MODELLING THE PROCESS OF IS AUDITING IN THE PUBLIC ADMINISTRATION USING UML DIAGRAMS

Dalibor Drljača[1], Branko Latinović[2], Dušan Starčević[2]

[1]Europrojekt centar, drljacad@gmail.com, [2]Pan European University Apeiron Banja Luka

branko.b.latinovic@apeiron-edu.eu, dusan.b.starcevic@apeiron-edu.eu

Case study

DOI: **10.7251/JIT1701032D** UDC: **35.07/.08:004.438UML**

Abstract: Although information system audit is a very important business process, at present this is not obligatory in the public administration institutions in Bosnia and Herzegovina and Republic of Srpska. Due to the importance of this process, this paper proposes a model for auditing of information systems in the public administration institutions. The model intends to explain the audit process using a visual representation of the process with UML diagrams. UML is an internationally recognised language for business process modelling and has a number of advantages over other similar languages and standards. Therefore, UML is selected in modelling for modelling of information system auditing process in the public administration institutions.

Keywords: UML, auditing, information systems, public administration, business process modelling.

INTRODUCTION

Implementation of e-government strongly depends on implemented and engaged information system with corresponding applications. In order to provide e-services to citizens and business, these information systems are dealing with a lot of sensitive data, such as bank accounts, transactions of funds, private data, etc. Due to the importance of these data, the public administration institutions need to secure communication and transaction of such data. For this, they use a number of different methods and tools. The information systems are very specific and require more attention in the provision of safety and security. The audit of information systems recently became a very important business process in companies and institutions dealing with sensitive data, such as investment funds, corporations, banks, etc. However, in Bosnia and Herzegovina, there is no legal obligation for the introduction of information system audit in the public administration institutions at any level (municipal, cantonal, entity or state level).

This paper intends to offer a model of information system audit in the public administration institutions using Unified Modeling Language (UML) diagrams. There are different types of public administration institutions and this model takes as an example an auditing process in one Ministry. The differences in the model may occur depending on the type of the institution, but these differences are minor. For example, in the Ministry, the ultimate authority is Minister, while in some Agencies this authority is the Director, etc. But this model does not depend on the size of the institution, which is more important. Also, the model assumes that the audit is performed by the external auditor, due to the fact that this is not legally regulated.

METHODS AND MATERIALS

The paper deals with several scientific fields, but the predominant are economics (in the frame of fi-

nances and auditing), information technologies (in the frame of information systems, structure and security), and law (in the frame of legislation and public administration structure and operations). Therefore, the methods and methodologies selected have to respond to such scientific mix – they **combine modern methods and tools (typical for information technologies) and traditional ones (typical for economics and law)**. This mix of methods and tools **enables a holistic approach to solving the problem**. Also, the basic research methods (applicable for all scientific fields) such as **deduction and induction, synthesis and analysis**, are used for better structuring of conclusions.

The main problem was **scarce literature available in local language** for the topic of auditing of the information system. The problem of information system auditing is not adequately presented in scientific or educational literature in Bosnia and Herzegovina and it is possible to conclude that such literature does not exist at all. There are just some individual attempts and efforts invested in the publishing of articles dealing with the auditing of information systems. Such articles are even more narrowed to an area of cyber-security and how to protect information systems, but not to auditing as the process, nor the use of UML in the modelling of such processes. Therefore, **the use of Internet as the primary source for most adequate information** was selected to compensate this lack of literature. As the auditing of information systems is very specific and information-sensitive process, the most important providers of standards for auditing were consulted such as ISACA (Information Systems Audit and Control Association), ISO (International Organization for Standardization) and INTOSAI (International Organisation of Supreme Audit Institutions). **Use of international standards** is important for maintaining the objectivity of the auditing process.

