GocNet 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 GocNet e-Government Project, which is executed by Ministry of Interior, Directorate General of Migration Management.

Information about the Project

The GocNet Project is able to integrate the works and transactions of foreigners to the electronic environment and integrate them with the related institutions and organizations.

The GocNet corporate IT project, which started in 2013 and started to be used in the Directorate General of Migration Management's central and provincial units as of May 2015, has a structure that serves in 46 physical and 210 virtual servers, as a closed circuit. It serves to the Directorate General of Migration Management's central organization, 81 provincial directorates, 14 district directorates and 20 return, acceptance and accommodation centres.

The Project is designed as a closed circuit project on 17 different modules. In addition, IP SEC VPN is integrated with the information systems of numerous public institutions and organizations through point-to-point and public connections.

Objective, Scope and Methodology of Audit

GocNet 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.

Not all the modules of the Application have been subject to application controls Therefore, the audit team has determined the modules to be tested according to the following criteria:

- **Materiality** (The impact of the application on the activities of the Institution and
- financial statements, etc.),
- **Criticality** (Integrity, confidentiality and availability of corporate information, etc.),
- **Complexity** (Number of users, transaction volume, etc.),
- **Technological Infrastructure** (Operating system, software development environment, database, etc.),
- **Control Environment** (Support personnel, documentation, errors, etc.),
- **Audit Resources** (Time and human resources constraints, etc.).

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.