Journal of Information Security, 2019, 10, 237-249
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Systematizing IT Risks

Georg Disterer

Department of Business Administration and Computer Science, University of Applied Sciences and Arts, Hannover, Germany
Email: georg.disterer@hs-hannover.de

How to cite this paper: Disterer, G. (2019) Systematizing IT Risks. *Journal of Information Security*, **10**, 237-249.
https://doi.org/10.4236/jis.2019.104013

Received: June 18, 2018
Accepted: October 11, 2019
Published: October 14, 2019

Abstract

IT risks—risks associated with the operation or use of information technology—have taken on great importance in business, and IT risk management is accordingly important in the science and practice of information management. Therefore, it is necessary to systematize IT risks in order to plan, manage and control for different risk-specific measures. In order to choose and implement suitable measures for managing IT risks, effect-based and cause-based procedures are necessary. These procedures are explained in detail for IT security risks because of their special importance.

Keywords

IT Risk, IT Security Risk, IT Risk Management, COBIT, ISO 27000

1. Introduction

Basic economic and political conditions for business are changing ever more rapidly, and technical developments in information technology (IT) advance at increased speed. IT is increasingly pervasive in business processes. At the same time, these business processes are becoming more complex. As a whole, many businesses have to manage a high degree of dynamic and complexity in using IT. As a result, the risk that negative deviations from plans and objectives will arise in using IT increases, along with IT risks as a whole.

The great significance that IT now has for many firms also causes new threats. As businesses rely more heavily on well-functioning IT, the risk is rising that IT will become a target of attacks for widely varying reasons (Disterer 2009), from a desire for recognition to greed, sabotage, or espionage, up to retaliation. As IT support becomes an integral part of business processes, the processed data from involved parties become increasingly more substantial. Therefore, the risk of a violation of these parties' interests—like privacy or business secrets—increases. Operational information processing provides a significant target, as it no longer takes place inhouse, isolated from the outside world. Instead, information processing is integrated into a wide variety of channels over the Internet and similar networks and the communication systems, applications and processes based on them. Legislators and authorities are increasingly compelled by this growing dependency and subsequent increase in risks to issue directives on the compliance of IT use and to exercise supervision and control. The risk of violating laws and other regulations grows as a result.

The term risk generally means an event or a situation that potentially results in negative outcomes or causes circumstances that produce negative deviations from plans or objectives. IT risks that stem from the operation and use of IT. Risk management represents the requirement and the aspiration not to let uncontrolled and unmanaged risks occur but to actively confront them instead. In risk management, risks are systematically planned, managed, and controlled. Risk management measures aim to avoid or reduce damage caused by negative results or conditions. Accordingly, risk management measures are preventive.

There are different types of risks. To meet the goal of risk management through planning, management and control of risks, it is necessary to systematize and differentiate risks in order to develop dedicated and suitable measures for avoiding or reducing damage. To that end, a variety of approaches for systematizing risks are put forth in professional literature [1], in which the results of the systematization are described in thoroughly differently terms: risk spheres, fields, types, categories, classes, objects, situations or events. The systematizations that are most important for IT risk management are discussed below.

Effect-based and cause-based procedures are necessary in order to choose and implement suitable measures for managing IT risks. The corresponding procedures are explained in detail for IT security risks because of their special importance.

2. Differentiation Criteria for IT Risks

A fundamental feature of the term risk is the uncertainty that prevails regarding the actual occurrence of a threat and the type and extent of likely consequences. Approaches of probability theory are established in natural and engineering sciences in order to differentiate risks based on their magnitude. This leads to a distinction between “big” and “small” risks. The corresponding calculation provided for this risk assessment multiplies the probability of occurrence of a risk by the expected amount of damage and thereby attains an adequate value for the magnitude of the risk. Assuming that the probability of occurrence and the amount of damage can be determined with sufficient exactness, a monetary value generally results.

This value is stochastic and provides the statistical expectation for the damage. Determining reliable values for the probability of an occurrence and the amount of damage, moreover, comes at significant expense and poses substantial problems in terms of methodology. In many cases, the values cannot be determined with sufficient exactness and estimates of unknown quality are used. Therefore, the calculation (magnitude of risk = probability of occurrence × amount of damage) is uncertain and only conditionally applicable, namely for a comparison between risks (using the same calculation and same certainty of input variables for probability of occurrence and amount of damage) or for evaluating the suitability of risk measures using a comparison of the amount of damage and the costs of the measures. Such a determination of risk level is still unsuitable in many situations. For example, if social factors such as consideration of human error need to be taken into account in risk management, then it is scarcely possible to determine the probability of occurrence with sufficient accuracy. Moreover, if there are threats to life or physical conditions, then the assumed amount of damage will be difficult to determine.

