Volume 16 • Issue 2 • 2024

sciendo

ISMSME International Society for Manufacturing, Service and Management Engineering

received: 1 October 2023
accepted: 15 March 2024

pages: 148-165

Process security methods and measurement in the context of standard management systems

Agnes Kemendi
Pal Michelberger

ABSTRACT

The main purpose of the paper is to identify ways to establish process security in the constantly changing risk and control environment and to introduce a new model. The research is based on a literature review of process security components. Qualitative content analysis was used to establish a linkage between the certified management systems and the level of process security. Elaborations have been conducted based on the survey data of the International Standards Organisation (ISO) and served as a basis for analysis of certification types and their sectoral division in the European Union (EU) member states. A new Balanced Scorecard has been developed to cover the security pillars in the context of standard management systems and serve as a framework for process security measurement. The research paper processes the state-of-the-art issue of process security, introduces components that help to establish process security, and establishes a linkage between the level of process security and certified management systems. An analysis was based on the ISO certification information related to different management system standards. Management systems were analysed in the context of process security and corresponding process performance measures. A brief walkthrough has been prepared to demonstrate the processes behind the underlying performance measures. A new Balanced Scorecard approach has been developed that maps and covers different security aspects retrieved from and linked to different management system standards. The new Balanced Scorecard based on different security aspects of entities can be leveraged by any organisation, regardless of its size or business profile.

KEY WORDS
process security, safety, security, ISO, standard management systems, Balanced Scorecard

10.2478/emj-2024-0019

Agnes Kemendi
Óbuda University, Doctoral School
on Safety and Security Sciences, Népszínház
Street 8 H-1081 Budapest, Hungary
ORCID 0000-0002-6452-8563
Corresponding author:
e-mail: kemendi.agnes@uni-obuda.hu

Pal Michelberger
Óbuda University, Faculty of Mechanical
and Safety Engineering
Becsi Street 96/B H-1034 Budapest, Hungary
ORCID 0000-0001-5752-0224
e-mail: michelberger.pal@bgk.uni-obuda.hu

Introduction

As a key component of resilience, process security is crucial in the changing risk and control environment of businesses and even state-owned entities. The publication primarily uses the term “process security” instead of the term “process safety”. The term “security” is preferred due to the intense role of information and communication technology in business processes and the significance of information security; though, the article covers both safety and security aspects, and the authors use the terms

Kemendi, A., & Michelberger, P. (2024). Process security methods and measurement in the context of standard management systems. *Engineering Management in Production and Services, 16*(2), 148-165. doi: 10.2478/emj-2024-0019 "safety" and "security" interchangeably (Wolter et al., 2009; Badreddine et al., 2009; Swuste et al., 2016). The objective of process security can be met using various methods, standards and recommendations. The research identifies ways to establish, maintain and monitor process security in compliance with corporate objectives. Management systems have become widespread, and entities tend to have more than one system selected based on professional judgment with the intention to best serve the organisation's interest. Standard management systems, such as ISO, serve to meet corporate objectives in different fields of operation, such as product or service quality, environmental performance, health and safety in the workplace, etc. The ISO's approach envisages the concept of integrated management systems. The goal of the standardisation organisation is an integrated management system composed of arbitrary components. The similar structures of process-oriented management systems enable their relatively easy integration. The integrated use of management system standards makes room for effective management of applied management systems and facilitates transparency, hands-on alignment to strategy, and handy reporting.

In the research, the authors introduce components that help to establish process security and the use of management systems, including the use of standard management systems. In this research, out of the introduced security components, the Balanced Scorecard (BSC) approach is used as a methodological background for further development. The authors analyse different management system standards and establish a new, security-focused Balanced Scorecard framework using different security aspects linked to management system standards. Several studies in the research area focus on Balanced Scorecard and standard management systems. The combination of the two research areas is yet to be explored and is a new approach that leverages their benefits in support of process security measurement. This approach helps organisations achieve their objectives and gives visibility, thus underpinning the necessity for security processes.

The literature review section explores the relevant literature in support of the research and formulates the hypothesis. It is followed by the research method, the results with the outcome of the research, the discussion, and conclusions.

1. Literature review

Since the eighties of the last century, process-oriented corporate operations have become widespread. Efficiency, quality, and the controlled execution of business and technological processes have become equally important with the previous profit- and/or sales revenue-centricity. The global economic crisis of 2008, the COVID-19 pandemic, and the current war situation in Ukraine are testing companies repeatedly.

IT reliability is crucial for the survival and sustainability of organisations. It is recommended that IT reliability is promoted and considered a source of organisations' sustainability in mitigating the negative effects of the COVID-19 pandemic (Tworek, 2023). Furthermore, digitalisation has set new directions and brought opportunities, risks, and obligations, such as privacy protection. The shift to data-driven decision-making, for example, puts reliance on sensitive data about identifiable persons (Bakthina et al., 2023). Digital systems are exposed to the risk of a cyberattack (Daubner et al., 2023). In addition, the structures of organisations, as well as their IT infrastructures in modern companies, are in constant change (Kern et al., 2022).

Corporate goals are differentiated in various ways, even in undisturbed external conditions. One definite strategic goal is long-term profit maximisation. Continuous product and technology innovation can ensure the company's long-term "survival", while the daily routine operative management tasks, such as production management, fixed asset, workforce and working capital management, ensure the going concern. On top of this, compliance with legal requirements, environmental protection and the operation of management systems are generally expected by external partners.

The marketing goal is to satisfy the consumer needs. The mindset of continuous improvement and delivering value to customers are key principles in the lean methodology as well, which in parallel promotes the elimination of waste, i.e., non-value-adding process steps (Kilpatrick, 2003). However, the implementation of the lean concept often faces some difficulties, e.g., some small- and middle-sized enterprises (Ulewicz & Kucęba, 2016). A successful adaptation of lean principles requires certain preconditions for all sizes and types of businesses and state-owned entities.

The safe operation of process-centric companies can be supported by several theoretical foundations, tools, methods, standards, and recommendations. It is the duty of business entities to create a governed and controlled operation that increases their resilience even under turbulent environmental changes and gives them and their partners a sense of security. "Process security can be defined as a state in which, with all required inputs (or resources necessary for execution of the process) given, the organisational units responsible for fulfilling process-related tasks will produce outputs (such as products, services, or information) in adequate quantity and quality in due time, and, upon any disturbance, normal operation of the process can be restored with the lowest possible use of resources within the shortest possible time" (Michelberger, 2014, p. 402).

The following components support process security:

- Porter's value chain model (Porter, 1985),
- Transaction management information systems (e.g., ERP systems),
- Business process reengineering (BPR),
- Information systems supporting process management (e.g., Aris),
- Prescribing and monitoring KPIs,
- Business continuity management and corporate flexibility (resilience),
- Standard management systems and their integrated implementation,
- Controlling systems (e.g., Balanced Scorecard).

Michael Porter's value chain concept — published in his book Competitive Advantage — differentiates primary (inbound logistics, operations, outbound logistics, marketing and sales, and service) and support activities (firm infrastructure, human resources management, technology, and procurement), and can be used as a basic tool in diagnosing competitive advantage, i.e., its two basic types: low cost or differentiation (Porter, 1985). The product goes through the chain of discrete activities and gains certain value in the value chain where technology pervades and culture is an important element (Porter, 1985). Porter's value chain concept identifies how inputs are transformed into outputs and is a process-oriented approach that uses an activity-based analysis in support of gaining market advantage.

Transaction management information systems, e.g., Enterprise Resource Planning (ERP), can achieve effective forecasting, planning and scheduling in support of productivity. Proper ERP implementation focuses on people besides computers and software and can provide a competitive advantage (Wallace et al., 2001). An ERP can treat the in-scope business processes in a single integrated system that enables proper information flow and smooth reporting, such as financials, payroll, customer orders, etc.

