Domestic CSDs

February 2022

THE DOMESTIC CSD AND REMOTE WORKING

Welcome to the second paper of a series of publications created by the Domestic CSD Working Group (WG). The aim of this paper is to record in one place the majority of considerations that a Central Securities Depository (CSD) needs to consider and address to ensure the success of remote working or Working from Home (WFH).

INTRODUCTION

Before the pandemic many CSDs were organizations where employees were fully Working From the Office (WFO). There was no opportunity for staff to work from a remote location and the view was that everyone was physically present in the office for work to be successfully performed and executed. However, as a consequence of the pandemic, CSDs around the world had to adapt their working methods and up to 95% of their workforce have been working remotely.

The CSDs have taken this experience and provided the key items that should be considered to be prepared for remote working. The list is unlikely to be exhaustive. However, it provides a level of information on remote working which, if applied at a CSD level, should help pre-position the CSD to successfully manage and sustain the introduction of a remote working environment. The steps identified are those which will generally require some lead time. Therefore the WG recommends that the creation of plan to successfully implement remote working is initiated, and then maintained, on a forward looking basis.

ORGANIZATIONAL & PERSONNEL ISSUES

This section provides guidance on the actions that a CSD should consider to ensure that both the staff and the management of a CSD have the best experience of remote working and that expectations are transparently aligned.

Employee Focused - CSD

1. While this is best practice in any circumstance, with the implementation of remote working it is particularly key that CSDs should ensure that the leadership is visible and is seen to be active and continuing to lead the organization despite the regulatory, time and personal pressures. This helps employees remain emotionally connected to the organization and helps both retention and a sense of purpose.
2. Remote work should be designed properly. Additions to contracts with employees should be issued including the work rules and requirements for the remote workplace and equipment. These should be accompanied by general recommendations to the staff on topics such as ergonomics.
3. In some circumstances remote work is limited and has to be performed within specified countries or regions due to tax, regulatory or licensing requirements. This potentially impacts both recruitment and remote working. These restrictions should be explained to the employees and form part of the working agreement.
4. Staff should be aware that certain set of statistics from monitoring systems are available for managers. In a remote working environment these are likely to be reviewed more frequently to ensure training can be given where needed, whereas in the office managers can literally see when employees are struggling. Transparency that the metrics are being used should overcome staff concerns of Orwellian supervision. The CSD should decide whether these metrics are always available to managers or only on request and explain that to staff in an adequate manner.
5. The schedule of remote work is unlikely to be the same for all functions and should be determined based on the capabilities of the business processes of each specific department.
6. It is up to the CSD to agree where the responsibility for the organization of the workplace, with a remote work format and everything necessary for work, lies with the employee or employer. E.g. the CSD should provide a laptop but the employee must provide the desk and a private location within the home to work from.

Employee Focused – Staff

1. In normal circumstances employees should be able to initiate the possibility of their (partial or full) remote work and coordinate their schedule with their direct supervisor. The supervisor should agree the schedule and coordinate the transition to a remote format based on the needs of the department.

2. Employees must ensure, before commencing remote work, that they have a stable internet connection that allows them to fully perform the official duties without violating internal regulatory documents and company requirements, as well as information security rules. The CSD should take all the necessary measures to provide secure access points and VPN connections.
3. The employee should have the right, in agreement with the direct supervisor, to come to the office outside the planned schedule in case of production necessity.

Operational Accommodation

1. It is recommended that the organization has a formal Teleworking Manual clearly defining and documenting processes and procedures, both of a technical nature relating to the role and expected behaviours in foreseeable circumstances such as loss of home internet connection. One element of the manual should be designed to raise awareness of the increased cyber threats from WFH. These include:
    - Antiquated, personally owned devices used for WFH may lack solid security controls and must be maintained with the latest patches and updates.
    - Devices may be shared among family members, including schoolchildren, who are less likely to be aware of potential hazards on the internet.
    - Heightened vulnerability to social engineering attacks, such as phishing, due to employees' distraction or changing routines and processes.
2. The CSD must ensure that it is monitoring and actively managing any key person dependencies, ensuring multiple people can perform the role by cross-skilling of team members to ensure ability to execute in need.
3. The CSD should implement heightened intra-day monitoring of operational activities by different functions to allow resource reallocation if necessary.

Mental and Physical Wellness

1. Ensure that the staff are capable of taking time for recreation even if it has to be mandatory, especially when the remote work is forced upon the employee due to a pandemic and business demands are high. This can be achieved through a comprehensive departmental Human Resources plan (including tracking leave), monitoring of screen time and ensuring that mandatory block leave is maintained.
2. Managers should establish consistent daily wellness check-ins with staff members and encourage the staff to leverage CSD provided ongoing training in wellness topics. This training can be provided either by the CSD if it has the competence or via an external supplier.