A simple example of calculating the magnitude of an IT risk: An IT system provides substantial support in order fulfillment. If the functions of the system drop out for about an hour due to a power outage, then between €100,000 and €300,000 is calculated for damage to the company, as the average damage amounts to €200,000. The probability of a power outage is to be determined from information from the electricity provider and from manufacturer specifications about the reliability of the components used inhouse for the electric supply. As a result, within a year, the expected probability of an occurrence of a power outage is 20%. The risk level is, therefore, calculated as follows: (probability of occurrence × amount of damage):

$$20\% \times €200,000 = €40,000$$

Subsequently, damage due to a power outage is to be expected as amounting to €40,000 yearly. This assumed amount of damage must be compared to the purchase and operational costs of components that ensure an uninterrupted power supply. An investment in such components represents a risk reduction measure, as the assumed probability of occurrence would be lowered. The economic benefits of an investment can be decided by varying methods of investment calculation methods.

If the probability of occurrence or amount of damage cannot be determined with sufficient accuracy, ordinal scales are often used as second-best approach and a distinction is made using levels of low/medium/high. The risks are assigned to predefined classes based on their magnitude [2]. Then the risks are shown in risk portfolios with coordinates for the probability of occurrence and amount of damage as in **Figure 1** with a few simple examples [3].

The differentiation of risks based on the level of magnitude is used above all to identify particularly pressing risks and to distribute available resources to different risks appropriately for risk management, to prioritize the risks and to allocate higher expenses to higher-level risks accordingly (see **Figure 2**). Risk portfolios are therefore used to ensure the efficiency of the risk management measures.

Risk portfolios are also used to identify appropriate risk management measures.

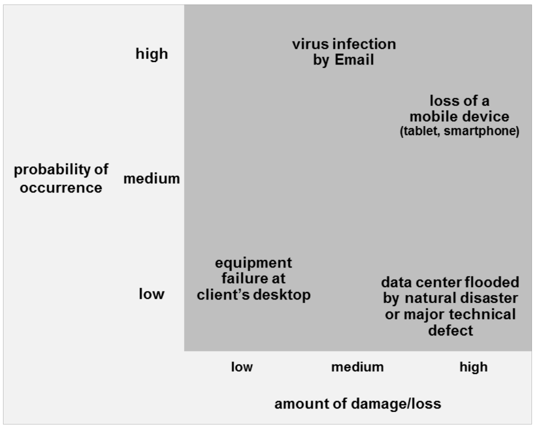
high
medium
low
probability of occurrence
virus infection by Email
loss of a mobile device (tablet, smartphone)
equipment failure at client's desktop
data center flooded by natural disaster or major technical defect
low
medium
high
amount of damage/loss

Figure 1. Risk portfolio with examples.

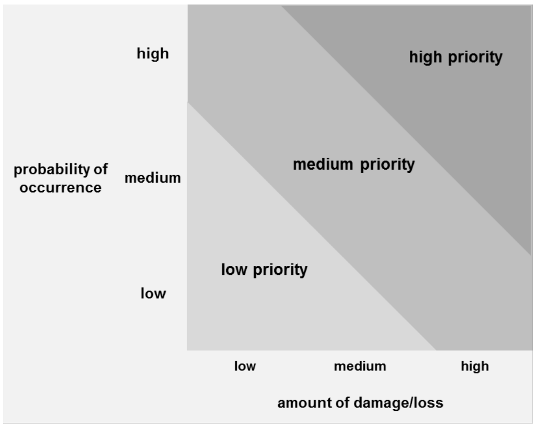

Figure 2. Risk portfolio with priorities.

These measures, called standard strategies, assigned to quadrants of risk portfolios can provide orientation [3] (see **Figure 3**). However, this approach offers hardly any reference as to which specific protective measures should be taken.

