Examination of Risks in Management of Software Licenses in Enterprises and Cost-Benefit Analysis

Araştırma Makalesi/Research Article

Ali DURDU[1], Abdullah TUTĞAÇ[2]*

[1]Yönetim Bilişim Sistemleri, Ankara Sosyal Bilimler Üniversitesi, Ankara, Türkiye
[2]Denetim ve Risk Yönetimi, Ankara Sosyal Bilimler Üniversitesi, Ankara, Türkiye
ali.durdu@asbu.edu.tr, abdullahtutgac@gmail.com
(Geliş/Received:07.11.2021; Kabul/Accepted:03.10.2022)
DOI: 10.17671/gazibtd.1019869

Abstract— In this study, a proposal on how software license assets should be managed with an enterprise risk management approach has been put forward. The study examined licenses, which mean software usage rights, and various license models with a complex structure. Within the scope of the study, the risks that might arise concerning software licenses were determined and these risks were categorized. Considerable risks prioritized by senior management in businesses were identified and responses and strategies were set out for each risk factor that needs to be kept under control. The method suggested in the study was applied in a large-scale enterprise acting in the telecommunications sector. As part of this application, the enterprise's current situation in software asset management was revealed. The outcomes of the application are expected to be beneficial in determining the risk models of the enterprises. The study presents the study's management of software assets, determination of risks, and solutions to be applied to risks.

***Keywords*—**audit, enterprise, risk, risk management, software, license

İşletmelerde Yazılım Lisanslarının Yönetiminde Risklerin İncelenmesi ve Fayda-Maliyet Analizi

Özet— Bu çalışmada, yazılım lisans varlıklarının kurumsal risk yönetimi yaklaşımıyla nasıl yönetilmesi gerektiğine dair bir öneri ortaya konmuştur. Çalışmada yazılım kullanım hakları anlamına gelen lisanslar ve karmaşık bir yapıya sahip çeşitli lisans modelleri incelenmiştir. Çalışma kapsamında yazılım lisanslarına ilişkin oluşabilecek riskler belirlenmiş ve bu riskler kategorize edilmiştir. İşletmelerde üst yönetimin önceliklendirdiği önemli riskler belirlenmiş ve kontrol altında tutulması gereken her bir risk faktörü için yanıtlar ve stratejiler oluşturulmuştur. Çalışmada önerilen yöntem telekomünikasyon sektöründe faaliyet gösteren büyük ölçekli bir işletmede uygulanmıştır. Bu uygulama kapsamında işletmenin yazılım varlık yönetimindeki mevcut durumu ortaya çıktı. Uygulama sonuçlarının işletmelerin risk modellerinin belirlenmesinde faydalı olması beklenmektedir. Çalışma, çalışmanın yazılım varlıklarının yönetimini, risklerin belirlenmesini ve risklere uygulanacak çözümleri sunmaktadır.

***Anahtar Kelimeler*—** denetim, kurumsal, risk, risk yönetimi, yazılım, lisans

1. INTRODUCTION

Risk management has become one of the areas that gain importance day by day and requires focus. As a result of the shift from traditional risk management to enterprise risk management, the risks are no longer limited to financial risks but have expanded to address the strategic, human resources, operational, and particularly information technology risks of the organizations holistically. With the development of technology and the rapid increase in internet access, the expectations of customers have also changed, and companies have increased their investments in information technologies to keep pace with these expectations. A considerable part of

the investments made by companies undergoing digital transformation in this context consists of software. Therefore, institutions now need to pay more attention to the management of software assets, whose share is increasing compared to other budget items.

Today, we hear the concepts of digitalization and digital transformation frequently. We often witness that it is not only heard but also it is in our daily lives. So what does this concept mean? Let's try to explain the difference between the two concepts thanks to a few examples. When you enter the office restroom in your workplace, the lighting is an example of digitalization, which detects you through sensors and turns on automatically. The lighting will automatically turn off after a certain period when you stand still and have not come out of yet. However, if you have not left yet, you will be in the dark and you will have to move somehow to make the lights come on. This is an indicator of the fact that digital transformation has not started yet. Whenever the aforesaid sensors recognize you and estimate the duration of the lights according to your age and gender and turn them off accordingly, then we can say that digital transformation has begun. To set another example of digitalization, being able to control an air conditioner running in your home through remote control and stabilizing the ambient temperature can be cited. When your air conditioner automatically informs you or the technical service by sending a text message when the gas is running out of, or when it calculates the energy consumption of the surrounding air conditioners, considers that it consumes more energy and informs you that there must be a problem in the engine, we can say that the digital transformation process has started. Thus, digital transformation is a process that starts with the customer (user) [1].

Institutions are increasing their technology investments day by day to adapt to the digital transformation process and not to stay behind it. Particularly, largescale companies have already begun to position themselves as technology companies. For instance, the CEO of Goldman Sachs, a multinational investment bank, describes his company as a technology company. In the headline of an article published in MIT Technology Review, expressions are drawing our attention that the Walmart Company has turned into a technology company [1]. In advertisements for the bank industry after 2015 in Turkey, now, we see that emphasis is placed on customers making their conversations with robot assistants.

