Information Security Journal: A Global Perspective

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uiss20

Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis

M. Suorsa & P. Helo

To cite this article: M. Suorsa & P. Helo (18 Oct 2023): Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2023.2270984

To link to this article: https://doi.org/10.1080/19393555.2023.2270984

© 2023 The Author(s). Published with license by Taylor & Francis Group, LLC.

Published online: 18 Oct 2023.

Submit your article to this journal

Article views: 165

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=uiss20

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
https://doi.org/10.1080/19393555.2023.2270984

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis

M. Suorsa and P. Helo

School of Technology and Innovations, University of Vaasa, Vaasa, Finland

ABSTRACT

This paper identifies the failures and impacts of information security, as well as the most effective controls to mitigate information security risks in organizations.Root cause analysis was conducted on all year 2020 GDPR penalty cases ($n = 81$) based on misconduct as defined in GDPR article 32: "security of processing." ISO/IEC 27,001 controls were used as failure identifiers in the analysis. As a result, this study presents both the most frequent and most expensive information security failures and correspondingly ranks and presents the correlation of the controls observed in the analysis. From a theoretical perspective, our study contributes by bridging the gap between regulation and information security and introduces a statistical method to analyze the GDPR penalty cases, and provides previously unreported findings about information security failures and their respective solutions. From a practical perspective, the results of our study are useful for organizations which aspire to manage information security more effectively in order to prevent the most typical and expensive information security failures. Organizations, as well as auditors implementing and assuring the ISO 27001, may use our results as a guideline whereby controls should be applied and verified first in sequential order based on their impact and interdependence

KEYWORDS

Information security; ISO 27001; GDPR; General Data Protection Regulation

1. Introduction

Information in its various forms is the most important asset of an organization; thus, failures in information security may not only threaten the integrity of organizations, but even their very existence (Gerber & von Solms, 2008). The primary objective of information security, the protecting of the confidentiality, integrity, and availability of information (Chapple et al., 2018), requires administration and governance (von Solms, 2006), whereby organizations' IT governance, risk management, and compliance function need to take decisions based on data-driven performance measurement metrics (Vaibhav, 2022).

International standardization frameworks play a necessary role in governing, assuring, and certifying effective information security in organizations (Siponen & Willison, 2009). The ISO/IEC 27,001 is considered the de facto standard on how information security is managed, and it functions as the criterion for determining the quality, breadth, and depth of an organization's security controls (Calder & Gerard, 2013). Similar commonly used control frameworks are, e.g. The National Institute of Standards and Technology (NIST), Cyber Security Framework (CSF), and Control Objectives for Information and Related Technologies (COBIT) (Sulistyowati et al., 2020).

Legal aspects in terms of complying with information security and privacy regulation are becoming increasingly complex (Gerber & von Solms, 2008). The European Union General Data Protection Regulation (GDPR) aims to protect the privacy of EU citizens and consequently requires all organizations operating within the EU to have adequate control of information security (Regulation (EU) 2016/679). Violating the GDPR can lead to substantial financial penalties, and many have already been enforced (Ruohonen & Hjerppe, 2022).

Simultaneously, worldwide, many comparable regulatory frameworks, such as the GDPR, form a blueprint for how personal data may be protected and processed in a secure way. Developments similar to GDPR are the California Consumer Privacy Act (CCPA) (cf. Thomas, 2020), Brazil's *Lei Geral*

CONTACT M. Suorsa k83110@student.uwasa.fi School of Technology and Innovations, University of Vaasa, PB 700, Vaasa 65101, Finland

© 2023 The Author(s). Published with license by Taylor & Francis Group, LLC.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

de Proteçao de Dados (LGPD) (cf. Macedo, 2021), India's Personal Data Protection Bill (PDPB) (cf. Deva & Suchithra, 2020), and Japan's Act on Protection of Personal Information (cf. Higashizawa & Aihara, 2017).

In order to govern information security and compliance with regulation, intelligence on information security failures and controls to effectively manage these failures are becoming ever more important (von Solms, 2006). The identification, ranking, and selecting of the most important information security controls is a fundamental step toward mitigating the risks and threats, but it is also a very tricky process, and has been a major management challenge for years (Tariq et al., 2020). Thus, more research efforts are needed to minimize the gap between regulation and information security (Dlamini et al., 2009).

Early GDPR penalties have already been studied (cf. Presthus & Sønslien, 2021). However, no studies have so far been conducted explicitly to analyze GDPR penalty cases with statistical methods to identify information security failures with control frameworks such as the ISO/IEC 27,001:Calder & Gerard, 2013. Likewise, standardization frameworks and ISO 27,001 have been utilized to construct capability maturity models to assess the information security posture of an organization (cf. Lopez-Leyva et al., 2020; Monev, 2020), but they do not rank the ISO/IEC 27,001:Calder & Gerard, 2013 controls based on their impact and interdependence.

Assessing information security can be a complicated and costly operation, thus simple analysis method should be applied. Root cause analysis (RCA) is an effective method to achieve this goal (York et al., 2014). This study presents a novel method to analyze information security failures of organizations with GDPR penalties. In this paper, we apply the RCA method to measure information security failures as identified and measured by analyzing European Union General Data Protection Regulation (GDPR) penalty cases. All year 2020 penalties ($n = 81$) throughout the EU member countries based on the definition of misconduct in GDPR article 32, "security of processing," were analyzed and matched with ISO/IEC 27,001:Calder & Gerard, 2013 standard controls. Our study matches the information security standard controls and the statistics from penalty cases, and provides previously unreported information about information security failure volumes and correlations within different industry domains.

The research problem of this paper is to identify and explore the failures and impacts of information security, as well as the most effective controls to mitigate the information security risks in organizations. More specific research questions are as follows:

RQ 1: What are the most frequent and most expensive information security failures corresponding to ISO 27,001 controls?

RQ 2: How many information security failures corresponding to ISO 27,001 controls typically exist in a GDPR penalty case?

RQ 3: How do the information security failures corresponding to ISO 27,001 controls correlate

RQ 4: Are there any industry type differences in information security failures and penalties?

The remainder of the paper is structured as follows. Section 2 presents a literature review and explores important aspects of GDPR, and positions the ISO/IEC 27,001:Calder & Gerard, 2013 standard in an IT governance, risk management and compliance (IT-GRC) framework. Section 3 presents the material and methodology of the study. The results of the study are presented and discussed in section 4. Finally, section 5 concludes the paper, presenting theoretical and practical contributions as well as the limitations and future direction of the study.

2. Literature review

In this section, the important features and relevant literature of GDPR and ISO 27,001 are presented and positioned in the IT governance, risk management and compliance (IT-GRC) framework. Table 1 presents the most relevant literature reviewed, bringing forth the research gap as well as positioning the IT-GRC as the overarching domain, governing information security with compliance with regulation and control frameworks.

Table 1. Literature review.

Authors	Category	Study design	Purpose
Selzer et al.(2021)	GDPR	Interviews	GDPR article 32 implementation impact
Ruohonen and Hjerppe (2022)	GDPR	GDPR penalty case document analysis with text mining technique	GDPR penalty impacts of individual articles
Presthus and Sønslien (2021)	GDPR	GDPR penalty case document analysis and interviews	GDPR penalty impacts of individual articles
Akhlaghpour et al., (2021)	GDPR	GDPR penalty case document analysis	GDPR compliance risk identification and categorization
Wolff and Atallah (2021)	GDPR	GDPR penalty case document analysis	GDPR violation type and penalty amount categorization
Wei et al., (2020)	GDPR	Privacy and security risk assessment tool design	Proposal of privacy and information security risk assessment tool
Osden and Lubbe (2009)	IT-GRC	Case study and interview	IT-GRC best practices identification
Nicho et al., (2017)	IT-GRC	Case study and interview	IT-GRC integration with standardization frameworks
Vaibhav (2021)	IT-GRC	Survey of literature	IT-GRC metrics identification
Sanskriti and Astitwa (2018)	IT-GRC	Literature review	IT-GRC and ISO 27,001 relationship identification
Diamantopoulou et al., (2020)	ISO 27,001	ISO 27,001 controls and GDPR requirements analysis	ISO 27,001 and GDPR synergies
Lopes et al., (2019)	ISO 27,001	Survey	ISO 27,001 as GDPR compliance facilitator
Shojaie et al., (2014)	ISO 27,001	ISO 27,001 analysis	ISO 27,001 controls effectiveness categorization
Monev, (2020)	ISO 27,001	Information security maturity model design	Proposal of ISO 27,001 based maturity model
Khajouei et al., (2017)	ISO 27,001	Fuzzy analytic hierarchy process analysis	Information security controls ranking

2.1. The European Union General Data Protection Regulation

The European Union General Data Protection Regulation (GDPR) came into force in May 2018, and unified the diverse data protection laws throughout the EU into one regulation fit for purpose in the 21st century (Cornock, 2018). The main objective of GDPR is to safeguard the fundamental right of EU citizens to data protection and protection with respect to the processing of their personal data. GDPR lays out a wide variety of requirements as to how personal data may be processed by an organization, as well as granting individuals, also known as data subjects, many rights, which enable them to have more control over how their personal data is processed (Regulation (EU) 2016/679).

