International Journal of Advanced Engineering and Management Research
Vol. 3 Issue 2; 2018

http://ijaemr.com/ ISSN: 2456-3676

SECURITY AND PERFORMANCE MEASUREMENT OF THE ELECTRONIC PROCUREMENT THROUGH INFORMATION TECHNOLOGY DEVICES

Dr. Sc. Besnik HAJDARI

University "Ukshin Hoti" Prizren, Kosovo

Faculty of Computer Science

Abstract

Security and performance measurement of the electronic procurement through information technology devices is something more than necessary based also on standards of advanced technologies where the time of testing and security is part of the production process of equipment and adequate software.

In this paper are described measurement processes of safety and electronic procurement (e-procurement) through information technology measuring devices as well as necessary standards according to theoretical and practical aspects.

Safety Issues

The average time between failures: is the average time measurement between failures. For example, if a year has 8,760 hours (365 days x 24 hours a day) than the average time between system failures can be divided by 8,760 to identify and find out for how long will the system work during the years. The system with a rate of 30,000 of the average time between failures operates an average of 3.42 years without any failure.

The average time for reparation: is the average time measurement that is required to carry out repairing maintenance in case of system failure. When the value of the average repairing time drops to zero the system availability increases to 100%.

The possibility of failure after application: is the system failure possibility measurement when there is a service request. For example: if the possibility for a failure after application is 0.01, it means that 1 out of 100 service requests results as a failure. This is important in having an uninterrupted operation of electronic procurement.

The rate of faults occurrence: referring the occurrence frequency of unexpected operations/actions. For example: if the value of faults occurrence is 0.02 degrees it means there are 2 possible failures in every 100 operational time units.

Since some electronic procurement system functionalities are more important than others, security requirements may be limited in the most important functionalities.

For example: the security of modules for bids submission and closure usually must be higher than the module that is used in creating the contract award notification.

When determining the security requirements metric, the government must specify the system conditions. For example, the security of any information technology system usually depends on the loads of user's requests and it can be deducted when the simultaneous transactions number increases. So, the security and scalability are closely related to each other.

The electronic procurement system must be easily accessible, ensuring minimal barriers in accessing the competitions through electronic procurement, not misusing the data confidentiality and security and always ensure transparency and non-discrimination. These requirements can only be met with a highly secured electronic procurement. The Government shall specify the security requirements according to its expectations. During the development stages can be made a broad range of testing techniques (including unit testing, integration testing, factory testing, load testing etc.) to ensure a good quality of programming code. Also, in addition to having a system implementation as secure as possible, it is recommended that the government establishes plans and mechanisms to address potential system obstacles in order to continuo operation recovery after the disasters.

Perhaps the most critical event is the time during the tenders' submission closing stages (the electronic tendering phase). In the case of electronic inverse auctions most tenders might be submitted in last minutes. Before the electronic tendering ends, the supplier is required to access the tender submission system. However, it often happens that suppliers submit their tenders close to the submitting deadline. In addition, depending on a specific notice, the offer may consist of several files. This can result in megabits data capacity which should be transferred from the supplier IT place to electronic procurement and to be stored in secured and appropriate servers. The combination of these parameters means that the closing period of each electronic tendering notification can cause failures due to problems with voluminous capacity. Also, the electronic procurement can be damaged when the internet connection is down, by malicious attacks, electricity outage, software/hardware failures etc. System executors must ensure that their systems are capable of dealing with these issues and should prepare plans to deal with critical failures in order to continuo operation recovery after the disasters.

The availability of electronic procurement could be improved by system components identification. If a component is likely to fail than the entire system would also be likely to fail.

The electronic procurement is usually made of three elements:

One or more servers, where most data are processed and stored;

One client, who submits requests to the server;

The network, which enables communication between the client and server.

