FUNCTIONAL MODELLING OF IT RISK ASSESSMENT SUPPORT SYSTEM

Artis Teilans[1], Andrejs Romanovs[2], Yuri Merkuryev[3], Arnis Kleins[4], Pjotrs Dorogovs[5], Ojars Krasts[6]

[1] *Rezekne Higher Education Institution, Latvia, artis.teilans@ru.lv*
[2] *Riga Technical University, Latvia, andrejs.romanovs@.rtu.lv*
[3] *Riga Technical University, Latvia, merkur@itl.rtu.lv*
[4] *Exigen Services, Latvia, arnis.kleins@exigenservices.com*
[5] *Ministry of the Interior, Latvia, pjotrs.dorogovs@ic.iem.gov.lv*
[6] *University of Latvia, Latvia, ojars.krasts@gmail.com*

Abstract

Information technology systems represent the backbone of a company's operational infrastructure. A company's top management typically ensures that computer software and hardware mechanisms are adequate, functional and in adherence with regulatory guidelines and industry practices. Nowadays, due to depressed economic and increased intensity of performed operations, business highly recognizes the influence of effective Information Technology risk management on profitability.

The purpose of this paper is to develop IT risks assessment systems support functional model, based on analysis of IT risks and assessment mechanisms, IT governance and risk management frameworks, functional analysis of IT risks assessment and management software, and, finally, to develop IT risk management domain specification language with a metamodel that defines an abstract UML based language for supporting model-based risk assessment. Usage of UML based domain specific language achieves synergy from in IT industry widely used UML modelling technique and the domain specific risk management extensions.

Keywords: IT risk, risk assessment, domain specific language, UML, CORAS, modelling.
JEL Classification: C51, C69.

Introduction

Nowadays, business recognizes a great influence of effective risk management on profit abilities. Therefore risk management techniques have become an important part of the company's management instrument. There is no general agreement on the most suitable definition of risk for economists, decision makers, and IT theorists. As a result, different types of risks and, respectively, different risk management methods are considered in different areas. Four main general types of risk can be recognized in business,: strategic, market, credit and operational risks. In many companies, Information Technology (IT) related risk is considered to be a component of operational risk. However, Information Technology risk consists not only of breakdowns in computer software or hardware, or lack of expertise of the IT staff. IT risk also may relate to risk of loss resulting from theft of company's data or client information. IT risk also may be the risk of loss that originates from computer software malfunction, such as a manufacturer's software license expiration or glitches, and the ways it affects corporate activities. A risk assessment initiative for IT systems generally helps management understand areas in which significant losses may arise. IT risk assessment is carried out by identifying and evaluating assets, vulnerabilities and threats of using information technologies in business. An asset is anything that has value to the company – hardware, software, people, infrastructure, data, suppliers and partners, etc.

Taking into consideration the extreme complexity of IT risk assessment, we conclude about that there is necessity to apply international frameworks of IT governance and risk management, such as Enterprise Risk Management Framework by Committee of Sponsoring Organizations of the Treadway Commission, Control Objectives for Information and related Technology, Code of Practice for Information Security Management, Information Technology Infrastructure Library, etc.

Within our research, IT risk management domain specific language is developed, with a metamodel that defines an abstract UML based language for supporting model-based IT risk assessment. Nowadays, in IT industry, majority of system specifications and procedure descriptions are made using Unified Modelling Language (UML). UML is a graphical language and it consists from diagrams which are united in a model. The description of a system can be made from just a few diagrams in case of simple system or from hundreds of diagrams in case of a complex system. These diagrams are designed by system architects and system

analysts. They are used in whole life cycle of a system. These models are frequently the main documentation for the system that is used for its operation and maintenance. That is why the authors have choosen UML as the base for designing the IT risk analysis system prototype. UML uses general system organization terms such as *Use Case*, *Activity*, *Action*, *State*, *Event* etc. However, risk analysis professionals work with terms such as *Threat*, *Vulnerability*, *Asset*, *Incident*, *Risk*, *Treatment* etc. Therefore, to create an IT risk analysis tool, it was necessary to extend UML modelling approach with elements used by risk analysts. In fact there was an attempt to develop our own Risk analysis Domain specific modelling language, suitable for system developers and maintenance personnel and for risk analysts as well. Design of modelling tools necessary for risk analysts was based on CORAS language which is well known in professional community (Lund *et al.*, 2010). The CORAS language is a graphical modelling language for communication, documentation and analysis of security threat and risk scenarios in security risk analyses. This paper explains how the authors use CORAS *Threat* and *Treatment* diagrams, connecting them with UML *Uses Case* and *Activity* diagrams (Kleins *et al.*, 2008). The result of this work provides means to unify both risk analysis model and IT system model.

Common IT risk management problems in Latvia

It is possible to indicate a set of IT risks management problems which are typical for Latvian business (Klimov *et al.*, 2008). They are:

- customer service malfunction due to interruptions of continuous access to IT services;
- unsatisfied demand for qualified IT personnel;
- delayed modernization of information systems software and hardware;
- insufficient IT qualification of information system users;
- inadequate level of existing IT services quality monitoring;
- inadequate level of cooperation between IT specialists and other employees;
- inadequate assessment of financial losses resulting from failures or interruptions within information systems;
- absence of IT system development strategic plan, based on a general development plan of company;
- inadequately low IT security level;
- absence of strategy of IT system restoration after potential failures and interruptions.

Taking into consideration the extreme complexity of IT risk management within the framework of operational risk management system, we conclude that we need to apply international standards and frameworks of IT governance, such as Information Technology Infrastructure Library, Control Objectives for Information and related Technology, Code of Practice for Information Security Management.

IT risks management mechanisms

The following documents were reviewed within the current research: Control Objectives for Information and Related Technology (CobiT), IT Infrastructure Library (ITIL) and Code of Practice for Information Security Management (ISO/IEC 27002).

Control Objectives for Information and Related Technology (CobiT) have been developed by IT Governance Institute as a set of documents describing IT governance and audit principles. CobiT precisely formulates governance purposes and principles, management objects, institution's IT processes, its requirements and possible realization approaches (CobiT, 2007). CobiT supports IT governance by providing a comprehensive description of the control objectives for IT processes and by offering the possibility of examining the maturity of these processes. It helps in understanding, assessing and managing the risks together with the benefits associated with information and related Technology. CobiT provides an IT governance instrument that allows managers to bridge the gap with respect to control requirements, information systems and IT issues and business risks, in order to communicate that level of control to stakeholders. It enables the development of clear policy and good practice for the control of IT throughout institutions.

IT Infrastructure Library (ITIL) is one of the most popular approaches to IT governance process organization. ITIL provides a detailed description of important IT division activities, most of which are determined as IT services processes (ITIL, 2007). ITIL is a best practice framework for IT service management and is seen as the de facto global standard in this area. ITIL structure consists of five core books, giving best practice guidance; complimentary material that offers for particular market sector or technologies and information on the web, offering topical support products, process maps and a glossary.

Code of Practice for Information Security Management (ISO/IEC 27002) is the IT security standard, which is based on risks analysis and management. It provides 127 information security guidelines structured under 10 major headings to enable readers to identity the security controls that are appropriate to their particular business or specific area of responsibility. This standard provides guidance on the following subjects: the development of IT security policies; organizational methods of information security ensuring; recourses management; information systems users; communication and processes management; access control; information system acquisition, development and maintenance, information security incident management; business continuity management (ISO/IEC, 2005).

IT risks management technique model

As a result of analysis of the aforementioned IT risk management regulating IT governance mechanisms and existing IT risk management systems in Latvian business, the following technique for IT risk assessment and management is proposed in Table 1, where corresponding (Romanovs *et al.*, 2008) with recommendations domains, sections and processes of IT governance standards and practices is advised.

Table 1. Recommendations for IT risk management

Management	Recommendation
Strategy development	IT risk management should be started with the development of IT risk management strategy, which obligatory should fit a general business-strategy of the company. The following IT mechanisms should be used for the development of the strategy: • CobiT PO1, PO4, ME4; • ITIL SS4, SS7, SD4.6; • ISO/IEC 27002 4, 5.1, 6.1, 8.1, 15.1.
IT threats determination	At the next stage all the possible IT threats to IT resources, information systems and company's information should be find out. The following IT mechanisms should be used for the IT threats determination: • CobiT PO9; • ITIL SS9.5, SD4.5.5, ST9, CSI5.6.3; • ISO/IEC 27002 5.1, 13.1, 14.1.
IT risk identification	All the possible IT risks should be identified and classified. Risks identification and classification should be prepared based on the previously conducted analysis of the possible IT threats. The following IT mechanisms should be used IT risks identification: • CobiT PO9; • ITIL SS9.5, ST9, CSI5.6.3; • ISO/IEC 27002 5.1, 12.1, 13.1.
IT risk assessment system development	The development of IT risk assessment system should be made, by using both qualitative and quantitative risks characteristics; to apply the developed system for assessment of the previously identified IT risks. The following IT mechanisms should be used for the development of the IT risk assessment system: • CobiT PO9; • ITIL SS9.5, ST4.6; • ISO/IEC 27002 5.1, 12.1.
Defining methods for IT risk management	IT risk management should be continued with the definition of the methods, which can be applied to the IT risk management systems and conducted their assessment as well. The following IT mechanisms should be used for defining methods for IT risks management: • CobiT PO9; • ITIL SS9.5, SD3.4, ST4.6; • ISO/IEC 27002 5.1, 12.1, 13.1.
Policy development for most effective methods of risk management	Next, the policy for the application of the most effective methods application for the elimination of previously defined threats should be developed. The following IT mechanisms should be used for policy development for the most effective methods of risk management: • CobiT PO10, DS4; • ITIL SD3.5, SD4.5, SD4.6, ST3.2; • ISO/IEC 27002 5.1, 6.1, 10.5, 14.1.

Management	Recommendation
Risk management system monitoring policy development	Monitoring policy for IT risk management system should be developed. The following IT mechanisms should be used for risk management system monitoring policy development: • CobiT PO10, ME1, ME2, AI7; • ITIL SS4.4, SD3.5, SDH, ST3.2, SO5.1; • ISO/IEC 27002 6.1, 8.2, 10.10, 12.4, 12.5.
Development of techniques for regular assessment of IT risks management system quality	Finally, to develop company's IT risk management system, a tool for continuous assessment of applied solutions of IT risk management should be developed. The following IT mechanisms should be used for development of techniques for regular assessment of IT risks management system quality: • CobiT ME4, DS4; • ITIL SS3.1, SS4.4, SS9.4, SD3.6, SD3.10, SD4.5, SD4.6, CSI4.3; • ISO/IEC 27002 5.1, 6.1, 10.5, 14.1.

Proposed technique for IT risk assessment and management could be successfully used as a start point for development of the IT risks assessment support systems prototype, based on IT risk management domain specification language with a metamodel that defines an abstract UML based language for graphical approach to identify, explain and document security threats and risk scenarios. The next chapter describes Domain Specific Language (DSL) for Risk Analysis Modelling and modelling tool prototype corresponding to this technique. The tool will provide both IT process modelling and documentation as well as connection of these processes with identified risks.

DSL for IT risk analysis

A Domain specific language (DSL) is language for programming, specification or modelling suitable for particular problem domain specialists to solve their specific technical tasks. This chapter describes domain specific language for IT risk analysis designed by the authors. This language has organically emerged from unifying several methods and graphical languages which are used by developers and maintenance specialists from information systems domain, and also analysts responsible for risk analysis and risk mitigation activities for IT systems. The designed DSL is based on approach to Unified Modelling Language (UML) (Kleins *et al*, 2008), CORAS method (Lund *et al.*, 2010) and Misuse Case Alignment Method (Sindre and Opdahl, 2000; Matulevicius *et al.*, 2008).

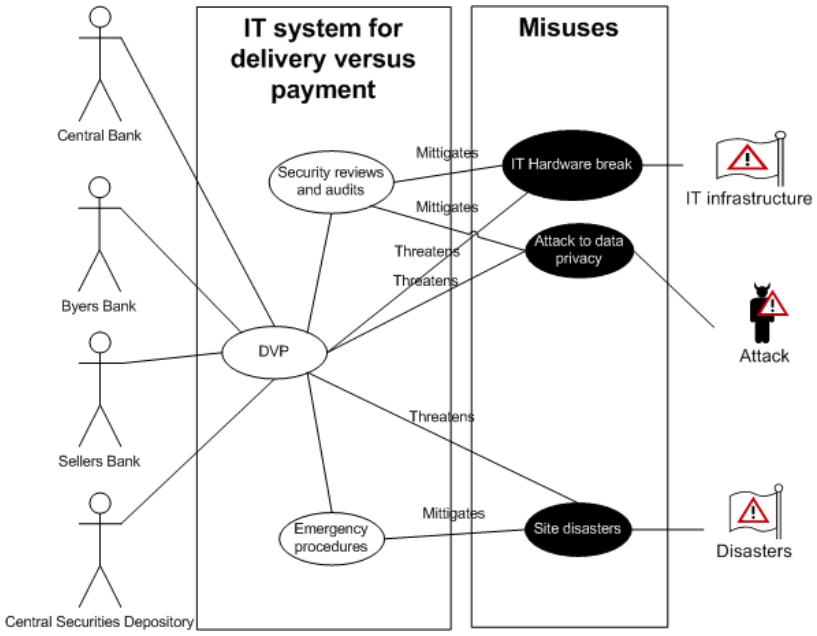

Figure 1. DVP IT system Use cases

Currently, using UML is one of the most commonly used approaches in IT system modelling. The authors' experience acquired while working in IT industry shows that UML modelling is used to some extent in every medium and large scale project.

UML belongs to the group of graphical modelling languages. Initially UML was built for information systems modelling to facilitate the development and maintenance processes. Nowadays the usage of UML is broadened. This language is used for building business models, which exceed the initial task of modelling of information systems.

As regards system modelling, UML modelling is widely used at systems development or enhancement phases. UML modelling describes the structure and behaviour of the system. This language consists of graphical notations called diagrams and builds up an abstract model of a system. The UML standard is maintained by OMG (Object Management Group). In the beginning, UML was built for specification visualization and documentation of IT systems development. Nowadays usages of UML are not only limited to tasks of software engineering. UML is also used for business process modelling and for the development of systems which are not pure information systems.

Modelling with UML promotes model-driven technologies, such as Model Driven Development (MDD), Model Driven Engineering (MDE) and Model Driven Architecture (MDA). Supplementing graphical notations with terms such as class, component, generalization, aggregation and behaviour, helps save system designer's time for system architectural tasks and design.

