Crowe

# Resuming WFO - a digital checklist

Crowe Advisory Services (India) LLP

Audit / Tax / Advisory

Smart decisions. Lasting value.

## Introduction

As the lockdown gradually lifts over the next several days and weeks, there will be an uncommon eagerness to get to the office.

As we restart WFO, there are digital risks that we could run; these could damage data, access, systems and security.

We have put together this checklist to help you plan and implement your re-start in a meaningful way.

## Checklist Matters

1. Prepare in advance for resumption of WFO. Conduct systems, servers and network health prior to re-opening after lockdown.

2. Check power, cooling, UPS backup, DG to ensure proper functioning and stability; this includes checking cables, wiring closets and data cables. Recognise that the power supply to the building and to the area may be seeing a surge after several works, as multiple offices re-open, and this may cause fluctuations initially.

3. Servers may likely have been shut down during lockdown; expect excess dust during boot and use appropriate protection.

4. Determine the booting and powerup order to ensure services proceed in a healthy manner. As a general guideline (but this may vary based on your infrastructure), the power-up order should typically be

    - Cooling systems
    - UPS
    - Network switches, routers, firewall etc.
    - Storage system
    - Servers – Infra Services such as DNS, NTP, Active Directory, DHCP
    - Production LOB applications
    - Server – LOB systems

5. Check the active directory server's system time and computer time; ensure the system has the correct time.

6. Delete or cancel overdue scheduled jobs.

7. Before resume production ensure tasks such as backup, routine tasks which are due are performed while resuming WFO.

8. Review the configuration changes on network, servers, computer devices, firewalls that were made to enable WFH; make necessary adjustments or restore previous settings.

9. Review protocol and controls for operations partly as WFO and partly as WFH; document and implement policy changes for sustainable WFH program and see the impact thereof on any client commitments made. Satisfy that these can work concurrently with either some employees WFO or any employees partially WFO and partially WFH.

10. Review and restrict any remote access to employees or remote administrative access, and remove remote administration tools which are no longer required.

11. Ensure anti-malware software is running and up-to-date; deploy critical security updates on servers, applications, and returning computers before employees are allowed to access IT systems.

12. Expect a surge in support calls from employees and be prepared to handle it. Likely support issues will include:
    - Connectivity problems (IP address)
    - Account lockout, password expiry
    - Obsolete computer accounts, Object tombstones (Active directory) due to long inactivity
    - Malware or other threats
    - Unauthorised system modifications or applications
    - Data copy/restore

13. If employees were using a personal computer at home, ensure the company data is properly copied to company systems and any company data on personal devices are wiped permanently.

14. Take assets inventory to ensure all assets are accounted for.

15. Ensure systems coming back to the network are clean from malware and other threats

16. Restore access permissions of users on the computer to the previous state, if required.

17. Check for unauthorised software, settings changes on returning computers.

18. If users carry their personal devices or personal storage to copy data back to company computer or system. Make sure they are clean from malware and threats.

## Caution

This checklist will assist SME organisations to resume work from office entirely or partially. The checklist is a general guideline to system admins, and IT managers. It cannot be considered as an exhaustive list because infrastructure at individual organisations may be different; accordingly proper discretion and caution must be applied for your respective cases – the checklist may help draw attention to these aspects.

## Conclusion

COVID-19 has presented an unprecedented situation across the world. Organisations must prepare long-term business continuity strategies to address such scenarios. Several companies are even considering changing the working model permanently by partially adopting work from home as part of their business strategy. This may also contribute to global sustainability.

While businesses adopt new approaches, it is imperative to consider cyber risk and data protection as a core component of the business strategy. Assess the cyber risk associated with the new approach and consider applicable controls to bring down the cybersecurity risk to acceptable levels.

## About Crowe India:

Crowe Advisory Services (India) LLP, a member of Crowe Global provides Risk Advisory, Corporate Finance, Taxation, Business Advisory, Digital Security Consulting, Data Sciences and Business Process Outsourcing services.

We have offices in eight cities in India. With our global network of 765 offices across 146 countries we render seamless professional services to local and multinational clients.

## Key Digital Security Contacts:

**Anil Aravind, Director, Digital Security Services**
anil.aravind@crowe.in

**Abhijeet Nath, Director, Digital Security Services**
abhijeet.nath@crowe.in

**Sreejith UG, Cyber Security Lead**
sreejith.ug@crowe.in

1105 Embassy Centre,
Nariman Point,
Mumbai 400021

+91 22 6631 1480
www.crowe.in

## Disclaimer: