IT RISK MANAGEMENT AND APPLICATION PORTFOLIO MANAGEMENT

Kovácsné Mozsár A.L., Michelberger P.[*]

Abstract: The article gives a new approach based on the ISO 31000, IT risk management and application portfolio management how an integrated methodology can support the safety operation within organizations. The aim of this article to understand the basic principles of the ISO31000, IT risk management and application portfolio management (APM) and to provide a new point of view for large organizations how they should analyse and integrate their different management areas following the different standards if they are able. The new approach is to give an overview about the frameworks and possible link points between the different guidance in overall management level.The result of this study to present the importance of integrating different management areas in IT. The daily and effective operative cooperation between IT risk management and application management areas will ensure more transparent and safety operations within organizations.

Key words: risk management, ISO31000, IT risk management, application portfolio management, IT risk

DOI: 10.17512/pjms.2018.17.2.10

Article's history:
Received October 22, 2017; *Revised* November 29, 2017; *Accepted* December 28, 2017

Introduction

Many different guidance and principles gives support for the organizations how they can define, assess and measure, and manage the business and IT risks of the enterprises: ISO/IEC 27001, ISO/IEC 27005, ISO 31000:2015, AS/NZS 4360:2004, (Standards New Zealand., 2004), COSO Enterprise Risk Management Framework, (COSO, 2004), Risk IT, (ISACA, 2009).The business risk effects the business performance (Kiseľákováet al., 2015) and IT risk effects the IT operations and performance. These principles, frameworks as part of the IT Governance they provide strategic alignment between the IT and business within an organization (Debreceny, 2013).We will give a short summary about 2 standards in our approach: ISO31000 and Risk IT.
After a brief introduction the article will sketch some possible connection points between IT risk management and application portfolio management.
The following hypotheses were set up with our research:
H1: Current risk management standards, guidelines, frameworks do not cover fully the demand on IT risk management of today's enterprises.

[*] **Alice Lívia Kovácsné Mozsár, Dr. Pál Michelberger,** Óbuda University, Keleti Faculty of Business and Management
✉Corresponding author: mozsar.livia@kgk.uni-obuda.hu
✉ michelberger.pal@kgk.uni-obuda.hu

H2:The IT risk management should be integrated part of the application portfolio management within organizations to support enterprise security.

The article provides an overview where the integrated application portfolio and IT risk management in corporate strategy as key part of the strategic decision making. Integrating those management areas can be a good base for the security management within companies. Currently there is no exact methodology for measuring, controlling the security level of different applications.

Our approach is to give a short overview about ISO31000, IT risk management and application portfolio management, and how those management areas can ensure and continuously support the overall IT strategy.

If the risk management is integrated into the overall management systems, it ensures effective cooperation between the different areas and consistent approach across the enterprise. Risk management creates value for companies and improves the efficiency and effectiveness. Most of the companies deal with many thousands of confidential data, customers, rating agencies, regulators (FFIEC-Federal Financial Instructions Examination Council's) and corporate governance increasing their interest on how companies manage their risks. Risk management is an important element of the rating agencies as well. (Moody, Standard and Pool's).As we know the most important IT risk is the cyber risks, problems for companies and they need to looking into potential solutions. One question is who should manage this IT risk within the organization. This risk is a business or a technical issue? We think if there is continuous cooperation between the IT departments and the business departments, units, it is easy to find answer, solution for this question.

Introduction to ISO31000

ISO 31000 explains and provides basic methods on how to assess, measure, control, and monitor different risks. It is a set of principles which provides guidelines for companies how to design, implement, monitor, review and improving their risk management processes. It has three components: principles, processes and framework.

Some basic definitions related to ISO 31000:

Risk: Effect of uncertainty on objectives.

It is possible to apply the objectives on different levels within organizations, like strategic management level, programs, projects, processes levels (ISO31000).

Risk management: Coordinated activities to direct and control an organization with regard to risk (ISO31000).

Risk management framework: Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improvingrisk management throughout the organization (ISO31000).

Risk management policy: Statement of the overall intentions and direction of an organization related to risk management (ISO31000).

Risk management process:Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoringand reviewing risk(ISO31000).

ISO31000 makes reference that the organizations need to identify their risks, tools, techniques and find out how to implement those items into their current processes or creating new processes.The missing elements of this standard is that it doesn't give details to organizationson how to deal with and assess their IT risks.Since 2009 aninformation technology continuously has been developing rapidly and ISO31000 is not suitable anymore to handle and support all risks highlighting the IT risks within enterprises.

Understanding, implementing and using ISO31000 standard requires support from the management. For IT companies and IT departments essential requirement to implement a centralized and integrated process-base risk management apporach. Continuous comparing and analyzing methodology is very important in the risk management area (Béatrix et al., 2017).

Most of the literature and COSO Enterprise Risk Management Framework (ERM) defines the different kind of risk. In our approach in this article we will focus on information technology processes within the organization.

Some risk examples are listed below:

— Strategic: innovation, customer, planning etc.,

— Operational:technology,communication,emerging,human capital etc.

— Financial:credit, market, asset,interest, inflation,valutation etc.

— Other: project, Environmental,ThirdParty,Investment etc. (COSO, 2004).

With the rapid development of information technology it was required to pay more attention and specially define risks categories which can outcrop in the information technology area and how they are related to information technology processes. Those risks and framework will be presented in the next section.

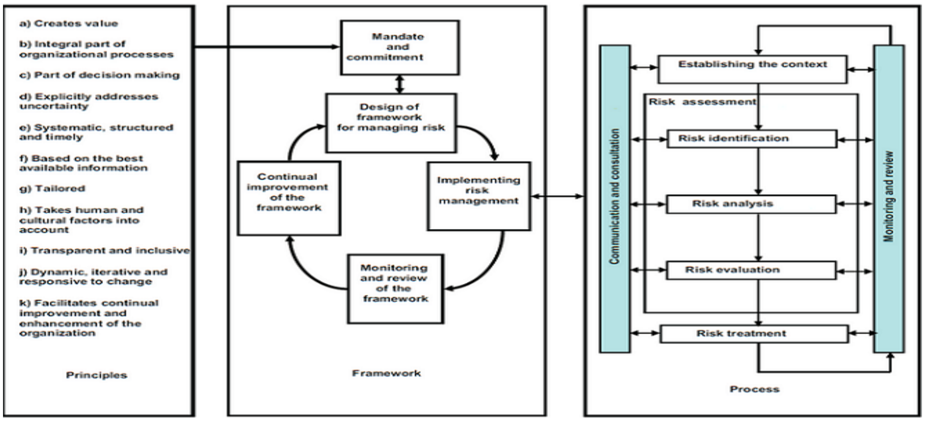

a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
Principles
Mandate and commitment
Design of framework for managing risk
Continual improvement of the framework
Implementing risk management
Monitoring and review of the framework
Framework
Communication and consultation
Establishing the context
Risk assessment
Risk identification
Risk analysis
Risk evaluation
Risk treatment
Monitoring and review
Process

Figure 1. Relationship between the risk management principles, framework and processe s*(ISO31000)*

Introduction to IT Risk Management

Open Group survey refers that 63% of the surveyed organizations use more than one framework to manage their IT risks. The most frequently used are: ISO/IEC 27001, ISO/IEC 27005, and ISO 31000 and they follow the FAIR/Open FAIR, NIST standards, and COBIT (OpenGroup, 2015).

The risk IT framework was developed by ISACA in 2009, because standards did not define the IT risks and their management steps. The framework includes guidance and principles about IT risks and it is based on the ERM. Definitions related to IT risk management:

IT risk: The IT risk is business risk related to the use of IT(ISACA,2009).

IT risks are related to IT projects, software projects, special types of IT systems, technologies, infrastructure (Susan and Steven, 2004).

