A WEB APPLICATION FOR URBAN SECURITY ENHANCEMENT

Denis Baumann[1], Ivo Häring[2], Uli Siebold[3], and Jörg Finger[4]

[1] *denis.baumann@emi.fraunhofer.de,* [2] *ivo.haering@emi.fraunhofer.de,*
[3] *uli.siebold@emi.fraunhofer.de,* [4] *joerg.finger@emi.fraunhofer.de*
Fraunhofer Ernst-Mach-Institut, EMI, Am Klingelberg 1, 79588 Efringen-Kirchen (Germany)

Abstract

Meeting urban security needs adequately is a prerequisite for sustainable economic and societal development. Within the EU FP7 project BESECURE, we investigate how urban security can be enhanced. This is conducted by providing best practices investigated in eight case study cities, methods documented in literature, making use of available data and supporting evidence-based decisions. The results are made accessible via a web-based application platform: Issues and Decisions: Analysis and Support (IDAS). IDAS supports users to address urban security issues in a systematic way and to select appropriate measures. As a motivation for the approach, we outline the advantages of applying risk management in the domain of urban security. Next, we show how IDAS guides stakeholders through a risk management process in operational settings. As structure for the security enhancement process, we chose a risk management scheme inspired by ISO 31000 in five steps. We show how end-users, stakeholders and decision makers can apply IDAS to obtain an overview of security objectives taking account of the context, and how to identify related risks of not achieving the objectives. Within the analytical framework, the risks are assessed and evaluated. For risk control, the selection of measures for improving issues and their critical evaluation is strongly supported, including the iterative consideration of secondary risks. For demonstration of the web application, we showcase the scenario of how to improve conditions of troubled families and young persons that are not in education, employment or training (NEETs) in a deprived urban area in London.

Keywords: Risk management, ISO 31000, urban security, best practices, decision support system, web application, security issues, security enhancement.

1 INTRODUCTION

Meeting urban security needs adequately is a prerequisite for the well-being of citizens, public participation of all citizens, sustainable economic growth and societal development as well as for inspiring vivid urban quarters. This end in mind, the EU FP7 project BESECURE [1] investigates how urban security can be enhanced. This is conducted by learning from practices investigated in eight case study cities, e.g., Belfast (Ireland), Freiburg (Germany), as well as from a comprehensive literature research, by making use of available data and by supporting evidence-based decisions. The results are made accessible via a web-based application platform: Issues and Decisions: Analysis and Support (IDAS).

As a motivation for the approach, we first sketch the advantages of applying risk management in the domain of urban security and detail the showcase. Section 2 also discusses related literature, in particular on possible measures used within the security improvement process of the showcase. Section 3 lists the technology used to enable a mobile and flexible application.

Next, we document in detail how the application IDAS enables risk management for urban areas (Section 4). Special attention is paid to three aims. The first aim is to enable sound use of existing knowledge of the stakeholders in combination with available data, e.g., geo-referenced data. The second aim is to efficiently guide stakeholders through a risk management process and ensure that important assessment principles are met. The third aim is to establish a strong match between process steps and operational realities.

In Section 4, the application is presented within the context of BESECURE and it is discussed what practices to use and how to include knowledge and data in the process. As structure for the security enhancement process, we chose a risk management scheme based on ISO 31000 which guides the user through five steps: establish context, risk identification, risk analysis, risk evaluation and risk treatment. For every step, we outline the inputs which have to be provided by the user and how they affect the application and the risk management process. This will be illustrated with screenshots and a fitting showcase scenario.

2 RISK MANAGEMENT IN URBAN SECURITY AND SHOWCASE SCENARIO

Decisions in urban environments usually take place in a very complex social system with very ambiguous and hardly quantifiable goals and values, see, e.g., [8], [10]. Therefore, risk management is expected to strongly support decisions and enhance the results of measures which are used to tackle security issues. Since such measures mostly have a high visibility and are often criticized by people from the outside, it is important to evaluate the risks and measures properly.

