Risk Management Software Platform ZOTY for SMEs

Martin Hirman, Andrea Benesova, Michal Svehla, Jiri Tupa, Frantisek Steiner, Tomas Rericha
Department of Technologies and Measurement
University of West Bohemia
Univerzitni 8, 306 14 Pilsen, Czech Republic
hirmanm@fel.zcu.cz, benesov2@fel.zcu.cz, svehlam@fel.zcu.cz, tupa@fel.zcu.cz,
steiner@fel.zcu.cz, trericha@fel.zcu.cz

Zdenek Kocourek, Petr Humpolicek
IDS Advisory s.r.o.
Otiskova 2823/30, Líšeň, 628 00 Brno, Czech Republic
zdenek.kocourek@idsa.cz, petr.humpolicek@idsa.cz

Abstract

This paper deals with the introduction and application of the software platform ZOTY, which is a new innovative software platform to accelerate the implementation of management and operation systems. In the first part, the research of available solutions for risk management on the market with the comparison of their pros and cons is described. This study shows that complex software with all intended functions was not available at a comparable price level which is acceptable for SMEs. In the next part, the functionalities of created software platform ZOTY are described. Also, one example of many methodologies used in the software platform is described in detail. At the end of the paper, the main benefits of the new software platform are described.

Keywords

Risk management software, risk analysis, ZOTY software tool

1. Introduction

Risk management is an important task in the business management area. It is a continuous, repetitive, set of connected activities prepared for managing of potential risks and for reducing their occurrence and their impact on the organization. Risk management means application of systematic approach to assessing and acting on risks for ensuring that objectives of organization are achieved (Berg, 2010). The purpose of risk management is to prevent problems or negative phenomena, to avoid crisis management. Risk management consists of several connected phases - risk identification, risk analysis, risk evaluation, risk mitigation, risk management, and risk monitoring. Risk management is a process that helps organizations to understand what the risk is, who is at risk and what are the control mechanism of current risks are for those risks. If current risk value level is too high, the action is necesery to manage the level of risk down to an acceptable level. At present, the implementation of risk management or safety system to the organization is necessary not only for any moral obligation to protect their employees but also due to the legislation requirements (Malik and Holt, 2013). The another possible impact of effective and integrated risk management system is company performance improving (Mohammed and Knapkova, 2016).

Risk Management Software is business software used for risk management, assessment, evaluation, audit, and impacts. There may be a wide range of risks types such as operational, financial, project, environmental, natural disasters, market risks, etc. The software should assist in identifying, evaluating, analyzing, setting, and managing measures for individual risks across the company, assigning those to responsible persons. The risk management

software is standardly used in large enterprises but for SMEs the implementation of suitable risk management software can be beneficial. The paper (Falkner and Hiebl, 2015) describes a systematic review of the implementation of risk management in SMEs and shows that risk management in SMEs is important and has a significant impact on the SMEs' business strategy.

2. State of Art

At the beginning of our work, the research of available solutions on the market was realized. The 12 commercial solutions for risk management have been found. The descriptions of the better solutions are shown below, and the comparison of important functionalities of each tested solution can be seen in Table 1.

A. Active Risk Manager (ARM)

The software covers the needs of risk management from project management to strategic planning and, last but not least, the planning of internal audits. ARM helps identify, analyze, manage, monitor, and reduce the impact of risk, including reporting across the organization. The software can be used for all sectors - state administration, health care, private companies. Current users of the software are: Airbus, General Dynamics, Alstom, RWE, Skanska, NASA, AT&T, Nestle, Alstom, Westinghouse, … (SWORD, 2020)

B. SWORM

Software is used to collect information necessary for comprehensive measurement and management of operational risk and for their subsequent processing. It consists of several modules. Each module is designed to cover a different area of operational risk measurement and management. The client has the option to purchase either selected modules or the whole solution, which allows him to measure and manage operational risk. Current users of the software are: Home Credit, TONA, a.s, … (Advanced Risk Management, 2019)

C. RSA Archer Risk Management

The software is designed to provide a comprehensive view of risk with a business context connected to risky cases of use and to facilitate the management of evaluation campaigns, metrics, and loss tracking and risk reporting by thousands of predefined reports, risk analyzes, dashboards, and reports improvised in a reporting tool. Current users of the software are: Adobe, Berkshire Bank, Partners Healthcare, Royal Dutch Shell, Raiffeisen Bank, Hong Leong Bank, … (RSA Security LLC., 2020)

D. HOPEX GRC

The software is designed for risk management, internal control, and internal audit support. The implemented GRC procedures are designed to provide critical information, support rapid decision-making, cost optimization and innovation opportunities. The modules support efficiency and performance enhancement through risk management and monitoring in collaboration with internal control and guidance support. Support for standards and procedures defined by IIA and OCEG. Current users of the software are: DBS Bank, UniCredit, United States Department of Defense Learning Institution, United States Navy Command, Seagate, Edison, United States Department of Agriculture, WallGreens, … (MEGA International, 2020)

E. Thomson Reuters RMS - Accelus

The software enables the dynamic interconnection of business transactions and strategies within a regulated environment. Procedures implemented to support risk management, internal control, and internal audit. Thomson Reuters Accelus Management control systems provide insight through the ability to identify, map and track changes, process integrity, audit results, including relevant training. Risk monitoring modules and direct integration of relevant directives. Current users of the software are: Fujitsu, NCDOT, Extraco Banks, Qatar National Bank, EY Team, … (Thomson Reuters, 2012)

F. MetricStream Enterprise GRC
G. BWise GRC platform
H. SAP Risk Management
I. OpenPages GRC Platform
J. GRC Portal
K. Enablon RM
L. Risk Management

Table 1. Functionalities of examined systems for risk management.

