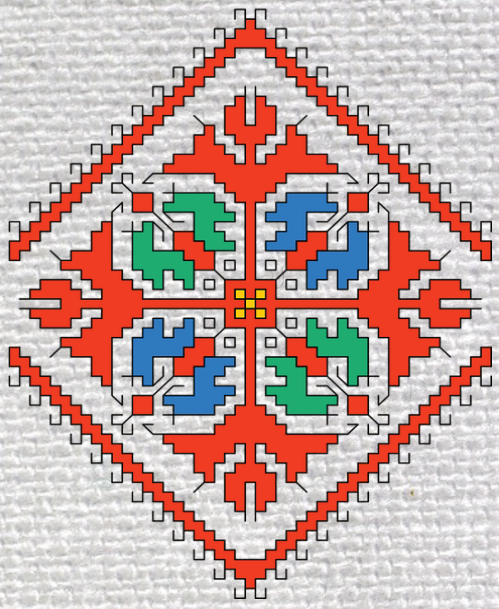
Образование, научни изследвания и иновации



Education, scientific research and innovation

ЗА БУКВИТЕ
О ПИСМЕНЕХЪ

Профил на списанието

„Образование, научни изследвания и иновации“ е двуезично (на английски и български език) научно списание, което се издава от Академично издателство „За буквите – О писменехь“ към Университета по библиотекознание и информационни технологии – гр. София, България. Изданието цели да популяризира висококачествени теоретични и приложни изследвания в научните направления, в които Университетът по библиотекознание и информационни технологии е акредитиран да обучава от Националната агенция за оценяване и акредитация. Във връзка с това основните тематични рубрики на списанието са:

- История и археология;
- Обществени комуникации и информационни науки;
- Информатика и компютърни науки;
- Национална сигурност;
- Актуално.

Списанието отразява иновативни идеи, научни резултати, съвременни тенденции и перспективи за развитие в изброените научни области. Публикуват се само оригинални научни статии, преминали двойно сляпо рецензиране.

Списание „Образование, научни изследвания и иновации“ е със свободен достъп.

https://e-journal.unibit.bg/
ISSN 2815-463

Journal Scope

“Education, Scientific Research and Innovations” is a bilingual (in English and in Bulgarian) scientific journal, which is published by the Academic Publisher “Za Bukvite – O Pismeneh”, at the University of Library Studies and Information Technologies – Sofia, Bulgaria. The publication aims to promote high-quality theoretical and applied research works in the scientific fields, accredited for teaching to the University of Library Studies and Information Technologies by the National Agency for Assessment and Accreditation.
In this regard, the main thematic sections of the journal are:

- History and archaeology;
- Public communications and information sciences;
- Informatics and computer sciences;
- National Security;
- Current topics.

The journal reflects innovative ideas, scientific results, modern trends and prospects for development in the listed scientific fields. Only original scientific articles that have passed double-blind peer review are published.

The “Education, scientific research and innovation” journal is open access.

https://e-journal.unibit.bg/
ISSN 2815-4630

ОБРАЗОВАНИЕ, НАУЧНИ ИЗСЛЕДВАНИЯ И ИНОВАЦИИ

Научно списание
Година II, книжка 6, 2024

EDUCATION, SCIENTIFIC RESEARCH AND INNOVATIONS

Scientific journal
Vol. II, Issue 6, 2024

ЗА БУКВИТЕ О ПИСМЕНЕХ

ГЛАВЕН РЕДАКТОР
гл. ас. д-р Елисавета Цветкова
Факултет по библиотекознание
и културно наследство
Университет по библиотекознание
и информационни технологии
бул. „Цариградско шосе“ № 119,
София 1784, България
тел.: +359 894 70 38 70
е-поща: e.cvetkova@unibit.bg

ИЗДАТЕЛ
Академично издателство
„За буквите – О писменехь“
Университет по библиотекознание
и информационни технологии
ДИРЕКТОР
доц. д-р Диана Стоянова
бул. „Цариградско шосе“ № 119,
ет. 2, стая 213
София 1784, България
тел.: +359 879 14 83 85
е-поща: d.stoyanova@unibit.bg

Списание „Образование, научни изследвания
и иновации“ излиза четири пъти годишно:
книжка 1 – януари – март;
книжка 2 – април – юни;
книжка 3 – юли – септември;
книжка 4 – октомври – декември.

EDITOR-IN-CHIEF
Chief Assist. Prof. Elisaveta Tsvetkova, PhD
Faculty of Library Studies
and Cultural Heritage
University of Library Studies
and Information Technologies
119, Tsarigradsko Shosse Blvd.
Sofia 1784, Bulgaria
tel. +359 894 70 38 70
E-mail: e.cvetkova@unibit.bg

PUBLISHER
Academic Publisher
“Za Bukvite – O Pismeneh”
University of Library Studies and Information
Technologies
DIRECTOR
Assoc. Prof. Diana Stoyanova, PhD
119, Tsarigradsko Shosse Blvd.
fl. 2, room 213
Sofia 1784, Bulgaria
tel.: +359 879 14 83 85
E-mail: d.stoyanova@unibit.bg

Journal “Education, Scientific Research and
Innovations“ is published four a year:
book 1 – January – March;
book 2 – April – June;
book 3 – July – September;
book 4 – October – December.

Съдържание | **Contents**

ОБЩЕСТВЕНИ КОМУНИКАЦИИ И ИНФОРМАЦИОННИ НАУКИ
PUBLIC COMMUNICATIONS AND INFORMATION SCIENCES

ENHANCING EXECUTIVE SELECTION: THE IMPACT OF FORENSIC PSYCHOLOGY ON PREDICTIVE VALIDITY AND ORGANIZATIONAL FIT

Lukas van Lengerich
University of Library Studies and Information Technologies

Abstract: *Integrating forensic psychology principles into Human Resources (HR) practices significantly advances modern recruitment, particularly in executive selection. This study develops a research model to evaluate the impact of these approaches. By using techniques like integrity tests, situational judgment tests, and behavioral interviews, the study explores their potential to improve predictive validity and organizational fit.The methodology includes quantitative and qualitative analyses, with surveys given to HR professionals, executive job applicants, and hired executives. The study hypothesizes that forensic-psychological principles enhance predictive validity for job performance and reduce misemployment risk. Key variables include the effectiveness of these techniques and their correlation with job performance, organizational fit, and retention.Findings suggest that situational judgment and integrity tests effectively assess candidate attributes, while techniques like the Forensic Assessment Interview Technique and stress interviews present biases and negative candidate experiences. The study emphasizes the need for appropriate technique selection, thorough training for HR professionals, and ethical application.The research concludes that integrating forensic-psychological principles can improve executive recruitment by enhancing hiring accuracy and cultural alignment.*
Keywords: *Forensic Psychology, Executive Recruitment, Candidate Assessment*

INTRODUCTION

The evolution of interview techniques and the increasing integration of interdisciplinary approaches, particularly from forensic psychology, into HR practices represents a significant development in modern recruitment. This research aims to develop a comprehensive research model and questionnaire that allows for the investigation of the impact and effectiveness of these approaches in the context of executive selection. By carefully analyzing theoretical foundations and considering practical examples, this study seeks to gain a deeper understanding of the potentials and limitations of forensic psychology in the context of selection procedures.

Forensic psychology offers unique insights into human behavior, integrity assessments, and psychological evaluations that extend beyond traditional interview methods. Incorporating these principles into executive selection processes aims to enhance the accuracy of predicting future job performance and organizational fit, thereby reducing the risks associated with misemployment and enhancing overall organizational effectiveness.

RESEARCH METHODOLOGY

The core question of this research is to what extent principles from forensic psychology have influenced and optimized the selection process for executives. Specifically, the effectiveness of these principles in predicting job performance and determining organizational fit of candidates will be evaluated. The research will explore whether and how the application of forensic-psychological techniques can contribute to improved identification of leadership talents who not only have the necessary professional skills but also the ethical and social competencies.

HYPOTHESES

This study proposes that applying forensic-psychological principles to executive selection enhances predictive validity for future job performance and organizational integration. Techniques like integrity tests, situational judgment tests, and behavioral interviews can identify suitable candidates, improve hiring accuracy, and ensure new hires align with company culture and ethical standards.

1. Predictive Validity: The first hypothesis posits that using forensic-psychological principles significantly increases the predictive validity of job performance and organizational integration. Candidates selected through these methods are likely to perform better and integrate more smoothly into the organization. Integrity tests assess honesty and ethical behavior, while situational judgment tests evaluate decision-making skills.

2. Misemployment Risk: The second hypothesis suggests that integrating forensic-psychological techniques reduces misemployment risk. By matching candidates with the company's values and ethical standards, organizations can improve retention and satisfaction, maintaining a cohesive and motivated workforce.

3. Personality Assessment: The third hypothesis highlights the value of forensic-psychological interviews for assessing candidates' personalities. These interviews reveal aspects of character not typically covered by conventional techniques, offering insights into candidates' integrity, reliability, and ethical orientation.

VARIABLES

The study identifies variables to measure these hypotheses effectiveness. Independent variables include the application of forensic-psychological principles and the type of techniques used, such as integrity tests for counterproductive behaviors, situational judgment tests for problem-solving skills, and behavioral interviews for assessing past behavior. Dependent variables are the predictive validity of the selection process and organizational fit, measured by performance indicators and employee satisfaction surveys. High predictive validity and organizational fit indicate effective hiring and employee retention.

Integrating forensic-psychological principles into executive selection can significantly improve hiring outcomes. These methods enhance predictive validity and align candidates with organizational culture and ethical standards, building a competent leadership team. Forensic-psychological interviews provide a valuable tool for identifying trustworthy and reliable candidates, reducing misemployment risk, and fostering a positive organizational environment.

DATA COLLECTION

A multi-stage research approach combining quantitative and qualitative research methods will be employed. This enables a comprehensive analysis of the effects of forensic-psychological principles on the selection process and offers the opportunity to gain deeper insights into practical applications and associated challenges.

SURVEYS

The study involves the design and administration of three distinct surveys tailored to different cohorts within the recruitment ecosystem: HR professionals/managers, executive job applicants, and successfully hired executives. Each survey aims to capture demographic data, the frequency and perceived effectiveness of various forensic-psychological techniques, and the challenges encountered during implementation.

RESULTS

Data was obtained through interviews with 46 HR professionals to determine whether they applied forensic psychology methodologies in their recruitment processes for executive positions. The findings provide insights into the prevalence and effectiveness of these techniques in the executive selection process.

DEMOGRAPHIC DISTRIBUTION

The surveys captured a wide range of demographic data to ensure a comprehensive understanding of the respondents' backgrounds and experiences.

– **Experience:** The average experience of respondents is approximately 6 years, with a range from 1 to 14 years. This variation provides insights from both relatively new and highly experienced HR professionals.

– **Current Role:** Predominantly HR generalists, with a significant number of responses from the engineering sector. This indicates a diverse perspective on the application of forensic-psychological techniques across different industries.

– **Application of Forensic-Psychological Methods:** All respondents indicated using forensic-psychological methods in the interview process, highlighting the widespread acceptance and implementation of these techniques in modern HR practices.

RESULTS VISUALIZATION

To better understand the distribution and effectiveness of forensic-psychological techniques, the following chart illustrates the average success rates and perceived effectiveness of each technique.

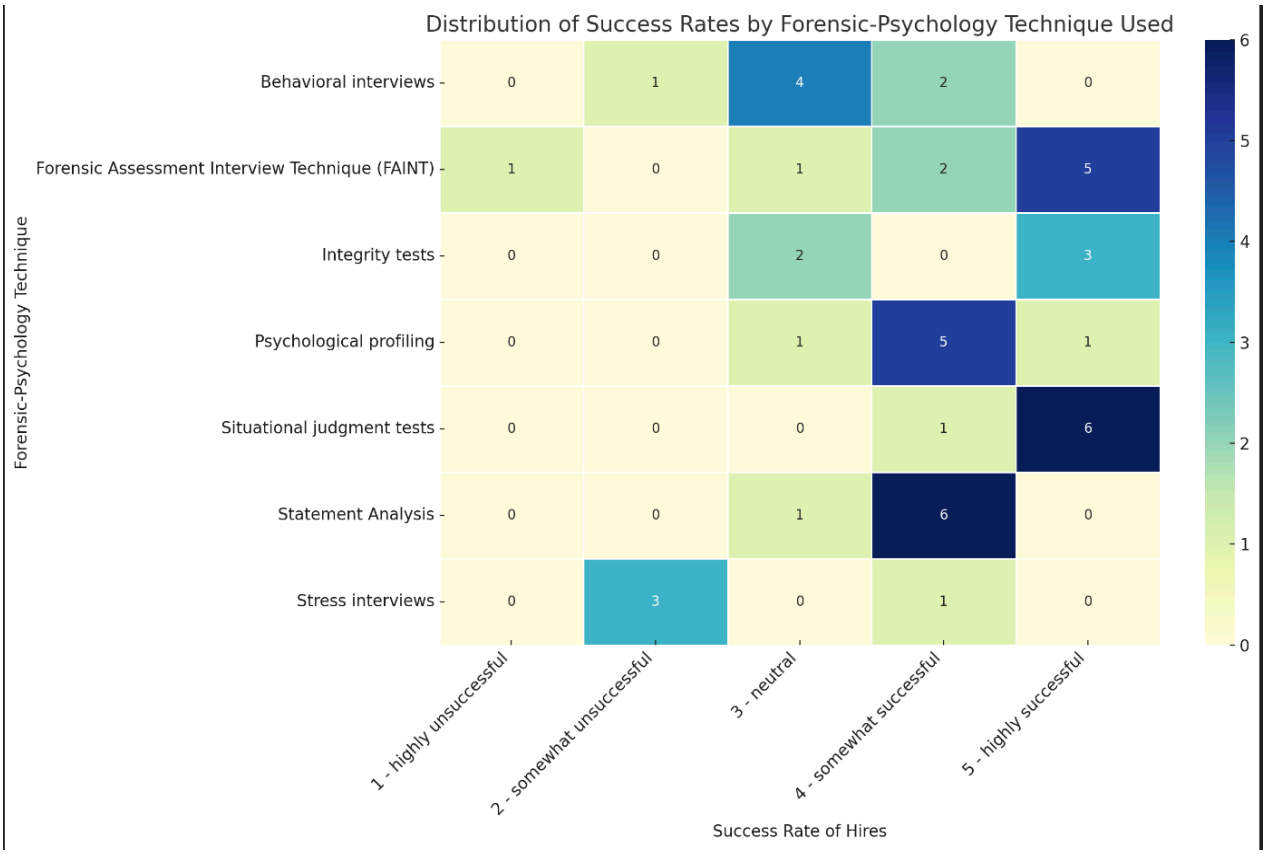


Fig.1. Heat map visualizing distribution of success rates

The heat map visualizes the distribution of success rates for each forensic-psychological technique used. Each cell shows the number of respondents who rated the success of their attitudes within a specific category for each technique:

– Series: Various forensic-psychological techniques.

– Columns: Categories of the success rate of hires, ranging from "1 – very unsuccessful" to "5 – very successful".

This visualization not only helps to understand which techniques are perceived as most effective (by looking at the concentration of higher success rates), but also provides insight into the variability and consistency of these perceptions. For example, techniques with a high concentration of responses in the

categories "4 – reasonably successful" and "5 – very successful" can be considered more consistently effective according to the respondents' experiences.

Some techniques may show a wide distribution across success categories, indicating different experiences among respondents, while others may have a focus on categories with higher success rates, suggesting a more consistent positive score.

EFFECTIVENESS OF TECHNIQUES

The effectiveness of forensic-psychological techniques was evaluated based on their impact on the selection process and organizational outcomes. The evaluation revealed distinct differences in how each method is perceived and utilized.

– Situational Judgment Tests (SJTs): SJTs are seen as the most effective, valued for assessing candidates' decision-making and problem-solving abilities in work-related scenarios. These skills are crucial for leadership roles, as they provide insight into how candidates might handle real-life situations (Lievens & Patterson 2011).

– Integrity Tests: These are rated highly effective for measuring honesty and ethical standards, essential for maintaining a positive organizational culture. By assessing traits like honesty and trustworthiness, integrity tests help ensure employees uphold the company's values (Ones, Viswesvaran & Schmidt 1993).

– Forensic Assessment Interview Technique (FAINT): FAINT is moderately effective, focusing on truthfulness and deception risks, though concerns about potential biases exist (Jansen & Vinkenburg 2006). It should be applied with caution and supplemented by other methods.

– Stress Interviews: These are perceived as the least effective, as they may negatively impact the candidate experience and lead to biased judgments. The anxiety induced by such interviews can result in poor performance that doesn't reflect candidates' true potential (Jansen & Vinkenburg 2006).

CORRELATION ANALYSIS

A correlation analysis examined relationships between forensic-psychological techniques and outcomes.

– Positive Correlations: Techniques like psychological profiling and SJTs showed positive correlations with successful evaluations and organizational fit, suggesting they effectively identify candidates who excel and fit well within the culture (Barrick & Mount 1991).

– Negative Correlations: FAINT and stress interviews correlated negatively with successful outcomes, highlighting potential drawbacks or contextual challenges. Stress interviews may induce anxiety, leading to poor performance, while FAINT's focus on deception might introduce biases.

CONCLUSIONS/DISCUSSION

Forensic-psychological techniques differ significantly in their perceived effectiveness. Situational Judgment Tests (SJTs) and integrity tests are considered the most effective, as they support hiring by accurately assessing critical candidate attributes and helping maintain a positive organizational culture. These methods are valued for their ability to evaluate decision-making skills, ethical standards, and overall suitability for leadership roles.

However, techniques like the Forensic Assessment Interview Technique (FAINT) and stress interviews present notable challenges. They can introduce potential biases and result in negative candidate experiences, which may lead to poor performance evaluations that do not accurately reflect the candidates' true potential.

Organizations should prioritize methods that enhance accuracy and create a positive candidate experience, while carefully reevaluating those with significant drawbacks. By focusing on refining and improving their selection processes, companies can ensure that they choose the best candidates who align with their values and culture, ultimately contributing to organizational success. Continuous assessment and adaptation of these techniques will be crucial to maintaining the effectiveness and integrity of the recruitment process.

IMPLICATIONS FOR HR PRACTICES

HR professionals require comprehensive training to apply forensic-psychological techniques ethically and effectively. Understanding both the theoretical foundations and practical applications of these techniques is crucial for maximizing their benefits (Schmidt & Hunter 1998). Regular feedback and evaluation are essential to refine these methods continually, ensuring transparency and fairness, which are vital for maintaining trust and integrity in the selection process (Archer 2008). By fostering an environment of continuous learning and improvement, HR practitioners can better align recruitment practices with organizational goals and cultural values.

CONCLUSION

The research emphasizes the importance of forensic-psychological principles in executive recruitment. While these techniques can enhance predictive validity and organizational fit, they require careful consideration, thorough training, and ongoing evaluation to maximize benefits and minimize ethical concerns. HR practitioners should strategically integrate these techniques to improve the effectiveness and integrity of executive selection.

Organizations should prioritize techniques with high predictive validity, such as psychological profiling and situational judgment tests (SJTs), especially for roles requiring strategic decision-making and ethical judgment. Ethical implementation, including candidate understanding of the assessment process, can improve experience and perceived fairness. Regularly updating training programs and incorporating feedback from candidates and HR practitioners enhance the techniques' effectiveness over time. Comprehensive evaluations of selection outcomes help identify the most effective techniques and areas for improvement.

Strategically implementing and refining forensic-psychological techniques can significantly enhance executive selection processes, leading to better hiring decisions and improved organizational performance. Future research should expand sample sizes to include diverse industries and roles and conduct longitudinal studies for deeper insights into long-term impacts. Integrating advanced data analytics and machine learning could further optimize selection processes and improve predictive accuracy.

REFERENCES

Archer, J. (2008). *The Behavioral Assessment of Human Resources.* New York: Springer.

Barrick, M. R. & M. K. **Mount** (1991). The Big Five personality dimensions and job performance: A meta-analysis. *Personnel Psychology, 44(1),* 1–26.

Jansen, P. G. & C. J. **Vinkenburg** (2006). The effect of stress interviews on interview anxiety, applicant reactions, and interviewer ratings. *Journal of Applied Psychology, 91(3),* 444–454.

Lievens, F. & F. **Patterson** (2011). The use of situational judgment tests in selection and assessment. *International Journal of Selection and Assessment, 19(1),* 65–73.

Ones, D. S., C. **Viswesvaran** & F. L. **Schmidt** (1993). Comprehensive meta-analysis of integrity test validities: Findings and implications for personnel selection and theories of job performance. *Journal of Applied Psychology, 78(4),* 679–703.

Schmidt, F. L. & J. E. **Hunter** (1998). The validity and utility of selection methods in personnel psychology: Practical and theoretical implications of 85 years of research findings. *Psychological Bulletin, 124(2),* 262–274.

ПОДОБРЯВАНЕ НА ПОДБОРА НА РЪКОВОДНИ КАДРИ: ВЛИЯНИЕТО НА СЪДЕБНАТА ПСИХОЛОГИЯ ВЪРХУ ПРЕДСКАЗВАЩАТА ВАЛИДНОСТ И ОРГАНИЗАЦИОННАТА ПРИГОДНОСТ

Резюме: *Интегрирането на принципите на съдебната психология в практиките в областта на човешките ресурси (ЧР) значително подобрява съвременното набиране на персонал особено при подбора на ръководни кадри. В настоящото изследване е разработен изследователски модел за оценка на въздействието на тези подходи. Чрез използване на техники като тестове за надеждност, тестове за преценка на ситуацията и поведенчески интервюта проучването изследва техния потенциал за подобряване на прогностичната надеждност и организационната*

пригодност. Методологията включва количествени и качествени анализи, като са проведени проучвания сред специалисти по човешки ресурси, кандидати за работа на ръководни длъжности и наети ръководители. Проучването изказва хипотезата, че криминално-психологическите принципи повишават прогностичната валидност за изпълнението на длъжността и намаляват риска от неправилно наемане на работа. Ключовите променливи включват ефективността на тези техники и тяхната корелация с изпълнението на работата, организационната пригодност и задържането на служителите. Резултатите сочат, че тестовете за преценка на ситуацията и за надеждност ефективно оценяват качествата на кандидатите, докато техники като техниката за интервю за съдебна оценка и интервютата за стрес създават предразсъдъци и негативен опит за кандидатите. Проучването подчертава необходимостта от подходящ избор на техники, задълбочено обучение на специалистите по човешки ресурси и етично прилагане. Изследването стига до заключението, че интегрирането на криминално-психологическите принципи може да подобри подбора на ръководни кадри чрез повишаване на точността на наемане и културното съответствие.

Ключови думи: *съдебна психология, подбор на ръководни кадри, оценка на кандидатите*

Лукас ван Ленгерих, докторант
Университет по библиотекознание и информационни технологии
E-mail: lukas.vanlengerich@live.ca

ОБЩЕСТВЕНИ КОМУНИКАЦИИ И ИНФОРМАЦИОННИ НАУКИ
PUBLIC COMMUNICATIONS AND INFORMATION SCIENCES

INPUT DEVELOPMENT FOR PROCESS CREATION FOR SUSTAINABLE INDUSTRIAL BUILDINGS

Nicole Sertorelli
University of Library Studies and Information Technologies

Abstract: *An analysis of the necessary input for the development of a sustainability strategy for global industrial construction projects of international automotive supplier from Germany will be carried out. In a first step, an analysis of internal and external stakeholders of the automotive supplier groups and their assessment of their relevance for the construction project will be carried out, considering the Group's sustainability strategy. In a second step, boundary conditions to be observed are analyzed, which apply both in Germany and abroad, and boundary conditions that must be taken into account especially for construction projects abroad. In a third step, the basic sustainability strategy for each construction project must be decided, in which the findings from the previous steps are incorporated. The aim of this process recommendation is to recommend action for companies in the automotive supplier industry to consider all relevant stakeholders and specific boundary conditions in the development of sustainable industrial buildings and to eliminate problems at an early stage of the project or to reduce them to a minimum.*
Keywords: *stakeholder, sustainability, industrial buildings, input*

INTRODUCTION

Global automotive suppliers place high demands on themselves and their suppliers in order to make a comprehensive contribution to sustainability. An important area that has a major influence on environmental and socially relevant criteria is the construction of new production properties.

Numerous national and international assessment and certification systems exist worldwide to prove that buildings comply with certain sustainability aspects and criteria. These assessment and certification systems are designed for specific building types and do not consider the specific requirements for automotive suppliers' production facilities or their Group's own cross-divisional sustainability strategies.

Based on a study in which the conformity of existing international sustainability certificates with the requirements for sustainability aspects of an automotive supplier was evaluated, the assessment and certification system DGNB (German Sustainable Building Council) is used as the basis for a concept of measures and evaluation for the implementation of new construction projects of sustainable production facilities of automotive suppliers.

The main arguments in favor of a Group's own sustainability action concept for its new production facility projects are that the Group's sustainability goals can be comprehensively taken into account, that the production facilities of an automotive supplier maintain comparable qualities worldwide, and that evaluation criteria can be adapted to local conditions.

RESEARCH METHODOLOGY

To create your own sustainability action concept, the relevant input must first be determined.

Of particular importance for determining the input is the knowledge of the relevant stakeholder groups for the Group's own construction projects. In a first step, all of the Group's stakeholders are examined

for their relevance for construction projects of automotive supplier production facilities. The stakeholder groups are internal and external groups or individuals who can affect or is affected by the achievement of the organization's objectives (Freeman 2010, p. 46). A stakeholder group analysis is therefore intended to investigate which stakeholder groups are important for the implementation of construction measures and in what form they should be involved in the further procedural steps.

Based on a relevance matrix from Müller-Stewens, which maps the influence on the own group and the influenceability of the stakeholder groups itself, and a materiality matrix from Lohrie, which determines the characteristics relevance of the stakeholder group and co-shaping competence, an own matrix is applied. The characteristics of power, conflict potential and interest are recorded. Power defines the means and possibilities of a stakeholder group to achieve or prevent successful implementation. The potential for conflict describes whether a stakeholder group is fundamentally positive or negative about the goals of the construction project. Interest represents the degree of participation of a stakeholder group in the construction project. The stakeholder groups (SG) can thus be located in 8 areas.

SG 1: high power, high potential for conflict, high interest.
SG 2: high power, increased potential for conflict, less interested.
SG 3: high power, low potential for conflict, high interest.
SG 4: high power, low potential for conflict, low interest.
SG 5: low power, increased potential for conflict, high interest.
SG 6: low power, increased potential for conflict, low interest.
SG 7: low power, low potential for conflict, high interest.
SG 8: neither power, conflict potentials or interest.

To form the rankings within the three attributes power, conflict potential and interest, an ordinal scale with a value spectrum (x) from 0 to 1 is used. 0 corresponds to weakly and 1 to a strong expression. The results are evaluated by determining the median. Intermediate values, as they would result from the calculation of the arithmetic mean, are not required. Due to the expected small size of the sample, the median is less susceptible to fluctuations. The modal value is not appropriate, since in the case of the topic of sustainable construction, which is subject to strong social discussions, the formation of two opposing but almost equally strong "opinion groups" would be conceivable, which would result in the complete embezzlement of the slightly weaker opinion group.

Thus, the following formula results for determining the median of the three attributes to be examined:

Formula 1: Calculation of the median

$$\overline{X}_{med,attribut} = X_{\left(\frac{n+1}{2}\right)} \quad (1)$$

Based on the stakeholder group analysis, the relevant special features of the construction measures are systematically recorded below. This includes the requirements from the analyzed stakeholder groups, and aspects that are independent of them, such as the site characteristics, the construction method or environmental influences. The phase is supplemented by the development of a sustainability strategy. It serves to provide a uniform understanding of the topic of "sustainable building" and to prioritize existing sustainability goals.

In the following, the three procedural steps mentioned above, which generate the necessary input for the further procedure, are described in detail and serve as a basis for the development of further procedural steps.

RESULTS

STAKEHOLDER GROUPS

Different stakeholder groups with different goals have an influence on the implementation of construction measures. Knowledge of relevant internal and external stakeholder groups is important for the success of construction projects. Internal stakeholder groups include a company's internal circle of management and employees, who can act as builders, owners, users, or operators. This group represents a stable constant, whereas external stakeholder groups can be very different and their influence can change,

which is why this group must be reviewed constantly and during the project. The external stakeholder groups include, among others, suppliers, competitors, media, trade unions, customers, etc.

In construction projects, the analysis, evaluation and participation of relevant stakeholder groups are used to try to prevent conflicts or minimise them as far as possible at an early stage. With the consistent involvement of all stakeholder groups is expected not only to consider corporate goals that have been defined in terms of sustainability and are pursued in the form of sustainability reporting, but also to develop new objectives and correct irrelevant ones.

A fictitious construction project for the construction of a new production facility was analyzed. In this context, the project sponsor was assessed as a C stakeholder group, as it has a high level of power and interest in the construction project. His potential for conflict, on the other hand, is to be assessed as low, as he formulated the need for this construction measure himself together with the user. The responsible building administration was classified in the same way. The Supervisory Board was assessed as an A stakeholder group because it has a high level of power and interest, but at the same time there may also be potential for conflict resulting from the financing of the construction project. The user was assessed as a G stakeholder group. He has a great interest, as he uses the building after completion, but his power is limited. The potential for conflict is generally low, since he has defined the basic need himself in the context of his needs assessment.