Especially, it is important to use **normative methods** to discover and define norms and rules of the process. As the paper deals with information systems in public administration, it was necessary to also use the **cybernetic method** to explore the functionality of complex public administration systems and its management. Most of the literature for investigation of this was found in the legal acts of the public administration institutions, Official Gazette and other legal documents. However, in order to make a generally accepted model, the **generalization method** was used to generalize and systematize acquired knowledge. **Modelling method** is frequently in use in the software engineering. This method allows consideration of all features, aspects and the impact of the business process being modelled.

Languages for modelling of business processes

In order to make a model of the IS auditing, for modelling of auditing as the business process we needed adequate modelling language. Each of modelling languages has its own syntax (set of graphics for description – notations) and semantics (interpretation of these graphic notations – the meaning) [1] The modern science recognizes a number of these languages, but there are three most accepted:

- **Business Process Modelling Notation** (BPMN),
- **Unified Modelling Language** (UML), and
- **Event-driven Process Chain** (EPC) or **extended Event-driven Process Chains** (eEPC).

BPMN is the international standard for modelling of business process maintained by the *Object Management Group* (OMG). The aim of BPMN is to provide a notation that integrates the best business process modelling practices and enable a better understanding of the notation by business analytics, programmers and business users [2]. BPMN uses simple diagrams that are created with the **limited set of the graphic elements** grouped into:

- **Flow objects** (*Events, activities, gateways*);
- **Connecting objects** (*Sequence flow, message flow, association*);
- **Swimlanes** (*Pool, lane*); and
- **Artefacts** (*Data object, group, annotation*).

BPMN business model is realized through **three sub-models**:

- **Processes or Orchestration** including *Private non-executable (internal) Business Processes*, *Private executable (internal) Business Processes*, and *Public Processes*;
- **Choreographies**, and
- **Collaborations**, which may include Processes or Choreographies.

UML is language and standard maintained also by OMG. But, it is universal and has more extending capabilities than BPMN. UML is platform-independent, universal modelling language primarily made for the creation of software solutions. [3]. Due to its simplicity and universality, it became a part of modern CASE (*Computer-Aided Software Engineering*) tools. Since its standardization in 1997, it significantly improved software development but also information systems development. In the core of UML lies object-oriented paradigm (OO) for software development, originating from three different OO development methods:

- *Object-Oriented Design OOD,*
- *Object-Oriented Software Engineering OOSE* and
- *Object-Modeling Technique OMT*.

According to the latest standard version (2.5 from March 2015), UML notation contains set of graphical symbols, but significantly larger set than the one in BPMN, and grouped into:

- ***Things*** (for description of behaviour, structure, grouping and explanation),
- ***Relations*** (main four: dependence, association, generalization and realization),
- ***Diagrams*** (7 structural and 8 behavioural)
- ***Mechanisms*** (general mechanisms and extensibility mechanisms)

EPC was created in 1992 in Germany by the Institute for Information Systems in Saarbrücken and World-famous company SAP [4]. Although developed before some other languages and very intensive in use, even today EPC is not standardized [5]. The notation uses following elements:

- **Event**,
- **Function**,
- **Process owner**,
- **Organisation unit**,
- **Information**, **material**, **or resource object**,
- **Logical connector,**
- **Logical relationships** that include,
  - Branch/Merge – XOR operand,
  - Fork/Join – AND operand,
  - OR operand,
- **Control flow**,
- **Information flow**,
- **Organisation unit assignment,**
- **Process path**.

Soon upon establishment of EPC, many shortcomings were observed, which caused the creation of **eEPC** (**extended EPC**), but also a dozen of other extensions of the basic and original EPC that prevented its standardization. **eEPC** is the main business process modelling language in ARIS (Architecture of Integrated Information Systems) managed by IDS Scheer AG from Germany.