Other important differences between risks—as possible events or conditions with negative consequences—are based on the principle of cause and effect. Possible events and conditions or (feared) negative consequences are identified using this principle. Assuming a causal relationship, the events and conditions, therefore, become causes or triggers of a risk, and the consequences are viewed as effects or results. Identifying the causes and effects of risks establishes cause-based and effect-based differences between risks.

Using effect-based differentiation of risks, e.g. differentiation of material or immaterial damages after a risk occurs, makes it possible to identify particularly serious effects and assign measures to reduce or avoid additional damage accordingly in risk management. Effect-based differentiation like this is commonplace for IT risks; this is covered in more detail in Section 3.

Using cause-based differentiation of risks, e.g. differentiation due to natural or external events, due to technical failure, or due to human error makes it possible to isolate the causes of risks and then take dedicated countermeasures in risk

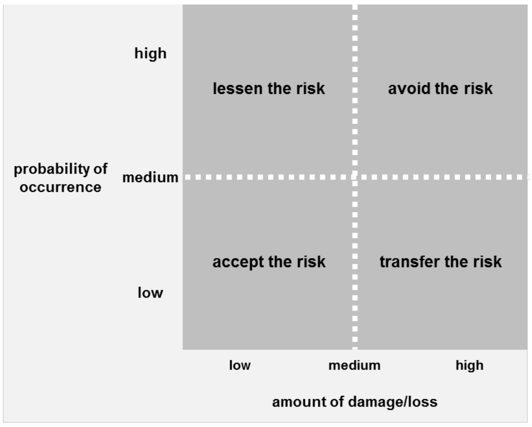

Figure 3. Risk portfolio with standard strategies of risk management.

management. The aim of the measures is to reduce or stop events or conditions that may cause the occurrence of risks and additional damage. Cause-based differentiation like this is commonplace for IT security risks; this is covered in more detail in Sections 4 and 5.

A number of other kinds of differentiations of IT risks are discussed in academic literature. Examples include differentiation based on business processes affected by the risks, whether the risks have an internal or external origin, whether they result from IT projects or IT operations, whether the resulting damage restricts operation of a business or "only" impedes IT operations, or whether it threatens routine IT operations or IT projects. Such differentiations are useful for certain issues but do not offer a comprehensive approach for planning, managing and controlling appropriate measures in IT risk management.

3. Effect-Based Differentiation of IT Risks

The word "consequence" in the concept "risks ~ possible events or conditions with negative consequences or negative deviations from the expected" is particularly of note when employing an effect-based perspective. Based on the principle of cause and effect, potential consequences or effects from the occurrence of an IT risk are sought [4]: Which types of damage resulting from events or conditions are to be expected? Which of these types of damage should be protected against? Which values (assets) require particular protection? Which IT objectives are in danger?

The objective of IT in business is generally to achieve the most efficient use of information as a resource. In risk management, formal objectives [5] are the next level to be differentiated: security and effectiveness and efficiency; to be expanded by adding the objective of governance, which includes compliance with company goals and with regulations and obligations for IT use. This makes it possible to differentiate IT risks based on the effects on various objective or protection areas:

- Risks to IT security.
- Risks to IT effectiveness and efficiency.

- Risks to IT governance.

Of these areas, IT security risks (see Section 5) have attained particular importance in recent years. The effectiveness objective [5] refers to the capability of IT systems to readily support the information and communication needs of a company. It is necessary to provide the proper IT systems to support business processes effectively. The efficiency objective [5] refers to the need for IT systems to support cost-effective development and operation. IT governance objectives dictate compliance with laws, regulations and legal requirements. Such effect-based differentiations are also established in common operational frameworks for IT management. For example, these types of objective areas are detailed in the APO12 "Manage Risk" process in COBIT 5 [6]. The differentiation acts to identify and prioritize each area in IT risk management which requires special attention. However, support is not offered for planning, managing and controlling specific protective measures.

4. Cause-Based Differentiation of IT Risks

The words "events" and "conditions" in the concept "risks ~ possible events or conditions with negative consequences or negative deviations from the expected" are particularly of note when employing a cause-based perspective. Based on the principle of cause and effect, events or conditions that cause IT risks and subsequent damages are sought. If the originating events (or conditions) are identified, preventive measures can be taken that either 1) prevent the events; 2) prevent the damage or 3) reduce the damage. Accordingly, cause-based differentiation is helpful in planning, managing and controlling specific measures—also when compared to differentiations according to risk level and risk effects ("effect-based").