GDPR carries a paramount requirement about information security. The GDPR article 32, "security of processing," obliges organizations to implement technical and organizational measures to guarantee the adequate security of personal data. Article 32, however, does not require a specific set of such measures, because GDPR is technology neutral and grants a great deal of freedom in terms of how to realize compliance (Selzer et al., 2021). Providing only a minimum amount of guidance to meet the information security requirement, the regulation outlines examples and protection objectives, which include (Regulation (EU) 2016/679):

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services
- The ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident
- A risk-based process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The distinction between data processors and data controllers is important in GDPR. The data controller is the entity determining how personal data is used and is thus ultimately responsible for information security. For example, if a vendor hosts a website on behalf of an organization, the organization becomes the data controller, and the vendor will be the data processor (Hintze, 2018). When processing is outsourced to a processor, the controller may only contract such processors which are able to provide sufficient guarantees of adequate information security (Regulation (EU) 2016/679).

GDPR defines a data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." As a consequence

of a data breach, the data controller is obliged to make a timely report about it to the supervisory authority, as well as inform the data subjects of whether their right to privacy is significantly compromised (Regulation (EU) 2016/679).

The supervisory authorities acting in each EU member country have the task of ensuring compliance with the GDPR, and in order to fulfil this function they have various investigative and corrective powers. The most severe form of corrective power is administrative fines, where the maximum penalty is up to 20 million euros, or 4% of the total worldwide annual turnover (Regulation (EU) 2016/679). Penalties issued by the supervisory authorities are public information; thus GDPR enables transparency in cases of data breaches caused by information security failures throughout the European Union (Garrison & Hamilton, 2019).

Penalties are imposed depending on certain criteria such as the nature, gravity, and duration of the infringement, categories of personal data affected, the number of data subjects in scope, and the level of damage suffered by them, as well as aggravating or mitigating circumstances such as relevant previous infringements and the degree of cooperation with the supervisory authority. GDPR has allowed each EU member state to establish its own rules on the calculation of penalties and determine whether and to what extent penalties may be imposed on public organizations (Regulation (EU) 2016/679). The European Data Protection Board, which ensures the consistent application of GDPR, has published draft guidelines on the calculation of penalties to harmonize the methodology of the supervisory authorities (EDPB, 2022).

The relationship and interdependency between GDPR and information security is recognized in the literature (cf. Geko & Tjoa, 2018), but it is not entirely clear how information security frameworks can support compliance with GDPR (Serrado et al., 2020). However, models and tools have been proposed to assess the privacy risk, together with information security related risk, in order to assist organizations to select high-risk areas for further control actions (Wei et al., 2020).

Violations which led to GDPR penalties have already been explored and studied (cf. Ruohonen & Hjerppe, 2022, and Presthus & Sønslien, 2021). A study by Akhlaghpour et al. (2021) was conducted on 93 GDPR enforcement cases, which identified several risk categories and their associated mitigation measures. A similar study by Saemann et al. (2022) presented a work that analyzed and categorized 856 GDPR fines based on different violations, where it was found that one of the main drivers for GDPR penalties was the data subjects' complaints to authorities, or existing incidents which were a public concern.

The supervisory authorities' enforcement actions show that organizations fail to ensure adequate technical and organizational measures in implementing GDPR article 32 (Degli-Esposti & Ferrándiz, 2021). Previous studies show that penalties issued following the first 24 months after GDPR implementation were relatively conservative and did not reach the maximum threshold. Most of these early penalties were a response to privacy violations, but notably the majority of the larger fines were triggered by information security incidents, and, on average, information security violations led to relatively weightier fines than pure privacy violations (Wolff & Atallah, 2021).

Craddock (2022) argues that early GDPR fines were largely inconsistent, and proposes a methodology to forecast the amount of GDPR penalties in future, which will be much higher. Since the authorities are expected to get tougher with prosecutions (Barret, 2020), more research efforts are needed to analyze the impacts of GDPR (Hirvonen, 2022) to minimize the gap between regulation and information security (Dlamini et al., 2009).

2.2. IT governance, risk management and compliance framework

The information technology governance, risk management and compliance (IT-GRC) framework is derived from corporate governance, where the business focus is aligned with the IT management of an organization (Osden & Lubbe, 2009). The objective of IT-GRC is to implement effective management techniques with business strategies and IT, and also to manage industry standards and compliance with information security and regulatory requirements (Schlarman, 2009).

IT-GRC integrates and streamlines essential processes to manage the risks which threaten the

confidentiality, integrity, and availability (CIA) of key operations of an organization (Nicho et al., 2017), while the primary focus of information security is, similarly, the commitment to ensuring the continuous CIA of information in an organization (Chapple et al., 2018). Information security is primarily risk management, and therefore it is a fundamental element of IT-GRC (Wright, 2019), where governing decisions should be based on data-driven performance measurement metrics (Vaibhav, 2021).

Effective control frameworks are necessary when managing the information security risk within the organizational IT-GRC structure. A wide variety of information security standards to certify an organization, such as NIST and COBIT, are available, whereas the ISO/IEC 27,001:Calder & Gerard, 2013 is one of the most facilitated standards (Dharmalingam et al., 2018; Sulistyowati et al., 2020) and recommended by the literature (see, for example, Brenner, 2007; Mayer & Smet, 2017). The relationship of ISO 27,001 with successful IT-GRC is well recognized, because the standard encompasses all the necessary goals under its Information Security Management System (ISMS) to support an effective IT-GRC implementation (Sanskriti & Astitwa, 2018).

2.3. The ISO/IEC 27,001:2013 in the ISO 27,000 family of standards

The ISO/IEC 27,000 family of standards is a numbered series of international information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The correct designation for the standard includes the ISO/IEC prefix, and a suffix which is their date of publication. The formal title of ISO 27,001 standard is "Information technology – Security techniques – Information security management systems – Requirements" and is referred to simply as ISO 27,001 (ISO/IEC 27,001:Calder & Gerard, 2013).

The core of the ISO 27,001 standard requires organizations to adopt a risk-based approach and provides a model for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) to protect the confidentiality, integrity and availability of information from threats and vulnerabilities." The standard requires establishing a risk assessment framework, identifying, analyzing, and evaluating risks, and finally selecting a risk treatment plan, which is the process of building the security controls to protect the organization's information assets (ISO/IEC 27,001: Calder & Gerard, 2013).

ISO/IEC 27,001:Calder & Gerard, 2013 controls are shown in Annex A, which first has 14 control clauses, each of which is identified with one or more control objectives, which are further served by a total of 114 controls (ISO/IEC 27,001:Calder & Gerard, 2013). Table 2 presents an overview of ISO/IEC 27,001:Calder & Gerard, 2013 Annex A.

The sequential ISO/IEC 27,002:Calder & Gerard, 2013 standard, in turn, provides the best practices of how to implement an effective ISMS and guidelines for controls in ISO/IEC 27,001:Calder & Gerard, 2013 Annex A, explaining how each control works and what its objective is (ISO/IEC 27,002:Calder & Gerard, 2013). Both ISO 27,001 and ISO 27,002 are often used together, but only ISO 27,001 is required for certifying an ISMS, so they are jointly referred to as the "common language of organizations around the world for information security" (Humphreys, 2011).