Although all of three selected languages have their advantages and shortcomings, it is up to the business analyst to choose the adequate one for the task of system analysis. Having in mind possibility for automation of the whole process, UML was selected as the language that supports many CASE tools and with the ability to convert diagrams into the programming code. Also, one of the main reasons for selecting UML is in its standardized approach, universality, and the ability to document processes important in the last phase of SDLC (Software Development Life Cycle). For the presentation purposes of this paper, Use case diagrams, Activity diagrams and Sequence diagrams will be mostly used. Also, we will consider the whole auditing process as a system for itself and therefore, we will use Use Case diagrams to present general scenarios of the system›s functionalities, and Activity and Sequence diagrams to described flow of the processes within the system. All these diagrams aim to present „what" system should do focusing on the role of the user and not on the implementation and realization details [6]. As CASE tool, which supports UML, the preference was to use a Visual Paradigm Community Edition v.14 (https://www.visual-paradigm.com). This Community Edition has all necessary functionalities and it is a freeware.

Results and discussion

According to existing legislation, the public administration institutions in Republic of Srpska and Bosnia and Herzegovina are not obliged to make a regular audit of the information systems in use. However, there is a lot of information systems in the public administration that were acquired without considerations about interoperability of these systems.

Therefore, for the purpose of modelling such process, a hypothetical approach is made using present organisational and functional structure of the public administration institutions that is given in the relevant legislation. The model considers a case of the information system in the Ministry, as it is the institution that is dealing with sensitive and important data requiring safe and functional information system. Also, the model considers the case of the auditing process done by the external auditing company since there are no regulations dealing with this issue.

Description of the IS audit process in the public administration institutions

The whole process has to start from the top-management and in the case of the Ministry, it is the Minister who should initiate this process. This process can be initiated based on legal obligations or voluntarily if the Minister considers that the security and safety of the data and information system are endangered. Again, there is no legal requirement and the model considers voluntary initiation.

In order to describe the process, a number of actors are recognised in the system that is of crucial importance for the realization of the process.Without these actors, the auditing (as the system) is not operable:

- The Minister (Minister)
- The legal department personnel (LegalDept)
- The financial department personnel (FinancDept)
- The employees of the Ministry (Empl)
- The external auditor personnel (ExtAud)

The actors are generalized for description purposes and there can be several executors within one actor (except for the Minister). Also, other actors can appear in the process and their role will be explained from case to case.

In brief, the description of the actors' roles is as follows:

- **The Minister** (as supreme authority) initiates the auditing process and initiates the procurement of the external auditor that will perform auditing process.
- **The legal department** in the Ministry is in charge of preparing all necessary documentation – both for procurement of the external auditor and for goals of the audit (Audit Charter) that will be at the same time the work description and content of the contract with the external auditor.
- **The financial department** task is to service all procedures related to the financial arrangements of the process (payments)
- **The employees** in the Ministry are expected to take part in the auditing process in accordance with the planned use of resources for the audit. It may be the case where the employees will play an active role (answering the questions, providing some tasks, etc.) or the case where they will be in a passive role (they will be looked as a part of the whole team or the system).
- **The external auditor** is expected to respond to the procurement call and it will include preparation of the procurement materials and applying process. Also, upon signing of the contract, external auditor should prepare the auditing conditions and goals together with the representatives of the Ministry (Legal dept). After that, auditor will perform the core of the audit and at the end will produce and deliver the auditing report that has to be agreed with the Ministry

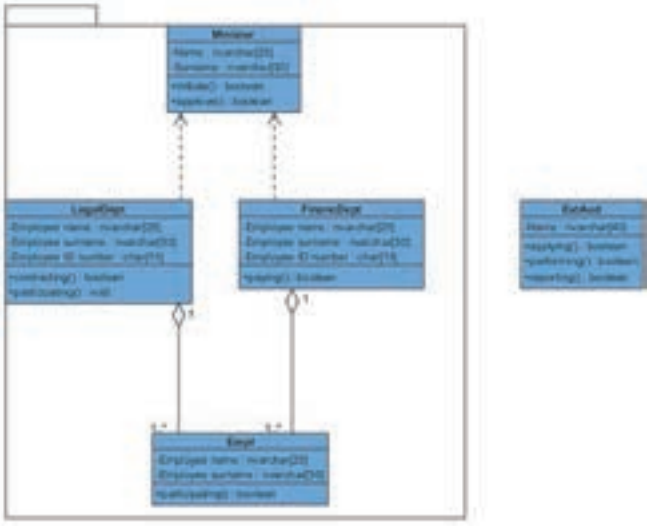

Figure 1. *Class diagram for IS audit system (author)*

Four main business processes are identified (functionalities) that are presented with UML Use

case diagrams:

