Workshop on Building Trust in Digital Government Services

Organized by ESCWA in collaboration with AICTO, Internet Society, and ITU.
Beirut, 11-12 Sept-2023

KEY MESSAGES

Key messages resulting from the workshop on Building Trust in Digital Government Services:

Developing Digital Government Services

1- Emerging technologies (such as artificial intelligence, cloud computing, and others) are considered essential for developing businesses and digital government services, especially since they offer additional advantages. National and regional digital strategies should be developed and regularly updated in a flexible manner, such that they include emerging technologies and consider local and societal specificities, rapid technological advancements and pressing developmental challenges.

2- Government entities should prioritize the design principles that focus on citizens when developing digital government services. This includes ensuring ease of use, accessibility, and responsiveness to the needs of citizens. Public sector entities should also engage citizens in the design process, solicit feedback and regularly improve services accordingly.

3- Raising awareness and familiarity of users with the digital government services should be performed when they are launched and when modified. It is essential to clarify the level of privacy associated with their usage and coordinate with the media to ensure their effective dissemination, wide adoption, and utilization in Arab countries.

Cybersecurity

4- All Arab countries can be guided by the Arab Cybersecurity Strategy and its fundamentals (prepared by the Arab ICT Organization) when developing their national cybersecurity strategies. It is advisable to monitor the Global Cybersecurity Index (GCI) - issued by the International Telecommunication Union (ITU), which tracks the development of regulatory, legislative, and procedural frameworks for cybersecurity in Arab countries and the world.

5- Strengthening awareness and political will regarding the enabling environment for cybersecurity are crucial. This can be sought through developing and implementing national cybersecurity strategies or integrating cybersecurity in the development of any national digital strategy, while supporting training and awareness of cybersecurity programmes that cover all sectors and engage all people.

6- Providing comprehensive access and a secure and safe Internet infrastructure are essential, as it is the fundamental lever for digital transformation, as well as relying on the guidelines issued by the Internet Society in this regard. The Public Key Infrastructure (PKI), electronic signatures, and digital identity are crucial components in the process of improving cybersecurity and building trust in digital government services.

7- Efforts should be made to establish Computer Security Incident Response Teams (CIRTs) at the national, sectoral, and regional levels to enhance response to computer security incidents.

Legal Frameworks

8- Legal legislations related to cybercrime should be developed, amended, and enforced and emerging technologies and digital government services should be regulated. It is crucial for Arab countries to comply with international standards and to join international agreements specialized in these fields.

9- Legal and legislative frameworks that govern cyberspace and protect privacy and personal data should be updated and harmonized; and the penalties outlined in personal data protection laws must be tightened to serve as deterrents against misuse.

10- It is essential to develop and adopt new codes of ethics for the use of artificial intelligence, as well as to strengthen research and development efforts for achieving operational security and mitigating cybercrimes while relying on and complying with good international standards.

Building Trust and Security

11- Building trust in digital government services is needed through the adoption of compatibility and interoperability of services and introducing these services to citizens and engaging with them regarding the benefits, risks and privacy associated with their use.

12- All stakeholders, especially the private sector, should be involved in facilitating access to cloud computing and a secure internet infrastructure, as well as in ensuring the safety of online processes for both organizations and individuals.

13- Strengthening coordination and collaboration efforts between Arab countries and various relevant international and Arab organizations, as well as with all stakeholders from the public and private sectors. This aims at exchanging experiences and successful practices, benefiting from Arab and international experiences in all areas related to digital government services and ensuring the security and safety of public and private institutions and individuals.