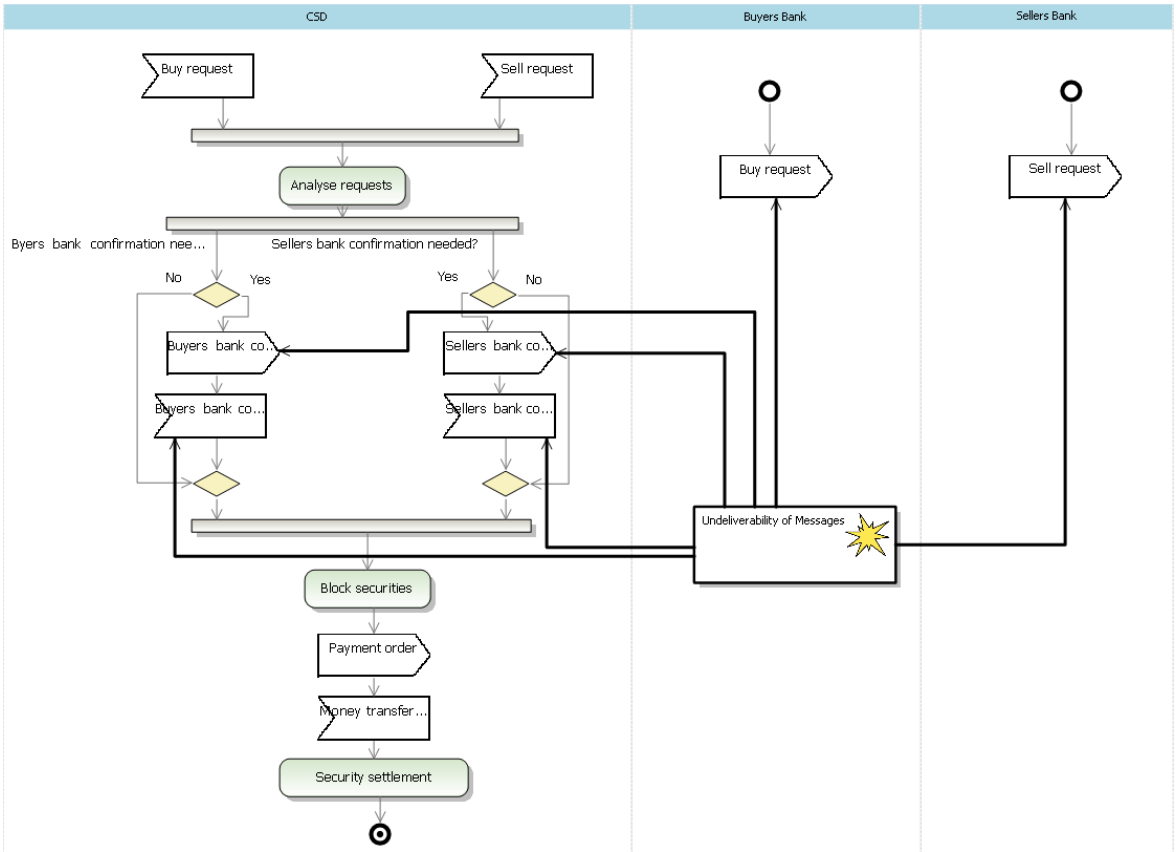

Figure 2. DVP Activity diagram

A UML model consists of a set of diagrams. A diagram is a partial representation of the model. A system model could be divided into two parts. The first part is a functional model, which reflects functionality of a system from the system user's point of view. This kind of model is constructed using *Use Case* diagrams. The second part is the dynamical model that reflects internal behaviour of the system. A model of that kind is constructed using *Activity*, *State*, *Sequence* and *Collaboration* diagrams.

A system model to be created with UML language should not necessarily contain all diagrams. For example, when creating Information System vision model or requirement specification, it is enough for the system analyst to create *Use Case* and *Activity* diagrams. *Use Case* diagram answers a question – what a

system does. *Activity* diagrams describe scenarios of every Use Case, i.e., Business processes. Therefore we prefer this work use only *Use Case* and *Activity* diagrams.

The other approach is applying *Misuse Case* in a UML *Use Case* model. Misuse cases improve UML diagrams with a better support to analyse problems of IT risk management. *Use Case* diagram is extended with graphically black Use case, called *Misuse Case* and black *Actor* called *Misuser*. *Misusers* are related with *Misuse* case. *Misuse cases* are related to *Use Cases* with relation <*threatens*>. During risk analysis stage *Use case* diagrams are extended with additional Use cases for risk mitigation, which are connected with system Use case with relation <include> and with *Misuse case* with relation <mitigate> (see Figure 1).

Considering that the task to be solved by the authors was to provide a government institution responsible for IT risk evaluation with tools necessary for such tasks, the third technology used in this work is security risk modelling, analysis and documentation language CORAS. The initial CORAS approach was developed within the CORAS project funded by the European Commission that ran from 2001 until 2003. CORAS is both a language and a methodology for its application, described in the book (Lund, 2010). Although initially CORAS was designed for security risk analysis, its syntax and semantics allows applying this language to complete IT risk analysis scope. In the developed prototype only one CORAS language diagram - the *Treatment* diagram - is used. *Treatment* diagram is CORAS method all-inclusive diagram, in which all main risk analysis entities – *Threat*, *Vulnerability*, *Risk*, *Asset*, *Threat Scenario*, *Unwanted Incident* and *Treatment Scenario* are included. In turn, by methodology developed by the authors, *Unwanted Incident* is common entity, which connects risk analysis *Treatment* diagram with UML *Activity* diagram used in IT system Activity diagram model (see Figure 2).

Using the DSL described in the paper, a corresponding *Activity* diagram describing IT system functionality should be designed for each system Use case, a corresponding risk mitigation Activity diagram for each risk mitigation *Use case* should be designed, and *Treatment* diagram should be designed for each *Misuse Case* (see Figure 3).