The model includes COBIT and Val IT and ERM principles as well. The IT risk model gives a comprehensive view on IT related risks and provides detailed process model with guidelines. To asses, gather, list and register all IT risks into an IT risk portfolio can increase the efficient and accurate management of IT risks (Jordan, 2005).

The risk IT framework includes 3 domains: risk governance, risk evaluation and risk response (ISACA, 2009).

Risk governance: Ensures that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return (ISACA, 2009).

Risk evaluation: Ensures that IT-related risks and opportunities are identified, analysed and presented in business terms (ISACA, 2009).

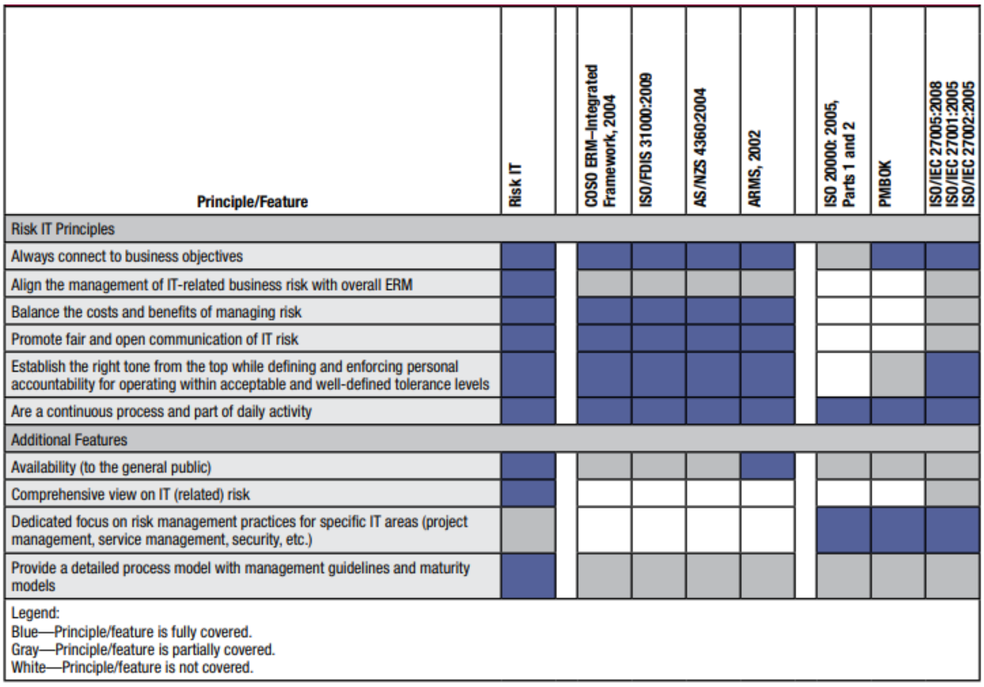
Risk response: Ensures that IT related risk issues, opportunities and events are addressed in a cost-effective manner and are in-line with business priorities (ISACA, 2009).

The framework defines the IT risk into 3 categories:

- Benefits/value enablement risks: these risks which are associated with missed opportunities.With cloud solutions,some benefits are: potential cost saving, time saving, easy deployment and increased flexibility and agility, easier evolution of technology. (Olszak, 2014) As an example: if a company does not pay attention to new technologies like cloud solutions. With this technology, enterprises are able to make their business processes and operationsmore effective(ISACA, 2011).
- IT programme and project delivery risk: the risks associated with continuous change. Changing existing technical solutions, or implementing new one through transformations programmes and projects bring many different unmanaged or misunderstood IT risks (ISACA, 2009).
- IT Operations and service delivery risks: these risks which are associated with the existing daily processes, environments, and IT systems (hardware, software etc.) and with changing them. Failures are related to Business Continuity

Planning (BCP), Disaster Recovery (DR), problem management processes, unresolved security issues etc. (ISACA, 2014).

