

Performance Audit of the Georgian electronic Government Procurement system

State procurement is one of the key components of public financial management. Its share in state budget is approximately 25 percent. Effective management of state procurements is an important sphere of interest for the State Audit Office.

Considering the fact that since 2010 major part of public procurements is being conducted electronically and there is no alternative tool, uninterrupted provision of a high-quality service has a particular importance.

It is noteworthy that establishment of open, transparent and competitive environment for the procurement parties mitigates the risks of corruption and fraud, which in return supports the successful implementation of country's anti-corruption policy. To develop such environment, the system must provide confidentiality, integrity and availability of existing data through effective procurement policies and procedures.

Having considered aforementioned factors, SAO conducted performance audit of the Georgian electronic Government Procurement system. The audit was aimed to identify system's shortcomings and issue recommendations to eliminate them.

To accomplish audit objectives, the auditors assessed the performance of Ge-GP system's management and control mechanisms. Electronic system's management compliance to relevant laws and regulations has also been studied in the course of the audit.

Keeping in mind the audit objective, the overall audit question was set:

How effective are management and control mechanisms of the Ge-GP system?

In order to answer the overall question, the team defined the following subsidiary questions:

- How effective are IT governance mechanisms of the system?
- Is the effectiveness of system's outsourcing management being ensured?
- Are the Agency's information assets secured?
- To what extent are the system's data confidentiality, integrity and availability being ensured?
- Are the system's management mechanisms in compliance with relevant legal framework or not?

Topics	State activity areas	Controls' groups	Perspective
-protection of information -IT investment	-public finance	- outsourcing - security	- effective state - efficient office

1. Risk-Case

WEAKNESSES IN LEADERSHIP results in WEAK IT GOVERNANCE

Cause	Issue	Impact on
<ul style="list-style-type: none">- There is no formal IT Strategic Plan- Corporate Strategic Plan includes IT objectives, which are not achieved.- There is no Business need identification policies in the Agency	<ul style="list-style-type: none">- Agency has not identified risks related to the business processes- The risks related to the IT are not managed	<ul style="list-style-type: none">effectivenessefficiencyinformation

2. Risk-Case

WEAKNESSES IN OUTSORCING results in INFORMATION SECURITY WEAKNESSES

Cause	Issue	Impact on
<ul style="list-style-type: none">- The Agency has full outsourcing model, but there are no informal and formal policies to manage outsourced services.- Data Right are not regulated- There is no SLA between the Agency and service provider- There is no Business Continuity Plan for outsourced services	<ul style="list-style-type: none">- Risks related to the poor quality service to be delivered to the end-users (society)- Risk of violation of data integrity and leak of information- Risks related to interruption of services	<ul style="list-style-type: none">information

3. Risk-Case

LACK OF LEADERSHIP results in INCOMPLIANCE WITH LEGAL REGULATIONS

Cause	Issue	Impact on
<ul style="list-style-type: none">- State Procurement Agency has Information Security Manager, but there are no Information Security Management Systems (ISMS) required by the Law on Information Security	<ul style="list-style-type: none">- Legal requirements are not satisfied	<ul style="list-style-type: none">information

-		
---	--	--

4. Risk-Case

INEFFECTIVE INFORMATION SECURITY CONTROLS results in NOT ACHIEVING LEGAL REQUIREMENTS

Cause	Issue	Impact on
<ul style="list-style-type: none"> - Weak Application Security Controls in place - The System assigned the same ID to the tenders registered on the exactly same time. - No cryptographic algorithms are used by the system to assure confidentiality of the tender data. 	<ul style="list-style-type: none"> - Information related to some tenders are not always available to the end-users (Transparency Issue required by the Law) - The unique identification number of the procurement is not reliable. There are gaps and duplications in the registered tenders. - Some tenders are missing from the database - Tender data information is not confidential to the representatives of the Agency (Confidentiality Issue required by the Law) 	mission

5. Risk-Case

LACK OF POLICIES results in NOT ACHIEVING BUSINESS AND LEGAL OBJECTIVES

Cause	Issue	Impact on
<ul style="list-style-type: none"> - Lack of effective application controls - Lack of monitoring and analysis over the tenders 	<ul style="list-style-type: none"> - The purchasers increasingly violate the law by procuring goods and services above the threshold set by the law. - 	mission