SYSTEMATIC RECORDING OF THE SPECIAL FEATURES

The special features of construction measures in Germany and abroad have a significant influence on the process of holistic sustainability integration. The implementation of defined sustainability goals is much more difficult for construction projects abroad, as construction requirements cannot be defined uniformly, and each country has individual differences. A detailed consideration of characteristics is therefore necessary. All the special features of industrial construction measures in Germany also apply to construction measures abroad, but not all the special features of construction measures abroad apply to domestic construction measures. Therefore, it is crucial that a systematic and as complete as possible recording of all special features of the construction measures should be investigated.

COMMON FEATURES OF INDUSTRIAL CONSTRUCTION PROJECTS AT HOME AND ABROAD

Laws: The consideration of all applicable laws is a basis for all projects in general and thus also for the process for holistic sustainability integration in particular. All applicable laws must be identified at the higher level and their influence on the objectives of the construction project must be described.

Stakeholder groups: Special features that result from special requirements of the relevant stakeholder groups, for example on the basis of the objectives of internal regulations, guidelines or standards. The consideration of special features can lead to certain qualities of a construction project being restricted or even completely excluded. Stakeholder groups can also make requirements that have to be included in the procedure as additional objectives.

Type of use: Different types of use usually also have different requirements for the individual aspects of sustainable construction.

The location of a construction project is of fundamental importance, as it exerts an influence on all achievable qualities. Especially abroad, the exact evaluation of the location is important, as there are always structural requirements that must be implemented.

Technology and building materials: In less developed regions, there may be a shortage of necessary technologies and building materials, which means that certain qualities are not achieved.

ADDITIONAL SPECIAL FEATURES FOR CONSTRUCTION PROJECTS ABROAD

Data: To prove compliance with the required qualities, a sufficient data basis is necessary. Without this data, neither the planning can be meaningfully optimized regarding the sustainability of the construction project, nor can transparent final documentation and evaluation be carried out.

Construction method: In the case of construction measures, if the availability of necessary

technologies, building materials and data is limited, it must be determined whether the construction project is to be carried out with local funds or whether these are to be imported in part or in full from third countries. A change in the construction method results in a fundamental change in the achievable qualities.

Skilled personnel: To achieve the required qualities, the availability of the necessary specialist personnel is usually required. However, this is not always available for construction work abroad. The availability of specialist personnel must also be observed during the use phase to ensure that any maintenance measures are carried out with local personnel if possible.

Environmental influences: Depending on the location, there can be very different environmental conditions. These include climatic conditions, forces of nature and influences from the existing environment. These environmental characteristics should always be discussed, as they have an influence on the structural requirements and qualities of a building.

Culture, society, and religion: These peculiarities occur primarily in construction projects abroad.

The special features described represent a general selection, which must always be checked on a project-specific basis. The early recognition of the special features of a construction project is of great importance, as this has an influence on all further procedural steps. The systematic recording of the characteristics described must always be reviewed on a project-by-project basis and adjusted if necessary.

DEVELOPING A SUSTAINABILITY STRATEGY

In addition to above mentioned analysis of the stakeholder groups and all special features, the definition of the strategic orientation of a construction project forms the basis for its sustainable development.

In the first step, all strategic sustainability goals of the construction project are identified by the relevant stakeholder groups. In the project development phase, the project promoters and users per se represent relevant stakeholder groups. It is possible to add other stakeholder groups and is to be carried out on a project-specific basis.

In the second step, concepts and measures are developed to implement the strategic sustainability goals. Similar measures can be combined into packages of measures. Only packages of measures that have a significant influence on the implementation of the Sustainable Development Goals are taken into account. The categories of measures form the object system, the utility analysis to be carried out in the third step. The target system for the utility analysis is formed by the protected goods of sustainable construction: ecology, economy and socio-cultural aspects. The protected assets are weighted by the stakeholders involved on a project-specific basis, considering their relevance. In a utility value analysis, the interactions between sustainability goals, suitable measures (packages) and protected goods of sustainable construction are then evaluated.

In the fourth step, the strategic sustainability goals are prioritized on the basis of the utility analysis. Only prioritizing the sustainability goals is not expedient.

In the fifth step, the sustainability strategy is composed of clearly defined main goals and secondary goals, which are positively influenced by the implementation of the main goal. With compensating and supplementary measures, an optimal sustainability profile is developed for the construction project. A comparison can be made at the quantitative level using the interactions already identified. Finally, a preferred combination is defined as the decisive sustainability strategy.

In the sixth step, concrete specifications and tools for the planning of the respective construction measure can be derived from the defined sustainability strategy.

CONCLUSION

By analyzing the necessary input, a common understanding of the required sustainability in construction projects is created at an early stage in companies in the automotive supply industry, thus developing processes and recommendations for action that include structured, content-related, and realistically implementable goals in the user's requirements planning. The focus of the analysis is not on quantitative results, but on qualitative interpretations and use of the information to prioritize and harmonize the sustainable development goals. This contributes to the development of sustainable industrial buildings by eliminating or minimizing problems in early project phases. This allows the focus to be placed on

achieving the sustainability goals at the development stage.

REFERENCES

Freeman, E. R., J. P. **Harrison,** A. C. **Wicks,** B. L. **Parmar,** S. **De Colle** (2010). *Stakeholder Theory – The state of the art.* New York: Cambridge University Press.

РАЗРАБОТВАНЕ НА ВХОДНИ ДАННИ ЗА СЪЗДАВАНЕ НА ПРОЦЕСИ ЗА УСТОЙЧИВИ ПРОМИШЛЕНИ СГРАДИ

Резюме: *Ще бъде извършен анализ на необходимия принос за разработване на стратегия за устойчивост на глобални индустриални строителни проекти на международен автомобилен доставчик от Германия. В първата стъпка ще бъде извършен анализ на вътрешните и външните заинтересовани страни от групите доставчици на автомобили и тяхната оценка на значимостта им за строителния проект, като се вземе предвид стратегията за устойчивост на групата. На втора стъпка се анализират граничните условия, които трябва да се спазват и които се прилагат както в Германия, така и в чужбина, както и граничните условия, които трябва да се вземат предвид особено за строителни проекти в чужбина. На трета стъпка трябва да се определи основната стратегия за устойчивост за всеки строителен проект, в която да бъдат включени констатациите от предишните стъпки. Целта на тази насока на процеса е да се препоръчат действия за дружествата в сектора на доставчиците на автомобили, за да вземат предвид всички съответни заинтересовани страни и специфични гранични условия при разработването на устойчиви промишлени сгради и да премахнат проблемите на ранен етап от проекта или да ги сведат до минимум.*

Ключови думи: *заинтересована страна, устойчивост, промишлени сгради, вложени ресурси*

Никол Серторели, докторант
Университет по библиотекознание и информационни технологии
E-mail: nsertorelli@hotmail.com

ОБЩЕСТВЕНИ КОМУНИКАЦИИ И ИНФОРМАЦИОННИ НАУКИ
PUBLIC COMMUNICATIONS AND INFORMATION SCIENCES

THE THEORETICAL MODEL OF INTERNAL CONTROL

Philipp Hoffmeister
University of Library Studies and Information Technologies

Abstract: *Internal control is a process designed to ensure that the corporate objectives defined by top management are achieved. The main objectives are to increase the effectiveness and efficiency of business processes, ensure the reliability of internal and external financial and non-financial reporting, and comply with applicable laws and regulations. Internal control can also be analysed theoretically, in addition to its practical application. The purpose of this article is to analyse the theoretical model of internal control. According to studies, this model consists of three levels: functional, institutional, and instrumental level, which are substantiated by internal control frameworks such as the COSO Internal Control Framework. This article elaborates on these three levels and their relation to internal control. Future work should follow on from this and, for example, extend the theoretical foundation of the construction model of internal control with macro-theories or analyse the model against the background of current internal control legislation.*
Keywords: *Internal Control, management control, risk management, Levers of Control Framework, Three Lines of Defence, COSO Internal Control Framework*

INTRODUCTION

"Internal Control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance" (COSO 2013, 3). This is the definition of internal control according to the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Internal control refers to the principles, procedures, and measures introduced by management in a company to ensure the organizational implementation of management decisions (cf. Bungartz 2020, 23). The objective is to enhance the efficiency and effectiveness of business processes, ensure the reliability of internal and external financial and non-financial reporting, and comply with applicable laws and regulations (cf. COSO 2013, 3). The term and concept of internal control originated from a strongly focused perspective on accounting. Since the early 1990s, internal control has developed towards a broader governance perspective that encompasses the entire organization, rather than solely focusing on accounting (cf. Maijoor 2000, 105). Internal control can be understood as a conceptual model in terms of model theory, which includes the relevant basic thematic concepts and their interrelationships (cf. Hunziker 2015, 29; Amshoff 1993, 77f; Harbert 1982, 140f). The basic concept of internal control is a theoretical construct with corresponding boundaries and delimitations, based on interrelationships (cf. Hunziker 2015, 29; Hahn/Hungenberg 2001, 266). This article analyses the conceptual levels of internal control from a theoretical perspective, using a theoretical model. Subsequently, this article will categorise tasks and functions as internal control from a theoretical model perspective and differentiate them from other aspects. The conclusion will summarise the key findings and provide an outlook for future research.

RESEARCH METHODOLOGY

When establishing concepts in business administration, it is recommended to use a multidimensional subdivision of the scientific construction model. This includes a functional, institutional, and instrumental

level (cf. Winter 2008, 7f; Becker 1990, 300, 313). The following figure illustrates the three model-theoretical levels in a sequential order and provides definitions for each level of the model (adapted from Hunziker 2015, 29; Ossadnik et al. 2010, 18ff; Wall 1999, 18f):

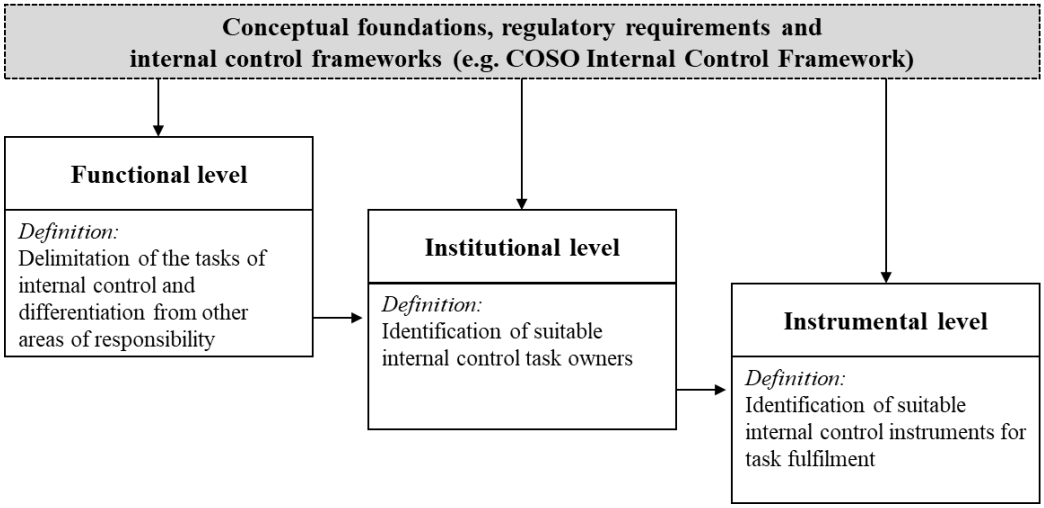


Fig. 1. The theoretical model of internal control

The following section analyses the three model-theoretical levels of internal control and provides a comprehensive scientific-theoretical view of internal control.

RESULTS

The internal control's functional level comprises the tasks of internal control. To fully comprehend these tasks, it is recommended to briefly examine the history of internal control. In both research and practice, internal control has traditionally been closely linked to accounting, resulting in a focus on this area for an extended period. Since the early 2000s, the importance of internal control has been steadily increasing (cf. Hunziker 2015, 50). This is due to the fact that internal control is now part of the audit subject matter for auditors, leading to an increase in audits (cf. Hunziker 2015, 50; Holm/Laursen 2007, 323; Power 1997, 67, 83). This led to the so-called "audit explosion" (Maijoor 2000, 101). However, internal control has evolved from a narrow focus on accounting to a more comprehensive approach (cf. Maijoor 2000, 105). This process is driven by dynamic technological developments and competitive pressures in a networked business world (cf. Stringer/Carey 2002, 62f). The construct of internal control has been expanded by modern management approaches. Frameworks for internal control, such as the COSO Internal Control Framework, have been published and some have become a quasi-standard in the corporate world (cf. Hunziker 2015, 50f). Furthermore, the significance of internal control has grown due to regulatory concretisation and tightening (cf. Hunziker 2015, 51). The responsibilities of internal control are described similarly in academic literature, although slight differences between the narrower, more traditional perspective and the broader organizational theory perspective can still be observed (cf. Hunziker 2015, 51; Sommer 2010, 20f). The tasks of internal control are essentially based on the definition provided by the COSO Internal Control Framework (cf. Hunziker 2015, 52). The following figure shows the organisational theory tasks of internal control (adapted from Hunziker 2015, 52; COSO 2013, 3):

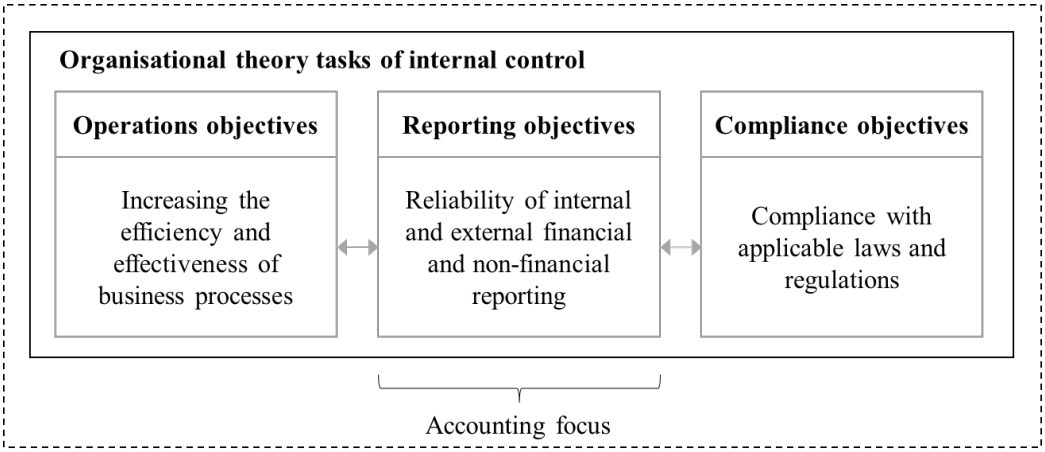


Fig. 2. The tasks of internal control

Corporate governance, management control and risk management are terms that are often mentioned in the context of internal control, but they are thematically and definitionally distinct from it (cf. Hunziker 2015, 66).

There is no generally recognised and uniform definition of corporate governance (cf. Lentfer 2005, 27). The question of a definition can be answered by looking at the core elements of corporate governance: Corporate management and monitoring that is orientated towards the value of the company, exercised by the administrative bodies (internal corporate governance) and by the markets, especially the (equity) capital market, on the basis of reliable corporate reporting (cf. Weber 2011, 29). When examining the various definitions of corporate governance, it is essential to consider the two terms 'corporate management' and 'corporate monitoring' (cf. Weber 2011, 23). Corporate governance represents a system for managing and monitoring companies (cf. Committee on the Financial Aspects of Corporate Governance 1992, numeral 2.5), which enables the recognition of the relationship to internal control (cf. Hunziker 2015, 67). In the context of corporate governance, internal control is considered as central mechanism for monitoring companies (cf. Rae/Subramaniam 2008, 106; Erfurt 2004, 53ff).

Management control is a term that lacks a clear and universal definition, too (cf. Hunziker 2015, 71). Instead, there are various definitions and concepts of management control that are relatively similar and coexist (cf. Strauß/Zecher 2013, 234; Berry et al. 2009, 2f). Many authors conclude that the two concepts are very similar in terms of content and definition, as they are both mechanisms for allocating resources and achieving objectives (cf. Fadzil et al. 2005, 846; Merchant/Otley 2007, 787). Other authors define internal control as either a concept (cf. Rikhardsson et al. 2005, 13f) or an element of management control (cf. Soltani 2007, 302f). Hunziker compares and contrasts these perspectives, concluding that they are interdependent due to their shared aim of directing employee behaviour in line with the company's objectives. Furthermore, while they are not involved in the management decision-making process, they do monitor the achievement of objectives and therefore have an indirect influence (cf. Hunziker 2015, 76). However, there are differences between them, as management control is more focused on influencing decision-making, while internal control tends to support it. Management control is more oriented towards strategy, while internal control is more transaction-oriented. Finally, it is worth noting that management control tends to focus on behaviour, while internal control is more mechanistic (cf. Hunziker 2015, 76f; Vaassen et al. 2009, 70).

According to the modern view, risk management is understood as a holistic approach with a strategic focus. This is known as enterprise risk management (cf. Hoyt/Liebenberg 2011, 795). Risks typically arise from a company's objectives, management processes, and business processes. Risk management aims to control all resulting risks (cf. Hahn 1987, 137ff). This involves identifying, assessing, and controlling individual risks, as well as understanding the interdependencies and effects of these risks on each other. It also includes controlling the overall aggregated risk of the company (cf. Gleißner 2004, 350f, 357f; Romeike/Hager 2020, 87f, 121f, 130; Gleißner 2001, 111, 125f). Additionally, the holistic approach to risk management takes into account non-quantifiable risks (cf. Mikes 2009, 25) and the risk/reward ratio

(cf. Farny 1979, 17, 19ff). It guides the company's risk policy and promotes a healthy risk awareness among employees (cf. Rogler 2002, 19ff; Hahn 1987, 139ff). The comparison between risk management and internal control reveals both differences and similarities. Risk management is more strongly oriented towards the company's strategy: it defines the risk policy with risk preferences, examines risk potential, evaluates and manages risks within the framework of the company's individual risk portfolio, and aggregates individual risks at the overall company level. These tasks are not typically included in internal control as strategic risks are generally not managed at the operational business process level. Instead, they usually arise from the corporate environment, which can be complex and difficult to capture through control mechanisms (cf. Hunziker 2015, 84). Internal control primarily manages individual operational risks (cf. Arwinge 2013, 85f; Schartmann/Lindner 2006, 43), while assisting risk management in managing individual operational risks (cf. Schmid/Stebler 2007, 643f). Risk management focuses on both internal and external strategic risks, while internal control focuses on internal risks with a strong process orientation (cf. Hunziker 2015, 85; Arwinge 2013, 88f; Reichert 2009, 28; Ruud/Jenal 2005, 459).

It is difficult to distinguish internal control from management control and risk management due to the absence of universally accepted definitions. In addition to the demarcation, there are overlaps, conditional and complementary connections between the three disciplines (cf. Arwinge 2013, 80f; Power 2007, 60ff; Spira/Page 2003, 651f; Kinney 2000, 83). These connections merge into what is known as the 'control mix' of the company (cf. Hunziker 2015, 87, based on Mikes 2009, 23). Winter (2008, 9) and Chmielewicz (1994, 18ff) recommend that authors choose their approach depending on the research purpose and objective of their studies and publications when engaging in a scientific-theoretical examination of the three subject areas.

The distribution of tasks to internal control task owners constitutes the institutional level of internal control (cf. Hampel et al. 2012, 204). The Three Lines of Defence model (TLoD model) is considered a comprehensive and widely applicable institutional framework and best practice approach for organizing a company's control (cf. Hunziker 2015, 52; Ruud/Kyburz 2014, 761; Eulerich 2012, 55). Particularly in the financial and banking sector (cf. Welge/Eulerich 2014, 60). The TLoD model includes duty bearers and bodies within the internal control and monitoring system, as well as their interfaces (cf. Eulerich 2012, 55ff). It describes the competences and responsibilities of task owners in monitoring for effective and efficient internal control and risk management within the company context (cf. Hampel et al. 2012, 204). The TLoD model is presented below (adapted from Bungartz 2020, 572; Wullenkord/Rapp 2019, 179; Welge/Eulerich 2014, 61; Hunziker 2015, 53):

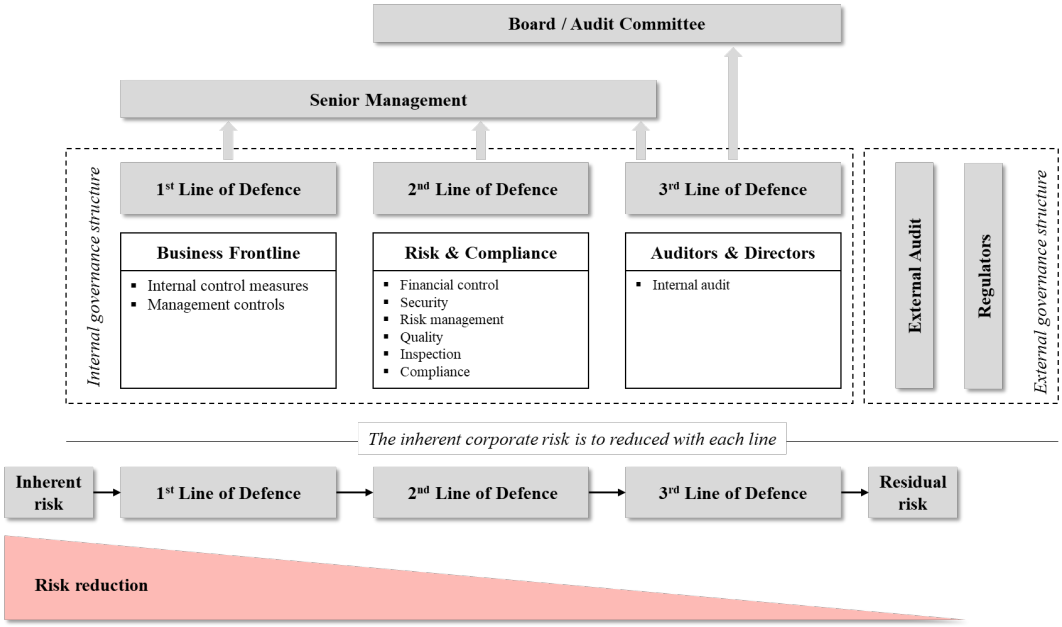


Fig. 3. The Three Lines of Defence model

The first line of defence in the TLoD model consists of conventional controls that are implemented in the operating units. These controls are the responsibility of middle management or the respective specialist departments as risk owners. Their purpose is to mitigate the company's risks at the first level (cf. Wullenkord/Rapp 2019, 179; Schiel 2014, 130; Welge/Eulerich 2014, 61). Regarding internal control, middle management is responsible for the processes and tasks of the operating units. It creates the conditions for effective risk management in the respective units (cf. Wullenkord/Rapp 2019, 179). Middle management identifies, assesses, manages, and monitors these risks on an ongoing basis, contributing to the quality of internal control (cf. Schiel 2014, 130; Lück 1991, 23ff). Therefore, the first line of defence is the foundation of internal control (cf. Eulerich 2012, 56).

The second line of defence regulates and monitors operational controls. This is carried out by various functional units within the company: controlling, risk management, compliance unit, quality management and IT security, but also by human resources and plant security (cf. Welge/Eulerich 2014, 62). The second line of defence units assist middle management or risk owners in implementing effective and efficient risk control structures. They shape the company's risk strategy and policy, create guidelines and directives for risk management, aggregate the control results from the first line of defence, prepare reports for top management and other supervisory bodies, and initiate risk reduction measures if necessary (cf. Wullenkord/Rapp 2019, 179; Schiel 2014, 130; Welge/Eulerich 2014, 62). Here, we can see an interlocking of the two levels (cf. Kreipl 2020, 91; Ruud/Kyburz 2014, 762), which reduces the overall risks of the company once again (cf. Kreipl 2020, 89).

The third line of defence consists of internal audit. It assesses the effectiveness and efficiency of the first two lines of defence (cf. Kreipl 2020, 91). It specifically assesses the suitability, regularity, efficiency, and expediency of the organizational and operational structures of the first and second lines of defence (cf. Wullenkord/Rapp 2019, 179f). Internal audit plays a crucial role in identifying weaknesses in the control system, creating benchmarks, and promoting good corporate practices overall (cf. Kreipl 2020, 91). It serves as an essential interface between the units and bodies of the TLoD (cf. Eulerich 2012, 57f) and occupies a significant position within the TLoD model (cf. Welge/Eulerich 2014, 60). Its role in supporting the achievement of corporate objectives is to systematically analyse and evaluate the effectiveness of internal control within the company (cf. Palazzesi/Pfyffer 2004, 7ff; Meyer et al. 2005, 31f). Internal audit serves as the third line of defence, reducing any remaining risk and detecting any previously undetected risks by the first two lines of defence (cf. Welge/Eulerich 2014, 62).

The internal control's instrumental level includes the mechanisms that a company employs to ensure that its employees implement the strategy defined by top management and achieve the company's objectives (cf. Merchant/van der Stede 2017, 9, 11). This level is linked to internal control, which should also contribute to achieving the overarching objectives (cf. Hunziker 2015, 62; Bungartz 2020, 56; CoCo 1995, 4). As with the two model-theoretical levels of internal control mentioned earlier, there is no universally accepted definition of the control mechanisms and their content (cf. Morris et al. 2006, 474). Instead, there is a wide range of definitions, designs, and attempts at categorization: Direct controls, e.g. budget controls (cf. Morris et al. 2006, 482; Bisbe/Otley 2004, 717) and flexible controls, e.g. principle of self-control and social control (cf. Hunziker 2015, 64; Morris et al. 2006, 472f) or formal control mechanisms that reward desired behaviour, e.g. bonus payments, formal control mechanisms that sanction undesired behaviour, e.g. access controls, and informal control mechanisms, e.g. corporate culture (cf. Feichter/Grabner 2020, 151) or results control (incentive and bonus systems), action control (time targets), cultural control (group rewards), and personnel control (recruitment process) (cf. Merchant/van der Stede 2017, 33ff, 86ff, 95ff, 97ff) or directive, preventive, detective, and corrective controls (cf. Ruud/Jenal 2005, 456) are some examples of non-exhaustive measures. Robert Simons' Levers of Control framework is a widely recognised approach to categorising control mechanisms (cf. Reichert 2009, 37). He identifies four control levers: the value system, which includes fundamental norms and goals; boundary systems, which consist of social and technical restrictions; diagnostic systems, which incorporate feedback systems and business plans; and interaction systems, which involve feedback and measurement systems (cf. Eisele/Steinmann 2015, 182f; Tessier/Otley 2012, 178; Mundy 2010, 505; Henri 2006, 533ff; Simons 1995, 33ff, 95f). The Levers of Control framework, with its four control levers, is intended to serve managers as an instrument

for carrying out management and control tasks. To ensure the framework's effectiveness, the four control levers should be used in a balanced and combined manner (cf. Mundy 2010, 502). The diversity and complexity of the control mechanisms can be recognised. The objective is to integrate various control mechanisms within the company, as they are interdependent. For instance, while detective controls identify errors and undesirable events, they alone are insufficient at a holistic level without corrective controls to rectify the situation (cf. Hunziker 2015, 65f; Moeller 2005, 72f).

CONCLUSION

The internal control construction model attempts to theoretically model and depict internal control through its functional, institutional, and instrumental levels. The functional level includes the tasks of internal control, which align with the objectives of the COSO Internal Control Framework: ensuring the effectiveness and efficiency of operational activities, the reliability of reporting, and compliance with laws and standards (cf. Hunziker 2015, 52). Internal control is also delineated at this level: corporate governance is a comprehensive system for managing and monitoring companies. Internal control is a central component of this system. Management control attempts to influence decision-making within the company, while internal control supports the implementation of decisions. Risk management focuses on both internal and external strategic risks, while internal control focuses on internal risks and has a strong process orientation. These two components complement each other. The institutional level of internal control includes the internal control function. The three lines of defence model is particularly important here. The instrumental level of internal control comprises the various control mechanisms in the company that are intended to ensure the implementation of the strategy defined by top management at employee level and the achievement of corporate goals. Future research should utilise macro-theories to expand the theoretical foundation of this internal control construction model for its specific application. Additionally, this scientific-theoretical model should be evaluated in the context of current regulatory requirements for internal control or recognised internal control frameworks used in practice, as both can impact this model. Above all, the empirical validity of this approach is a fundamental consideration.

REFERENCES

Amshoff, B. (1993). *Controlling in deutschen Unternehmungen: Realtypen, Kontext und Effizienz, 2nd edition.* Wiesbaden (Germany): Springer Verlag.

Arwinge, O. (2013). *Internal Control: A Study of Concept and Themes.* Berlin, Heidelberg (Germany): Physica Verlag.

Becker, W. (1990). Funktionsprinzipien des Controlling. *Zeitschrift für Betriebswirtschaft, 60, 3,* 295–318.

Berry, A. J., A. F. **Coad,** E. P. **Harris,** D. **Otley,** C. **Stringer** (2009). Emerging Themes in Management Control: A Review of Recent Literature. *The British Accounting Review, 41, 1,* 2–20.

Bisbe, J., D. **Otley** (2004). The Effects of the Interactive Use of Management Control Systems on Product Innovation. *Accounting, Organizations and Society, 29, 8,* 709–737.

Bungartz, O. (2020). *Handbuch Interne Kontrollsysteme (IKS): Steuerung und Überwachung von Unternehmen, 6th edition.* Berlin (Germany): Erich Schmidt Verlag.