As part of cause-based differentiation [4], all causal events and conditions must be identified if possible—otherwise, gaps will exist in IT risk protection. Starting from events and conditions that can trigger damage, the search should look for potential consequences using a top-down approach. Likewise, a bottom-up approach should be used to search for causal events and conditions starting from potential consequences. As thoroughness is important during risk identification, these two procedures are often iteratively linked.

In principle, measures that limit damage can be taken against all events with negative consequences. Examples include:

- Protecting buildings or having alternate buildings ready in the event of natural disaster.
- Having a backup system ready in case of technical components fail.
- Conducting plausibility checks before entries or operator actions are forwarded and processed in the event of user errors.
- Testing systems before putting them into operation during the development of IT systems.

The measures detailed in these examples usually cannot neutralize potential consequences completely. For example, switching time needs to be taken into account when using a prepared substitute. Nonetheless, suitable measures can substantially reduce consequences. If a threatening event occurs for which measures are planned and these measures have the expected effect, then the damage is substantially minimized. However, if the measures do not have the expected effect, more damage occurs than had been predicted. In this case, a risk has been clearly identified, but either sufficient measures were not applied or the measures did not function as intended. The protective measures are then inadequate; they are incomplete, insufficient or inappropriate. The measures are therefore described as "vulnerabilities" and the threatening events or conditions are described as "threats".

In the case of a cause-based approach, additionally, threats and vulnerabilities are differentiated. Threats are causal events or conditions that are likely to occur and cause damage; vulnerabilities represent problems or deficiencies in protective measures. Common classifications differentiate threats by harmful natural or external events, technical failures and human errors, vulnerabilities by technical, personal and organizational deficiencies [7].

Following the aforementioned premise that sufficient protective measures can be taken against all threats, indefensible damage only occurs if a threat finds a vulnerability. Differentiating between threats and vulnerabilities opens the way to identify two complementary analysis tasks. Threat analysis has the primary objective to account for all risks and to define corresponding protective measures—if possible, otherwise, threats may occur that are not covered by measures. A vulnerability analysis is then conducted to check whether the protective measures are complete, sufficient and appropriate, otherwise, vulnerabilities may arise. Protective measures are usually only sufficient if they consist of a range of coordinated measures.

Within this concept of threats and vulnerabilities, the original definition…

risk ~ possibility that events or conditions with negative consequences or negative deviations from the expected occur is used synonymously in common frameworks [7] [8] [9] [10]:

risk ~ possibility that "threat meets vulnerability" occur and damage results.

An arrangement like the one in **Table 1** can be chosen in IT risk management using this definition of risk. This structure illustrates the "threat meets vulnerability" relationship: If a threat (column) meets a vulnerability (row), then a risk

Table 1. Mapping of threats and vulnerabilities.

Vulnerabilities in protective measures	Threats		
	Natural or external events	Technical failure	Human error (intention, ignorance, mistake)
Technical			
Personal			
Organizational			

occurs and damage will result (cell). Therefore, if possible, all threats are to be identified and covered by protective measures, making sure at the same time that these measures are sufficient, as otherwise, vulnerabilities appear and risks occur.

A few examples demonstrate the "threat meets vulnerability" interaction:

- Users make mistakes by accident (third column), for example, because they are inattentive or distracted. As long as the technical systems (row 1) are fault-tolerant in this respect (thanks to plausibility checks upon input or through questions such as "Are you sure?") no damage results from the threat and the protective measures succeed. Only when accidental user errors occur that are not caught by the technical systems does the risk become real and damage occur. The threat of "accidental user errors" can be met also through personnel measures (row 2), for example, by not imposing any unnecessary time pressure or by paying attention to sufficient awareness of the personnel in question when assigning tasks. The threat of "accidental user errors" can be met also through organizational measures (row 3), for example, if workstations are sufficiently isolated from disruptive noise or rules are put in place for taking breaks to refresh oneself. If these technical, personnel or organizational measures are insufficient, then they will have vulnerabilities—and accidental user errors will cause damage despite the protective measures.
- Users could purposely try to gain unauthorized access to IT systems and data (column 3). This threat can be countered technically by having IT systems include functions to properly authenticate and authorize users, for example, by requiring input of a username and password and assigning appropriate access rights (row 1). A personnel measure would be to penalize unauthorized use of IT systems and data (row 2). Organizationally, the threat could be met by making the rights clear, understandable and appropriately structured for the respective work (row 3). Again, if the mentioned technical, personnel or organizational measures are insufficient or faulty, then they will have vulnerabilities.
- All kinds of events can cause data loss: natural events such as lightning striking a data center or technical failure of a storage component (column 1 and 2). Technical protective measures can prevent this or minimize the damage; for example, use of redundant components as a substitute (row 1). Personnel measures such as training can minimize malfunctions and misuses and their consequences. Organizational measures, such as regularly creating backup copies, can minimize the damage by enabling databases to be quickly restored (row 3). Again, if the mentioned technical, personnel or organizational measures are insufficient or faulty, then they will have vulnerabilities. Using the example of backup copies: To cover potential vulnerabilities, it is necessary to test regularly whether the copies are created properly and can be restored without any problems.
- Project risks: Many activities for developing information systems are organized in the form of projects. This covers the risk that events or circums-

