SOFTWARE DEVELOPMENT TEAMWORK FROM AN INFORMATION SECURITY PERSPECTIVE

SZOFTVERFEJLESZTÉSI CSOPORTMUNKA AZ INFORMÁCIÓBIZTONSÁG SZEMSZÖGÉBŐL

KERTI András[1] – NYÁRI Norbert[2]

Abstract

The present study demonstrates how to combine the international standard ISO/IEC 27005 and the US standard NIST SP 800-30 to perform risk analyzes, through the example of a fictional software development company. Starting with a brief introduction to the company, the reader can get acquainted with the basic concepts of the DevOps approach in order to have a more accurate view of the processes taking place within the development company. Subsequently, starting from the Hungarian regulatory environment, an overview is presented of the current state of information security standards, taking into account the NATO and ENISA information security product catalogues. After that an ISO-NIST combined risk analysis technique is briefly described, the foundations of which were laid in 2017 by Putra, Fandi A., and others. A simple example of the application of the technique is also shown.

Keywords

risk assessment, IT security, information security, standards theory, software development

Absztrakt

Jelen tanulmány egy kitalált szoftverfejlesztőcég példáján keresztül mutatja be, hogy hogyan kombinálható kockázatelemzések végrehajtása céljából az ISO/IEC 27005 nemzetközi és a NIST SP 800-30 amerikai szabvány. A cég rövid bemutatásától indulva az olvasó megismerkedhet a DevOps megközelítés alapfogalmaival, annak érdekében, hogy pontosabb rálátása legyen a fejlesztő cégen belül zajló folyamatokra. Ezt követően a magyar szabályozási környezetből kiindulva áttekintő képet kaphat az információbiztonsági szabványok aktuális helyzetéről figyelembe véve a NATO és az ENISA információbiztonsági termékkatalógusait. Ezt követően röviden ismertetésre kerül egy ISO-NIST kombinált kockázatelemzési technika, melynek alapjait 2017-ben fektették le Putra, Fandi A. és mások. A technika alkalmazására is láthatunk egy egyszerű példát.

Kulcsszavak

kockázatelemzés, IT biztonság, információbiztonság, szabványelmélet, szoftverfejlesztés

[1] kerti.andras@uni-obuda.hu | ORCID: 0000-0003-2149-5500 | associate professor, Faculty of Military Science and Officer Training of the University of Public Service | egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar

[2] nyari.norbert@uni-obuda.hu | ORCID: 0000-0003-0229-7584 | doctoral candidate, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

INTRODUCTION

Information security is a key factor in today's life, regarding that many aspects of our life depends on data stored and managed in various IT systems operated by either governmental bodies or business organizations.

This study aims to address the IT security aspects of the modern software development process including agile development, devops, cloud technology etc. In order to facilitate full understanding, the aforementioned methodologies and techniques shall also be briefly described.

After that a risk analysis shall be presented based on a fictional software development company called SoDevCo Ltd. (it stands for Software Development Company Ltd.). The complete risk analysis however would be way too lengthy to fit into an article like this, so I shall focus on the software development related risks.

The following section introduces the organization under inspection, the SoDevCo Ltd starting with a short historic overview.

SODEVCO LTD. COMPANY OVERVIEW

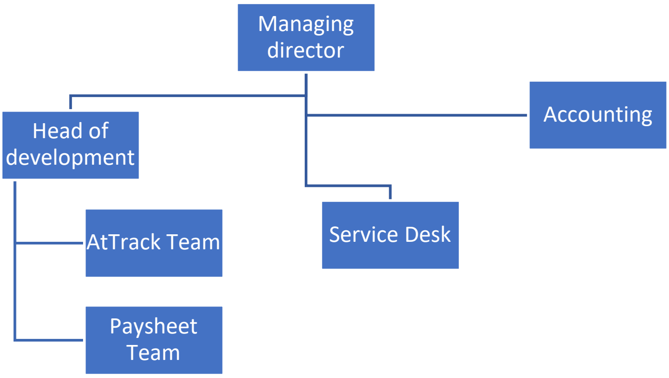
SoDevCo Ltd. is a fictional software development company based in Budapest, Hungary. The main activity of the company is the development of a cloud-based attendance tracking and payroll software. The owners of the firm are a Hungarian married couple. The husband is the managing director with a 90% share.

Founded in 2009, the company started to develop a payroll software called Paysheet with five developers. At first Paysheet was an on-prem intranet web application. A few years later, in 2014, thanks to the success of Paysheet, the company was able to embark on the development of a cloud-based attendance tracking software called AtTrack. In 2016 Paysheet was also moved to the cloud, however there are a few clients who still uses the on-prem version of Paysheet.

Since 2011 the company has an ISO 9001 certified quality management system. In 2012, the company introduced the self-developed payroll application for its own employees, and starting from 2018 AtTrack is also in use within the company.

The current organigram can be seen on the diagram below. Due to size constraints, I shall only describe IT-related organizational units in detail. The number of employees in the past years is ranging from 25 to 35. The company currently has two devops teams, one for each product. The teams are led by the Head of Development.

There is also a Service desk in the company with five employees. Led by a Service Desk Manager the four Service Desk Analysts provide the 1st line support of the company for the clients. It is a relatively newly established organizational unit, due to the growing clientele, operating since 2020 in an ITIL-like manner. The client-reported issues are stored in a third-party issue tracker application in the cloud, called JetBrains YouTrack with a monthly subscription.



1. Table: The organigram of SoDevCo Ltd. Self-editing.

The composition of the two DevOps teams is shown in the table below. Each of the teams has a product manager. They are in charge of the long-term product strategies and the roadmaps of each product; they also work on requirements coming from the clients. Sales activities are also performed by product managers, complemented by the managing director.

Role name	Paysheet Team	AtTrack Team
Product manager	1	1
Developer	6	5
Team lead	1	1
Tester	2	3
Cloud architect	1	2
System administrator	2	2

2. Table: Teams of SoDevCo Ltd. Self-editing.

Both teams have a Team lead, who works on the requirements in conjunction with the product manager, makes architectural decisions and delegates task to the team members. The cloud architects are specialized in cloud technologies, they are in charge of cloud architecture related tasks. Tasks of System administrators include operations related tasks, like cloud monitoring and 2nd line support, they are also in charge of the operation of the OpenVPN solution to support Home Office, and the on-prem third-party build server, called JetBrains TeamCity.

Among the developers there are experts of various fields related to both frontend and backend, they also provide 3rd line support if needed.

The codebase (the collection of all related source codes) of the two applications are also stored in the cloud, on GitHub.com. The scrum process of the developers is also supported by the aforementioned third-party issue tracker application, YouTrack. The team practices Continuous Integration, and Continuous Deployment.

The firm has an OpenVPN based infrastructure to support the telecommuting of mainly the System administrators. Telecommuting is the primary form of work from the spring of 2020, due to the COVID-19 situation. The main communication channel for teleworkers is a third-party cloud-based solution called Slack, with a monthly subscription.

One last thing before moving to the next topic is the pricing of the products of the company. Each product (Paysheet and AtTrack) has a monthly subscription-based licensing, having 3 plans (Free, Standard and Enterprise). The Free plan is quite limited though in both services and number of users. The Standard plan makes all services available to up to 100 users. The Enterpise plan is individually priced, supporting unlimited number of users

The company plans to implement an ISO/IEC 27001 certified information security management system, during the process a risk assessment must be done. [1] But before moving on to risk assessment, I shall introduce some basic concepts of DevOps.

The term DevOps however does not seem to have a concrete shared definition. [2] It is somewhat striking though that it comes from the combination of the words: developer and operations, being a practice based on close collaboration between software developers and software operators it aims to deliver services and applications quicker and more effectively than other conventional software development processes. [3] [4]

In the 2015 book DevOps: A Software Architect's Perspective the authors suggested a definition as follows "a set of practices intended to reduce the time between committing a change to a system and the change being placed into normal production, while ensuring high quality". [5]

DevOps however on its own is only a theoretical framework providing a seamless and cohesive functioning of the operations and development teams within the company when properly adapted utilizing tools and techniques like automation (infrastructure and tests), configuration management, monitoring and log management. One possible adaptation is the CAMS framework. [3] [4]

CAMS is an acronym for the words Community (or Culture), Automation, Measurement, and Sharing, which are the high-level concepts of the framework detailed as follows. [3]

Firstly Culture, DevOps mainly intended to eliminate conflicts of interest between developers and operators, so it deals with problems related to people and organizational culture. While developers tend to try out cutting-edge technologies and solutions, operators strive to maintain a stable environment and infrastructure. Traditionally developers and operators were often separated into different teams speaking "two different languages" making the situation even worse. Sharing responsibility is a major goal of DevOps. Culture can also bring in good practices like applying Scrum. [6] [7]

Secondly Automation, with proper automation significant amount of effort and money can be saved. Not only it speeds up the processes and the information flow but also minimizes human error. Two main concepts come along with automation: Infrastructure as Code and Continuous Deployment Pipelines. [6] [7]

Continuous integration is a primary DevOps practice of automating the integration of code changes from multiple contributors into a single software project, through the use of a central version control system. [8]

Continuous deployment (CD) is the process of rapidly deploying software or services automatically to end-users without any human interaction. If no automated test case or quality check fails the changes made to software and services are automatically deployed to production servers. Infrastructure as Code is a key element in implementing CD. [9]

Simply put, Infrastructure as Code (IaC) means managing an IT infrastructure using configuration files. In other words, IaC is the practice of automatically defining and managing system configurations through source code. [9]

Thirdly Measurement, measuring the correct metrics will help determine if progress is being made in the intended direction, they can also help in making the right decisions. [6] [7]

Sharing is the last word in CAMS, DevOps places a great emphasis on information exchange, transparency and openness. The team's comprehensive, collective knowledge greatly enhances its effectiveness. [6] [7]

In the 2019 article authors state that on one hand there is not enough evidence on DevOps facilitating software quality, on the other hand CAMS has a positive effect on it. [3]

In the following I shall present a quick review on various risk assessment frameworks.

RISK MANAGEMENT METHODOLOGIES

So many risk management methodologies exist that introducing all of them would surely not fit into this article, in the 2012 study "A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in Information Systems" the author stated that the number of the different available methods was about 200, so I shall describe only some of them based on the Hungarian regulatory environment. [10]

In 2008 the Hungarian Administrative IT Committee (Közigazgatási Informatikai Bizottság, KIB) published recommendations regarding IT security called Hungarian IT Security Recommendations (Magyar Informatikai Biztonsági Ajánlások, MIBA). The Hungarian IT Security Framework (Magyar Informatikai Biztonsági Keretrendszer, MIBIK) is one of these recomendations. [11]

MIBIK is a Hungarian framework for the management, requirements and examination of IT security, which is based on relevant international ISO standards, technical reports, NATO Council Memorandums and regulations of the European Union. [11]

Speaking of NATO and EU regulations, NATO has a website called NATO Information Assurance Product Catalogue (NIAPC), which provides a catalogue of Information Assurance products, Protection Profiles and Packages that are in use or available for procurement to meet operational requirements for NATO nations and affiliated civil or military bodies. [12]

The official website of European Union Agency for Cybersecurity (ENISA) states that "ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow." [13]

Should someone be interested in this topic the aforementioned product catalogues could serve as a good place to start for gathering information. During my research I have checked both of them for the products and technologies in this topic, I shall share my findings at the description of each product.