Chmielewicz, K. (1994). *Forschungskonzeptionen der Wirtschaftswissenschaft, 3rd edition*. Stuttgart (Germany): Schäffer-Poeschel Verlag.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013). *Internal Control – Integrated Framework, Executive Summary.* Durham, North Carolina (USA).

Committee on the Financial Aspects of Corporate Governance (1992). *Report of the Committee on the Financial Aspects of Corporate Governance,* pp. 1–91 [viewed 23 July 2024]. Available from:https://www.icaew.com/technical/corporate-governance/codes-and-reports/cadbury-report.

Criteria of Control (CoCo) Board of the Canadian Institute of Chartered Accountants (1995). *Guidance on Control,* pp. 1–32 [viewed 29 July 2024]. Available from: https://de.scribd.com/document/245653921/CoCo-Guidance-on-Control.

Eisele, S., J.-C. **Steinmann** (2015). Das Levers of Control Framework: Der Harvard Business Controlling Ansatz. *Controlling, 27, 3,* 182–184.

Erfurt, R. A. (2004). *Corporate Governance in der Netzökonomie: Auswirkungen der Einbindung in Netzwerke auf die Corporate Governance am Beispiel Schweizer und deutscher Unternehmen.* Berlin (Germany): Buchbinderei Klünder.

Eulerich, M. (2012). Das Three Lines of Defence-Modell: Ein mögliches Rahmenwerk für die Positionierung der Internen Revision. *Zeitschrift Interne Revision, 47, 2,* 55–58.

Fadzil, F. H., H. **Haron,** M. **Jantan** (2005). Internal Auditing Practices and Internal Control System. *Managerial Auditing Journal, 20, 8,* 844–866.

Farny, D. (1979). Grundfragen des Risk Management (pp. 11–37). In: *Risk-Management – Strategien zur Risikobeherrschung: Bericht von der 5. Kölner BFuP-Tagung am 5. und 6. Oktober 1978 in Leverkusen.* Goetzke, W., H. D. Bürgel, G. Sieben. Cologne (Germany): GEBRA.
Feichter, C., I. **Grabner** (2020). Empirische Forschung zu Management Control: Ein Überblick und neue Trends. *Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung, 72, 2,* 149–181.
Gleißner, W. (2001). Identifikation, Messung und Aggregation von Risiken (pp. 111–137). In: *Wertorientiertes Risiko-Management für Industrie und Handel: Methoden, Fallbeispiele, Checklisten.* Gleißner, W., G. Meier. Wiesbaden (Germany): Gabler Verlag.
Gleißner, W. (2004). Die Aggregation von Risiken im Kontext der Unternehmensplanung. *Zeitschrift für Controlling & Management, 48, 5,* 350–359.
Hahn, D. (1987). Risiko-Management: Stand und Entwicklungstendenzen. *Zeitschrift Führung + Organisation, 56, 3,* 137–150.
Hahn, D., H. **Hungenberg** (2001). *PuK: Planung und Kontrolle, Planungs- und Kontrollsysteme, Planungs- und Kontrollrechnung – Wertorientierte Controllingkonzepte, 6th edition.* Wiesbaden (Germany): Gabler Verlag.
Hampel, V., M. **Eulerich,** J. **Theis** (2012). Das Three-Lines-of-Defence-Modell und die Positionierung der Internen Revision innerhalb der Corporate Governance: Konzeptionelle Überlegungen und empirische Ergebnisse für Deutschland. *Zeitschrift für Corporate Governance, 7, 5,* 201–207.
Harbert, L. (1982). *Controlling-Begriffe und Controlling-Konzeptionen: Eine kritische Betrachtung des Entwicklungsstandes des Controlling und Möglichkeiten seiner Fortentwicklung.* Bochum (Germany): Studienverlag Dr. N. Brockmeyer.
Henri, J.-F. (2006). Management Control Systems and Strategy: A Resource-based Perspective. *Accounting, Organizations and Society, 31, 6,* 529–558.
Holm, C., P. B. **Laursen** (2007). Risk and Control Developments in Corporate Governance: Changing the Role of the External Auditor? *Corporate Governance: An International Review, 15, 2,* 322–333.
Hoyt, R. E., A. P. **Liebenberg** (2011). The Value of Enterprise Risk Management. *The Journal of Risk and Insurance, 78, 4,* 795–822.
Hunziker, S. (2015). *Erfolg der Internal Control: Eine empirische Analyse aus Sicht des Managements.* Bamberg (Germany): Difo-Druck.
Kinney, W. R. (2000). Research Opportunities in Internal Control Quality and Quality Assurance. *Auditing: A Journal of Practice & Theory, 19, s-1,* 83–90.
Kreipl, C. (2020). *Verantwortungsvolle Unternehmensführung: Corporate Governance, Compliance Management und Corporate Social Responsibility.* Wiesbaden (Germany): Springer Gabler Verlag.
Lentfer, T. (2005). *Einflüsse der internationalen Corporate Governance-Diskussion auf die Überwachung der Geschäftsführung: Eine kritische Analyse des deutschen Aufsichtsratssystems.* Wiesbaden (Germany): Deutscher Universitäts-Verlag.
Lück, W. (1991). *Wirtschaftsprüfung und Treuhandwesen: Institutionelle und funktionale Aspekte der betriebswirtschaftlichen Prüfungslehre, 2nd edition.* Stuttgart (Germany): Poeschel Verlag.
Maijoor, S. (2000). The Internal Control Explosion. *International Journal of Auditing, 4, 1,* 101–109.
Merchant, K. A., D. **Otley** (2007). A Review of the Literature on Control and Accountability (pp. 785–802). In: *Handbook of Management Accounting Research – Volume 2*. Chapman, C. S., A. G. Hopwood, M. D. Shields. Amsterdam (The Netherlands): Elsevier.
Merchant, K. A., W. A. **van der Stede** (2017). *Management Control Systems: Performance Measurement, Evaluation and Incentives, 4th edition.* Harlow (United Kingdom): Pearson Education.
Meyer, C., D. **Widmer,** J. **Meisterhans** (2005). Interne Kontrolle in der Schweizer Praxis: Eine aktuelle Standortbestimmung. *KPMG Schweiz and University of Zurich, Institut für Rechnungswesen und Controlling,* pp. 1–76 [viewed 09 March 2024]. Available from: https://www.business.uzh.ch/dam/jcr:ffffffff-d7d1-41c2-ffff-ffffb8cf5b81/KPMG_Studie_397869.pdf.
Mikes, A. (2009). Risk Management and Calculative Cultures. *Management Accounting Research, 20, 1,* 18–40.
Moeller, R. (2005). *Brink's Modern Internal Auditing, 6th edition.* Hoboken, New Jersey (USA): John Wiley & Sons.
Morris, M. H., J. **Allen,** M. **Schindehutte,** R. **Avila** (2006). Balanced Management Control Systems as a Mechanism for Achieving Corporate Entrepreneurship. *Journal of Managerial Issues, 18, 4,* 468–493.
Mundy, J. (2010). Creating Dynamic Tensions through a Balanced Use of Management Control Systems. *Accounting, Organizations and Society, 35, 5,* 499–523.
Ossadnik, W., E. **van Lengerich,** D. **Barklage** (2010). *Controlling mittelständischer Unternehmen: Empirischer Status quo und Handlungsempfehlungen.* Heidelberg (Germany): Physica Verlag.
Palazzesi, M., H.-U. **Pfyffer** (2004). Interne Revision und Unternehmensüberwachung – Von der Konkurrenz zur Kooperation: Vielerorts noch großer Handlungsbedarf. *Der Schweizer Treuhänder, 78, 1–2,* 7–16.
Power, M. (1997). *The Audit Society: Rituals of Verification.* New York, New York (USA): Oxford University Press.
Power, M. (2007). *Organized Uncertainty: Designing a World of Risk Management.* New York, New York (USA): Oxford University Press.
Rae, K., N. **Subramaniam** (2008). Quality of Internal Control Procedures: Antecedents and Moderating Effect on Organisational Justice and Employee Fraud. *Managerial Auditing Journal, 23, 2,* 104–124.
Reichert, F. (2009). *Internal Control bei mittelständischen Dienstleistungsgesellschaften: Eine empirische Studie zur Ausgestaltung der COSO-Zielkategorien.* Göttingen (Germany): Cuvillier Verlag.
Rikhardsson, P., C. **Rohde,** A. **Rom** (2005). Exploring Enterprise Systems and Management Control in the Information

Society: Developing a Conceptual Framework, *6th International Research Symposium on Accounting Information Systems, Las Vegas, Nevada (USA),* pp. 1–18 [viewed 29 February 2024]. Available from: https://pure.au.dk/portal/files/14/M-2005-05.
Rogler, S. (2002). *Risikomanagement im Industriebetrieb: Analyse von Beschaffungs-, Produktions- und Absatzrisiken.* Wiesbaden (Germany): Gabler and Deutscher Universitäts-Verlag.
Romeike, F., P. **Hager** (2020). *Erfolgsfaktor Risiko-Management 4.0: Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel, 4th edition.* Wiesbaden (Germany): Springer Gabler Verlag.
Ruud, F., L. **Jenal** (2005). Licht im Internal-Control-Dschungel: Begriffsdefinitionen sind unerlässlich. *Der Schweizer Treuhänder, 79, 6–7,* 455–460.
Ruud, F., A. **Kyburz** (2014). Gedanken zum Three Lines of Defence Modell – Was ist mit Verteidigung gemeint? Analyse des Governance-Modells aus der Sicht des internen Audits. *Der Schweizer Treuhänder, 88, 9,* 761–766.
Schartmann, B., M. **Lindner** (2006). Prüfung des Internen Kontrollsystems (IKS) durch die Interne Revision (IR) (pp. 33-61). In: *Zentrale Tätigkeitsbereiche der Internen Revision: Aktuelle und zukünftige Schwerpunkte erfolgreicher Revisionsarbeit.* Lück, W. Berlin (Germany): Erich Schmidt Verlag.
Schiel, C. (2014). *Management moralischer Risiken in Unternehmen: Mit moderner Risiko Governance Vertrauen schaffen und Wettbewerbsvorteile sichern.* Berlin, Heidelberg (Germany): Springer Gabler Verlag.
Schmid, M., W. **Stebler** (2007). Risikobasiertes Internes Kontrollsystem: Risikoidentifikation von grundlegender Bedeutung. *Der Schweizer Treuhänder, 81, 9,* 642–646.
Simons, R. (1995). *Levers of Control: How Managers Use Innovative Control Systems to Drive Strategic Renewal.* Boston, Massachusetts (USA): Harvard Business School Press.
Soltani, B. (2007). *Auditing: An International Approach.* Harlow (United Kingdom): Financial Times Prentice Hall.
Sommer, K. (2010). *Risikoorientiertes Zusammenwirken der Internal Control, des Risikomanagements, des Internen Audits und der Externen Revision – Theoretische Analyse, konzeptionelle Ansätze und praktische Gestaltung.* Bamberg (Germany): Difo-Druck.
Spira, L. F., M. **Page** (2003). Risk Management: The Reinvention of Internal Control and the Changing Role of Internal Audit. *Accounting, Auditing & Accountability Journal 16, 4,* 640–661.
Strauß, E., C. **Zechner** (2013). Management Control Systems: A Review. *Journal of Management Control, 23, 4,* 233–268.
Stringer, C., P. **Carey** (2002). Internal Control Re-Design: An Exploratory Study of Australian Organisations. *Accounting, Accountability & Performance, 8, 2,* 61–86.
Tessier, S., D. **Otley** (2012). A Conceptual Development of Simons' Levers of Control Framework. *Management Accounting Research, 23, 3,* 171–185.
Vaassen, E., R. **Meuwissen,** C. **Schelleman** (2009). *Accounting Information Systems and Internal Control, 2nd edition.* Chichester (United Kingdom): John Wiley & Sons.
Wall, F. (1999). *Planungs- und Kontrollsysteme: Informationstechnische Perspektiven für das Controlling. Grundlagen – Instrumente – Konzepte.* Wiesbaden (Germany): Gabler Verlag.
Weber, S. C. (2011). *Externes Corporate Governance Reporting börsennotierter Publikumsgesellschaften: Konzeptionelle Vorschläge zur Weiterentwicklung der unternehmerischen Berichterstattung.* Wiesbaden (Germany): Gabler Verlag.
Welge, M. K., M. **Eulerich** (2014). *Corporate-Governance-Management: Theorie und Praxis der guten Unternehmensführung, 2nd edition.* Wiesbaden (Germany): Springer Gabler Verlag.
Winter, P. (2008). "Controlling Conceptions" in Management Accounting and Control Research in German Speaking Countries Revisited: Definition of Citeria for Controlling Conceptions and Theses on Conceptional Management Accounting and Control Research. *Munich Personal RePEc Archive,* pp. 1–33 [viewed 01 March 2024]. Available from: http://mpra.ub.uni-muenchen.de/10503/1/MPRA_paper_10503.pdf.
Wullenkord, A., M. J. **Rapp** (2019). *Unternehmenssteuerung durch den Finanzvorstand (CFO): Praxishandbuch operativer Kernaufgaben, 3rd edition*. Wiesbaden (Germany): Springer Gabler Verlag.

ТЕОРЕТИЧЕН МОДЕЛ НА ВЪТРЕШНИЯ КОНТРОЛ

Резюме: *Вътрешният контрол е процес, предназначен да гарантира постигането на корпоративните цели, определени от висшето ръководство. Основните цели са повишаване на ефективността и ефикасността на бизнес процесите, гарантиране на надеждността на вътрешната и външната финансова и нефинансова отчетност и спазване на приложимите закони и разпоредби. Вътрешният контрол може да бъде анализиран и теоретично, в допълнение към практическото му приложение. Целта на настоящата статия е да се анализира теоретичният модел на вътрешния контрол. Според проучванията този модел се състои от три нива: функционално, институционално и инструментално ниво, които се обосновават*

от рамките на вътрешния контрол, като например Рамката за вътрешен контрол на COSO. В настоящата статия се разглеждат тези три нива и тяхната връзка с вътрешния контрол. Бъдещата работа следва да продължи на тази основа и например да разшири теоретичната основа на модела за изграждане на вътрешен контрол с макро теории или да анализира модела на фона на действащото законодателство в областта на вътрешния контрол.
Ключови думи: *вътрешен контрол, управленски контрол, управление на риска, рамка за контрол, три линии на защита, рамка за вътрешен контрол COSO*

Филип Хофмайстер, докторант
Университет по библиотекознание и информационни технологии
E-mail: p.hoffmeister@t-online.de

ОБЩЕСТВЕНИ КОМУНИКАЦИИ И ИНФОРМАЦИОННИ НАУКИ
SOCIAL COMMUNICATIONS AND INFORMATION SCIENCES

ANALYSIS OF INFORMATION SYSTEMS IN THE INDUSTRIAL CONTEXT

Maximilian Renke
University of Library Studies and Information Technologies

Abstract: *This paper explores the role of information systems like ERP, PLM, CRM, MES, and EAM in driving digital transformation and improving operational efficiency within industrial organizations. The study uses a methodology based on secondary research, including a review of literature, market reports, and industry data, to analyze key system providers and their respective market shares. It identifies key trends in cloud adoption, cross-platform integration, and market fragmentation, offering insights into how these systems impact business operations.*
Key findings highlight the growing adoption of cloud-based solutions, particularly among small and medium-sized enterprises, due to their scalability and cost-saving potential. Cross-platform integration is also becoming essential, with companies like SAP advancing efforts to streamline workflows across different systems. Additionally, the study reveals significant market fragmentation in CRM and MES sectors, creating opportunities for niche players to innovate and cater to specific industries or regional needs.
Keywords: *Digitalization, Cloud, Information Systems, Market Fragmentation*

INTRODUCTION

The paper explores the role of information systems such as ERP, PLM, CRM, MES, and EAM in modern organizations in the industrial context. Focusing on their contribution to digital transformation, operational efficiency, and market competitiveness. By reviewing existing literature, market reports, and industry data, the research provides an analysis of how these systems are evolving within businesses, highlighting key providers and their respective market shares. This comprehensive methodology incorporates both academic research and industry insights, offering a balanced perspective on the growing importance of these systems in enhancing organizational processes.

The study's data collection methods rely on secondary research, using reports from market intelligence providers and academic sources to cross-reference and ensure the reliability of findings. The analysis first examines the overall impact of each system category, followed by specific market data on leading providers. Through a combination of quantitative and qualitative approaches, the research identifies market dynamics and factors that contribute to the dominance of certain players, such as integration capabilities, scalability, and industry-specific features. To guide the research, the following key research questions have been identified:

1. What are the leading systems in each category?
2. What is their market share?

RESEARCH METHODOLOGY

The research methodology applied in this study involves a review and analysis of existing literature, market reports, and industry data to evaluate the role of information systems such as ERP, PLM, CRM, MES, and EAM in modern organizations. This method focuses on the identification of key system providers, their respective market shares, and their influence on organizational processes. The study incorporates both academic research and industry insights to form a balanced view of how these systems

contribute to digital transformation, operational efficiency, and market competitiveness.

Data collection was conducted through secondary research methods, relying on publicly available market research reports, academic publications, and relevant industry sources. These reports include detailed market share analyses and insights into the competitive landscape of enterprise systems. To ensure the credibility of the findings, data from multiple sources, such as IDC, 6sense, and other market intelligence providers, were cross-referenced. By aggregating this information, the study provides an up-to-date overview of system providers, their products, and the industries they serve.

The analysis is structured to first present the general impact of each system category on business operations, followed by specific market data related to key providers. Quantitative data was extracted from various market share reports to build a snapshot of the current standing of major players in each category. This approach allowed the research to identify not only the leading providers but also the factors contributing to their market dominance, such as integration capabilities, scalability, and industry-specific functionalities. The methodology emphasizes both qualitative and quantitative aspects, providing a view of the information systems landscape in the industrial context.

RESULTS

Information systems, such as Enterprise Resource Planning (ERP), Product Lifecycle Management (PLM), Customer Relationship Management (CRM), Manufacturing Execution Systems (MES), and Enterprise Asset Management (EAM), are part to the digital transformation of modern organizations. These systems streamline core business functions like finance, supply chain, human resources, manufacturing, and customer relations by providing integrated platforms that enable data sharing, operational efficiency, and improved decision-making. Leading providers, such as SAP, Oracle, Microsoft Dynamics, and others, offer customizable solutions to meet the specific needs of various industries, enhancing their competitiveness in the global market.

Academically and within the industry, these systems are recognized as drivers of organizational agility and collaboration across departments. ERP systems, for instance, help businesses integrate core operations, improving productivity and lowering costs. Similarly, PLM and CRM systems support innovation and customer-centric strategies, while MES and EAM systems focus on optimizing production and asset utilization. This section presents an analysis of the key systems in each category: ERP, PLM, CRM, MES, and EAM, and their respective market shares. It provides a detailed overview of leading providers in each category, illustrating their influence on the market and the factors contributing to their adoption. By examining these market dynamics, the following analysis sheds light on the competitive landscape and the evolving role of enterprise systems in modern business operations.

ERP

Enterprise Resource Planning (ERP) systems are integrated software platforms designed to manage and streamline an organizations core business processes, such as finance, supply chain, human resources, and manufacturing. By consolidating these processes into a single, unified system, ERPs enable real-time data sharing and improve efficiency, decision-making, and operational performance. ERP systems are highly customizable, allowing organizations to adapt them to their specific industry needs, which makes them popular across sectors like manufacturing, healthcare, and retail (Kumar & van Hillegersberg 2000). Leading ERP solutions include SAP, Oracle, and Microsoft Dynamics, each offering a range of modules to handle diverse business operations.

From an academic perspective, ERP systems are seen as essential tools for fostering organizational integration and improving overall business agility. Research shows that successful ERP implementation can lead to enhanced productivity, reduced costs, and better management of resources (Dezbar & Sulaiman 2009). However, ERP projects are complex and often face challenges related to high implementation costs, user resistance, and the need for significant organizational change (Davenport 1998). As technology evolves, ERP systems are increasingly integrating cloud capabilities, artificial intelligence, and machine learning, making them more accessible and intelligent. The following Table 1 provides an overview of the ERP market in 2023.

Table 1. ERP provider and market share globally (6sense.com 2024)

System	Provider	Market Share 2023
SAP ERP	SAP	9%
Oracle ERP Cloud	Oracle	2%
Microsoft Dynamics	Microsoft	25%
Workday	Workday	17%
Sage ERP	Sage	3%
Other	Other	44%

As displayed in Table 1, in 2023, Microsoft Dynamics emerged as the leading ERP provider, commanding a 25% share of the global market. Its popularity is largely attributed to its seamless integration with other Microsoft products and cloud capabilities, making it a strong choice for businesses of varying sizes. Workday followed closely with a 17% share, benefiting from its focus on human capital management and financial planning, particularly among medium to large enterprises.

SAP ERP, held 9% of the market in 2023. Its comprehensive and customizable suite continues to attract large enterprises, especially in sectors like manufacturing and healthcare. Meanwhile, Oracle ERP Cloud, known for its robust cloud-based solutions, accounted for 2% of the market, reflecting steady adoption despite the overall competition. Sage ERP, with 3%, appeals to small and medium-sized enterprises for its ease of use and affordability. The remaining 44% of the market is shared among various other ERP providers.

PLM

Product Lifecycle Management (PLM) systems are integrated solutions that manage the entire lifecycle of a product, from its initial conception, design, and manufacturing through its end of life, including disposal or recycling. These systems provide a digital framework to streamline product-related processes, allowing for the management of data, resources, and decision-making across various stages. PLM systems enable cross-functional teams to collaborate on product development, improving efficiency, reducing costs, and enhancing innovation capabilities. They support the integration of various software tools, data, and workflows within a unified platform, making them critical for managing complex, multi-disciplinary projects (Stark 2015).

Academically, PLM systems are often viewed as enablers of innovation and sustainability in manufacturing and design. By fostering collaboration across multiple departments and organizations, PLM enhances decision-making processes and improves product quality (Grieves 2006). Furthermore, PLM systems promote sustainability by tracking product data throughout its lifecycle, ensuring compliance with environmental regulations, and optimizing product designs for recyclability and reuse (Sudarsan, Fenves, Sriram & Wang 2005). In doing so, PLM has become a cornerstone in the digital transformation of industries seeking to compete in a global marketplace driven by efficiency, sustainability, and innovation. The following Table 2 presents a snapshot of the competitive landscape of PLM systems by showcasing the market share of key providers.

Table 2. PLM provider and market share globally (Thibaud & Xavier 2021)[a], (Abiresearch 2024)[b]

System	Provider	Market Share 2021
Siemens Teamcenter	Siemens	22%[a]
Dassault Systèmes ENOVIA	Dassault Systèmes	29%[a]
PTC Windchill	PTC	10%[a]
Autodesk Fusion Lifecycle	Autodesk	9%[a]
SAP PLM	SAP	10%[b]
Other	Other	20%

As presented in Table 2, in 2021, Dassault Systèmes ENOVIA claimed the largest share of the global Product Lifecycle Management (PLM) market with 29%, positioning it as a leader, particularly in industries requiring extensive engineering and design collaboration. ENOVIA's integration capabilities and collaboration tools have made it popular across sectors such as aerospace and defense. Following closely, Siemens Teamcenter held a market share of 22%. Known for its capabilities in managing complex product data and digital twins, Siemens Teamcenter has presence in industries like automotive and electronics, contributing to its high adoption rate.

PTC Windchill accounted for 10% of the market in 2021, gaining traction due to its integrated product data management (PDM) features, which are essential for industries like industrial manufacturing. SAP PLM also held a 10% share, leveraging SAP's expertise in enterprise resource planning (ERP) to integrate PLM with broader business processes. Autodesk Fusion Lifecycle captured 9% of the PLM market, known for its cloud-based solutions that appeal to small and medium-sized enterprises (SMEs). The remaining 20% of the market was held by various other providers.

CRM

Customer Relationship Management (CRM) systems are software platforms designed to help businesses manage interactions and relationships with current and potential customers. By integrating data from various touchpoints, such as marketing, sales, and customer service, CRM systems enable organizations to track customer interactions, improve communication, and provide personalized service. These systems are essential for managing the customer lifecycle, helping companies identify sales opportunities, automate marketing efforts, and improve customer retention (Buttle & Maklan 2019).

CRM systems are recognized as key enablers of customer-centric strategies, enhancing both operational efficiency and customer satisfaction. They offer businesses valuable insights into customer behavior through data analysis and reporting, allowing for more informed decision-making (Payne & Frow 2013). Moreover, CRM systems support the integration of customer data across departments, fostering collaboration and ensuring that teams have a comprehensive view of customer needs. As organizations increasingly focus on digital transformation, CRM systems continue to evolve with the incorporation of advanced technologies like artificial intelligence and machine learning, further enhancing their capabilities (Mithas, Krishnan & Fornell 2005). CRM solutions as presented in Table 3 showcase the provider, their systems and market share.

Table 3. CRM provider and market share globally (IDC 2024)

System	Provider	Market Share 2023
Salesforce CRM	Salesforce	22%

Microsoft Dynamics 365 CRM	Microsoft	6%
SAP CRM	SAP	4%
Oracle CX Cloud (CRM)	Oracle	4%
Adobe CRM	Adobe	4%
Other	Other	60%

As showcased in Table 3, in 2023, Salesforce led the global CRM market with a dominant share of 22%. Salesforce has solidified its position as the top CRM provider through its comprehensive platform, offering tools for sales, customer service, marketing, and analytics. Its widespread adoption is attributed to its customization options and scalability, making it suitable for businesses of all sizes across various industries.

Other players include Microsoft Dynamics 365 CRM, which held 6% of the market, known for its integration with other Microsoft products and strong appeal in enterprise settings. SAP CRM, Oracle CX Cloud, and Adobe CRM each captured 4% of the market, catering to specific business needs with their CRM offerings, such as ERP integration for SAP and marketing-focused solutions for Adobe. The remaining 60% of the market consists of various smaller CRM providers, highlighting the fragmented nature of the CRM landscape, where niche and specialized solutions continue to play a significant role.

MES

Manufacturing Execution Systems (MES) are software solutions designed to monitor, track, and control production processes on the shop floor in real-time. MES systems help bridge the gap between Enterprise Resource Planning (ERP) systems and the physical manufacturing processes by capturing real-time data from equipment, machines, and workers. By doing so, MES enhances production efficiency, quality control, and regulatory compliance, giving manufacturers better insight into production schedules, material usage, and labour management (MESA International 2016). Common features of MES include production tracking, order management, machine monitoring, and performance analysis, enabling manufacturers to optimize their production workflows and make informed decisions based on real-time data (Jansen-Vullers 2006).

In research, MES are crucial for the development of smart manufacturing within the context of Industry 4.0. MES solutions help bridge the gap between Enterprise Resource Planning (ERP) systems and physical production processes by providing real-time monitoring and control of manufacturing operations. This is achieved through the integration of technologies such as the Internet of Things, big data, and artificial intelligence, which improve decision-making, operational efficiency, and overall responsiveness (Kusiak 2018). By leveraging these technologies, MES enables manufacturers to track production data, optimize equipment usage, and enhance predictive maintenance capabilities. MES solutions as gathered in the following Table 4 showcase the provider, their systems and market share.

Table 4. MES provider and market share globally (6sense II 2024)

System	**Provider**	**Market Share**
Wonderware	AVEVA	44%
Fishbowl Inventory	Fishbowl	8%
SAP Manufacturing Integration	SAP	15%
Siemens SIMATIC IT	Siemens	1%
Other	Other	32%

Following Table 4, the current market for MES, Wonderware, provided by AVEVA, holds the largest

market share at 44%, making it a dominant player. Wonderware's popularity stems from its capabilities in process management and integration with other industrial systems, which has earned it widespread adoption across various industries. Following Wonderware, SAP Manufacturing Integration takes another portion of the market with a 15% share. SAP's solution is known for its strong integration with other enterprise systems, particularly its ERP offerings, making it a preferred choice for large-scale manufacturers who require seamless integration across their business processes.

Fishbowl Inventory captures 8% of the market, mainly serving small to medium-sized businesses with its inventory management and manufacturing control capabilities. Its user-friendly design and affordability make it attractive for companies that don't require the robust features of more complex MES solutions. On the lower end of the market, Siemens SIMATIC IT holds only 1% of the market share. Despite Siemens being a leader in automation technology, its SIMATIC IT MES product is niche, selected for specific high-precision manufacturing applications. The remaining 32% of the market is comprised of various other MES providers.

EAM

Enterprise Asset Management (EAM) systems are comprehensive platforms that help organizations manage the entire lifecycle of their physical assets, from acquisition through maintenance and disposal. EAM systems focus on optimizing asset performance, reducing downtime, and ensuring compliance with industry regulations. These systems provide functionalities such as asset tracking, work order management, preventive maintenance, and inventory control, all designed to maximize asset availability and reliability. EAM systems are used extensively in asset-intensive industries such as manufacturing, utilities, energy, and transportation, where effective asset management is crucial for operational efficiency and cost control (Tsang 2002).

Recent advancements in EAM systems have incorporated smart technologies, such as Machine Learning and Multi-Criteria Decision-Making, to enhance asset management capabilities. According to (Gorski, Loures, Santos, Kondo & Martins 2021), these technologies enable EAM systems to improve decision-making processes by analyzing vast amounts of data to predict asset failures, schedule maintenance more effectively, and optimize resource allocation. The integration of these technologies allows organizations to transition from reactive to predictive maintenance, leading to more efficient asset utilization and reduced operational risks.