tances over the course of the project lead to missed project goals with respect to time, costs and quality. Project risk management should comply with the structure shown in Table 1: Threats such as harmful natural or external events, failure of technology or human error jeopardize the project goals; protective measures in the areas of technology, personnel and organization prevent or minimize damage. An example of frequent human error that is typical for projects is insufficient effort estimates, for example, because the complexity of a project task is underestimated (column 3). For projects, the focus is on organizational protective measures in the form of tried-and-tested methods and processes of project management (row 3). Damage in the form of unachieved goals is triggered if threats meet vulnerabilities in the protective measures.

The procedures in IT risk management get a concrete form with the "threat meets vulnerability" interaction (see Table 1): When identifying risks, it is critical to cover all threats completely (with the columns). When planning, controlling and monitoring protective measures (with the rows), it is critical that the measures be sufficient for every threat. Table 1 complies with common methods and procedures in IT risk management when using cause-based differentiation [3] [4] [7] [9] [10].

5. Methodology for Managing IT Security Risks

For effect-based differentiation of IT risks (Section 3), IT security risks are distinguished from IT risks that threaten achievement of the IT effectiveness and efficiency as well as IT compliance. In contrast, IT security risks threaten the basic values of availability, integrity and confidentiality of information [8]:

- Availability: property of being accessible and usable upon demand by an authorized entity.
- Integrity: property of protecting the accuracy and completeness of information.
- Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

IT security is, therefore, the condition in which availability, integrity, and confidentiality of information and information technology are protected by appropriate measures such that the risks from threats and vulnerabilities are reduced to an acceptable level [9]. Achieving and maintaining this condition has become a significant duty for companies in recent years because processing of information is subjected to significant risks from connecting to the Internet and similar networks, and it particularly provides a large area or surface that can be attacked.

Thus IT security risks become recognizable through effect-based differentiation of risks (Section 3). Also carrying out cause-based differentiation of IT risks (Section 4) relies on differentiating threats and vulnerabilities (based on Table 1). That means IT security risks represent the possibilities that the basic values of availability, integrity, and confidentiality are violated because threats meet vulnerabilities; Figure 4 illustrates this relationship.

Figure 4 also clarifies the basic methodology for risk and security analyses: After an analysis of the threats, technical, personnel and organizational protective measures are taken, which are then reviewed as part of the analysis of vulnerabilities and improved if necessary.

In the course of the threat analysis, as many threats as possible are identified and checked for relevance. Typical threats that must be addressed by all means include fire or water ingress, failure of technology such as servers or network components, incorrect user input, operator error and viruses. However, it is virtually impossible to achieve a complete analysis of all threats by enumerating the threats, which is why it is necessary to follow a systematic approach. In this approach, it is necessary to distinguish between whether threats are caused by harmful natural or external events, failure of technology or human error (Figure 4).