According to Hammer and Champy, business process reengineering (BPR) means "the fundamental rethinking and redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance, such as cost, quality, service and speed" (1993). The work focuses on the process of how work gets done rather than on specialisation, i.e., the division of labour promoted by Adam Smith in the Wealth of Nations in 1776 (Hammer & Champy, 1993). BPR tools and techniques include process visualisation, process mapping/operational method study, change management, benchmarking, process and customer focus (O'neill & Sohal, 1999). Organisations face the technical risk that the process changes will not work and the organisational risk that the corporate culture is against the changes related to the implementation of BPR.

Information systems (e.g., Aris) support business processes. Business processes can be modelled using process modelling and planning software capable of capturing AS-IS and TO-BE modelling. For example, ARIS can be used as a powerful tool for process modelling (Davis, 2008). The availability of quality enterprise process models ensures the skeleton of well-structured process documentation that helps to meet quality objectives set by customers. Customer satisfaction is the key objective of the ISO 9001 Quality Management Standard, and the processes of an organisation serve to meet this objective. Process approach and continuous improvement are inherent to quality management as well. Process maps present the process steps visually and strengthen the enterprise's safety and security by serving as a basis for process documents and highlighting the most critical points in the processes that are a subset of related control process documents. Process maps capture the control points and control activities built into the processes, which are the fundamental elements of the corporate safety network (Kemendi, 2022).

Key performance indicators (KPIs, aka process performance measures) should comply with the strategic objectives of the organisation and must be associated with target values. Process improvements are required to meet the KPIs, i.e., the strategic objectives. A better process contributes to meeting strategic objectives better, and KPIs can measure the level of improvement. Some KPIs are easy to gather, and others are more difficult and time-consuming (van der Aalst et al., 2016). Performance indicators serve to reflect process performance, and the design of the KPI set is a prerequisite for proper process performance measurement. The captured data should be accurate and reliable, top and line management should monitor the KPIs regularly and define actions as and when needed.

Business continuity management (BCM), covered in the ISO 22301 standard, helps corporations to be prepared for possible business disruptions with its elements of Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP). BCP provides alternative solutions in the event of downtime in the support processes to make business processes possible. DRP provides the required resources for the processes involved in the business operation — to replace and restore — in the event of an emergency (Michelberger & Kemendi, 2020). Organisational resilience capabilities increase organisational performance during unexpected events. They have an established relationship with organisational sustainability, and both relate to BCM through crisis management (Corrales-Estrada et al., 2021).

1.1. Standard management systems and process security

Management systems serve to support organisations to achieve their objectives related to different aspects. These systems are process-oriented and can be integrated due to their similar structure, which permits the avoidance of multiple process controls and excessively frequent external audits. In recent years and decades, the International Organisation for Standardisation has created and continuously developed several auditable and certifiable management systems, e.g., for quality, environment, information security, food safety, supply chain operation, business continuity, and in the field of occupational health protection. Certificates issued by external, independent certification bodies prove the company's well-organised and controllable operations. These certificates can strengthen business confidence.

In many cases, the existence of a management system is a precondition for establishing a business relationship. Establishing and maintaining the management system means additional work for the organisation. It is important to choose standard packages that correspond to the external (market) expectations and the internal organisational culture. The pressure of over-regulation and excessive expectations set by the owners/management (e.g., irrational profit or turnover, market expansion, and technology change) can break a company down.

The number of certified organisations/companies is constantly increasing worldwide (ISO.org), and it is not only the ISO that recommends standard management systems and methodologies supporting process-based company operations. The application and design of different management systems vary greatly depending on the country, continent, and industry. In many cases, their design and operation are invisible to the world outside. New entrants and those who lose their certificates are constantly changing these numbers. However, the numbers in the ISO survey do not include all management systems. For example, there are companies that do not boast about their existing information security management system, as it indicates the presence of protected information that may be valuable/interesting for others. The ISO Survey of Certifications is an annual survey of the number of valid certificates to ISO management system standards worldwide. The providers of data are the certification bodies accredited by the IAF MLA Members (ISO Explanatory note, 2021). Own elaborations have been conducted based on the survey data of the ISO and served as a basis for the analysis of certification types and their sectoral division in the European Union (EU) member states. The scope of covered ISO standards is listed in Section 3.1. Standard management systems and process security.

The analysis of ISO Certificates per certificate type in the European Union (EU) member states (EU-27), which is own elaboration based on "1. ISO Survey 2020 results — Number of certificates and sites per country and the number of sectors overall", shows that the dominating percentage of 68 % of all ISO certificates are related to the ISO 9001 Quality management standard. This comes as no surprise since this is the quality management system standard which supports an organisation in achieving its goals and objectives, document processes, policies, roles, and responsibilities to meet customer satisfaction and the necessary statutory and regulatory requirements. The ISO 9001:2015 standard is built on seven principles: customer focus, leadership, engagement of people, process approach, improvement, evidence-based decision-making, and relationship management (ISO, 2019). The second most frequent ISO standard is the ISO 14001:2015 Environmental management systems standard, which helps organisations to fulfil compliance obligations and achieve environmental objectives, enhance environmental performance, and promote reduction in waste and emissions (Keen, 2022). The third most frequent standard is the ISO 45001:2018 Occupational health and safety management systems standard. The occupational health and safety (OH&S) standard is fundamental and important in any sector because it promotes safe and healthy workplaces. It is important to identify related risk factors (Erazo-Chamorro et al., 2022). OH&S management systems are adopted to control hazards (Čiutienė et al., 2022). The sectoral division shows almost equal distribution in the named sectors; the only outstanding sector was construction. The construction sector carries a number of critical safety hazards that justify the highest frequency of certifications in this sector. The top three standards cover 94.1 % of the reviewed population.

The sectoral division of ISO certifications per certificate type in EU-27 was done according to 39 economic sectors. The sectoral analysis is own elaboration based on "2. ISO Survey 2020 results — Number of sectors by country for each standard". The survey results for the number of sectors for each standard show that the distribution of certificates in relation to various standards was relatively even amongst the different sectors with some — typically sector-specific — concentrations. It is noted that "Sector unknown" was reported for approx. half of the number of certificates. This category could not be used to retrieve information for analysis purposes.

The ISO 9001 certificates mostly belong to wholesale and retail trade, repairs of motor vehicles, motorcycles and personal and household goods, metal products, construction, and other services (around 5 % per frequency per sector). The frequency of ISO 14001 certificates shows similar results to the results of ISO 9001 certificate frequencies, with the exception of the construction sector, which has a frequency of 9.5 % for ISO 14001 and shows an outstanding role of environment management systems in the sector. Moreover, 13 % of the ISO 45001 certificates belong to the construction sector, which is in line with the expectations and shows the significant role of OH&S in this sector. The distribution of ISO 45001 certificates follows a similar dynamic to the frequencies of the ISO 14001 certificate frequencies.

The information technology sector has the highest frequency of getting certified for the ISO/IEC 27001 (35.5 %), ISO/IEC 20000-1 (35.7 %), and ISO 22301 (12.7 %) standards. 33.5 % of the ISO/IEC 27001 certificates belong to the information technology sector, which shows the centric role of information security management systems and of the treatment of information security risks in the IT sector. 35.7 % of ISO IEC 20000-1 certificates and 12.7 % of ISO 22301 certificates are related to the IT sector. The mentioned standards focus on IT security, IT service management, and BCM, all of which are essentially important in the IT sector.

Regarding the actual numbers of ISO certificates in the information technology sector, the ISO/IEC 27001 and ISO 9001 standards show the highest numbers. This shows the fundamental role of quality management systems in this sector. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems standard promotes Information Security Management Systems (ISMS), which serve to meet the goals of information security, i.e., confidentiality, integrity, and availability (Michelberger & Kemendi, 2020) and help the organisations to manage information security risk systematically. The role of information security in the ever-changing world is critical (Kemendi et al., 2021), which justifies the ranking of the related management system standards. The market participants set high expectations for businesses in the IT sector, and the outcome of the analysis confirms that IT sector participants adopt the related management systems and obtain certificates to prove their compliance.