Digital Transformation Office established under the Presidency of the Republic of Turkey in 2018, enables our country to follow its adaptation to this transformation process in a more institutionalized structure. In the Information and Communication Security Guide released by the Office on 24 July 2020, the obligations are included, which makes software asset management mandatory for public institutions and private companies providing critical infrastructure. A 2-year schedule has been planned for the institutions to adapt to this transition [2]. Durdu and Eren worked on integrating information security with information systems. The software has been proposed so that institutions can carry out and maintain their continuity by transferring all the processes required by ISO 27001, which is the information security management system standard, to the digital environment [3].

It is software, which is one of the most fundamental elements that constitute the infrastructure of products produced by companies for digital transformation in terms of information technologies. Bill Gates highlights that the software development business is the closest profession to magic in the world [1]. Companies take advantage of software-based platforms while introducing their products to their customers in different media (websites, social media, mobile applications, etc.). These software are procured either by in-house coding with the help of their own human resources or by acquisition from outside. Just as an artist demanding a certain fee for the lyrics s/he writes or a poet demanding fee for the poetry s/he composes, as it is subject to copyright, individuals and institutions that generate a work (software) by coding also demand a certain fee and copyright. The fee required is called the copyright license [4].

Table 1. Worldwide information technology spending forecast (S:Spending, G:Growth %)[5].

	2019 S	**2019 G**	**2020 S**	**2020 G**	**2021 S**	**2021 G**
Data center systems	210,053	0.6	188,365	-10.3	200,094	6.2
Enterprise coftware	476,687	11.7	449,506	-5.7	482,666	7.4
Devices	711,525	-0.3	596,914	-16.1	611,303	2.4
IT services	1,040,263	4.8	969,438	-6.8	1,023,179	5.5
Commun. services	1,372,236	-0.6	1,326,492	-3.3	1,366,419	3.0
Overall IT	**3,810,764**	**2.3**	**3,530,714**	**-7.3**	**3,683,661**	**4.3**

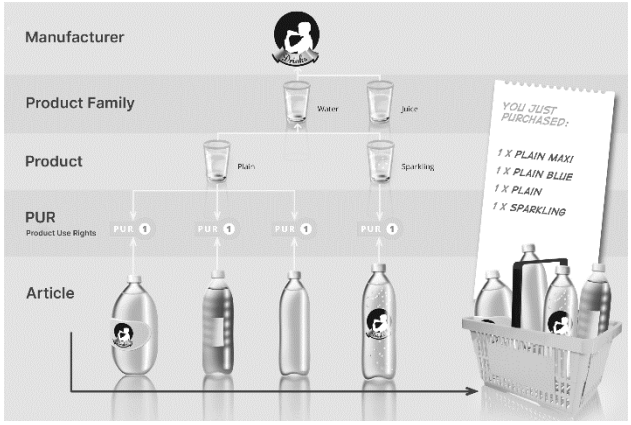

Figure 1. An example of product use rights [6].

Information as to how much companies invest in information technology across the world and how much these investments are expected to increase in the long view is available in Table 1. This table illustrates the trend of worldwide information technology expenditures

between the years 2019-2021, which was published by Gartner in July 2020. Realizing in particular that corporate software expenditures will increase at a greater rate in 2021 compared to other investment items reveals the fact that it is a demanding area for companies.

The concept of license defines the complexity and limits of the authorization to use the software owned by the licensee. When you buy software, you have a license that means the right to use it. With exceptions, the software itself always belongs to the software vendor. No price is paid for free software, open-source software or software for a definite period of use. Our research will not cover this type of software. There may be differences in licensing models of software purchased on the basis of a certain contract for a fee. In the research we performed in a telecommunication company, more than 1000 different software purchased from more than 100 different companies were encountered. Considering the licensing models of this software, it is seen that there are more than 100 different license models. Some of these licenses are user-based, earning-based, per central processing unit (CPU), per seat, usage-based etc. These models are changed by software vendors at certain periods and differ in terms of the infrastructures they are installed on. User licenses are commonly installed on client hardware. To set an example, laptop or desktop computers, mobile phones, tablets, etc. devices can be specified. Moreover, there is hardware such as servers or storage devices in data centers. Many different operating systems and software such as virtualization run on this hardware. A large-scale telecommunications company has more than 20,000 clients, 10,000 servers, and devices such as storage. Considering the software traces coming from these devices, it was observed that over 1 million data were received.

Apart from the variety and different software license models, it is also significant for companies to clearly define the right to use the purchased software in the contract. An example of product usage rights is given in Figure 1. In the example in Figure 1, a water order is received from a company that produces water and fruit juice. Some of the water is sparkling water and some is normal water. But some water is packaged in 1-liter, some in 0.5-liter bottles. Some of them are packaged in 6 pieces and they contain 3 normal and 3 sparking water bottles, each of which is 0.5 liters. Even though it seems that only water has been ordered, the fee and usage rights paid for each product are different

The points that demonstrate how important it is for organizations to manage assets effectively are the following: the product variety in the above-mentioned software licenses, the differences in licensing models, the change of usage rights according to the contract, and the fact that it constitutes an important expenditure item in the budget. The underlying idea of this study is what kind of risks organizations will face in case they cannot effectively manage these complex assets in a manner and how these risks should be managed.

