GÜN + PARTNERS
AVUKATLIK BÜROSU

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

Audit Standards for Information Security Processes

Introduction and Developments

With the Presidential Circular on Information and Communication Security Measures which came into force once published on July 6, 2019 (the "Circular"), it was aimed to mitigate and neutralize serious security risks encountered in the digitalization process and ensure the security of critical data for public institutions and organizations and enterprises providing critical infrastructure services.

The Information and Communication Security Guide ("Security Guideline") was also prepared by the Digital Transformation Office ("DTO") in order to explain how the Circular and the measures under the Circular would be implemented and the security measures was regulated in the Security Guideline accordingly. You can refer to our Article named "Developments for Local Storage in Turkey" for our evaluation about the Circular and the Security Guideline as well as applicable sanctions in case of any incompliance.

The Circular also states that institutions and organizations shall establish an audit mechanism for the implementation of the Security Guideline, audit the implementation at least once a year and report the results of the audit and any corrective and preventive actions to DTO in accordance with the principles and procedures determined under the Security Guideline. It was underlined that the relevant audit activities shall be performed in accordance with the Information and Communication Security Audit Guideline ("Audit Guideline"); however, the Audit Guideline was not published together with the Security Guideline.

The Audit Guideline (available in Turkish here) prepared by DTO which regulates practicing audit procedures and reporting of the audit results was published on October 27, 2021. Besides the Audit Guideline, DTO announced that a certification program was realized by DTO in cooperation with Turkish Standards Institution and Scientific and Technological Research Council of Turkey in order to certify auditors and firms ("Certification Program").

GÜN + PARTNERS
AVUKATLIK BÜROSU

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

The relevant institutions and organizations are required to plan and realize an audit once a year at least with regard to their information security processes as part of their processes to plan, implement, revise if deemed necessary, control and take necessary actions for studies required to be conducted for the Security Guideline. The audit shall be performed in accordance with the Audit Guideline.

Scope of the Audit Guideline

The Audit Guideline shall also apply to public institutions and organizations as it is regulated under the Circular and Security Guideline. On the other hand, although the Circular refers only to public institutions and organizations with regard to the obligations about audit, it is clear that the Audit Guideline is also important for enterprises providing critical infrastructure services. We are of the opinion that the Audit Guideline is also applicable to enterprises providing critical infrastructure services. Still, a new document about frequently asked questions about Audit Guideline will also be published and this is expected to clarify the scope of the Audit Guideline.

Furthermore, in addition to public institutions and organizations as well as enterprises providing critical infrastructure services, as the Circular and Guide, obligations imposed on these institutions with the Audit Guideline will also affect private legal entities who provide services to such institutions within the scope of the Audit Guideline. Consequently, we are of the opinion that the Audit Guideline may also be indirectly applicable to suppliers and business partners of public institutions/organizations and enterprises providing critical infrastructure services.

Principles of the Audit Guideline

Except for the general explanations about the purpose and structure of the Audit Guideline, it consists of 3 parts as follows.

GÜN + PARTNERS
AVUKATLIK BÜROSU

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

1. Preparation For Audit Studies

As of July 27, 2020, the Security Guideline introduced a 24-month implementation period consisting of various stages. Within this scope, the subjects of the Audit Guideline shall start their preparation for their first audit activities based on the Audit Guideline on July 27, 2022 at latest.

The Audit Guideline imposes that the audit activities shall be performed with internal auditors in principle, but it is clearly emphasized that especially for enterprises providing critical infrastructure services, the legislation of the supervisory public authorities shall also be considered for audit activities.

In addition, for cases when enterprises providing critical infrastructure services and institutions/organizations which do not have internal auditors outsource the audit activities, all obligations of the institutions subject to audit and auditors have also been explained under the Audit Guideline.

Under the Audit Guideline, there are also explicit obligations with regard to contracts to be executed for audit services to be outsourced. In this respect, the following matters shall be taken into consideration by the persons in the scope of audit when they negotiate with the audit companies:

- The company which will provide audit services required by the Audit Guideline shall have been certificated within the context of the Certification Program.
- The company which will provide audit services required by the Audit Guideline shall not have provided to the institution subject to the audit any consultancy services regarding compliance with the Security Guideline in the last 2 years.
- The relevant company can provide audit services for a maximum of 3 consecutive years to an institution subject to the audit.
- The contract to be signed with the audit company shall explicitly include some issues directly regulated under the Audit Guideline (and therefore shall be subject to a legal review for confirmation).

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

- The audit company and their personnel shall be subject of strict confidentiality obligation. In this context, the institution under the audit requirement shall provide the audit company with complete and accurate information about all the studies made in electronic or physical environment with regard to audit process, infrastructure and security implementation processes, which also requires the institutions to arrange all information about their security processes as to be recorded in a systematic way in order to be ready for the audit. The institution shall also provide sufficient human resources to support the audit activities.
- Audit activities may also be conducted at workplaces of the institutions physically.