Table 5. EAM provider globally (marketsandmarkets 2024) (emergenresearch 2024)

System	Provider	Market Share
IBM Maximo	IBM	undisclosed
SAP EAM	SAP	undisclosed
Infor EAM	Infor	undisclosed
Oracle EAM	Oracle	undisclosed
IFS Applications	IFS	undisclosed
Other	Other	undisclosed

The key players in the EAM market, such as IBM Maximo, SAP EAM, Infor EAM, Oracle EAM, and IFS Applications, hold significant positions due to their comprehensive solutions that cater to a wide range of industries. These platforms manage the entire lifecycle of physical assets, from procurement to disposal, helping organizations maximize asset efficiency, reduce downtime, and ensure regulatory compliance. IBM Maximo, for example, is renowned for its robust asset management and IoT integration capabilities, making it popular in sectors like energy and utilities. SAP EAM, similarly, integrates with broader enterprise resource planning (ERP) systems, offering a comprehensive solution for managing assets, maintenance,

and business operations. Providers like Infor EAM, Oracle EAM, and IFS Applications each offer niche advantages such as industry-specific functionalities, cloud-based flexibility, and advanced analytics, further cementing their importance in the EAM space.

However, these companies typically do not disclose specific market share data due to the proprietary and competitive nature of this information. Revealing precise market positions could impact their standing in competitive bids or influence customer decisions by highlighting relative strengths or weaknesses. This withholding of data helps providers maintain a strategic advantage by preventing competitors from exploiting detailed insights into their market positioning. Additionally, the EAM market is dynamic and evolving, especially with the rise of cloud-based systems, predictive maintenance technologies, and IoT integrations. Providers often focus on delivering product innovations rather than releasing detailed financial breakdowns, contributing to the difficulty in accessing precise market share data. For a comprehensive understanding of the market, stakeholders usually rely on private market research reports from firms like Gartner or Frost & Sullivan, which compile data from various sources but are not available to the general public.

FINDINGS AND DISCUSSION

As businesses increasingly adopt cloud-based solutions across critical enterprise systems such as ERP, CRM, PLM, MES, and EAM, the shift toward cloud-driven infrastructure is reshaping the market landscape. Major providers like Microsoft Dynamics and Oracle ERP Cloud are capitalizing on the growing demand for scalability and cost efficiency. Additionally, the push for cross-platform integration, seen in systems like SAP, reflects a broader need for unified workflows and seamless data management across diverse systems. Despite the dominance of large providers, the CRM and MES markets remain highly fragmented, with numerous niche players thriving by addressing specific business needs, creating space for innovation and further specialization.

INCREASING CLOUD ADOPTION ACROSS SYSTEMS

The growing integration of cloud capabilities across ERP, CRM, PLM, MES, and EAM systems suggests a broader trend toward cloud-based enterprise solutions. Providers such as Microsoft Dynamics, Oracle ERP Cloud, and Autodesk Fusion Lifecycle have seen success partly due to their strong cloud offerings. As more businesses prioritize scalability, remote access, and lower infrastructure costs, cloud-based enterprise systems will continue to gain momentum, particularly for small and medium-sized enterprises.

CROSS-PLATFORM INTEGRATION

The success of systems like SAP, which holds notable market shares in both ERP and PLM, highlights the growing importance of cross-platform integration. Businesses increasingly seek solutions that can seamlessly integrate with other critical systems, such as CRM or MES, to enable smoother workflows and unified data management. This trend is likely to drive further consolidation in the market, with larger providers expanding their portfolios to offer end-to-end solutions.

FRAGMENTED MARKETS WITH NICHE PLAYERS

In both CRM and MES markets, the data indicates a high degree of fragmentation, with many niche providers holding substantial portions of the market. For example, 60% of the CRM market and 32% of the MES market are categorized under „Other“ providers, suggesting that many smaller companies are catering to specific business needs or regions. This fragmentation presents opportunities for innovation and specialization, particularly in underserved industries or geographies.

CONCLUSION

In conclusion, the growing adoption of cloud-based solutions across critical enterprise systems is reshaping the business landscape by offering scalable, cost-effective, and flexible infrastructure. Major players like Microsoft and Oracle have capitalized on this trend, while cross-platform integration, as seen

with SAP, has become a vital component for businesses seeking streamlined workflows and unified data management. The continued growth of cloud capabilities is expected to benefit enterprises of all sizes, particularly small and medium businesses that seek agility and cost savings.

Despite the dominance of large providers, the CRM and MES markets remain highly fragmented, with numerous niche players occupying significant market shares. This fragmentation presents unique opportunities for smaller companies to innovate and cater to specific industries or geographic needs, driving further specialization in the market. As cloud adoption and cross-platform integration expand, the enterprise technology landscape will likely see more consolidation, innovation, and tailored solutions across sectors.

REFERENCES

6sense II (2024, October 22). 6sense.com. Retrieved from https://6sense.com/tech/manufacturing-vertical-software/siemens-simatic-it-market-share#free-plan-signup.

6sense.com (2024, October 21). 6sense.com. Retrieved from https://6sense.com/tech/erp/sap-erp-market-share.

Abiresearch (2024, October 21). abiresearch.com. Retrieved from https://www.abiresearch.com/blogs/2024/05/03/product-lifecycle-management-software-2024/.

Buttle, F. & S. **Maklan** (2019). *Customer Relationship Management: Concepts and Technologies.* London: Routledge.

Davenport, T. H. (1998). Putting the enterprise into the enterprise system. *Harvard Business Review, 76(4),* 121–131.

Dezdar, S. & A. **Sulaiman** (2009). Successful enterprise resource planning implementation: Taxonomy of critical factors. *Industrial Management & Data Systems, 109(8),* 1037–1052.

emergenresearch (2024, October 22). emergenresearch.com. Retrieved from https://www.emergenresearch.com/blog/top-10-companies-in-enterprise-asset-management-market.

Gorski, E. G., E. F. **Loures,** E. A. **Santos,** R. E. **Kondo** & G. R. **Martins** (2021). Towards a smart workflow in CMMS/EAM systems: An approach based on ML and MCDM. *Journal of Industrial Information Integration.* doi: https://doi.org/10.1016/j.jii.2021.100278.

Grieves, M. (2006). *Product lifecycle management: Driving the next generation of lean thinking.* New York: McGraw-Hill.

IDC (2024). IDC 2024 Worldwide Semiannual Software Tracker.

Jansen-Vullers, M. H. (2006). Business process simulation – tool survey. *Journal of Manufacturing Technology Management, 17(5).*

Kumar, K. & J. **van Hillegersberg** (2000). ERP Experiences and Evolution. *Communications of the ACM, 43(4),* 22–26.

Kusiak, A. (2018). Smart manufacturing. *International Journal of Production Research,* 508–517.

marketsandmarkets (2024, October 22). marketsandmarkets.com. Retrieved from https://www.marketsandmarkets.com/ResearchInsight/enterprise-asset-management-market.asp.

MESA International (2016). MES Explained: A High Level Vision. MESA White Paper. White Paper 6.

Mithas, S., M. S. **Krishnan** & C. **Fornell** (2005). Why Do Customer Relationship Management Applications Affect Customer Satisfaction? *Journal of Marketing, 69(4),* 201–209.

Payne, A. & P. **Frow** (2013). *Strategic Customer Management, Integrating Relationship Marketing and CRM.* Sidney: Cambridge University Press.

Stark, J. (2015). *Product lifecycle management: 21st century paradigm for product realization.* Heidelberg: Springer. doi:10.1007/978-3-319-17440-2.

Sudarsan, R., S. J. **Fenves,** R. D. **Sriram** & F. **Wang** (2005). A product information modeling framework for product lifecycle management. *Computer-Aided Design, 13(37),* 1399–1411.

Thibaud, L. & B. **Xavier** (2021). S&P Global Ratings. Paris: Standard and Poor.

Tsang, A. (2002). Strategic dimensions of maintenance management. *Journal of Quality in Maintenance Engineering, 8(1),* 7–39. doi:https://doi.org/10.1108/13552510210420577.

АНАЛИЗ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ В ИНДУСТРИАЛЕН КОНТЕКСТ

Резюме: *В този доклад се разглежда ролята на информационните системи като ERP, PLM, CRM, MES и EAM за стимулиране на цифровата трансформация и подобряване на оперативната ефективност в индустриалните организации. В проучването е използвана методология, основана на вторични проучвания, включително преглед на литература, пазарни доклади и данни за индустрията, за да се анализират основните доставчици на системи и съответните им пазарни дялове. То идентифицира ключови тенденции в приемането на облака, интеграцията между*

платформите и фрагментацията на пазара, като предлага информация за това как тези системи влияят върху бизнес операциите. Основните заключения показват нарастващото приемане на решения, базирани на облачни технологии, особено сред малките и средни предприятия поради тяхната мащабируемост и потенциал за спестяване на разходи. Интеграцията между различни платформи също става съществена, като компании като SAP напредват в усилията си да оптимизират работните процеси между различни системи. Освен това изследването разкрива значителна пазарна фрагментация в секторите на CRM и MES, което създава възможности за нишови играчи да иновират и да отговорят на специфични индустриални или регионални нужди.
Ключови думи: *цифровизация, облак, информационни системи, фрагментация на пазара*

Максимилиан Ренке, докторант
Университет по библиотекознание и информационни технологии
E-mail: maximilian.renke@gmail.com

ИНФОРМАТИКА И КОМПЮТЪРНИ НАУКИ
INFORMATICS AND COMPUTER SCIENCES

IMPACT OF ROBOTIC PROCESS AUTOMATION ON THE DESIGN OF MANAGEMENT REPORTING

Ahmad Jawed Ghaffari
University of Library Studies and Informational Technologies

Abstract: *In the age of digitalisation, various technologies are increasingly having a direct impact on controlling processes. Robotic Process Automation (RPA) has a significant impact and some benefits on the way companies create and manage their management reporting. Applying Robotic Process Automation (RPA) technology to controlling and management reporting tasks can lead to cost savings, improved process documentation, lower error rates and better report quality. The aim is to test this hypothesis through a qualitative literature review. In the age of digitalisation, reporting is undergoing major changes. Robotic Process Automation is repeatedly mentioned as one of the defining technologies. The results of the study show that Robotic Process Automation brings benefits to the controlling process. At the same time, it poses a risk to the competitiveness of companies that do not implement this technology. Digitalisation can therefore be both an opportunity and a risk.*
Keywords: *Robotic Process Automation, Impact, Management Reporting, Controlling, Digitalisation*

INTRODUCTION

Many CFOs and heads of controlling are currently working intensively on developing and implementing plans for the future structure of their finance and controlling departments. They face the complex challenge of simultaneously building new skills to continuously enhance the value offering for internal customers while also reducing costs. Emerging digital technologies offer effective tools to achieve these diverse goals. One of these technologies, Robotic Process Automation (RPA), can significantly contribute to increasing the efficiency of finance and controlling functions. In corporate practice, most common RPA applications are currently found in key controlling processes such as management reporting, data management, cost, performance, and profitability accounting, as well as planning, budgeting, and forecasting. These processes benefit from not only reduced personnel requirements but also higher processing speeds, constant availability around the clock, and consistent quality through robotic automation. As a result, the capacities of the affected controllers are freed up for more demanding, high-quality tasks (Gleich 2020). Many companies in Germany, Austria and Switzerland have already recognised the potential of Robotic Process Automation. An increasing number of companies are implementing this technology in their finance and controlling processes (PwC 2020, 6).

In literature and practice, a comparatively high degree of application of RPA can be seen in the controlling process ‘management reporting’. Therefore, it seems reasonable to specifically examine this context. The present scientific work therefore deals with the impact of RPA technologies on the design of management reporting in companies in Germany, Austria and Switzerland.

The purpose of reporting is to provide management with the information obtained from controlling. It is therefore of great importance to the management that the data is prepared in such a way that all information can be accessed in a compressed form. The reporting is adapted to the individual context and the respective addressee, so that the reporting provides a targeted overview of the situation (Taschner 2019, 1). Management reporting occupies a special position among the various types of internal reporting. It is used for reporting directly to the board or top management. For this reason, it has some special

features, such as explanations of the information, which are designed to make it easier for management to understand the facts. This is because they may not have direct access to the relevant departments, but still need to gain an overall understanding of the company's situation (Waniczek et al 2018, 6).

The topic of robotic process automation deals with programmable robots that automate and autonomously handle entire processes in companies. The capabilities and functions can be expanded depending on the software and process. The interaction of robotic process automation is intended to serve as a replacement for a human part within processes. In principle, potentials such as increasing efficiency and saving human resources should be utilized here. In the course of the dynamic digitalization of processes and the simultaneous demand for continuous improvement, new technologies and systems for automation and optimization are increasingly emerging. Robotic process automation is one such innovative approach to meeting these requirements. The focus here is on minimizing necessary manual activities in the company and thus achieving an increase in efficiency. Selected activities are to be taken over by robots so that human intervention is no longer necessary. The activities are to be implemented in such a way that no changes need to be made to the underlying processes. Manual human intervention should be imitated as closely as possible without having to adapt systems and system logic on the robots. This also makes it possible to use robotic process automation on existing systems, which is a significant advantage. The special feature is essentially that manual process executions are digitized without the need for high implementation costs. This technology is particularly attractive for companies with time-intensive, repetitive activities (Czarnecki 2018, 113).

Innovative digitalization trends are creating new potential and changing requirements for management reporting. The digital tools that will increasingly change reporting in the future include BI technologies such as Robotic Process Automation (RPA) (Najderek 2020, 132).

RESEARCH METHODOLOGY

This paper is presented on the basis of a literature analysis. A literature analysis deals with the task of systematically comprehending and analysing existing and published knowledge. It is an internationally recognised research method, although it is mainly used in English-speaking countries. Existing works are analysed with regard to a defined question. The added value lies in collating a large amount of relevant research and thus answering a research question. Gaps in research can thus be closed. Various works of literature were considered for this study. On the one hand, scientific papers were consulted to create a theoretical basis. On the other hand, studies by the largest auditing and consulting firms were consulted to establish a practical reference. First, the current state of research is reviewed. The study examines the positive impact that RPA technologies already have on management reporting in practice. At the same time, it provides explanations as to why their use in controlling is still limited. Finally, the possible future development is evaluated.

RESULTS

The impact of robotic process automation on management reporting is currently still limited in performance-oriented corporate management. The technology is primarily used in the automated processing of standardized and repetitive processes (KMPG 2019, 12).

Robotic process automation is therefore often used in processes that have a high potential for optimization through automation. On the one hand, overall efficiency can be increased through faster processing of the tasks. On the other hand, the technology can be used to reduce errors because of automation. If the technology is currently only used to a limited extent, the potential is considered to be highly relevant. Digitalization can therefore be used even more in this context (Dillerup et al 2019, 49).

The advantages of software robots in the context of RPA technologies are manifold. Companies in Germany, Austria and Switzerland cite the following aspects as one of the main advantages. More than 80 per cent of all respondents named time savings as one of the main objectives of automation. Other aspects include more understandable processes, achieving higher levels of digitalization and using existing resources for more interesting activities. In addition, learning effects, scalability and better compliance were mentioned as advantages, but these currently play a rather minor role (PwC 2020, 15). It is clear that

the full benefits are not yet apparent to everyone.

One of the main reasons why RPA is still rarely used in practice is the lack of knowledge and education in the field. Although most companies have accepted digitization as an important topic, the RPA technology is not yet widely recognized. Studies show that the upper management of many companies misjudges the technology and overestimates the implementation costs. As a result, the potential of RPA is not yet being fully utilized. This emphasizes the importance of education. The PwC study shows that over half of all companies state that they have not yet looked in depth at RPA technologies. The main reasons cited are the high level of implementation effort expected, the high level of complexity and difficulties in understanding (PwC 2020, 9). In addition, many companies are experiencing a shortage of IT staff. Since the IT department is often responsible for the introduction and ongoing maintenance of RPA technologies, or at least has to provide support, this represents an obstacle for many companies. IT departments are already working at full capacity and it is comparatively difficult to find qualified employees on the market (PwC 2020, 21). This makes it clear that education and openness towards the technology could minimize barriers and enable more companies to benefit from RPA. At the same time, it makes it clear that there is a high potential for consulting or implementation services for experts in the field.

The use of RPA is seen in the literature as having great potential in this context. A significant effect is seen here in the automation of repetitive processes. The use of software robots can significantly optimize efficiency, use of resources and productivity. The challenges here lie primarily in the IT integration of the applications into the respective systems. Here, however, the integration of robots proves to be an advantage, as no completely new systems need to be developed, but the robots support existing systems. In principle, the technology is suitable for the automated creation of reports and the preparation of data. It can be assumed that this will increasingly simplify reporting and that the rapid analysis of large volumes of data will continue to come to the fore in the context of controlling (Deloitte 2019, 31).

In future, robotic process automation (RPA) will also be an important part of the reporting process. RPA refers to the automation of company processes that were previously carried out by employees. RPA is seen as a software employee who executes company processes and thus replaces the employee. The automation of manual tasks can therefore reduce costs in controlling and increase productivity (Heimel 2019, 423).

Ad-hoc reporting is used when management needs information on a specific occasion. Ad hoc reporting usually deals with specific issues arising from a particular situation. As these situations can often arise at short notice, controlling must be able to collect and process the data in a timely manner. This form of reporting places greater demands on controlling structures, such as the IT infrastructure, which are directly related to the evaluation and comprehensible preparation of data and information (Waniczek et al 2018, 7). RPA technology can therefore offer significant added value, especially in ad hoc reporting. Data can be captured and interpreted in real time.

A common criticism of automation is of an ethical and human nature. In connection with technologies such as RPA, the potential risk that the technology will replace human labor and thus jeopardize many jobs is often mentioned. A study by one of the leading consulting and auditing firms (PwC) cannot confirm this connection. Around 75 per cent of the companies surveyed stated that they do not dispense with human personnel as a result of RPA bots, but rather that additional opportunities arise. This is another area where openness to technology can refute some of the prejudices (PwC 2020).

The technology can link data relevant for reporting, create interfaces and process it as needed. However, within this controlling process, there are regularly self-contained ERP systems that cannot interact with other systems. At these points, manual human intervention is required to keep the applications in a functional state. The software also needs to be implemented and updated to ensure that the best possible results are achieved (Alexander et al 2019). Humans are therefore not being completely replaced, as some critics often claim.

CONCLUSION

Companies in the D-A-CH region have already recognized the potential of RPA technologies to some extent. A large proportion of them are already using the solutions, at least in individual processes. It

is clear that those who do not yet use the technology lack information and understanding. Overestimating the implementation effort is one of the biggest barriers to using the technology. It can be assumed that more and more companies will use this technology in the future. Digitization as a whole is increasing in practice. RPA is one of the key terms in this context.

The advantages of RPA are diverse and almost obvious. Processes can be automated and handled more efficiently. However, the advantages can go much further. It is clear that the use of the technology in companies is only just beginning and that its full potential is far from being exhausted. It is also clear that ethical risks have not yet been confirmed. This also speaks in favor of further promoting the technology. So far, RPA has been used in companies primarily in controlling. Within this discipline, management reporting has so far offered the most opportunities for the application of robotics and automation. In the future, the technology will probably – and there are indications that this is the case – be used more and more in other controlling disciplines.

REFERENCES

Alexander, S., A. **Haisermann,** T. **Schabicki,** S. **Frank** (2018). Robotic Process Automation (RPA) im Rechnungswesen und Controlling – welche Chancen ergeben sich? *Controlling-Zeitschrift für erfolgsorientierte Unternehmenssteuerung, issue 3* [viewed 01 June 2024]. Available from: https://web.archive.org/web/20220308113908id_/https://www.beck-elibrary.de/10.15358/0935-0381-2018-3-11.pdf.

Czarnecki, C., G. **Auth** (2018). *Prozessdigitalisierung durch Robotic Process Automation,* vol. 1. Wiesbaden.

Deloitte (2019). Wie digital ist das Schweizer Controlling? – Eine schweizweite Analyse auf Basis eines Reifegradmodells [viewed 18 April 2024]. Available from: https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/finance-transformation/ch-finance-transformation-Wie-digital-ist-das-Schweizer-Controlling-HSLU-Deloitte-2018.pdf.

Dillerup, R., T. **Witzemann,** S. **Schacht,** L. **Schaller** (2019). Planung im digitalen Zeitalter. *Controlling & Management Review, issue 3,* 46–53. [viewed 05 February 2024]. Available from: https://www.researchgate.net/profile/Ralf-Dillerup/publication/332417463_Planung_im_digitalen_Zeitalter/links/5d0b3fd2a6fdcc35c15bcc98/Planung-im-digitalen-Zeitalter.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19.

Gleich (2020). Robotic Process Automation im Controlling: Ergebnisse einer empirischen Studie. Controlling Challenge 2024 – Agil, digital, effektiv. Haufe. [viewed 01 June 2024]. Available from: https://www.researchgate.net/profile/Helge-Wild/publication/346392915_Robotic_Process_Automation_im_Controlling_Ergebnisse_einer_empirischen_Studie/links/65b6a4b234bbff5ba7cee7da/Robotic-Process-Automation-im-Controlling-Ergebnisse-einer-empirischen-Studie.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19.

Heimel, J., M. **Müller** (2019). *Controlling 4.0 – Unternehmensführung im digitalen Zeitalter.* Springer Gabler, Wiesbaden.

KMPG (2019). Digitalisierung im Rechnungswesen – Eine Bestandsaufnahme im Accounting und Controlling. [viewed 05 February 2024]. Available from: https://assets.kpmg.com/content/dam/kpmgsites/ch/pdf/digitalisierung-im-rechnungswesen-2019.pdf.coredownload.inline.pdf.

PwC (2020). Robotic Process Automation (RPA) in der DACH-Region – Analyse mit Blick auf Finance & Controlling. [viewed 07 July 2024]. Available from: https://www.pwc.de/de/rechnungslegung/robotic-process-automation-rpa-in-der-dach-region.pdf.

Taschner, A. (2019). *Management Reporting und Behavorial Accounting,* vol. 2. Wiesbaden.

Waniczek, M., A. **Feichter,** P. **Schwarzl,** C. **Eisl** (2018). *Management Reporting. Berichte wirksam und adressatengerecht gestalten,* vol. 1. Wien.

ВЛИЯНИЕ НА АВТОМАТИЗАЦИЯТА НА РОБОТИЗИРАНИТЕ ПРОЦЕСИ ВЪРХУ ДИЗАЙНА НА УПРАВЛЕНСКИТЕ ОТЧЕТИ

Резюме: *В епохата на цифровизацията различните технологии все повече оказват пряко въздействие върху процесите на контрол. Автоматизацията на роботизираните процеси (RPA) има значително въздействие и някои ползи за начина, по който компаниите създават и управляват управленската си отчетност. Прилагането на технологията за автоматизация на роботизирани процеси (RPA) към задачите по контролинг и управленска отчетност може да доведе до намаляване на разходите, подобряване на документацията на процесите, намаляване на процента на грешки и по-добро качество на отчетите. Целта е да се провери тази хипотеза*

чрез качествен преглед на литературата. В епохата на цифровизацията отчетността претърпява сериозни промени. Автоматизацията на роботизираните процеси многократно се споменава като една от определящите технологии. Резултатите от проучването показват, че роботизираната автоматизация на процесите носи ползи за процеса на контролинг. В същото време тя представлява риск за конкурентоспособността на компаниите, които не прилагат тази технология. Следователно цифровизацията може да бъде както възможност, така и риск.
Ключови думи: *роботизирана автоматизация на процесите, въздействие, управленска отчетност, контрол, дигитализация*

Ахмад Джовед Гафари, магистър
Университет по библиотекознание и информационни технологии
E-mail: jawed@global-act.de

НАЦИОНАЛНА СИГУРНОСТ
NATIONAL SECURITY

CYBER SECURITY AND INFORMATION SECURITY

Mark Dietz
University of Library Studies and Information Technologies

Abstract: *In recent decades progressive digitalization and networking of industrial plants have led to considerable efficiency gains and innovations. At the same time, however, this development has also massively increased the surface of attacks for cyber threats. Industrial plants, which used to be largely isolated and protected by physical security measures, are now part of complex, globally networked systems. This makes them vulnerable to various cyberattacks from criminal organisations and state actors. To meet these challenges, numerous standards have been developed to strengthen cyber security in the industrial environment. Two of the most important and widely used standards are IEC 62443-x series and ISO/IEC 2700x series. The ISO/IEC 2700x series describes establishing and operating an IT security management system (ISMS). This series of standards deals with information security and does not differentiate between data in IT systems and intellectual property. The IEC 62443-x series focuses on protecting industrial automation systems and is therefore assigned to the area of Operational Technology.*
Keywords: *information security, cyber security, vocabulary, requirements, guidelines*

INTRODUCTION

IEC 62443-x is a series of standards developed specifically for the safety of industrial automation and control systems (IACS). It provides comprehensive guidelines for implementing safety measures throughout an industrial plant's life cycle, from planning and design to operation and decommissioning.

ISO/IEC 27001, on the other hand, is an internationally recognised standard for information security management systems (ISMS). It provides a systematic approach to managing sensitive corporate information and aims to ensure its confidentiality, integrity, and availability. Although ISO/IEC 27001 is not specifically designed for industrial environments, it still provides valuable guidelines that can be applied in these contexts.

By combining both standards, companies can develop a holistic security strategy that considers the specific requirements of industrial systems and the general principles of information security management.

Scientific research and innovation in this area are essential to keeping pace with constantly evolving threats. New technologies and approaches need to be developed and tested to continuously improve the effectiveness of security measures. It is, therefore, vital that scientists, engineers, and security experts work closely together to develop innovative solutions that ensure the protection of industrial facilities against cyber threats.

To summarise, securing industrial facilities against cyber threats is one of the critical challenges of our time. IEC 62443-x and ISO/IEC 2700x provide valuable tools to meet this challenge, and continuous research and innovation in this area are crucial to ensure the security and resilience of industrial systems.

ISO/IEC 2700x series of standards

The ISO/IEC 2700x series of standards is a series of sixty sub-standards on information security management systems (ISMS). The most important of these are ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, and ISO/IEC 27019.

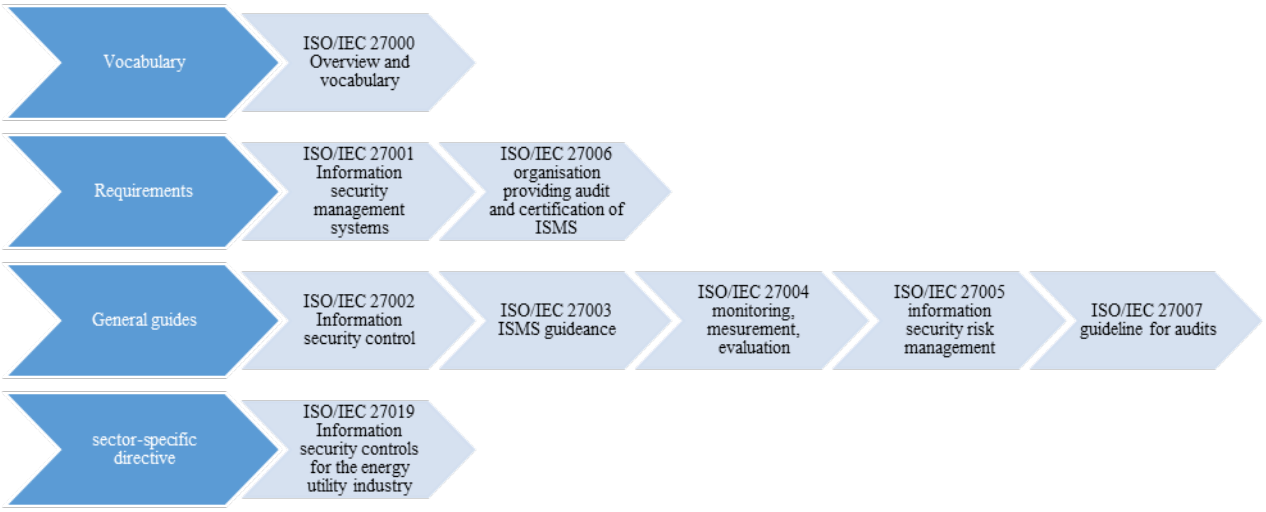


Fig. 1. Extract from the structure of the ISO/IEC 2700x series of standards (Kroeselberg 2017)

ISO/IEC 27000 first explains the technical terms used and then provides an overview of the other standards in the series. The series of standards deals with the establishment of an information security management system (ISMS). The standard focuses on information security to ensure the availability, integrity, and confidentiality of information (ISO/IEC 27000 2018).

ISO/IEC 27001 defines requirements for ISMS. It specifies the requirements for introducing, implementing, operating, monitoring, reviewing, maintaining, and improving formalised information security management systems (ISMS) about an organisation's overarching business risks. The content includes, among other things, the organisation's context, management leadership and commitment, the company's security policy, the organisation's responsibilities and authorities, and measures for dealing with risks and opportunities, including the improvement processes (ISO/IEC 27001 2022).

ISO/IEC 27002 is a guide for implementing information security measures. It provides specific advice and best practice guidance on implementing measures specified in ISO/IEC 27001. These include, for example, the assignment of access rights, user management, access management, password management, data carrier disposal, physical security perimeter, protection against malware, and data backup (ISO/IEC 27002 2022).

