International Securities Services Association

Domestic CSDs

March 2022

THE DOMESTIC CSD AND RESILIENCE

Welcome to the first paper of a series of publications created by the Domestic CSD Working Group (WG). The aim of the paper is to record in one place the key considerations that a Central Securities Depository (CSD) should address to ensure the resilience of its operations.

INTRODUCTION

A CSD's operational resilience depends on multiple factors. However, the key factors are the accessibility and integrity of resources, such as personnel, infrastructure, technologies and data.

For each of these types of resources, the CSD is required to determine resilience and recovery strategies. It is imperative that CSDs take measures to maintain their ability to identify, respond to, resist and recover from threats and their potential negative impact. The results of the analysis of business continuity threats and risks as well as the Business Impact Analysis (BIA) are used as a foundation for forming the resilience strategies regarding CSD resources.

The Domestic CSD WG has created this paper to highlight the key actions required to ensure resilience of a CSD. Below are the key approaches to building resilience into the daily operations of CSDs. The list is unlikely to be exhaustive. However, it provides a minimum level of information on resilience practices, which if applied should help position the CSD for a successful management of any unforeseen disruption.

BUSINESS RESILIENCE

Business resilience is an imperative for all CSDs. For ease of the discussion, this paper does not focus on the financial resilience of CSDs, which is covered in depth in other ISSA papers. The assumption is that all CSDs have detailed financial scenario planning to ensure sustainability based on actual and forecast financial performance.

CSDs should engage continuously with Regulators and stakeholders to better understand the current landscape and emerging threats, or changes to business practices to mitigate impact of unforeseen circumstances. Based on the information gathered, CSDs should strategically review and reprioritize projects and deliverables to ensure that the resilience of their business is maintained.

If a non-financial resilience event occurs, then the key actions which will reduce the impact are:

1. CSD should have a clear communication rule set. This should address who can communicate to the external world and an approval process for that communication should be in place. It is important that all staff understand that social media channels should not be used at this time.
2. The CSD should continuously re-evaluate client contexts and update the Business Impact Analysis (BIA) and resulting plans and actions from that BIA to respond to the event.
3. Simultaneously, the CSD should engage with the Regulators to highlight impacts - and where appropriate ask for help in mitigating the impacts – for example, by requesting the Central Bank to extend its settlement window for the day.

OPERATIONAL RESILIENCE

This section provides guidance on what the WG believes a CSD should look to do to ensure that it is positioned for success in respect of operational resilience in planning, testing and automation.

Planning and Business Impact Assessment

1. The CSD should ensure that they conduct a BIA and, from this analysis, create and document a Response Plan, in order to ensure resilience in the event of a crisis. The BIA should establish how clearing and settlement, information technology (including technology infrastructure services) and procurement activities should support and sustain the delivery of key products and services during a crisis.
2. The maximum tolerable period of disruption (maximum acceptable outage) for each activity should be determined in the BIA, taking into consideration dependencies on other activities - such as funding and liquidity resources - which may be outside the CSD's control.

Testing

1. The BIA should be used to identify the dependency mapping of critical business services, people, processes, systems, facilities and information (internal and external dependency mapping).
2. The CSD should have redundancy in facilities, with a separate disaster recovery site. This site, located away from the production office, should allow robust Disaster Recovery (DR) and enable a business continuity plan with multiple layers of redundancies. The business continuity plan should at a minimum include the siting and protocols for both production and DR servers (see further below), as well as physical office location and a business continuity location. This needs to be known by all potentially affected parties.
3. As a result of the pandemic, a potentially optimal alternative 'office' space could be a Working from Home (WFH) arrangement, assuming current technology and other infrastructures as well as the controls that have enabled WFH are maintained post-pandemic.
4. A CSD should make an assessment of third-party delivery capabilities, for instance - if the cloud is used to provide server capacity – does the cloud provider has a realistic plan for business continuity in the event of an unforeseen event or crisis. Beyond the initial comfort on the adequacy of the business continuity plan of third parties, CSDs should maintain ongoing monitoring of the third party's ability to sustain business continuity plan and ensure adherence to relevant service level agreements, if they are vital to the CSD's operation and ability to effectively perform its role.
5. Business continuity processes validation and testing on an ongoing basis is a prerequisite for successful and sustainable resilience.

Automation

1. It should be part of a CSD's ongoing management to implement process enhancements/automation to introduce and maintain efficiencies, where possible. It is the belief of the WG that these automations should also provide resilience to the CSD. The reduction of manual tasks and replacement by automated processes allows, in most circumstances, a greater resilience to be built into the CSD. If the automation is executed well, it will introduce latent capacity, which can be used in circumstances of high volumes, whether under normal business scenarios or outstanding service volumes accumulated during an incident.
2. Project schedules need to be actively managed to ensure correct prioritization and delivery of initiatives within approved timelines and with the relevant awareness of project teams on the expected impact of the initiatives on business resilience.

TECHNOLOGY RESILIENCE

This section considers the options that CSDs have to address the technology resilience plan. There is not one singular recommended solution, as the requirements will vary by market.