In addition to the lack of a mere explanation agreed on the concept of risk, it is considered as a threat or opportunity that may have an impact on the achievement of the company or institutions' goals [7]. This concept was first used in the field of insurance in the 1950s. While the traditional understanding of risk management focused more on financial risks in the 1970s and 1980s, we can observe that organizations also focused on operational risks as of the early 1990s and switched to an enterprise risk management approach. After 2004, the risk was not only deemed as a threat but also as an opportunity that could be turned into an advantage [8].

In traditional risk management, silo-based risk management was adopted. Every single unit within the company focused on its own risks. Financial risks were mostly prioritized, and hedge transactions were performed using derivative instruments in order to avoid these risks. While shifting to enterprise risk management, a holistic approach to risks was adopted. Not only financial risks but also operational and strategic risks came to the fore. In addition to financial risks, the following risks also started to be managed in coordination: supply chains, distribution systems, corporate management, information technologies, and human resources [9].

Especially with the emergence of the enterprise risk management approach, that is, after the 1990s, the number of studies and publications on risk management has increased significantly. As can be seen in Figure 2, we can say that since the second half of the '90s, the rate of increase of publications on enterprise risk management has increased significantly compared to the increased rate of publications on internal control and internal audit.

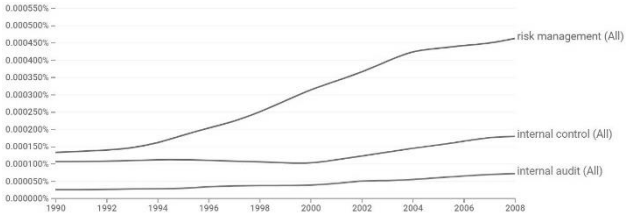

Figure 2. Publications on risk management, internal control, and internal audit [10].

The outbreak of the Enron crisis in 2001 and the Worldcom scandal at about the same time heralded a new era in financial circles and particularly in the enterprise risk management discipline. In the Enron crisis, thanks to the manipulation of the company's accounting records, a company that was indeed at loss was depicted as profitable for years. Following this crisis, the Public Company Accounting Reform and Investor Protection Act, known as the Sarbanes-Oxley Act, was enacted in the United States in 2002 [11]. With this act, it was obligatory for public

companies to adopt the risk management principles, and to document and evaluate the controls related to the identified risks. Moreover, the major responsibility for these processes is given to top executives [11].

In 2004, the COSO (Committee of Sponsoring Organizations of the Treadway Commission) put forth the Enterprise Risk Management Framework. Normally, in 1992 COSO introduced the Internal Control Framework, but especially following the Sarbanes-Oxley Act, it tried to clarify which methods and how should be employed in risk management and internal control issues during the implementation phase of this act [11].

Along with the COSO framework, many different organizations issued guidelines on risk management [12]. In 2009, ISO (International Standards Organization) published a guide that includes the application of risk management principles well-accepted in international standards known as ISO 31000 [11].

The proliferation of risk management in the course of time, its being subject to laws and its continuous improvement are the indicators demonstrating the fact that it has become more important for organizations. It has been criticized in the literature that there are few empirical studies evaluating the contributions that enterprise risk management (ERM) makes to organizations [11]. In general, there are studies on the following subjects: practices that measure the maturity levels of companies in different sectors in enterprise risk management, the effects of enterprise risk management on company performance, and its interaction with internal audit and internal control. For instance; to measure the impact of ERM on the financial performance of companies, samples were taken from publicly traded companies in the Istanbul Stock Exchange, which is among the largest 500 industrial companies published by the Istanbul Chamber of Industry (ISO) in 2014 [8]. In a study performed on 62 companies selected from the first 250 companies in Bursa, it was observed that the level of ERM implementation was positively affected by the increase in the turnover and degree of centralization of the companies [13]. 25 companies operating in the energy sector, which are among the ISO 500 companies in Turkey, were selected as samples, and with the surveys carried out, it was tried to reveal the maturity level and profile of enterprise risk management practices in our country [14].

Apart from the above-mentioned examples, many studies were also discussed in terms of managing software development project risks. A bank ATM project was taken as an example and an approach was put forward on how to identify and analyze risks in software development projects, plan risk response strategies, and design control activities [15]. There are also studies in which smart methods are employed in order to manage costs and risks in software projects. The software data between 2007 and 2014 of a company acting in the telecommunications sector were compiled. Thanks to these data, an approach was suggested that can predict how a software project will result when it starts using the fuzzy logic method [16]. In parallel, artificial intelligence-based risk management studies became apparent. In the study conducted on 467 software project data collected from 774 different software companies, a web-based model that performs risk management based on artificial intelligence was produced. Using this model, the project budget, time plan, and deviations from achievements can be estimated as per the risk levels [17]. Fuzzy methods were used in the selection and evaluation of enterprise resource planning [18].

On the management of software assets, a thesis study was conducted in 2018 within the University of Twente, School of Management and Governance MBA (Business Administration) program in the Netherlands. Within the scope of this thesis, Thales Huizen, a large technology company, was chosen as a case study. In the study, it was mentioned that the purchasing costs cover 50 to 80 percent of the operations of the companies and the place of software costs in this cost was emphasized. Suggestions were put forward on how to improve the software acquisition and asset management process and what should be done in order to minimize the risks. The study is based on three main questions. Answers to the following questions were sought: Is software asset management applied in Thales company and similar companies acting in the same industry? What are the risks and problems in the current software sourcing and management process? Finally, what are the requirements for developed software procurement and management process in order to minimize risks and problems? A descriptive qualitative research method was adopted by using process modeling and semi-structured interviews [19]. In terms of software asset management, it can be argued that it is the most comprehensive academic study we encountered.

