APCICT
Asian and Pacific Training Centre for Information and Communication Technology for Development
ESCAP

Capacity Building Programme on Digital Government and Cybersecurity for Public Sector Innovation

High-Level Briefing for Senior Officials and Training of Trainers

6-9 July 2026, Manila, Philippines

BACKGROUND

Digital transformation is reshaping governance across the Asia-Pacific region and globally. Governments are increasingly adopting digital technologies to modernize administrative systems, enhance transparency, and deliver more efficient and inclusive public services. Emerging tools such as big data analytics, blockchain, and the Internet of Things are becoming integral to the public sector's innovation and reform agendas. However, with these opportunities come new challenges, including data privacy, cybersecurity, ethical risks, and persistent digital divides.

Digital government remains the broader foundation for public sector transformation. Beyond technology adoption, digital government is about redesigning governance processes to be more agile, participatory, and citizen-centric. It encompasses strategies for open data, whole-of-government and whole-of-society approaches, digital literacy, and the use of emerging technologies for innovation. Countries that have advanced in digital government demonstrate the value of integrated digital ecosystems in driving efficiency, transparency, and trust in government.

As digital government initiatives expand, cybersecurity has become a critical concern for public administrations. The growing reliance on digital infrastructure and interconnected systems exposes governments to an increasingly complex threat landscape, including data breaches, ransomware attacks, and disruptions to essential public services. Protecting government networks, citizen data, and digital assets is no longer solely a technical issue, but rather a governance imperative. Public officials must understand cybersecurity risks, frameworks, and best practices to build resilient digital government environments. Robust cybersecurity governance, including clear policies, institutional accountability, and a well-trained public sector workforce, is essential to sustaining public trust and ensuring the continuity and integrity of digital public services.

The Philippines is among the countries in the region that have made significant strides in advancing its digital government agenda. Through its national digital transformation strategy and the leadership of the Department of Information and Communications Technology (DICT), the Philippines has been actively pursuing digital innovation in public service delivery, expanding e-government services, and promoting digital inclusion. The government has also

recognized cybersecurity as a national priority, with efforts to strengthen the country's cybersecurity posture through policy development, institutional capacity building, and public awareness.

At the same time, sustaining and deepening these gains requires a public sector workforce that is well-equipped with the knowledge and competencies to drive digital innovation and manage cybersecurity risks. Building the capacity of government officials, not only to understand these issues, but also to train and mentor their peers, is critical to ensuring that digital transformation efforts are implemented effectively, securely, and at scale.

In this context, the Department of ICT of the Philippines and the Asian and Pacific Training Centre for ICT for Development (APCICT) are co- organizing the **Capacity Building Programme on Digital Government and Cybersecurity for Public Sector Innovation**. The programme will comprise two components: (1) a High Level Briefing for senior officials of DICT and other government ministries, providing a strategic overview of digital innovation in the context of public sector governance; and (2) a Training of Trainers (ToT) for DICT Philippines, equipping selected civil servants with the knowledge and skills to cascade training on digital innovation and cybersecurity across their respective agencies and teams.

OBJECTIVES

The programme comprises two components, each with distinct objectives.

The High Level Briefing aims to:

- Enhance the awareness and understanding of senior government officials on the opportunities and challenges of digital innovation in public service delivery.
- Provide a strategic overview of global and regional trends, good practices, and frameworks on digital government, to inform policy directions and institutional priorities.
- Foster high-level dialogue and exchange of experiences among senior officials on advancing digital transformation effectively in the Philippine public sector context.

The Training of Trainers (ToT) aims to:

- Equip participants with a strong understanding of digital government principles, frameworks, and strategies, enabling them to effectively train and mentor other public sector officials.
- Build participants' knowledge of cybersecurity risks, governance frameworks, and best practices, so that they can cascade this knowledge within their respective agencies and teams.

- Strengthen participants' capacity to design and deliver training programmes on digital innovation and cybersecurity for public sector audiences.

PARTICIPANTS

The High Level Briefing will be attended by senior officials of DICT and other relevant government ministries and agencies of the Philippines involved in digital transformation, digital government, and cybersecurity policy and governance.

The Training of Trainers (ToT) will be attended by civil servants and training officers of DICT Philippines who are responsible for or engaged in the delivery of capacity building programmes within their organization, and who will serve as trainers and resource persons for the wider cascade of training on digital innovation and cybersecurity across their respective agencies and teams.

DRAFT PROGRAMME

Monday, 6 July 2026	
Time	
08:30 – 9:00	*Registration*
9:00 – 10:00	**Opening Session** **Group Photo**
10:00 – 12:00	**Session 1: High Level Briefing on Digital Government in the AX Era: Opportunities and Challenges** *The briefing provides an introduction and comprehensive overview of the evolution of digital government in the context of rapid technological advancement. By examining the past, present, and future of digital government, the course emphasizes the importance of a strategic approach to developing AI-driven governance, addressing both the opportunities and challenges associated with AI technologies. Selected case studies of AI-based government initiatives will be presented to illustrate practical applications and lessons learned.*
12:00 – 1:30	*Lunch*
	TRAINING OF TRAINERS
1:30 – 2:00	**Self-introduction by Participants**
2:00 – 3:30	**Session 2: Digital Government for Public Sector Innovations and Good Governance** *This session explores how digital technologies are transforming the public sector and enabling innovative governance. It examines the role of digital government in improving administrative efficiency, enhancing transparency, and delivering citizen-centered public services. Through case studies and policy discussions, participants will analyze key technologies such as cloud computing, artificial intelligence, and data-driven platforms, and their implications for public sector innovation and good governance. The session also considers global trends and practical strategies for implementing digital government initiatives, particularly in the context of sustainable development and public sector reform.*
3:30 –3:45	*Coffee Break*
3:45 – 5:00	**Session 2 continued**