The Examination of IT Security Management (Informatikai Biztonság Irányításának Vizsgálata, IBIV) is a methodology providing unified approach for examining IT systems of an organization in order to be able to prove that the IT system meets its own security requirements and that security threats affecting interested external parties are duly taken into account. IBIV helps in conforming ISO/IEC 27001:2005 as well. [11]

IBIV recommends the performing of a risk analysis describing two different approaches. The first procedure is based on the NIST SP 800-30 and the FIPS 199 documents. This methodology allows for relatively simple risk assessment with little effort. The second approach is based on CRAMM (CCTA Risk Analysis and Management Method), which is costly, since it explores the risks of each and every threat. [11]

NIST (National Institute of Standards and Technology) is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce, promoting industrial competitiveness and innovation since its foundation. [14]

NIST has six research laboratories, one of them is ITL (Information Technology Laboratory). ITL is focusing on IT measurements, testing and standards. ITL publishes papers in numerous series, the two relevant to this article are FIPS PUBS (Federal Information Processing Standards Publications) and Special Publication (SP) 800 series. [14] The following table contains the relevant NIST publications.

NIST number	Title
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
SP 800-30 revision 1	Guide for Conducting Risk Assessments
SP 800-37 revision 2	Risk Management Framework for Information Systems and Organizations: A system Life Cycle Approach for Security and Privacy
SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
SP 800-61 revision 2	Computer Security Incident Handling Guide

3. Table: Relevant NIST publications. Self-editing.

SP 800-30 provide guidelines conducting risk assessments in accordance with other NIST recommendations standards aiming to promote the organization’s risk management abilities. [15]

SP 800-37 defines the Risk Management Framework which is a United States federal government policy and standards providing structured and yet flexible process for managing security and privacy risks relying on the concepts defined in FIPS 199, FIPS 200 and SP 800-53. [16]

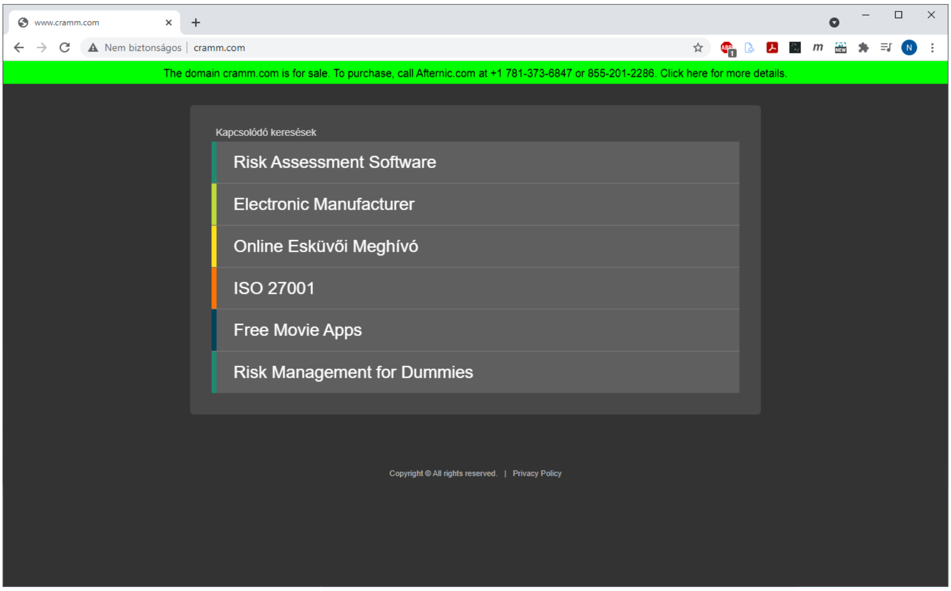
The 2002 version of SP 800-30 has an ENISA product page, but unfortunately the “Official website” link is outdated being broken. [17] NIAPC has no information on SP 800-30 whatsoever. [12]

The other method of IBIV is based on CRAMM. I was really trying to gather information on the CRAMM methodology. The ENISA product page for CRAMM states that CRAMM was created in 1987 by the Central Computer and Telecommunications Agency (CCTA), now renamed into Cabinet Office, of the United Kingdom government. It is currently on its fifth version, CRAMM Version 5.0. [18] CRAMM is stated to be a comprehensive risk assessment tool that's fully compliant with the British BS7799 and the international ISO/IEC 17799. [19]

Based on the Manufacturer's Brochure which can be downloaded from the NIAPC product page of CRAMM, the latest version of CRAMM supports ISO/IEC 27005. The NIAPC product page of CRAMM was updated in 2013 though, which was quite long ago. [19]

The two standards, ISO/IEC 17799 and ISO/IEC 27001, based on the BS7799 British standard, the former is derived from the BS7799:1 and the latter on BS799:2. [20] ISO/IEC 17799 was however superseded by the ISO/IEC 27002 in 2005. [21] With this in mind, CRAMM theoretically seems compatible with the ISO/IEC 27000 series.

CRAMM looks also somewhat neglected or abandoned, given that the official website domain name, www.cramm.com, is for sale at the moment as it can be seen on the figure below. [22] In addition, I have not been able to find any information on the Internet that proves CRAMM being either in effect or withdrawn.



The domain cramm.com is for sale. To purchase, call Afternic.com at +1 781-373-6847 or 855-201-2286. Click here for more details.