Module (group of properties)	Properties / functionality / tools	A	B	C	D	E	F	G	H	I	J	K	L
Strategic risks	Evidence of incidents and problems (knowledgebase for further analysis) common to all modules	X	X		X	X	X	X	X			X	X
	Development and innovation plans		X				X						
	Forced price changes (policy, regulation)					X							
	Technological progress						X						
	Change of customer preferences												
	Market stagnation					X							
Process management risks (QMS - ISO 9001)		X	X	X			X	X					
Environmental risks (EMS - 14001)				X		X	X						
Human resources and labor safety risks OHSAS - 18001)	Motivation system			X			X						
	Personal development plans, training plans			X		X	X						
	Evaluation of training effectiveness					X							
	Fluctuation	X	X										
	Records of accidents at work												
	Capacity planning		X			X		X					
Information security risks (ISMS - 27001)	Records of information assets	X			X	X	X	X					
	Threat catalog	X	X	X	X	X	X	X					
	Identified risks and their status	X	X	X	X	X	X	X			X	X	X
	Risk Management Plans			X									
	Effectiveness of the measure			X	X	X		X					
	Declaration of applicability												
	Support of ISO / IEC 27002: 2013			X	X	X							
	ISMS internal audit support	X	X	X	X		X	X	X	X	X		
	Corrective and preventive measures	X	X	X		X	X	X					
Financial risks	Cash Flow	X				X	X		X		X		X
	Investment					X	X		X		X		X
	Credits and loans			X					X		X		X
	Receivables and payables					X			X		X		X
	Liquidity	X		X		X			X		X		X
	Solvency	X		X					X		X		X
	Pricing policy - fixed x variable					X							
135/5000 Risks of the social environment (customers, policy, raw materials, suppliers) Social risks (Corporate Social Responsibility - CSR)							X						
Risks of business continuity	Records of crisis and recovery plans (for individual activities and types of risk events)		X				X	X					
	Search of crisis and recovery plans (for individual activities and types of risk events)	X	X				X	X					
	Planning and control of emergency plan practice - early warning system	X	X	X				X					
	Monitoring the results of individual business continuity plans		X	X				X					
	Testing continuity plans		X	X				X					
Others	Support for risk simulation			X		X				X	X		
	Disaster Recovery Planning			X		X					X		
	User-definable environment					X	X	X	X	X			

3. Software ZOTY

The main aim of the developed software was to increase business competitiveness through a new innovative software platform to accelerate the implementation of management and operation systems. The platform ensures rapid business adaptation to changes in the business, legislation, and security environment. At the same time, it ensures the efficient and rapid implementation of advanced traffic management and automation systems. It enables companies to group into larger cooperating clusters, including the interconnection of separate IS / ICT systems with the maximal emphasis on information security in shared Internet services. The platform enables companies to integrate the existing IS / ICT they are using so far, which will save costs on IS /ICT. This solution is also applicable to public sector environments (e.g., universities) and local governments and their needs.

ZOTY is software to support risk management, auditing, and compliance with requirements or legislation. The ZOTY software is primarily intended for SMEs. ZOTY's functionalities are designed to respect multiple different risk management approaches. From the simplest, when you don't engage in any risk analysis, you select and implement a basic set of measures from a catalog. Despite the basic, indicative risk analysis, you quickly perform with the help of experienced experts in your field and then evaluate possible scenarios. Up to comprehensive and detailed risk analysis, including the evaluation of assets, threats and vulnerabilities. The biggest advantage of ZOTY software is that with one pack of my data (e.g., process model or list of assets) is possible to make many different risk analysis from different perspectives (e.g., information security perspective, business perspective - threats, opportunities, cybersecurity perspective, etc.). Another advantage of the software is integrated control of measures to risk mitigation and the observation of changes in time.