The IDAS web application tries to accomplish this through assisting the user during the risk management process. The main advantages of applying risk management in the domain of urban security include [4], [14]: Organizational structures, stakeholders, decision makers and security objectives are made explicit, risks on objectives are identified, risks are assessed using comparable overall scales, risk evaluation/assessment is documented as well as decisions to try to mitigate risks or not, finally, counter-measures are assessed.

Applications of risk management in similar domains include [5], [6]. Online databases that also cover methods for improving urban spaces are listed in [16]. Sample textbooks on methods and measures with the aim of improving public security are [3], [7]. Typical measures that are relevant for young persons that are not in education, employment or training (NEETs) are described in [15].

We apply a showcase scenario to the IDAS software to demonstrate its functionality and benefits. In [15], research on NEETs is described. One of the main questions in [15] that should be answered also by the present showcase in terms of technical support of a structured decision process is the identification of best and emerging practice examples to engage young people away from NEET pathways in London. In the following, all steps of the risk management process and the corresponding screenshots will be based on this showcase scenario.

3 TECHNOLOGY

IDAS is implemented as a webpage accessible in the World Wide Web. The application is written in C# and uses ASP.NET, see, e.g., [11], as well as T4 text templates [12]. In this way, C# and HTML code can be easily combined. For some functions which affect the layout and behavior of the pages, JavaScript scripts are used, see, e.g., [13]. The application runs on Microsoft Internet Information Server (IIS 7.5).

4 THE RISK MANAGEMENT PROCESS

The risk management process used within the IDAS web application is based on the risk management process as described in ISO 31000:2009 [2]. Fig. 1 shows the risk management process modeled in SysML [14].

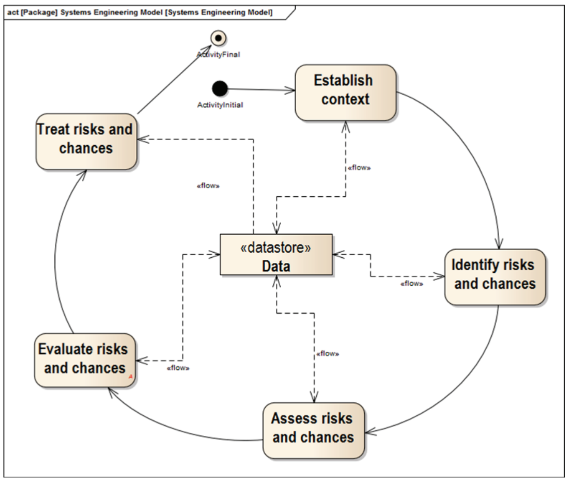


Figure 1: Risk management process in five steps of ISO 31000:2009 modeled with SysML.

The risk management process suggested by ISO 31000:2009 consists of five steps, which have to be traversed to minimize risks in the given context. IDAS focuses on the urban security context and implements the five steps of risk management for the end-user as an urban security project. Therefore, in the following each step is described in the light of urban security.

4.1 Establishing the context

Establishing the context is step 1 of the risk management process as shown in Fig. 1. For the urban security domain, it is divided into the three sub-steps: external context, internal context and risk criteria. In this domain, context can be seen as everything framing the specific needs of the urban area that is in focus as well as everything within it that frames the decision making, e.g., players and roles, organizational structures, area considered, resources at hand, timeline, and legal, ethical, economic and societal context. As a matter of course, not all of the context is relevant for assessing the risks. IDAS supports the user in the selection of relevant items for the context. Next, we sketch the content of the sub-steps with examples for the showcase.

4.1.1 External context

Basically, the external context comprises all external stakeholders, this means groups, communities and people which are not part of the project but may be affected by the outcomes of the project or implemented methods. E.g., young people that are not NEET in the showcase might be affected by the measures which are put in place but they are at first not directly involved in the risk management process. Every stakeholder is assigned with an importance and attitude value. IDAS then allows the allocation of impact scales and objectives like “inform ext. stakeholder” or “involve ext. stakeholder” to each stakeholder that was identified.