- Audit initiation,
- Procurement of the external auditor,
- Auditing process,
- Reporting.

Therefore, the context diagram presented with UML Use case diagram looks as in illustration 2 below.

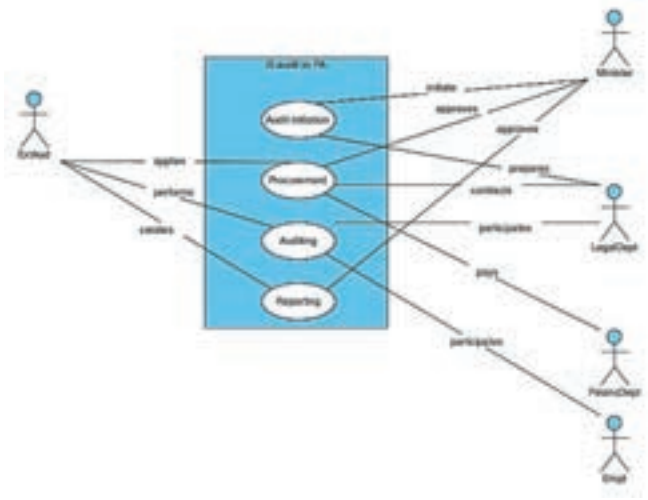

Figure 2. *Context diagram presented with UML Use Case diagram (author)*

The whole system is divided into four main functionalities at the context level and it is presented with the UML Use Case diagram (Figure 2.) titled „IS audit in PA". This diagram shows main interactions between identified actors that are responsible for planning, organizing, performing and reporting in the auditing process. The ExtAud actor is on the left side (usually the side of system's user), while other actors are on the right-hand side of the system (usually the side of system's owner and maintenance). These functionalities should lead to the completion of the auditing process and are in line with the local legislation regulating work of the Ministry.

The first functionality - „**Audit initiation**" covers set of activities and procedures needed to initiate auditing process. Unless it is regulated in a different way, the initiator should be institution authorized person – in this case, actor „Minister". We presumed this case, but it can be the case (such as in banking system) that the auditing process is initiated automatically and similar to the financial audit. It the latter case, there is a slight and not essential change of the model. It is very crucial that this functionality is initiated by the top-level authority since information system audit will have at disposal all elements of the information system (hardware, software, employees, network, etc.) in order to perform check of control points. This functionality engages actors „Minister" and „LegalDept" as the leading actors.

The flow of activities is following (as presented in Figure 3):

- „Minister" initiates (orders) the audit process by sending formal request to the „LegalDept";
- „LegalDept" examines the internal procedures, collects materials and prepares necessary documents for „Minister"'s decision;
- After preparation of the legal document, „LegalDept" sends the documents to the „Minister" for signature;
- „Minister" signs the official documents and returns it to the „LegalDept".

Having the documents signed, the „LegalDept" can now close the functionality „Audit initiation" and start the functionality „Procurement" of the external auditor.