ISACA defined that COSO ERM and ISO31000 Frameworks do not give focus on IT risk and to specific IT areas, like project management, service management and security(ISACA,2009) (Figure 2.).It becomes a challenge for large organizations to deal with IT risks and manage as they cannot fully implement the COSO ERM and ISO31000 standards and recommendations. As a solution, the enterprises need to build their IT Risk Management (ITRM) framework. Measuring, controlling, managing the different IT risks is a new challenge for the companies. The registration of the different risks is difficult and unresolved.



Principle/Feature	Risk IT		COSO ERM–Integrated Framework, 2004	ISO/FDIS 31000:2009	AS/NZS 4360:2004	ARMS, 2002		ISO 20000: 2005, Parts 1 and 2	PMBOK	ISO/IEC 27005:2008 ISO/IEC 27001:2005 ISO/IEC 27002:2005
Risk IT Principles										
Always connect to business objectives	🟦		🟦	🟦	🟦	🟦		▩	🟦	🟦
Align the management of IT-related business risk with overall ERM	🟦		▩	▩	▩	▩		⬜	⬜	▩
Balance the costs and benefits of managing risk	🟦		🟦	🟦	🟦	🟦		⬜	⬜	▩
Promote fair and open communication of IT risk	🟦		🟦	🟦	🟦	🟦		⬜	⬜	▩
Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels	🟦		🟦	🟦	🟦	🟦		⬜	▩	🟦
Are a continuous process and part of daily activity	🟦		🟦	🟦	🟦	🟦		🟦	🟦	🟦
Additional Features										
Availability (to the general public)	🟦		▩	▩	▩	🟦		▩	▩	▩
Comprehensive view on IT (related) risk	🟦		⬜	⬜	⬜	⬜		⬜	⬜	▩
Dedicated focus on risk management practices for specific IT areas (project management, service management, security, etc.)	▩		⬜	⬜	⬜	⬜		🟦	🟦	🟦
Provide a detailed process model with management guidelines and maturity models	🟦		▩	▩	▩	▩		▩	▩	▩

Legend:
Blue—Principle/feature is fully covered.
Gray—Principle/feature is partially covered.
White—Principle/feature is not covered.

Figure 2. Risk management frameworks and standards compared *(ISACA, 2009)*

Identifying and mitigating IT risks are part of the IT risk management process. There are different information technology risk mitigation tools to support the management, but they are not providing risk reduction advice (Anthony, 2015). IT risk management is highly recommended, as it creates and protects value for the companies.

Some created values:

“Protecting core business processes and data from disruption or corruption via cyber-attack, protecting customer data and funds, protecting company confidential information.”

“Prevented unnecessary activity thereby creating opportunity cost savings.”

Some protected values:
"The process has brought to light many issues in our business that had more risk than leadership had thought. The process brought that to light with some risks mitigated."
"Ensures priorities for implementing security controls." (Open Group, 2015).
This framework is one step in the right decision for organizations. It supports the bottoms up approach for organizations. Senior management and executives are encouraged in this framework. It focuses on improving the current IT controls rather than recommending new investments to IT control.
Based on Deloitte survey over 60% of respondents answered: IT risk exposure had increased in the last 12 months. The major IT risks are the new markets and business changes, technical needs changing, disruptive technology entrants, cyber risks, implementation of new technologies and platforms. The top 5 IT risks in 2016: vulnerability to external threats, loss of sensitive client or proprietary data, inability of the IT function to keep up with the pace of change required, inedaquate oversight of third parties and loss of operational capability due to a lack of a sufficient organisational resilience capability (Deloitte, 2016). Enterprises realize the need of IT risk management. It is a strategic business objective to focus on IT risk management. Most of the companies don't have stable IT risk management program. For effective IT risk management is very important to establish a good organizational and management reporting structure, because the board leadership and Chief Information Officer (CIO) reporting structure effects the IT risk management processes within an organization (Vincent et al., 2017).