3.1. SMART.PORTAL (SP) - ZOTY

Our solution consists of SMART.PORTAL (SP) (see Figure 1) with commercial name ZOTY. This SP is an integration and visualization platform - the core of the solution. The main functionality of SP is LDAP integration for importing users from directory servers, which is very important for larger customers with a large number of centrally managed user accounts. Support of e-mail notifications is also present. The mxGraph graphics library is implemented for the ability to visualize process models in the PROCESS.PORTAL module. A system for automatic logging of user activities is also implemented.
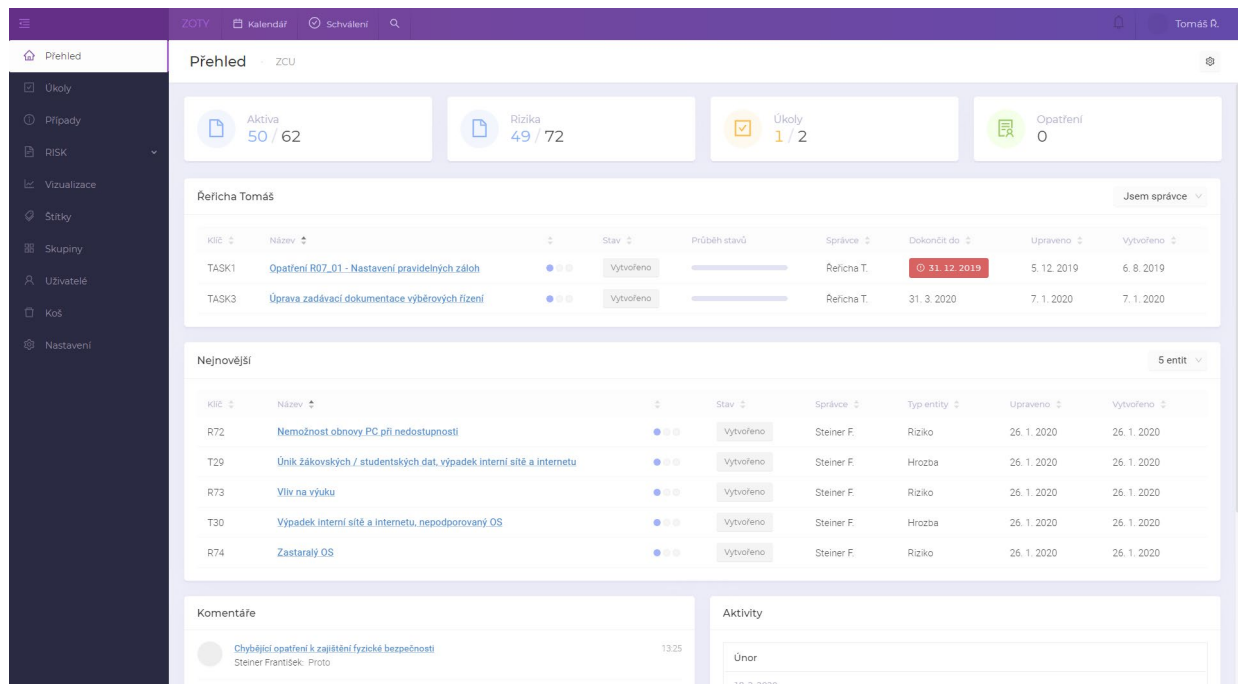

Figure 1. Title page example of ZOTY software (SMART.PORTAL).