In a thesis study performed within the MBA program of Helsinki Metropolia University in Finland, the current situation of software asset management of a large telecom operator in Finland was analyzed. Using the results of the current situation analysis, improving the company's software asset management was set as the objective. As in the example of Thales, in terms of its method, it was qualitative research where interview workshops were performed. Participants representing the entire company were carefully selected in these interviews. In the study, it was revealed that there were positive developments in software asset management within the company, but the process remained isolated and the whole company should become organized. It was particularly emphasized that a tool (system) should be used in order to manage software asset management effectively and a program should be initiated within the company to improve the competencies [20].

Academic studies and private companies' surveys contain important examples regarding the prevalence of enterprise risk management in the world and the level of

maturity achieved by the institutions in Turkey [19]. Also, rapidly developing and transforming technology tools have a serious impact on institutions. One of the key components of these technology tools, the software licenses, are complicated and expensive, thus it's vital to manage them systematically.

Licenses for software assets are very complex for businesses and useless licenses are created if not managed effectively. In the report published by Gartner in July 2020, it was emphasized that it should be realized that especially enterprise software expenditures in enterprises will increase more than other investment items in 2021. Therefore, it has been clearly stated that the management of software licenses is an important risk for businesses to be managed. With the holistic perspective of enterprise risk management, companies need to focus on financial and technological risks.

In this study, it has been tried to start an application for the effective management of software licenses used by companies by adopting the enterprise risk management approach and to analyze the profit-benefit analysis provided to the institutions by discussing the post-implementation results. In the second part of the study, information is given about the methods to be used within the scope of the study. The methods used in the study were applied to a private company operating in the telecommunications sector and the details of the risks identified after the application were given. In the third part, current risks are given. In the fourth chapter, current risks are answered and suggestions are made. In the conclusion part, information was given to the institutions for the purpose of advice.

2. METHODS USED IN THIS STUDY

During the implementation phase, a company was selected as a pilot company acting in the telecommunications sector in Turkey. Having over 30 thousand employees and serving over 40 million customers, the company is among the leading companies in terms of its size in its sector. In this respect, it is expected that the application made specific to the selected company provides an advantage in terms of being inclusive for other companies implementing software license management.

Two different methods were employed in order to identify risks in information technology (IT) software license management. One-on-one interviews and focus group meetings were held. Moreover, in order to take advantage of the enterprise risk management approach, risk classes mentioned in the Public Internal Audit Manual were utilized [21].

2.1. Current situation (One-to-one interviews)

In order to determine the maturity level of software license management in the pilot company, the existing inventory was revealed. 166 units were contacted one-on-one and a set of 25 questions was delivered. These questions were: the name of the software, the number of licenses, license metric, contact information, validity periods, whether the measurement was made or not (Annex-1).

As a result of the study, it was revealed that there are more than 1600 different types of software licenses in the inventory of the company. These licenses were observed to be obtained from more than 100 different companies/vendors. Also, it was seen during the examinations that there were 132 different license models (Annex-2). The sub-category licenses given in Annex-2 are the licenses under the main category licenses. For example, "User" based license is determined as the main category, but there are "User" licenses in many different subcategories such as "concurrent" or "named user". It was stated that the licenses in the inventory run by around 15,000 servers and approximately 21,000 client devices. According to the declaration of the relevant teams, it was understood that 15% of the software licenses in their inventory were not managed effectively. 65% of the software in the inventory was observed to be in the IT category and 35% in the Network/Access category. When the contract prices are considered, it was seen that an annual total investment and maintenance budget of more than 100 million TL was allocated.

2.2. Focus group meetings

The main purpose of this study is to determine the risks with one-to-one and group meetings in order to manage software licenses and make profit-benefit analysis in businesses. As a result of one-on-one interviews, the current inventory was revealed. Data revealing the complexity of license management was obtained. As the second stage, focus group meetings were held. Five competent experts in their fields, who engage in contract and license management, attended these meetings.

At the meetings held, the current software inventory was examined and the possible risks that might be encountered by the company in this regard were determined. The probability of occurrence and possible effects of the identified risks scored between 1-5. Risk scores were determined by multiplying the obtained impact-probability scores and prioritized considering the risk appetite of the company. The strategies to be adopted by the company against these risks, the responses to the risks and the controls to be applied were determined.

3. RISKS

A focus group can be broadly defined as a type of group discussion on a topic under the guidance of a trained group moderator [22]. As stated in the literature, one of the main purposes of the research is to manage software licenses and to identify risks with group meetings in order to make profit-benefit analysis in businesses. To summarize the picture that emerged as a result of the interviews; keeping the asset inventory up-to-date, which

includes software running on thousands of servers and clients in physical and virtual environments and with hundreds of complex license models, is a necessity and is of great importance. It is believed that the evaluation of this area, for which a remarkable amount of budget has been allocated, from an enterprise risk management perspective will be beneficial for the members of the board of directors and shareholders of the companies. Details of the 12 risks identified in focus group meetings are illustrated in Table 2.

Table 2. Risks identified in focus group meetings.