In addition to external stakeholders, external indicators that might be relevant for the project like time-referenced or geo-referenced indicators can be attached to the external context, e.g., the number of young people that are NEET in certain areas or over a certain period of time. They can be analyzed if the user has access to the corresponding data sets. Time-referenced data can be represented as time-series; geo-referenced indicators can be represented visually as augmented maps.

4.1.2 Internal context

In the internal context, internal stakeholders are identified, analogously to the identification of external stakeholders. Stakeholders are classified as internal if they directly work in the project. In the showcase, politicians, the mayor and schools could be identified as internal stakeholders. Furthermore, the user can identify and set the objectives for which he wants to assess the risks and go through the risk management process. In addition, automatically created impact scales on the objective “ensure cooperation of int. stakeholders” will be created if the summed-up importance of all stakeholders exceeds a certain threshold. Examples of objectives are given in Fig. 2 below.

4.1.3 Risk criteria

In this sub-step, the user is able to edit scales for the risk matrix for each type of impact (consequence), e.g., the likelihood scale and the impact scales, which are later used to analyze the risks (see Section 4.2.2, Fig. 3). It is possible to add more values to the likelihood and impact scales or to rename the default values. In the main risk matrix, which uses the main likelihood scale and the main impact scale, the user determines how risks which fall into the corresponding table cells are evaluated. It is used for the overall evaluation of all risks.

4.2 Risk assessment

The term risk assessment sums up the risk management steps 2 to 4: risk identification, risk analysis and risk evaluation. It is the “core” part of the process and paves the way for risk treatment (see Section 4.3).

4.2.1 Risk identification

Step 2 identifies all risks which “prevent” reaching the given objectives as good as possible, that means the list of risks should be as complete as possible. Risks can be added to the risk identification graph, as primary risks which are linked directly to the objectives, or secondary risks which are linked to measures (only possible after first iteration of the process (see Section 4.5). The user can choose between predefined risks, e.g., located within the best practice database, or create his own risks. After measures have been assigned during the risk treatment step (Section 4.3), secondary risks can be identified. Fig. 2 shows the risk identification graph that visualizes all identified risks allocated to an objective.

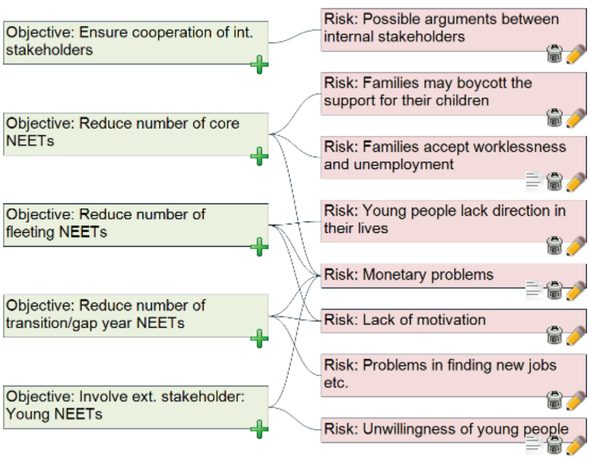
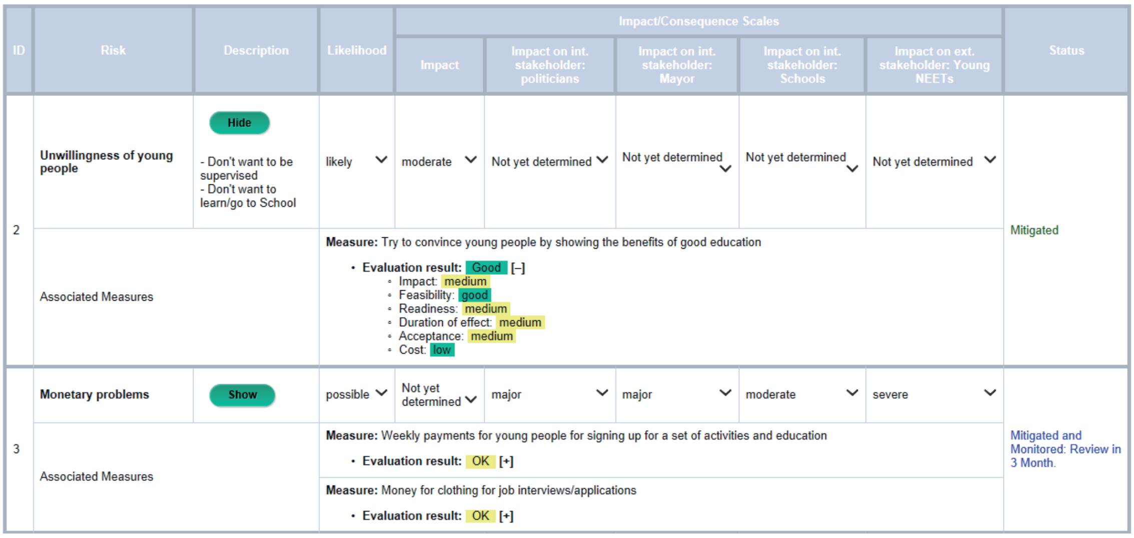