Figure 3. *Activity diagram for audit initiation (author)*

The functionality „**Procurement**" aims to make procurement of the external auditor for information system auditing. The prerequisite for this functionality is the completion of the functionality „Audit initiation" as described above. This functionality is

not necessary if the auditing process is performed by the internal auditor. Since there is no explicit regulation (actually no regulation at all), we assumed procurement of the external auditor. As a part of the previous functionality, the „LegalDept" should create one document with details on the content of the audit. This will use as the description of the work and will constitute the Audit Charter. It is a crucial document because it expresses the wish of the institution to do the audit and what volume of the audit, which controls to check and test, what resources will be analyzed etc. As this document is a „wish" of the institution, the agreement can be made upon selection of the auditor to extend or modify the content and framework of the audit. However, this should be done in a mutual agreement since the content and framework shall determine the price of the service and this should be done prior to the contracting. This functionality is split into two parts:

- First part is commercial procurement and procedures related to the procurement (tender). This part will end but the functionality then goes to the stand-by, and
- The second part of this functionality will start after the performed audit and relates to the payment procedure for completed task.

The flow of activities is following (as presented in Figure 4):

- „LegalDept" based on official documents prepares the call text for the advertisement and initiates procurement procedure by sending the add to the „Media"
- „Media" is publishing the add, and sending the invoice to the „LegalDept"
- „LegalDept" forwards the invoice to the „FinancDept" that prepares documents for payment.
- „FinancDept" forwards payment documents to the „Minister" for signature and approval.
- „Minister" signs the documents and returns it to the „FinancDept" that makes the payment to the „Media".
- During the advertising period (declared by the legislation), the auditing companies submit application („ExtAud")
- „LegalDept" makes a proposal for the selection „Committee" and forwards it to the „Minister" for approval.

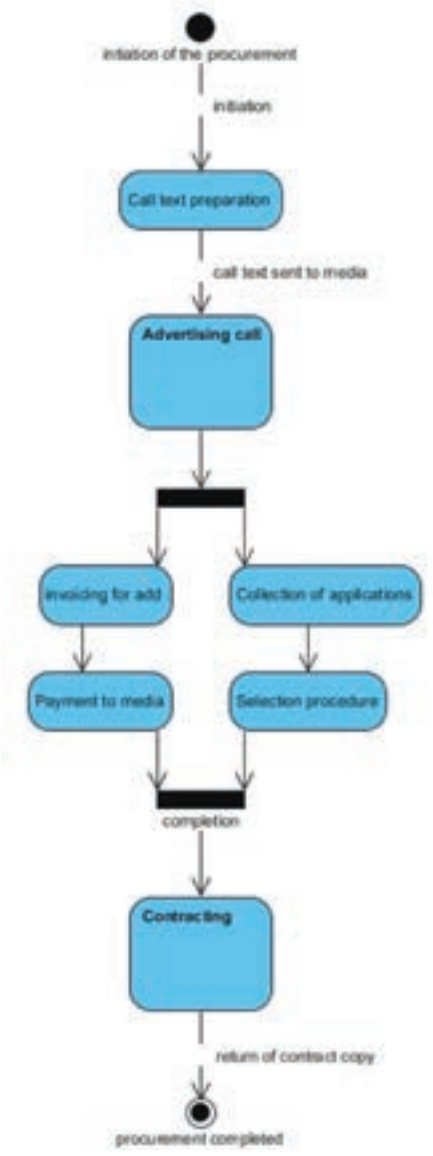

Figure 4. *Activity diagram for external auditor procurement (author)*

- „Minister" approves and appoints the „Committee" that will review all applications and make a selection of the most suitable bidder.
- „LegalDept" is in charge of the whole selection process and prepares the final decision on selection based on the report from the committee and forwards it to the „Minister" for approval.
- „Minister" approves the selected company and orders contracting procedure from the „LegalDept"
- „LegalDept" creates a contract and forwards it to the selected company for signature.
- If all clauses are ok, „ExtAud" signs the contract and returns it to the „LegalDept"

- „LegalDept“ forwards the contract to the „Minister“ for signature.
- „Minister“ signs the contract and returns it to the „LegalDept.
- „LegalDept“ dispatches the copy of the contract to the „ExtAud“ and with this, the procurement process is completed.