No	Risks	Risk causes
1	Inactive (Idle) software cost risks	Risk of financial loss that may occur due to the failure in pursuing the issues regarding the existing software: necessity, benefits and use cases
2	Duplicate procurement risks	Risk of duplicate procurements and possible financial loss due to the lack of existing inventory control in new software requests.
3	External audit risks	Loss of reputation and financial risks that may arise as a result of the audits performed by the software suppliers
4	Failure in being up to date with the versions	Security and business continuity interruption risk that may occur due to the lack of support by the relevant vendors for the old version software used
5	Ineffective inventory control	Workforce loss risk due to repeating of inventory work during contract renewal periods
6	Deficiency in alternative product analysis	Risk of financial loss due to not using more cost-effective or open source products having the same functions
7	Long procurement processes	The risk of loss of workforce and bargaining power due to prolonged procurement processes caused by not keeping track of the software inventory up to date.
8	Inadequate contract control	The risk of financial and business loss due to software contracts not being concluded in favor of the enterprise
9	Ineffective contract tracking	Business continuity interruption risk that may occur due to the inefficient tracking of software license contract periods
10	Internal audit risks	Possible risk of loss of workforce in the internal audit process due to inefficient software inventory management
11	Inefficiency in following the license model	Financial loss risk that may arise due to delays in adapting to licensing models that have changed as a result of the strategies of the vendors
12	Risks from incomplete feasibility	The risk of financial and business loss that may arise in case the software requirement request is not analyzed properly during the planning phase.

After the risks were determined, the impacts of these risks on the company were evaluated. While performing this assessment, the risk analysis model (risk map) was utilized. In the light of the scores obtained as a result of the focus group meetings, the dangers that will be encountered by the company were evaluated through the risk analysis model.

The information on the impact range of the scored risks as a result of the creation of the risk analysis model is available in Table 3. According to the scores, it can be seen that 3 risks marked with dark grey are determined as high level, 5 risks marked with grey as medium level, and 4 risks marked with light grey as low-level risks. How the Company's top management plans to respond to these risks considering the risk appetite is also illustrated in the relevant table.

Table 3. Effects of risks and responses (I: Impact, P: Possibility, S: Score, R: Responses, C: Controls, CT: Control Type).

No	Risks	I	P	S	R	C	CT
1	Inactive (Idle) software cost risks	4	4	16	Check it	Preventive	Semi-automatic
2	Duplicate procurement risks	4	4	16	Check it	Preventive	Semi-automatic
3	External audit risks	5	2	10	Check it	Detective	Semi-automatic / Strict
4	Failure in being up to date with the versions	5	2	10	Check it	Preventive	Semi-automatic
5	Ineffective inventory control	1	4	4	Admit it	-	-
6	Deficiency in alternative product analysis	3	2	6	Admit it	-	-
7	Long procurement processes	2	3	6	Admit it	-	-
8	Inadequate contract control	4	2	8	Check it	Directing	Manual
9	Ineffective contract tracking	5	3	15	Check it	Preventive	Automatic
10	Internal audit risks	2	2	4	Admit it	-	-
11	Inefficiency in following the license model	3	3	9	Check it	Corrective	Semi-automatic
12	Risks from incomplete feasibility	4	3	12	Check it	Directing	Manual

4. RESPONSES AND PROPOSALS TO RISKS

It was determined that the 3 risks, which are considered as higher level among the 12 risks illustrated in Table 3, are the ones that primarily need to be taken precautions. How the company will respond to these risks (risks 1, 2 and 9) and what kind of controls should be applied are clarified. These 3 risks were evaluated collectively.

Three different proposals were put forward in order to keep under control the High-Level Risks (1,2,9), which are Inactive (Idle) Software Cost Risks, Duplicate Procurement Risks and Ineffective Contract Tracking risks, and to minimize their impacts.

4.1. 1st proposal; team building (SAM team)

To build a license inventory management-focused team, referred to as the Software Asset Management (SAM) Team. This is the team that centrally creates and manages the software license inventory. It can obtain information from relevant users, request contract details from purchasing teams, and follow up updates. The team to be built is positioned as the internal control team. It is of importance to be in a strong position within the technology organization, with equal measure to each unit. Otherwise, it will have problems in reaching the necessary information quickly and its power of sanction will be limited. Considering the size of company, where the pilot application is performed, the team is recommended to consist of at least 5 people. The team can be expanded according to the number of software vendor companies to be managed. In order to ensure an effective inventory management in light of the best practices, 1 expert should be allocated per 10 vendors.

4.2. 2nd proposal; SAM system setup

It is recommended to provide a license inventory management system (Software Asset Management Tool) in order to manage license management with actual data. The following information about the software procured by the company should be kept regularly: what the license models are, number, right of use, duration of use, etc. What's more, actual usage and installation data are of vital importance. Within the scope of usage data, it is necessary to access real data through automation by scanning servers and clients rather than statements of individuals. Due to the size of the organization, different units can perform installations unaware of each other within the company. By ensuring a central control, possible under licensing or over licensing information can be monitored in an effective manner. In the light of this information, duplicate procurements can be prevented thanks to analyzing new license requests by checking current uses. By monitoring less frequent usage, savings can be achieved by excluding the related products from the scope of the contract during maintenance times. It is possible to be reminded about the renewal of license contracts by automatically delivering the usage periods to the teams responsible for the system.

