

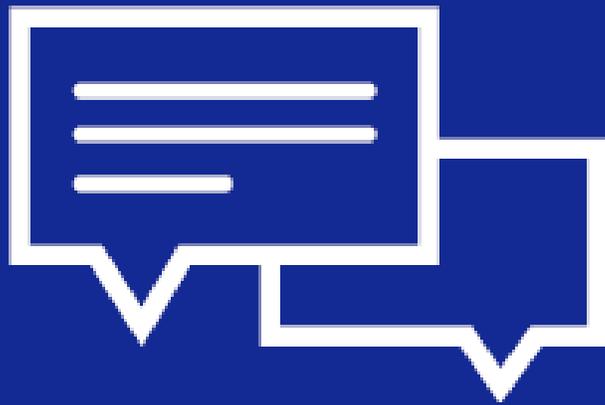


Pan American  
Health  
Organization



World Health  
Organization

REGIONAL OFFICE FOR THE Americas



# IS4H TOOLKIT KNOWLEDGE CAPSULES

**TECHNOLOGY READINESS IN  
PUBLIC HEALTH**

---

DEPARTMENT OF EVIDENCE AND INTELLIGENCE FOR  
ACTION IN HEALTH  
PAHO/WHO

[www.paho.org/ish](http://www.paho.org/ish)



# Information Systems for Health Toolkit

## Knowledge Capsules

# Technology Readiness in Public Health

## IS4H-TR



### Acknowledgments

This work would not have been possible without the technical and financial support of the **United States Agency for International Development (USAID)**, the **Government of Canada** and the **Spanish Agency for International Development Cooperation (AECID)**

**Version 1.0 – July 6, 2019**

Department of Evidence and Intelligence for Action in Health  
Pan American Health Organization - World Health Organization

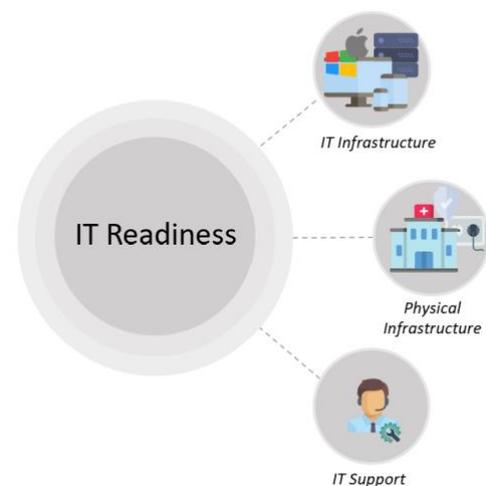
## What is Information Technology (IT) Readiness?

- Many countries are looking to invest in systems to support public health surveillance including the monitoring, protection, prevention, and health promotion of all individuals.
- Large-scale, potentially transformative investments in information technology streamline individual and organizational work processes, and improve the quality, safety, and efficiency of care. However, before investments in IT are made, it is essential for an organization to assess their information technology readiness, which aims to evaluate the preparedness of the organization to support technological change.
- An IT readiness assessment is an assessment of an organization's technical environment, infrastructure and IT service capabilities. By assessing readiness, gaps can be identified which will highlight potential areas for increased planning or procurement prior to implementation.
- Conducting an IT readiness assessment can help prevent common challenges that arise with IT implementations, and thereby ensure the successful adoption of information technology systems in an organization.

*Information technology readiness assessments help to prepare organizations for technological change. The assessment investigates the physical and technical environment of an organization and helps to identify any gaps prior to implementation.*

## What domains should be evaluated to determine your organization's IT readiness?

- The IT readiness domains listed in the table below provide a framework which outlines what an organization should consider before implementing an IT system.
- The framework considers not only the technical requirements such as the hardware, software, and supporting devices, but also assesses the organizations facilities such as the power supply and the temperature needed to support and maintain the systems in place.
- These assessments enable a comprehensive understanding and appraisal of the systems surrounding the new technology, thereby ensuring that no unforeseen complications disrupt technology implementations and adoptions.