Upon receipt of the copy of the contract, „ExtAud“ is starting its own preparations for the audit (selection of staff, preparation of template materials, etc). „ExtAud“ is now ready to schedule the whole auditing knowing what exactly it has to do. Therefore, the first step in new functionality called „**Auditing**“ is organizing an initial meeting to fix the dates for a physical visit to the site and to the information system. During this meeting, the last details are negotiated for smooth and seamless audit. „ExtAud“ introduces working templates, explains the flow of action and fixes other dates for visit, if necessary. It is important that in this meeting all key stakeholders in the process participate, especially the „Minister“ as it has to authorize the use of resources (hardware, software, access, employee etc). After the meeting, „ExtAud“ is fully ready to start the auditing process. This process has its dynamics defined at the meeting. If everything is done smoothly, the auditing process ends with „ExtAud“ last meeting organized with „Empl“ (employees on site). For performing the audit, the „ExtAud“ shall use methodology prescribed by some of internationally accepted standards and frameworks for an audit of information systems, such as COBIT, ITIL, ISO, VAL-IT etc.

The flow of activities is following (as presented in Figure 5):

- „ExtAud“ receives the copy of signed contract and starts its internal preparations;
- „ExtAud“ proposes the term for the first joint meeting for organization of work;
- The meeting is organized and realized, all details are agreed;
- „ExtAud“ performs activities within auditing process with assistance from „Empl“;
- If needed, „ExtAud“ calls for another joint meeting to finalize the work;

Otherwise, with its last visit „ExtAud“ completes the auditing process.

Figure 5. *Activity diagram for auditing process (author)*

Now the auditing process is complete and functionality „**Reporting**“ starts. „ExtAud“ is back to its premises and organizing the work for preparation of the audit report. The audit report has own structure and has to be completed in agreement with the institution ordering the audit. This means that „ExtAud“ has to prepare the first draft of the report and discuss it with the institution. This will be done at one joint meeting organized in the premises of the institution and it is very similar like in the case of a financial audit. „ExtAud“ presents the findings and discusses them with the management of the institution and key stakeholders that participated in the auditing. This is positive practice because it may help „ExtAud“ to clear some suspicious elements which occurred during the preparation of the report. Upon the completion of this meeting, „ExtAud“ is back home and formulating the final version of the report, including the invoice for the services. At this point, we are back in the functionality of „Procurement“ – second part dealing with payment of auditor’s work.

The flow of activities is following (as presented in Figure 6):

- „ExtAud“ is working on a report in its own premises;
- „ExtAud“ drafts report and organizes the meeting in the institution;
- The meeting is done in the institution and draft report is analyzed with key actors;
- „ExtAud“ completes the report in its own premises and sends the final report with the invoice;
- „FinancDept“ completes the payment.

Upon payment completion, the whole „Reporting“ and „Procurement“ functionalities are completed, as well as the whole proposed auditing process.

Figure 6. *Activity diagram for reporting functionality (author)*

Each of this Use Case can be further decomposed due to the complexity of the procedures, and one proposal is given in figure 7 in a form of UML Sequence diagram. The Sequence diagram gives an overview of the process as a whole divided into frames in accordance with the described four functionalities.

Conclusion

The auditing of the information systems is becoming a crucial business process for institutions and companies dealing with a large quantity of very sensitive data, such as banks, insurance companies, telecoms etc. However, information systems in the public administration institutions should also be a subject of the regular audit. Due to the importance of data in such information systems, they can be a target of misuse that should be prevented from the initiation of the information system.

