Understanding the Importance of the Turkish Information and Communication Security Guide on Cybersecurity

Countries around the world are looking to invest in infrastructure that will allow for the use and dissemination of innovative technologies. The infrastructure should ensure that data are processed and interpreted within national boundaries. With this in mind, Turkey has taken significant steps to aggregate cybersecurity coordination following its transition to a presidential government system. These steps include developing domestic and national innovative technologies, promoting national software, protecting critical infrastructures, and utilizing big data and artificial intelligence (AI).[1] To better align the fragmented activities of digital transformation, cybersecurity, national technologies, big data and AI with advancing technologies, social demands, and reform trends in the public sector, the Digital Transformation Office of the Presidency of the Republic of Turkey was established on 10 July 2018.[2] The Digital Transformation Office then published the *Information and Communication Security Guide*, the first reference document specific to Turkey, on 24 July 2020.[3]

The main goals of the Guide are to:

- Mitigate information security risk
- Contribute to the continuity of business processes
- Determine the responsibilities within the organization by using responsible, accountable, consulted and informed (RACI) charts and provide awareness of information security
- Protect the organization's reputation
- Minimize potential tangible and intangible losses

By means of these goals, the guide plays an important role in closing the information and communication security gap in Turkey's public organizations and organizations within Turkey's critical infrastructures.

Understanding the Guide

The Guide is applicable to public organizations and organizations within the critical infrastructures that host IT systems or access IT systems through third-party institutions. It includes five chapters, 15 main sections (**figure 1**), 62 subsections and 661 items of security measures. The chapters are:

1. Introduction
2. Implementation Process of the *Information and Communication Security Guide*
3. Security Measures for Asset Groups

TOLGA MATARACIOGLU | CISA, CISM, COBIT FOUNDATION, BS 25999 LA, CCNA, CEH, ISO 27001 LA, MCP, MCTS, VCP

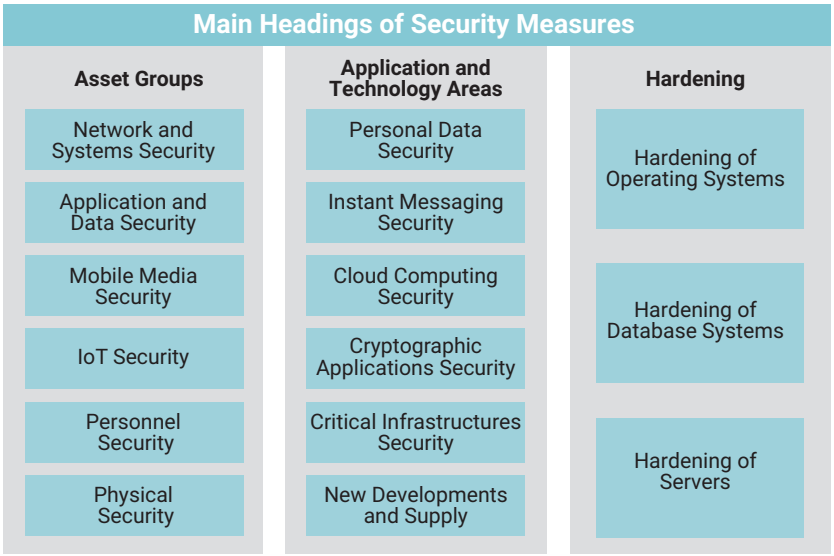
Is chief researcher at the Scientific and Technological Research Council of Turkey (TÜBİTAK) Informatics and Information Security Research Center (BİLGEM) (Turkey). He is the author of many papers about information security published nationally and internationally. His areas of specialization are system design and security, operating systems security, information security management systems, business continuity, COBIT® and social engineering.