Kapcsolódó keresések

- Risk Assessment Software
- Electronic Manufacturer
- Online Esküvői Meghívó
- ISO 27001
- Free Movie Apps
- Risk Management for Dummies

Copyright © All rights reserved. | Privacy Policy

4. Table: www.cramm.com

However, the Hungarian IBIV is based on the ISO/IEC 27000 series of standards it never mentions ISO/IEC 27005 as an option for risk assessment, no wonder, because its first version was published in 2008, in the same year as MIBIK. [21] Given all the above information on MIBIK and CRAMM, performing a risk assessment based on ISO/IEC 27005 is not against the principles of MIBIK. On one hand MIBIK is a recommendation, this means no prohibition to deviate from its principles at all. On the other hand, the latest version of CRAMM supports ISO/IEC 27005 as stated before. [19] MIBIK however references the predecessor of ISO/IEC 27005, the ISO/IEC TR 13335-3 and ISO/IEC TR 13335-4. [11]

As for the Hungarian standards situation, according to the official site of the Hungarian Standards Board (Magyar Szabványügyi Testület, MSZT) the ISO/IEC 27001 was published in Hungary in 2014, but the naturalization of the other standards of the series has not started yet. ISO/IEC 27002 is published though in Hungary, but only in English. [23]

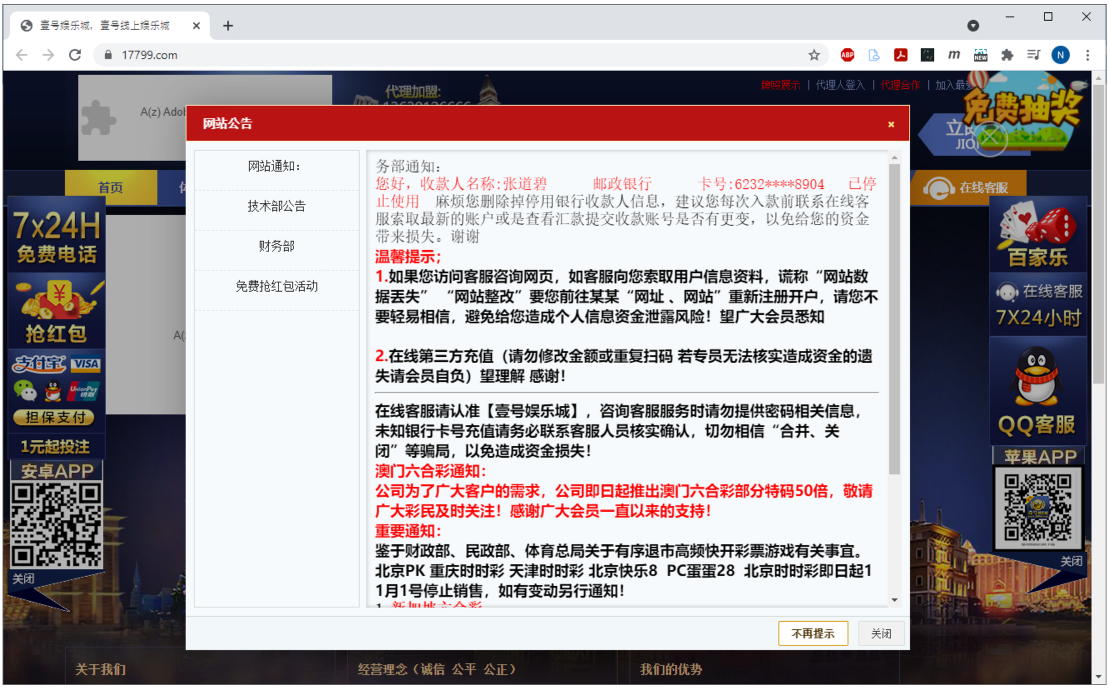
MSZT is an observing member of the ISO/IEC JTC 1/SC 27 technical committee which develops ISO/IEC 27005. [21] It would be highly desirable to be a participating member.

According to the official site of National Accreditation Authority (Nemzeti Akkreditáló Hatóság, NAH), nah.gov.hu five organizations are entitled to certificate ISMS's based on the MSZ ISO / IEC 27001: 2014 standard and two organizations are accredited to perform services based on MIBÉTS:2009. [24]

NIAPC does not seem to have anything on ISO/IEC 27000 series. [12] ENISA has a product page for ISO/IEC 27001 but it is way too much out of date. It has a link to www.17799.com, which is a working page, but its content has presumably changed significantly over the years for currently it seems to be a Chinese phishing site, as it can be seen on the figure below. [25]

Based on my experience with either NIAPC or the ENISA Catalogue they are unfortunately both seem to be somewhat outdated, neglected. A comprehensive content analysis and an analysis-dependent update should be considered.

Back to IBIV, the combined methodology proves to be a valid approach over the years though, since there are other studies that support its effectiveness. In the 2017 article "Design of Information Security Risk Management using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A Case Study at Communication Data Applications of XYZ Institute" the issue of combining ISO/IEC 27005 and NIST SP 800-30 had been discussed, resulting in a new technique for information security risk assessment. [26]



务部通知:
您好，收款人名称:张道碧 邮政银行 卡号:6232****8904 已停止使用 麻烦您删除掉停用银行收款人信息，建议您每次入款前联系在线客服索取最新的账户或是查看汇款提交收款账号是否有更变，以免给您的资金带来损失。谢谢

温馨提示;

1.如果您访问客服咨询网页，如客服向您索取用户信息资料，谎称"网站数据丢失" "网站整改"要您前往某某"网址、网站"重新注册开户，请您不要轻易相信，避免给您造成个人信息资金泄露风险！望广大会员悉知

