T.C.
SAYIŞTAY
1862

BELBIS 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 BELBIS Project, which is executed by the Union of Municipalities of Turkey (TBB).

Information about the Project

BELBIS Project was set out in Article 20 of the Local Administration Associations Law No. 5355 within the TBB in 2011 it aims to assist the development of municipalities, train and guide the personnel, encourage cooperation and collaboration between municipalities, technical and administrative experience and information sharing, and help the spread of good practice examples. As stated in Article 7 of the TBB regulation, the project started to operate in order to support the development of e-Municipality with the use and dissemination of its technologies in municipalities.

BELBIS Project is an IT project. TBB develops BELBIS Project in order to provide a standard operation to municipalities with open source code, web-based, modular structure, where municipalities can monitor financial and administrative affairs and transactions. In BELBIS Application, TBB has defined 28 different modules.

With BELBIS Project, it is aimed to eliminate the costs to be incurred by municipalities with its cloud architecture infrastructure, to create inter-module integration, to ensure integration with institutions and e-government, to provide all standard forms used in municipalities from the system, to prevent tax losses and leakage, and to make system users obliged to act in accordance with the legislation.

BELBIS Project is already in progress and TBB is developing it. TBB started the project in November 2010 and determined the technologies and standards to be used in the software in February 2011.

TBB started the analysis and coding studies of the project in July 2011 and opened the modules in the system to pilot municipalities in the test environment starting from mid-2014.

As of 2018, 62 municipalities use various modules of the system in live environment. The number of active users in these municipalities is 752 people. In addition, about 80 municipalities use the test environment. TBB trainers continue to provide training and promotion for the municipalities using the system.

Objective, Scope and Methodology of Audit

BELBIS 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 **ISSAI**s (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.

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.