Figure 2: Risk identification graph: objectives and associated risks on objectives.

4.2.2 Risk analysis

In step 3, the user gets an overview of the identified risks (events) for which he should determine the likelihood and the impact (consequence) value. The overview table contains the name of the risk, a short description, likelihood and impact values, assigned measures plus their evaluation (after the risk evaluation has been completed) and the current status of the risk, in particular if the analysis is complete and how it has been evaluated within the risk evaluation step (Section 4.2.3), which may be important for later iterations of the process. Fig. 3 shows a part of the risk analysis table as shown in the web application. "Impact" is the overall impact. It is assumed that all impact types have the same likelihood, i.e., the risk event takes place and is evaluated with respect to different impact types.



ID	Risk	Description	Likelihood	Impact/Consequence Scales: Impact	Impact on int. stakeholder: politicians	Impact on int. stakeholder: Mayor	Impact on int. stakeholder: Schools	Impact on ext. stakeholder: Young NEETs	Status
2	**Unwillingness of young people**	Hide - Don't want to be supervised - Don't want to learn/go to School	likely	moderate	Not yet determined	Not yet determined	Not yet determined	Not yet determined	Mitigated
	Associated Measures		**Measure:** Try to convince young people by showing the benefits of good education • **Evaluation result:** Good [–] ◦ Impact: medium ◦ Feasibility: good ◦ Readiness: medium ◦ Duration of effect: medium ◦ Acceptance: medium ◦ Cost: low						
3	**Monetary problems**	Show	possible	Not yet determined	major	major	moderate	severe	Mitigated and Monitored: Review in 3 Month.
	Associated Measures		**Measure:** Weekly payments for young people for signing up for a set of activities and education • **Evaluation result:** OK [+] **Measure:** Money for clothing for job interviews/applications • **Evaluation result:** OK [+]						

Figure 3: Part of the risk analysis table.

4.2.3 Risk evaluation

In step 4, the risks are positioned inside the risk matrix (see Fig. 4) depending on the likelihood and impact scale values which have been assigned to each risk. Using the risk assessment scales for the impact types, the risks are categorized within the overall impact scale of the risk management context step 1. Risks in green within the global risk matrix can be categorized as "ignore", "critical" and "monitor"; risks in yellow areas as "critical" and "monitor"; risks in orange and red areas can only be categorized as "critical".