© 2022 ISACA. All rights reserved. *www.isaca.org*

4. Security Measures for Application and Technology Areas
5. Hardening Measures

FIGURE 1

Main Sections of the Information and Communication Security Guide



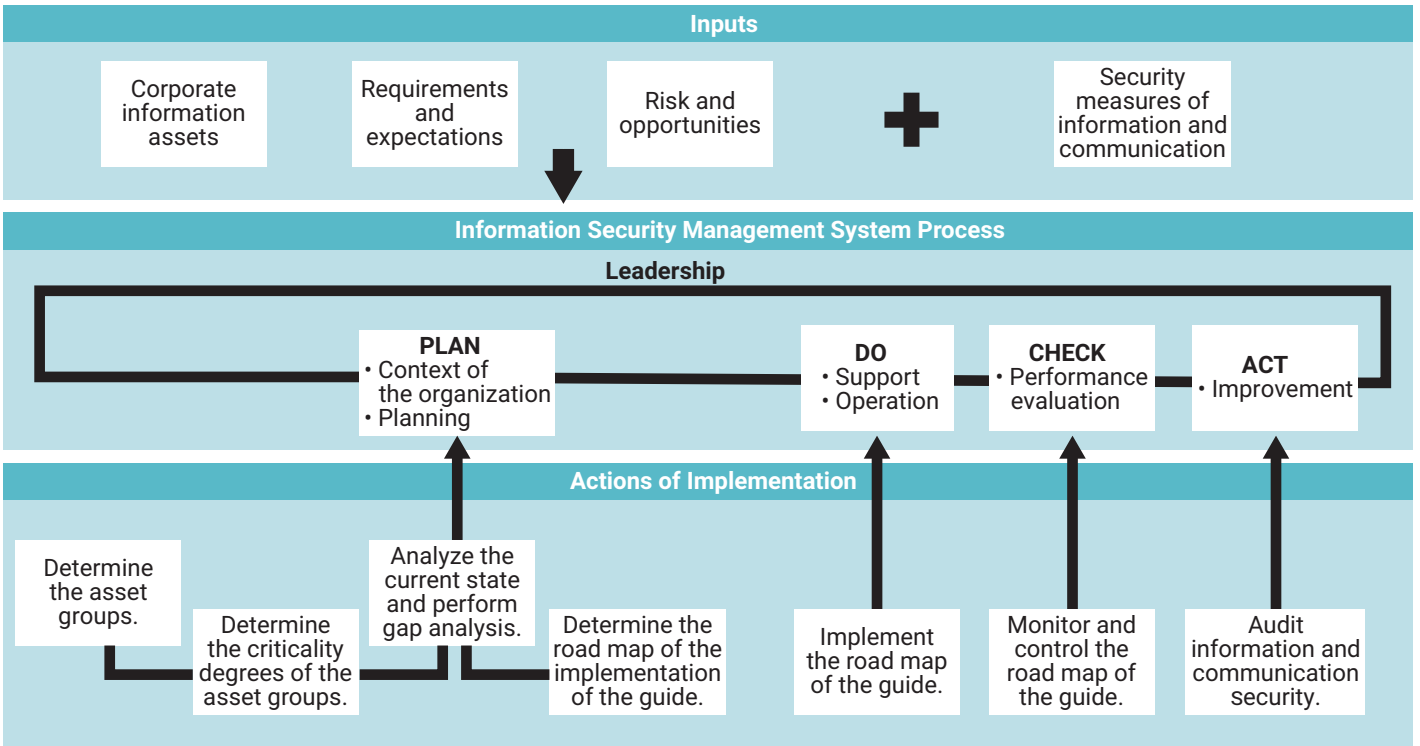
Organizations within the scope of the document must integrate the Guide's information security management system processes and implement its security measures, according to the Presidency of the Republic of Turkey Digital Transformation Office.[4] Implementing the security measures defined in the office, including the security measures defined in the *Information and Communication Security Guide*, is required for all public institutions and critical infrastructure service providers in Turkey.

The implementation process of the guide is compatible with the Plan-Do-Check-Act (PDCA) cycle (**figure 2**). The PDCA cycle is an iterative design and management method used in business for the control and continuous improvement of processes and products. It is also known as the Deming cycle.

In the plan phase of the PDCA cycle, asset groups are determined, along with their degrees of criticality. Next, a current-state analysis and gap analysis are performed. Actual implementation of the guide is performed in the Do phase of the PDCA cycle. In the Check and Act phases, the road map of the guide is monitored and controlled. Finally, an information and communication security audit is performed by the internal auditors of the organization.

FIGURE 2

The Relationship Between PDCA Cycle and the Information and Communication Security Guide



© 2022 ISACA. All rights reserved. www.isaca.org

Planning the Guide Implementation Process

This phase consists of determining the asset groups and the degrees of criticality of the asset groups, analyzing current state and performing gap analysis, and determining the implementation road map.

- **Determining the asset groups**—The enterprise's assets must be organized according to the groups named in the Guide:
  - **Networks and systems**—Router, modem, switch, virtual network, end user computer, server, firewall, intrusion detection systems (IDS)/intrusion protection systems (IPS), supervisory control and data acquisition (SCADA) system, remote terminal unit (RTU), programmable logic controller (PLC)
  - **Applications**—Personnel application, internal portal, main service application
  - **Removable media**—Smart phone, tablet, laptop, universal serial bus (USB), CD/DVD
  - **Physical media**—Data center, disaster recovery center, personnel room, manager room, floor switch room
  - **Internet of Things (IoT) devices**—Camera, sensor (measuring humidity, gas, temperature)
  - **Personnel**—Board member, manager, system administrator, developer, end user
- **Determining the criticality degrees of the asset groups**—Criticality degrees of each asset group must be determined using the Asset Group Criticality Degree Rating Survey in the Guide. The survey contains eight questions regarding eight dimensions of information security:
  1. Confidentiality
  2. Integrity
  3. Availability
  4. Dependent assets
  5. Impacted amount of users
  6. Corporate results
  7. Sector-specific impacts
  8. Social results
- **Analyzing current state and performing gap analysis**—The current state of the asset groups is determined based on:
  - Security measures for asset groups
  - Security measures for application and technology areas
  - Hardening measures
- **Determining the implementation road map**—The actions needed for determining the road map include:
  - Skill development and training
  - Product supply
  - Service procurement
  - Consultation
  - Development
  - Design
  - Hardening
  - Version updating
  - Documentation
  - Corporate process remediation

Implementation of the Road Map

Once the implantation plan is determined, the applicable actions are taken to follow the road map. The main principles to consider when implementing such actions are shown in **figure 3**.