Introduction to Application Portfolio Management

Application portfolio management (APM) is becoming mandatory elements in the digital firm's years for companies to manage their applications. APM is a framework.
"[APM] is really about implementing a repeatable process to assess what we have, and, if an application is not performing or does not meet our architectural requirements, eliminating it, and replacing it with a better performing application. We're doing it to try and reduce the money we spend on maintaining existing applications (that don't perform well) and freeing up that money to invest in new and better performing applications."NASA's Office of the Chief Information Officer (Aspireys).
Application rationalization supports the cost reduction goals in the IT areas and allocates the resources to different areas within organization. Applications or assets support the daily business process. An application or asset can be: Word documents, programs as well. APM helps to reduce the number for redundant applications, IT costs, identify the most critical applications to the business with listed business functions. This management area has focus on which applications should maintain, invest, retire or consolidate.

Measuring and analysing the business value of the applications can assess cost savings and grow on IT investments. Rationalisation of IT applications in the application portfolio can support the cost-effectiveness within organizations (Lily et al., 2016).

APM defines how the IT should look in the future, what the roadmap is for the changing with IT technologies. It helps to understand the IT costs, achieving savings with resources optimizations. APM is one key element of the IT strategy decisions for the CIO in large companies. It provides consistent, up-to date, vital information about enterprise for risk management. APM gives a good picture about the values of each application, health of IT infrastructure and it creates a scoring framework.

Integrated IT Risk and Application Portfolio Management

The literatures treat the above described standards, frameworks as a unit, and does not take into consideration that big companies have big complexity. Part of the company IT strategic management is that application portfolio management and IT risk management should work as a consolidated management area as both areas brings value to the business and ensure the secure operations within company. There is no alignment cooperation between these two management areas.Organizations have risk management and some of them separate the application portfolio management. APM framework and IT risk management framework are regulated separately.

As part of the IT risk management process the key players and experts should build an IT risk portfolio and after this to integrate and monitor the IT risks.Next step should be to assign the IT risks to applications.

Related to the APM are the key players monitoring and reporting the risks related to the application without specific knowledge. In the IT risk management framework the application is mentioned as an "other enterprise architecture "component. (ISACA, 2009). However, this component, the application is one, that directly supports the business and business users use them directly. Any transformation or change effects the applications and thereby the associated IT risks as well.

In large companies where the number of applications are many hundreds or thousands it is a challenge to assess and measure the IT environment and technology.

Identifying, assessing, managing the IT risks related to information systems is a key activity. Organizations need to focus on legacy applications which are the most expensive and carry greatest risk. The business needs to collaborate with the IT areas identifying the risks related to their business functions as the business functions are in the information systems and the information systems are managed by IT. IT risk management area has the specific, right knowledge to assess, identify, analyse and evaluate the different IT risks related to applications. With the integrated operation, all the IT risk associated with applications would be adequately addressed and managed. Addressing, managing applications and the IT risks an IT risk management information system is essential to develop and use to support the integrated operation work between these two management areas. Based on (Grob et al., 2008) model it needs to be developed with the application portfolio related IT risks and to store and manage all IT risks and information application elements in one database.

Business critical data are stored and managed by IT. Risk management steps, principles should appear in most of the management areas within companies. In our opinion to apply this model, it is necessary to involve many experts and the management support is also an essential element.

Comparison with Other Studies

SANS had a survey on Application Security Programs and Practices with 700 participants in 2012. The researches present the answer for some specific questions related to managing application and application risks.28% of respondents don't know how many applications they manage. The organizations have demand on application security programs and they use already something, but they need to improve it or to implement another one (Bird and Kim, 2012).