ISO 27,002 was updated on February 15, 2022, and Annex A of ISO 27,001 was aligned with those changes in the last quarter of 2022. In the new versions, the number of controls has decreased from 114 to 93, and these are placed in 4 sections instead of the previous 14. In the new versions, the security controls are divided into separate sections according to their specific type, which are organizational security controls ($n = 37$), personal safety controls ($n = 8$), physical security controls ($n = 14$), and technical safety controls ($n = 34$). In the new versions, there are 11 new controls. While none of the controls were deleted, some controls were merged together (ISO/IEC 27,002:Bashofi & Salman, 2022).

Notably, ISO/IEC 27,701: is an auxiliary standard to ISO 27,001 and ISO 27,002, and it specifies requirements and provides guidance for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS). ISO 27,701 is not mandatory for ISO 27,001 certification, but it

Table 2. ISO/IEC 27,001:Calder & Gerard, 2013 Annex A.

Control clause	Control objective	Number of controls
A.5 Information security policies	A.5.1 Management direction for information security	2
A.6 Organization of information security	A.6.1 Internal organization	5
	A.6.2 Mobile devices and teleworking	2
A.7 Human resource security	A.7.1 Prior to employment	2
	A.7.2 During employment	3
	A.7.3 Termination and change of employment	1
A.8 Asset management	A.8.1 Responsibility for assets	4
	A.8.2 Information classification	3
	A.8.3 Media handling	3
A.9 Access control	A.9.1 Business requirements of access control	2
	A.9.2 User access management	6
	A.9.3 User responsibilities	1
	A.9.4 System and application access control	5
A.10 Cryptography	A.10.1 Cryptographic controls	2
A.11 Physical and environmental security	A.11.1 Secure areas	6
	A.11.2 Equipment	9
A.12 Operations security	A.12.1 Operational procedures and responsibilities	4
	A.12.2 Protection from malware	1
	A.12.3 Backup	1
	A.12.4 Logging and monitoring	4
	A.12.5 Control of operational software	1
	A.12.6 Technical vulnerability management	2
	A.12.7 Information system audit considerations	1
A.13 Communications security	A.13.1 Network security management	3
	A.13.2 Information transfer	4
A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems	3
	A.14.2 Security in development and support processes	9
	A.14.3 Test data	1
A.15 Supplier relationships	A.15.1 Information security in supplier relationships	3
	A.15.2 Supplier service delivery management	2
A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	7
A.17 Information security business continuity management	A.17.1 Information security continuity	3
	A.17.2 Redundancies	1
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	5
	A.18.2 Information security reviews	3
Total		**114**

extends the information security requirements of ISO 27,001 to take into account the protection of privacy and personally identifiable information, and provides guidance on how these requirements should be implemented (ISO/IEC 27,701:).

When placing ISO 27,001 and GDPR side by side, it is clear that even though ISO 27,001 and GDPR have different standpoints, they both apply a risk management approach to data. GDPR aims to mitigate the privacy risks of data subjects by placing various provisions on personal data processing, while ISO 27,001 obliges organizations to adopt a continuously maintained ISMS (Diamantopoulou et al., 2020), which is a compliance facilitator to support the response of organizations to the security requirements of GDPR (Lopes et al., 2019).

As the ISO 27,001 provides a deep-rooted history of development and best practices, it has been a basis for studies assessing the information security maturity and risks of organizations. However, these studies typically do not rank the ISO 27,001 controls based on their impact or provide further input on how to improve the assessed maturity and risk levels (Anass et al., 2020).

For example, Monev (2020) proposes a methodology for performing information security maturity assessment solely based on ISO 27,001 and ISO 27,002. Another study by Nungky et al. (2022) proposes a situational awareness model to assess cybersecurity risks based on Annex of ISO/IEC 27,001:Calder & Gerard, 2013.

A study by Shojaie et al. (2014) classified the ISO/IEC 27,001:Calder & Gerard, 2013 controls into categories which support organizations in evaluating and improving their ISMS performance, as well as providing understanding of relevant security flaws. Another study by Khajouei et al. (2017) provided a ranking of effective ISO/IEC 27,001 control objectives in a single case organization. For similar studies, see, for example, Lopez-Leyva et al. (2020) and

Makupi and Karume (2019). Furthermore, many of the proposed maturity models have been greatly influenced by the ISO 27,001 (cf. Al-Matari et al., 2021; Bashofi & Salman, 2022).

3. Material and method

In this section the approach to gathering and analyzing the research data is described.

3.1. Material of the study

The publicly available data source for this study is the GDPR Enforcement Tracker, which is a freely accessible website maintained by a global law firm, CMS. The database contains formal GDPR penalty case reports, which have been issued by the data protection authorities in EU member countries to organizations not complying with the regulation (GDPR Enforcement Tracker Barrett, 2020).

The database was searched with the year 2020, together with GDPR article 32 "security of processing," which resulted in 81 GDPR penalty case reports, where the penalty type was "insufficient technical and organizational measures to ensure information security." These GDPR penalty case reports formally describing and specifying information security failures accounted for the penalties issued to 81 different organizations. Out of the total of 81 GDPR penalty case reports, there were 25 cases which also included references to articles other than information security. The supervisory authorities issue penalties as a whole and do not distinguish the penalty amounts between failures in different quoted GDPR articles.

3.2. Methodology of the study

The method applied in the study was root cause analysis (RCA) to identify what caused the information security failures and what their impacts were. Root cause analysis as a method is a process which applies data collection, cause charting, root cause identification, and generation of recommendations. Only when root causes are determined can corrective measures that prevent future events of the type observed be specified (Rooney et al., 2004). The different RCA subtype methods can be summarized into the following three categories (York et al., 2014):

- Chart type RCAs, which are constructed in the style of a flow chart
- Tabular type RCAs, which are constructed in a table with predefined column headings and categories
- Graphical RCAs, which visualize the results in a bar graph or any graphical display of numerical data

Popular examples of chart type RCAs are the cause and effect diagram, current reality tree, and the cause and interrelationship diagram (Doggett, 2005). Tabular type RCAs are, for example, the 5 whys method (Card, 2016) and the Failure Modes and Effects Analysis (FMEA) (Paciarotti et al., 2014). Typical graphical RCAs are histograms and the pareto 80/20 method (York et al., 2014).

RCA as a methodology is challenged by the problem of "many hands," which means that the root causes cannot easily be pinpointed to a single individual or contributing factor responsible for the outcome or the solution that fixes the problem. RCA implies that there is only a single root cause, which often is not the case in a complex environment. RCAs also typically lack solutions to eliminate the root cause problems (Peerally et al., 2016).

The RCA method of this study is a mixture of tabular and graphical RCA types.

Each GDPR penalty case, with its respective information security failures corresponding to a specific failure identifier (ISO 27,001 control), as well as the total penalty of the case, were mapped in a table. This table, which contained

Table 3. RCA table example.

GDPR penalty case	Failure identifier a	Failure identifier b	Failure identifier c	Failure identifier n
Case 1	0	0	1	0
Case 2	1	0	1	1
Case 3	0	0	0	1
Case n	1	1	1	0

binary variables, enabled further analysis, and the graphical presentation of results is presented in Table 3.

This study was conducted before the new version of ISO/IEC 27,001:2022 was published, and therefore the criteria of this analysis were the ISO/IEC 27,001:Calder & Gerard, 2013 Annex A controls, which were used as root cause identifiers in each individual 81 GDPR penalty case.

There were 38 individual information security failures on the ISO 27,001 control level, which included five failures that could not be matched with any exact ISO 27,001 control. These five failures were included in the scope of the analysis because they were specifically addressed by the supervisory authorities, and consequently were the cause of the issued penalties. In the presented results, these unmatched information security failures do not have the ISO number prefix, unlike the failures which were mapped to a specific ISO 27,001 control. The 38 information security failures on the ISO 27,001 control level were mapped to their respective 21 control objectives and further to their respective 12 control clauses, while the five unmatched failures were mapped within their own groups.

Penalty amount calculations for each individual information security failures were first conducted separately on the ISO 27,001 control level. The total penalty amount of a single GDPR penalty case was divided by the number of information security failures that were observed in the case. For example, in a GDPR penalty case, where there were three observed information security failures and the total penalty was 600 euros, the cost of an individual failure was 200 euros. Next, the average was calculated for all information security failures, which became the penalty for each individual information security failure. Penalty amount calculations were further conducted separately on ISO 27,001 control objectives and control clauses.