The intention of this paper was to present one of the possible models for auditing of the information system in public administration institutions. The proposed model can have slight changes and variations due to the complexity and internal organization of the institution. This model presented auditing in the Ministry, where the ultimate decision-making authority is the Minister. The model follows four (4) main functionalities that can be decomposed further on individual actions, even to the level of automation of the process. There were two options for engagement of the auditor: internally or externally. Again, the model could be slightly changed, but it was decided to present the case of engagement of the external auditor. There are a number of reasons why the external auditor should be preferred. One of them is that the external auditor can have more experience, knowledge and expertise in implementing the auditing of the information system compare to the internal auditor. The public administration institutions usually do not have such profile among the employees. Also, to acquire the psychological effects of the audit and to obtain objective and relevant auditing data, the engagement of the external auditor justifies this decision for described model.

For the visualisation and description of the modelling process UML was used as a worldwide recognised unified modelling language. The main classes or actors were presented using the Class diagram. A context diagram of the auditing was given using Use Case diagram showing the top-level functionalities of the auditing system. More details on the flow of the auditing process were given with the use of Activity diagrams for each phase of the process. Overall functioning of the system and relevant steps were presented with a Sequence diagram presenting the system functionalities against the flow of the time.

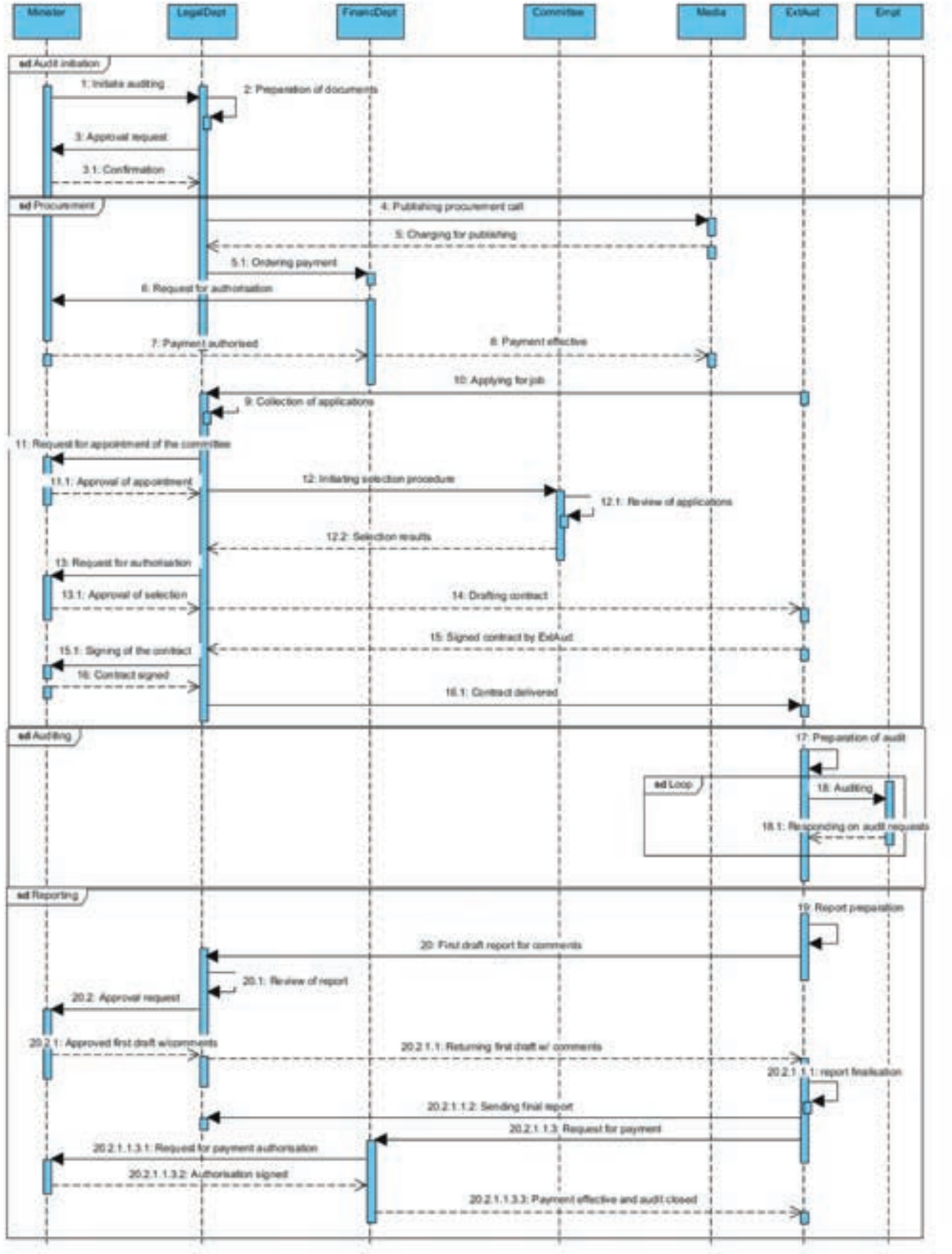

Figure 7. *UML Sequence diagram presenting flow of procedures in auditing process (author)*

With its essence, this paper is a pioneering step in Bosnia and Herzegovina and even abroad. The novelty is in the first instance, a proposing of the model since the auditing of the information systems is (in the contemporary literature) described just textually with the use of recommended and recognised frameworks and standards. It was always up to the auditing body (usually a non-IT expert) to define this process. This leads to the second novelty of this model and that is the use of CASE tools (in this case Visual Paradigm) for modelling and visualisation purposes.