4.3. 3rd proposal; software life cycle process

During the phases of team building and establishment of license inventory management system, it is of vital importance to write the software life cycle process, which determines roles and responsibilities, and to be implemented after approval by top managers. If an approved process is not initialized, the responsibility areas of the SAM team will not be clear. Therefore, the established system will become dysfunctional in the course of time.

If these three proposals are put into practice effectively in the organization of the company, the impacts of risks 1, 2 and 9 will be minimized as far as possible. For risks 1 and 2, automatic and manual controls will be provided with the help of both system and process support. Automatic controls will be ensured for the number 9 risk. As a result of the market researches, it was estimated that the cost of the first investment (CAPEX) that the company has to bear for these controls will be around 2 and 3 million TL. The annual operational (OPEX) cost for the team (5 people) was calculated to be 0.75 million TL. It can be suggested that this cost is acceptable in terms of effective management of assets for a company that spends more than 100 million TL on license annually.

In an analysis released by Gartner in 2016, it was stated that companies that built the SAM system could save up to 30% in license expenditures [23]. In another analysis of Flexera company released in 2011, it was stated that companies that built the SAM system would make annual savings of up to 10% in license expenditures [24].

4.4. External audit risks

In software license contracts notedly owned by largescale international corporate companies, the relevant vendor's right to audit is included as standard. The products of 5 big companies, referred to as “Top 5 Vendors”, are commonly used across the world. These big 5 companies are known as Oracle, Microsoft, IBM, SAP and Micro Focus (formerly HPE). As a matter of course, there are other companies that include the audit article in the contracts they made. However, these 5 companies have higher audit risks. Because the business volume with these companies is higher, the products used are directly related to critical infrastructure and business processes. As a priority, it is recommended to follow the licenses of these companies. No matter how many precautions are taken, the contractual request of the vendor for an external audit will not be prevented legally. However, once the risk occurs, some actions can be taken in order to minimize the possible impact. Especially, thanks to the building of the SAM system, license usage can be tracked automatically. Furthermore, resolutions should be released and it should be ensured that the software licenses, which are used within the company with the ethical license model, are not used over the amount of product (under licensing) purchased. If the problems that may arise after the audit are known, negotiations can be

made with the relevant vendor accordingly and the audited company can overcome this process with the least damage.

4.5. Failure in being up to date with the versions

SAM system is thought to be used in order to control the license versions of software products. With the automatic discovery, software licenses coming from data sources to the SAM system can come together with version information. However, it will not be enough to get this information alone. It should be compared with an information repository that checks the up-to-dateness of the incoming version information and whether it is supported by the vendor. This information repository is formed by the shares of vendors who openly share license information with the public. When a catalog, referred to as the "Master Catalog", is included in the SAM system, automatic checks can take place. Products referred to as "End of Support" or "End of Life" can be reported to responsible users at certain periods.

Version information of companies whose license information is not openly disclosed can be added to the system manually and reported. Reports must also be delivered simultaneously to cyber security teams. Through implementing these controls, it can be targeted to minimize the risk impact by preventing possible security gaps and interruptions in business continuity.

4.6. Inadequate contract control

In the technical specifications (RFX) and administrative contracts to be issued when purchasing software products, arrangements regarding license models or source code ownership of the software must be made in favor of the company. Especially in purchases by tender, in projects for which the solution is not yet clear, the license model may be requested to be perpetual. Making the preference not dependent on a variable metric such as the number of users, the number of processes and subscribers is important in terms of preventing additional costs that may arise after the project. Also, if possible, requesting the source code of the software to be procured will reduce the dependency of the company. In order to take these measures, the claimant technical units, procurement units and legal teams must be informed in writing in advance. In addition, obtaining consultancy from the SAM team during the technical specification preparation phase by the claimant teams and checking the documents by the SAM team are directing manual controls that will minimize the risk.

4.7. Inefficiency in following the license model

It is known that software license models are changed over time by the vendors. They make this change sometimes to simplify complex license models, sometimes to increase their revenues, and sometimes due to the developments and changes in technology. Many manufacturing companies announce these changes to their customers and the public in advance. Companies, on the other hand, need to take necessary precautions beforehand for these changes. With respect to these changes, the "Master Catalog" information repository working with the aforementioned SAM system can be utilized automatically, and it will be possible for the SAM team to follow up these changes manually. SAM team can analyze the impacts of license model changes that may be encountered in the future on the company and report them to the relevant parties. In this way, the company will be least affected by this risk. One point that should be kept in mind is that in order for the license model and metric change to occur, this change must be registered with a new contract.

4.8. Risks from incomplete feasibility

The needs analysis should be performed accurately for the software that are planned to be procured at the stage of making a new investment decision. If the need is not determined accurately, there may be a risk of higher costs than the initial investment for the company. In order to minimize these risks, the SAM team can be included in the feasibility processes. Predictions and recommendations can be added to the checklist as to what the software model should be, which will be created without feasibility approval.

The responses to be given by the company for 8 risks out of the 12 identified risks and proposals regarding the controls are summarized above. For the remaining 4 risks, the company is not considering any control; these risks are (risks 5, 6, 7 and 10): Ineffective Inventory Control, Deficiency in Alternative Product Analysis, Long Purchase Processes, Internal Audit Risks. Due to the fact that the probability and possible impacts of the risks will be low, these risks are among the acceptable risks. It is expressed as the residual risk in the literature.