Standard management systems increase the organisation's performance. Furthermore, the integration of separate management systems, such as quality, environment, and/or health and safety management systems, is found to be increasingly desirable and feasible (Labodová, 2004). The integration of a management system serves as a common platform for the applied management systems, consequently reducing redundancies, contributing to transparency and possibly reducing time spent on audits. Furthermore, processes are linked to each other, and the resulting duplications can be eliminated using an integrated management system. The benefits of integration can contribute to achieving higher quality standards and easier decision-making. This, however, is the prerequisite for proper project implementation beforehand. Organisations that are certified for management systems can face challenges when implementing a new management system; successful implementation requires the right competence and engagement (Fiore et al., 2023).

Certified management systems are beneficial for organisations because they help to improve their process performance. These systems are based on solid requirements, which make the system stable and transparent, and help to reduce the risk exposure. For this reason, the following hypothesis was formulated.

H1: Certified management systems increase the level of process security.

1.2. Controlling systems (e.g., Balanced Scorecard)

Controlling systems (e.g., Balanced Scorecard) enable the management and control of the organisation's activities in line with the organisational objectives. Anthony segmented organisational planning and control into strategic planning, management control and operational control (1965). These processes relate to the organisational hierarchy and to respective management levels (Strauss & Zecher, 2013). Anthony's work was a milestone in management control, but over time, it was criticised, e.g., for its narrow view due to its focus on financial and accounting-based controls and for the separation of management control from strategic and operational control (Strauss & Zecher, 2013). To meet the needs of the dynamic, constantly changing business environment, adequate dynamic controlling systems are required, e.g., the Balanced Scorecard (BSC), which is a management control and strategy communication device which offers a superior combination of financial and non-financial performance measures (Malina & Selto, 2001).

The Balanced Scorecard is a strategic performance assessment method that captures four perspectives, i.e., customer (How do customers see us?), internal (What must we excel at?), innovation and learning (Can we continue to improve and create value?), and financial (How do we look at shareholders?). The Balanced Scorecard focuses on the most critical measures and minimises information overload due to the limited number of measures (Kaplan & Norton, 1992).

The measurement of security process performance delivers essential information to the top management about the status quo of the security processes and serves as a basis for identifying areas of focus and the performance of the related action plans. Proper measurements are linked to strategic objectives.

The four perspectives of the balanced scorecard are interlinked and should be derived from the strategy. The four perspectives are related to each other and should be applied to capture these relationships. For instance, continuous improvement is a subset of innovation, and related projects are linked to the financial perspective on the input, processing and output side: CI projects usually require resources, such as time, cost, and expenses and may require investments, which will result in simpler processes that require less resources, including human. This means a direct financial benefit which should be measured, and, in turn, the resources can be used for other tasks and jobs. The changed process feeds the learning perspective. The improvement is also a feed into the internal process perspective, which generates value for the customers as defined in the customer perspective. The impacts of particular actions should be evaluated from all angles. The above example also illustrates the strive for balance in the Balanced Scorecard.

The four key categories of the Balanced Scorecard are financial, customer, internal process, and innovation and learning. As for the customer perspective, the key factors are time, quality, performance and service, and cost. The internal business perspective focuses on measures that have the greatest impact on customer satisfaction. The financial measures are associated with shareholder value. The financial consequences of a company's performance should be captured well to explicitly see the linkage between operations and finance. In the rapidly changing world, the company's ability to innovate, improve and learn has become a critical success factor that is directly linked to the company's value. Existing products, services, and processes should be subject to continual improvement and should be innovative to launch new products and services as needed. Companies should improve their ability to deliver value to customers and shareholders. Internal company processes, including the human resources associated with the processes, should embrace the innovative changes. The innovation and learning layer is inherently associated with a company that wants to continually deliver value to its stakeholders (Kaplan & Norton, 1992; Kaplan & Norton, 1993). The management systems also promote this attitude (reference in italics in Table 2). Performance objectives and measurements in line with ISO standards per Security groups). Each ISO standard has an innovation and learning layer. End-to-end processes, including inputs, processes and the resulting outputs, should be subject to continuous improvements. With reference to performance goals, people should be trained and developed as needed and attend the required training.

Security management is a unique function. When security is present, no one notices its efforts. If there is, however, a process failure, the role of security comes into focus. The performance of information and process security requires a unique mindset to design and analyse the relevant figures in a way that shows the actual and potential gaps in the process and security efforts, which represent the achievement in the security field. Performance indicators show the process's health. This has, however, the prerequisite that they are designed properly and fit the organisational processes as well. Process security is linked to the underlying safe processes, which are based on relevant security policies and procedures. It is also linked to the security culture, which is supported by appropriate training with a proper learning loop and support from the top management.

The use of standard management systems and process measurement, e.g., the Balanced Scorecard, has demonstrated benefits for an organisation. The measurement of process security is beneficial for an organisation. It is worthwhile to leverage the benefits of the Balanced Scorecard and of the standard management systems in support of process security measurement. For this reason, the Security Balanced Scorecard linked to standard management systems should be developed as a new approach to managing the performance of security processes. The Balanced Scorecard approach is to be used to create a framework for process security measurement in the context of standard management systems. In this new framework, authors identify security groups that target different corporate strategic objectives and link the corresponding ISO standard(s) to that security group, which is a comprehensive approach to security process measurement.

2. Research method

The research is based on a literature review of the components of process security.

Qualitative content analysis is used to establish a linkage between the certified management systems and the level of process security (Graneheim et al., 2017; Lindgren et al., 2020). Content analysis is a systematic method for analysing data (Lindgren et al., 2020). The analysis focuses on the theme and the context and emphasises variation as similarities and differences between passages of text. It provides an opportunity to analyse not only clear, descriptive content but also latent, interpretive content (Graneheim et al., 2017).

A new Balanced Scorecard has been developed, covering the security pillars in the context of standard management systems. It serves as a framework for process security measurement. The Balanced Scorecard approach has been researched based on a literature review and has been developed further based on the review conducted about the standard management systems. The research has been accompanied by a thorough research on standard management systems. The new Balanced Scorecard cover different security aspects (controlling areas) linked to standard management systems.

3. Results

3.1. Standard management systems and process security

Research analysis is conducted to identify the linkage between process security and certified standard management systems. Qualitative content analysis on the related ISO standards has been selected as a research method (Graneheim et al., 2017; Lindgren et al., 2020). The ISO standards subject to review were identified based on the scope of the ISO survey (ISO, 2021). The in-scope ISO standards are listed in Table 1. Three ISO standards available in the ISO survey were descoped from the detailed analysis due to their unique sectorial nature, i.e., ISO 22000:2018 Food safety management system, ISO 13485:2016 Medical devices Quality management systems, and ISO 39001:2012 Road traffic safety management systems. It should be noted that the ISO 31000 Risk management standard is a management standard and not a management system standard (ISO, n.d.). It promotes the integration of risk management into the corporate governance system and, consequently, strengthens it. Also, it establishes adequate risk management processes, which is important from the process security perspective. The ISO 31000 standard cannot be certified for; hence, no certification data is available and is therefore out of the scope of this analysis.

The in-scope ISO standards define the requirements for the specific management systems and are security-oriented bold highlights in Table. Per definition, the operation of the management systems is based on the so-called Plan-DO-Check-Act (PDCA) cycle and has a process-oriented approach. There is a built-in component for a continuous improvement mindset in each standard, i.e., in the Act phase of the PDCA cycle, following the performance evaluation in the Check cycle. The training and development cycle is an important element of the standards ensuring the availability of the required skillset. Certified management systems are attested by an independent body that applies a standard, formal, and acknowledged process, which further increases the reliability of given management systems. These factors help to increase process performance and security (Table 1). Consequently, the hypothesis is proven that the certification of management systems increases the level of process security.