Threats due to harmful natural or external events are beyond direct control and cannot be directly neutralized or prevented; companies can only protect themselves through measures for reducing damage. Examples include preventive measures taken for catastrophic events such as flooding, hurricane, earthquake or war. Many technical measures for this depend on redundancy, *i.e.* on having multiple instances of important technology available so that, in the event of a disaster, it is possible to switch over from affected technology to an undamaged instance. Personnel measures usually include continuing education and training to prepare for catastrophic events and thereby ensure sufficient competency when there is a need to respond amid the hectic mindset resulting from a threat

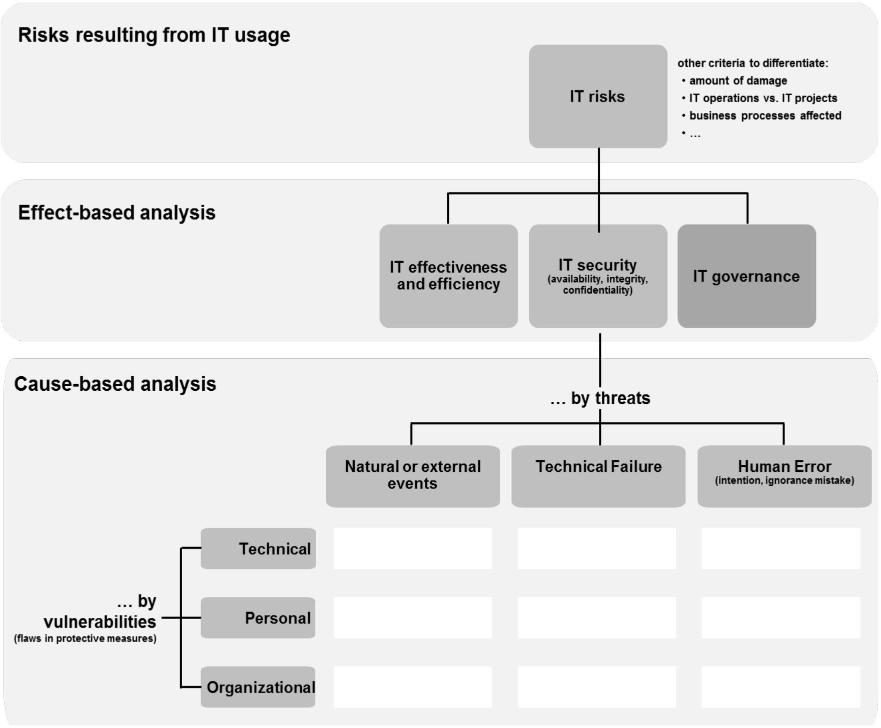
Risks resulting from IT usage
IT risks
other criteria to differentiate:
• amount of damage
• IT operations vs. IT projects
• business processes affected
• ...
Effect-based analysis
IT effectiveness and efficiency
IT security (availability, integrity, confidentiality)
IT governance
Cause-based analysis
... by threats
Natural or external events
Technical Failure
Human Error (intention, ignorance mistake)
... by vulnerabilities (flaws in protective measures)
Technical
Personal
Organizational

Figure 4. Effect-based and cause-based differentiation of IT risks.

and time pressure. Organizational measures provide for structured and targeted action in the form of emergency plans; organization also includes practicing implementation of the plans.

Threats due to technical failure can be countered with technical measures that involve redundancy. Personnel measures include training and instruction for replacing components; organizational measures include establishing instructions and guidelines for controlling and monitoring systems.

Threats due to human error are to be distinguished according to the various reasons of intention, ignorance and mistake. In the event of intentional (incorrect) actions, persons purposely try to cause damage or improperly create an advantage for themselves. Today this form of human error is pragmatically labeled as an "attack" and can result from a wide variety of motives [11]. It is also regarded as intentional incorrect action if persons knowingly exploit properties of information systems because of laziness; for example, taking shortcuts or misusing gaps to make things easier and thus increase the convenience when using the IT systems. Technical measures are essentially based on preventing unauthorized access to IT systems, that is, technically issuing, controlling and monitoring access rights. Personnel measures include, for example, not hiring anyone for critical tasks in the company if events in their past or personal life give occasion to doubt their reliability. Organizational measures include defining access rights to IT systems so that they are sufficient for the respective tasks and responsibilities, but do not go beyond those.

Human error is due to ignorance if persons unintentionally and mistakenly use IT systems and thereby incur damage for the company. This can be prevented using technical measures, for example, by providing sufficient instructions and help systems. Examples of personnel protective measures can include sufficient training. Organizational measures can ensure that tasks and responsibilities are assigned only within the scope of existing skills.