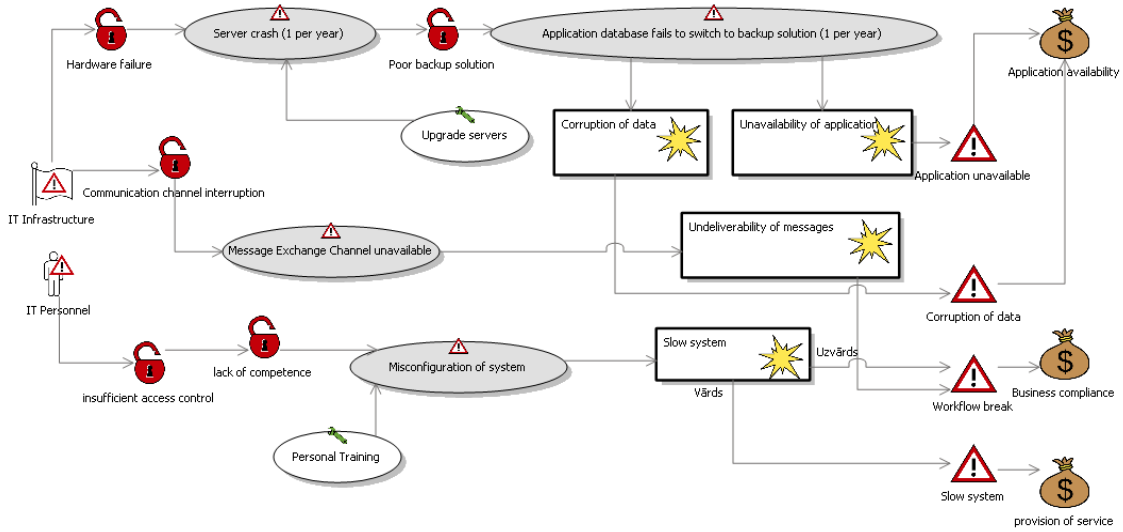

Figure 3. Treatment diagram for IT Hardware break

For such IT risk analysis approach, a tool prototype which is based on Microsoft Visualization and Modelling SDK (VMSDK) is developed while designing DSL. This implemented modelling tool is functioning inside Microsoft Visual Studio Shell. It could be distributed either with Microsoft Visual Studio Shell, or as Microsoft Visual Studio Add-In (see Figure 4).

Conclusions

The current situation within Latvian business indicates the necessity for more complicated and more effective IT risk management system development. In the current paper, it is advised to apply IT governance mechanisms in order to create more appropriative IT risk management. Thus, the IT risk management technique model is developed based on the analysis of IT risk management regulating IT governance mechanisms and existing IT risk management systems in Latvian business. The proposed technique is used

as a basis for development of the prototype IT risk assessment support system. The given approach allows to perform IT risk analysis which is based on unified IT system model specification. In this way one window approach is realised for both system developers and for those responsible for a security policy of a system. This approach is still in the early stages. Further work will be performed to improve Domain specific language. Stochastic attributes will be added to *Unwanted incidents* and *Threats*. This will allow to perform simulation experiments on the risk analysis model and gather more adequate risk estimation results. This approach will be approved on state-wide IT systems and important financial sector IT systems.