2.在线第三方充值（请勿修改金额或重复扫码 若专员无法核实造成资金的遗失请会员自负）望理解 感谢！

在线客服请认准【壹号娱乐城】，咨询客服服务时请勿提供密码相关信息，未知银行卡号充值请务必联系客服人员核实确认，切勿相信"合并、关闭"等骗局，以免造成资金损失！

澳门六合彩通知:
公司为了广大客户的需求，公司即日起推出澳门六合彩部分特码50倍，敬请广大彩民及时关注！感谢广大会员一直以来的支持！

重要通知:
鉴于财政部、民政部、体育总局关于有序退市高频快开彩票游戏有关事宜。北京PK 重庆时时彩 天津时时彩 北京快乐8 PC蛋蛋28 北京时时彩即日起11月1号停止销售，如有变动另行通知！

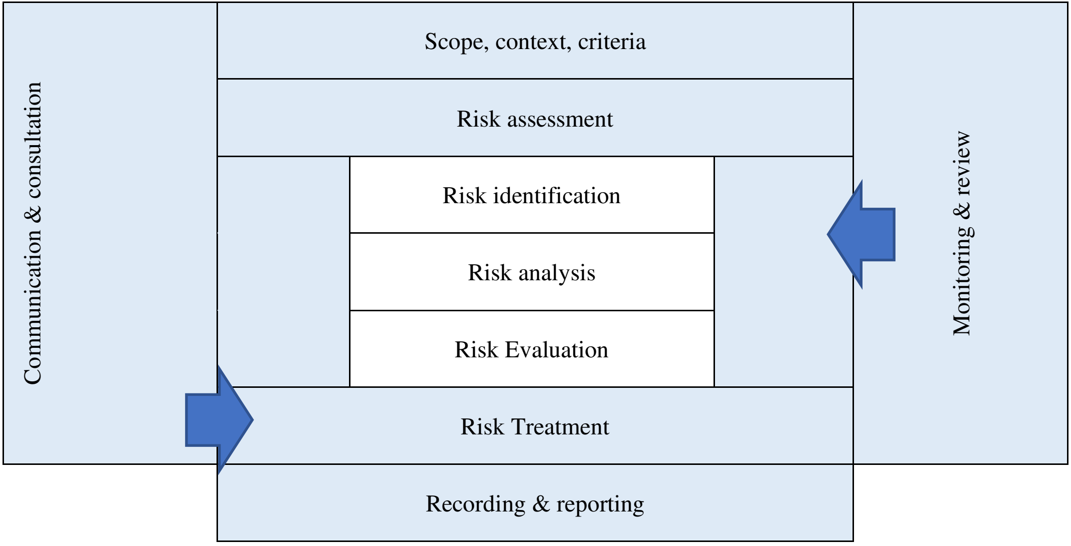
5. Table: www.17799.com

Two years later, in 2019, in the article "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency" the authors also stated that

“NIST SP 800-30 revision 1 can be used as a complement to the risk assessment process and can be applied to the ISO 27005 risk management framework”. [27]

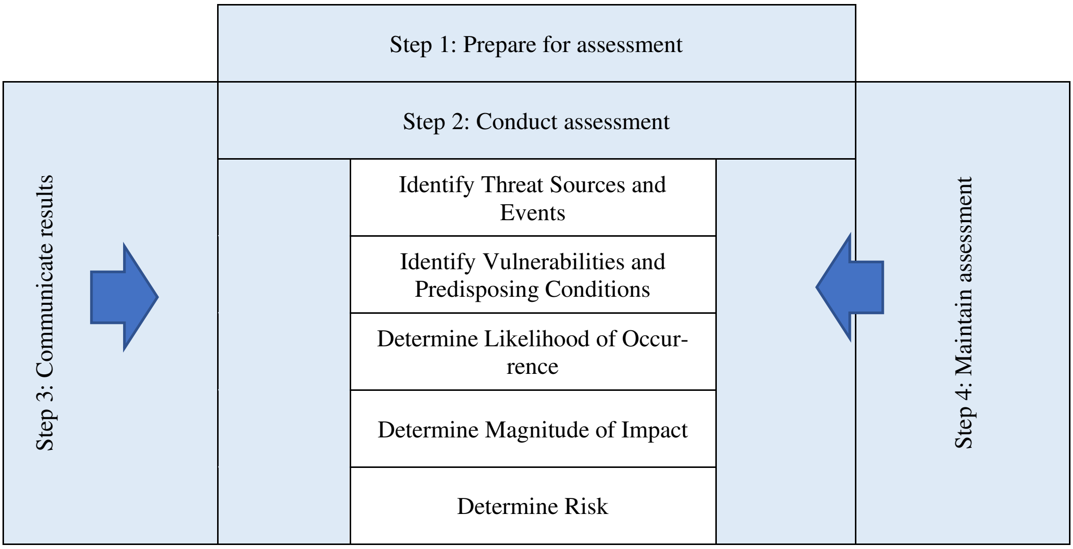
ISO/IEC 27005 references ISO 31000 Risk management — Guidelines when describing the high-level risk management process. [28] ISO 31000 describes an industry and sector independent risk management approach. [29]

The high-level risk management process is shown in the following figure, based on the ISO 31000:2018 standard. [29]



6. Table: Risk management process. Self-editing.

The NIST way of assessing risks are quite similar as it can be seen on the figure below.