The 81 GDPR penalty cases were grouped to present the number of information security failures per case, which ranged from 1 to 13. The average penalty was calculated for each of these groups.

Information security failure correlations were calculated separately on ISO 27,001 controls and further on their respective control objectives and control clauses. To emphasize their strategic significance, the ISO 27,001 controls which had very strong (0.65 and above) correlation are presented in the results. After that, the fairly strong (0.35 and above) correlation of ISO 27,001 control objectives and the correlation (0.3 and above) of ISO 27,001 control clauses are presented in the results. P-values of the Pearson correlation were used, and results where the p-value was lower than 0.05 were considered statistically significant.

Finally, all the 81 GDPR penalty cases were grouped to present the penalty amounts and frequencies in different industry sectors.

4. Results and discussion

In this section the results of the analysis and answers to the research questions are presented. Both ISO/IEC 27,002:Calder & Gerard, 2013 and ISO/IEC 27,701: standards are used for interpreting the results.

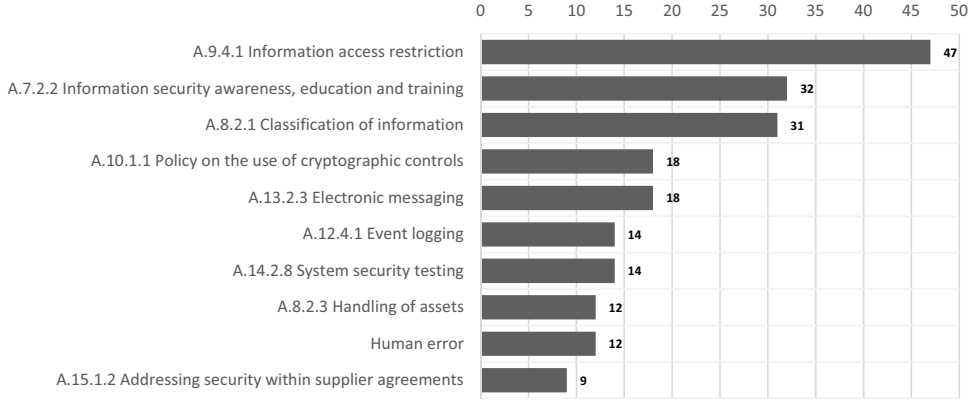

Figure 1. Top 10 most frequent information security failures corresponding to ISO 27001 controls.

4.1. The most frequent information security failures

The top 10 most frequent information security failures corresponding to ISO 27,001 controls are presented in Figure 1.

The most frequent ($n = 47$) failure is the lack of "A.9.4.1 Information access restriction." Unauthorized access to organizational data was a very common cause of a data breach. Access restrictions such as controlling which data can be accessed by a particular user, controlling the access rights of users such as read, write, delete and execute, as well as limiting the information contained in outputs, should be based on individual business application requirements in accordance with the defined access controls policy (ISO/IEC 27,002:Calder & Gerard, 2013).

The second most frequent failure ($n = 32$) are inadequacies in "A.7.2.2 Information security awareness, education and training." Shortcomings in this control can lead to a multitude of different problems if staff members do not know what is expected of them. Therefore, all employees of the organization and, where relevant, contractors, should receive appropriate awareness education and training and regular updates on organizational policies and instructions, as relevant to their job function (ISO/IEC 27,002:Calder & Gerard, 2013). ISO 27,701 further recommends ensuring that staff members are aware of the possible consequences of breaching privacy or security rules, especially those addressing the handling of personally identifiable information (ISO/IEC 27,701:). ISO 27,001 ISMS also requires organizations to determine the competence necessary for information security performance and ensure that employees have such competence through appropriate education, training, or experience (ISO/IEC 27,001:Calder & Gerard, 2013).

The third most frequent failure ($n = 31$) is lack of "A.8.2.1 Classification of information." Information shall be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification (ISO/IEC 27,001:Calder & Gerard, 2013). The organization should mandate asset owners to follow the formal classifying scheme, which further specifies how the asset should be protected (ISO/IEC 27,002:Calder & Gerard, 2013), while ISO 27,701 further recommends taking personally identifiable information into consideration (ISO/IEC 27,701:). This control applies to the GDPR article 32 requirement of having risk assessment conducted in order that adequate organizational and technical controls are further selected and implemented (Regulation (EU) 2016/679).

The fourth most frequent failure ($n = 18$) is lack of implementation of "A.10.1.1 Policy on the use of cryptographic controls," which is necessary to maximize the benefits of using cryptographic techniques and to avoid inappropriate or incorrect use. GDPR addresses encryption as a technique to secure personal data processing (Regulation (EU) 2016/679), although making a decision on whether a cryptographic solution is appropriate should be seen as part of the wider risk assessment process, which is used to determine whether a cryptographic control is appropriate and applied (ISO/IEC 27,002: Calder & Gerard, 2013). ISO 27,701 additionally guides the organization to provide information to the data subject regarding the circumstances in which it uses cryptography to protect personally identifiable information. The organization should also provide information to the data subject which can assist them in applying their own cryptographic protection (ISO/IEC 27,701:).

The fifth most frequent failure (also $n = 18$) is lack of control in "A.13.2.3 Electronic messaging." Information involved in electronic messaging shall be appropriately protected (ISO/IEC 27,001:Calder & Gerard, 2013). There are many types of electronic messaging such as e-mail, electronic data interchange, and social networking, which play a role in communications. Information security considerations should include, e.g. protecting messages from unauthorized access, or modification or denial of service in line with the risk-based classification scheme adopted by the organization (ISO/IEC 27,002:Calder & Gerard, 2013).

The sixth most frequent failure ($n = 14$) is inadequate "A.12.4.1 Event logging." Many data breaches were caused by lack of tracing of user actions in systems. Therefore, event logs recording user activities, exceptions, faults, and information security events should be produced, kept, and regularly reviewed (ISO/IEC 27,002:Calder & Gerard, 2013). ISO 27,701 provides additional guidance by

recommending a process to review the event logs, and where possible, event logs should specifically record user access to personally identifiable information (ISO/IEC 27,701:).

The seventh most frequent failure (also $n = 14$) is lack of "A.14.2.8 System security testing," which is important because GDPR requires regular testing and assessment of the effectiveness of measures for ensuring the security of processing (Regulation (EU) 2016/679). New and updated systems require thorough testing and verification during the development processes, including the preparation of detailed schedules of activities and test outputs under a range of conditions. The extent of testing should be in proportion to the importance and nature of the system (ISO/IEC 27,002:Calder & Gerard, 2013), which once again refers to the need for having risk assessment conducted.

The eighth most frequent failure ($n = 12$) is lack of control in "A.8.2.3 Handling of assets." Procedures for handling an asset shall be developed and implemented in accordance with the information classification scheme adopted by the organization (ISO/IEC 27,001:Calder & Gerard, 2013). The classification scheme used within the organization may not be equivalent to the schemes used by other organizations, which should be taken into account when information is transferred (ISO/IEC 27,002: Calder & Gerard, 2013).

The ninth most frequent failure (also $n = 12$) is "Human error," which was not mapped to any specific ISO 27,001 control. Human errors can be caused by insufficient information security awareness, education, and training. Human errors addressed by the supervisory authorities, however, also comprised pure accidents or the mistakes of well-educated staff members, leading to loss of confidentiality, integrity, or availability of information.

Finally, the tenth most frequent failure ($n = 9$) is lack of control in "A.15.1.2 Addressing security within supplier agreements", which is also required by GDPR (Regulation (EU) 2016/679). Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organization and the supplier regarding both parties' obligations to fulfil relevant information security requirements. The agreements may vary considerably for different organizations and among different types of suppliers; thus, care should be taken to include all relevant information security risks and requirements (ISO/IEC 27,002: Calder & Gerard, 2013). ISO 27,701 further guides the organization to specify in agreements with suppliers whether personal data is processed and the minimum technical and organizational measures that the supplier needs to meet (ISO/IEC 27,701:). All 38 information security failures

Table 4. Most frequent information security failures corresponding to ISO 27,001 control.