3. Consider remote psychological counseling and psychosocial risk factors and other risks and offer counselling as needed, especially as part of a return to the office strategy.
4. The CSD should try to make remote life more engaging by running such things as virtual:
    - Nutrition month / healthy breaks events
    - Quality of life talks
    - Teleworking contests such as “Quarantined panoramas”
    - The value of coffee

TECHNICAL REQUIREMENTS

This section provides guidance on the actions that a CSD should consider to ensure that the security, especially cyber security, of the CSD is maintained or enhanced and those actions it should consider to enhance its technological capabilities. Remote working is not a free option - major capital expenditure investment in remote / mobile working devices and mobile device managers are recommended, however it is a capability which may help in retention and recruitment.

1. It should be clearly understood by all staff and especially suppliers to the CSD that WFH brings unique cyber risks to bear on the CSD’s operations.
2. The CSD should set rules that should be implemented by staff and suppliers to reduce the surface area of this risk. It is recommended that adherence to these rules is tested.
3. Additional cyber / information security training for all staff members and how to secure their home network and data, tailored to remote working topics should be rolled out.
4. A Network Access Control solution should be implemented - i.e. use of remote intranet capability. This solution should provide assurance to the organization by giving visibility and control, allowing knowledge of who comes into the domain (Network) wirelessly (WLAN), direct physical access (LAN) and - most importantly - from the internet (VPN). The solution should give a high level of control to the IT team to monitor and profile users as they access resources in the Datacenter.
5. The IT team should consider retiring Adaptive Security Appliance (ASA) in favour of a Unified Threat Manager. In summary for non-technical readers an ASA is a layer 3 and layer 4 firewall. UTM stands for Unified Threat Management, meaning it performs layer 3 and layer 4 firewalling but also has the capacity (much larger storage, more RAM, and faster CPUs) and capability (with licensing, usually) to go beyond and may filter up to layer 7. UTM appliances are required when not only a firewall is needed but also the ability to filter spam, geo-filter, web filtering (blocking sites by category) etc., i.e. UTM is more capable especially if staff are WFH.

6. The IT team should increase bandwidth resources to manage network traffic
7. The CSD should establish
    - electronic (emails) document classification and enforcement by implementing a Data Leak Prevention tool to monitor data that traverses in and out of CSD domain
    - tools/software to enable remote working such as MS 365, electronic signatures, and cloud services
    - two-factor authentication that should be considered mandatory in most circumstances.
8. Remote access to be granted taking into account the requirements of security and data encryption. It is recommended that a VPN solution is used to increase productivity as employees can work from anywhere and anytime by accessing corporate files and applications securely via a virtual private network. By encrypting data in transit, a VPN secures the connection to the remote server.
9. For employees working with assets, access should be permitted only using double validation checks, in case of an emergency by an additional solution.
10. The IT Security department should prevent the increase in privileged access grants to users or administrators and consider creating new forms of privileged access for smaller subsets of applications.
11. The CSD should ensure that the operating system and software used on the computer from which remote work is carried out is still supported by the manufacturer. The automatic update installation mode must be enabled. Updates and the transition to a new software version should occur immediately after their release by the manufacturer. The employee is obliged to independently ensure that updates are installed in a timely manner if they are using a personal device to connect to the CSD.
12. Within the CSD, continuation and monitoring of hygiene practices - patching, versioning, user management, mandatory updates, password changes - are essential to allow safe working in the office and these are especially needed to reduce the risk surface area when allowing remote working .
13. The work account on the computer should not be used to access prohibited resources, and this should be clearly laid out in the manual and contract.
14. It should be highlighted to employees that the use of company equipment for personal use can lead to the introduction of vulnerabilities. For example where an organization’s staff allow their work devices to be used by their children for home schooling and downloading programmes or unsecure documents, this has the potential to introduce vulnerabilities and children are less questioning of launching an executable programme.
15. Anti-virus software must be installed and activated on the computer. In addition, automatic updating of the anti-virus databases must be ensured and the CSD must periodically check that the anti-virus databases are up to date.

16. Work on the computer must be carried out under a separate account that does not have local administrator rights.
17. During the absence of an employee at the workplace, the computer must be blocked from extraneous actions. The computer should be automatically locked for inactivity (e.g. for a period of 5 minutes), followed by the requirement of a password to unlock.
18. Any means of remote access to the computer must be removed or deactivated.
19. It is recommended that there should be increased monitoring of network traffic and connections to the organizational systems and enhancements of data protection mechanisms are made.
20. If signs of a possible cyber threat from an employee's computer are detected, remote access should be restricted for the employee. In case of non-compliance with information security requirements, remote access should be suspended and consideration should be given to whether the employee should lose of the right to work remotely and consequently should work in the office on a permanent basis. The potential consequences should be clearly documented in the contract (see above).
21. The appropriate updates should be made to the organizations information security policies by the Enterprise Risk Management Unit to accommodate remote working requirements.