3.2. RISK.PORTAL (RP) – ZOTY Risk

The next part of the solution is module RISK.PORTAL (RP) with commercial name ZOTY Risk. Module for risk management with relation to processes and key performance indicators (KPIs) incl. business continuity. This module contains various functionalities that support not only the risk management itself but also the management of compliance with legislative or other requirements or, e.g., management of audits (ZOTY Audit). This module contains a comprehensive modular solution providing software support for the entire area of Governance, Risk & Compliance - ZOTY GRC. The main functionalities of this module can be seen in Figures 2 – 8.
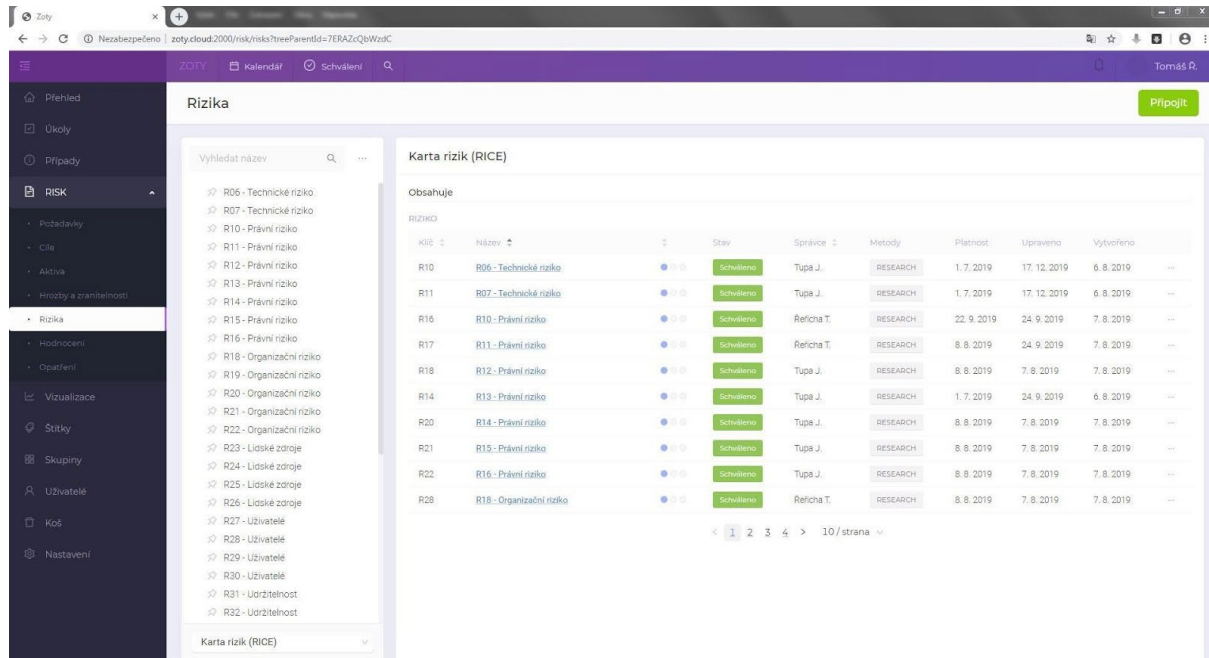
Figure 2. ZOTY Risk – example of defined risks database
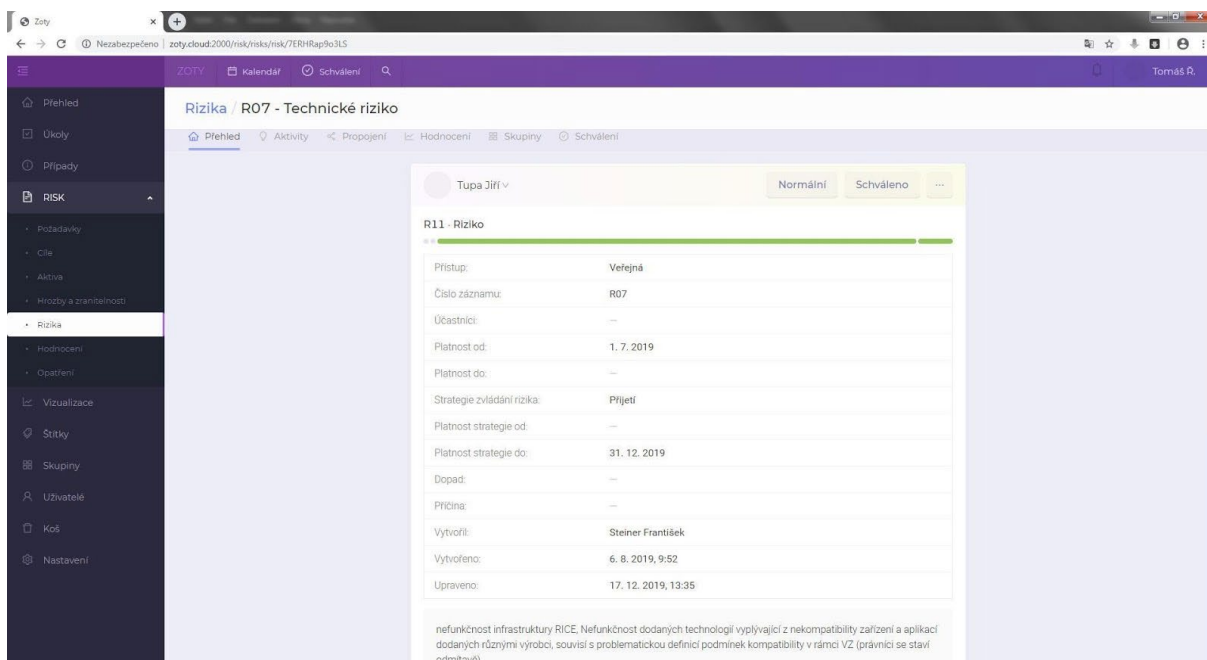
Figure 3. ZOTY Risk – created risk card
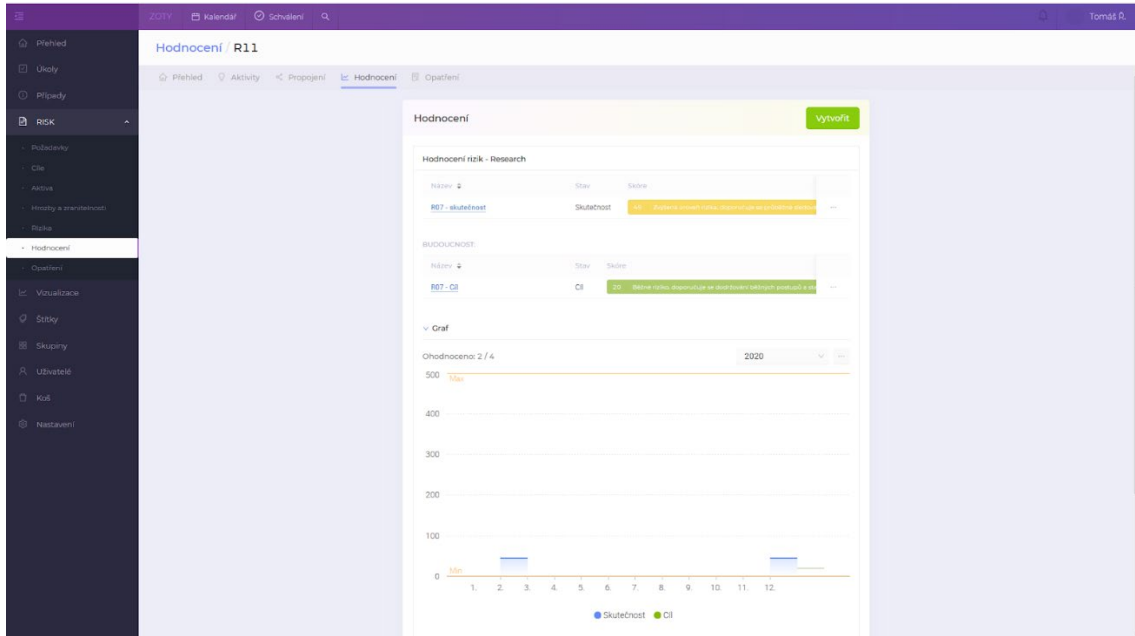
Figure 4. ZOTY Risk – created risk card - evaluation (for current and target status)