ISO/IEC 27003 guides the requirements for an information security management system (ISMS) specified in ISO/IEC/IEC 27001 and gives recommendations and explanations for better understanding (ISO/IEC 27003 2017).

ISO/IEC 27004 guides to help organisations evaluate the ISMS's information security performance and effectiveness to meet the requirements of ISO/IEC 27001. It addresses the monitoring and measurement of information security performance, the monitoring, the measurement of the effectiveness of an information security management system, including the processes and measures, and the analysis and the evaluation of the results of the monitoring and measurements (ISO/IEC 27004 2016).

ISO/IEC 27005 contains guidelines for the risk management of information security. In addition to supporting the general ideas outlined in ISO/IEC 27001, its goal is to facilitate the application of risk-based information security. To fully comprehend, one must be familiar with the concepts, models, procedures, and jargon covered in ISO/IEC 27001 and ISO/IEC 27002. This document pertains to all categories of organizations (such as for-profit businesses, government agencies, and nonprofits) that plan to manage risks that could jeopardize their information security. (ISO/IEC 27005 2022).

The requirements outlined in ISO/IEC 27001 provide guidance to organizations that must manage an ISMS audit program or conduct internal or external audits of an ISMS. An audit can be conducted against several audit criteria, for example, the requirements defined in ISO/IEC 27001; policies and requirements specified by relevant interested parties; legal and regulatory requirements; ISMS processes and controls defined by the organisation or other parties; and plans for achieving information security objectives (ISO/IEC 27007 2020).

ISO/IEC 27019 is of interest in the context of automation technology. This provides guidance based on ISO/IEC 27002 and is applied to process control systems used by the energy supply industry to control and monitor the production or generation, transmission, storage and distribution of electrical energy, gas, oil, and heat, and to control the associated supporting processes. Nuclear facility process control is not covered by ISO/IEC 27019. ISO/IEC 27019 also includes adapting the risk assessment and handling processes described in ISO/IEC 27001 to the energy utility sector (ISO/IEC 27019 2017).

IEC 62443 series of standards

Based on the models and requirements of the ISO 2700x series of standards, the IEC 62443 series of standards considers the special requirements of IT security in the production sector. Figure 2 shows the structure of the standard series.

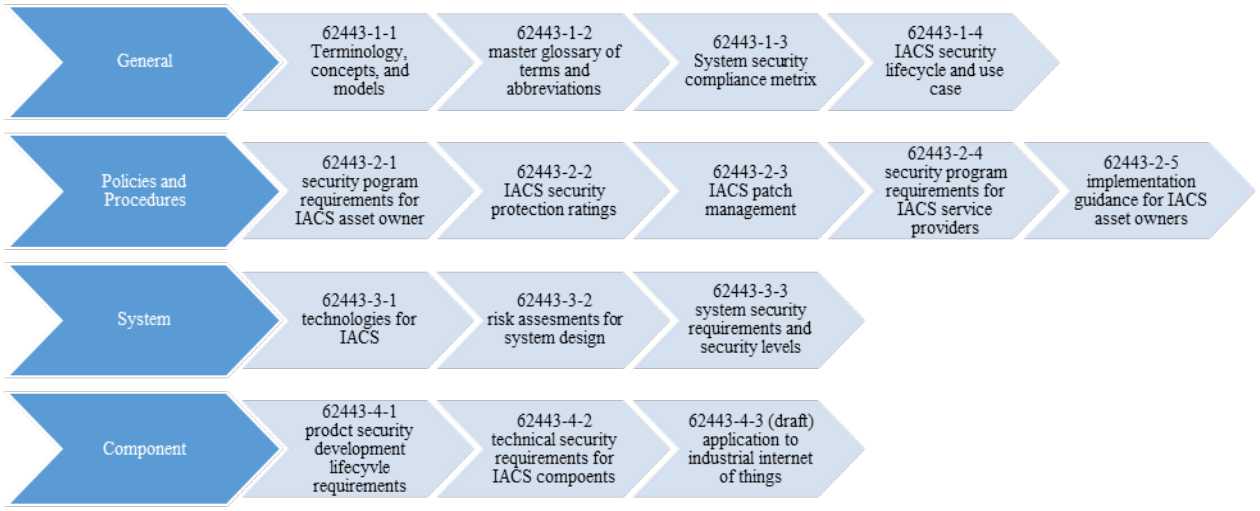


Fig. 2. Extract from the structure of the IEC 62443 series of standards (DKE, 2020)

IEC/TS 62443-1-1 is a technical specification that defines the terminology, concepts and models for *the* security of industrial automation and control systems (IACS). It forms the basis for the other standards in the IEC 62443 series, and its components include risk assessment, the maturity level of the security programme, policies, models, and reference architecture (IEC/TS 62443-1-1 2009).

IEC/TR 62443-1-2 defines all the terms used in the technical standards (IEC/TR 62443-1-2 2010). IEC/TS 62443-1-3 defines the metrics for evaluating IT security in technical specification (IEC/TS 62443-1-3 2014), and IEC 62443-1-4 describes the security lifecycle and use cases (IEC 62443-1-4 2018).

OPERATORS AND SERVICE PROVIDERS

IEC 62443-2-1 describes the requirements for an IT security management system, including the definitions of security procedures, risk management, training requirements, business continuity plans, access control, and the improvement process (IEC 62443-2-1 2024).

IEC 62443-2-2 guides how and in which areas these procedures will be implemented. It specifies a framework for evaluating the protection of an IACS. It contains a method for combining the evaluation of organisational and technical security measures in numerical values, the so-called “protection level” (IEC-62443-2-2 2020). The framework forms the structure for evaluating the defence-in-depth strategy of the IACS in operation based on the technical and organisational requirements specified in other documents of the IEC 62443 series of standards (DKE 2020).

IEC/TR 62443-2-3 is dedicated to updating the software of automation systems for technical standards. Patching is critical because improper procedures can lead to malfunctions (IEC/TR 62443-2-3 2015).

IEC 62443-2-4 deals with using service providers for commissioning and service from an IT security perspective. It specifies requirements for IT security guidelines, procedures and practices that apply to suppliers of industrial automation systems during the life cycle of their products and to maintenance

service providers (IEC 62443-2-4 2023).

IEC 62443-2-5 contains implementation instructions for operators (IEC 62443-2-5 2024). The Processing status of IEC is in planning.

REQUIREMENTS FOR AUTOMATION SYSTEMS

IEC/TR 62443-3-1 first describes the underlying technologies, such as authentication, encryption, filtering and logging for techical standards (IEC/TR 62443-3-1 2009).

IEC 62443-3-2 describes the entire safety analysis process and, based on this, the structuring of a system into zones (isolated areas) and conduits (secured connections between the regions). This is intended to divide an automation system into sub-areas, which are sealed off from each other (IEC 62443-3-2 2020).

IEC 62443-3-3 describes specific requirements for automation systems in the form of foundational requirements. These Foundational Requirements (FR) define the IT security aspects of the system. This part provides concrete instructions for planners and operators of automation systems about specific technical measures and so-called security levels (SL) assigned (IEC 62443-3-3 2013).

Table 1. Security Level based of IEC 62443-3-3, 2013

SL	Description – security level defined
1	Protection against casual or coincidental violation
2	Protection against intentional violation using simple mean
3	Protection against intentional violation using sophisticates means
4	Protection against intentional violation using sophisticates means with extended resources

Specifies SL1 (low requirements) to SL4 (high requirements). Depending on the system's protection requirements, the requirements can be selected according to the desired security level (IEC 62443-3-3 2013).

REQUIREMENTS FOR AUTOMATION COMPONENTS

IEC 62443-4-1 defines the development process that must be observed when developing components for automation technology.

Fig. 3. Secure development life cycle (Waldeck 2020)

Figure 3 shows the secure development life cycle described in the standard. This extends across all phases of the development process. By implementing this standard, manufacturers of automation components can build up the product development life cycle in accordance with the security-by-design approach and thus lay the foundation for component certification. The abbreviations in the grey boxes correspond to the requirement classes from the respective parts of the standard. Maturity levels from 1 to 4 are assigned for an organisation structured in this way.

IEC 62443-4-2 describes the technical requirements for the components of automation systems, applications and functions. The structure of the requirements follows IEC 62443-3-3, but the requirements

that the components must fulfil are described here. A distinction is made between component requirements (CR) and further requirements (RE = Requirement enhancements). These requirements are derived from the system requirements (SR). The components of an IACS defined in this document are the software applications, host devices, embedded devices and network components (IEC 62443-4-2 2019).

IEC/TR 62443-4-3 has been published as a technical standard draft and deals with the Industrial Internet of Things (IIoT). It deals with components and products (IEC/TR 62443-4-3 2024).

Assignment of the IEC 62443-x standard parts to the players in the safety process

The operator Service provider is responsible for operating and maintaining a production facility. The guidelines for operation and maintenance are relevant for these actors. The parts of the standard that regulate the structure and operation of the ISMS (IEC 62443-2-1) and the involvement of service providers (IEC 62443-2-4) are relevant here. IEC/TR 62443-2-3, which regulates updating the control system software (patch management), is also appropriate for operators.

The role of the system integrator is to design and install the automation system. IEC 62443-3-3 is relevant here, as it specifies the design and structure of the system. IEC 62443-3-2 can also be used for safety risk assessment and system design. If a service provider carries out the planning process, IEC 62443-2-4, which describes the requirements for service providers, must also be observed. If the system operator carries out the planning work themselves, the standards mentioned in this section also apply to the operator in their role as system planner. The third role is that of the product supplier. IEC 62443-4-1, which specifies the requirements for a secure development process (security by design), initially applies to these suppliers. The requirements for the products developed by the product supplier are described in IEC 62443-4-2 and IEC 62443-4-3, which has been published as a draft.

DELIMITATION OF IT SECURITY STANDARDS

Now that the two series of standards, IEC 62443-x and ISO 2700x, have been described in the previous chapters, a distinction must be made between them regarding their applicability in the production sector. Therefore, these requirements are described below, and the areas of IT (Information Technology and ISO 2700-x) and OT (Operational Technology ans ISO 2700x) are differentiated from each other.

Table 2. Delimitation of the IT and OT domains (Gartner 2024).

Domain	Definition	Application examples
IT	”IT“ is the common term for information processing technologies, including software, hardware, communication technologies and related services. In general, IT does not include embedded technologies as long as they do not generate data for corporate use.	• Client systems for personal • Notebooks • Web server • Mail server • SAP systems • File Server • Networks
OT	Operational technology (OT) is hardware and software that detects or causes a change by directly monitoring and/or controlling industrial devices, systems, processes, and events.	• Programmable logic controllers (SPS) • Display systems (touch panels) • Server for production control • Industrial robots • Remote IO systems • Real-time networks

Information security is defined by ISO/IEC 2700x as guaranteeing the confidentiality, availability, and integrity of data. The term IT security is a sub-aspect of information security. It refers to the protection of technical systems. The term “cyber security” or “ICS security” is often used for production systems (BSI, 2014). This focuses on the security of production systems (OT). The term data protection is only

mentioned here for the sake of completeness but has no relevance here. The different areas of application of IT and OT also result in different requirements in terms of IT and OT security.

CONCLUSION

The ISO/IEC 2700x series describes the structure and operation of an IT security management system (ISMS). The series of standards addresses information security in general and does not differentiate between data in IT systems or intellectual property. The ISO/IEC 27001 standard is to be regarded as the basic standard by which essential requirements for IT security, such as planning, responsibilities, risk assessment, communication, resources, and internal audit) are defined. The focus is on the organisational and process-related aspects of IT security. ISO/IEC 27002 defines specific requirements for IT security, such as access control, network security, separation of networks, etc. One focus of the series of standards is monitoring and evaluating the ISMS ISO/IEC 27004 and certification per ISO/IEC 27007. The standard is generic and can be used for IT applications in the same way as for OT. However, the standard makes no specific reference to the requirements of OT. One exception is IEC 27019, which refers to energy supply systems.

The IEC 62443 series focuses on protecting industrial automation systems and is therefore assigned to the area of Operational Technology (OT). Specific features of OT are taken into account. For example, the requirements relating to service providers (IEC 62443-2-4) are considered, as is patch management in production facilities (IEC/TR 62443-2-3). The aspect of setting up and operating an ISMS is also included in the series of standards (IEC 62443-2-1), but the focus is on specific technical requirements for automation systems (IEC 62443-3-3) and the components of automation systems (IEC 62443-4-2), with the latter being aimed at the manufacturers of automation components.

Both series of standards have similarities. The basic concepts and technologies can be found in both series of standards. However, it should be noted that the IEC 62443 series of standards clearly focuses on automation technology, while the ISO/IEC 2700x series is more process-orientated and generic (Kohl 2018).

REFERENCES

BSI (2014). *ICS-Security-Kompendium. Testempfehlungen und Anforderungen für Hersteller von Komponenten*. Bundesamt für Sicherheit in der Informationstechnik [viewed 30 August 2024]. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.pdf?__blob=publicationFile.

DKE (2020). *Elektronik Informationstechnik DIN und VDE EC 62443*. Die internationale Normenreihe für Cybersecurity in der Industrieautomatisierung. Deutsche Kommission Elektrotechnik [viewed 30 August 2024]. Available from: https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung.

Gartner (2024). *Glossary Information Technology* [viewed 30 August 2024]. Available from: https://www.gartner.com/en/information-technology/glossary?glossaryletter=I.

IEC/TS 62443-1-1 (2009). *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*. International Electrotechnical Commission.

IEC/TR 62443-1-2 (2010). *Security for industrial automation and control systems – Master Glossary*. International Electrotechnical Commission.

IEC/TS 62443-1-3 (2014). *Security for industrial process measurement and control – Network and system security – Part 1-3: System security compliance metrics*. International Electrotechnical Commission.

IEC 62443-1-4 (2018). *Security for industrial automation and control systems Life Cycle and Use Cases.* International Electrotechnical Commission.

IEC 62443-2-1 (2024). *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program.* International Electrotechnical Commission.

IEC-62443-2-2 (2020). *Security for industrial automation and control systems – Part 2-2: IACS security program rating.* International Electrotechnical Commission.

IEC/TR 62443-2-3 (2015). *Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment.* International Electrotechnical Commission.

IEC 62443-2-4 (2023). *Security for industrial automation and control systems – Network and system security – Part 2-4: Requirements for IACS solution suppliers.* International Electrotechnical Commission.

IEC 62443-2-5 (2024). *Implementation guidedance for IACS asset owners.* International Electrotechnical Commission, not released [viewed 30 August 2024]. https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung.

IEC/TR 62443-3-1 (2009). *Industrial communication networks – Network and system security – Part 3-1: Security*

technologies for industrial automation and control systems. International Electrotechnical Commission.
IEC 62443-3-2 (2020). *Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design.* International Electrotechnical Commission.
IEC 62443-3-3 (2013). *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels.* International Electrotechnical Commission.
IEC 62443-4-1 (2018). *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.* International Electrotechnical Commission.
IEC 62443-4-2 (2019). *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components.* International Electrotechnical Commission.
ISA/TR 62443-4-3 (2024). *Security for industrial automation and control systems – Part 4-3: Application to industrial internet of things.* International Electrotechnical Commission.
ISO/IEC 27000 (2018). *Information technology – Security techniques – Information security management systems – Overview and vocabulary.* International Standardization Organization.
ISO/IEC 27001 (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements.* International Standardization Organization.
ISO/IEC 27002 (2022). *Information security, cybersecurity and privacy protection – Information security controls.* International Standardization Organization.
ISO/IEC 27003 (2017). *Information technology – Security techniques – Information security management systems – Guidance.* International Standardization. Organization. International Standardization Organization.
ISO/IEC 27004 (2016). *Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation.* International Standardization Organization.
ISO/IEC 27005 (2022). *Information security, cybersecurity and privacy protection – Guidance on managing information security risks.* International Standardization Organization.
ISO/IEC 27006 (2024). *Information security, cybersecurity and privacy protection – Requirements for bodies providing audit and certification of information security management systems.* International Standardization Organization.
ISO/IEC 27007 (2020). *Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing.* International Standardization Organization.
ISO/IEC 27019 (2017). *Information technology – Security techniques – Information security controls for the energy utility industry.* International Standardization Organization.
Kohl, A., C. **Bisale** (2018). *Effektive und effiziente Security auf Basis internationaler Standards.* In np, 9, S. 12–14.
Kroeselberg, D., F. **Buchi,** H. **Meulenbroek** (2017). *Cyber Security Tutorial Energy Automation and IEC 62443* [viewed 30 August 2024]. Available from: https://www.pcic-library.com/sites/default/files/final/EUR17_63.pdf.
Waldeck, B. (2020). *Zertifizierter Entwicklungsprozess nach 62443-4-1* – Security by design, Online Seminar, Lemgo.

КИБЕРСИГУРНОСТ И ИНФОРМАЦИОННА СИГУРНОСТ

Резюме: *През последните десетилетия прогресивната цифровизация на промишлените предприятия и свързването им в мрежа доведоха до значително повишаване на ефективността и до иновации. В същото време обаче това развитие увеличи значително и полето на атаките за киберзаплахи. Промишлените предприятия, които преди бяха до голяма степен изолирани и защитени с физически мерки за сигурност, сега са част от сложни, глобално свързани в мрежа системи. Това ги прави уязвими за различни кибератаки от страна на престъпни организации и държавни субекти. За да се отговори на тези предизвикателства, са разработени множество стандарти за укрепване на киберсигурността в индустриалната среда. Два от най-важните и широко използвани стандарти са сериите IEC 62443-x и ISO/IEC 2700x. Серията ISO/IEC 2700x описва създаването и функционирането на система за управление на информационната сигурност (СУИС). Тази серия стандарти се занимава със сигурността на информацията и не прави разлика между данните в ИТ системите и интелектуалната собственост. Серията IEC 62443-x се фокусира върху защитата на системите за индустриална автоматизация и поради това е отнесена към областта на оперативните технологии.*
Ключови думи: *информационна сигурност, киберсигурност, речник, изисквания, насоки*

Д-р Марк Дийтц
Университет по библиотекознание и информационни технологии
E-mail: mark-dietz@gmx.net

НАЦИОНАЛНА СИГУРНОСТ
NATIONAL SECURITY

ПАЦИФИСТИТЕ НЕ ПРИЕМАТ ВОЙНАТА, А ПРИЕМЛИВ ЛИ Е ПАЦИФИЗМЪТ?

Нено Димов
Университет по библиотекознание и информационни технологии

Резюме: *Не приемам за вероятно да съществуват психически нормални, разумни и здравомислещи хора, които да подкрепят войната и изобщо насилието. Но насилието все пак съществува и нещо повече, то е постоянен спътник в живота на Земята. Дали е възможно това да се промени? Пацифистките движения насочват усилията си именно в тази посока и си поставят за цел да избавят човечеството от войната и насилието. Тази статия разглежда различните видове пацифизъм, каквито са абсолютният и условният, максималният и минималният, универсалният и особеният, скептичният и привидният и накрая трансформационният, както и техните разновидности, за да потърси отговор на въпроса „Приемлив ли е пацифизмът?“. Пълното отказване от войната като средство за разрешаване на конфликти, моралното ѝ осъждане, както и осъждането на всяко насилие, неразривното обвързване на мира с достойнството на хората могат да се разглеждат като благороден и възвишен идеал. Дали тези хубави намерения, този възвишен идеал, не са основата на поредна неприложима утопия? И дали нейното практическо прилагане не може да ни доведе до катастрофа?*
Ключови думи: *пацифизъм, видове пацифизъм, морал, етика, война*

ВЪВЕДЕНИЕ

Пацифизмът е пълното отказване от войната като средство за разрешаване на конфликти и приема, че тя, войната, и насилието са морално грешни. Това движение представлява осъждане на всички войни, а мира приема за неразривно свързан с достойнството на хората. Най-общо може да се каже, че пацифизмът има три основни части: философска, морална и религиозна (Kellenberger 1987).

Във философско отношение може би най-старият философ пацифист е основателят на даоизма Лао Дзъ, който казва, че *„няма слава в победата и да възхваляваш нейната злоба е все едно да се радваш на смъртта на хората“* (Andregg 2018). За съвременната философия идеята за *„вечния мир“* на Имануел Кант се появява през XVIII в. Според нея след като е възможно разумно да се определят отношенията вътре в една държава и така се постига вътрешен мир, то би следвало по същия начин да е възможно разумно да се определят отношенията и между различните държави, с което да се постигне външен мир. Залагайки на разума и морала, Кант смята, че няма как войната да бъде избрана пред мира[1].

В морално отношение пацифизмът е отхвърляне на насилието във всички човешки отношения. Това до голяма степен съответства на християнското разбиране за ненасилие. В християнската религия е заложена етиката на любовта, която се съдържа в разказите за живота и думите на Христос. Неговото учение очевидно е несъвместимо с одобрението на войната.

Пацифизмът често се съотнася с идеята за оправдано насилие, даващо моралната основа на справедливата война.[2] Един от основните въпроси е дали войната може да бъде морално оправдана. Дали, парадоксално, може да се твърди, че война, целяща постигане на мир, в същността си е пацифизъм? Или пацифизмът изобщо отрича войната, чийто основен морален проблем е преднамерено, систематично и масово убиване на хора.

Отговорът на този въпрос не е еднозначен и именно поради това пацифизмът има две основни версии – абсолютна и относителна. Аргументът на първата е, че *„при всички обстоятелства е грешно да се отнема човешки живот“,* а втората се състои в убеждението, че *„злините на войната са почти винаги по-големи, отколкото изглеждат в момента на нейното избухване“* (Russell 1943).

За да може по-ясно да се изучи пацифизмът, е важно да погледнем по-внимателно неговата цел (мира), както и това, което отрича (войната). Войната обикновено се смята за насилие между държави (Ангелов 2022), а може да се разглежда и като насилствен конфликт между индивиди. От своя страна насилието

нормативно се определя като неправомерно нараняване или вреда. Но това само по себе си допуска, че може да има и правомерно нараняване.

Мирът е състояние на не-война, не-насилие, не-убиване... Тоест е дефиниран предимно като отрицание. Науката за мира е направила разграничение между отрицателен и положителен мир. Първият е липсата на насилие или война, а вторият обхваща отношения на сътрудничество, спокойствие, хармония и по-широките грижи за човешкото процъфтяване, интеграция, състояние на цялост и завършеност, солидарност, взаимно уважение и задоволяване на нуждите (Boersema 2017). Може дори да се каже, че мирът е човешка добродетел и присъща ценност.

Мирът като начин на живот включва ненасилие спрямо себе си и другите и се ръководи от сътрудничество, взаимно уважение, творческо решаване на проблемите, преговаряне на различията и състрадание (Fox 2014). Това разбиране за мир се вписва в етиката на добродетелта, в която миролюбието се свързва със скромност, толерантност и милосърдие.

Отричането на войната може да се разшири с отричането на всяко насилие, като отричане на смъртното наказание, домашното насилие и това над животните, над природата изобщо и прочее. За да се избегне прекаленото разширяване на темата, което крие риск от разводняване, ще се занимая само с различните видове пацифизъм, отричащ напълно или частично войната или както отбелязах по-горе, абсолютната и условна негова версия.

ВИДОВЕ ПАЦИФИЗЪМ

АБСОЛЮТЕН И УСЛОВЕН ПАЦИФИЗЪМ

Абсолютният пацифизъм е максимално, универсално и категорично отхвърляне на насилието и войната. За моралния абсолютизъм моралните принципи са вечни, непроменливи и без изключения. Изхождайки от това разбиране, абсолютният пацифизъм твърди, че войната и насилието винаги са грешни. Или иначе казано, не е допустимо с едни неморални действия да се борим с други – били те много по-неморални. В екстремните си варианти дори отрича идеята за самозащита (Fiala 2014).

Условният пацифизъм е значително по-разнообразен от това да е задължителен само за определена група хора до отхвърляне на определена военна система (Holmes 1999). Ще разгледам шест негови разновидности:

1. Най-близко до абсолютния пацифизъм е този, който се насочва към начина на водене на конкретна война и отхвърлянето на онези средства на воденето на война, които приема за неморални. Този вариант може да изглежда, че се доближава до теорията за справедливата война, но всъщност значително повече се доближава до идеята на абсолютния пацифизъм, защото най-вероятно ще отрече всяко средство за водене на война и по този начин ще достигне до абсолютната ѝ забрана, без последното да се заявява директно.
2. Вторият вариант е този, при който само представителите на определена група или групи хора, които са част от дадени съсловия или представители на определена професия, трябва да бъдат пацифисти. В този случай миролюбието се приема като морален идеал, с който тези, които го изповядват, превъзхождат останалите. При този подход съвсем реална е възможността за осъждане или дори порицание на неизповядващите морала на пацифизма.
3. Следва вариантът, при който конкретна война или конкретна милитаристична политика е обект на отхвърляне от пацифистите. Това е основано на разбирането, че в конкретния случай войната или политиката са неразумни. Но разумни доводи могат да се дават както в подкрепа, така и за отхвърляне на дадена теза. При това разбиране на пацифизма за разумна се приема оценката на ползите и вредите, като също така се приема, че конкретната война или милитаристична политика ще доведе до повече негативни, отколкото позитивни резултати.
4. Политическият пацифизъм е друга разновидност на условния. Привържениците му отхвърлят и се противопоставят на всяка милитаристична политика. Наречени *„гълъби“,* те нямат ясен ангажимент било към *„справедливата война“,* било към ненасилието изобщо. По-скоро политически се противопоставят на привържениците на финансирането на военната система, наречени *„ястреби“.*
5. Условният пацифизъм може да разглежда и войната в трите ѝ етапа – правото на война (jus ad bellum), правото във войната (jus in bellum) и правото след войната (jus post bellum). В първия случай може да бъде отхвърлена властта, която воюва, да се оспори справедливостта на каузата или че не са изчерпани всички останали средства. Във втория случай на прицел на умерените пацифисти може да е положението на невоюващото население, което може да пострада както от самите военни действия, така и от действия на военните (примерно изтезания, изнасилвания и прочее). В третия случай може да се твърди, че всяка война подкопава дългосрочния мир, справедливостта и стабилността.
6. Последният вариант, който ще разгледам, е „либерален пацифизъм“. Има се предвид, че който

изповядва ценностите на либералната демокрация, не трябва да подкрепя войната. В основата на това е идеята, че никой няма право да заповядва на другите да убиват и никой не е оправдан да убива по команда.

Освен разделението на абсолютен и условен съществуват и други варианти. Най-често срещаните са максимален и минимален пацифизъм, универсален и особен, скептичен и привиден и накрая трансформационен.

МАКСИМАЛЕН И МИНИМАЛЕН ПАЦИФИЗЪМ

Разликата при тези две вариации е свързана със степента, видовете и субектите на насилието. Максималният пацифизъм на практика е другото име на абсолютния. Те всъщност не се различават. Минималният пацифизъм разглежда всеки случай поотделно. Той е насочен най-вече към субектите на насилие и конкретните частни случаи. Важно при него е как се дефинира насилието изобщо и войната в частност. Минималният пацифизъм разглежда различни действия, които могат да бъдат описани като „война“. Те могат да варират в диапазона от бунтове до тотална ядрена война. Това включва гражданска война, терористични атаки, хуманитарна намеса, локална война, пълноценен междудържавен конфликт, световна и накрая ядрена война. Минималните пацифисти ще отхвърлят локалните, международните и световните войни по подразбиране. Но това не се отнася за случаите с хуманитарната намеса или гражданските войни. Тук се намесва въпросът с причините за насилието. Съществена трудност пред този вид пацифисти е свързана с ключови ценности като суверенитет и тирания, права на човека и робство и прочее. Както вече казахме, максималните пацифисти ще отхвърлят всеки аргумент, който защитава каквото и да е насилие. Те принципно и безалтернативно се противопоставят на отнемането на живот. Тук можем да разширим тяхното виждане към смъртното наказание, абортите, че дори и яденето на месо. Минималната версия на пацифизма е способна да различава насилник и жертва, като приема за недопустимо насилието над вторите. В това се крие и противопоставянето на войната, при която много невинни (жертви) губят живота си. По същите причини се противопоставят на смъртното наказание и аборта (освен ако не е задължителен за спасяване на живота на майката). Моралното противопоставяне на насилието може да се разшири към всички живи същества със забрана за ядене на месо, защита на животните от жестокост и прочее (Fiala 2018).

УНИВЕРСАЛЕН И ОСОБЕН ПАЦИФИЗЪМ

Моралният въпрос, пред който се изправят тези две разновидности на пацифизма, е дали всеки е длъжен да е пацифист, или е въпрос на личен избор. Няма да е изненада, че в универсалния си вид тази версия на пацифизма не се различава особено от абсолютния и маскирания, защото абсолютизмът е неограничена тотална власт, независимо дали се отнася до човек, или идея. Той не познава нюанси и изключения. Затова и универсалният пацифизъм приема, че след като войната е грешна по принцип, то тя ще е грешна без изключение и за всички. Това включва от системата, предизвикала войната, до войниците, участващи в нея. Особената форма на пацифизма се придържа към идеята, че изборът е личен, и не съди войниците, а в най-крайния си вариант не съди и самата военна система. Това много се доближава до идеята, че пацифизмът се изисква само от определени професии и/или хора. Разликата е в начина, по който се приема ненасилието, а именно дали е морална необходимост, или просто е морално позволен. За универсалиите отговорът е лесен – войната и насилието са зло, следователно пацифизмът е морално необходим (задължителен). Това обаче не се отнася до особената версия. Тя дава правото на пацифиста да не използва насилие (да не участва във война например), но заедно с това не осъжда онези, които го правят при определени условия (отново разграничавайки жертва и насилник). В частност човек може да възприеме един вид „личен пацифизъм“, който не е необходимо да се прилага универсално. Тоест убеждението се свежда до личен избор. Даден индивид може да приеме, че това е правилно и да избере да е (личен) пацифист, като същевременно проявява толерантност към други, които не правят същия избор (Reitan 2000).