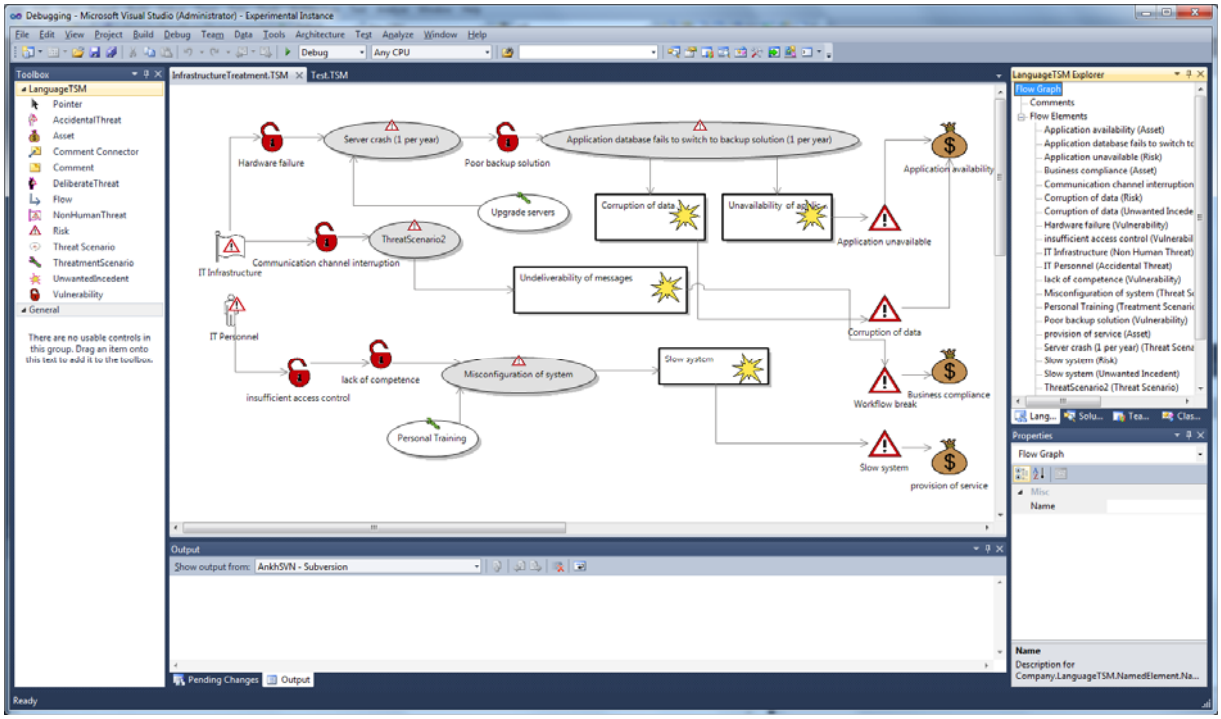

Figure 4. IT risk analysis tool

Acknowledgment

The presented activity is funded by the project "Support of FP7 ICT STREP project “Simulation highway” proposal development” supported by European Regional Development Fund (Nr. 2010/0191/2DP/2.1.1.2.0/10/APIA/VIAA/001) and has been supported by the European Social Fund within the project “Support for Doctoral Studies at University of Latvia”.

References

1. CobiT 4.1. (2007). IT Governance Institute.
2. ISO/IEC 27002. (2005). Information Technology. Security Techniques. Code of Practice for Information Security Management. ISO/IEC.
3. ITIL (2007). ITIL Lifecycle Publication Suite: Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement. The Office of Government & Commerce.
4. Klimov R., Reznik A., Solovjova I., Slihte J. (2008) The Development of the IT Risk Management Concept. Scientific Proceedings of Riga Technical University, Vol.5 (pp. 131-139).
5. Romanovs A., Merkuryev Y., Klimov R., Solovjova I. (2008) A Technique for Operational IT Risk Management in Latvian Monetary and Financial Institutions. Proc. of 8th WSEAS International Conference on Applied Computer Science „Recent Advances on Applied Computer Science” (pp. 230-235).
6. Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen. (2010) Model-Driven Risk Analysis. The CORAS Approach. Springer, 2010.
7. G. Sindre and A. L. Opdahl. (2000) Eliciting Security Requirements by Misuse Cases. In Proceedings of the TOOLS Pacific 2000.
8. Raimundas Matulevicius, Nicolas Mayer, Patrick Heymans (2008) Alignment of Misuse Cases with Security Risk Management. Proceedings of the The Third International Conference on Availability, Reliability and Security,

ARES 2008, March 4-7, 2008, Technical University of Catalonia, Barcelona , Spain. IEEE Computer Society (pp. 1397-1404).

9. Arnis Kleins, Yuri Merkuryev, Artis Teilans, Maxim Filonik. (2008) A meta-model based approach to UML modelling and simulation. Proceedings of the 7th International Conference on System Science and Simulation in Engineering. Venice, Italy, November 21-23, 2008.