All three elements can be broken down into components, such as hardware, software, processes, procedures etc. All these components should be checked for their safety, to ensure the system availability. The most specific thing is that the hardware that constitutes the system includes, among other things, the following components which should be checked:

Central processing unit;

Storage devices;

Input devices (keyboard, serial ports, mouse, etc.);

Output devices (monitors, printers, etj.);

Cables.

The system operating software generally consists of the following elements, which all should be safe:

Firmware found in hardware (BIOS) which enables the communication with the operating system;

Operating systems, like Windows, Linux, etc;

Programs used by administrators or maintenance personnel who carry out controls and data handling;

Applications that perform specific tasks or operations depending on the user;

Middleware Software that support communication and data exchange .

Processes that are required for system operation will normally include:

Electricity and system starting;

Network management and operation;

Monitoring system;

Storage and archive;

User management, including the security;

System shut down.

When all relevant system components are identified, the following approaches can reduce the risk associated with critical components, respectively those that are system single point failure:

System failure frequency reduction by finding out the ways to prevent the termination of some critical components;

Time minimization of system failure in attempt to prevent critical components interruption and reducing the number of critical components that could be affected by any interruption;

Reducing the number od system parts that are likely to be affected by any interruption.

System developers can measure the availability in quantitative way through some specific approaches and at regular intervals by calculating the values and degree of attained availability in setting targets in order to improve the availability values. An indicative calculation for quantifying the availability is as follows:

Hours per month when the system should be available: 24 hours a day x 7 days x 4.33 weeks a month (on the average) » 720 hours / month

Hours per month when the system was out of order: 5 hours due to repairing maintenance (ex. fixing the software fault), 3 hours due to perfection maintenance (ex. fixing the hardware), 1 hours due to hard disk failure, total 9 hours of unavailability.

Availability net: ((720 – 9) / 720) * 100% = 98.75%

High availability: 3 of 9 hours due to maintenance activities and only 6 hours (5 + 1) were because of failures. Thus, the high availability is ((720-6)/720)*100% = 99.16%. The availability of functional class often is five nines – 99.999%.

System Performance

The following definitions are commonly used for performance measurement:

A simple request: is evaluating request of the database single chart or a combination of two charts;

A complicated request: is the combination of three or more database charts;

Report: is a report ready to print, produced by a server generating PDF, reported device connection or any other technology;

Document management: the document transfer, shift and opening into document library system of the customer's working place or out of it;

Active user: is the application user who constantly performs common operations;

Reaction time: is the period of time from the moment that the user initiates an action (ex. by clicking a button or a link) until the moment when the required information or order for update confirmation is fully relocated and displayed on the user's screen. The reaction times may be affected by internet latency condition; therefore the reaction time us usually tested in the local area network (LAN).

Performance goals examples may be:

At least 50 active contemporaneous users with a maximum response time; Up to 200 active contemporaneous users with 10% increased response time

The maximum response time that turns back up to 200 results lines is X. For every 100 additional results, the maximum response time can be increased up to X seconds.

The maximum response times (in LAN) can be:

90% of simple requirements to have a maximum response time of 2 seconds; 99% of simple requirements to have a maximum response time of 5 seconds;

95% of complicated requirements to have a maximum response time of 5 seconds; 99% of complicated requirements to have a maximum response time of 10 seconds; 95% of reports generated for less than 6 seconds;

99% of reports generated for less than 15 seconds;

95% of the document management activities to have a maximum response time of 5 seconds;

99% of the document management activities to have a maximum response time of 8 seconds;

The response times for performance testing of an electronic procurement should be measured in a database that previously had loaded a significant amount of data, while simulating the system performance in real terms. In addition, the actual system usage should be stimulated by including simultaneous data uploads and downloads.

Literature

1. Dr.Sc. Besnik HAJDARI - Doctoral Thesis - Requirements for Electronic Procurement Implementation in the Republic of Kosovo - Opportunities and Challenges.

2. Dr.Paul R.Schapper (2012) - Electronic Procurement Report for Kosovo.

3. Law on Public Procurement of the Republic of Kosovo (2010) Nr.04 / L-042.