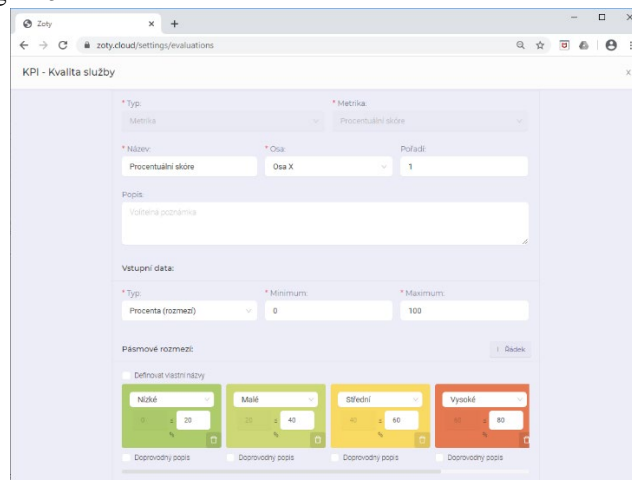Figure 5. ZOTY Risk – detail of created risk card – risk evaluation

Figure 6. ZOTY Risk – example of establishing a new KPI to measure and evaluate the quality of service.

Figure 7. ZOTY Risk – example of the proposed measure to risk mitigation.

Figure 8. ZOTY Risk – summary of measures, including financial costs.

3.3. PROCESS.PORTAL (PP) – Zoty Architect

The next part of the solution is module PROCESS.PORTAL (PP) with commercial name ZOTY Architect. A module / portal for publishing process models from any process analytics tool, starting with accenting the industry's most widely used tool, ARIS. An example of imported process model from the ARIS tool to the ZOTY Architect can be seen in Figure 9. From the beginning, everything has been developed in an open way, with an emphasis on the possibility of using any process tool that the customer already uses as a data source.
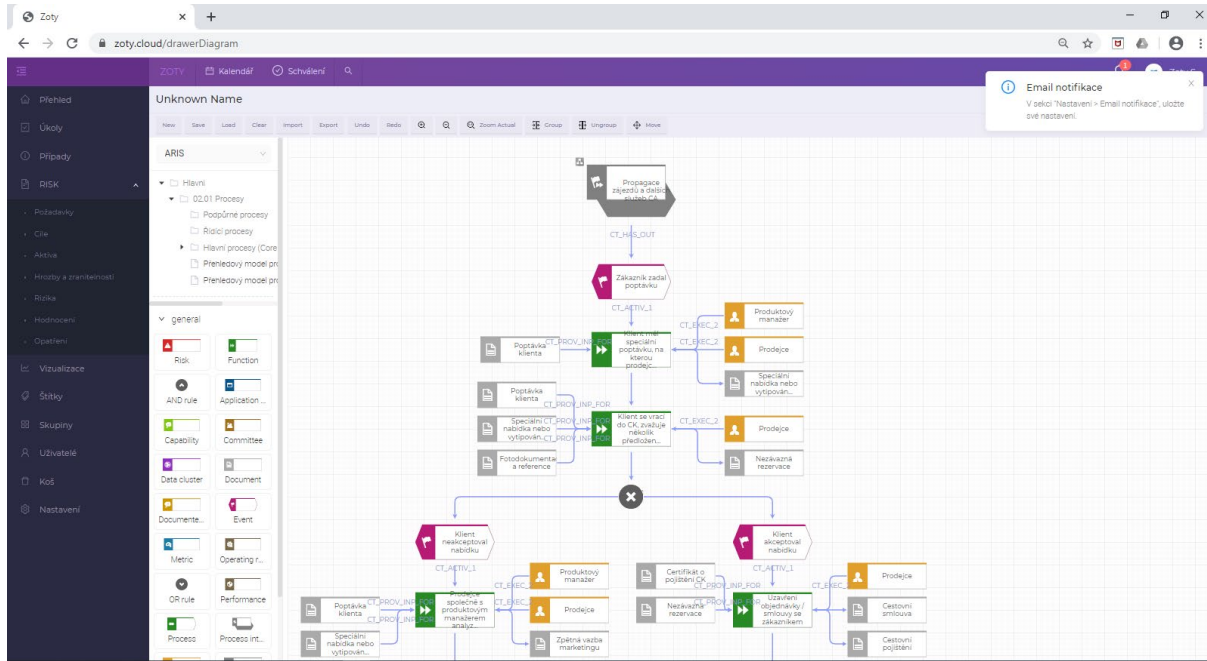
Figure 9. ZOTY Architect – example of an imported process model from ARIS tool.

