Digital working models amidst crisis – data management, privacy and protection

The 30 day plan: Focus on continuity and risk mitigation, but improve preparedness for the future

Infrastructure capability

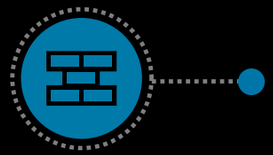
- Identify **critical applications and databases** to achieve scale while employees login remotely.
- Migrate **key services to the cloud** and prioritise access for specific user groups.
- **Ensure adequate network bandwidth availability** and implement necessary **data governance** measures to safeguard data.

Remote working

- **Scale Virtual Private Network (VPN) and Bring Your Own Device (BYOD) tools** to ensure secured connectivity to personal Wi-Fi or shared networks.
- **Use the journaling features of your email service provider.** In addition, expand server mailbox size and disable local downloading or saving of emails on computers.
- Conduct awareness campaigns to educate employees about new techniques adopted by cyber-criminals during this unprecedented situation.

Cyber security and data breach

- Deploy **secure infrastructure controls** such as Multi-Factor Authentication (MFA) , malware protection, etc.
- Set up capabilities for around-the-clock **incident and event monitoring, and deploy a robust incident response strategy.**
- **Raise awareness** about cyber-risks, and educate users about best practices to safeguard against such risks.



Privacy and data protection

- Ensure **adherence to privacy principles** such as data minimisation, purpose limitation, etc.
- Embed '**privacy by design' policies and carry out privacy impact assessments** for new systems or processes.
- Deploy **technical safeguards such as encryption** for secure transmission and storage of personal data.

Tax, legal and regulatory frameworks

- **Respond swiftly to COVID-19 tax and fiscal measures announced by governments** across jurisdictions. Also, assess the business impact that such measures will bring about, by undertaking impact assessments.