3.2. New Balanced Scorecard based on different security aspects

In this research, the Balanced Scorecard approach is used to create a framework for process security measurement in the context of standard management systems. Though performance indicators are expected to be tailored to the unique objectives of an organisation, the identified set of performance indicators can be commonly used in many cases.

The scopes of the standards used to create a new balance scorecard based on different security aspects (the so-called "Security Balanced Scorecard") overlap with the scope for the Analysis based on the ISO survey of certifications to management system standards (above and are described in Table 1). Due to its importance and relevance, the authors put in the

Tab. 1. Scope of ISO standards

Name of the ISO standard	Extract from scope
ISO 9001:2015 Quality management systems — Requirements	… to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements; to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements
ISO 14001:2015 Environmental management systems — Requirements with guidance for use	… to enhance its environmental performance
ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements; Technical Corrigendum in 2014 & 2015 *	… continually improving an information security management system within the context of the organisation; includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation
ISO 45001:2018 Occupational health and safety management systems — Requirements with guidance for use	… to enable organisations to provide safe and healthy workplaces by preventing work-related injury and ill health, as well as by proactively improving its OH&S performance
ISO 50001:2018 Energy management systems — Requirements with guidance for use	… to enable an organisation to follow a systematic approach in achieving continual improvement of energy performance and the Energy management systems (EnMS)
ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements	… improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise
ISO/IEC 20000-1:2018 Information technology — Service management — Part 1: Service management system requirements	… continually improve a service management system (SMS). The requirements specified in this document include the planning, design, transition, delivery and improvement of services to meet the service requirements and deliver value
ISO 28000:2022 Security and resilience — Security management systems — Requirements	… specifies requirements for a security management system, … which intend to establish, implement, maintain and improve a security management system
ISO 37001:2016 Anti-bribery management systems standard	… improving an anti-bribery management system. The system can be stand-alone or can be integrated into an overall management system

*Note that since the review date, the ISO/IEC 27001:2013 standard has been revised by the ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements standard. The wording about the scope of the standards is identical.

Source: Extracted from the named ISO standards (ISO 9001, ISO 14001, ISO/IEC 27001, ISO 45001 ISO 50001, ISO 22301, ISO/IEC 20000-1, ISO 28000, ISO 37001).

scope the ISO/IEC 33001:2015 Information technology — Process assessment standard that provides a repository for key terminology relating to process assessment. It gives overall information on the concepts of process assessment, the application of process assessment for evaluating the achievement of process quality characteristics, and the application of the results of process assessment to the conduct of process management (ISO/IEC 33001, 2015). ISO/IEC 33xxx family of standards revises the ISO/IEC 15504 series, aka Software Process Improvement and Capability dEtermination (SPICE), which is an international framework for accessing software development processes.

The controlling areas of the new, security-focused Balanced Scorecard are based on management system standards, which cover the most important and critical controlling areas of different entities. These controlling areas are also referred to as Security groups in the publication and relate to different security aspects.

3.2.1. Security groups — key factors in determining the performance measures for the Security Balanced Scorecard

I. Quality management. In line with the ISO 9001 Quality management standard, organisations maintain, update and review the quality policy and standard operating procedures, including control activities available for in-scope business processes with clear roles and responsibilities, to have a document management system, up-to-date organisation chart and job descriptions for each job/role. These measures help organisations to maintain well-structured processes that are resilient to withstand the changes, e.g., if a key employee leaves the organisation. They are transparent and can be measured with process performance measures, which, in turn, can serve as a tool for identifying continuous improvement opportunities. The QMS aims to ensure customer satisfaction, which has to be measured to obtain the necessary feedback from the customers (external measure) and to be supported by regular QM audits performed (internal measure).

II. Process management (internal). Internal business processes are required to continually serve customer requests. They must ensure reliable and secure business operations. Businesses also must be maintained under unexpected circumstances. Internal processes should be subject to process assessments to achieve the required quality and identify improvements.

III. Information technology and information security. Information technology services and information security management systems (ISMS) ensure confidentiality, integrity and availability. Information technology is deeply embedded into corporate processes and is required for undisturbed business operations together with human resources. Information security is essentially important for organisations. Breach of information and ICT security can have serious consequences, including direct financial losses, business disruptions due to unavailability of systems, breach of confidentiality, fines related to violations of the General Data Protection Regulation, reputational issues, etc. Information and cybersecurity controls are needed to ensure confidentiality, availability, and integrity. Security is the result of adequate processes and procedures, which should be supported by technology (software solutions for security activities to handle various risks) and people (who should have adequate skills, knowledge, competences, e.g., to identify and withstand social engineering attacks).

IV. Human resources. Human resources are an integral part of business processes that require them. Occupational health and safety is an essential issue. Any safety hazard, related issues, injuries, and incidents should be taken seriously and followed up to prevent future reoccurrence. These incidents are not only a safety matter for people but can turn into an actual financial loss due to the lost time and production/value creation in the connected business processes. Consequently, such incidents directly impact the business results and cause reputational damage. The diligent follow-up on OH&S matters is essential.

V. Supply chain security. The security of the supply chain results in stable delivery of products and services to the customers, which is essential for short and long-term business success.

It is also advisable to establish business relationships with counterparts with proven quality management standards.

VI. Energy and other infrastructures. The most suitable performance measures for energy and other infrastructure primarily depend on the business profile. To determine the proper performance measures, the related processes need to be analysed in detail. The energy crisis of recent days emphasises the need for well-thought-out energy consumption. The efficient use of energy ultimately helps to reduce operating costs; thus, the price of products and services can remain lower, which is of decisive importance from the point of view of customer satisfaction. Further-

Tab. 2. Performance objectives and measurements in line with ISO standards per Security groups

Security group with ISO standards	Objective	Measurement - Performance indicators
I. ISO 9001 Quality management systems	• Continuous improvement (CI) of processes in place, including proper documentation • KPIs, e.g., customer satisfaction measures, first pass yield, are in line with business processes, regularly monitored and actioned as needed • No overdue actions • No overdue audit actions • Employees aware of the Quality Policy, Quality objectives and their QMS obligations/ contributions • Promote quality culture	• Nr. of CI projects (open, completed) and gained efficiency • KPI reviews performed and actions defined after KPI reporting by management and top management • Nr. of open/overdue actions • Nr. of open/overdue audit actions • Regular QM training with exam testing per training schedule, training records retained; Attendance rate • Regular communication on quality management, e.g., email, floor- walk, quality sessions
II. Process management (internal) ISO 22301, & 33001 Business continuity management systems; & Information technology - Process assessment	• Business continuity maintained • Reliable ICT service delivery in line with Service Level Agreements (SLAs); ICT and information security policy defined, operated and reviewed regularly; process performance is monitored; • Identify gaps and improvement areas for the information security processes and procedures to ensure information-, and cybersecurity controls are in place and updated as needed to ensure confidentiality, availability and integrity. • Persons employed aware of their obligations regarding BCM-related issues	• Nr of BCM testing • Nr of efficient BCM testing • Nr. of ICT reviews/audits performed, Nr. of audit actions/actions related to gaps, Nr of CI actions defined and completed on time/overdue • Regular training with exam testing per training schedule, training records retained; Attendance rate
III. ISO/IEC 20000-1, & 27001 Information technology - Service management; & Information technology - Security techniques	• Enterprises do not experience any problems due to ICT and/or information security incidents, e.g., unavailability of ICT services, corruption of data, or disclosure of confidential data (Kemendi et al., 2021). • Persons employed aware of their obligations in ICT security-related issues (Kemendi et al., 2021)	• Nr. of ICT incidents (target: zero) and of ICT incidents actioned as per SLA (Compliance ratio) • Nr. of ICT requests and of requests actioned as per SLA • Average resolution time for incidents • Nr. of Segregation of duties conflicts (target: zero) • Nr. of training sessions regarding ICT security & of people attended; Attendance rate
IV. ISO 45001 Occupational health and safety management systems	• accident-free working days • work-related incidents/accidents/near misses • provide and ensure attendance at OH&S training	• Nr. of work-related incidents (target: zero); Lost time due to OH&S issues • Nr. of safe (i.e., free of accident, OH&S incidents, injuries) working days • Nr. of OH&S training provided, & of people attended; Attendance rate
V. ISO 28001 Security management systems for the supply chain	• Conduct supply chain security assessment and define actions for gaps and development opportunities	• Reduce lead time of delivery • Increase preferred supplier purchases
VI. ISO 50001 Energy management systems; Energy and other infrastructure	• Review energy-absorbing processes (e.g., production units or office buildings) and seek for energy optimalisation solutions • Energy performance measured, energy data tracked and analysed • Improve energy efficiency by v%	• Energy consumption metrics • Nr of identified optimalisation solutions • Financial amount of gained efficiency