Tuesday, 7 July 2026	
Time	
08:30 – 9:00	*Registration*
9:00 – 10:30	**Session 3: Open Data, Data Use, and Data Governance** *This session examines the role of open data and effective data governance in advancing transparency, innovation, and evidence-based policymaking. It explores key concepts, frameworks, and practices related to data sharing, management, and responsible use within governments and across sectors. Participants will learn how open data initiatives can enhance public value, support digital government, and foster collaboration among governments, citizens, and the private sector. The course also addresses critical issues such as data privacy, security, ethics, and regulatory frameworks in the age of data-driven governance.*
10:30 – 10:45	*Coffee Break*
10:45 – 12:30	**Session 3 continued**
12:30 – 2:00	*Lunch Break*
2:00 – 2:15	*DICT Presentation*
2:15 – 3:30	**Session 4: AI as a Driver for Digital Transformation in Government & Action Plan Exercise** *This session explores how AI is driving digital transformation in the public sector. It examines how governments can leverage AI technologies to improve administrative efficiency, support data-driven decision-making, and deliver smarter, more personalized public services.*
3:30 – 3:45	*Coffee Break*
3:45 – 4:45	**Session 4 Continued**
4:45 – 5:00	**Evaluation**

Wednesday, 8 July 2026	
Time	
08:30 – 9:00	*Registration*
9:00 – 10:30	**Session 1: Need for Information Security** *This session introduces the concept of information security, exploring why the protection of information assets is a fundamental concern for organizations in an increasingly digital environment. It examines the various types of information that require protection, as well as the threats and vulnerabilities that put them at risk. Participants will also be introduced to the key standards applied to information security activities, providing a structured approach to managing and safeguarding information.*
10:30 – 10:45	*Coffee Break*
10:45 – 12:30	**Session 2: Information Security Trends and Directions** *This session provides an overview of the evolving threats to information security, examining the latest trends and directions shaping the cybersecurity landscape. It explores the nature and scope of various threats that organizations face, from malicious attacks to unintentional vulnerabilities, and the potential impact these pose to digital systems and data. The session also describes key countermeasures and response strategies that can be adopted to mitigate these threats and strengthen an organization's overall security posture.*
12:30 – 2:00	*Lunch Break*
2:00 – 2:15	*DICT Presentation*
2:15 – 3:30	**Session 3: Session 3: Information Security Activities** *This session draws on examples of information security activities from various countries to illustrate how different governments have approached information security policymaking and implementation. It examines how these country experiences can serve as practical guides and reference points for developing and strengthening national information security policies. The session also highlights the importance of international cooperation in implementing information security policy, recognizing that cybersecurity threats transcend national borders and require coordinated responses across governments and institutions.*
3:30 – 3:45	*Coffee Break*

3:45 – 5:00	**Session 4: Group Discussion**

Thursday, 9 July 2026	
Time	Description
08:30 – 9:00	*Registration*
9:00 – 10:30	**Session 5: Information Security Methodology** *This session describes the internationally used methodologies for information security, covering the three core dimensions of administrative, physical, and technical approaches. It examines how these methodologies are applied in practice to establish comprehensive and layered security measures that protect information assets across different organizational contexts.*
10:30 – 10:45	*Coffee Break*
10:45 – 12:30	**Session 6: Protection of Privacy** *This session traces the evolution of the concept of privacy, examining how its meaning and scope have shifted in response to technological advancements and the growing digitization of personal information. It describes international trends in privacy protection, highlighting the frameworks and regulatory developments that governments and organizations have adopted to safeguard individuals' personal data. The session also provides an overview of Privacy Impact Assessment, with practical examples of how this tool is used to identify and address privacy risks in the design and implementation of policies, programmes, and digital systems.*
12:30 – 2:00	*Lunch Break*
2:00 – 3:30	**Session 7: CSIRT Establishment and Operation** *This session explains the process of establishing and operating a national Computer Security Incident Response Team (CSIRT), covering the key organizational, operational, and technical considerations involved in setting up an effective incident response capability. It discusses the roles and responsibilities of a national CSIRT in detecting, managing, and responding to cybersecurity incidents, as well as the coordination mechanisms needed to function effectively within the broader national cybersecurity ecosystem. The session also presents models of CSIRTs from various countries, offering practical insights and lessons learned that can inform the establishment and strengthening of national incident response teams.*

3:30 – 3:45	*Coffee Break*
3:45 – 4:45	**Session 8: Lifecycle of Information Security Policy** *This session provides an overview of the information security policymaking process, tracing the key stages involved in developing, implementing, reviewing, and updating information security policies over their lifecycle. It discusses the critical issues and considerations that policymakers must navigate in crafting effective information security policies, including the need to balance security requirements with operational realities, stakeholder interests, and evolving threat landscapes.*
4:45 – 5:00	**Evaluation & Certificates** **Closing**