



State Comptroller Of Israel | Special Report: The State of Israel's  
Coping with the Covid-19 Pandemic | 2021

National Level Issues

---

# **The Covid-19 Pandemic – The IT Perspective**





## The Covid-19 pandemic – The IT Perspective

### Background

The labor market faces numerous challenges, including the need to prepare for a changing and flexible work environment that will be affected, among other things, by technological and digital advances. One of the changes that will characterize the labor market in the future, which came to the fore during the Covid-19 period, is work by remote connection to the organization's computerized systems (remote work). Remote work presents advantages from various aspects, such as reducing air pollution caused by transport, alleviating traffic congestion on the roads and facilitating access to the workplace for people with access difficulties. At the same time, remote work poses various challenges for employers and employees, such as reducing social interaction between the organization's workers and limiting the employer's ability to supervise his staff.



## Key figures

**Approx.  
40,000**

employees are employed in government ministries and auxiliary units

**Approx.  
4%**

of employees in Israel before the pandemic outbreak worked from home (according to figures for 2018), compared with 5.4% of employees in the OECD (according to figures for 2019)

**48%**

of all government ministry employees received approval to work from home in May 2020

**51%–  
57%**

of essential workers in government ministries worked from home during the emergency period<sup>1</sup>

**13%**

of work hours in May 2020 were performed from home

**Approx.  
2,500**

laptops were lacking in government ministries and government hospitals at the start of the Covid-19 pandemic (March 2020)

**51%**

percentage of women in government ministries who were given approval to work from home in May 2020, compared with 43% of men

**48%**

increase in the number of cyber attacks identified by the Israeli Cyber Emergency Response Team (CERT) in 2020 (in which there were 3,662 cyber incidents) compared with 2019 (in which there were 2,443 cyber incidents)


**5**

government ministries (out of 36) indicated that they had experienced a cyber incident through the remote access interface

<sup>1</sup> From March 22, 2020 to April 30, 2020.




## Audit Actions

 From May 2020 to February 2021 the State Comptroller's Office examined aspects related to ICT preparation by government ministries for remote work and its implementation during the Covid-19 pandemic period. The audit was conducted at the Information and Communication Technology Authority (the ICT Authority), and supplementary examinations were carried out at five government ministries: the Ministry of Interior, the Ministry of Transport and Road Safety, the Ministry of Science and Technology, the Ministry of Justice and the Ministry of Environmental Protection, as well as at the Civil Service Commission, the Ministry of Finance and the Israel National Cyber Directorate in the Prime Minister's Office.

## Key findings



 **Formulation of an ICT policy for remote work** – The ICT Authority has published several directives dealing with remote work that focus mainly on aspects of information security and business continuity. However, these directives do not comprise an overall policy on the subject of remote work and do not address a range of ICT-related aspects, such as: the infrastructure and equipment needed by employees for optimal work performance; government services that can (or cannot) be provided via remote work; possible alternatives for implementing this work model and the role of the cloud in remote work.




**Business continuity plan** – It was found that as of November 2020, 21 (57%) of 37 audited government ministries had not formulated a business continuity plan to ensure the continued normal functioning of the organization. Regarding the five government ministries that underwent a specific audit, it was found that the Ministry of Transport and the Ministry of Science and Technology had not completed the formulation of a business continuity plan, while the Ministry of Interior, the Ministry of Justice and the Ministry of Environmental Protection had business continuity plans in place at that time, but only one – that of the Justice Ministry – also dealt with remote work.





**Infrastructure aspects** – An analysis of the ICT Authority's data shows the following: at the onset of the covid-19 pandemic in March 2020, 19 of 42 government ministries (45%) indicated that all employees requiring a remote connection had a desktop or laptop computer (or any other means of connection) enabling them to connect remotely; 22 government ministries (52%) indicated that they did not have enough computers to allocate to all the employees requiring a remote connection, while one ministry did not respond to the question; 19 government ministries (45%) stated that their systems had




coped with the load and enabled normal and continuous remote work, two of the ministries (4%) stated that their systems were not able to cope with the load, and the other ministries did not respond to this question or stated that they were working to acquire the missing equipment and infrastructure so that all employees having to work remotely would be able to do so. At that time, the government ministries and government hospitals were lacking some 2,500 laptops, and they took a variety of steps to expand the scope of remote work. Thus, for example, old computers intended for scrap were brought back into use, computers were allocated to employees by rotation and adjustments were made to employees' private computers. It should be noted that several months after the outbreak of the pandemic, an improvement was apparent in the ability of the government ministries to support this mode of work.