СКЕПТИЧЕН И ПРИВИДЕН ПАЦИФИЗЪМ

Както казах в началото, мирът е състояние на не-война, не-насилие, не-убиване... Тоест пацифизмът е дефиниран предимно като отрицание, което ни казва какво не трябва да правим. Това може да се определи като скептична позиция. Чейни Райън[3] смята, че подкрепящите убийството не могат да аргументират тази своя позиция с никакъв убедителен аргумент (Ryan 1983). Това твърдение веднага намира морална опозиция във въпроса с убийството при самозащита. След като жертвата е убила нападателя, то означава, че вторият не е осъществил агресивното си намерение. Така убийството при самозащита се оказва непропорционално на нанесената вреда, защото жертвата не е била убита, докато самата тя извършва убийство. В този случай

скептичният пацифизъм не оправдава действието на жертвата, защото приема, че не са били изчерпани всички други възможности преди да се стигне до насилие. За тях винаги съществуват по-хуманни средства, които могат да решат конфликта преди да се стигне до насилие. Пренесен на по-широка плоскост, този подход критикува милитаризма и подкрепата на войната. Това може да се разглежда и като политически пацифизъм, който приема, че правителствата не заслужават доверието на гражданите си, когато пропагандират война, защото те, правителствата, укриват истината. Опора за тази своя позиция скептичните пацифисти намират в твърдението, че исторически погледнато правителствата манипулират, а защо не директно лъжат, за да подтикнат гражданите си към война (Fiala 2010). По този начин на правителството се вменява задължението да докаже необходимостта от извършването на неморалното действие война, което включва в себе си доказване, че всички алтернативи са изчерпани. От една страна, връщайки се към случая със самозащитата, се оказва, че действието е оправдано едва когато вече е невъзможно, от друга, се допуска, че при определени извънредни обстоятелства и убедителни доказателства, въпреки че е грешна, войната е оправдана. Второто може да се определи като привиден пацифизъм.

ТРАНСФОРМАЦИОНЕН ПАЦИФИЗЪМ

Под това се разбира стремеж към фундаментална културна промяна, водеща към отхвърляне на насилието и войната. Това този вид пацифисти искат да постигнат, като насочват усилията си към изграждане на психологическа, социална и морална чувствителност, недопускаща насилие. Целта е чрез реформиране на образователните и културните практики да се изгради свят, в който войната да е останка от минала, по-малко цивилизована епоха (Fiala 2018). Такава практика можем да видим в учението на християнството, което казва: *„ако някой те удари по едната буза, предложи му и другата. Ако ти отнеме връхната дреха, остави му и ризата си“* (Евангелие на Лука 6:29). В по-ново време пример може да се даде с онази част от феминизма, която е основана на етиката на грижите. Нейните привърженици се противопоставят на онези мъжки разбирания, които са характерни за войнстващите култури, а именно „митологията“ за мъжествения справедлив воин, готов на саможертва и героична смърт (Ruddick 1995).

ЗАКЛЮЧЕНИЕ

Както видяхме, има много видове пацифизъм, минаващи от абсолютна крайност, през различни морални оправдания и извинения и накрая достигащи до идеята за формиране на цяла нова цивилизационна култура. В крайна сметка пресечна точка на всички тези течения е да се замени реалният свят, в който живеем, с някакъв по-добър, идеален. Това изцяло попада в сферата на утопиите. Буквално утопията е място (или в по-общото разбиране – идеал), което не съществува (от древногръцки). Абсолютният пацифизъм напълно се покрива с идеята за непостижим идеал, което го прави категоричен представител на утопичните идеи. Идеалният мир изисква идеални държави, населявани от идеални хора, които да притежават идеална разумност и алтруизъм, както и манталитет, водещи до спонтанно отсъствие на нужда от външна защита (Griffith 1939). Пацифизмът е неприложим като всички други утопии, които си поставят за цел да заменят реалния свят с някакъв идеален.

Идеята, че всички нации на земята едновременно могат да се откажат от войната, агресията и използването на сила, изглежда логична и дори юридически приложима, но има една голяма и непреодолима слабост, която е психологическа.

Ние, хората, се отнасяме към себеподобните с относително добре балансирано доверие и недоверие, увереност и страх. Същото се отнася и за връзките между човешките групи, като дори можем да заявим, че при тези взаимоотношения страхът е повече, доверието по-малко. Причина за това е, че групите като цяло са по-малко етични от индивида. Разумно погледнато, това е разбираемо, защото в нашата природа има както добродетели, така и пороци. Съотношението между тях е достатъчно променливо, че да предизвика както доверие, така и страх. Социалната основа на живота ни предполага да имаме доверие помежду си и ние сме се научили на него, защото в противен случай социалният живот би бил унищожен. Но също така проницателното и продължително натрупване на опит е показало, че ако доверието е доведено до крайност, то съвсем възможно е да предизвика агресия и да подтикне към нечестност. Тоест ние сме в постоянен сблъсък с две сили. От едната страна са страховете, комплексите, несигурността, които могат напълно да унищожат склонността ни да се доверяваме. От другата са твърденията, че хората са склонни да бъдат това, за което ние ги мислим, че са надеждни само когато им вярваме, че обичат само когато са обичани. Привържениците на това мислене винаги се стремят не просто да укрепят силите на добродетелта, но и да преодолеят всяко развитие на злото, което не е осъзнало и овладяло този възглед. Резултатите от подобен тип философия можем да видим многократно назад в историята. Нека само припомним католическата инквизиция или европейските тоталитарни режими от XX в.

Тези, които подкрепят каузата на пацифизма, на отсъствието на несъпротива и на взаимно доверие, настояват, че ако една нация реши да се разоръжи, с което да демонстрира доверие към другите, то тя успешно може да подтикне своите съседи към същото доверие, а оттам и към разоръжаване. На практика това е точно противоположното на базисната концепция за национална мощ (Денчев 2018; Ангелов 2024). Най-яркият пример за абсолютната безпочвеност на това твърдение е разиграният вариант между британския премиер и пацифист Невил Чембърлейн и германския канцлер Адолф Хитлер на срещата в Мюнхен през 1938 г. Прословутият документ *„Мир за нашето време“*[4] трябва да предотврати избухването на нова война в Европа. Това е епилог на последователната британска *„политика на умиротворяване“,* започната след Първата световна война, която цели с политически, икономически и териториални отстъпки да се избегне въоръжен конфликт. Успоредно с това протича и процес на разоръжаване, който трябва да спечели доверието на съседните държави. По повод документа *„Мир за нашето време“* Уинстън Чърчил[5] се обръща към премиера с пророчески думи: „*Вие имахте да избирате между войната и позора. Вие избрахте позора. Но вие ще получите и войната!“.* Всъщност пацифистката политика, наложена след Първата световна война, до голяма степен е в основата на катастрофата, до която ни доведе Втората световна.

Защитата на живота, на достойнството и на собствеността ни е неизменно право.[6] Нима не е естествено към това да добавим борбата с робството, с тиранията и за свободата… Още св. Августин от Хипо[7] определя войната като справедлива, когато каузата, за която се води, е справедлива. В наше време това е развито в теорията за *„Справедливата война“,* която се основава на справедлива кауза. Именно тя, Справедливата война, е моралният отговор на Пацифизма.

БЕЛЕЖКИ

[1] Трябва да отбележим, че самият Кант определя тази своя теория като утопична.

[2] Теорията за справедливата война е етична рамка, използвана за определяне кога е допустимо да се води война. Тя е обвързана със *„справедливата кауза“,* която може да е борбата за свобода, за защита на достойнството, защита на фундаменталните човешки права и прочее.

[3] Старши научен сътрудник в Института по етика на Оксфордския университет.

[4] Известно и като Мюнхенско споразумение, то изпълнява претенции на Германия за анексиране на части от Чехословакия, с което Чембърлейн се надява да не се стигне до война.

[5] Британски политик и държавник, премиер на Великобритания по време на Втората световна война, единствената държава, воювала с Хитлер през целия период на конфликта.

[6] Общото събрание на ООН през 1948 г.; още в първия параграф се казва, че *„признаването на човешкото* ***достойнство*** *на всички хора е в основата на справедливостта и мира в света“.*

[7] Св. Августин от Хипо е една от най-важните личности в развитието на западното християнство.

ЛИТЕРАТУРА

Ангелов, Г. (2022). *Държавност и национална сигурност.* София: Военно издателство, 208 с. ISBN 978-954509-584-9.

Ангелов, Г. (2024). Някои аспекти на националната мощ на съвременната държава. *Национална сигурност,* с. 15–21, ISSN 2682-941X; ISSN 2682-9983.

Денчев, Стоян, Груди **Ангелов** (2018). Базова концепция за националната мощ. – В: *Сборник научни доклади от годишна научна конференция на факултет „Национална сигурност и отбрана“, 17–18 май 2018 г.* София: Военна академия „Г. С. Раковски“, I Ч., с. 13–19, ISBN 978-619-7478-05-1.

Andregg, M. (2018). 48th Annual ISCSC Conference Soochow University, Suzhou, China June 15–17, 2018. Proceedings: How to Escape Thucydides's Trap: A Dialogue Among Sages. *Comparative Civilizations Review, (79),* pp. 114–129, ISSN 0733-4540.

Boersema, D. (2017). *Positive and Negative Peace.* The Routledge Handbook of Pacifism and Nonviolence, Andrew Fiala (ed.). New York: Routledge, ISBN 9781138194663.

Fiala, A. (2010). *Public War. Private Conscience: The Ethics of Political Violence.* London: Continuum, ISBN 9781441182586.

Fiala, A. (2018). The Pacifist Tradition and Pacifism as Transformative and Critical Theory. *The Acorn 18 (1)*, 5–28.

Fiala, A. (2018). *Transformative Pacifism: Critical Theory and Practice.* Bloomsbury Publishing, ISBN 9781350039209.

Fiala, A. (2014). Contingent Pacifism and Contingently Pacifist Conclusions. *Journal of Social Philosophy, 45(4),* ISSN 1467-9833.

Fox, M. Allen (2014). *Understanding Peace: A Comprehensive Introduction.* New York/London: Routledge. ISBN 10 0415715709.

Griffith, G. O. (1939). Absolute Pacifism. *Baptist Quarterly, 9(8),* pp. 468–474, ISSN 2056-7731.

Holmes, R. (1999). Pacifism for Nonpacifists. *Journal of Social Philosophy,* ISSN 1467-9833.

Kellenberger, J. (1987). A Defense of Pacifism. *Faith and Philosophy, 4(2),* pp. 129–148, ISSN 2153-3393.

Reitan, E. (2000). Personally Committed to Nonviolence: Toward a Vindication of Personal Pacifism. *The Acorn 10 (2),* 30–41.

Ruddick, S. (1995). *Maternal Thinking: Toward a Politics of Peace.* Boston Boston: Beacon Press, ISBN-10 0807014095.
Russell, B. (1943). The Future of Pacifism. *The American Scholar 13, no. 1,* ISSN 00030937.
Ryan, C. (1983). Self-Defense, Pacifism and Rights, Ethics 93, 508-24, ISSN 0014-1704.

REFERENCES

Andregg, M. (2018). 48th Annual ISCSC Conference Soochow University, Suzhou, China June 15–17, 2018. Proceedings: How to Escape Thucydides's Trap: A Dialogue Among Sages. *Comparative Civilizations Review, (79),* pp. 114–129, ISSN 0733-4540.
Angelov, G. (2022). *Darzhavnost i natsionalna sigurnost.* Sofia: Voenno izdatelstvo, 208 s. ISBN 978-954-509-584-9.
Angelov, G. (2024). Nyakoi aspekti na natsionalnata mosht na savremennata darzhava. *Natsionalna sigurnost,* s. 15–21, ISSN 2682-941X; ISSN 2682-9983.
Boersema, D. (2017). *Positive and Negative Peace.* The Routledge Handbook of Pacifism and Nonviolence, Andrew Fiala (ed.). New York: Routledge, ISBN 9781138194663.
Denchev, Stoyan, Grudi **Angelov** (2018). Bazova kontseptsia za natsionalnata mosht. – V: Sbornik nauchni dokladi ot godishna nauchna konferentsia na fakultet „Natsionalna sigurnost i otbrana", 17–18 may 2018 g. Sofia: Voenna akademia „G. S. Rakovski", I Ch., s. 13–19, ISBN 978-619-7478-05-1.
Fiala, A. (2010). *Public War. Private Conscience: The Ethics of Political Violence.* London: Continuum, ISBN 9781441182586.
Fiala, A. (2018). The Pacifist Tradition and Pacifism as Transformative and Critical Theory. *The Acorn 18 (1)*, 5–28.
Fiala, A. (2018). *Transformative Pacifism: Critical Theory and Practice.* Bloomsbury Publishing, ISBN 9781350039209.
Fiala, A. (2014). Contingent Pacifism and Contingently Pacifist Conclusions. *Journal of Social Philosophy, 45(4),* ISSN 1467-9833.
Fox, M. Allen (2014). *Understanding Peace: A Comprehensive Introduction.* New York/London: Routledge. ISBN 10 0415715709.
Griffith, G. O. (1939). Absolute Pacifism. *Baptist Quarterly, 9(8),* pp. 468–474, ISSN 2056-7731.
Holmes, R. (1999). Pacifism for Nonpacifists. *Journal of Social Philosophy,* ISSN 1467-9833.
Kellenberger, J. (1987). A Defense of Pacifism. *Faith and Philosophy, 4(2),* pp. 129–148, ISSN 2153-3393.
Reitan, E. (2000). Personally Committed to Nonviolence: Toward a Vindication of Personal Pacifism. *The Acorn 10 (2),* 30–41.
Ruddick, S. (1995). *Maternal Thinking: Toward a Politics of Peace.* Boston Boston: Beacon Press, ISBN-10 0807014095.
Russell, B. (1943). The Future of Pacifism. *The American Scholar 13, no. 1,* ISSN 00030937.
Ryan, C. (1983). Self-Defense, Pacifism and Rights, Ethics 93, 508-24, ISSN 0014-1704.

PACIFISTS DO NOT ACCEPT WAR, BUT IS PACIFISM ACCEPTABLE?

Abstract: *I do not consider it is likely that there are mentally normal, sane and sane people who would support war and violance in general. But violence exists, and more, it is a constant companion in life on Earth. Is it possible to change this? Pacifist movements direct their efforts in this direction and set themselves the goal of freeing humanity from war and violence. This article examines the different types of pacifism, such as absolute and conditional, maximal and minimal, universal and particular, skeptical and apparent, and finally transformational, as well as their varieties, to seek an answer to the question "Is pacifism acceptable?". The complete rejection of war as a means of resolving conflicts, its moral condemnation, as well as the condemnation of all violence, the inextricable connection of peace with the dignity of people can be seen as a noble and lofty ideal.Are these good intentions, this lofty ideal, not the basis of yet another inaplicable utopia? And may not its practical application lead us to disaster?*
Keywords: *pacifism, types of pacifism, morality, ethics, war*

Neno Dimov, PhD
University of Library Studies and Information Technologies
E-mail: dimov.neno@gmail.com

НАЦИОНАЛНА СИГУРНОСТ
NATIONAL SECURITY

ЗАЩИТА НА ЛИЦАТА, СИГНАЛИЗИРАЩИ ЗА НЕРЕДНОСТИ – ПРЕДИЗВИКАТЕЛСТВА ПРЕД НЕОБХОДИМОСТТА ОТ ПО-СОЛИДНА ЗАЩИТА И ВЪЗМОЖНИТЕ РЕШЕНИЯ

Стойчо Георгиев
Университет по библиотекознание и информационни технологии

Резюме: *Без важната информация, разкрита от подателите на сигнали за нередности, значителна част от съвременните институционални и корпоративни скандали, свързани с нарушения срещу обществения интерес, нямаше да се случат. Безспорно е, че сигнализирането, веднъж пуснато в публичното пространство, е в състояние да причини непредвидени и непоправими вреди и да надвисне като дамоклев меч в биографията на подателите, което може да доведе до загуба на работното място или на финанси, да засегне аспекти от личния живот, а в някои по-тежки случаи и до здравословни проблеми. Дори подаващият сигнал за нарушение да действа добросъвестно, той рискува да бъде публично осъден и репутацията му да остане опетнена от липса на адекватна защита. Сигнализиращите лица могат дори да бъдат доведени до пълна изолация или да платят с живота си или с този на семействата си. Имат ли достъп до защита тези субекти и каква е връзката на Комисията за защита на личните данни в качеството ѝ на централен орган за външно подаване на сигнали? При какви условия лице, подаващо сигнал за нарушения чрез вътрешен или външен канал по смисъла на законодателството, ще има право на защита? Европейският съюз е положил основите на законодателство със съвременни правила и регулации с цел по-добра защита за лицата, докладващи за нередности, чрез въвеждането на тристранна система за подаването на сигнали от такъв характер, възприета и прилагана от българските компетентни органи.*

Ключови думи: *сигнали за нередности, механизми за защита, засегнати лица, защита на сигнализиращите, гражданско общество*

ВЪВЕДЕНИЕ

В съвременния динамичен свят корупционните действия и неправомерното поведение продължават да се разглеждат като сложни явления, свързани основно с публичния характер на властта. В определени ситуации тези процеси се развиват и в дейността на частните и гражданските организации. По своята същност те следва да се дефинират като девиантно поведение, което се разминава с възприетите обществени норми. Тези деструктивни постъпки с основание смущават гражданското общество и в тази връзка следва да бъдат предприети корективни действия от страна на законодателните и правоприлагащите органи, които да бъдат адекватни спрямо предизвикателствата пред защитата на лицата, подаващи сигнали или публично оповестяващи информация за нарушения (застрашаващи или увреждащи обществения интерес) на българското законодателство или на актове на Европейския съюз.

От съществено значение е действията на компетентните органи да бъдат съобразени и съгласно перспективите, пред които са изправени гражданите, публичните институции и частните организации при прилагане на способите за докладване и приемане на сигнали за нарушения. В настоящото изследване се разглеждат някои важни аспекти от националното и наднационалното

законодателство, касаещи условията, реда и мерките за защита на лицата в публичния и в частния сектор, които подават сигнали или публично оповестяват информация за нередности, и при какви условия се подават и разглеждат докладваните сигнали. Целта на настоящата статия е да се направи опит за систематизиране на минималните стандарти, на които следва да отговарят тези предпоставки, и да се изследват възникващите слабости и/или недостатъци в практиката по прилагането на този нов за нашата страна механизъм за защита на определен кръг лица. Представят се предложения за нестандартни и нетрадиционни решения за отстраняване на част от изложените отрицателни явления, като се посочват добрите практики на различни национални законодателства на държави както от ЕС, така и на страни с юрисдикции извън рамките на Съюза.

ЗНАЧЕНИЕТО НА ЛИЦАТА, ПОДАВАЩИ СИГНАЛИ ЗА НЕРЕДНОСТИ, ОТНОСНО РАЗКРИВАНЕ НА НАРУШЕНИЯ В ПОЛЗА ЗА ГРАЖДАНСКОТО ОБЩЕСТВО

Институционалните и корпоративни нарушения на законодателството са голямо предизвикателство както в развиващите се, така и в развитите икономики, а лицата, подаващи сигнали за нарушения и нередности, заемат важна роля в разкриването им. На практика въпросът за защитата на тези лица се възприема с приоритет в международните програми за борба с корупцията, например в обхвата на групата Г-20, обединяваща 20-те най-големи и най-бързо развиващи се икономики, Съвета на Европа, ОИСР и много други съвременни организации. От друга страна, национални законодателства за защита на лицата, сигнализиращи за нередности, вече съществуват и в страни като България. Резултатите показват, че защитата на лицата, сигнализиращи за нередности, действително насърчава докладването на неправомерното поведение, но последиците от тази защита в полза на откриване и възпиране на девиантното поведение имат сложен по своето естество характер.

Проучвания, проведени от Европейската комисия през 2017 г.[1], установяват, че на терена само на обществените поръчки годишната загуба на потенциални ползи за правилното функциониране на единния пазар ще бъде в диапазона от 5,8 до 9,6 милиарда евро. Освен това само по отношение на въздействието върху бюджета на ЕС, предназначен за превенция на измами и корупция, текущият риск от загуба на приходи се оценява на между 179 и 256 милиарда евро годишно. Защитата на лицата, сигнализиращи за нередности, е с необходимост да допринася за по-ефективно данъчно облагане в ЕС чрез борба с избягването на данъци. Последното води до загуби на данъчни приходи за държавите членки и Съюза от около 50 до 70 милиарда евро годишно. Това доказателство предполага, че разкриването на съществуващи нередности и възпирането на потенциални нарушения на законите следва да бъдат с висок приоритет за законодателите и политиците.

В действителност през последните години става все по-очевидно значението на лицата, подаващи сигнали за нередности (които не участват в неправомерното поведение), за разкриване на нарушения главно поради достъпа им до важна информация (по-специално по отношение на нарушенията, извършвани от служители в публичните или частни организации).

„Информация за нарушение“[2] е информация, включваща основателни подозрения за действителни или потенциални нарушения, които са извършени или е много вероятно да бъдат извършени в организацията, в която работи или е работило сигнализиращото лице, или в друга организация, с която то е или е било в контакт по време на работата си, както и за опити за прикриване на нарушения. Служителите, които съобщават за нередности, обичайно чувстват морално задължение да го направят, но страхът от отмъщение на колегите или ръководството често се оказва силен възпиращ фактор. В резултат на това общата им готовност да съобщават за неправомерно поведение често бива възприемана като ниска. Вследствие на тези предпоставки препоръките за най-добри практики на международните органи са в насока за всеобхватна правна защита при наличие на ответни репресивни действия от страна на разобличените нарушители.

Няма съмнение, че разобличителите на потенциални нарушители заслужават силна защита и точно в това е целта на съвременните регулации, обособени в законодателството на ЕС, които правни норми са транспонирани и адаптирани към българската нормативна база.

НАЦИОНАЛЕН И НАДНАЦИОНАЛЕН ПРАВЕН МЕХАНИЗЪМ ЗА ЗАЩИТА НА ЛИЦАТА, ПОДАВАЩИ СИГНАЛИ

С цел ефективни мерки за защита на лицата, които съобщават за нарушения на правото на Съюза, европейските законодатели издават **Директива (ЕС) 2019/1937 на Европейския парламент и на Съвета от 23 октомври 2019 г.**[3] (т.нар. Wistleblower Directive). В директивата е указано, че европейските законодатели разполагат с две години на национално ниво за транспониране на разпоредбите ѝ в националните законодателства за защита на лицата, сигнализиращи за нарушения. Съвременната характеристика на този основен правен акт за защита на подателите на сигнали е задължението за създаване на вътрешни канали за сигнализиране на нередности за юридически лица в публичния и частен сектор с най-малко 50 или повече служители. В публичния сектор държавите членки могат да освободят общини с по-малко от 10 000 жители или по-малко от 50 служители, работещи в публичния орган, от задължението за създаване на канали за сигнализиране на нарушения. В обяснителния меморандум[4] към предложената директива са изброени няколко положителни икономически ефекта от включването на правила за защита на лицата, подаващи сигнали за нередности.

С цел транспонирането разпоредбите на директивата в българското законодателство на 27 януари 2023 г. 48-ото Народно събрание приема **Закон за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения** – **ЗЗЛПСПОИН**[5] (т.нар. Wistleblower Protection Act). Законът е обнародван в бр. 11 на „Държавен вестник“ от 2 февруари 2023 г. и влиза в законна сила на 4 май 2023 г. С този закон се уреждат условията, редът и мерките за защита на лицата в публичния и в частния сектор в Република България, които подават сигнали или публично оповестяват информация за нарушения на българското законодателство или на актове на Европейския съюз, които застрашават или увреждат обществения интерес, както и редът и условията за подаване и разглеждане на такива сигнали или публично оповестена информация. Законът е широкообхватен и има за цел да осигури защитата на лицата в публичния и в частния сектор, които подават сигнали или публично оповестяват информация за нарушения на българското законодателство или на актове на Европейския съюз, станала им известна при или по повод изпълнение на трудовите или служебните им задължения, или в друг работен контекст, като разпоредбите са съобразени изцяло с директивата. След приемането на **ЗЗЛПСПОИН** и възникналите множество затруднения и неясноти по повод прилагането му в практическата дейност на публичния и частния сектор се налага неговото изменение на няколко пъти, като последното е от 20 октомври 2023 г.

МЕТОДИ ЗА ИЗВЪРШВАНЕ НА ПРОВЕРКИ И ПРЕДПРИЕМАНЕ НА АДЕКВАТНИ ДЕЙСТВИЯ ПО ВСЕКИ ПОСТЪПИЛ СИГАНАЛ

По отношение на идентифицирането на рисковете каналите за докладване на нередности са средство за подпомагане при установяването на нарушения в частния и публичния сектор. Поради това е с характер на задължителност за всички организации, които покриват условията на закона (и препоръчително за тези, които са със структура и форма на управление извън наложените изисквания), установяване на канали за докладване на лица, подаващи сигнали за нередности, независимо дали тези канали са под надзора на звена за човешки ресурси, правен отдел, дирекция за одит, надзорен орган или под всякаква друга структурна форма на функциониране. Каналите за докладване на нередности могат да позволят на подателите на сигнали да ги депозират писмено (чрез специално изготвен за конкретното действие формуляр, одобрен от КЗЛД), включително чрез електронна поща (т.е. чрез докладване на нередности по канал, установен в интернет и/или интранет на компанията) или устно (по телефон или чрез други системи за гласови съобщения), или в други случаи подателят може да се свърже със служител, отговорен за получаване на доклади за сигнализиране в зависимост от организационната форма на институцията.

От друга страна, ако съществува основателно предположение, че за сигнализиращото лице е налице риск от ответни, дискриминиращи го действия, както и че вероятността за предприемане на ефективни мерки за проверка на сигнала не е висока, съществува възможност същият да бъде подаден чрез канал за външно подаване на сигнали по смисъла на законодателството. Централен

орган за външно подаване на сигнали и за защита на лицата, на които такава защита се предоставя съгласно закона, е **Комисията за защита на личните данни.**

Предоставен е и друг способ за сигнализиране за нарушения чрез публично оповестяване на информация за нередности, като лицата, които публично оповестяват такава информация, освен със закрилата на закона за защита, се ползват и с установената в Конституцията закрила за свободно разпространяване на информацията.

Много важно условие е всяко обработване на лични данни, извършено по силата на този закон, включително обмен или предаване на лични данни от компетентните органи, да се извършва в съответствие с **Регламент (ЕС) 2016/679[6],** а когато в предаването участват институции, органи, служби или агенции на Европейския съюз – в съответствие с **Регламент (ЕС) 2018/1725[7],** както и със **Закона за защита на личните данни** – **ЗЗЛД[8].**

Включването на канали за докладване за лица, сигнализиращи за нарушения, чрез системи за управление на сигнали за нередности не е нещо ново и отдавна се счита за основен елемент в структурните рамки на ефективни програми за съответствие с минималните стандарти за изпълнение в нормативната база, служеща за защита на гражданското общество на всяка държава – членка на ЕС. Работата с подателите на сигнали в европейските публични институции и мултинационалните компании е многостранна и се счита за уникална по силата на самия предмет, тъй като лицата, подаващи сигнали за нередности, принадлежат към различни култури, броят и качеството на функциите на гражданите, участващи в оформянето на сигналите, са разнородни. От друга страна, предизвиква интерес и въздействието, което може да бъде причинено от жалба, подадена от лице (подател на сигнала), във връзка с последващи прояви на репресия от страна на засегнатите лица. Следва да се има предвид, че **„засегнато лице“[9]** по смисъла на закона е физическо или юридическо лице, което се посочва при подаването на сигнала или при публичното оповестяване на информация като лице, на което се приписва нарушението или с което това лице е свързано.

ВЪЗНИКВАНЩИ ПРОБЛЕМИ И НЕДОСТАТЪЦИ ВЪВ ВРЪЗКА С ОСИГУРЯВАНЕТО НА ПОВЕРИТЕЛНОСТ И НАДЕЖДНА ЗАЩИТА НА ЛИЦАТА, СИГНАЛИЗИРАЩИ ЗА НЕРЕДНОСТИ

Съгласно изложеното дотук може да се изведе заключение, че настоящите способи за докладване по **ЗЗЛПСПОИН** са адекватни, тъй като лицата, сигнализиращи за нередности, имат възможността да сигнализират, например по електронна поща, телефон и чрез директна среща с компетентен служител, притежаващ правомощия по смисъла на закона. Това ниво на сигурност колкото и широкообхватно да е обаче, не съответства за покриване изискванията на Директивата за защита на лицата, които съобщават за нарушения.