Security group with ISO standards	Objective	Measurement - Performance indicators
VII. ISO 14001 Environmental management systems	• Minimise the environmental impact of the operation by: • Reducing emissions in the supply value chain by x% • Increase renewable energy/material consumption in favour of non-renewable by y% • Increase reused material consumption in favour of traditional materials by z% • Identify improvement areas • Persons employed aware of their obligations regarding environmental management	• Percentage of completion achieved compared to the target values (x;y;z) • Nr. of CI projects (open, completed) and gained efficiency • Nr. of training sessions regarding environment preservation & of people attended; Attendance rate
VIII. ISO 37001 Anti-bribery	• Combat bribery-, and terrorist financing	• Nr. of anti-bribery-, and terrorist-financing-related breaches, incidents (target: zero)

more, it helps to ensure environmentally conscious, sustainable operations. Below, the authors broadly outline a walkthrough of the key points to identify the proper performance measurements and targets for an organisation.

Walkthrough to identify energy performance objectives and targets. The basic value of the energy savings depends on the nature of the entity's facility, i.e., whether it is productive (production plant factory) or non-productive (office building).

In the case of a non-production enterprise facility, important factors are the energy demand of technological processes, previous assessments of efficiencies, their previous analysis, and the type of available historical data. Based on this analysis, it is advisable to examine the possibility of modernisation. It is advisable to investigate the possibility of reducing energy demand and costs, to consider investing in heat recovery equipment, which can be done based on the knowledge of technologies, and alternative energy replacement, which is also expensive. Therefore, an impact analysis is required. The solar system is reliable in the long term, and a solar collector is also very good in the case of a high demand for hot water. However, during the planning, care must be taken to ensure the safe removal of heat due to overheating (heating-up) during the shutdown period without heat consumption. The possibility of building a heat pump system should also be investigated.

In the case of a non-production enterprise facility, the heat demand and its heat supply, as well as the heat removal (cooling demand) of the building complex along with the production plants, must be considered. It is important to solve the energy demand of the energy consumers operating during operation, as well as the associated heat generation and the removal of excess heat. How does this happen? Is there a heat recovery device built into the ventilation system? Is it possible to use computer equipment with lower energy needs and to evaluate building properties by evaluating the energy consumption data of the previous period? The modernisation and transition to a more favourable energy source for non-production facilities is in many ways the same as for production plants, but it depends on the company's profile, strategic plans and available financial funds, and the resource needs also vary. For example, the domestic hot water demand will probably be lower, and the work schedule, the working hours, and the resulting distribution of the energy demand on the time axis will be different.

VII. Environment management. Minimising environmental impact of corporate operations has become more and more relevant. To have a clear view on environmental impact of the operation, to identify environmental risks and improvement areas are important steps in the successful environmental management process.

VIII. Anti-bribery. Combating bribery and terrorist financing is an important topic for companies. This demonstrates the need for robust anti-bribery controls. Management of anti-bribery controls should be present in all contexts where the risk can arise, e.g., employees, customers, vendors, and any counterparts.

Table 2 contains generic performance objectives and measurement indicators per Security groups

(I–VIII) together with the corresponding ISO standards. All this can serve as a good practice and is recommended as a model when implementing a comprehensive security management system as a whole or in part.

3.2.2. "Security Balanced Scorecard" — the new Balanced Scorecard based on security groups

Security objectives and goals are a subset of corporate strategy, and in the changing business and risk environment, their role has become increasingly important. The integrated risk management approach also promotes the treatment of security management processes as an inherent part of the corresponding business processes. The Balanced Scorecard is implemented based on strategic objectives, which should be linked to performance goals and measures related to the four perspectives of the Balanced Scorecard.

Fig. 1 lists strategic objectives related to the categories of the Security BSC. The categories are linked to relevant ISO standards.

Table 3 presents performance goals and measures with reference to Security groups. The structure of the Security Balanced Scorecard follows the structure of the original Balance Scorecard, i.e., the financial, customer, and internal process, as well as innovation and learning perspectives, together with performance goals and measures. The Security BSC adopts the structure of the original BSC and applies it from the security perspective. The Security groups of the Security BSC were defined in line with the related ISO standards. The Security BSC contains generic security performance goals and measures that can be tailored and leveraged by any organisation.

4. Discussion

The application of standard management systems helps organisations to achieve their objectives. These systems cover different objectives. Processes perform well when the underlying security objectives are met. The objectives of management system standards are security-oriented and contribute to the increase in process performance. Management systems are linked to the continuous improvement mindset. Furthermore, these systems pay sound attention to training and development. These factors also contribute to increased process security. The attestation of an independent certification body of the management system has sound requirements. In case these requirements are met, an organisation is able to demonstrate the performance of its management system, which increases the level of process security.

As for information security, the ISO/IEC 2700x family of information security management system standards and guidelines serve as a common language worldwide for engaging in business securely (Hum-

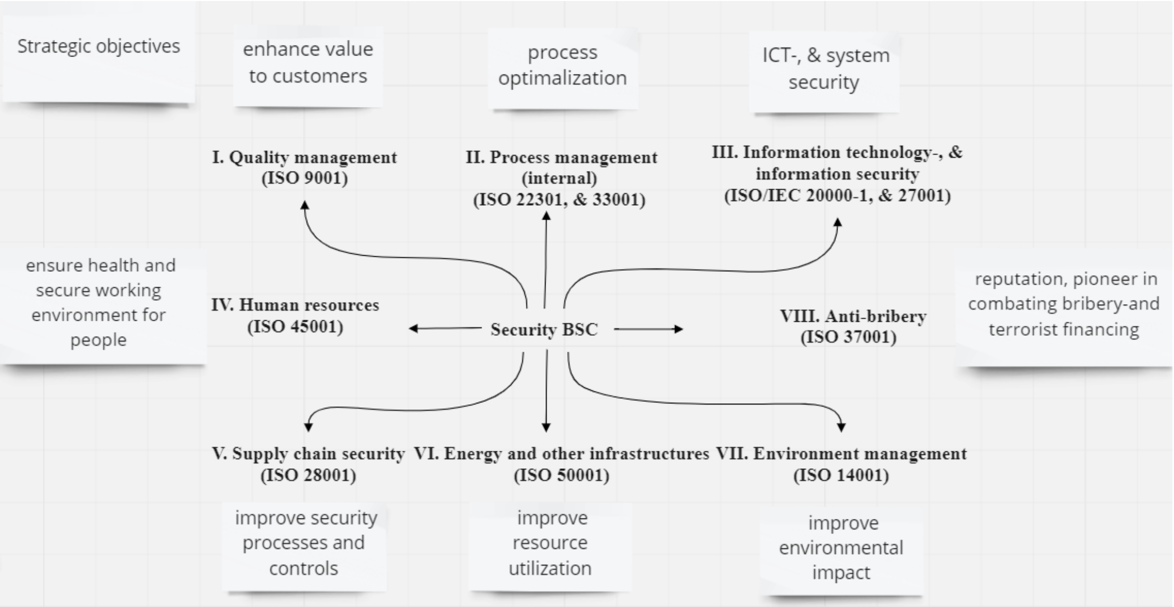
Strategic objectives
enhance value to customers
process optimalization
ICT-, & system security
I. Quality management (ISO 9001)
II. Process management (internal) (ISO 22301, & 33001)
III. Information technology-, & information security (ISO/IEC 20000-1, & 27001)
ensure health and secure working environment for people
IV. Human resources (ISO 45001)
Security BSC
VIII. Anti-bribery (ISO 37001)
reputation, pioneer in combating bribery-and terrorist financing
V. Supply chain security (ISO 28001)
VI. Energy and other infrastructures (ISO 50001)
VII. Environment management (ISO 14001)
improve security processes and controls
improve resource utilization
improve environmental impact