ISO 27,001 control	Failure frequency	Penalty
A.9.4.1 Information access restriction	47	225,065 €
A.7.2.2 Information security awareness, education, and training	32	40,598 €
A.8.2.1 Classification of information	31	603,400 €
A.10.1.1 Policy on the use of cryptographic controls	18	317,993 €
A.13.2.3 Electronic messaging	18	9,904 €
A.12.4.1 Event logging	14	309,183 €
A.14.2.8 System security testing	14	1,102,858 €
A.8.2.3 Handling of assets	12	69,025 €
Human error	12	149,951 €
A.15.1.2 Addressing security within supplier agreements	9	308,324 €
A.16.1.5 Response to information security incidents	9	223,375 €
Neglect of instructions	8	5,026 €
A.9.4.2 Secure log-on procedures	7	580,427 €
A.9.1.2 Access to networks and network services	6	297,929 €
A.16.1.4 Assessment of and decision on information security events	6	326,678 €
A.12.6.1 Management of technical vulnerabilities	5	42,019 €
A.9.4.3 Password management system	4	446,182 €
A.11.2.9 Clear desk and clear screen policy	4	11,685 €
A.12.1.4 Separation of development, testing, and operational environments	4	432,402 €
A.8.3.1 Management of removable media	3	10,483 €
A.14.1.2 Securing application services on public networks	3	569,592 €
A.16.1.1 Responsibilities and procedures	3	592,221 €
A.16.1.2 Reporting information security events	3	593,171 €
A.8.3.3 Physical media transfer	2	10,700 €
A.9.2.3 Management of privileged access rights	2	1,984,034 €
A.11.2.8 Unattended user equipment	2	5,250 €
A.12.2.1 Controls against malware	2	1,214,167 €
A.14.2.2 System change control procedures	2	11,714 €
A.14.2.7 Outsourced development	2	101,056 €
A.14.3.1 Protection of test data	2	21,463 €
A.5.1.1 Policies for information security	1	693 €
A.5.1.2 Review of the policies for information security	1	1,400 €
A.8.2.2 Labelling of information	1	7,083 €
A.11.1.5 Working in secure areas	1	7,083 €
A.12.1.2 Change management	1	2,272,222 €
Technical data integrity inconsistencies in systems leading to confidentiality breach	1	9,266,667 €
Personal data availability loss due to unspecified root cause	1	15,000 €
Usage of surveillance video cameras without proper authorization	1	1,667 €
Total	**294**	**22,187,689 €**

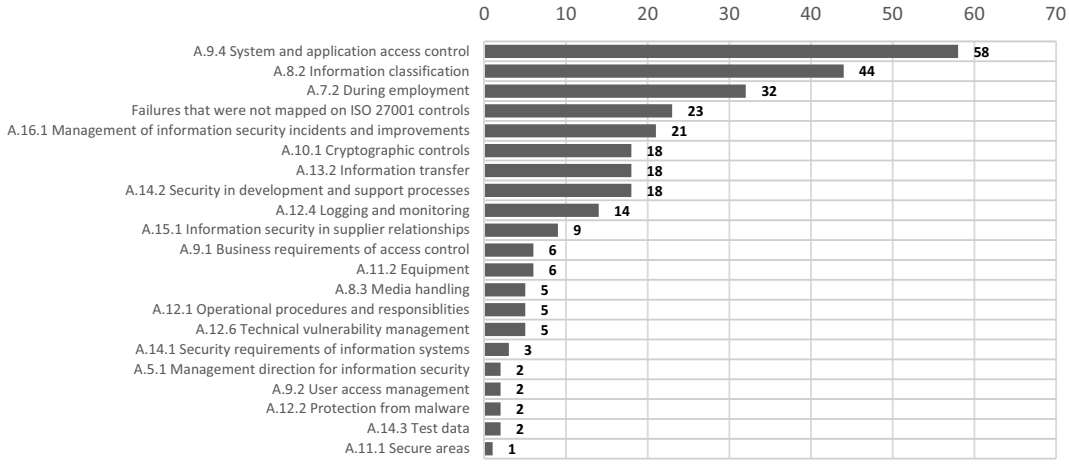

Figure 2. Most frequent information security failures corresponding to ISO 27001 control objectives.

corresponding to ISO 27,001 controls are ranked based on their frequency and presented in Table 4.

A ranking of the most frequent information security failures corresponding to ISO 27,001 control objectives is presented in Figure 2.

Information security failures corresponding to ISO 27,001 control objectives reaching the threshold of 20 observations are explained here. The most frequent failure ($n = 58$) is the lack of "A.9.4 System and application access control," where the objective is to prevent unauthorized access to systems and applications. The second most frequent failure ($n = 44$) is the lack of "A.8.2 Information classification," where the objective is to ensure that information receives an appropriate level of protection in accordance with its importance to the organization. The third most frequent failure ($n = 32$) is lack of controls "A.7.2 During employment," where the objective to ensure that employees and contractors are aware of and fulfil their information security responsibilities after being recruited by an organization.

Fourth ($n = 23$) are information security failures that were not mapped on ISO 27,001 controls, which form their own category. Most of these failures consist of pure human errors or the neglect of given instructions. The fifth most frequent failure ($n = 32$) is lack of "A.16.1 Management of information security incidents and improvements," where the objective is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A ranking of the most frequent information security failures corresponding to ISO 27,001 control clauses is presented in Figure 3.

The most frequent information security failure corresponding to the ISO 27,001 control clause is "A.9 Access control" ($n = 66$), followed by "A.8 Asset management" ($n = 49$) and "A.7 Human

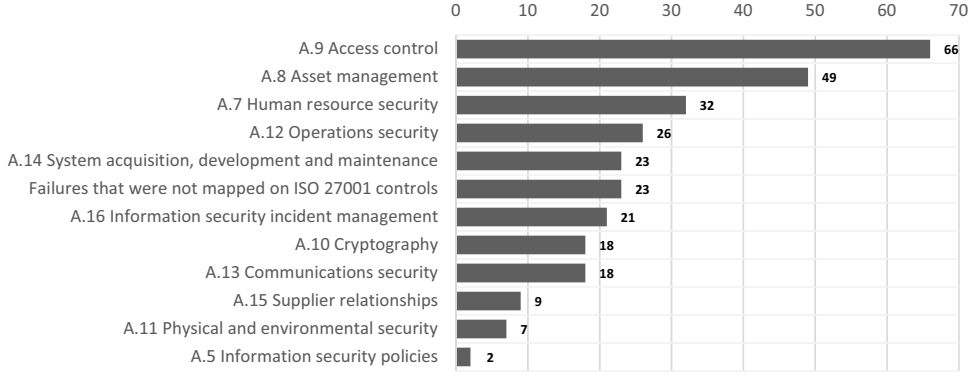

Figure 3. Most frequent information security failures corresponding to ISO 27001 control clauses.

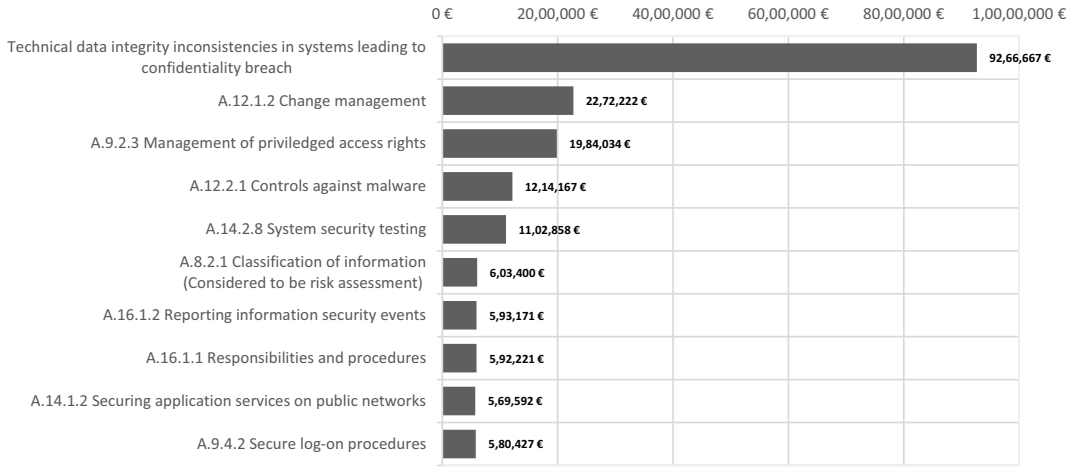

Figure 4. Top 10 most expensive information security failures corresponding to ISO 27001 controls.

resource security" ($n = 32$). In conclusion, these results can be taken into account in organizations which aspire to manage information security more effectively to prevent the most typical failures by implementing controls based on their importance.

