e-Nabız e-Government Project Information Systems Audit (Summary)

Introduction

With the 2016-2019 National e-Government Strategy and Action Plan, the Turkish Court of Accounts (TCA) bears responsibility for "ensuring the efficiency of audit for e-government projects in public sector". In this context; the TCA has created an audit model for egovernment projects, prepared a draft audit guideline concordant with the model, and carried out a pilot audit on e-Nabız Project, which is executed by the Ministry of Health.

Information about the Project

National Health System (USS) is a record system developed and operated by the Ministry of Health in order to create health policies and improve the quality of health services. It aims to collect and process the health data generated in all health institutions and improve the data quality, as well.

e-Nabız, which is a component of the USS and the subject of the audit, is a "national personal health record system" that allows citizens to access their own health data via the internet and mobile devices and share them with their family members and physicians they choose and authorize.

In addition, through e-Nabız, blood, bone marrow and organs can be donated; visited health facilities can be evaluated; healthcare appointments can be made; prescriptions, prospectus and box picture of the medicines can be viewed. Using e-Nabız mobile application, 112 emergency command centres can be contacted and data from mobile health applications and wearable mobile devices can be transmitted to the personal health records.

In September 2016, the Ministry signed a contract with a semi-public software firm and procured the maintenance, repair, development, integration and technical support services for USS for 24 months. The audit was conducted from October 2017 to May 2018 within the framework of the "software modernization project", which includes e-Nabız and is carried out in accordance with the contract mentioned above.

Objective, Scope and Methodology of Audit

e-Nabız Project Pilot Audit aimed at:

- Examination and evaluation of IT controls, which are set to ensure confidentiality, integrity, availability, reliability, efficiency, effectiveness and compliance to legislation of the project itself and the IT environment in which it is executed,

- Contributing to the Institution by identifying the problems that may prevent the

successful completion of the project and by providing recommendations for taking the necessary precautions,

- Providing information about the project to its stakeholders through reporting.

In the audit, the methodology determined in the e-Government Projects Audit Guideline (Draft) was followed. The Guide has been prepared on the basis of COBIT (Control Objectives for Information and Related Technologies), ITAF (Information Technology Assurance Framework), PMBOK (Project Management Body of Knowledge), ISO/IEC 27000 Standard Series and ISSAIs (International Standards of Supreme Audit Institutions).

In this context; the following risk-based audit approach was followed:

1. Identifying the risks related to the Project itself and the IT environment where it is executed,

2. Determination of the controls that can minimize these risks,

3. Examination of whether these controls are established by the Institution, and if so, whether they are functioning effectively,

4. Evaluation of the control weaknesses identified,

5. Reporting of material control weaknesses to the stakeholders.

Besides the project and the application itself, the corporate IT environment and infrastructure (servers, network, databases) and the web and mobile structures, where the application was put into service, have been subject to audit and specific audit tests. The information systems that generate the health data, and the processes related to data transfer were excluded from the scope of the audit.

During the audit; the presence, design and functioning efficiency of the controls specified in following sub-control areas have been examined and evaluated:

Within the scope of **IT Governance Controls;** “Strategic Management”, “Policies and Procedures”, “Organization, Roles and Responsibilities”, “Human Resources and Training”, “Defining Requirements”, “Compliance with Legal and Other Regulations”, “Risk Assessment” and “Asset Management”,

Within the scope of **Project Management Controls;** “Pre-Project Studies”, “Integration Management”, “Scope Management”, “Time Management”, “Budget Management”, “Quality Management”, “Human Resources Management”, “Communications Management” “Risk Management” and “Stakeholder Management”,

Within the scope of **Outsourcing/Procurement Controls;** "Tender Process", "Contract Implementation Process" and "Examination and Acceptance",

Within the scope of **Information Security Controls;** "System Security Requirements Design", "Physical and Environmental Security", "Network Security", "Operating System Security", "Database Security", "Web Application Security" and "Mobile Application Security"",

Within the scope of **Operating and Maintenance Management Controls;** "Service Level Management", "Configuration Management", "Event and Problem Management", "Change Management" and "Capacity Management",

Within the scope of **Business Continuity and Disaster Recovery Planning Controls;** "Business Continuity Organization", "Risk Assessment", "Business Impact Analysis", "Business Continuity Plan", "Disaster Recovery Plan", "Documentation", "Test and Update" and "Backup",

Within the scope of **Application Controls;** "Input", "Data Transfer", "Process" and "Output",

Within the scope of **Project Content and Process Controls;** "Planning", "Design", "Code Development", "Testing", "Acceptance and Installation", "Parallel Running and Monitoring" and "Data Transfer".

Detected control weaknesses have been negotiated with the audited Institution and explained in the Report in such a way as to include the relevant control area, the associated audit criteria, the level of risk, the relevant legislation and/or standards, the possible effects, actions taken by the auditee and the recommendations thereof.

A follow-up audit will be planned and conducted separately.