Fig. 1. Pillars and Strategic objectives related to the Security Balanced Scorecard

Tab. 3. Performance goals and measures related to the Security Balanced scorecard

Security Balanced Scorecard					
Reference to Security groups with ISO standards in Tab. 4.	**Financial perspective**		**Reference to Security groups with ISO standards in Tab. 4.**	**Customer perspective**	
	goals	**measures**		**goals**	**measures**
I. QMS	Profitability - going concern	Cash flow; Income; Expenses	I. QMS	Customer satisfaction	Customer satisfaction index (customer value: price, quality, reliability of products and services, availability-delivery time)
I. QMS	Reliability of financial reporting	Adequate internal processes; internal control reviews; audit findings (internal; external)	I. QMS	Market share	Key accounts; customer acquisition, retention
I. QMS; II. Process management; III. ICT security; IV. OH&S	Stable operation	Time spent due to lost time related to process failure, incident; returned product/complaints; customer orders processed on time			
III. ICT / data related compliance (Confidentiality, GDPR etc.); IV. OH&S; V. Supply chain; VII. Environment; VIII. Anti-bribery	Compliance with law, regulations	No fines due to non-compliance			
V. Supply chain; VI. Energy	Improve cost structure, optimalization solutions	Cost reduction, reduced expenses			
I. QMS; II. Process management; III. ICT security	Project management	Budgeting and results (end-to-end tracking)			
Reference to Security groups with ISO standards in Tab. 4.	**Internal business perspective**		**Reference to Security groups with ISO standards in Tab. 4.**	**Innovation & learning perspective**	
	goals	**measures**		**goals**	**measures**
II. Process management (BCM, IT service)	Provide fast response to unexpected events	Efficiency of BCM readiness; SLAs - service quality	I-VIII.	Improve ICT-, and system security level	Gap analysis; development projects/actions; Continuous improvement projects (open, closed)
II. Process management	Simplify processes, minimize potential problems	Security incidents, near misses	I-VIII.	Corporate security culture	Staff security attitude survey; development trainings (on-the-job; classroom; online)
I. QMS	First pass yield	Rework, complaint	I-VIII.	Employees' competences	Training
IV. OH&S	Preserve employee health and safety	Safe working days	I-VIII.	Employees' commitment	Employee satisfaction index; Employee retention index
V. Supply chain security	In-time delivery	Reduced lead time			

phreys, 2011). The ISO/IEC 2700x standard package, differently from other management system standards, contains a risk management standard dealing with information security (ISO/IEC 27005). This proves the importance of risk management in the field of information protection. An ISO/IEC 27001-certified business must have put in place all protection measures that were specified in the standard (Kitsios et al., 2023). The certification of the information security management system guarantees that the information security requirements are met through the implemented controls; the certification helps to build trust in an organisation's capacity, as well as reduces the risks (incl. business loss, the risk of fines or compensation payments due to legal disputes) and helps to prevent security breaches (Disterer, 2013; Saint-Germain, 2005). Furthermore, successful implementation of ISO/IEC 27001 requires that employees provide their full support and contribution (Kitsios et al., 2023). Given the significant risk exposure that comes from inside the organisation (Arsenault, 2023; ENISA, 2006; van Zadelhoff, 2016), the information security management system contributes to reducing the risks related to the human factor.

The systematic approach to standard management systems, clear processes, and the list of steps defined as a part of management system are in support of process performance management as well.

The Balanced Scorecard approach is a sound approach to measuring process performance since it pays attention to financial, customer, internal business, and learning and development perspectives. These perspectives are interconnected. This interconnected nature represents the context of security matters as well and is found to be a good basis for the purposes of this research. For this reason, the new Balanced Scorecard leverages the benefits of the Balanced Scorecard methodology and that of standard management systems, which are well aligned with corporate objectives.

The BSC has been successfully used by many different organisations to measure and evaluate performance (Mendes Jr. & Alves, 2023). The BSC is regarded as one of the most influential strategy implementation and control tools, but data about its impact on performance is mixed (Tawse & Tabesh, 2023). The BSC can be viewed critically, e.g., as a new fashion in management or a consulting product. Its underlying assumption is that organisations implement a strategy in a rational top-down process or that this is built on notions of strong organisational control (Madsen & Stenheim, 2015).

Many studies show that the BSC can be successfully implemented in large-scale companies and organisations. The BSC appears to be suitable for all types and sizes of businesses, large and small. However, based on research data from 500 companies in the UK and Cyprus, very few small companies use the BSC, especially in the UK (Giannopoulos et al., 2013). There are good examples beyond the business sector as well, such as higher education (Mendes Jr. & Alves, 2023) or healthcare (Amer et al., 2022; Peters et al., 2007), where the BSC is proven to be an effective strategic management tool.

However, the concept of the BSC can be utilised as a meaningful tool in support of process performance measurement and in particular to develop it further for the purposes of security process measurement. Regardless the criticism, the implementation and operation of the BSC should happen in a way that it can well support organisational objectives.

There are studies that deal with the BSC in the context of safety such as adaptation of the BSC to measure organisational safety culture (Mohamed, 2003), occupational health and safety (Mearns & Håvold, 2003), health, safety and environment management systems (Beheshti et al., 2018; Azour et al., 2017), school safety performance (Alolah et al., 2014), to improve maritime safety through enhancing marine process management (Lin & Cheng, 2021), etc. There are studies on security matters, e.g., the BSC is researched from the perspective of information security (Fatkieva & Krupina, 2020; Herath et al., 2023) or information security investment decisions (Tallau et al., 2010).

As a subject of the current article, the BSC approach is applied to a number of security areas in the context of standard management systems. The outlined new concept of the Security BSC, i.e., the subject of this paper, offers a comprehensive approach that uses standard management systems and explores security groups linked to standard management systems (i.e., controlling areas, such as quality management, process management, information technology and information security, human resources, supply chain security, energy and other infrastructures, environmental management, or anti-bribery measures). This Security BSC presents an integrated approach to different security matters. It can serve as a best practice to address security process performance at the organisational level and is recommended as a model when implementing a comprehensive security management system in whole or in part.

Conclusions

Process security is crucial for businesses and state-owned entities. To establish, maintain and reinforce process security, it is recommended to use state-of-the-art methods and tools.

The results of the research show that the application of management system standards supports process security. It has been proven that the certification of management systems increases the level of process security.