4.2. The most expensive information security failures

The top 10 most expensive information security failures corresponding to ISO 27,001 controls are presented in Figure 4.

The most expensive failure (€ 9,266,667) was "Technical data integrity inconsistencies in systems leading to confidentiality breach." This failure was not mapped to any specific ISO 27,001 control, and it was part of a penalty in a case where the total penalty was almost 28 million euros. In that penalty case there were only two other information security failures, which explains the high penalty amount for this failure, which can further be traced to controls and measuring how information systems shall be developed, tested, and maintained to protect data integrity and confidentiality.

The second most expensive failure (€ 2,272,222) was lack of control in "A.12.1.2 Change management." Inadequate control of changes to information security processing, facilities, and systems is a common cause of a data breach. Changes to the operational environment, especially when transferring a system from the development to operational stage, can impact the reliability of applications, and therefore formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes (ISO/IEC 27,002:Calder & Gerard, 2013).

The third most expensive failure (€ 1,984,034) was inadequate "A.9.2.3 Management of privileged access rights." Inappropriate use of system administration privileges (any feature of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems. Thus, the allocation of privileged access rights should be controlled through a formal authorization process in accordance with the relevant access controls policy (ISO/IEC 27,002:Calder & Gerard, 2013).

The fourth most expensive failure (€ 1,214,167) was inadequacies in "A.12.2.1 Controls against malware." Protection against malware shall be based on malware detection and repair software, information security awareness, and appropriate system access and change management controls (ISO/IEC 27,001:Calder & Gerard, 2013). The use of malware detection and repair software as the sole malware control is not usually adequate and commonly needs to be accompanied by operating procedures that prevent the introduction of malware (ISO/IEC 27,002:Calder & Gerard, 2013).

The fifth most expensive failure (€ 1,102,858) was inadequate "A.14.2.8 System security testing," followed by the sixth most expensive failure (€ 603,400) lack of control in "A.8.2.1 Classification of information," which were both present in the top 10 most frequent information security failures.

The seventh most expensive failure (€ 593,171) was inadequacy in "A.16.1.2 Reporting information security events." All employees and contractors should be made aware of their responsibility to report information security events to the proper channels as quickly as possible (ISO/IEC 27,002: Calder & Gerard, 2013).

The eighth most expensive failure (€ 592,221) was lack of "A.16.1.1 Responsibilities and procedures" concerning incident management, where management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents (ISO/IEC 27,001:Calder & Gerard, 2013). If incidents are not reported, further investigated, and fixed, then incidents remain unaddressed, which consequently causes data breaches to become even more severe and more extensive. ISO 27,701 further guides on establishing responsibilities and procedures for the identification and recording of breaches of personal data as well as notification to required parties, including the timing of such notifications and the disclosure to authorities (ISO/IEC 27,701:), which is also required by GDPR (Regulation (EU) 2016/679).

The ninth most expensive failure (€ 569,592) was lack of control in "A.14.1.2 Securing application services on public networks." Applications accessible via public networks are subject to a range of network related threats, and therefore a detailed risk assessment and selection of controls is indispensable. The required controls often include cryptographic methods, authentication, and securing data transfer (ISO/IEC 27,002:Calder & Gerard, 2013). ISO 27,701 recommends encryption, specifically when personal data is transmitted over untrusted data transmission networks (ISO/IEC 27,701:).

Finally, the tenth most expensive failure (€ 580,427) was lack of control in "A.9.4.2 Secure log-on procedures." The procedure for logging into a system or application should be designed to minimize the opportunity for unauthorized access, and thus a suitable authentication technique should be chosen to substantiate the claimed identity of a user. Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, or biometric means, should be used (ISO/IEC 27,002:Calder & Gerard, 2013). ISO 27,701 additionally guides the organization on providing the capability for secure log-on procedures for any user accounts under the data subjects control (ISO/IEC 27,701:).

All 38 most expensive information security failures corresponding to ISO 27,001 controls are presented in Table 5.

Table 5. Most expensive information security failures corresponding to ISO 27,001 control.

ISO 27,001 control	Penalty	Failure frequency
Technical data quality inconsistencies in systems leading to confidentiality breach	9,266,667 €	1
A.12.1.2 Change management	2,272,222 €	1
A.9.2.3 Management of privileged access rights	1,984,034 €	2
A.12.2.1 Controls against malware	1,214,167 €	2
A.14.2.8 System security testing	1,102,858 €	14
A.8.2.1 Classification of information	603,400 €	31
A.16.1.2 Reporting information security events	593,171 €	3
A.16.1.1 Responsibilities and procedures	592,221 €	3
A.14.1.2 Securing application services on public networks	569,592 €	3
A.9.4.2 Secure log-on procedures	580,427 €	7
A.9.4.3 Password management system	446,182 €	4
A.12.1.4 Separation of development, testing, and operational environments	432,402 €	4
A.16.1.4 Assessment of and decision on information security events	326,678 €	6
A.10.1.1 Policy on the use of cryptographic controls	317,993 €	18
A.12.4.1 Event logging	309,183 €	14
A.15.1.2 Addressing security within supplier agreements	308,324 €	9
A.9.1.2 Access to networks and network services	297,929 €	6
A.9.4.1 Information access restriction	225,065 €	47
A.16.1.5 Response to information security incidents	223,375 €	9
Human error	149,951 €	12
A.14.2.7 Outsourced development	101,056 €	2
A.8.2.3 Handling of assets	69,025 €	12
A.12.6.1 Management of technical vulnerabilities	42,019 €	5
A.7.2.2 Information security awareness, education, and training	40,598 €	32
A.14.3.1 Protection of test data	21,463 €	2
Personal data availability loss due to unspecified root cause	15,000 €	1
A.14.2.2 System change control procedures	11,714 €	2
A.11.2.9 Clear desk and clear screen policy	11,685 €	4
A.8.3.3 Physical media transfer	10,700 €	2
A.8.3.1 Management of removable media	10,483 €	3
A.13.2.3 Electronic messaging	9,904 €	18
A.8.2.2 Labelling of information	7,083 €	1
A.11.1.5 Working in secure areas	7,083 €	1
A.11.2.8 Unattended user equipment	5,250 €	2
Neglect of instructions	5,026 €	8
Usage of surveillance video cameras without proper authorization	1,667 €	1
A.5.1.2 Review of the policies for information security	1,400 €	1
A.5.1.1 Policies for information security	693 €	1
Total	**22,187,689 €**	**294**

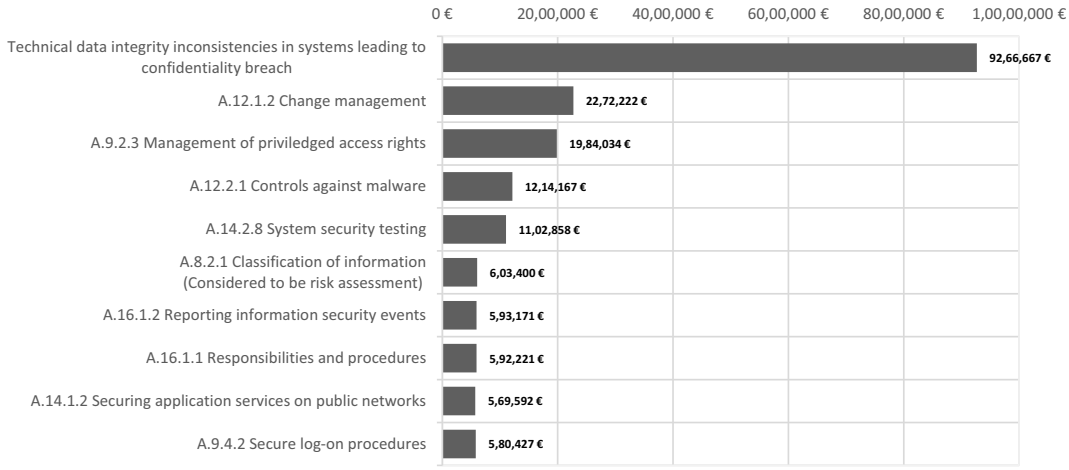

Figure 5. Most frequent information security failures corresponding to ISO 27001.