In the next iteration (see Section 4.5) of the risk evaluation phase, if the mitigation measures of step 5 are in place, the user evaluates the risks again and is now able to categorize them as, e.g., "mitigated", "mitigated and monitor" or again as "critical" if the risks can be found in the green, yellow or orange areas. If the risk can be found in the red area, it can be categorized as "mitigated and monitor" or "critical".

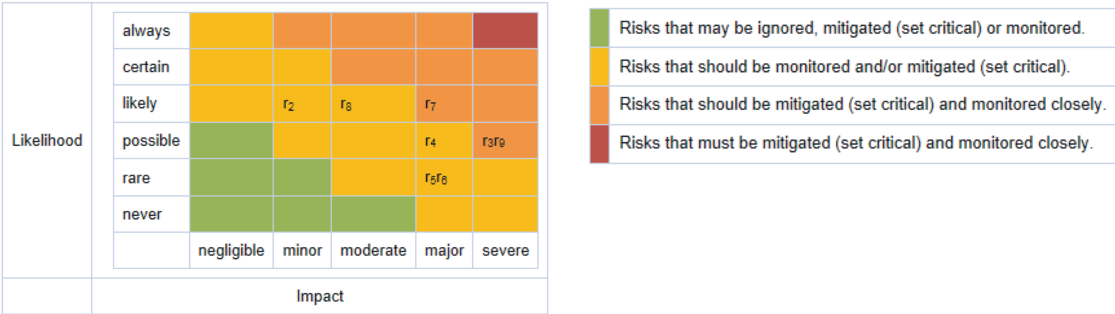


Figure 4: Risk matrix and overall risk assessment scale.

4.3 Risk treatment

After the user has finished evaluating the risks in step 4, the ones which have been evaluated as critical have to be treated (step 5). This happens by assigning (mitigation) measures to risks. The user selects measures analogous to the selection of risks on objectives during the risk identification step 2 (Section 4.2.1). After choosing either a predefined measure or creating a user-defined measure, the measure is evaluated. Thus, the user gets a first impression whether the measure should be considered or not.

Measures are evaluated in regard to impact, feasibility, readiness, duration of effect, acceptance and cost as seen in [9]. In order to get a valid evaluation result, all of these aspects have to be evaluated, the evaluation options range from 1 to 3, where 1 can be interpreted as “bad” and 3 can be interpreted as “good”. The result is defined as the average value of all aspects. The measure evaluation result is shown by coloring them accordingly within the treatment graph, see Fig. 5. In addition, the evaluation result can be seen inside the risk analysis table (Fig. 3) where the colors can be interpreted in the same way as in Fig. 5 and Fig. 6.