SET UP AND INTERNAL COMMUNICATIONS

This section provides guidance on the actions that a CSD should consider to ensure that the staff have visibility and leadership during this potentially confusing time. It also addresses some of the challenges of returning to the office after potentially a long period away.

1. Communication should be a key facet of leading through crisis and a sustained WFH set-up. There is no one singular answer but aspects that CSD Management should consider are:

    - Video capsules / events focusing on the staff needs
    - Leadership newsletters – covering both the successes and challenges and thanking individuals or teams for particular triumphs
    - E-Leader manual – helping middle and junior managers learn the skills to help them perform
    - Creation of start of day and end of day virtual “huddles” to allow people to ask for help or advice and ensure distribution of key tasks
    - Resource an emotional management and quality of life programme
    - Rolling out a remote work implementation survey every two months to understand the challenges and morale of the team

Domestic CSDs

The Domestic CSD and Remote Working

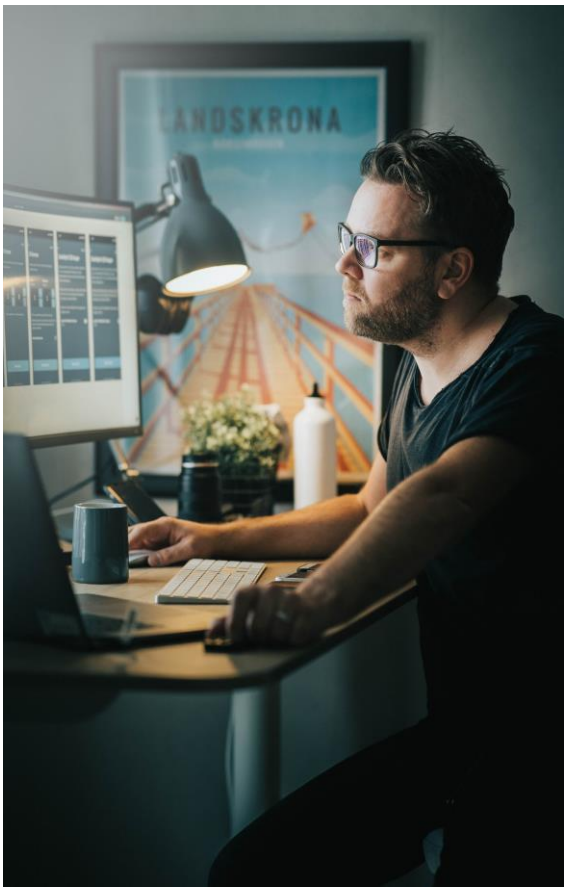
BACK TO THE OFFICE

Returning to the workplace after prolonged absence increases the stress on a person and the organization. Some recommendations to allow a simpler return to the office strategy with inbuilt resilience include:

1. Prevention kit delivery – ensuring staff have the necessary confidence to return to the workplace before they even come to the office as they have the required Personal Protective Equipment (PPE) for travelling etc.
1. If possible Anti-COVID/influenza vaccine could be offered.
2. Bipartisan team should organize the return to work with transparent goals and criteria.
3. If the circumstances warrant it, it is recommended 50% of staff are off site on a rostered basis.
4. Review, update and publish both:
    - Covid emergency protocols and
    - prevention and control measures.
5. Establish and publish the rules of office attendance i.e. only vaccinated staff onsite, high risk staff remote etc.
6. Implement transport rules for all those attending the office such as maximum 4 lift share, PPE on public transport
7. Where possible offset/restrict hours in the office to avoid rush hours
8. Management should consider whether catering can be safely provided or staff should bring food from home.
9. As teams return to the office the CSD should promote prevention measures (screens and elevator rules) and take engineering (desk spacing) and organizational measures to ensure that the workplace feels safe. Adopt regular cleaning and disinfection measures.
10. Provide personal protective equipment and ensure its effective use
11. Monitor the health of those who work in the office
12. Limit visitor access and ensure the highest level of care is used and where visitors must attend ensure PPE is mandatory
13. Paying a high degree of attention to laptops and other portable devices when are taken outside of remote working places (to prevent the risk of robbery or accidental destruction)

Domestic CSDs

The Domestic CSD and Remote Working



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

SUMMARY AND CONCLUSION

As outlined above many CSDs have been working in a remote manner during the pandemic. This has generally been very successful.

The aim of the WG was to bring as many of the techniques that have been seen to be successful into one resource so that every CSD can benchmark their approach to others.

The focus on staff and enabling technology are in the WG's view the two most important factors.

Remote working may not be possible in all cases and good implementation comes at a cost. However, where remote working is executed well it both contributes to the resilience of CSDs and opens up opportunities to a wider segment of society to participant in high quality jobs, which helps both recruitment and retention.

Tel: +41 58 399 23 68
Email: issa@issanet.org
c/o SIX Group Services AG Hardturmstrasse 201, P.O.Box, CH-8021,Zurich, Switzerland
www.issanet.org