Tata Consulting Company has published the next generation APR Framework in 2011. One of the principles is to analyse and cover all risks related to applications in the application lifecycle. Application portfolio risk: Assesses the level of risk to business in terms of the probability of failure or degradation of functionality as well as the extent of impact on business operations due to application, vendor or platform obsolescence (TATA, 2011). The study identifies four different risk categories: operational risks, risk of failure, system complexity and application support risk. The study doesn't go into detail about IT risk management steps, it focuses on IT risks which are associated to applications. Our suggestion is to create an IT risks portfolio as part of the IT risk management and then to assign the IT risks to applications in the application portfolio.

Managerial Implications of the Research

The study focuses on highlighting the importance of relationship between application portfolio management and IT risk management. By establishing cooperation between the two management areas can increase security in companies.Companies need to see the risks associated with their applications. The FERMA (Federation of European Risk Management Association) conducted a survey with 634 participants in 2016. The researches show that the cyberproblem is classified as an IT risk, but the IT departments don't show continuous, effective and close cooperation with other organizational units (FERMA, 2016). Follow the safety rules and regulations are mandatory for organizations. If organizations don't have a centralized, transparent inventory for applications how they can assess, define, measure, control the associated risks? The relevance of IT risk management increasingly importantfor companies because of using new technologies such cloud solutions.

Summary

The new approach in this article provides an opportunity for large companies to redesign their organizations structures and to ensure a more efficient management in the IT field, including APM and ITRM integration. As the ISO 31000 does not give principles, guidance to some IT areas, we focused on some linking between APM and ITRM. Companies use more than one framework or standard to manage their IT risk.ISACA IT risk management defines the application as an asset, resource which helps to support and achieve business goals. This framework can be expanded how to determinate IT risks which are associated with applications and give focus on application portfolio management. The assumption of this article is that the two management area's cooperation increases the safety operations within organizations and the ITRM should focus how ITrisk management as an integrated part of an organizational processes.Top management support is essential for this coordinated operation.The outlined interfaces between these two management areas give opportunity for further research, to design, develop the detailed steps.We think that an integrated model could help companies in their everyday operations.

References

Béatrix B., Antoni-L.M., Antonai M., 2017, *Integrating risk management in IT settings from ISO standards and management system perspectives,*"Computer standards and Interfaces", (54/3)

Bird J., Kim F., 2012, *SANS Survey on Application Security Programs and Practices,*Available at: https://www.sans.org/reading-room/whitepapers/analyst/survey-application-security-programs-practices-35150, Access on: 26.11.2017.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004, *Enterprise Risk Management Integrated Framework,* Executive Summary.

Debreceny R.S.,2013,*Research on IT governance, risk, and value: Challenges and opportunities, "*Journal of Information Systems", 27(1).

Deloitte, 2016, *EMEA Financial Services IT Risk Management Survey*, Available at: https://www2.deloitte.com/uk/en/pages/risk/articles/it-risk-management.html, Access on: 28.03.2017.

FERMA, 2016, *Risk Management Benchmarking Survey 2016*, Available at: http://www.ferma.eu/app/uploads/2016/09/FERMA-European-Risk-and-Insurance-Report-Full-set-of-results.pdf, Access on 24.11.2017.

Grob L., Strauch G., Buddendick C., 2008,*Conceptual modeling of Information Systems for Integrated IT-Risk and Security Management,*Proceedings of the 2008 International conference on Security and Management, SAM 2008.

ISAC, 2009, *The Risk IT Framework,* Available at: http://www.isaca.org/knowledge-center/research/documents/risk-it-framework-excerpt_fmk_eng_0109.pdf, Access on: 19.11.2016.

ISACA, 2014, *Assessing and Managing IT Operational and Service Delivery Risk*, Available at: https://www.isaca.org/Journal/archives/2014/Volume-5/Documents/Assessing-and-Managing-IT-Operational-and-Service-Delivery-Risk_joa_Eng_0914.pdf, Access on: 19.01.2017.

ISACA, 2011, *Control Objectives for Cloud Computing: Controls and Assurance in the Cloud* Available at: https://www.isaca.org/chapters2/kampala/newsandannouncements/Documents/IT%20contro%20objectives%20for%20Cloud%20computing.pdf, Access on: 18.02.2017.