5. CONCLUSION AND DISCUSSION

We can also consider the old quotation of "if you can't measure it, you can't manage it" attributed to Peter Drucker as a principle for license inventory management [25]. It is the ability to measure, the precondition for the discipline of software products tracking purchased by companies for millions of liras. Only then can forwardlooking strategic decisions be made easily. Otherwise, it will continue to be the bleeding wound of companies as an uncertainty.

The aim of this study is to reveal the risks or opportunities that companies face while managing their IT software license assets and the measures to be taken against these risks with an enterprise risk management approach. While revealing these risks, one of the largest companies in terms of sample size was chosen as a pilot. The results are expected to be a guide for companies using software. The emergent results as a recipe are particularly advisory for companies managing complex and diverse software assets in their inventory. Moreover, it is thought to make a

contribution to the literature in terms of demonstrating whether the application of enterprise risk management adds value to companies.

Among the possible gains to be achieved with the study, the following can be listed: prevention of duplicate software procurement, optimization opportunities that may arise as a result of reducing maintenance costs by tracking the usage of purchased software.

As proposals, the following can be stated: to be prepared against vendor audits (external audit) while managing software assets, to protect against both reputational loss and business continuity risks thanks to the detection of old version software that may cause security vulnerabilities.

Companies need to create their own software inventories as a priority step. When starting the inventory conduct, taking a certain starting date as a baseline will make the process run more effectively. Otherwise, searching for very old-dated contracts will lead to both a waste of time and will not make any additional contribution. Also, it may not always be possible to access very old-dated contracts and information. There may be no detailed information in the contract documents, the contracts may be missing in the archives, the responsible persons may have quitted the job or the owner of the vendor may have changed.

Following a software inventory conduct based on a certain date, priority should be given to the software licenses of the most used and risky vendors. Building a SAM system according to the size and complexity of the companies is recommended.

In future academic studies, new risks can be added to the aforementioned risks, and the responses to be given according to the risk appetite, strategies and controls of the companies can be changed. Moreover, the maturity levels of companies regarding their information technology units in our country in their license inventory management can be questioned. The following issues can be examined: How many companies have set up and operated the SAM system and how many companies have not centrally managed any software license inventory.

REFERENCES

[1] H. Aksu, Dijitopya Dijital Dönüşüm Yolculuk Rehberi, Pusula 20 Teknoloji ve Yayıncılık, İstanbul, 2018.

[2] Internet: Presidency of the Republic of Turkey Digital Transformation Office, Information and Communication Security Guide, https://cbddo.gov.tr/bgrehber

[3] A. Durdu, A. Eren, (2021) "ISO 27001 Bilgi Güvenliği Yönetim Sistemi Yazılım Tasarımı", *Bilişim Teknolojileri Dergisi*, 14 (3), 255-266, 2021.

[4] Internet: Wikipedia. Software Licence, https://en.wikipedia.org/wiki/Software_license

[5] Internet: Gartner, Newsroom, https://www.gartner.com/en/newsroom/press-releases/2020-07-13-gartner-says-worldwide-it-spending-to-decline-7-point-3-percent-in-2020

[6] Internet: Aspera Training Catalog, Compiled from Aspera Company's End User Training Catalog, https://learning-aspera.usu.group

[7] Ş. Güneş, **Enterpirse Risk Management and A Survey Study Related ERM Awareness In Turkey**, Master Thesis, İstanbul Technical University, Institue of Science, 2009.

[8] Z. Şenol, Z. **The effect of enterprise risk management on firm performance: A Case Study on Turkey,** Ph. D. Thesis, Gaziosmanpaşa University, Social Science Institution, 2016.

[9] M. K. McShane, A. Nair, E. Rustambekov, "Does Enterprise Risk Management Increase Firm Value?", Journal of Accounting, Auditing & Finance, 26(4), 641-658, 2011.

[10] Internet: Google, Google Books Ngram Viewer. https://books.google.com/ngrams/graph?content=risk+management%2C+internal+audit%2C+internal+control&year_start=1920&year_end=2000&corpus=15&smoothing=3&share=&direct_url=t1%3B%2Crisk%20management%3B%2Cc0%3B.t1%3B%2Cinternal%20audit%3B%2Cc0%3B.t1%3B%2Cinternal%20control%3B%2Cc0

[11] H. Kıral, "Risks of Enterprise Risk Management", *Denetişim*, (18), 5-14, 2018.

[12] H. Kıral, İç Denetimin Kurumsal Risk Yönetimindeki Rolü, H. Kıral, (Ed.), İç Denetim "Yönetime Değer Katmak", Ankara: İç Denetim Koordinasyon Kurulu Yayınları No:1, 317-332, 2014.

[13] M. M. Şener, **A Research On The Determinants of Implementation Level of Enterprise Risk Management In Organizations**, Master Thesis, Bursa Uludağ University, Social Science Institution, 2019.

[14] Ş. Güneş, S. Teker, "Enterprise Risk Management Awareness In Turkish Energy Sector", *Doğuş University Journal*, 11(1), 64–76, 2010.

[15] H. R. Yazgan, P. Sönmez, "Risk Management of Software Development Project: An Example of A Bank ATM Project", *Ege Academic Review*, 15(1), 111–125, 2015.

[16] A. B. Olcaysoy, **Usage of Intelligent Methods In Cost and Risk Management Software Projects**, Ph. D. Thesis, Yıldız Technical University, Institue of Science, 2016.