Human error due to mistakes or accidents must always be considered for complex tasks or IT systems that are complicated to operate. The errors usually occur due to lack of attention because of distractions, excessive stress or fatigue. Considerable damage can result from such factors. Classic examples include accidentally entering incorrect information or accidentally operating IT systems incorrectly. Technical measures depend on checking the plausibility of input or operator actions before executing the respective function and, if necessary, rejecting them. Or automatic prompts such as "Are you sure that…?" alert the user before the execution of critical functions. Technical measures like this are used to strive for fault tolerance of the IT systems to rule out accidental incorrect actions. Personnel measures can increase awareness and reduce work-related pressure and stress. Organizational measures can ensure that distractions, stress and fatigue are as low as possible, for example, through suitable workstation design or regulation of work time and breaks.

In the case of a threat analysis, external sources of information are to be used to ensure that the threats are identified completely. Thus the international standard ISO 27005 contains a detailed list of threats, even if they are merely examples. Companies can use this list to check and supplement their own efforts [7]. And reports like "The IT Security Situation in Germany" [12] published annually describe and analyze current threats for IT systems specifically explaining current means and methods of attack.

A threat analysis and development of technical, personnel and organizational protective measures based on that are followed by a vulnerability analysis. Taking into account the "threat meets vulnerability" interaction (**Figure 4**), an assessment is carried out to see whether the goals of the protective measures are actually achieved. In the case of a vulnerability analysis, external sources of information are to be used as supplements. Thus the "IT risk management guide" [13] contains a description of the procedure and a generic list of over 200 vulnerabilities that companies can use for internal testing. Likewise, the ISO 27005 standard contains an extensive catalog of typical vulnerabilities that companies can use to check and supplement their own measures [7]. Another useful source is the "vulnerability traffic light" at the Warning and Information Services website of the German Federal Office for Information Security (Computer Emergency Response Team of the German Federal Government at https://www.cert-bund.de/schwachstellenampel). The current situation with regard to security gaps in common software products is listed entering and evaluating publicly known vulnerabilities of the products.

A vulnerability analysis usually results in necessary improvements and supplements of the protective measures, which then have to be planned, managed and controlled. This kind of analysis is to be carried out regularly after the control loop of planning, managing and controlling measures, both during initial planning and later during managing and controlling.

6. Conclusion

The integration of IT in business processes will continue to increase even as IT risks rise. Managing the great number and variety of IT risks will require to use a systematical risk management process in order to address each different risk specifically. In practice, systematization approaches are used for various purposes. For a viable methodology for managing security risks, a combination of effect-based and cause-based differentiation of the risks is advisable for selecting complete, sufficient and appropriate measures.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Romeike, F. (2003) Risikoidentifikation und Risikokategorien. In: Romeike, F. and Finke, R., Eds., *Erfolgsfaktor Risikomanagement*, Gabler, Wiesbaden, 165-180. https://doi.org/10.1007/978-3-663-05715-4

[2] ISACA and Risk Management Association (2014) Leitfaden ISO 31000 in der IT. Kelkheim.

[3] Prokein, O. (2008) IT-Risikomanagement. Gabler, Wiesbaden.

[4] Knoll, M. (2014) Praxisorientiertes IT-Risikomanagement. Dpunkt, Heidelberg.

[5] Heinrich, L.J., Stelzer, D. and Riedl, R. (2014) Informationsmanagement. Oldenbourg, München. https://doi.org/10.1524/9783110353068

[6] ISACA (2012) COBIT 5—Enabling Processes. Rolling Meadows.

[7] ISO 27005 (2011) Information Technology—Security Techniques—Information Security Risk Management. Geneva.

[8] ISO 27000 (2009) Information Technology—Security Techniques—Information Security Management Systems. Geneva.

[9] Bundesamt für Sicherheit in der Informationstechnik (2009) Informationssicherheit Ein Vergleich von Standards und Rahmenwerke. Bonn.

[10] ISACA (2013) COBIT 5 for Risk. Rolling Meadows.

[11] Disterer, G. (2012) Attacks on IT Systems: Categories of Motives. In: Chou, T.-S., Ed., *Information Assurance and Security Technologies for Risk Assessment and Threat Management*: *Advances*, Information Science Reference, Hershey, 1-16. https://doi.org/10.4018/978-1-61350-507-6.ch001

[12] Bundesamt für Sicherheit in der Informationstechnik (2014) Die Lage der IT-Sicherheit in Deutschland. Bonn.

[13] ISACA (2013) ISACA-Leitfaden: IT-Risikomanagement—leicht gemacht mit COBIT. Kelkheim.