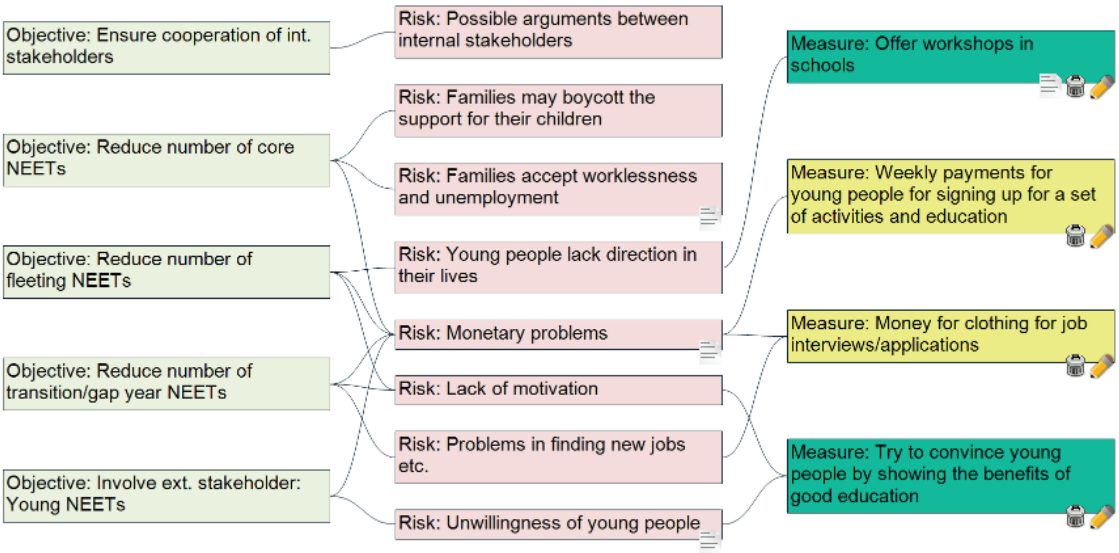


Figure 5: Risk treatment graph: security objectives (left), risks affecting objectives (middle), measures for reducing risks for security objectives (right). Color codes for measures see Fig. 6.

Not Done	Done	Description
		Measure evaluation result not good, measure should be reconsidered
		Measure evaluation result ok/average, measure could be reconsidered
		Measure evaluation result good, measure should be fine
		Measure evaluation not finished, please finish the evaluation by editing the measure

Figure 6: Legend for measure colors.

4.4 Status

The IDAS software provides a short summary and quick overview of the current project. This comprises monitored risks and a table with statistics. Fig. 7 shows an overview over risk management phases as part of the status page.

Phase	Sub Item	Status
Context	External Context	1 external stakeholder(s)
	Internal Context	3 internal stakeholder(s)
	Risk Criteria	0 custom impact scale(s). Additional impact scale(s) for 1 of 1 external stakeholders and for 3 of 3 internal stakeholders.
Risk Identification		Risks for 5 of 5 objective(s) identified. 0 secondary risk(s) for 0 of 4 measure(s) identified
Risk Analysis		8 of 8 risk(s) analyzed
Risk Evaluation		0 risk(s) not categorized. 0 risk(s) ignored. 3 risk(s) monitored. 0 risk(s) critical. 2 risk(s) mitigated. 3 risk(s) mitigated and monitored.
Risk Treatment		4 measure(s) associated to 5 risk(s)

Figure 7: Status overview over risk management phases.

4.5 Iterations

After every step has been completed once, right after the risk treatment step 5 (Section 4.3), the user is directed back to the risk identification step (Section 4.2.1) where the second iteration of the risk management cycle begins. In this iteration, the user can identify secondary risks of measures he applied and if there are any, he has to manage them in a similar way like the primary risks.

There are also corresponding changes in the risk matrix if the user has assigned measures to risks which have been categorized as critical in step 5. The user has to decide if the risks have been mitigated by the measures, if they have been mitigated and should be monitored or if they are still critical, in which case the measures were not successful. The only exceptions are risks which are found inside a red area. Those risks can either be categorized as mitigated and at the same time be monitored or categorized as critical again.

The second iteration of the risk management cycle was successful if all risks are assessed as critical, mitigated or should be monitored. Further iterations of the risk management again take place in pairs if risks are evaluated as critical. Then always counter-measures are asked for. Only if explicit statements on ignoring risks are made, one iteration suffices. Typically, iterations are done every month, quarter or year.

5 SUMMARY, CONCLUSION AND OUTLOOK

In this paper, we described the web application IDAS and the risk management process on which it is based. We detailed the implementation of the analytical process and associated analytical tabular methods with its five steps establishing the context, risk identification, risk analysis, risk evaluation and risk treatment using a showcase with screenshots of the application.

We described the minimal analytical assessment framework that links all steps. The model implemented contains several constraints for user inputs that ensure logical soundness and compactness. Examples include each objective has at least one stakeholder, risk assessment criteria must be set for at least one global (overall) scale and for each impact (consequence) type used, risks must be assigned to objectives, likelihood and impact on objectives (consequences) must be determined for each risk (event), each risk must be evaluated on at least one overall assessment scale, risks that are critical must be attempted to be mitigated using measures, each measure should be assessed for applicability in the present context, and finally, for each measure secondary risks on all objectives must be determined.