[17] M. H. Calp, **Artificial Intelligence Based Risk Management For Software Projects**, Ph. D. Thesis, Gazi University. Informatics Institute, 2017.

[18] Y. D. Ö. Özen, A. Koçak, "Selection and Evaluation of Enterprise Resource Planning Software by Using Fuzzy Analytical Hierarchy Process and Fuzzy Dematel", *Journal of Management & Economics*, 24(3), 929–957, 2017.

[19] J. B. Gugler, Procurement and Asset Management of Commercial-Off-The-Shelf Software, Master Thesis, University of Twente School of Management and Governance Chair of Technology Management, 2018.

[20] V. P. Peltonen, **Sofware Asset Management, Current State and Use Cases**, Master Thesis, Helsinki Metropolia University of Applied Sciences, Master of Business Administration, 2015.

[21] Internet: Minister of Treasury and Finance, Public Internal Audit Manual, https://ms.hmb.gov.tr/uploads/2019/06/4046elkitabipdf.pdf

[22] J. Sim, J. Waterfield, "Focus group methodology: some ethical challenges", Qual Quant 53, 3003–3022, 2019.

[23] Internet: H. Marquis, G. Spivak, B. Victoria, Cut Software Spending Safely with SAM, http://gartner.com/home ID: G00301780.

[24] Flexera, Software Asset, and Licence Management Best Practice, Guidelines for IT Management, Number 340.

[25] Ö, Yanar, "Entelektüel Sermaye ve Örgütlerin Performansı Üzerine Etkisi", Maltepe University Faculty of Economics and Administrative Sciences, *Journal of Economic*, Social and Political Analysis, 2013(2), 79-96, 2013.

Annex 1. Questions

1	Licenses
2	Product/license description
3	Application/system name where the license is used
4	License model (category)
5	License model (sub-category)
6	Declared license model
7	Current quantity
8	Activation date
9	Expiration date
10	Contact person
11	Department name
12	Directorate name
13	Cost center
14	Supplier name
15	Manufacturer name
16	Purchase order number
17	Price per unit
18	Renewal price
19	Remarks
20	The licenses are managed?
21	Is there any unlicensed position?
22	The license can be replaced?
23	What are the alternatives?
24	Is the meeting completed?
25	Operation contact

Annex 2. License models

Category	Category Description	Sub Category
User	Licensing is based on users directly using the application	User
		Non Employee User
		UVU (User Value Unit)
		VUH (Virtual User Hour)
		Active User
		Concurrent User
		Active Concurrent User
		Authorized User
		Profile-based User
		Named User
		Virtual User
		Floating User
		Admin User
		GUI User
		Retail User
		Professional User
		Limited Professional User
		Employee Self-Service User
		Manager Self-Service User
		Employee User
		Developer User
		Expert User
		Business Information User
		Process Control User
		Partner User
		MSS User
		ESS User
		Agent
		Concurrent Agent
		Seat
		Site
CPU	Licensing based on CPU and components	CPU
		Processor
		Socket
		Core
		PVU (Processor Value Unit)
		RVU (Resource Value Unit)
Device	Licensing is based on using all kinds of device and device concepts (port, IP, instance)	Device
		Device (Concurrent)
		Network Device
		Mobile Device
		Agent
		Disk Drive
		Probe
		Point
		Instance
		Operating System Instance
		Home Gateway
		Rack
		Cabin
		Station (Concurrent)
		Phone
		Mobile Phone
		Server
		Application Server
		Exchange Server
		Virtual Server
		Database Server
		Client
		PC
		IP
		Port
		Node
		Platform
		Host
		Hardware
		RAM
		Named Host
		Environment
		Terminal
		Firewall
		Access Point
		Active Concurrent Access Point
		Router
		Switch
		Installation
Transaction / Traffic	Licensinis g based on using metrics	TPS (Transaction Per Second)

	containing transaction/traffic information of the service provided by the application	MBPS (Mega Bit Per Second)
		GBPS (Gigabit Per Second)
		Gigabyte Per Day
		(Inter)Connection Per Day
		Call
		Conference
		Concurrent Call
		Concurrent Conference
		Call per Month
		Call per Second
		EPS (Event Per Second)
		MSU (Message Signal Unit)
		MPS (Message Per Second)
		Query per Month
		MMS per Day
		CDR per Day
		Concurrent Session
		Log per Day
		CAL (Client Access License)
Capacity / Activity	Licensing is based on using metrics containing transaction/traffic information of the service provided by the application	Subscribers
		Mobile Subscribers
		Prepaid Subscribers
		Gigabyte
		Concurrent Video Stream
		VoD (Video on Deman) Content
		Concurrent VoD (Video on Deman)
		Connection
		Concurrent Connection
		Process
		Scenario
		Channel
		Object
		Data Objects
		Master Data Objects
		HAVE
		Payroll
		Engine
		Document
		Personnel
		Mailbox
		Subscription
		Application
Indirect	Licensing based on indicators not related to the service provided by the application	Customers
		Mobile Customers
		All Subscribers
		All Mobile Subscribers
		Budget
		Employee
		Full-Time Equivalent
		Spend Volume
		Flat Fee
		Revenue
Freeware	Situations that do not require any payment	Freeware
		Inhouse
		Bundle