Planning

1. All CSDs should have a Recovery Time Objective (RTO). This metric governs how quickly a CSD must recover its Information Technology infrastructure and services following a disaster to maintain business continuity. The RTO should be tailored to the importance and immediacy of the critical business operations that should be available at that point in time. An example being that the settlement function at the start of the day potentially can be recovered in the afternoon before the settlement deadline, but as the settlement deadline approaches the recovery time needs to be of heightened importance and the RTO adjusted.
2. All CSDs should agree a Recovery Point Objective (RPO). This is the measurement of maximum tolerable amount of data that could be lost. This helps to measure how much time can occur between the last data backup and a disaster without causing serious damage to the business. Each CSD should set internal RPO benchmarks with an awareness of the business' peculiar volumes, specific technical and practical local conditions and the operational control environment.
3. The CSD management must understand the business vulnerability to manual processes and ensure the correct prioritization, planning and delivery of digital solutions and its efficient adoption to replace high risk manual processes.
4. CSDs are part of a complex ecosystem and are a fundamental element in the local capital market. As such CSD management should have an "inside out" awareness of that ecosystem, with the monitoring of direct stakeholder changes and disruptions, tracking participants' implementation or resolution of potentially systemic issues, and continuously track BIA impact of CSD's vulnerability to failure of one or more participants, especially the systemically important participants..
5. CSDs should have established protocols and communication channels for emergency management, a 24/7 channel which should be provided for the gathering of the emergency management committee (for example, a conference call or a group in secure fault-tolerant corporate messengers).

Execution and testing

1. As noted above the CSD's ability to access and run its technology is critical to business resilience. The requirement is that CSDs should have a data centre recovery plan and site. The data centre recovery site may have numerous configurations:
    - Dedicated data centre and office space combined – access controls need to be appropriate
    - Dedicated data centre with no office space
    - Shared data centre (partitioned and segregated) which is unlikely to be with any office space especially in Tier 2 & 3 data centres
    - Cloud based capabilities

    The WG makes no specific recommendation about the choice of the data centre recovery plan and solution as it is dependent on the specific situation of the CSD. If a CSD elects a cloud-based solution then at a minimum it is recommended that the CSD contractually requires audited reports and certifications, for example - ISAE3402, ISO 27001, ISO 22301, SOC 1, SOC 2, SOC 3 and tests the capabilities of the cloud services annually, using the built-in disaster recovery tools.
2. Redundancy in file transfer mechanisms to and from the Exchanges, CCPs and custodian chain should be in place and regularly tested.
3. CSDs should ensure that disaster recovery testing occurs as per normal schedule as agreed by the management and involve Regulators. The outcomes should be used to validate capabilities and extreme but plausible scenarios should be explored either through desktop exercises or simulations.
    - A CSD should review any of the incidents experienced in these exercises and these should lead to the continual adaptation and improvement of the resilience plan, based on the findings.
    - Stringent testing of any changed technology or business processes, including analysis of the effect on resilience should be undertaken during these exercises.

PEOPLE RESILIENCE

This section looks at the actions that CSDs can take in advance of an incident, which will help their resilience and recovery due to the clarity which all members of staff have around their roles and responsibilities.

CSD responsibilities

1. A CSD should have a communication strategy to ensure that timely and relevant information is disseminated across the CSD staff and management.

2. The CSD should create a plan with roles and responsibilities of each area to ensure resilience in the event of an issue (Management, Corporate Communications, Response teams and Recovery Teams). An emergency response scheme should be defined by the organization to escalate any problems that arise. In the scheme there should be clarity on who is responsible for the directions / zones / functions, along the lines of which incidents may occur, and their deputies if they are out of contact for any reason. The communication channels / procedures shall be tested for identified scenarios.
3. The CSD should develop a document outlining what employees should do to support the organization in achieving strong resilience in the event of an occurrence or crisis.
4. Resilience incidents caused by a person's incapacitation can generally be avoided by good planning. A CSD should ensure that they have the workforce/skills needed to run the business. This requires that open positions should be filled as required and that the CSD mandates cross trainings between the staff to ensure that single points of failure are avoided and segregation of duties are maintained.
5. Training needs should be addressed as identified by the CSD management including cross-skilling of staff (as above). It is recommended that there is a rotational allocation of responsibilities amongst staff to ensure continuity of training and expertise as a single training event fades in people's memories within months and repetition breeds familiarity.
6. If a resilience event occurs, the firm should have "grab bag" books of procedures available (preferably with copies held at the homes of key people), an intranet site with Frequently Asked Questions (and the answers) for scenarios that the CSD foresees and a "hotline" which can be called if the intranet is not accessible. The hotline number should be printed on access cards to allow easy retrieval.

Staff responsibilities

1. Staff also have accountability within any resilience plan and should highlight when they require further training and cross training.
2. People resilience should be situational and role based. However, where a process is critical, a requirement that the employee should be able to arrive from home to the office as soon as possible - preferably within 2 hours or less if necessary - is not unreasonable .
3. If a resilience event occurs, the staff should have knowledge of and ability to gather the "grab bag". In addition, they should have already bookmarked the intranet site with Frequently Asked Questions on their devices and stored the emergency number on their phones.

Domestic CSDs

The Domestic CSD and Resilience

Institutions represented by experts in the Working Group "Domestic CSD"

BUSINESS RECILIENCE SUMMARY

Preparation is better in maintaining a resilient business posture than actions that can be taken on the day of an event.

The planning, and more importantly regular testing, of all the resource elements involved in the daily business of a CSD can help mitigate the impacts of an event. Additional automation can both mitigate the impact of unforeseen event and reduce the likelihood of occurrence.

It is highly likely that events will occur - potentially they could be driven by a failure of a national infrastructure or an idiosyncratic event at a CSD.

All CSDs must act as if they could be affected by an event and build robust BIA and disaster recovery solutions for multiple scenarios.

Staff and third-party suppliers are key vulnerabilities which must be managed well to ensure resilience, as there is always the tendency for these important stakeholders to be overlooked.

Technological resilience and disaster recovery capabilities are normally the focus for Boards. The WG would recommend that these are regularly tested and, where feasible, production is regularly switched between disaster recovery and production sites.