3.4. Reference database (RD) and ISO.PORTAL (IP) – Smart Portal

The next part of the solution is the Reference database (RD) and ISO.PORTAL (IP) with commercial name Smart Portal. Reference, respectively knowledge database for individual software modules. It contains "best practices" for Business Process Management (BPM). ISO.PORTAL is a simplified model for working with a reference database.

3.5. SMART.EDU (SE) - Extension pack SmartEdu

The next part of the solution is module SMART.EDU (SE) with the commercial name Extension pack SmartEdu. This extension module / bundle for support of school management (HE / SS) is a combination of specific functionalities PROCESS.PORTAL + RISK.PORTAL + reference content for the education sector, which is in line with current changes and trends in the management of educational institutions.

4. Example of used methodology for risk management

Our software has implemented more methodologies for risk management and evaluation which is possible to choose and used. One of them is given in this section as an example. This methodology consists of the identification and analysis of risks. In this case, the risk analysis is a combination of quantitative and qualitative risk analysis. This methodology is possible to use for process risk analyses or risk analyses of defined assets (objects). The principle of this method is defining assets and threats.

Risk management methodology is fully implemented in the module RISK.PORTAL. The reference database with evaluated risks is created here. Risks are created by combining rated assets, threats, and vulnerabilities. Risk management is not only concerned with risk identification. The identified risks need further evaluation. The risk assessment must be carried out to ascertain the seriousness of the risk and subsequently, during the implementation of the measure to determine the effectiveness of the implemented measure. At the time of risk assessment, it is possible to link to specific processes, assets, threats, or vulnerabilities. After the risk assessment, it may be necessary to introduce measures to reduce or eliminate the risk.

4.1. Asset value determination

The assets are evaluated on the basis of three parameters evaluation:

- Confidentiality (A)
- Availability (B)
- Integrity (C)

Each parameter has set the scale from 1 to 5. The overall value of an asset (OA) is calculated by counting of all parameters divided by 3 (OA=(A+B+C)/3). Each level of individual factors are described also by short description, see Table 2, 3, 4.

Table 2. Confidentiality (A)

Level	Description
1	Publicly accessible assets
2	Accessible assets within the organization
3	Assets that includes an organization's know-how; important to the organization's operations
4	The assets are not publicly accessible and their protection is required by legal regulations, other regulations or contractual arrangements (e.g., business secrets, personal data, …)
5	Assets are not publicly available and require above-standard protection beyond the previous category

Table 3. Availability (B)

Level	Description
1	Asset unavailability is not important and in case of unavailability, a longer correction period of about a month is normally tolerated.
2	Asset unavailability is not important and in case of unavailability, a longer correction period of about a week is normally tolerated.
3	Asset unavailability is maximally a day. The longer unavailability may cause a potential threat to the interests of the organization.
4	Asset unavailability is maximally a few hours. Any unavailability is necessary to solve immediately because it causes a direct threat to the interests of the organization. These assets are considered as very important.
5	Asset unavailability is not possible. Even long-time unavailability causes a serious threat to the interests of the organization. These assets are considered as critical.

Table 4. Integrity (C)

Level	Description
1	The asset does not require integrity protection.
2	The asset may need integrity protection. Impairment of the asset integrity may result in damage to the organization's interests by minor effects on the primary assets.
3	The asset needs integrity protection. Impairment of the asset integrity leads to damage to the organization's interests with a significant impact on the primary assets.
4	The asset needs integrity protection. Impairment of assets integrity leads to very serious damage to the organization's interests with indirect impacts on primary assets.
5	The asset needs integrity protection. Impairment of assets integrity leads to very serious damage to the organization's interests with direct and very serious impacts on primary assets.

4.2. Threat assessment

Threats are evaluated using probabilities of occurrence from 1 to 5, see Table 5. This probability is primarily based on experience from the past.

Table 5. Probability of asset occurrence (PoO)

Probability of Occurrence PoO	Value
Practically impossible occurrence	1
Not common, but can occur under special circumstances	2
Possible occurrence that has already occurred	3
Frequent occurrence	4
Too frequent (recurring) occurrence	5

4.3. Risk evaluation

The overall risk evaluation is calculated by multiplication of overall asset value and probability of asset occurrence (R=OA*PoO).