 **Implementation of controls for secure remote access** – To minimize the risks inherent in remote work, it is necessary to implement various controls enabling information protection, monitoring of unusual activity and documentation. An analysis of data of the ICT Authority's Cyber Risk Unit (CRU) shows that as of December 2020, all the government ministries that were audited, apart from one (35 ministries), met the controls designated by the CRU as threshold conditions for secure remote access. However, differences were found in the implementation of other controls: in 15 of the audited ministries (41%) there is no identification and authentication of the device initiating the remote connection; in ten ministries (27%) no check is carried out when a computer connects to the network to verify that it has an antivirus program installed on it; in three ministries (8%) there is no restriction on the number of connections one user is allowed simultaneously; in five ministries (14%) access to the ministry systems is not enabled solely via a dedicated hardened component; in ten ministries (27%) access is not restricted to IP addresses from Israel only, and in three ministries (8%) the remote access systems are not linked to a monitoring system. Additionally, an analysis of the data shows that one ministry has not implemented four of the additional controls, while three ministries have not implemented three of the additional controls.

 **Compliance with ISO 27001<sup>2</sup>** – It was found that as of February 2021, six of the 40 government ministries subject to CRU guidance were not in compliance with ISO 27001, although they were required by the relevant Government decision to be in compliance already in February 2020.

 **Performance of penetration testing** – It was found that the controls carried out by the CRU on government ministries include penetration tests to evaluate the security of the organization, but these tests did not include an aspect of remote work.

 **Use of instant messaging software** – It was found that government ministries are forced to use commercial instant messaging software, mainly due to the lack of a secure quality alternative to these products. This results in exposure of organizational

---

2 International standard for information security in an organization.



information and significantly increases its accessibility to unauthorized and malicious elements. The information stored on a device is unprotected and unmanaged and thus exposed to the simplest malware. In 2020 the CRU examined the possibility of providing the government ministries with a secure instant messaging system with end-to-end encryption, but the development of this application was not advanced.



**Employees' user experience** – Findings based on employee surveys conducted during the emergency period and the period of work under the Purple Badge<sup>3</sup> restrictions (restrictions on gatherings and occupancy ratios) show that approximately one third of workers reported that they had experienced problems with their remote connection. The findings show, furthermore, that it is necessary to provide training for employees, in order to improve the ability to work remotely and to ensure that the work is performed efficiently.



At the onset of the Covid-19 pandemic, in March 2020, the government ministries had the necessary remote access infrastructure for work from home – 95% of the ministries indicated that there was remote access to the infrastructures and operating systems required for regular and continuous work. The deficiencies noted related mainly to the need to expand the infrastructure and means of remote access in order to meet the needs of the ever growing number of employees working from home. In July 2020, several months after the outbreak of the pandemic, an improvement was apparent in the ability of the government ministries to support this mode of work. The State Comptroller's Office notes positively the progress in the preparedness of the government ministries for remote work and the controls carried out by the ICT in this regard.






## Key recommendations



It is recommended that the ICT Authority formulate an ICT policy for remote work, after mapping the current situation, performing a needs analysis and defining the desirable situation, while identifying challenges and opportunities in the near and far term. The policy will serve the government ministries as a reference when considering and formulating their own policy on remote work, and may also help the Civil Service Commission and the Finance Ministry in examining the feasibility of applying the remote work model more broadly to the civil service.

3 Amendment No. 7 to the Emergency Regulations (Limiting the Number of Workers in the Workplace to Reduce the Spread of the New Coronavirus) 2020, Government Decision 5037 (May 2, 2020).