ISO 31000, 2015, *ISO 31000 Risk management-Principles and Guidelines: 2015*, Available at:https://www.iso.org, Access on: 03.04.2017.

ISO/IEC 27001, 2013, *Information security management: 2013*, Available at: https://www.iso.org, Access on: 03.04.2017.

ISO/IEC 27005, 2011, *Information security risk management:2011*, Available at: https://www.iso.org, Access on: 03.04.2017.

Jordan E., 2005, *An integrated IT risk model*, PACIS.

Kiseľáková D., Horváthová J., Šofranková B., Šoltés M., 2015, *Analysis of risks and their impact on enterprise performance by creating enterprise risk model*, "Polish Journal of Management Studies", 11.

Lily S., Kecheng L., Dian I., Vaughan M., 2016, *Evaluating business value of IT towards optimisation of the application portfolio, "*Enterprise Information Systems", 10(4).

Olszak C.M., 2014, *Business Intelligence in cloud*, "Polish Journal of Management Studies", 10.

Open Group, 2015, *IT Risk Management Survey Summary,*White Paper, Available at: https://www2.opengroup.org/ogsys/catalog/w154, Access on: 12.02.2017.

Standards New Zealand, 2004, *AS/NZS 4360:2004*, Access on: 14.03.2017.

Susan A.S., Steven A., 2004, *Information System risks and risk factors: Are they mostly about information systems? "*Communications of the Association for Information Systems", 14.

TATA Consultancy Services, 2011, *Next generation application portfolio rationalization*, White Paper.

Vincent N.E., Higgs J.L., Pisnker R.E., 2017, *IT Governance and the maturity of IT risk management practices*, "Journal of Information Systems", 31(1).

ZARZĄDZANIE RYZYKIEM IT I ZARZĄDZANIE PORTFELEM APLIKACJI

Streszczenie: W artykule przedstawiono nowe podejście, oparte na ISO 31000, w zarządzaniu ryzykiem IT i zarządzaniu portfelami aplikacji. Opisano w jaki sposób zintegrowana metodologia może wspierać operacje bezpieczeństwa w organizacjach. Celem tego artykułu jest zrozumienie podstawowych zasad ISO31000, zarządzania ryzykiem IT i zarządzania portfelem aplikacji (APM) oraz przedstawienie nowego punktu widzenia dla dużych organizacji, w jaki sposób powinno się analizować i integrować różne obszary zarządzania zgodnie z różnymi standardami, jeśli to możliwe. Nowe podejście polega na przedstawieniu przeglądu ram i możliwych powiązań między różnymi wytycznymi na ogólnym poziomie zarządzania. W wyniku tego badania przedstawiono znaczenie integracji różnych obszarów zarządzania w IT. Codzienna i efektywna współpraca operacyjna między zarządzaniem ryzykiem IT a obszarami zarządzania aplikacjami zapewni bardziej przejrzyste i bezpieczniejsze operacje w organizacjach.

Słowa kluczowe: zarządzanie ryzykiem, ISO31000, zarządzanie ryzykiem IT, zarządzanie portfelem aplikacji, ryzyko IT

IT风险管理和应用程序组合管理

摘要：本文提出了一**种基于**ISO31000，IT风险管理和应用程序组合管理的新方法，该方法可以帮助组织内的安全操作。本文旨在理解ISO31000，IT风险管理和应用程序组合管理（APM）的基本原则，并为大型组织提供一个新的观点，他们应该如何分析和整合不同管理领域，遵循不同的标准他们能够。新方法是概述整体管理层面不同指南之间的框架和可能的联系点。这项研究的结果表明了在IT中整合不同管理领域的重要性。IT风险管理与应用管理领域之间的日常和有效的操作合作将确保组织内更透明和安全的运营。

关键词：风险管理，ISO31000，IT风险管理，应用组合管理，IT风险