Сигнализирането чрез личен, а дори и служебен имейл адрес или по телефона включва при всички положения разкриване на самоличността или е с риск от лесно идентифициране на подателя на сигнала. Това обстоятелство може да възпре разобличителите поради често обземащия ги основателен страх от последиците от идентифицирането.

Въпреки това оперирането чрез напълно анонимна платформа за докладване ще може да предостави възможността за изграждане на доверие между сигнализиращия и организацията, като по този начин съответно ще се увеличи броят на сигналите. В дългосрочен план това се очертава да е подходящ начин да се гарантира, че организациите ще могат да осъществяват дейността си в спокойна обстановка и без наличието на корупционни практики.

Българското законодателство като цяло изисква лицата, подаващи сигнали за нередности, да се идентифицират. Член 9 от **ЗЗЛПСПОИН** предпоставя пречки за образуване на производство по анонимни сигнали и сигнали, отнасящи се до нарушения, извършени преди повече от две години. Европейската директива също така оставя отворен въпроса за анонимните доклади. Това е възможност, която всяка държава членка трябва да вземе като решение съгласно собственото си законодателство. Ако държавите разрешават анонимни сигнали, те все пак ще следва да бъдат обект на специални правила. Съгласно действащите разпоредби на закона подателят на сигнала е

длъжен да предостави своето име и адрес и да декларира, че прави уведомлението добросъвестно за обстоятелствата, за които има знания или основателни причини да смята, че са достоверни, като на същия се предоставят определени права. Една от най-важните разпоредби на закона обаче е, че ако сигнализиращият не предостави своето име и адрес, получилите сигнала организации имат правото да се въздържат от разследване по него. Това очевидно не обслужва интересите на разобличителите, които по-скоро предпочитат анонимността.

Наблюдават се и други недостатъци в законодателната рамка, като например сигнализиращ, който разкрива силно чувствителна информация или класифицирани под ниво на сигурност данни и материали, който не разполага със способи за специална защита. От друга страна, относително незащитени остават и тези, които съобщават за неправомерни действия чрез медиите или извършват някакъв вид нарушение в служебната си дейност, за да се снабдят с релевантна информация относно докладването за извършване на нередности и идентифициране на нарушителите. Не на последно място са и служителите на правоохранителните и правозащитни организации, които и към настоящия момент чувстват несигурност за подаване на сигнал при положение, че нарушават правилата на съответната структура чрез способите за сигнализиране за нередности. Всички тези лица с различни професии и дейности рискуват да платят твърде висока цена при вземане на решение да представят истината пред обществеността. В книгата „Разобличаване на промяната“ авторката Татяна Базичели (основател и директор на Disruption Network Lab в Берлин) описва различни истории за хора със специфични професии, които са променили изцяло живота си, често срещайки социална стигматизация и правно преследване след докладване за нарушения (Bazzichelli 2021).

Съдебната практика в България към настоящия момент е изключително оскъдна откъм съдебни решения, свързани с производства по **ЗЗЛПСПОИН,** тъй като лицата, които са подали сигнал или публично са оповестили информация за нарушение, очевидно не желаят да се възползват от това свое право. Все пак са налице няколко съдебни решения, които застъпват до някаква степен материята на сравнително новия закон (Решение № 187 от 16.01.2024 г. на Районен съд – Варна по гражданско дело № 1938/2023 г. по описа на съда, потвърдено в определени негови части с Решение № 310 от 26.03.2024 г. на Окръжен съд – Варна по гражданско дело № 415/2024 г.; Определение № 11161 от 08.07.2024 г. на Административен съд – София-град по дело № 3772/2024 г., касаещи казуси, свързани с искане за защита), но въпреки изминалия относително продължителен срок от влизането в сила на закона, не се наблюдава сериозно наличие на производства по него.

Тази фактическа обстановка при липса на сигнали и производства доказва, че лицата, сигнализиращи за нередности в България, предпочитат анонимността и не желаят да се възползват от правото да подсилят обществения интерес за намаляване на нивото на нарушения и корупционни действия.

Законът също така не предоставя възможности за финансова подкрепа за подателите на сигнали, които са изправени пред ответни репресивни мерки. Повечето европейски правителства отдавна се чувстват неудобно от идеята за изплащане на парични награди на лицата, подаващи сигнали за нередности, въпреки че има някои забележителни изключения, включително Унгария, Словакия и Полша. Освен това Директивата на ЕС за разобличаване, която сега е приложена в целия Европейски съюз, не предвижда възнаграждаване на сигнали за нередности. Ситуацията е различна в Съединените щати, където има четири основни програми за възнаграждение на лицата, сигнализиращи за нередности в съответни икономически сектори, с различни правила и процедури, като подобни схеми за възнаграждение са възприети от канадските, австралийските и южнокорейските регулатори. В САЩ тези програми изпитват възходяща тенденция в отчитането на положителни резултати. В края на 2022 г. програмата SEC на Комисията по ценните книжа и фондовите борси на САЩ съобщава, че е изплатила 1,3 млрд. долара на 328 разобличители през последното десетилетие, като тези рекордни суми неизбежно фокусират вниманието върху въпроса дали е правилно да се стимулира финансово разобличаването. В допълнение, проучванията, проведени през последните години, потвърждават, че програмите за възнаграждение на лицата, подаващи сигнали за нередности в САЩ, са работили добре и са увеличили разкриването и възпирането на престъпността по икономически ефективен начин. От извършените изследвания

и проучвания в последните години става ясно, че страните, които предлагат награди, изпращат позитивен сигнал към лицата, подаващи сигнали, че тяхната информация е ценна и че техните права и защита се приемат сериозно.[10]

Възможните решения са публичните или частни организации, при които постъпва сигналът, да разполагат със свободата да решават дали да предложат начин за анонимно или частично анонимно сигнализиране, тъй като законодателят не е успял да дефинира такъв вариант. Вътрешният канал за докладване също следва да има способност да обработва анонимни сигнали, като формата на самоличност на лицата, сигнализиращи за нередности, и лицата, засегнати от доклада, да подлежат на специална закрила. Изключения следва да са възможни само при наличие на условия за наказателно преследване на сигнализиращото лице или когато лицето съзнателно е подало сигнал с невярна информация или публично е оповестило невярна информация, доказано с процедура чрез справедлив съдебен процес.

От друга страна, защо България да не последва добрите практики на посочените по-горе в изложението държави, намиращи се извън ЕС, и да създаде законодателна основа за финансово стимулиране на лицата, подаващи сигнали за нередности. Някои страни в ЕС вече успешно прилагат механизми за изплащане на парични награди при „резултатно“ докладване за нарушения. Тъй като подателите на сигнали страдат лично и професионално при условие, че решат да говорят открито, те често губят работата си и могат да бъдат отлъчени от професията си. В резултат на това може да им се наложи да заплатят значителна лична цена, като се превърнат в участници в процес с продължителност от много години. Някои инициатори на проучвания в областта на докладването за нарушения поддържат тезата, че финансовите награди на разобличителите ще ги подпомогнат за преминаването през тази финансова тежест. Том Мюлер, автор на книгата „Криза на съвестта: разобличаване в епоха на измама“, пише, че наградата е грешната дума (Mueller 2019). Писателят подчертава, че всяка финансова компенсация за разобличителите би била по-добре описана като „нетно настоящо плащане на еднократна стойност за загубена кариера“. Следователно има възможности за внедряване на платформа за предоставяне на парични стимули в справедлив размер на лица, които не са анонимни и са разкрили информация за неправомерни действия или злоупотреби по реда на **ЗЗЛПСПОИН**. Платформата ще има за цел да постигне баланс между предоставяне на атрактивни стимули и сериозни санкции срещу клевети, лъжесвидетелстване или подвеждащо представяне на информация, като се приемат строги стандарти на доказване срещу умишлена злоупотреба с предоставените на разобличителите права. В случай че няколко лица едновременно сигнализират за една и съща нередност или възникване на закононарушение, управляващият орган следва да има възможността да раздели финансовия стимул сред множеството сигнализиращи лица според приноса им в процеса на разкриване и елиминиране на последиците от нарушението.

ЗАКЛЮЧЕНИЕ

В сегашната действителност при наличието на „безброй“ публични и граждански организации, притежаващи неизмеримо влияние върху вземането на изключително важни и отговорни решения, свързани с обществено-икономическия живот, както и опериращи с колосални парични капитали, е от огромно значение механизмите за защита на лицата, сигнализиращи за нередности, да осигуряват в пълен обхват закрила от последващи репресивни и злонамерени действия.

От незначителния брой получени сигнали (съответно и образувани производства) следва несъмненият извод, че липсата на популярност и участие на заинтересованите страни води до неефективно законодателство с множество предизвикателства, свързани с прилагането му. Желателно е да бъдат създадени условия за улеснение и насърчаване на лицата, подаващи сигнали за нередности, както и да бъдат провеждани специфични кампании за информиране на обществеността за общото благо. Основната цел е предпазване на обществото от прояви на икономически вреди и деморализиращи действия, особено в страни като България, където все още цивилизационното възприятие за разобличителите е отрицателно и те продължават да се разглеждат като доносници или дори шпиони. Безспорно е обстоятелството, че без силна и

ефективна защита на лицата, подаващи сигнали или публично оповестяващи информация за нередности, корупцията и неправомерните действия могат да се развиват дори в среда, в която други субекти са наясно с тези противоправни явления. Поради изложените негативни изводи следва да се изменят и допълнят някои от предпоставките за защита на сигнализиращите лица с оглед приемането на един солиден правен акт, което ще бъде съществена стъпка към осигурена защита на гражданите и институциите от злоупотреби и негативни прояви. В дългосрочен план приемането на надежден правен механизъм ще гарантира, че организациите и учрежденията ще могат да осъществяват дейността си прозрачно и без корупционни практики, което от своя страна ще легитимира България като предвидим стратегически партньор със съвременно и конкурентно законодателство за защита на гражданското общество и неговите институции.

БЕЛЕЖКИ

[1] Estimating the economic benefits of whistleblower protection in public procurement – Final report. https://op.europa.eu/en/publication-detail/-/publication/8d5955bd-9378-11e7-b92d-01aa75ed71a1/language-en.

[2] ЗЗЛПСПОИН – обн. ДВ, бр. 11/02.02.2023 г., изм. и доп. ДВ, бр. 88/20.10.2023 г. – § 1, т. 3 от Допълнителните разпоредби.

[3] По-подробно вж. Директива (ЕС) 2019/1937 на Европейския парламент и на Съвета от 23 октомври 2019 г. относно защитата на лицата, които подават сигнали за нарушения на правото на Съюза.

[4] По-подробно за обяснителния меморандум към Директивата вж. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0218&from=DA.

[5] Закон за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения – обн. ДВ, бр. 11/02.02.2023 г., последно изм. и доп. ДВ, бр.88/20.10.2023 г.

[6] По-подробно вж. Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защита на данните).

[7] Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО.

[8] ЗЗЛД – обн. ДВ, бр. 1/2002 г., последно изм. и доп. ДВ, бр.84/06.10.2023 г.

[9] ЗЗЛПСПОИН – обн. ДВ, бр. 11/02.02.2023 г., изм. и доп. ДВ, бр.88/20.10.2023 г. – § 1, т. 5 от Допълнителните разпоредби.

[10] За повече подробности вж. https://www.integrityline.com/expertise/blog/ethics-behind-whistleblower-rewards/.

REFERENCES

Mueller, T. (2019). *Crisis of Conscience: Whistleblowing in an Age of Fraud.* Published by Riverhead Books.

Bazzichelli, T. (2021). *Whistleblowing for Change: Exposing Systems of Power and Injustice.* Transcript Verlag.

PROTECTION OF WHISTLEBLOWERS – CHALLENGES FACING THE NEED FOR STRONGER PROTECTION AND POSSIBLE SOLUTIONS

Abstract: *Without the important information disclosed by whistleblowers, a significant proportion of contemporary institutional and corporate scandals involving violations against the public interest would not have occurred. It is undeniable that whistleblowing, once released into the public space, is capable of causing unforeseen and irreparable harm and hanging like a sword of Damocles in the biography of the senders, which can lead to the loss of a job or finances, affect aspects of private life, and in some more severe cases to health problems. Even if the whistleblower acts in good faith, he or she risks being publicly condemned and his or her reputation tarnished by a lack of adequate protection. Whistleblowers may even be placed in total isolation or pay with their lives or those of their families.Do these individuals have access to protection and what is the relationship of the Commission for the Protection of Personal Data in its capacity as a Central Whistleblowing Authority? Under what conditions will a person reporting violations through an internal or external channel in the sense of the legislation have the right of protection?The European Union has laid the foundations for legislation with modern rules and regulations to better*

protect whistleblowers by introducing a tripartite whistleblowing system adopted and implemented by the Bulgarian competent authorities.
Keywords: *Signals of irregularities, protection mechanisms, affected individuals, protection of whistleblowers, civil society*

Stoycho Georgiev, PhD candidate
University of Library Studies and Information Technologies
E-mail: adv_st.georgiev@abv.bg

НАЦИОНАЛНА СИГУРНОСТ
NATIONAL SECURITY

SYSTEMATIC RISK MANAGEMENT IN GERMAN MUNICIPALITIES

Jonas Heesch
University of Library Studies and Information Technologies

Abstract: *The article analyzes the importance and necessity of systematic risk management in German municipalities. It is established that local authorities, like companies, are exposed to a variety of risks, including financial, personnel, IT and reputational risks. Despite these risks, unlike private companies, there are no legal requirements for systematic risk monitoring in the public sector. The following section provides a rough description of the structure of municipal risk management, from the creation of a risk mission statement and risk inventory through to risk assessment and the implementation of measures.It is pointed out that both preventive and detective measures are required for effective risk management. In addition, the importance of a risk culture within the administration and the active involvement of managers and employees is emphasized. Particular attention is paid to the need for the use of IT-supported systems in larger administrations, while existing measures are often sufficient in smaller municipalities. The article concludes by stating that an unprepared crisis situation such as the recent pandemic leads to avoidable errors and inefficiencies.*
Keywords: *Municipality, risk monitoring, risk management system, risk mission statement, risk inventory, risk assessment*

INTRODUCTION

German municipalities also face risks, just like companies. Slumps in trade tax and staff problems can lead to reputational damage.

Many local authorities initially appear to be insufficiently prepared for the latest risks. Even outside of the recent pandemic, municipal action is associated with risks. The retirement of the baby boomer generation, the demands of digitalization and the risks of climate change could lead to staff shortages in the near future. However, financial risks or IT security risks have not yet been taken into consideration.

It is striking that public bodies, unlike the private sector and public companies, have no statutory requirements for risk monitoring and management. Although the municipal budget regulations of the federal states often require statements on opportunities and risks in the management report/financial report, in practice these statements are often limited to generalities and the obvious. For example, it is pointed out that cost increases in construction projects are possible and that there is a threat of interest rate increases for municipal loans, but there is no systematic basis.

In contrast to private-sector companies, insolvency is ruled out by law for municipalities, cities and districts. Nevertheless, the risks to which they are exposed should be analyzed systematically.

RESEARCH METHODOLOGY

The occurrence of events that result in a negative deviation from a specific target, is referred to as a ‘risk’. An ‘opportunity’ is an event that brings you closer to your goal than expected (Seidel 2011, 26). For this reason, risks and opportunities are not limited to the financial side of a municipality. Reputational risks, IT risks, political risks and personnel risks must also be taken into account. The primary task of risk management is to systematically avoid the unprepared occurrence of these and other risks.zu vermeiden. Successful risk management in the municipality requires a risk culture, which should be described in a mission statement for the municipality (Romeike/Hager 2020, 135). It should be emphasized that the topic

of 'risk management' is of fundamental importance for the municipality's managers. It is essential that the municipality's management board not only talks about risk management, but also supports and helps shape the process. Managers and employees should also be involved by acquiring expertise at different levels and transferring responsibility to the operational level.

Financial risks can cause public administrations to lose their ability to manage themselves. The higher-level authority (municipal supervisory authority) can take supervisory measures ranging from the obligation to draw up a budget protection concept to forced administration if a municipality is unable to balance its budget over several financial years. However, reputational risks can have a more subtle but equally lasting effect on the municipality.

Late-recognized cases of embezzlement in local government often lead not only to direct financial losses, but also to a loss of trust in the administration on the part of citizens. This can lead to a decline in voluntary commitment and less identification with the local authority. To prevent these risks, it is advisable to implement a municipal risk management system. The operational implementation of the risk management system begins with the risk inventory following the adoption of a risk mission statement by the local authority.

The aim of the risk inventory is to systematically identify potential risks, developments and trends that could jeopardize the realization of municipal objectives (Gräf 2011, 35).

In order to identify risks, it is advisable to use existing systems within the municipality, for example the organizational structure at department, division or office level. This structural risk identification within the organization helps to clearly address the risk. This organizational structural risk identification supports a clear addressing of the risk to a department and its managers as the 'risk owner'. Risk identification is illustrated below using an example process (risk inventory).

Table 1. Risk inventory (process)

Department	Environment	Object	Explanation	Responsible person
Building Authority	Allocation	Supplements	Significant supplements that are equivalent to a new contract award are subject to repeated tendering.	Max Mustermann

The next step involves a more detailed description of the identified risk and an initial rough assessment. An assessment is made as to whether the risk is relevant in the analyzed period or whether it cannot currently be taken into account. It must be taken into account that the expenditure for risk mitigation must always be commensurate with the consequences in the event of a risk materializing.

Table 2. Initial risk assessment (compliance risk)

Explanation	Detailed risk	Existence	Note
Supplements are erroneously updated on the basis of old contracts	Lack of technical expertise Different evaluation of offers	Relevant	…

A detailed assessment of the relevant risks should follow a rough risk assessment. The hazards to which the municipality is exposed without countermeasures must be documented (Gleißner 2022, 216).

In this phase, the probability of occurrence and the potential for damage are determined for each identified risk.

Table 3. Risk assessment (gross risk)

Probability of occurrence				Risk class	Potential damage
Frequency	Complexity	Personnel qualification	Technical support		
Frequent to very frequent annually.	High to very high complexity	Low qualification	Not available	Very high	…

Risk management can only be effective if there is an appropriate response to risks. Those responsible, both managers in the administration and those responsible for risk, must determine which measures have already been taken in the administration to manage risk. New measures should be established where there are gaps. For example, further training (Seidel 2011, 45) can be installed as an effective category of compliance measures (see Table 4).

Table 4. Measures (compliance measure category (Part I)

Measure Category	Previous measures	Enquiries	Possible measures	
			Preventive	Detective
Fortbildung	keine	…	Employee training, follow-up by Internal Audit	Contract award audit by Internal Audit

It is advisable to divide the measures into preventive and detective measures. Preventive measures help to avoid risks from the outset, while detective measures help to uncover risk situations that have already been realized.

It is often necessary to take additional measures to deal with risks that have not yet been taken into account (Diederichs 2023, 301). Finally, an assessment of the risks should be carried out after the application of measures (see Table 5).

Table 5. Measures with net risk (compliance measure category (Part II)

				Net risk
Result	Realization		Controls	Risk class
	Personal responsibility	Delegation		
…	Employee training	Contract award audit by Internal Audit	Internal audit	medium

It ensures that risks are systematically avoided or minimized by categorizing them and linking them

directly to measures and responsibilities.

A risk management system is not a rigid construct. Ongoing monitoring is required to regularly assess the effectiveness of the existing monitoring procedures both internally and externally (by internal audit) (DIIR Auditing Standard No. 2 2023, 14). Monitoring should essentially be a part of the risk management process that was planned in advance.

Incorporating the described processes of a risk management system into day-to-day municipal work requires a considerable amount of work. Those responsible must always bear in mind that local authority employees must be able to deal with risks. All local authorities have a large number of instructions and guidelines, such as the 'four-eyes principle', which in some cases has been extended to 12 or more eyes. However, there is often a lack of systematization and documentation.

During the last pandemic, it became clear that an unprepared crisis inevitably leads to avoidable errors and inefficiencies in dealing with the situation.

In larger administrations, IT-supported systems must be used. In smaller municipalities, however, it is often sufficient to record, structure and, if necessary, expand existing measures.

RESULT

There is an urgent need to establish systematic risk management in German municipalities in order to be prepared for a variety of challenges. In particular, financial risks, staff shortages due to demographic change, IT security threats and reputational risks require a structured approach. Although many local authorities recognize risks, there is often a lack of systematic and legally regulated risk monitoring, which can lead to inefficient action in crisis situations.

Preventive and detective measures and the establishment of a strong risk culture are crucial to the success of a risk management system. Managers and employees must be actively involved in the process and risk management processes must be consistently monitored and adapted. In larger administrations in particular, IT-supported systems should be used to optimize management, whereas in smaller local authorities, simplifying and structuring existing measures can often be sufficient.

CONCLUSION

In view of the increasing complexity of challenges such as digitalization, climate change and demographic change, the importance of professional risk management will continue to grow in the coming years. Local authorities must continuously develop their structures and processes in order to not only respond to risks, but also to recognize and exploit opportunities. New technologies such as artificial intelligence and machine learning could enable even more precise risk identification and assessment in the future. It may also become necessary to establish legal requirements for risk monitoring in public administration in order to ensure uniform standards and better prepare local authorities for future crises.

REFERENCES

Diederichs, M. (2023). *Risk management and risk controlling* (5. Aufl.). München: Vahlen.

Diederichs, M. (2023). *Risikomanagement und Risikocontrolling* (5. Aufl.). München: Vahlen.

DIIR – Deutsches Institut für Interne Revision e. V. (2023). *Revisionsstandard Nr. 2: Prüfung des Risikomanagementsystems durch die Interne Revision.* Version 2.1. Verfügbar unter: https://www.diir.de/content/uploads/2023/09/DIIR_Revisionsstandard_Nr._2_Version_2.1.pdf (Abruf: 15. April 2024).

DIIR – Deutsches Institut für Interne Revision e. V. (2023). *Auditing Standard No. 2: Audit of the risk management system by Internal Audit.* Version 2.1. Verfügbar unter: https://www.diir.de/content/uploads/2023/09/DIIR_Revisionsstandard_Nr._2_Version_2.1.pdf (Retrieval: 15. April 2024).

Gleißner, W. (2022). *Grundlagen des Risikomanagements: Handbuch für ein Management unter Unsicherheit.* Verlag Franz Vahlen.

Gleißner, W. (2022). *Fundamentals of risk management: Handbook for management under uncertainty.* Verlag Franz Vahlen.

Gräf, J. (2011). Risikomanagement: Umsetzung und Integration in das Führungssystem. In: Klein, A. (Hrsg.). *Risikomanagement und Risiko-Controlling* (S. 51–73). Freiburg: Haufe Lexware.

Gräf, J. (2011). Risk management: implementation and integration into the management system. In: Klein, A. (Hrsg.). *Risk management and risk controlling* (S. 51–73). Freiburg: Haufe Lexware.

Romeike, F. und P. **Hager** (2020). *Erfolgsfaktor Risiko-Management 4.0: Methoden, Beispiele, Checklisten Praxishandbuch*

für Industrie und Handel. Wiesbaden: Springer Gabler.
Romeike, F. und P. **Hager** (2020). *Risk management as a success factor 4.0: Methods, examples, checklists Practical handbook for industry and trade*. Wiesbaden: Springer Gabler.
Seidel, U. M. (2011). Grundlagen und Aufbau eines Risikomanagementsystems. In: Klein, A. (Hrsg.). *Risikomanagement und Risiko-Controlling: Moderne Instrumente, Grundlagen und Lösungen* (S. 21–50). Freiburg: Haufe Lexware.
Seidel, U. M. (2011). Fundamentals and structure of a risk management system. In: Klein, A. (Hrsg.). *Risk management and risk controlling: modern instruments, principles and solutions* (S. 21–50). Freiburg: Haufe Lexware.

СИСТЕМНО УПРАВЛЕНИЕ НА РИСКА В ГЕРМАНСКИТЕ ОБЩИНИ

Резюме: *Статията анализира значението и необходимостта от системно управление на риска в германските общини. Установено е, че местните власти, подобно на дружествата, са изложени на различни рискове, включително финансови, свързани с персонала, ИТ и с репутацията. Въпреки тези рискове, за разлика от частните компании, в публичния сектор не съществуват законови изисквания за систематичен мониторинг на риска. В следващия раздел е представено приблизително описание на структурата на управлението на риска в общините – от създаването на декларация за мисията и списък на рисковете до оценката на риска и прилагането на мерки.*
Посочва се, че за ефективното управление на риска са необходими както превантивни, така и мерки за набелязването му. Освен това се изтъква значението на културата на риска в администрацията и активното участие на ръководителите и служителите. Особено внимание се обръща на необходимостта от използване на системи, поддържани от ИТ, в по-големите администрации, докато в по-малките общини съществуващите мерки често са достатъчни. Статията завършва с констатацията, че липсата на подготвеност за кризисна ситуация, каквато беше неотдавнашната пандемия, води до грешки и неефективност, които могат да бъдат избегнати.
Ключови думи: *община, мониторинг на риска, система за управление на риска, мисия за риска, опис на риска, оценка на риска*

Йонас Хеш, докторант
Университет по библиотекознание и информационни технологии
Email: JonasHeesch@web.de

АКТУАЛНО
CURRENT TOPICS

ATTACHMENT IN THE CONTEXT OF SYSTEMIC PARADIGMS: A MULTIDISCIPLINARY PERSPECTIVE

Jana Johnson
University of Library Studies and Information Technologies

Abstract: *This paper explores the development of attachment within systemic paradigms, offering a multidisciplinary perspective on the complexity of attachment processes. While classical attachment theory focuses primarily on the relationship between child and caregiver, this article expands the understanding by including familial, social and cultural systems. Based on an extensive literature review that integrates studies from developmental psychology, family therapy and comparative cultural psychology, this paper highlights how systemic and cultural influences shape attachment styles and practices. The findings highlight the need to consider attachment theory within a broader social and cultural context and point to the importance of a multidisciplinary approach for a comprehensive understanding of human attachment processes. These findings offer important implications for research and practice by emphasising the complexity of factors that influence the development of attachment.*
Keywords: *Attachment Theory, Systemic Paradigms, Multidisciplinary Perspective, Cultural Influences, Family Structures*

INTRODUCTION

Attachment theory, pioneered by John Bowlby in the late 1950s and early 1960s, has become a central concept in developmental psychology. Bowlby's postulate that the need for closeness to an attachment figure is a fundamental biological need that is crucial for survival and psychological development forms the basis of attachment theory (Bowlby 1991). The continuation and empirical underpinning of this theory by Mary Ainsworth, particularly through the development of the "Strange Situation" procedure, has contributed significantly to the understanding of different attachment styles (Ainsworth et al. 1979).

In recent decades, however, research has increasingly recognised the limitations of a purely dyadic perspective on attachment. The growing recognition of systemic and cultural factors shaping attachment development has necessitated an extension of classical attachment theory (Minuchin 2018). Urie Bronfenbrenner's ecological systems model, which emphasises the multi-layered nature of environmental influences on human development, provides a framework for integrating these broader perspectives (Bronfenbrenner 1979). This model underscores the interaction between different environmental systems, from the immediate family to broader cultural and societal influences.

In addition, comparative cultural studies have shown that attachment patterns and practices can vary considerably depending on cultural norms and values (Van IJzendoorn & Kroonenberg 1988). These findings shed light on the variability of attachment processes and challenge the assumption of universal attachment patterns. Recognising this diversity requires a multidisciplinary approach that combines psychological, sociological, anthropological and cultural perspectives in order to paint a comprehensive picture of the factors that shape attachment relationships. The work of Patricia Crittenden (2013) and Hildenbrand (2014) makes a decisive contribution to this expansion. Crittenden (2013) develops the understanding of attachment theory further by emphasising the role of socio-economic factors, family structures and social support networks. Bruno Hildenbrand expands on attachment theory with his genogram work, which involves analysing three generations (Hildenbrand 2018). This approach enables a

deeper understanding of family decision-making processes and their influence on attachment patterns by reconstructing life practices individually and collectively across generations. Hildenbrand's methodology thus offers new insights into the complexity of attachment constructs within familial and socio-cultural contexts (Hildenbrand 2014).

This thesis aims to examine the concept of attachment within a systemic framework by looking at these multi-layered influences that go beyond the immediate relationship between child and caregiver. By integrating insights from different disciplines, it aims to provide a more comprehensive understanding of attachment development that reflects the complexity of human relationships within a broader social and cultural context.

RESEARCH METHODOLOGY

This thesis employs a comprehensive literature review. This method identifies the current state of knowledge, highlights research gaps, and proposes directions for future research. The primary aim of the thesis is to achieve a convergent synthesis of multidisciplinary perspectives on attachment theory. This systematic investigation was carried out with the aim of bringing together the interdisciplinary strands of research that deal with attachment theory in the context of systemic and cultural paradigms. The focus here was particularly on studies that deal explicitly with the interactions between systemic approaches and cultural factors influencing attachment processes. The methodological approach to identifying relevant literature included a targeted and structured search in leading academic databases. This search was guided by the use of specific key terms such as 'attachment', 'systemic theory', 'family structures' and 'cultural influences on attachment' to ensure that the studies searched were relevant in content and aligned with the specific questions posed in this article. The careful selection of literature included both classic works that laid the foundations of attachment theory and more recent research that explores innovative systemic and cultural perspectives on attachment phenomena.