During implementation, progress should be tracked.

Audit principles must be based on the *Information and Communication Audit Guide* published by the Digital Transformation Office of Turkey.[5]

Further, change management protocols concerning updates to the Guide's asset groups must be established in the organization.

Security Measures for Asset Groups

Several components should be taken into consideration so practitioners can harden their organizations' network and system assets, including:

- **Network and system security**—Asset inventory management, threat and vulnerability management, email security, network security, logging, virtualization security, event management, business continuity management, and remote working
- **Application and data security**—Authentication, file and source security, secure installation and configuring, secure software development, log management, and communication security

JOIN THE DISCUSSION

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

© 2022 ISACA. All rights reserved. *www.isaca.org*

FIGURE 3

Main Principles for Implementation

- **Mobile media security**—Smart phone and tablet security, portable computer security, and removable media security
- **IoT security**—Internal data storage, authentication and authorization, and application programming interface (API) and connection security
- **Personnel security**—Topics such as training and awareness and supplier relations security
- **Physical media security**—Data center security and Telecommunications and Electrical Machinery Protected from Emanations Security (TEMPEST)

Security Measures for Application and Technology Areas

Personal data, instant messaging, cloud computing, cryptographic applications, critical infrastructures (e.g., energy and electronic communications), new developments and supply topics are all growing in popularity and use and, therefore, must be taken into consideration so practitioners can improve the security of their organizations' application and technology areas. Since protecting critical infrastructures is imperative in today's information security world, this topic, especially the security measures for energy and electronic communications areas are included.

Hardening Measures

Hardening is a key security measure against cyberattacks. All organizations use servers (i.e., database servers or web servers) and those servers' operating systems. Therefore, Linux and Windows operating systems, database systems, web servers, and visualization servers topics must be taken into consideration so practitioners can harden them.

The Relationship Between the Global Cybersecurity Index and the Guide

To understand the role and importance of the Guide and its contribution to Turkey's information and communication security, the ITU Global Cybersecurity Index (GCI) should be understood. The GCI is an initiative of the International Telecommunication Union (ITU), a specialized United Nations agency for information and communications technologies (ICTs). The GCI is shaped and improved by the work of a diverse range of experts and contributors within countries and other international organizations,[6] and it maps member-state cybersecurity commitments across five dimensions:[7]

1. **Legal measures**—Based on the existence of legal frameworks dealing with cybersecurity and cybercrime
2. **Technical measures**—Based on the existence of technical institutions and frameworks related to cybersecurity
3. **Organizational measures**—Based on the existence of coordination institutions, policies and strategies for cybersecurity development at the national level
4. **Capacity development measures**—Based on the existence of research and development, education and training programs, certified professionals, and public sector agencies fostering capacity building
5. **Cooperation measures**—Based on the existence of partnerships, cooperative frameworks and information-sharing networks

The *Information and Communication Security Guide* impacts all five dimensions of the GCI, and in 2020, Turkey scored 97.49 points and ranked 11th and 5th place in the global and European rankings, respectively.[8]

© 2022 ISACA. All rights reserved. *www.isaca.org*

Conclusion

Practitioners must understand the *Information and Communication Security Guide* to use it effectively to help close the information and communication security gap in public organizations and organizations within the critical infrastructures. Practitioners and enterprises who are not subject to the Guide can use it as a resource to improve their security practices.

The Guide addresses a diverse group of security measures that are growing in popularity and importance, including asset groups, application and technology areas, and hardening. The Guide implementation process has been designed to feed these security measures, similar to other successful standards used throughout the world such as International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) standards ISO/IEC 27001 and ISO/IEC 27002. As organizations implement the security measures stated in the guide, Turkey's rank will continue to progress in the ITU GCI.

Author's Note

The author would like to thank Derya Cincioglu from the Digital Transformation Office of Turkey for assistance creating the figures within this article.

Endnotes

1 KOC, A.Taha; "Message from the GCDO," Presidency of the Republic of Turkey Digital Transformation Office, Turkey, *https://cbddo.gov.tr/en/message-from-the-cdo*

2 Presidency of the Republic of Turkey Digital Transformation Office, "About DTO," Turkey, *https://cbddo.gov.tr/en/about-dto*

3 Presidency of the Republic of Turkey Digital Transformation Office, "Information and Communication Security Guide," Turkey, 27 July 2020, *https://cbddo.gov.tr/en/announcements/4848/bilgi-ve-iletisim-guvenligi-rehberi-yayimlandi*

4 Presidency of the Republic of Turkey Digital Transformation Office, *Information and Communication Security Guide*, Turkey, 2020, *https://cbddo.gov.tr/en/icsguide/*

5 Presidency of the Republic of Turkey Digital Transformation Office, *Information and Communication Security Guide*, 2020, *https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf*

6 International Telecommunication Union (ITU), *Global Cybersecurity Index 2020*, Switzerland, 2021, *https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/*

7 *Ibid*.

8 *Ibid*.

© 2022 ISACA. All rights reserved. *www.isaca.org*