Step 1: Prepare for assessment
Step 3: Communicate results
Step 2: Conduct assessment
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 4: Maintain assessment

7. Table: NIST SP 800-30 rev 1 Risk Assessment Process. Self-editing.

The combination of the ISO and NIST approach can be seen in the table below, based the standards and on the 2019 article. [27] [28] [15]

No.	ISO 27005/ISO 31000	NIST SP 800-30 rev1	Updated Combination technique
Context Establishment			
1.	Scope, context, criteria	Prepare for assessment	Determination of Risk Assessment Criteria and Scale
Risk Assessment			
2.	Risk Identification	1. Threat Source Identification 2. Threat Event Identification 3. Vulnerability Identification	1. Risk Identification, a) Threat Source Identification; b) Threat Event Identification; c) Vulnerability Identification
3.	Risk Analysis	4. Determining the Likelihood 5. Determining Impact	2. Risk Analysis, a) Determining the likelihood in the risk scenario; b) Determining the impact on the risk scenario
4.	Risk Evaluation	6. Determine Information Security Risk Level	3. Risk Evaluation, a) Determining the level of information security risk; b) Determining Risk Priority

8. Table: ISO-NIST combination risk assessment technique [27]

The combined approach basically follows the steps of ISO/IEC 27005, while using some features of the NIST SP 800-30 revision 1, when applicable. For example, in the Threat Event Identification step, the Threat Event categories come from the ISO standard, but the Relevance scale is used from the NIST publication.

In the following a possible application is described of the above-mentioned NIST-ISO combination technique assessing the risks of SoDevCo Ltd.

RISK ASSESSMENT OF SODEVCO LTD.

First things first, the *establishment of the risk management context* including a risk management approach, risk evaluation criteria, impact criteria, and risk acceptance criteria. ISO/IEC 27005 only recommends that these criteria should be developed somehow. [28] According to ISO 31000, the organization should specify the amount and type of risk that it may or may not take, relative to objectives. This is often called Risk Appetite. [29]

Applying the NIST SP 800-30 rev 1 scales, Impact of Threat events, Likelihood of Occurrence, Likelihood of Adverse Events as suggested in the 2019 article can simplify the task of setting up these criteria. I shall not list these scales due to size constraints; they can easily be looked up in the NIST recommendation. [15] [27]

A company like SoDevCo Ltd. has to face many types of risks, including human risk, financial risks, information security risks etc. A comprehensive risk management framework would cover all of them, but describing the assessment all these types of risks would be way too lengthy, so the scope of risk analysis has to be narrowed down to information security risks related to the software development process.

The next step is the *risk identification*, which starts with the *identification of the assets*. According to ISO 27005 assets can be categorized into two main categories: primary (denoted as P) and supporting (S) assets. Primary assets can be of two types: the core processes and activities of the company and information. Any other types of assets like hardware, software and personnel are considered as supporting assets. [28]

In the following table I shall list a few examples of the assets of the company, the type of asset is identified based on the asset category of the ISO standard. Besides these examples many other assets would be incorporated in the risk assessment, including network equipment, hardware etc. Each asset has a unique identifier so that they can be referenced later.

ID	Type	Name	Kind of asset	Owner	Location
A1	Information	Source code repository of AtTrack	P	AtTrack DevOps team	Data center
A2	Information	Source code working copies of AtTrack	P	AtTrack DevOps team	Employee's workstations
A3	Information	Documentation of AtTrack	P	AtTrack DevOps team	Data center
A4	Process	CD pipelines	P	AtTrack DevOps team	Data center
A5	Information	User-reported issues and responses	P	Service Desk	Data center
A6	Information	Scrum process documentation (epics, user stories etc.)	P	AtTrack DevOps team	Data center
A7	Information	Collective knowledge base of the company	P	The company	Data center
A8	Technology	Production AtTrack Application	S	The company	Data center
A9	Information	Production AtTrack Database	P	The users	Data center
A10	Personnel	DevOps team members	S	The company	Site
A11	Hardware	Workstations for team members	S	AtTrack DevOps team	Employee
…	…	…	…	…	…

9. Table: Example assest of SoDevCo Ltd. Self-editing.

Next, the *threat sources should be identified*, ISO 27005 has an annex (Annex C) of typical threats which can be complemented by the NIST SP 800-30 exemplary taxonomy of threat sources (Table D-2 in the recommendation). [28] [15] Threats can be broadly categorized as adversarial and non-adversarial (accidental, structural and environmental). [15] The threat sources identified are shown in the following listing with a unique identifier.

ID	Name
Adversarial Threat Sources	
S1	Hacker, cracker
S2	Computer criminal
S3	Industrial espionage
S4	Insider
S5	Trusted insider
S6	Privileged insider
S7	Outsider
S8	Competitor Organization
S9	Supplier Organization

ID	Name
S10	Customer Organization
Accidental Threat Sources	
S11	Human error – user
S12	Human error – administrator
Structural Threat Sources	
S13	Communications Equipment
S14	Networking
S15	General-Purpose Application
S16	Mission-Specific Application
Environmental Threat Sources	
S17	Fire
S18	Flood
S19	Telecommunications Outage

10. Table: Threat sources of SoDevCo Ltd.

Threat events are connected to assets; threat sources capable of exploit vulnerabilities of assets cause threat events. The following matrix shows a few examples of the *possible threat events*. The values of the threat event column come from the ISO/IEC 27005 Annex D. [28] The relevance of a threatening event is intended to express the probability that the event in question may occur in the course of the company's operations, SP 800-30 revision 1 describes an exemplary scale for reference. [15]

No.	Asset ID	Threat event	Threat Sources	Relevance
1	A1	Abuse of rights (T1)	S1, S2, S3, S4, S5, S6, S7, S8, S12	Anticipated
2	A1	Forging of rights (T2)	S1, S2, S3, S4, S5, S6, S7, S8	Predicted
3	A1	Theft of media or document (T3)	S1, S2, S3, S4, S5, S6, S7, S8	Possible
4	A1	Failure of telecommunication equipment (T4)	S11, S12, S13, S14, S19	Confirmed
5	A8	Illegal processing of data (T5)	S1, S2, S3, S4, S5, S6, S7, S8, S10	Possible
6	A8	Tampering with software (T6)	S1, S2, S3, S7, S11, S12	Anticipated
7	A9	Abuse of rights (T1)	S1, S2, S3, S4, S5, S6, S7, S8, S12	Predicted
…				