This way the auditing process is seen from the perspective of IT and opens a serial of new questions related to the improvement of the process, proposed model but also wide-recognized standards for the auditing of the information systems. In the future, it is necessary to further develop proposed model to the level of automatization and possible computerization of the process. The auditors are using CAATT (Computer Aided Techniques and Tools) of a different kind for data acquisition and processing, in accordance with the its own preference of the auditor. One of the possible new insights could be the influence of selected CAATT tool for success and quality of the auditing process.

References

[1] Harel D, Rumpe B (2004) Modeling Languages: Syntax, Semantics and all that Stuff, The Weizmann Institute of Science, Israel

[2] Object Management Group (2011) Business Process Model and Notation (BPMN) Version 2.0, OMG Document Number: formal/2011-01-03, Standard document URL: http://www.omg.org/spec/BPMN/2.0

[3] Object Management Group (2015) OMG Unified Modelling Language (OMG UML) Version 2.5, OMG Document Number: formal/2015-03-01, Standard document URL: http://www.omg.org/spec/UML/2.5

[4] Keller G, Nüttgens M, Scheer AW (1992) Semantische Prozeßmodellierung auf der Grundlage - Ereignisgesteuerter Prozeßketten (EPK) In: Veröffentlichungen des Instituts für Wirtschaftsinformatik (IWi), No. 89, Universität des Saarlandes

[5] Ko RKL, Lee SSG, Lee EW (2009) Business process management (BPM) standards: a survey, Business Process Management Journal 15, pp. 744–781.

[6] Pilone D, Pitman N (2005) UML2.0 in a Nutshell, O'Reilly Media, Inc., USA

Submitted: April 7, 2017.
Accepted: June 13, 2017.

About the Authors

Dalibor Drljača is a Ph.D. candidate at the Faculty of Information Technologies at the Pan-European University APEIRON Banja Luka and has MA in information technology and MA in technologies for the Development of European Projects. His main research interests are in e-Government, audit of information systems and e-Commerce. He is part-time engaged as a Senior teaching and research assistant at Pan-European University APEIRON Banja Luka.

Branko Latinović, Ph.D., is a full-time professor and Dean of the Faculty of Information Technologies at the Pan-European University APEIRON Banja Luka since its establishment. His research interests are in information systems, e-Commerce and e-Government.

Dušan Starčević is a full professor at the Faculty of Organizational Sciences, University of Belgrade. His main research interests include human–computer interaction, distributed information systems, multimedia, and computer graphics. Starcevic received his BS and MS in electrical engineering and his PhD in information systems from the University of Belgrade.