MOROĞLU ARSEVEN

Digital Transformation Office of the Presidency of Turkey has published the Guideline on Information and Communication Security Audit

24 Dec 2021

In accordance with the Presidential Circular on Information and Communication Security Measures published on 6 July 2019, public institutions and businesses providing critical infrastructure services are obliged to implement certain security measures in order to reduce and neutralize the security risks encountered and to ensure the security of critical types of data that may threaten national security or cause disruption of public order, when their confidentiality, integrity or accessibility is impaired.

In this direction, the Digital Transformation Office of the Presidency of Turkey has published the Guideline on Information and Communication Security ("**Guideline**") on 27 July 2020, which includes measures at different security levels.

The audit process, which is one of the steps that institutions must fulfill while adapting to the Guideline, is regulated by the Guideline. Institutions included in the Guideline are expected to carry out certain studies in planning, implementation, managing changes, controlling and taking precautions. In order to carry out the audit, which is a part of the process of controlling and taking precautions, at least once a year, it is envisaged that the necessary plans to be made and operated by the institutions.

Following the Guideline, on 27 October 2021, the Guideline on Information and Communication Security Audit ("**Audit Guideline**") has been prepared in order to guide the institutions and auditors in the independent planning, execution and reporting of the audit.

With the Audit Guideline,

- Institutions have been given a 24-month adaptation period as of 27 July 2020, the publication date of the Guideline. In the first-year audits, institutions should start the preparatory work related to the audit activities at the end of the 24-month period at the latest. However, institutions that have completed their compliance work before 24 months have been given the opportunity to start the preparatory work for the audit activities without waiting for the compliance period to expire.
- For all institutions within the scope of the Guideline, it is essential that audit activities are primarily carried out by internal auditors who work in internal audit units and are assigned to audit in the field of information technologies. In enterprises providing critical infrastructure services, regulatory and supervisory institutions may also carry out audit activities in accordance with the Audit Guideline within the framework of their relevant legislation.
- In cases where internal audit units are absent, insufficient or incompetent to carry out the audit, audit activities can be carried out through other in-house personnel, personnel to be assigned from other public institutions and organizations, or service procurement in order to ensure that audit activities are carried out independently.

- In case the institution has an ISO/IEC 27001 compliant Information Security Management System ("**ISMS**") installation, operation and certification obligation in line with the legislation that it is currently obliged to comply with, and if the ISMS scope and the Audit Guideline compliance scope are the same within the framework of this obligation, ISMS internal audit studies and Audit Guideline compliance audits can be carried out under a single audit. However, the information and documents that must be submitted to the Digital Transformation Office of the Presidency of Turkey as a result of the audit work should be created in accordance with the formats defined in this document. In the audits to be carried out in this way, the measure matching tables to be published at https://cbddo.gov.tr/ can be used.
- The minimum obligations to be complied with in the audit service procurement contract for the institutions, the firms and the auditors are as follows:
- To obtain the audit service from companies authorized within the scope of the Certification Program.
- Not to have received more than three consecutive audit services from the company from which audit service will be provided.
- To include the purpose and scope of the audit, and the conditions for termination of the contract in the contract.
- To include in the contract the measures under the title of "Supplier Relationship Security" in the Guideline in accordance with the information security requirements of the institution.
- The methodology to be applied in the Guideline compliance audit proceeds in three main process axes: planning the audit, applying the procedures and reporting the results. In the planning of the audit, which is the first stage, the audit team should be determined. Then, the institution needs to be understood and the scope of the audit should be determined as the next step. Once the scope is determined, the audit strategy and program need to be established. After these are completed, the implementation of the audit procedure begins. At this stage, the effectiveness of the Guideline implementation process is evaluated first, followed by the effectiveness of the measures. Finally, the findings are identified, evaluated and monitored. At the end of all these stages, an audit report is prepared and submitted to the authority. Each page of the documents that make up the audit report, including the annexes, is signed by the auditors in the audit team with a secure electronic signature created in accordance with the provisions of Electronic Signature Law numbered 5070, and the report is finalized. Audit team should only record the scope of the audit, the size of the audit file submitted to the agency, the summary (hash) information of the file and the date of delivery, and keep them electronically. The audit team should not take any other document or other information out of the institution. The audit results, corrective and preventive actions will be submitted to the Digital Transformation Office of the Presidency of Turkey as a report in accordance with the procedures and principles specified in the Guideline.
- Within the scope of the Guideline compliance audit, a confidentiality agreement must be signed within the scope of Personal Data Protection Law numbered 6698, in order to specify the information obtained or produced by auditors/experts in the audit team during the audit work and the principles of use of the information assets they use, to define their responsibilities and to inform the relevant person of their responsibilities.

You can access the full text of the Audit Guideline via this link. (Only available in Turkish)