5. Benefits of ZOTY software

ZOTY's functionalities are designed to respect multiple different risk management approaches. From the simplest, when you don't engage in any risk analysis, you just select and implement a basic set of measures from a catalog. From the basic indicative risk analysis, which is possible quickly perform with the help of experienced experts in your field and then evaluate possible scenarios. Up to comprehensive and detailed risk analysis, including the assessment of assets, threats, and vulnerabilities.

Every data are together in one software and clearly visible. In one software can be assets (tangible, intangible), human resources, processes, projects, information (data, knowledge),… All these data are clearly stored and clearly sorted in folders in the asset register. If the predefined folder structure in the registered is not suitable, it is possible to simply create your own. Within a user-definable catalog. It is also possible to have even more such catalogs. The definition of each object stored and managed in the system ZOTY registry is unique. In the user catalogs there are only references to these object definitions in the registry. This eliminates any duplication and facilitates overall administration. The principle of registers and catalogs is common not only to different types of assets but also to requirements, objectives, risks, threats and vulnerabilities.

The software can be used by all key employees. It is possible to give them the appropriate roles (Risk Manager, Risk Owner, Internal Auditor, etc.) and allow them to collaborate comfortably with each other. I.e., communicate easily in the system in the form of shared comments or tasks involved in the overall context.

It is also possible to use the software for internal or external audits where requirements of legislation, internal regulations, ISO standards or contracts are necessary to control. It is possible to create or import these documents into the ZOTY registry simply. Then it is possible to create and attach a user-understandable request to each paragraph or specific paragraph of the law, or any other type of document, and assign to it a responsible person. Then it is possible to link it all to the risk, any type of asset, target, or other related requirements. The clear link between the responsible person, the requirements and the requirements solution throughout the risk management system is visible (i.e., for example, what critical assets have been identified, what threats they face despite what vulnerabilities, how high is the risk of damage to the asset, whether and what measures you take to minimize the risk, etc.)

The registers are ready to import data from external systems and their regular synchronization. Typically, for example, organizational structures and human resources from personnel modules of information systems or IT assets from configuration management database (CMDB). From process modeling tools, the processes and activities with associated risks are visible. The same applies to projects that are risks to project objectives. The result is up-to-date and consolidated data that enters the entire risk management system on a unified ZOTY platform. It follows that this solution saves time and reduces error rates.

6. Conclusion

In this paper, we presented a software solution for implementation in small and medium size enterprises. The research of available solutions for risk management on the market is presented in the first part of this paper. The pros and cons of available solutions were founded and compared. This study shows that complex software with all intended functions was not available at a comparable price level which is acceptable for SMEs. The software platform has implemented many methodologies for risk management. These methods are not possible to describe in the paper due to the limited length. It follows that only one method was described in the paper as an example. Also, the benefits of our software ZOTY were described in the paper. Our solution is reasonably priced and is suitable for SMEs.

Acknowledgments

References

- Advanced Risk Management, s. r. o. (2019) *Advanced Risk Management*. Available at: https://www.arm.cz/?lang=en.
- Berg, H.-P. (2010) 'Risk management: procedures, methods and experiences', *RT&A*, vol.1(17), pp. 79–92.
- Falkner, E. M. and Hiebl, M. R. W. (2015) 'Risk management in SMEs: a systematic review of available evidence', *The Journal of Risk Finance*, 16(2), pp. 122–144. doi: 10.1108/JRF-06-2014-0079.
- Malik, S. A. and Holt, B. (2013) 'Factors that affect the adoption of Enterprise Risk Management (ERM)', *OR Insight*, 26(4), pp. 253–269. doi: 10.1057/ori.2013.7.
- MEGA International (2020) *HOPEX GRC*. Available at: https://www2.mega.com/en/lp/report/managing-and-modeling-grc-dynamic-environments-mega-hopex-grc-solutions.
- Mohammed, H. K. and Knapkova, A. (2016) 'The Impact of Total Risk Management on Company's Performance', *Procedia - Social and Behavioral Sciences*, 220, pp. 271–277. doi: 10.1016/j.sbspro.2016.05.499.
- RSA Security LLC. (2020) *RSA Archer Platform*. Available at: https://www.rsa.com/en-us/products/integrated-risk-management/archer-platform.
- SWORD (2020) *Active Risk Manager (ARM)*. Available at: https://www.sword-activerisk.com/products/active-risk-manager-arm/.
- Thomson Reuters (2012) *Accelus Risk Manager*. Available at: https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/governance-risk-compliance/fact-sheet/accelus-risk-manager.pdf.

Biographies

Martin Hirman is a member of the Regional Inovation Centre of Electrical Engineering and of the Department of Technologies and Measurement at the University of West Bohemia in Pilsen. In 2013 he obtained masters degree in Commercial Electrical Engineering at University of West Bohemia in Pilsen, diploma thesis "Optimization stock processes". In 2017 he obtained doctors (Ph.D.) degree at University of West Bohemia in Pilsen, Faculty of Eletrical Engineering, Department of Technologies and Measurement. The topic of his dissertation was "Material and process aspects of components connecting to flexible substrates".