The analysis of the ISO standard certifications has shown the dominance of the ISO 9001 quality management standards. Building and maintaining a quality management system is a good basis for establishing further management systems. Quality management is also a mindset embedded in the possibility of continuous improvement initiatives. The delivery of quality products and services helps organisations to be resilient, maintain more transparent processes, operate processes with less "waste", and be more efficient and effective. This requires significant efforts when adopting a quality management system and continuous maintenance. The commitment to this way of working generates real value not only for the customers but for the organisation itself. Thus, it contributes to long-term corporate success. Obtained and maintained ISO management system certifications helps to demonstrate management efforts to stakeholders. Moreover, diligent audits help to improve the management system.

The analysis has shown that the top three ISO certificate types in the EU-27 cover 94.1 % of the reviewed population. The top three certified management system standards were the ISO 9001 Quality management (67.6 %), the ISO 14001 Environment management (19.3 %), and the ISO 45001 Occupational health and safety management (7.3 %). The distribution of certificates in relation to various standards was relatively even amongst the different economic sectors with some — typically sector-specific — concentrations. Mostly, the participants in the information technology sector had a certified information security management system, information technology service management, and business continuity management systems related to ISO standards.

Process performance measures, aka KPIs, should be tracked over time and compared to targets. This living process provides management with regular information on the state of the organisation and its specific units' performance and provides the framework for follow-ups when and where there is a discrepancy. Also, it helps to identify development opportunities. With respect to security performance indicators, it is advisable to find the right balance in proactively defining measures and focusing not only on what went wrong but also on the achievements and results of the security management process. It is advisable to find an optimal number of performance measures focusing on the most critical ones. The number of performance indicators should be just enough to give the proper status of the measured processes and should not be too much. Otherwise, information overload can occur, making it harder to focus on the most important items. The creation of a too-complex system is undesirable. Simplicity is a recommended direction. The focus should be on creating a simple system that contains the most important and critical items and that is easier to be managed. It is also advisable to consider starting from scratch when creating a system of performance measures that is simple and fit for purpose.

The Balanced Scorecard encompasses performance measures in financial, customer, internal process, and innovation and learning categories. These categories are closely interlinked, so the measures should be applied and interpreted comprehensively, looking at the cause-and-effect relationships. The goals and measures of the scorecard should be derived from the strategy. The authors have prepared a brief walkthrough to identify energy performance objectives and targets to illustrate the process behind each process performance measure. The research has led to the development of the Security Balanced Scorecard. The recommended set of process performance measures in the Security Balanced Scorecard helps the management to see the most important measures at a glance and view the effects of particular decisions. This promotes system thinking and better decision-making. The controlling areas of the new, security-focused Balanced Scorecard are based on management system standards, which cover the most important and critical controlling areas of different entities. The introduced list of recommended security process measures can be leveraged as good practices for any organisation and selected according to the organisation's goals.

The research is based on a thorough literature review related to the research area and standard management systems. It aimed to exhaust the research scope to offer a fair recommendation for the Security Balanced Scorecard. However, the recommendation should be reevaluated for possible changes in the future. The future direction of the research will be to integrate the research field with further research objectives.

Literature

Alolah, T., Stewart, R. A., Panuwatwanich, K., & Mohamed, S. (2014). Determining the causal relationships among balanced scorecard perspectives on school safety performance: Case of Saudi Arabia. *Accident Analysis & Prevention*, *68*, 57-74.

Amer, F., Hammoud, S., Khatatbeh, H., Lohner, S., Boncz, I., & Endrei, D. (2022). The deployment of balanced scorecard in health care organisations: is it beneficial? A systematic review. *BMC Health Services Research*, *22*(1), 1-14.

Anthony, R. N. (1965). *Planning and control systems: a framework for analysis*. Boston: Harvard Business School.

Arsenault, B. (2023). *Your Biggest Cybersecurity Risks Could Be Inside Your Organisation*. Harvard Business Review. Retrieved from https://hbr.org/2023/03/your-biggest-cybersecurity-risks-could-be-inside-your-organisation

Azour, F., Moussami, H. E., Dahbi, S., & Ezzine, L. (2017). Integration of health and safety at work and environment perspectives in the balanced scorecard. *Proceedings of the International Conference on Industrial Engineering and Operations Management Rabat Morocco*, 1113-1121.

Badreddine, A., Romdhane, T. B., & Amor, N. B. (2009). A New Process-Based Approach for Implementing an Integrated Management System: Quality, Security, Environment. *International Multi-Conference of Engineers and Computer Scientists*, 1742-1747.

Bakhtina, M., Matulevičius, R., & Seeba, M. (2023). Tool-supported method for privacy analysis of a business process model, *Journal of Information Security and Applications*, *76*. doi: 10.1016/j.jisa.2023.103525

Beheshti, A. R., Kamali, K., Arghami, S., & Mohammadi, A. (2018). Assessing the Performance of the Health, Safety and Environment Management System (HSE) using the Modified Balanced Scorecard Model. *Journal of Iranian Medical Council*, *1*(2), 87-95.

Čiutienė, R., Čiarnienė, R., & Gaidelys, V. (2022). Safety and Health at the Workplace in the Context of COVID-19: The Case of a Dental Clinic. *Engineering Management in Production and Services,14*(2), 95-105. doi: 10.2478/emj-2022-0019

Corrales-Estrada, A. M., Gómez-Santos, L. L., Bernal-Torres, C. A., & Rodriguez-López, J. E. (2021). Sustainability and Resilience Organisational Capabilities to Enhance Business Continuity Management: A Literature Review. *Sustainability*, *13*(15), 8196. doi: 10.3390/su13158196

Daubner, L., Macak, M., Matulevičius, R., Buhnova, B., Maksović, S., & Pitner, T. (2023). Addressing insider attacks via forensic-ready risk management, *Journal of Information Security and Applications*, *73*. doi: 10.1016/j.jisa.2023.103433

Davis, R. (2008). Aris Design Platform (Advanced Process Modelling and Administration). Springer London Ltd.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2), 92-100. doi: 10.4236/jis.2013.42011

ENISA. (2006). Risk Management – Principles and Inventories for Risk Management/Risk Assessment methods and tools. Trusted Business Partners Technical Department of ENISA Section Risk Management ENISA.

Erazo-Chamorro, V. C., Arciniega-Rocha, R. P., Nagy, R., Babos, T., & Szabo, Gy. (2022). Safety Workplace: The Prevention of Industrial Security Risk Factors. *Applied Sciences*, *12*(21). doi: 10.3390/app122110726

European Union. (2022). Country profiles EU-27. Retrieved from https://european-union.europa.eu/principles-countries-history/country-profiles_en

Fatkieva, R., & Krupina, A. (2020). Enterprise Information Security Assessment Using Balanced Scorecard. Advances in Automation: Proceedings of the International Russian Automation Conference, RusAutoCon 2019, September 8-14, 2019, Sochi, Russia, 1147-1157.

Fiore, A. P., Facin, A. L. F., & Muniz, J. Jr. (2023). Information security and quality management systems integration: challenges and critical factors. *International Journal for Quality Research*, *17*(3), 635-650.

Giannopoulos, G., Holt, A., Khansalar, E., & Cleanthous, S. (2013). The use of the balanced scorecard in small companies. *International Journal of Business and Management*, *8*(14), 1-22. doi: 10.5539/ijbm.v8n14p1

Graneheim, U. H., Lindgren, B. M., & Lundman, B. (2017). Methodological challenges in qualitative content analysis: A discussion paper. *Nurse Education Today*, *56*, 29-34.

Hammer, M., & Champy, J. (1993). Reengineering the Corporation: A Manifesto for Business Revolution. *HarperBusiness.* doi: 10.1016/S0007-6813(05)80064-3

Herath, T. C., Herath, H. S., & Cullum, D. (2023). An information security performance measurement tool for senior managers: Balanced scorecard integration for security governance and control frameworks. *Information Systems Frontiers*, *25*(2), 681-721. https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/0

Humphreys, E. (2011). Information security management system standards. *Datenschutz und Datensicherheit – DuD*, *35*(1), 7-11. doi: 10.1007/s11623-011-0004-3

International Organisation for Standardization (ISO). Management System Standards. Retrieved from https://www.iso.org/management-system-standards.html

ISO 14001:2015. Environmental management systems — Requirements with guidance for use.