The application already offers entries for user input boxes, e.g., stakeholder types, objectives, impact category and scales, risks, counter-measures, etc. The entry options and how they are presented could be further improved in the application. In particular, the method repository could be extended and be made more systematically accessible. One desirable feature is further to assist the end user with useful hints, possibly taking the information already provided into account, to propose, e.g., which risk identification, assessment and evaluation methods could be used in addition in the respective risk management steps. Most importantly, in this way counter-measures could be proposed in a ranked order. In all cases, the user should be supported but not manipulated to select appropriate methods, e.g., using color-coded lists.

ACKNOWLEDGEMENTS

We acknowledge substantial contributions of our former co-workers Clemens Schoppe and Emin Karayel. This publication results from the BESECURE project (Best Practice Enhancers for Security in Urban Environments, [1]), funded by the European Union FP7 Security Programme under Grant Agreement No. 285222.

REFERENCES

[1] *EU FP7-project BESECURE*. http://www.besecure-project.eu.

[2] AS/NZS ISO 31000:2009. *Risk Management–- Principles and Guidelines*.

[3] Augustinus, C. 2003. *Handbook on Best Practices, Security of Tenure, and Access to Land*. *Implementation of the Habitat Agenda*. United Nations Human Settlements Programme, [Nairobi].

[4] Fischer, K., Siebold, U., Vogelbacher, G., Häring, I., and Riedel, W. 2014. Empirische Analyse sicherheitskritischer Ereignisse in urbanisierten Gebieten. *Bautechnik* 91, 4, pp. 262–273.

[5] Holevas, K., Bonazountas, M., and Sabanegh, R. 2005. Urban Risk Assessment and Management in the Enlarged EU, Recent Status and Trends. In: *Safety and Security Engineering*. WIT transactions on the built environment. WIT Press, ASHURST LODGE, SOUTHAMPTON SO40 7AA, ASHURST, ENGLAND, 223–232.

[6] Johansson, A.C.H., Svedung, I., and Andersson, R. 2006. Management of Risks in Societal Planning – An Analysis of Scope and Variety of Health, Safety and Security Issues in Municipality Plan Documents. *Safety Science* 44, 8, pp. 675–688.

[7] Kemp, R.L. 2001. *The Inner City*. *A Handbook for Renewal*. McFarland, Jefferson, N.C.

[8] Lewis, M. and Hartley, J. 2001. Evolving Forms of Quality Management in Local Government: Lessons from the Best Value Pilot Programme. *Policy & Politics* 29, 4, pp. 477–496.

[9] Luzern, C. o. 2013. *Sicherheitsbericht Stadt Luzern 2013*.

[10] March, J.G. and Olsen, J.P. 1989. *Rediscovering Institutions*. *The Organizational Basis of Politics*. The Free press, New York [etc.].

[11] Microsoft. *ASP.NET Documentation*. http://msdn.microsoft.com/de-de/library/4w3ex9c2(v=vs.100).aspx.

[12] Microsoft. *Code Generation and T4 Text Templates*. http://msdn.microsoft.com/de-de/library/bb126445.aspx.

[13] Mozilla. *JavaScript Reference*. https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference.

[14] Schoppe, C., Häring, I., and Siebold, U. 2013. Semi-Formal Modeling of Risk Management Process and Application to Chance Management and Monitoring. In: *Safety, Reliability and Risk Analysis*, R. Steenbergen, P. van Gelder, S. Miraglia, and A. Vrouwenvelder, Eds. CRC Press, pp. 1411–1418.

[15] Tanner, S., Obhrai, A., and Spilsbury, M. 2007. *What Works in Preventing and Re-Engaging Young People NEET in London*. *Research on Young People "Not in Education, Employment, or Training (NEET)"*.

[16] Work Group for Community Health and Development at the University of Kansas. *Community Tool Box*. http://ctb.ku.edu/en/databases-best-practices.