Andrea Benesova is a president of University of West Bohemia IEOM chapter. She obtained bachelor degree in Commercial Electrical Engineering at the University of West Bohemia in Pilsen in 2013. In 2015 obtained master degree in Commercial Electrical Engineering at the University of West Bohemia in Pilsen, diploma thesis "Analysis and modeling of selected processes in electrical engineering production ". From 2015 to present she is a Ph.D student at the University of West Bohemia in Pilsen, Faculty of Electrical Engineering, Department of Technologies and Measurement, topic of her doctoral thesis is "Management of prospective technological processes in electrical engineering". Her fields of study are Industry 4.0,

Maturity Model for Industry 4.0, Education 4.0, Process Management and Risk Management. She has published conference papers such as Requirements for Education and Qualification of People in Industry 4.0 or Determination of Changes in Process Management within Industry 4.0.

Michal Svehla is a vicepresident of University of West Bohemia IEOM chapter. He is also a student of doctoral study program at faculty of Electrical Engineering University of West Bohemia in Pilsen. Before doctoral study he earned Bachelor and Master degree in the same University as mentioned above. His research interests include e-Health/healthcare, processes, optimization.

Jiri Tupa received his MSc (2002) and PhD (2006) in Electrical Engineering from Faculty of Electrical Engineering, University of West Bohemia in Pilsen in Czech Republic. He is a Vice-dean of faculty and Senior Lecturer at Department of Technologies and Measurement. Dr. Tupa is member of executive management at Regional Innovation Centre for Electrical Engineering of the Faculty of Electrical Engineering at the University of West Bohemia in Pilsen. He is also PhD supervisor, reviewer of journal and conference publications and co-organizer of conferences. His research interests include Business Process Management, Quality Management, Risk and Performance Management in Electrical Engineering Industry, Industrial Engineering, Electronics Manufacturing and Diagnostics, Financial and Project Management, Copyrights and patents law, information law and transfer of IPR. Jiri Tupa is responsible for several international research and development projects with industrial and University partners. The project RiMaCon - Risk Management Software System for SMEs in the Construction Industry is one of the important international projects. This project has received funding from the European Union's Seventh Framework Program for research; technological development and demonstration (2013-2017). The RiMaCon project's main goal is to implement a collaborative effort to promote the sharing of knowledge and competencies in a long-term strategic research partnership around the development, testing and validation of a cost effective and user-friendly risk management system for SMEs in the construction sector.

Frantisek Steiner was born in Rokycany in 1973. He was awarded an Ing. (MSc) degree in the field of Applied Electronics in 1996, a PhD degree in the field of Electronics in 2001 and an Associate Professorship in Electrical Engineering in 2008. He is an Associate Professor at the Faculty of Electrical Engineering of the University of West Bohemia. He is the head of the Diagnostics and Testing Engineering Team at The Regional Innovation Centre for Electrical Engineering (RICE). His research fields include risk management, information security management systems and IT services management. He has published more than 120 papers and presented 45 contributions in 35 congresses.

Tomas Rericha is a member of the Department of Technologies and Measurement at the University of West Bohemia in Pilsen. He received his Ph.D. degree in 2007. He focused on the optimization and simulation of industrial processes and the implementation of lean manufacturing in production companies. He is currently working as secretary of the Department of Technology and Measurement.

Zdenek Kocourek has been working as a Business Process Management (BPM) consultant since 2003. Customers can benefit in his person from brilliant harmony of business processes knowledge, strategy planning and ICT awareness. These key competencies led him from his very first steps to domain of EA (Enterprise Architecture). On the top of that he is used to utilizing widely known and accepted frameworks (TOGAF, ArchiMate, Zachman, ITIL, etc.) together with leading process platform ARIS and integration component DataLink while being involved in BPM projects. Through his certification in TOGAF and ARIS (certified professional), years of experience together with tons of successful customer's projects from various field such as Engineering, Construction, Automotive, Healtcare, Utilities, Public sector, there can be no doubts about his competencies. He received recognition for his professional skills and passionate approach by board of the Custom Administration of the Czech Republic in project of successful complex implementation of BPM, process performance and optimization. Besides work on projects Zdenek demonstrates his skills as a lector who trains and coaches experts in the field of Enterprise Architecture Management (EAM) as well as an implementation of Integrated Management Systems.
Since 2009 Zdeněk has been giving presentations at various Czech universities and professionally focused conferences as well.

Petr Humpolicek has 20 years of working experience in ICT field. He has 10 years of experience with leading of people and projects in field of implementatiton of complex ERP system for manufacturing and trading companies. He is a founder of IDS Advisory s.r.o. company. He participated in successful R&D of DataLink's own software solution for simple integration scenarios connecting ARIS process platform with external ones systems. He built an application support center for the ARIS process platform products at Škoda Auto and conclude a long - term contract for security of worldwide technical support for users of VW Group companies. He participated on sales of software process platform including risk management and process performance measurement at the Ministry of Defense.