## Additional factors to consider when conducting a readiness assessment:

- Before investing in new technology, assess the technology currently present in the organization or system, and determine if those technologies might be modified or configured to sufficiently support your organization's needs.
- Additionally, organizations should consider the following questions prior to conducting an IT Readiness Assessment:
  - Is the IT aligned to support the goals and operations of the organization?
  - Is the IT aligned to support the key business requirements and workflow of end users? Are there any opportunities for improvement or these workflows?
  - Is the IT system and architecture sufficiently robust to support anticipated growth throughout the upcoming years?

<i>Domain</i>	<i>Examples</i>	<i>Description</i>
IT Infrastructure		
<b>End-User Devices</b>	<ul style="list-style-type: none"> <li>• Workstations</li> <li>• Laptops</li> <li>• Tablets</li> </ul>	<ul style="list-style-type: none"> <li>• Analyze user workflows to determine whether existing devices meet needs in terms of number and availability, location, features, and mobility. If current devices are insufficient, consider investing in additional hardware. If users are supported, proceed with assessment.</li> </ul>
<b>Software</b>	<ul style="list-style-type: none"> <li>• Business applications</li> <li>• Operating System</li> </ul>	<ul style="list-style-type: none"> <li>• Assess whether the new technology's software will integrate with other software and operating systems, or whether configuration of systems will be necessary. Ensure that the new technology will be sufficiently adaptable to support IT systems in the future, if new systems are added.</li> </ul>
<b>Network</b>	<ul style="list-style-type: none"> <li>• LAN/WAN</li> <li>• Wireless</li> <li>• Routers</li> </ul>	<ul style="list-style-type: none"> <li>• Assess the current network infrastructure and determine whether a wireless or cabled connection is required. Ensure that the network has enough bandwidth, and that there are enough wireless access points.</li> </ul>
<b>Storage capabilities</b>	<ul style="list-style-type: none"> <li>• On-premise</li> <li>• Off-premise</li> </ul>	<ul style="list-style-type: none"> <li>• If on-premise: consider what server types that maximize space and minimize cooling requirements. An above-ground, climate-controlled facility with non-water-based fire prevention must be used for storage.</li> <li>• If off-premise: consider cost and options to maximize control of data while remaining compliant with privacy legislation.</li> </ul>
<b>Information Security</b>	<ul style="list-style-type: none"> <li>• VPN</li> <li>• Firewalls</li> </ul>	<ul style="list-style-type: none"> <li>• Ensure that all patient information will be adequately protected against security threats. Depending on the size and nature of the internet-reliant systems, firewalls may be necessary. Consider whether staff may need to access systems remotely, and whether VPNs may be required.</li> </ul>
<b>Supporting Devices</b>	<ul style="list-style-type: none"> <li>• Kiosks</li> <li>• Printers</li> </ul>	<ul style="list-style-type: none"> <li>• Assess clinical workflows involving supporting devices and determine whether they meet current and future workflow needs once the new technology is introduced (e.g., printers in every consultation room).</li> </ul>
Physical Infrastructure		
<b>Physical Security</b>	<ul style="list-style-type: none"> <li>• Card scanners</li> <li>• Door alarms</li> </ul>	<ul style="list-style-type: none"> <li>• Assess the current physical security measures in place and consider whether they are and will be adequate given the new technology.</li> </ul>
<b>IT Environment</b>	<ul style="list-style-type: none"> <li>• Power supply</li> <li>• Climate control</li> </ul>	<ul style="list-style-type: none"> <li>• Determine whether the physical environment will support the needs of the technology, particularly adequacy and consistency of power supply for all devices, including presence of back-up power sources.</li> </ul>
IT Support		
<b>IT Support Services</b>	<ul style="list-style-type: none"> <li>• On-site vs. off-site</li> <li>• Hardware/software</li> </ul>	<ul style="list-style-type: none"> <li>• Determine whether the on-site IT support will be adequate to support clinical staff, or if additional staff support be required.</li> <li>• If off-site support is required, consider the service level agreement models available from vendors and third parties.</li> </ul>