A ranking of the most expensive information security failures corresponding to ISO 27,001 control objectives is presented in Figure 5.

Information security failures corresponding to ISO 27,001 control objectives reaching the threshold of a 500,000 euro penalty are explained here. The most expensive failure (€ 1,984,934) was inadequate "A.9.2 User access management," where the objective is to ensure access for authorized users and to prevent unauthorized access to systems and services. The second most expensive failure (€ 1,214,167) was lack of "A.12.2 Protection from malware," where the objective is to ensure that information and information processing facilities are protected against malware. The third most expensive failure (€ 870,309) was lack of control in "A.14.2 Security in development and support processes," where the objective is to ensure that information security is designed and implemented within the whole development lifecycle of information systems.

The fourth most expensive failure (€ 800,366) was inadequate control in "A.12.1 Operational procedures and responsibilities," where the objective is to ensure correct and secure operations of information processing facilities. The fifth most expensive failure (€ 569,592) was lack of "A.14.1 Security requirements of information systems," where the objective is to ensure that information security is a fundamental element of information systems across their entire lifecycle.

A ranking of the most expensive information security failures corresponding to ISO 27,001 control clauses is presented in Figure 6.

The most expensive information security failure corresponding to ISO 27,001 control clause (€ 757,272) was inadequate "A.14 System acquisition, development and maintenance," followed by the category of failures (€ 483,607) which were not mapped specifically on any ISO 27,001 control. The

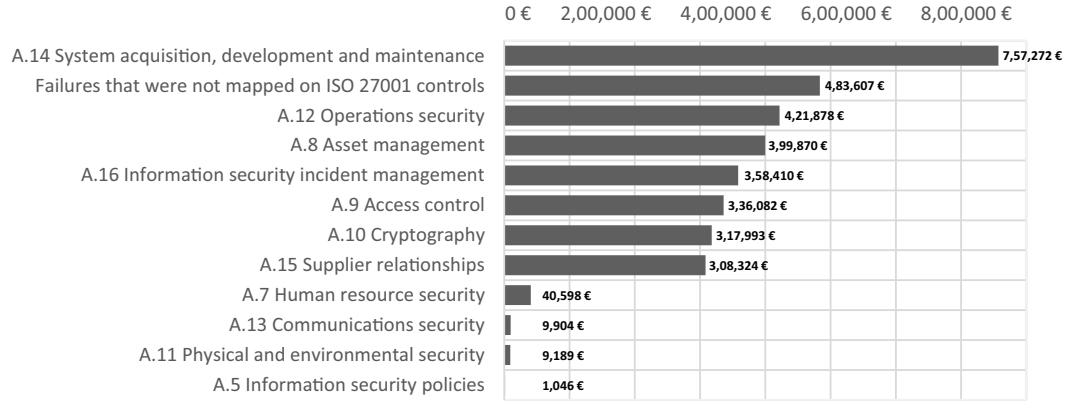

Figure 6. Most expensive information security failures corresponding to ISO 27001 control clauses.

Table 6. The amount of information security failures corresponding to ISO 27,001 controls typically in a case.

Information security failures in a case	Number of cases	Percentage	Average penalty of the group
2	24	30%	317,341 €
3	20	25%	1,601,131 €
1	10	12%	€ 73350
5	7	9%	€ 41530
4	6	7%	€ 89991
8	4	5%	€ 102,150
7	3	4%	€ 4,241,867
9	3	4%	€ 7,363,433
6	2	2%	€ 147,420
12	1	1%	€ 85000
13	1	1%	€ 22046,000

third most expensive failure was lack of control in "A.12 Operations security" (421,878 €), and in conclusion, these results can be taken into account in organizations which aim to manage information security more effectively to prevent the most expensive failures by implementing controls based on their importance.

4.3. The amount of information security failures in a GDPR penalty case

The amount of information security failures corresponding to ISO 27,001 controls typically existing in GDPR penalty cases in the year 2020 is presented in Table 6.

The amount of information security failures ranges from 1 to 13 failures per GDPR penalty case. There are typically a low number of failures in a case. In 30% of the cases there were only 2 failures, and in 25% of the cases only 3 failures were observed, while single failure cases consisted of 12% of the cases analyzed. Cases where there were four or more failures comprised 33% of all the cases. Notably, there were only two cases with more than ten failures, and in the single case with the most observed – thirteen -information security failures, the penalty was over 22 million euros.

4.4. Information security failure correlations

Next, the results on how the information security failures corresponding to ISO 27,001 controls correlate are presented. Information security failures which have a fairly strong (0.30 and above) correlation, and which have statistical significance (p-value lower than 0.05) consist of a total of 61 observations. To highlight the strategic significance of these correlated controls, Table 7 presents the set of seven controls which have a very strong (0.65 and above) correlation.

Table 7. Information security failure correlations corresponding to ISO 27,001 controls.

ISO 27,001 control 1	ISO 27,001 control 2	Correlation	P-value
A.11.1.5 Working in secure areas	A.8.2.2. Labelling of information	1.00	***
A.8.3.3. Physical media transfer	A.8.3.1. Management of removable media	0.81	***
A.8.3.3 Physical media transfer	A.5.1.2. Review of the policies for information security	0.70	***
A.12.1.2 Change management	A.9.2.3 Management of privileged access rights	0.70	***
A.12.2.1 Controls against malware	A.12.1.2 Change management	0.70	***
A.16.1.2 Reporting information security events	A.16.1.1 Responsibilities and procedures	0.65	***
A.16.1.5 Response to information security incidents	A.16.1.4 Assessment of and decision on information security events	0.65	***

The controls "A.11.1.5 Working in secure areas" and "A.8.2.2. Labelling of information" have a very strong correlation. In the analyzed cases, there were many data confidentiality breaches, where employees had not handled information within the organizations' physical premises in a secure way. Often, paper documents or other physical media containing sensitive personal data were transported outside of secure areas, and were later found in waste bins by complete outsiders. Therefore, a data labeling scheme, which further instructs on how information should be processed within the physical premises, is crucial. ISO 27,701 additionally guides the organization on making their employees aware of the definition of personal data and how to recognize such information (ISO/IEC 27,701:).

The control "A.8.3.3. Physical media transfer" correlates with "A.8.3.1. Management of removable media" and "A.5.1.2. Review of the policies for information security." In many cases there were data breaches, where staff-members had lost unencrypted equipment or media containing sensitive information. Therefore, organizations should have a policy and instructions on how media containing information should be protected against unauthorized access, misuse, or corruption during transport, as well as procedures for the management of removable media in accordance with the classification scheme adopted by the organization (ISO/IEC 27,002:Calder & Gerard, 2013). ISO 27,701 guides organizations on applying additional measures

such as encryption to ensure that the removable media can only be accessed at the point of destination and not in transit (ISO/IEC 27,701:).

The control "A.12.1.2 Change management" correlates with "A.9.2.3 Management of privileged access rights" and "A.12.2.1 Controls against malware." Changes to the organization, business processes, information processing facilities, and systems that affect information security should be managed together with privileged access rights administration because inappropriate system administration privileges are a major contributory factor to failures and system breaches. This has a connection to malware protection, because if malware is injected successfully to hack and misuse administrative accounts, the attackers gain the ability to make changes within IT systems, steal information, and possibly cover their tracks by disabling monitoring solutions and deleting system and security event logs (ISO/IEC 27,002:Calder & Gerard, 2013).

A group of controls concerning incident management are naturally correlated together, because organizations need to have responsibilities and procedures in place to ensure a quick, effective, and orderly recognition of unexpected information security disruptions and incidents. Potential data breaches shall be reported through appropriate management channels as quickly as possible in order to be thoroughly assessed by competent personnel who are responsible for taking timely decisions on further actions.

Table 8. Information security failure correlations corresponding to ISO 27,001 control objectives.

