designed and implemented in pre-pandemic BCP for other scenarios did help institutions to rapidly deploy new ways to execute their operations in the pandemic and deal with the new risks that have emerged.

Working from home offers various benefits to organisations in terms of resilience. However, if adopted on a permanent and widespread basis, it also involves new risks for information security. These new risks must be recognised, managed and addressed as part of the operational risk or internal control programme. They also require staff to be aware of information security policies and good cyber security practices when operating from home.

Developing and maintaining an organisational culture without a common physical place is a difficult challenge. Team building strategies will be vital for the long-term success of hybrid work schemes. In addition, management must pay special attention to provide equal opportunities for employees working on site and those working off site.

No organisation is the same. The set of practices regarding operational continuity described in this document will therefore have to be considered in light of the circumstances faced by each organisation. Sometime after their implementation, organisations will be able to analyse and validate those practices and, if needed, update or replace them. As there is still a lot to learn, it is proposed that the task force that prepared this document will continue to be the forum for exchanging information on this subject.

Annex 1: Definitions

Terms	Descriptions
Alert or warning scheme	Some central banks have implemented an alert or warning scheme to notify staff about the expected severity of a contingency and the general guidelines that staff must follow.
Business continuity coordination and senior leadership	In case of a contingency, central banks have a top management group in order to follow events, make decisions in a timely manner and support and give instructions to the expert group (HR, IT, Security, General Services and others) in charge of executing them, keeping track of the contingency and notifying others of the evolving status.
Business continuity Plan	Documented strategies for management of the operational continuity of the organisation. It implements the necessary actions to prevent and act in a timely and coordinated manner in the face of events that interrupt or may interrupt its daily operation. Additionally, the business continuity plan provides a common language and criteria that help to have a better understanding and better coordination among staff for the recovery of operations.
Business impact analysis (BIA)	Method to identify the consequences or impact (from different perspectives) which the interruption of the operation of a process has for the organisation, taking into consideration time frames.
Communication	Communication is a relevant aspect of a business continuity plan. Central banks should ensure that, in case of a contingency, all staff are rapidly informed about its status and evolution. If communication tools depend on the bank's infrastructure, it is important to consider alternative mechanisms in case the infrastructure fails.
Contingency	Unforeseen event that may alter or disrupt the operation of the organisation.
Dependencies on external resources	It is important that business continuity strategies consider dependencies on key external resources provided by third parties. Some strategies are deployed on the assumption that these resources will be available during a contingency, because a contingency is only expected to affect the organisation (ie local contingency, not generalised contingency).
Digitisation	The procedure for changing a process or information from analogue to digital form.
Identification of critical processes	A process is classified as critical if its interruption in a narrow time frame could cause significant damage, preventing the central bank from achieving its objectives.
Operational disruption	Any significant delay or disturbance in the execution of one or more processes arising from an event that affects, among other things, the availability of human resources, buildings and facilities, infrastructure, information technology services and communications infrastructure of the organisation.

Terms	Descriptions
Operational resilience	The capacity of any institution to prevent, respond, adapt, recover and learn from any type of disruptive event.
Phishing	A kind of cyber attack that starts with a decoy when you receive an email that appears to be from a trusted sender, has a high sense of urgency and prompts you for immediate action such as opening a link to a fake site, downloading files or sending personal information (user logins and passwords, credit cards information, etc) in order to be used fraudulently.
Ransomware	A type of harmful programme that restricts access to certain infected parts or files and asks for a ransom for removing this restriction.
Resilience	The ability to prevent, respond, adapt and recover from a disruptive event and be able to learn from it.
Risk scenarios	For implementing a business continuity plan, central banks consider several scenarios that differ by the risks to which they are exposed and their institutional circumstances.
Staff roles	Employees can be appointed to a specific role in case of a contingency. The objective is that every person has a well defined set of tasks in the processes during a contingency and is prepared.
Testing and training	To ensure that business continuity strategies work adequately, central banks train staff in charge of critical processes. Most training consists of drills and top-table exercises. It is relevant to put in place an annual calendar for these drills and exercises to test business continuity strategies and ensure that all staff are prepared to deal with any kind of contingency.
Time frame	Generally, this narrow time frame is at the basis of the design and development of business continuity frameworks. Most contingencies faced by central banks before the pandemic lasted some hours or days only.

Annex 2: Members of the Consultative Group on Risk Management (CGRM) task force on business continuity planning

Central Bank of Brazil	**Marcelo Garrido** Head of Business Continuity Division
Bank of Canada	**Marty Olson** Director, Continuity of Operations, Corporate Services **Brian Rheault** Senior Analyst, Continuity of operations, Corporate Services **Syed Asghar** Analyst, Financial and Enterprise Risk
Central Bank of Chile	**Maria Jesus Orellana** Operational Risk & Business Continuity Manager
Central Bank of Colombia	**Diego Vasquez** Head of Non-Financial Risk Department and the BCP area
Bank of Mexico	**Claudia Alvarez Toca** (Chair) General Director of Comptroller and Risk Management **Lissete Ponce** Head of the Non-Financial Risk Division
Central Reserve Bank of Peru	**Hector Jaime** Business Continuity Leader **Wilder Mantilla** Business Continuity Specialist
Federal Reserve Bank of New York	**Mark Harvey** Business Continuity and Resiliency Senior Leader
Bank for International Settlements (BIS)	**Anne Ponton** Principal business transformation and resiliency/Business Continuity Manager
Observers (from the BIS)	**Alexandre Tombini** Chief Representative, Representative Office for the Americas **Jaime Cortina** Deputy Chief Representative and Regional Head of Treasury and Asset Management **Fabrizio Zampolli** Head of Economics for Latin America and the Caribbean

	Christian Upper Senior Adviser **Victor Riquelme** Visiting Economist