11. Table: Example threat events

The next step is the *identification of existing controls*, surely every company has controls already in place before conducting a risk assessment. According to ISO/IEC 27005 this step is important for multiple reasons: on one hand unnecessary work and expenses can be avoided, on the other hand ensuring the proper operation of existing controls is also achievable. [28]

The following controls were identified regarding the DevOps process of the company, password policy on team members' workstations (C1), two-factor authentication with smart cards on workstations (C2), full-disk encryption on workstations (C3), security awareness training of employees (C4), group policy on team members' workstations (C5), GitHub.com two-factor authentication (C6), GitHub.com password policy (C7). There are a few controls incorporated in connection with the production AtTrack application (A8), which are the following: storing user passwords hashes (C8), user password policy (C9), automated tests incorporated in the CD pipelines (C10), database encryption (C11) of the Production AtTrack database (A9).

Next, the *Identification of vulnerabilities*, in this step vulnerabilities that can be exploited by threats to cause harm to assets or to the organization should be identified. [28] In the 2019 article, the suggested NIST-ISO approach focuses on the implemented, existing controls to protect assets from threats, utilizing the NIST-based vulnerability measurement, which is known as the Vulnerability Severity. [27] [15]

Asset	Existing Control	Vulnerability	Vulnerability Severity
A1	C3, C6, C7, C8	Lack of identification and authentication mechanisms like user authentication	High
A3		Wrong allocation of access rights	Moderate
A11	C4, C5	Uncontrolled downloading and use of software	Moderate
A2	C4, C5	No 'logout' when leaving the workstation	Moderate
A8	C10	No or insufficient software testing	High
A8	C8	Unprotected password tables	High
A10	C4	Lack of security awareness	High
…	…	…	…

12. Table: Example Vulnerabilities. Self-editing.

The table above shows, among other things, that the organization does not have any existing controls regarding the access right management of product documentations.

Risk analysis is the core step in conducting a risk assessment. The combined approach utilizes the NIST SP 800-30 revision 1 semi-quantitative scales of overall likelihood and level of impact to create a matrix which can describe the risk appetite of the company. [27]

Risk appetite needs to be defined with the company's goals, capabilities, and the interests of all stakeholders in mind. [28]

Overall Likelihood	**Level of Impact**				
	Very low (0)	**Low (2)**	**Moderate (5)**	**High (8)**	**Very High (10)**
Very Low (0)	Accept	Accept	Accept	Mitigation	Mitigation
Low (2)	Accept	Accept	Mitigation	Mitigation	Mitigation
Moderate (5)	Accept	Mitigation	Mitigation	Share	Share
High (8)	Accept	Mitigation	Mitigation	Share	Share
Very High (10)	Accept	Mitigation	Mitigation	Share	Share

13. Table: Risk Appetite of SoDevCo Ltd.

The above table shows that the company is willing to accept risk with Very Low Level of Impact and even risks with Moderate impact if the Overall Likelihood is low enough, and plans to share the responsibility of risk management in cases where the impact of the risk is High or Very High and the Overall likelihood of the risk is above Low. In any other cases the risk treatment is Mitigation.

The following table is the risk analysis table, showing the connections between assets, threat sources, threat events with the corresponding likelihoods and levels of impact. [27] Based on the Likelihood of Attack Initiation and Likelihood of Attack Success the Overall Likelihood can be read from the Table G-5: Assessment Scale – Overall Likelihood table of the NIST SP 800-30 revision 1. The Level of Risk comes from the above Risk Appetite table based on the Overall Likelihood and Level of Impact values of the rows. [15]

No.	Asset	Threat Event	Threat Sources	Likelihood of Attack Initiation	Likelihood of Attack Success	Overall Likelihood	Level of Impact	Level of Risk/Treatment
1	A1	T1	S1, S2, S3, S4, S5, S6, S7, S8, S12	Moderate	Moderate	Moderate	High	Moderate (Share)
2	A1	T2	S1, S2, S3, S4, S5, S6, S7, S8	Low	Moderate	Low	High	Low (Mitigate)
3	A1	T3	S1, S2, S3, S4, S5, S6, S7, S8	Low	High	Moderate	Very High	High (Share)
4	A1	T4	S11, S12, S13, S14, S19	Moderate	Low	Low	Low	Low (Accept)
5	A8	T5	S1, S2, S3, S4, S5, S6, S7, S8, S10	Moderate	Moderate	Moderate	High	Moderate (Share)
6	A8	T6	S1, S2, S3, S7, S11, S12	Moderate	Moderate	Moderate	High	Moderate (Share)
7	A9	T1	S1, S2, S3, S4, S5, S6, S7, S8, S12	Low	Moderate	Low	High	Low (Mitigate)
…								

14. Table: Risk analysis table. Self-editing.

To highlight just a few examples, firstly the asset of the greatest value of a software development company is the codebase of its product (denoted as A1). Row #1 in the table above means that the responsibility should be shared in case of the risk of right abuse on the main source code repository, which is fulfilled since the codebase is stored in a GitHub repository which has its own measures, controls and solutions regarding security.

Another example of sharing responsibility is row #6 the tampering with the production AtTrack Software (A8), it is shared with customer organizations, since they are the end-users of the application, so it is their responsibility as well that the users of the application are well-trained, trustworthy and disciplined.