1. Audit Methodology

The Audit Guideline states that the main purpose of the audit is to evaluate the efficiency of the implementation of the Security Guideline and of measures applied on information technology assets. The teams who should be responsible for audit processes in the relevant institutions are also regulated under the Audit Guideline.

The audit activities shall consist the following 3 steps:

1. Audit Planning

- Determining the audit team: The team must consist of at least two auditors. Qualifications of auditors, ethical audit principles and matters required to be considered for selection of auditors are explained in detail under the Audit Guideline.
- Understanding on the institution subject to audit: In this section, the Audit Guideline regulates how the information will be collected to understand the structure of the institution. In this context, the audit team must examine organization structure, business process, audit reports of previous terms, content of the audit services received from third parties, legal obligations and assets of the institution.

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

- Determining the scope of audit (determining the scope of assets subject to audit): The audit team must adopt a risk-based approach and take into consideration the importance of the assets. The audit team conducts a risk audit regarding the possible consequences (which affect the information and communication security of the institution) of the situations that may arise as a result of the audit.
- Preparing the audit strategy and program: The audit team must determine the audit strategy that addresses how they conduct effectiveness evaluations. Afterwards, an audit program must be prepared in order to carry on the studies within a certain program for the main purposes of the Audit Guideline (i.e., to evaluate the efficiency of the measures applied on assets and the implementation of the Security Guideline).

2. Implementation of Audit Procedures

- Audit methods: It should be determined which audit methods will be implemented. Audit methods consisting of interview, revision, security audit, penetration testing and source code analysis can be implemented. The audit method should be determined in accordance with how the relevant security measure is implemented and the asset in which the relevant security measure is implemented.
- Gathering audit evidence: Audit evidence is all the information and documents obtained during the audit process. Auditors can use audit report and audit findings related to the previous years during gathering audit evidence. Audit evidence should be obtained from a secure source, be suitable and sufficient for the purpose of the measure implemented by the institution and could be reached by any other auditor as well in case of any separate audit activity. Auditors should base on audit evidence gathered by the auditor with regard to its report.
- Evaluation of the effectiveness of the Security Guideline implementation process and the measures taken within the scope of the Security Guideline: The auditor shall evaluate the effectiveness of the Security Guideline implementation process and the measures applied to

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

equipment and assets in general. Some audit questions which may be used for such an evaluation are also provided under the Audit Guideline as a general framework and examples to assist the auditors in this respect. In order to decide whether any measures are effective or not, the auditors shall conduct their studies on a specific sample that has the potential to provide efficient and qualified information regarding the compliance of the relevant institution.

- Detection, evaluation and monitoring of findings: The auditors will reach a finding as a result of the evaluation of the risks that may occur in the information security of the audited institution at the end of the audit. The auditors will classify their findings according to the criticality levels by using the explanations in the finding criticality level table in the Security Guideline about the possibility of the risks to occur and their effects upon evaluation of the deficiencies and risks which may be caused by such deficiencies. The findings will be evaluated in a meeting to be held between the responsible units and/or managers within the scope of the audit in order to evaluate whether the findings are accurate or not. After the evaluation of the detected findings, the relevant findings will be monitored. At this stage, it is necessary to determine and plan corrective and preventive actions to eliminate the findings or reduce the criticality level and to determine who will be responsible for the relevant activities.

3. Reporting of Audit Results (Preparation of Audit Report)

- Audit team shall prepare the audit report if the information and documents are complete and sufficient for them to convey an opinion and if they are convinced that the audit could be completed properly. The audit report will be confidential.

1. Sending Audit Results to DTO

As regulated under the Circular, audit reports will also be sent to DTO. DTO will create a system for reports to be shared. The audit reports must be uploaded to such a system within 2 months from the date of the audit.

GÜN + PARTNERS
AVUKATLIK BÜROSU

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

If the audit activities could not be performed for any reason, this shall be explained to DTO with sufficient reasoning by the management. DTO's role here is to examine the results of the audit reports and to supervise the relevant institutions in accordance with its legislation.

Expected Developments and Conclusion

Preparatory studies for the audit shall be initiated at the earliest convenience. Since the implementation process of the Security Guideline will end on July 27, 2022, it would be appropriate to prepare the first audit report after this date and it must be prepared within 2022 at the latest. It is also expected that DDO publish a 'Frequently Asked Questions' document on matters to be further clarifies with regard to the Audit Guideline.

The process should be followed closely in terms of institutions and enterprises providing critical infrastructure services. There may be sanctions for non-compliance with these regulations for institutions and enterprises providing critical infrastructure services. We would like to emphasize that the binding nature of the Circular, the Security Guideline and the Audit Guideline on private legal persons is still controversial in practice and according to the scholars.

In any case, we think that the Audit Guideline can be taken as a reference together with the Security Guideline for all other data controllers operating an information management system even if they are not within the scope of this regulations in principle. It is possible that these regulations, which are mostly compatible with certification processes applicable to information management systems in terms of data security, may soon be accepted as a minimum standard for the Personal Data Protection Authority in terms of data security.

Special thanks to Atacan Yılmaz for his contributions.