-  It is recommended that the relevant government bodies, including the Ministry of Finance, the Tax Authority, the Labor Branch at the Ministry of Labor, Social Affairs and Social Services and the National Insurance Institute examine, in collaboration with the Ministry of Justice, the need to regulate the transition of the labor market to remote work and to create conditions enabling the expansion of the remote work model to the entire economy. In this context, thought should be given to various issues, among them the determination of employer and employee rights and obligations, the economic and social feasibility of this work model and its effects on different employment sectors.
-  It is recommended that the 21 government ministries that have not yet completed the formulation of a business continuity plan complete it in accordance with the CRU's instructions. The ICT Authority should follow up the implementation of the directive issued in November 2020 regarding preparations for business and operational continuity in an emergency, including the need to enable remote access in a crisis.
-  It is recommended that the government ministries continue strengthening in normal times the infrastructures required for remote work, to ensure a complete and flexible solution in emergencies when it is necessary to enable a stable and secure remote work environment for larger numbers of workers. They should also draw up a procurement plan that meets all the needs for this purpose, based on a policy to be determined by them. This is especially necessary in government ministries that used temporary solutions to provide an immediate response during the Covid-19 pandemic.
-  It is recommended that in view of the expansion in the scope of remote work during the Covid-19 pandemic and the understanding that remote work may become part of the normal work environment in the future, and considering the risks inherent in this work model, the CRU should continue working with the government ministries to ensure that they meet all the information security controls specified in its directives; it should instruct the government ministries to complete an up-to-date risk survey to determine which changes have occurred in their mode of work (remote work, incorporation of new systems, technological changes, changes in business processes) and perform penetration tests including tests on the remote connection; and it should complete the development of a government instant messaging system and put it into operation as soon as possible.
-  It is recommended that the Civil Service Commission consider, in collaboration with the government ministries, the circumstances under which it will be possible to work remotely at a level of effectiveness that compares satisfactorily with work in the office; it should also verify if the control tools established in the Civil Service Commission directives during the Covid-19 period are adequate or there is room for developing additional tools to provide an effective and convenient solution in this regard. Additionally, the officials in the Civil Service Commission and in the Ministry of Finance who are studying the feasibility of a wider application of the remote work model in the civil service should also consider the aspect of the work environment in the home, including the equipment required by the worker for working remotely (such as a fast internet connection, a desktop or laptop, an ergonomic chair, a keyboard, earphones and cameras).



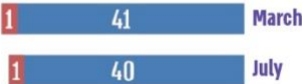


**Degree of government ministries' preparedness for remote work, based on the number of ministries that responded to each of the questions in the survey, March and July 2020**

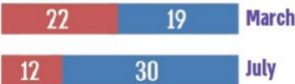
Yes - ■ No - ■ In progress - ■



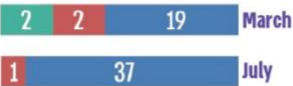
Is there remote access to the operating systems required for these employees?



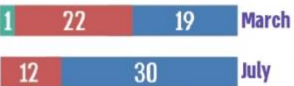
Do all the employees requiring a remote connection have a laptop/desktop computer (or any other means of connection) enabling a remote connection?



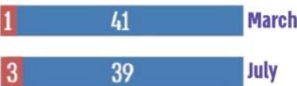
Were the systems able to cope with the heavy load, allowing regular and continuous work?



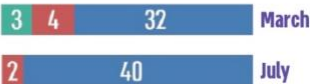
Was a trial remote connection performed under a heavy traffic load?



Is there remote access to the required IT infrastructure systems (management servers, communication, storage, etc.)? Was a trial remote connection performed under a heavy traffic load?



Was a trial performed to test for remote support capability (system)?



Was the support center of the Digital Technologies and Information Department able to provide a remote solution?





---

---

## Summary

While Covid-19 pandemic is a medical, economic and social crisis on a global scale, it has also opened up opportunities. The regulation of remote work over the long term alongside work in the office offers an opportunity to create a new reality in which the advantages inherent in this mode of work can be realized, while contending with the challenges it presents. Such regulation will enable government ministries to improve their preparedness for operational continuity, allowing them to continue providing services with optimal efficiency to the residents of Israel in both normal times and emergencies, especially in view of the ongoing need to cope with the Covid-19 pandemic and to prepare for environmental and other global challenges that lie ahead.