The last step of a Risk Assessment process is the *Risk evaluation*, the goal is to create a prioritized list of risks according to the risk criteria. The following table show the risk priority matrix, classified based on the NIST SP 800-30 revision 1, describing the relationship between assets and threats. [27]

		Threats						
		T1	T2	T3	T4	T5	T6	…
Assets	A1	🟧	🟩	🟥	🟩			
	…							
	A8					🟧	🟧	
	A9	🟩						
	…							

Priority color codes
Very High
High
Moderate
Low
Very Low

15. Table: Risk priority matrix. Self-editing.

SUMMARY

The combination technique focuses on information security risk assessment resulting in a comprehensive risk assessment by following the ISO 27005 standard, utilizing the simplicity of the NIST SP 800-30 semi-quantitative scales. Using these supports the ISO standard when it requires the development of metrics. Although the example in this study is based on a business organization, the methodology is surely suitable for government bodies as well.

Based on my experience, unfortunately the product catalogues of ENISA and NATO (NIAPC) are both seem out of date. In my humble opinion it seems timely to conduct a comprehensive content review and update on both catalogues.

ISO/IEC 27001 certification is a hot topic these days even in Hungary, but unfortunately not all standards of the ISO/IEC 27000 series are published in our country. It would be highly desirable to publish all standards of the series in Hungarian and also MSZT being a participating member of the technical committee in charge of developing the series.

A family of Hungarian national recommendations such as the KIB-published MIBA is of great importance on information security trends, being a great initiative, it should be kept updated through regular revisions.

RESOURCES USED

[1] ISO, ISO/IEC 27001:2013, ISO, 2013.

[2] F. Erich, C. Amrit and M. Daneva, Report: DevOps Literature Review. University of Twente, Enschede, Netherlands, 2014.

[3] R. T. Yarlagadda, How DevOps Enhances the Software Dévelopment Quality, International Journal of Creative Research Thoughts (IJCRT), vol. 7, no. 3, pp. 358-364, 2019.

[4] R. T. Yarlagadda, DevOps and Its Practices, International Journal of Creative Research Thoughts (IJCRT), vol. 9, no. 3, pp. 111-119, 2021.

[5] L. Bass, I. Weber and L. Zhu, DevOps: A Software Architect's Perspective, Pearson Education, Inc., 2015.

[6] B. Delb, The CAMS model to better understand the DevOps movement, 22 07 2018. [Online]. Available: https://brunodelb.medium.com/the-cams-model-to-better-understand-the-devops-movement-ffe6713c3fd7. [Accessed 07 05 2021].

[7] S. Guthrie, DevOps Principles- The CAMS Model, 05 05 2019. [Online]. Available: https://medium.com/@seanguthrie/devops-principles-the-cams-model-9687591ca37a. [Accessed 07 05 2021].

[8] Atlassian, What is Continuous Integration?, [Online]. Available: https://www.atlassian.com/continuous-delivery/continuous-integration. [Accessed 15 05 2021].

[9] Mohammed Mehedi Hasan; Farzana Ahamed Bhuiyan; Akond Rahman, Testing Practices for Infrastructure as Code, ESEC/FSE '20: 28th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, 2020.

[10] I. El Fray, A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in Information Systems, In: Cortesi A., Chaki N., Saeed K., Wierzchoń S. (eds) Computer Information Systems and Industrial Management. CISIM 2012. Lecture Notes in Computer Science, vol. 7564, 2012.

[11] Magyar Informatikai Biztonsági Keretrendszer (MIBIK), KIB, 2008.

[12] NIAPC (NATO Information Assurance Product Catalogue), NATO Information Assurance Product Catalogue, [Online]. Available: https://www.ia.nato.int/NIAPC. [Accessed 02 05 2021].

[13] ENISA, European Union Agency for Cybersecurity, ENISA, [Online]. Available: https://www.enisa.europa.eu/. [Accessed 07 05 2021].

[14] NIST, NIST, [Online]. Available: http://nist.gov. [Accessed 02 05 2021].

[15] NIST, SP 800-30 revision 1, NIST, 2012.

[16] NIST, NIST SP 800-37 revision 2, NIST, 2018.

[17] ENISA, SP800-30 (NIST), [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_sp800_30.html. [Accessed 02 05 2021].

[18] ENISA, Cramm, [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html. [Accessed 30 04 2021].

[19] NIAPC (NATO Information Assurance Product Catalogue), CRAMM, [Online]. Available: https://www.ia.nato.int/niapc/Product/CRAMM_257. [Accessed 30 04 2021].

[20] IT Governance , Information Security and ISO27001 – an Introduction, [Online]. Available: https://www.itgovernance.co.uk/files/Infosec%20101v1.1.pdf. [Accessed 30 04 2021].

[21] ISO, iso.org, ISO, [Online]. Available: www.iso.org. [Accessed 05 04 2021].

[22] CRAMM, CRAMM, [Online]. Available: http://www.cramm.com/. [Accessed 30 04 2021].

[23] MSZT, Magyar Szabványügyi Testület - Az információbiztonság-irányítás szabványai, [Online]. Available: http://prod.mszt.hu/hu-hu/szabvanyositas/hirek/2015/03/az-informaciobiztonsag-iranyitas-szabvanyai. [Accessed 29 04 2021].

[24] NAH, NAH, NAH, [Online]. Available: https://www.nah.gov.hu/. [Accessed 10 04 2021].

[25] ENISA, ISO/IEC 27001, [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_iso27001.html. [Accessed 02 05 2021].

[26] Putra, Fandi A., S. Hermawan, and R.P. Anggi., Design of Information Security Risk Management using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A Case Study at Communication Data Applications of XYZ Institute, International Conference on Information Technology Systems and Innovation, vol. 8, no. 4, pp. 251-256, 2017.

[27] Muhamad Al Fikri et al., Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency, Procedia Computer Science - The Fifth Information Systems International Conference, vol. 161, pp. 1206-1215, 2019.

[28] ISO, ISO/IEC 27005:2011, ISO, 2011.

[29] ISO, ISO 31000:2018, ISO, 2018.