ISO 22301:2019. Security and resilience — Business continuity management systems — Requirements.

ISO 28000:2022. Security and resilience — Security management systems — Requirements.

ISO 28001:2007. Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance.

ISO 31000:2018. Risk management — Guidelines.

ISO 37001:2016. Anti-bribery management systems — Requirements with guidance for use.

ISO 45001:2018. Occupational health and safety management systems — Requirements with guidance for use.

ISO 50001:2018. Energy management systems — Requirements with guidance for use.

ISO 9001:2015. Quality management systems — Requirements.

ISO Survey of certifications to management system standards – Full results. Retrieved from https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

ISO. (2019). *ISO 9001: 2015 How to use it*. International Organisation for Standardization. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100373.pdf

ISO. (2021). The ISO Survey of Management System Standard Certifications – 2020 – Explanatory Note. International Organisation for Standardization. Retrieved from

ISO/IEC 20000-1:2018. Information technology — Service management — Part 1: Service management system requirements.

ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.

ISO/IEC 27001:2013/Cor 1:2014. Information technology — Security techniques — Information security management systems — Requirements — Technical Corrigendum 1.

ISO/IEC 27001:2013/Cor 2:2015. Information technology — Security techniques — Information security management systems — Requirements — Technical Corrigendum 2.

ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection Information security management systems Requirements.

ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection Guidance on managing information security risks.

Kaplan, R. S., & Norton, D. P. (1992). The balanced scorecard: measures that drive performance. *Harvard Business Review*, *70*(1), 71-79.

Kaplan, R. S., & Norton, D. P. (1993). Putting the balanced scorecard to work. *Harvard Business Review*, *71*(5), 134-147.

Keen, R. (2022). *Benefits of and Environmental Management System*. Retrieved from https://www.iso-9001-checklist.co.uk/ISO-14001/benefits-of-an-environmental-management-system.htm

Kemendi, A. (2022). The safety-net – the safety network of controls [A biztonság hálózata - a kontrollok biztonsági hálózata]. *Current Social and Economic Processes* [*Jelenkori Társadalmi és Gazdasági Folyamatok*], *17*(1-2), 77-90. doi: 10.14232/jtgf.2022.1-2.77-90

Kemendi, A., Michelberger, P.; & Mesjasz-Lech, A. (2021). ICT security in businesses – efficiency analysis, *Entrepreneurship and Sustainability Issues*, *9*(1), 123-149. doi: 10.9770/jesi.2021.9.1(8)

Kern, S., Baumer, T., Groll, S., Fuchs, L., & Pernul, G. (2022). Optimization of Access Control Policies. *Journal of Information Security and Applications, 70*. doi: 10.1016/j.jisa.2022.103301

Kilpatrick, J. (2003). Lean principles. *Utah Manufacturing Extension Partnership*, *68*(1), 1-5.

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*, *15*(7), 5828.

Labodová, A. (2004). Implementing integrated management systems using a risk analysis based approach. *Journal of Cleaner Production, 12*(6), 571-580. doi: 10.1016/j.jclepro.2003.08.008

Lin, W. C., & Cheng, H. H. (2021). Improving maritime safety through enhancing marine process management: The application of balanced scorecard. *Management Decision*, *59*(3), 604-615.

Lindgren, B.-M., Lundman, B., Graneheim, U. H. (2020). Abstraction and interpretation during the qualitative content analysis process. *International Journal of Nursing Studies*, *108*. doi: 10.1016/j.ijnurstu.2020.103632

Madsen, D. Ø., & Stenheim, T. (2015). The Balanced Scorecard: A Review of Five Research Areas. *American Journal of Management*, *15*(2), 24-41.

Malina, M. A., & Selto, F. H. (2001). Communicating and Controlling Strategy: An Empirical Study of the Effectiveness of the Balanced Scorecard. *SSRN*. doi: 10.2139/ssrn.278939

Mearns, K., & Ivar Håvold, J. (2003). Occupational health and safety and the balanced scorecard. *The TQM Magazine*, *15*(6), 408-423.

Mendes, Jr., De Jesus Alvares, I., & Alves, M. D. C. (2023). The balanced scorecard in the education sector: A literature review. *Cogent Education*, *10*(1), 2160120.

Michelberger, P. (2014). Risk Management for Business Trust. In: Michelberger, P. (Ed.) *MEB 2014: Management. Enterprise and Benchmarking in the 21st Century* (pp. 401-413). Budapest, Hungary: Óbuda University.

Michelberger, P., & Kemendi, A. (2020). Data, information and IT security – software support for security activities. *Problems of Management in the 21st Century*, *15*(2), 108-124. doi: 10.33225/pmc/20.15.108

Mohamed, S. (2003). Adaptation of the balanced scorecard to measure organisational safety culture. *Journal of Construction Research*, *4*(01), 45-57.

O'Neill, P., & Sohal, A. S. (1999). Business Process Reengineering A review of recent literature. *Technovation, 19* (9), 571-581. doi: 10.1016/S0166-4972(99)00059-0

Peters, D. H., Noor, A. A., Singh, L. P., Kakar, F. K., Hansen, P. M., & Burnham, G. (2007). A balanced scorecard for health services in Afghanistan. *Bulletin of the world Health Organisation*, *85*(2), 146-151.

Porter, M. E. (1985). *Competitive Advantage Creating and Sustaining Superior Performance.* New York, USA: Free Press.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal – Prairie Village*, *39*(4), 60.

Strauss, E., & Zecher, Ch. (2013). Management Control Systems: A Review, *Journal of Management Control, 23*, 233-268. doi: 10.1007/s00187-012-0158-7

Swuste, P., Theunissen, J., Schmitz, P., Reniers, G . , & Blokland, P. (2016). Process safety indicators, a review of literature. *Journal of Loss Prevention in the Process Industries, 40*, 162-173. doi: 10.1016/j.jlp.2015.12.020

Tallau, L. J., Gupta, M., & Sharman, R. (2010). Information security investment decisions: evaluating the balanced scorecard method. *International Journal of Business Information Systems*, *5*(1), 34-57.

Tawse, A., & Tabesh, P. (2023). Thirty years with the balanced scorecard: What we have learned. *Business Horizons*, *66*(1), 123-132.

Tworek, K. (2023). IT reliability as a source of sustainability for organisations operating during the COVID-19 pandemic. *Engineering Management in Production and Services,15*(1) 29-40. doi: 10.2478/emj-2023-0003

Ulewicz, R., & Kucęba, R. (2016). Identification of problems of implementation of Lean concept in the SME sector.

Engineering Management in Production and Services, *8*(1) 2016, doi: 10.1515/emj-2016-0002

van der Aalst, W. M. P., La Rosa, M. & Santoro, F. M. (2016). Business Process Management: Don't Forget to Improve the Process!. *Business and Information Systems Engineering, 58*(1), doi: 10.1007/s12599-015-0409-x

van Zadelhogg, M. (2016). *The Biggest Cybersecurity Threats Are Inside Your Company*. Harvard Business Review. Retrieved from https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

Wallace, T. F., Kremzar, M. H., & Kremzar, M. (2001). *Erp – Making It Happen; The Implementers' Guide to Success with Enterprise Resource Planning.* John Wiley & Sons.

Wolter, C., Menzel, M., Schaad, A., Miseldine, P., & Meinel, C. (2009). Model-driven business process security requirement specification. *Journal of Systems Architecture*, *55*, 211-222. doi: 10.1016/j.sysarc.2008.10.002