RESULTS

The integration of systemic perspectives into the study of attachment processes requires a detailed consideration of the multi-layered environmental factors that influence the development of attachments. Within this framework, Bronfenbrenner's (1979) ecological systems model offers a robust theoretical basis for understanding the intricate interactions between individuals and their environments. Bronfenbrenner's model articulates the existence of multiple interconnected system levels, ranging from direct interactions in the immediate environment to more abstract, overall societal influences. The microsystem includes immediate environments such as family and school, which are essential for the formation of emotional bonds (Berk 2003). The mesosystem refers to the interactions between these microsystems and their influence on attachment quality (Bronfenbrenner/Morris 2007). The exosystem, including parental working conditions and legal frameworks, has an indirect effect on development (Bronfenbrenner & Morris 2007). The macrosystem includes cultural norms that shape attachment practices (Keller 2022), while the chronosystem considers temporal changes and their effects (Bronfenbrenner & Morris 2007). Applying Bronfenbrenner's ecological systems model to attachment theory provides a multidimensional understanding of how different levels of the environment, from family interaction to cultural norms, interact to reciprocally influence the development of attachment relationships.

In addition to Bronfenbrenner's systems model, comparative cultural studies also emphasise the importance of cultural influences on attachment patterns. The groundbreaking meta-analysis by Van IJzendoorn and Kroonenberg (1988) marks a significant turning point in attachment research by revealing profound cross-cultural differences in the prevalence of attachment styles. Their systematic investigation of attachment behaviour in different cultural contexts makes it clear that cultural characteristics have a considerable influence on the development of attachment styles and patterns. The authors found that the distribution of secure, avoidant and ambivalent attachment styles differs significantly between cultures, indicating the formative role of cultural practices and social norms in the development of attachment relationships. These findings express the critical need to take cultural contexts into account when analysing attachment processes and point to the limitations of universal assumptions in attachment theory (Van

IJzendoorn/Kroonenberg 1988).

Since then, numerous studies have further differentiated and deepened the findings of Van IJzendoorn and Kroonenberg. In particular, the work of Keller (2022) has shown how culturally specific parenting practices, values and beliefs influence expectations of attachment relationships and actual attachment behaviour. Keller postulates that cultural contexts not only shape the interactions between parent and child, but also influence the interpretation and evaluation of attachment behaviour. For example, in some cultures, independence-promoting practices may prevail that favour the development of an avoidant attachment style, while in other cultures closer physical proximity and greater dependence are seen as an expression of secure attachment (Keller 2022).

Cultural variations in attachment expression and evaluation underscore the necessity of examining attachment processes within their specific cultural contexts. Instead, they require a differentiated approach that takes culturally specific practices, norms and values into account.

The consideration also includes sociological and anthropological perspectives by highlighting the role of social structures and institutions. For example, research shows that socio-economic factors, family structures and social support networks are important determinants of the quality and security of attachment relationships (Crittenden 2013). Patricia Crittenden's work in the field of attachment theory is well known for her developments and adaptations of the original attachment model, particularly through her dynamic maturational model (DMM) of attachment and adjustment. Crittenden's research emphasises how individuals from early childhood develop adaptive strategies to cope with stress and danger in their environment, and how these strategies are influenced by socioeconomic conditions, family structures and the availability of social support networks (Crittenden 2013). Crittenden's work expands the understanding of how children and adults process and respond to information in dangerous or unsafe situations, and how these processing and response patterns develop into complex behavioural strategies over time. These strategies can affect the quality and security of attachment relationships by impacting how individuals regulate closeness and distance in relationships.

In addition, Crittenden (2013) stresses the importance of the socio-cultural context for the development of attachment strategies. She argues that the cultural and social environment in which an individual grows up has a decisive influence on which types of adaptive strategies are considered acceptable or useful (cf. Crittenden 2013). This implies that socioeconomic factors and family structures not only affect the availability of attachment figures and the quality of attachment, but also the types of adaptive strategies that individuals develop to deal with stress and uncertainty.

The sociological perspective on attachment emphasises the role of social structures and institutions. It examines how social agreements and conflicts, such as the distribution of resources and opportunities, influence the living conditions and experiences of individuals (Thompson 2016). Sociological approaches, such as functionalism and Marxism, offer different perspectives on these dynamics and their impact on attachment relationships.

The renowned clinical sociologist Bruno Hildenbrand (2014) also sets himself apart from conventional approaches, particularly in systemic (family) therapy, in three key respects with his modern concept of genogram work. Firstly, the nuclear family and its internal relationship triangles are regarded as the central unit of analysis. Secondly, Hildenbrand emphasises the consideration of family structures by analysing 'objective' data such as birth, marriage and occupational data over at least three generations. Thirdly, illness is seen as an attempt to solve problems in crisis situations, which makes it necessary to analyse the genogram data sequentially. For almost two decades, the author has been intensively involved with genogram work in order to explore its fundamentals in greater depth than before. In 2018, this led to the publication of a book that presents advanced techniques of genogram work and emphasises a view of humanity that highlights the individual's creative possibilities within a given framework (Hildenbrand 2018). In this way, genogram work implies attachment patterns, as it offers insights into the emergence and transmission of attachment behaviour through the in-depth analysis of family histories and structures across generations. By recognising recurring patterns in family relationships, behaviour and attachment styles that are deeply rooted in the family history become visible, which could contribute to the clarification and possible treatment of attachment problems.

CONCLUSION

The extensive study of attachment theory, initiated by John Bowlby's and Mary Ainsworth's groundbreaking work (Ainsworth et al. 1979; Bowlby 1991) has been significantly expanded through the integration of systemic and cultural perspectives, illustrates the complexity of attachment development beyond the dyadic relationship between child and caregiver. By applying Bronfenbrenner's ecological systems model (Bronfenbrenner 1979), it becomes clear how the fusion of different environmental levels, from intimate family interactions to far-reaching cultural influences, characterises the shaping of attachment relationships. The meta-analysis by Van IJzendoorn and Kroonenberg (1988), complemented by Keller's comparative cultural work (Keller 2022), emphasises the need to consider the diverse cultural influences and their effects on attachment styles, which calls into question the universal validity of attachment patterns. This provides fresh insights into the ongoing debate on independence and interdependence within modern societies, revealing the profound impact of cultural values and practices on individual and collective perceptions of autonomy and connectedness (Johnson 2021). The inclusion of sociological and anthropological insights, as presented in the work of Crittenden (Crittenden 2013) and Hildenbrand (2018), further emphasises the role of social structures and belief systems in shaping attachment relationships, creating a multifaceted picture of the determinants of attachment, while also providing a valuable tool for holistic consideration with the work of Hildenbrand (2014/2018). In view of this multidisciplinary perspective, it is clear that future research should shed further light on the dynamic interactions between the various levels of influence in order to gain a comprehensive understanding of the processes of attachment development. It is also important to explore the effects of modern developments such as digitalisation on attachment relationships. In practical terms, this comprehensive analysis emphasises the importance of culturally sensitive approaches in educational and therapeutic contexts in order to meet the diverse needs of individuals in a global context and thus promote the well-being of families worldwide.

REFERENCES

Ainsworth, M. D., M. C. **Blehar,** S. Wall und E. **Waters** (1979). *Patterns of attachment: A psychological study of the strange situation.* Nashville, TN, USA: John Wiley & Sons.

Berk, L. E. (2003). *Child Development.* 6. Aufl. Allyn & Bacon.

Bowlby, J. (1991). *Attachment and Loss: Attachment v. 1.* Harlow, England: Penguin Books.

Bronfenbrenner, U. (1979). *The ecology of human development: Experiments by nature and design.* London, England: Harvard University Press.

Bronfenbrenner, U. und P. A. **Morris** (2007). The bioecological model of human development. *Handbook of Child Psychology.* Wiley. doi: 10.1002/9780470147658.chpsy0114.

Crittenden, P. M. (2013). *Raising parents: Attachment, parenting and child safety: Attachment, parenting and child safety.* Routledge.

Hildenbrand, B. (2014). *Einführung in die Genogrammarbeit.* 4. Aufl. Heidelberg: Carl-Auer Verlag.

Hildenbrand, B. (2018). *Genogrammarbeit für Fortgeschrittene: Vom Vorgegebenen zum Aufgegebenen.* 1. Aufl. Heidelberg: Carl-Auer Verlag.

Johnson, J. (2021). *Einflussfaktoren auf das Selbstkonzept.* München: GRIN Verlag. Verfügbar unter: https://www.grin.com/document/1436702.

van IJzendoorn, M. H. und P. M. **Kroonenberg** (1988). Cross-cultural patterns of attachment: A meta-analysis of the strange situation. *Child development,* 59(1), S. 147. doi: 10.2307/1130396.

Keller, H. (2022). *Cultures of infancy.* London, England: Routledge.

Minuchin, S. (2018). *Families and family therapy.* Routledge.

Thompson, K. (2016). Sociological perspectives: The basics. *ReviseSociology – A level sociology revision - education, families, research methods, crime and deviance and more!* ReviseSociology, 5 Juli. Verfügbar unter: https://revisesociology.com/2016/07/05/sociological-perspectives-the-basics/ (Zugegriffen: 27. März 2024).

ПРИВЪРЗАНОСТ В КОНТЕКСТА НА СИСТЕМНИТЕ ПАРАДИГМИ: МУЛТИДИСЦИПЛИНАРНА ПЕРСПЕКТИВА

Резюме: *Тази статия разглежда развитието на привързаността в рамките на системните парадигми, като предлага мултидисциплинарна перспектива за сложността на процесите на привързаност. Докато класическата теория на привързаността се фокусира предимно върху връзката между детето и грижещия се за него, тази статия разширява разбирането, като включва семейните, социалните и културните системи. Въз основа на обширен литературен преглед, който интегрира изследвания от психологията на развитието, семейната терапия и сравнителната културна психология, тази статия подчертава как системните и културните влияния оформят стиловете и практиките на привързаност. Констатациите подчертават необходимостта от разглеждане на теорията за привързаността в по-широк социален и културен контекст и посочват значението на мултидисциплинарния подход за цялостно разбиране на процесите на човешката привързаност. Тези констатации предлагат важни последици за научните изследвания и практиката, като подчертават сложността на факторите, които влияят върху развитието на привързаността.*

Ключови думи: *Теория на привързаността, системни парадигми, мултидисциплинарна перспектива, културни влияния, семейни структури*

Яна Йонсон, докторант
Университет по библиотекознание и информационни технологии
E-mail: j.johnson@institut-johnson.de

АКТУАЛНО
CURRENT TOPICS

NAVIGATING PRIVACY IN CRYPTO: CURRENT CHALLENGES AND (FUTURE) SOLUTIONS

Vyara Savova
University of Library Studies and Information Technologies

Abstract: *This article examines the evolving relationship between privacy and blockchain technology, examining the challenges and innovations in the context of decentralized finance (DeFi) and smart contracts. It explores the complex interplay between blockchain's transparency and the necessity for user privacy, drawing insights from previous research, including the works of Michèle Finck and Primavera De Filippi, who analyze the impact of GDPR and the dichotomy of decentralization and privacy. The article further delves into recent proposals, notably Vitalik Buterin et al.'s 'Privacy Pools', addressing the balance between privacy and regulatory compliance through the use of cryptography. It concludes by acknowledging ongoing privacy challenges while highlighting promising developments, suggesting a possibility of blockchain technology reaching a harmonious co-habitation with privacy principles.*
Keywords: *Blockchain, Privacy, GDPR, Zero-Knowledge Proofs, Privacy Pools*

INTRODUCTION

Blockchain technology can be defined as a "decentralized ledger (or state machine) that relies on cryptographic algorithms and economic incentives in order to ensure the integrity and legitimacy of every transaction (or state change)". A fundamental aspect of the technology is that a copy of the blockchain is shared amongst all nodes (or computers) connected to the network, comprising the history of all valid transactions. Then, "each transaction is recorded into a 'block', which is appended sequentially to the previous block of transactions" (De Filippi 2017). The technology has proven to be among the groundbreaking innovations of the past few decades due to its potential to revolutionize numerous sectors with its unique technical and social attributes, notably decentralization, transparency, and immutability.

Originally conceptualized for digital currency transactions, its application has since expanded far beyond, permeating various fields such as finance, art, healthcare, and governance. However, this rapid integration brings forth significant privacy concerns. As blockchain networks often operate on public and permissionless ledgers, the balance between transparency and user privacy becomes a complex issue, particularly in the context of stringent data protection regulations such as the EU's General Data Protection Regulation (GDPR 2020). Generally, to better understand the difference between permissioned / permissionless and public/private blockchains, by using the Bitcoin blockchain as an example, see Michèle Finck's article Blockchains and Data Protection in the European Union, where the author explains how "[t]he original Bitcoin blockchain is a public and unpermissioned (or 'permissionless') blockchain, which means that it is open-source and open-access so that anyone can create a Bitcoin address and download or design software to run nodes" (Finck 2018).

Moreover, the rise of decentralized finance (or DeFi, refers to a "set of newly emerging financial products and services that operate on decentralized platforms using blockchains to record and share data". Furthermore, "DeFi products and services are conducted without a trusted central intermediary" such as a bank, and they include various services like payments, lending and borrowing, trading and investments, capital raising (crowdfunding), and insurance, among others (Carapella et al. 2022). and the implementation of smart contracts have further complicated the privacy landscape.

Smart contracts, although not legal contracts but instead self-executing lines of code, already pose unique legal challenges, including data protection and user privacy. While there isn't a unified agreement reached around the definition of a smart contract, for the purposes of this article, we may understand smart contracts as 'automated software agents hosted on blockchains that are capable of autonomously executing transactions on the triggering of certain conditions' (Goldenfein and Leiter 2018). While they offer automation and efficiency, they also raise questions about the control and confidentiality of personal data. An intriguing aspect of the broader discussion around blockchain and privacy is the status of smart contracts in the context of the limitations around automated decision-making and solely automated data processing under the GDPR. See, for example, Michèle Finck's article Smart contracts as a form of solely automated processing under the GDPR, in which the author argues that "[s]mart contracts indeed appear to qualify as a form of solely automated data processing under Article 22(1) GDPR" (Finck 2019).

In addressing these challenges, this article will delve into the intricate relationship between blockchain technology and privacy. Drawing from the works of experts such as Michèle Finck and Primavera De Filippi and considering the latest proposals from Vitalik Buterin et al., we will explore the current state of privacy in blockchain, the ongoing challenges, and the promising solutions on the horizon. The objective is to provide a comprehensive understanding of where blockchain stands in terms of privacy and what the future may hold for this rapidly evolving technology.

OVERVIEW OF PAST DEVELOPMENTS

Even though the introduction of blockchain technology predates that of the GDPR, the fragile relationship between an infrastructure that is by design transparent and the concerns around personal data protection has been ongoing since the very genesis of the technology. The Bitcoin whitepaper, authored by the pseudonymous Satoshi Nakamoto, addresses the issue of privacy on-chain, however, primarily in the context of the anonymity of transactions. It further emphasizes that while the transaction flow is public on the blockchain, the identities of the parties involved in transactions are not directly linked to their public keys. According to the author(s) of Bitcoin's whitepaper, this design offers a level of privacy by keeping users' identities separate from their transaction history, although it is not completely anonymous. The whitepaper discusses methods to increase privacy, such as using new addresses for each transaction. However, it also acknowledges that linking public keys to real-life identities can potentially reduce this privacy (Nakamoto 2008). Furthermore, the reason for this fragile relationship can be traced back to the design of both blockchain and GDPR, as "[w]hereas the GDPR was fashioned for a world where data is centrally collected, stored, and processed, blockchains decentralize each of these processes" (Finck 2018).

Beyond that, the evolution of the concerns around privacy in blockchain technology can further be traced through seminal works of research conducted in the past decade, such as the publications of Michèle Finck and Primavera De Filippi – although far not the only researchers in the fields, those two authors have been chosen to be highlighted here as their seminal research not only lay at the intersection of technical and legal analysis, without focusing disproportionately on one of the two but also covers and analyses a significant number of other publications.

In a nutshell, Michèle Finck's studies examine the intersection of blockchain technology with data protection laws, particularly focusing on the European Union's GDPR. In her work, Finck highlights the complexities of categorizing blockchain within existing legal frameworks, emphasizing the challenges posed by the decentralized and immutable nature of blockchain data. As described above, she also delves into the concept of smart contracts, exploring their designation as a form of solely automated data processing under the GDPR and discussing the implications for user privacy and data protection rights.

Below are listed some of the conclusions of her work that are considered crucial for the current understanding of the conflict between privacy and blockchain and, therefore, also fundamental for finding solutions to this conflict.

According to Finck, "[m]ost DLTs [short for distributed ledger technologies] contain two types of data: (i) the header which includes the timestamp, the identity of the data's source such as an address and the previous block hash, whereas (ii) the block content (or payload) contains the data to be stored (on the

Bitcoin blockchain this would be the relevant transactions as well as the coinbase transaction). Whereas the header is usually not encrypted, the payload normally is" (Finck 2018).

It is important to mention here that according to Opinion 04/2014 on Anonymization Techniques, 0829/14/EN, by Article 29 Working Party (the organization is a precursor of the currently active European Data Protection Board), encryption is considered a pseudonymization technique under EU data protection regime given that the data subject can still be indirectly identified (Article 29 Data Protection Working Party 2014). Therefore, the use of encryption would not preclude the application of GDPR but instead would deem all encrypted personal data as pseudonymized. Nevertheless, considering that the European Data Protection Board has included the drafting of new Guidelines on Anonimyzation in its work program for 2023–2024, the topic is worth revisiting once those guidelines are published (European Data Protection Board 2023).

In terms of potential solutions, Finck stresses on multiple occasions that personal data could (and should) be stored off-chain and merely linked to the blockchain "through a hash pointer" (without going into too many technical details, hash pointers can be defined as a "data structure containing the previous block's hash value and a pointer to that block", basically meaning that the data is chronologically ordered in a manner that makes it difficult to tamper with information without altering subsequent blocks on the blockchain. The term "hash" refers to a cryptographic hash function, such as SHA256). "In such a scenario," Finck explains, "personal data is recorded in a referenced encrypted and modifiable database and not on the blockchain," solving, to a large extent, the fundamental issue of blockchain and data protection, as no personal data will be stored on-chain and would therefore be visible to practically anyone with an internet connection. Nevertheless, Finck is careful to point out that "[d]evelopers working on such solutions must, however, be careful to ensure that metadata is also treated appropriately as it can reveal personal information even where personal data is not directly stored on-chain".

Furthermore, Finck concludes, "[b]lockchains are a technology that might in the future achieve some of the objectives inherent to the GDPR through technological means, although through mechanisms distinct from those envisaged by the legal framework itself". The possibility of such future achievements is at the very heart of the current analysis, as it traces the earlier concerns expressed by academia and technical development alike and finds them within the solutions currently developed in the blockchain space (see Section 3 below).

Therefore, Primavera De Filippi's research deserves a special mention in this article, as it takes a broader view, analysing the interplay between decentralisation and privacy in blockchain technologies. In a nutshell, in her article titled "The interplay between decentralization and privacy: the case of blockchain technologies", De Filippi underscores the tension between the inherent transparency of blockchain and the need for user anonymity, particularly in the context of decentralized finance. Her work brings to light the challenges in maintaining privacy in decentralized systems and the potential trade-offs between decentralization, security, and privacy.

De Filippi concludes that "in spite of the obvious benefits they provide when it comes to data sovereignty, decentralized architectures also present certain characteristics that – if not properly accounted for – might ultimately impinge upon users' privacy," further adding that while such architectures are capable of preserving the confidentiality of data, they cannot "easily protect themselves against the analysis of metadata". Therefore, if not properly designed, "decentralized infrastructures intended to promote individual privacy and autonomy might turn out to be much more vulnerable to governmental or corporate surveillance than their centralized counterparts" (De Filippi 2017).

Further, De Filippi explains the fundamental differences between centralized and decentralized architectures, paving in the process also our current understanding of the dichotomy between privacy and blockchain as a conflict between a framework aimed at minimizing centralized control over data and a technical architecture created to make central control impossible:

"[D]ecentralised systems are much more difficult to implement than centralized platforms. In order to allow for an effective coordination amongst a distributed network of peers, decentralized architectures generally rely on the disclosure of everyone's interactions. Hence, if the price of centralization is trust (as users need to trust centralized operators with their data), decentralization comes at the price of transpar-

ency (as everyone's interactions are made visible to all network's nodes)." Echoing Finck's delineation between blockchain's two types of data, De Filippi further adds that "while decentralized architectures can provide more privacy at the content layer (to the extent that content has been encrypted), they cannot protect themselves against the third parties' analysis of data (or metadata) which are publicly disclosed on a decentralized network". Therefore, the possible solution would be to implement additional technical means to protect the confidentiality of online communications, such as advanced cryptographic techniques, leading to a future where "in spite of the apparent dichotomy between transparency and privacy, there is no real conflict between the two."

The analysis of these foundational works is crucial, as, to a large extent, they set the stage for understanding the current blockchain privacy challenges that must be addressed for its future development. They are, in a sense, also a blueprint for finding solutions.

LATEST PROPOSALS ON PRIVACY AND BLOCKCHAIN

Apart from the theoretical concerns, it is no less important to highlight the significant developments taking part in the technical side of blockchain applications, occurring since the articles highlighted above were published.

The co-creator of Ethereum, Vitalik Buterin, has been directly involved in fixing some of the issues around the Ethereum blockchain, key among which was the migration to a more ecologically friendly consensus mechanism through the adoption of Proof-of-Stake (Ethereum 2024). However, he has also been focusing on addressing concerns about privacy in blockchain. In the "Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium" article, authored by Buterin and a collective of technical experts (further referenced as Buterin et al.), the authors call for creating a balance between maintaining user privacy and fulfilling regulatory compliance through the development of "Privacy Pools", citing the currently insufficient privacy on-chain as the rationale behind their work (Buterin 2022).

These pools utilise advanced cryptographic techniques, such as zero-knowledge proofs (a zero-knowledge proof, or ZKP, is a cryptographic method which makes it possible to prove the validity of a statement without revealing the statement itself. In the ZKP context, the 'prover' is the party trying to prove a claim, while the 'verifier' is responsible for validating the claim (Ethereum May 2024) and, in particular, the ZK-SNARKs (the so-called ZK-SNARKs, a General-purpose zero-knowledge proofs that allow a prover to prove mathematical claims about some combination of public data and private data that the prover holds in such a way that satisfies two key properties: "Zero-Knowledge: nothing about the private data is revealed, aside from the fact that the private data satisfies the claim that is being proven" and "[s]uccinctness: the proof is short (in bytes), and can be verified very quickly, even if the underlying claim being proven involves a heavy computation that takes a very long time to run."), to ensure transactional privacy while adhering to regulatory requirements (such as, potentially, to the GDPR by the creation of custom privacy pools that would align with the regulation's requirements without exposing any personal data). As described by the authors themselves, the core idea of the proposal is to "allow users to publish a zero-knowledge proof, demonstrating that their funds (do not) originate from known (un-) lawful sources, without publicly revealing their entire transaction graph". The above can be achieved by membership in custom association sets that are able to satisfy certain properties required by regulation — for example, GDPR — as well as social consensus and agreements, with privacy pools merely giving "additional options by extending the users' action set. [The users] can still provide more detailed proofs to specific counterparties, if needed" (Buterin 2022). Therefore, participation in such a custom association should not preclude the rights of the data subjects to exercise control over the data they share with other parties. Instead, it would allow for the execution of on-chain transactions without exposing its content or metadata.

Furthermore, this approach would represent significant strides in addressing other privacy challenges in blockchain, particularly in the context of decentralized finance and the use of smart contracts. Its basis is the introduction of two sets of smart-contract-based "proofs", or association sets that can be used interchangeably: membership proofs ("I prove that my withdrawal comes from one of these deposits") or exclusion proofs ("I prove that my withdrawal does not come from one of these deposits") which are

then used "to reach a separating equilibrium between honest and dishonest protocol users" (Buterin 2022). It is important to note that the privacy pools as described exist beyond the theoretical ideation and are already available to the Ethereum blockchain users – with more information provided on the website privacypools.com and by accessing the documentation required for their execution on-chain from a GitHub repository – https://github.com/ameensol/privacy-pools.

In more legal terms, their proposal will likely still fall within the current scope of the GDPR, as zero-knowledge proofs and their sub-category ZK-SNARKs would still be considered an encryption mechanism. Nevertheless, the "Privacy Pools" concept provides an interesting solution to the privacy on blockchain conundrum – one that is based on data subjects exercising control over their data and actively participating in the process of its placing in a specific pool by also following its rules and incentive mechanisms. What is more, the de-linking between the pooled deposit and the original deposit provides a solution to Finck's on-chain data storage issue, as no personal data will be shared publicly due to the use of validation mechanisms that don't rely on data exposure. However, as is the case with many such proposals, despite the positive outlook, time and adoption will show the exact benefits of this solution in practice.

CONCLUSION

In conclusion, while there are significant challenges regarding privacy in the realms of blockchain, decentralized finance, and smart contracts, there is also substantial and promising work underway to address these issues. The insights and proposals from experts like Michèle Finck, Primavera De Filippi, and the work by the likes of Vitalik Buterin highlight a dynamic field where technological innovation is continually being balanced against privacy concerns and regulatory requirements. As the technology evolves, these ongoing efforts are crucial in shaping a blockchain ecosystem that upholds privacy without compromising on the decentralized principles that grant it with the potential of being a truly transformative technology. It is, therefore, also crucial that the topic is often revisited in order to interpret the legal and privacy implications of the latest technical developments, ensuring that the blockchain ecosystem not only evolves but does so in a manner that aligns with core principles of user privacy and data protection.

REFERENCES

Article 29 Data Protection Working Party (2014). Opinion 04/2014 on Anonymisation Techniques, 0829/14/EN,.

Buterin, V. et al. (2022). Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium. In: *Crypto Valley Conference on Blockchain Technology (CVCBT 2022),* LNCS, vol. 12345, pp. 567–585. Springer, Cham.

Carapella, F., E. **Dumas,** J. **Gerszten,** N. **Swem,** L. **Wall** (2022). *Decentralized Finance (DeFi): Transformative Potential & Associated Risks.* Federal Reserve Bank of Boston.

De Filippi, P. (2017). *The Interplay Between Decentralization and Privacy:* The Case of Blockchain Technologies. Journal of Peer Production (9), 75–96.

European Data Protection Board. EDPB Work Programme 2023–2024. [Online]. Available: https://edpb.europa.eu/system/files/2023-02/edpb_work_programme_2023-2024_en.pdf.

Ethereum. Consensus Mechanisms – Proof of Stake (PoS). Available at: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

Ethereum. Zero-Knowledge Proofs. Available at: https://ethereum.org/en/zero-knowledge-proofs/.

Finck, M. (2018). Blockchains and Data Protection in the European Union. *European Data Protection Law Review 4(1),* 17–35.

Finck, M. (2019). Smart Contracts as a Form of Solely Automated Processing Under the GDPR. *Journal of Information, Communication and Ethics in Society 17(2),* 177–194.

GDPR (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union L 119,* 1–88.

Goldenfein, J., A. **Leiter** (2018). Legal Engineering on the Blockchain: "Smart Contracts" as Legal Conduct. Law and Critique. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3176363.

Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf.

ТЕМАТА ЗА ПОВЕРИТЕЛНОСТТА В КРИПТО: ТЕКУЩИ ПРЕДИЗВИКАТЕЛСТВА И (БЪДЕЩИ) РЕШЕНИЯ

Резюме: Тази статия проследява развиващата се връзка между защитата на личните данни и блокчейн технологията, като разглежда предизвикателствата и иновациите в контекста на децентрализираните финанси (DeFi) и интелигентните договори. Изследва се сложното взаимодействие между прозрачността на блокчейна и необходимостта от защита на личните данни на потребителя, стъпвайки върху изводите от предишни изследвания, включително трудовете на Мишел Финк и Примавера Де Филипи, които анализират въздействието на GDPR и дихотомията на децентрализацията и поверителността. Статията допълнително се задълбочава в скорошни предложения, по-специално „Privacy pools“ на Виталик Бутерин и др., насочени към баланса между поверителността и съответствието с нормативните изисквания чрез използването на криптография. Анализът включва обзор на продължаващите предизвикателства, свързани с поверителността, като същевременно подчертава обещаващите развития, които дават възможност на блокчейн технологията да постигне хармонично съжителство с принципите за защита на личните данни.

Ключови думи: блокчейн, поверителност, GDPR, доказателства с нулево знание, Privacy pools

Вяра Савова, докторант
Университет по библиотекознание и информационни технологии
E-mail: v.savova@unibit.bg

ИЗДАТЕЛ

Академично издателство
„За буквите – О писменехь“
Университет по библиотекознание и информационни технологии

ДИРЕКТОР

доц. д-р Диана Стоянова
бул. „Цариградско шосе“ № 119,
ет. 2, стая 213
София 1784, България
тел.: +359 879 14 83 85
е-поща: d.stoyanova@unibit.bg

Списание „Образование, научни изследвания и иновации“ излиза четири пъти годишно.

PUBLISHER

Academic Publisher
“Za Bukvite – O Pismeneh”
University of Library Studies and Information Technologies

DIRECTOR

Assoc. Prof. Diana Stoyanova, PhD
119, Tsarigradsko Shosse Blvd.
fl. 2, room 213
Sofia 1784, Bulgaria
tel.: +359 879 14 83 85
E-mail: d.stoyanova@unibit.bg

Journal “Education, Scientific Research and Innovations” is published four a year.

ISSN 2815-4630

ISSN 2815-4630