ISO 27,001 control objective 1	ISO 27,001 control objective 2	Correlation	p-value
A.9.2 User access management	A.12.1 Operational procedures and responsibilities	0.62	***
A.9.2 User access management	A.12.2 Protection from malware	0.49	***
A.11.2 Equipment	A.11.1 Secure areas	0.40	***
A.9.2 User access management	A.14.1 Security requirements of information systems	0.39	***
A.8.3 Media handling	A.5.1 Management direction for information security	0.39	***
A.9.4 System and application access control	A.13.2 Information transfer	−0.37	***
A.14.2 Security in development and support processes	A.12.4 Logging and monitoring	0.37	***
A.9.4 System and application access control	A.12.4 Logging and monitoring	0.36	***
A.12.1 Operational procedures and responsibilities	A.10.1 Cryptographic controls	0.36	***
A.9.2 User access management	A.12.4 Logging and monitoring	0.35	***
A.15.1 Information security in supplier relationships	A.14.1 Security requirements of information systems	0.35	***

Next, the results on how the information security failures corresponding to ISO 27,001 control objectives correlate are presented. Information security failures, which have a fairly strong (0.30 and above) correlation, and which have statistical significance (p-value lower than 0.05), consist of a total of 19 observations. To foreground the strategic significance of these correlated controls, Table 8 presents the set of 11 controls which are above the 0.35 correlation rate.

The ISO 27,001 security objective "A.9.2 User access management" correlates with many other security objectives. Unauthorized access to systems and services should be prevented in order that the secure operations of information processing facilities are assured. In addition, logging and monitoring are a crucial part of user access management in order that user specific actions can be traced, and this needs to be ensured within the whole development lifecycle of an information system according to control objective "A.14.2 Security in development and support processes."

The security control objectives "A.11.2 Equipment" and "A.11.1 Secure areas" correlate. So do the control objectives "A.8.3 Media handling" and "A.5.1 Management direction for information security." These correlation sets are explained by many data breaches being caused by inadequate organizational data labeling schemes, which should lead to further policies instructing how information within the premises of an organization needs to be handled, as well as how physical media and equipment need to be encrypted or otherwise adequately protected before they are transferred outside the organizational premises.

The security control objectives "A.9.4 System and application access control" and "A.13.2 Information transfer," however, have a negative correlation. The prevention of unauthorized access to systems has no relation to procedures on how information should be transferred within an organization and with external entities.

Table 9. Information security failure correlations corresponding to ISO 27,001 control clauses.

ISO 27,001 control clause 1	ISO 27,001 control clause 2	Correlation	p-value
A.14 System acquisition, development and maintenance	A.12 Operations security	0.41	***
A.9 Access control	A.13 Communications security	−0.39	***
A.16 Information security incident management	A.12 Operations security	0.34	***
A.9 Access control	A.7 Human resource security	−0.32	***
A.7 Human resource security	A.13 Communications security	0.30	***

Table 10. GDPR penalties based on article 32 "security of processing" in the year 2020 per industry sector.

Industry sector	Total penalty	Average penalty	Number of cases
Media, Telecoms and Broadcasting	€ 42050,136	€ 2,473,537	17
Transportation and Energy	€ 22060,000	€ 4,412,000	5
Accommodation and Hospitality	€ 20450,000	€ 20450,000	1
Health Care	€ 7,166,987	€ 447,937	16
Industry and Commerce	€ 3,875,520	€ 276,823	14
Finance, Insurance and Consulting	€ 1,608,750	€ 201,094	8
Public Sector and Education	€ 1,606,300	€ 94488	17
Real Estate	€ 20600	€ 10300	2
Employment	€ 15000	€ 15000	1
Total	**€ 98853,293**	**€ 28381,179**	**81**
Average	**€ 1,220,411**		

In many GDPR penalty cases the failure was caused due to the supplier not being able to provide sufficient guarantees to supply adequate information security to the organization, which ultimately was the data controller. Therefore, security objective "A.15.1 Information security in supplier relationships" naturally correlates with "A.14.1 Security requirements of information systems."

Next, the results on how the information security failures corresponding to ISO 27,001 control clauses correlate are presented. Information security failures, which have a fairly strong (0.30 and above) correlation and have statistical significance (p-value lower than 0.05) consist of a total of five observations. These are presented in Table 9.

The ISO 27,001 control clause "A.12 Operations security" correlates with "A.14 System acquisition, development and maintenance" and "A.16 Information security incident management." It is natural that operations are closely connected to how systems security is continuously maintained, while efficient incident management should be at the heart of the daily business of an organization.

The control clause "A.9 Access control" has a negative correlation with "A.13 Communications security," which is explained by many GDPR penalty cases where failures in access control management do not coexist with failures regarding information transfer requirements.

However, the control clause "A.9 Access control" correlates with "A.7 Human resource security." Processes concerning employees hired by or departing from the organization, as well as staff-members changing positions within the organization, are governed by the HR function. Therefore, these processes should be aligned with access control management in order that new and obsolete, as well as the changing organizational roles of employees, correctly match with the access they have or should not have in systems and applications.

The control clause "A.7 Human resource security" also correlates with "A.13 Communications security." In the analyzed GDPR penalty cases, a multitude of data breaches took place in different electronic messaging channels such as e-mail, websites, and social media. These failures were caused by a lack of proper instructions and awareness training, which should be provided by the HR departments of an organization.

4.5. Industry type differences in information security failures and penalties

Table 10 presents the total and average GDPR penalties, as well as the number of cases based on article 32 "security of processing" in the year 2020 per industry sector.

In the year 2020 all the issued 81 GDPR penalties based on article 32 "Security of processing," where the penalty type was "insufficient technical and organizational measures to ensure information security," amounted to almost 100 million euros. The average of total penalties within all industry sectors was € 1,220,411.

The number of cases and total and average penalties vary significantly between different industry sectors. The largest amount of total GDPR penalties was € 42050,136, and the most issued 17 penalty cases were issued to the industry sector "Media, Telecoms and Broadcasting," which averaged a penalty of € 2,473,537 per case.

The industry sector "Public Sector and Education" was also issued with 17 penalty cases, but the total penalty was only € 1,606,300, averaging a penalty of € 94488 per case. The results concerning public sector and education are affected by the inconsistent administrative fine calculation methods of the supervisory authorities. GDPR has allowed each EU member state to establish their own rules on penalties applicable to infringements, and to determine whether and to what extent administrative fines have been imposed on public organizations.

The industry sector "Accommodation and Hospitality" received the biggest average GDPR penalty of € 20450,000 with its single penalty case. The industry sector "Transportation and Energy" had the second biggest average penalty of € 4,412,000, with five penalty cases issued. The industry sectors "Real estate" and "Employment" in turn received the smallest penalties, which are meager compared to other sectors.

5. Conclusions

This study has presented the most frequent and most expensive information security failures and consequently ranked the corresponding ISO 27,001 controls that were used as failure identifiers in the analysis. The answer to RQ 1 is as follows: poor access control restriction and management of privileged access rights were very common causes of data confidentiality loss. The lack of implementing an appropriate information classification scheme was a cause of many different failures, because without risk assessments, further risk-based controls such as adequate cryptographic measures, suitable controls against malware, or proportionate system security development and testing could not be implemented. Failure to address security within supplier agreements was a common cause of incidents, as often there was a misunderstanding between the organization and supplier regarding both parties' obligations to fulfil the relevant information security requirements. Shortcomings in information security awareness, education, and training led to a multitude of different problems as staff members did not know what was expected of them.

This study further presented how many information security failures typically exist in a GDPR penalty case. The answer for RQ 2 is as follows: the amount of information security failures ranges from 1 to 13 failures per GDPR penalty case. There are typically a low number of failures in a case. In 30% of cases, there were only 2 failures, and in 25% of cases, 3 failures were observed, while single failure cases comprised 12% of the cases analyzed.

This study also presented how the observed information security failures correlate. The answer to RQ 3 is as follows: the top correlation was observed in inadequate organizational data-labeling schemes and lack of education on how employees should handle information assets within the premises of an organization. Several data confidentiality breaches were caused by careless staff members carrying documents containing sensitive personal data outside the facilities of an organization, which were later discovered in waste bins by complete outsiders. In many cases, staff-members had lost unencrypted equipment or media containing sensitive information during transfer. Inadequate control in information security incident management led to data breaches being unaddressed, which consequently caused failures to become more severe and more extensive; thus, a group of controls concerning incident management were naturally correlated together.

This study additionally presented insights into industry type differences in information security failures and penalties. The answer to RQ 4 is as follows: the number of cases, as well as total and average penalties, vary significantly between different industry sectors. The largest amount of total GDPR penalties (€ 42050,136) and most issued (n = 17) penalty cases were experienced by the industry sector "Media, Telecoms and Broadcasting," while the industry sector "Employment" received only one (€ 15 000) penalty.

5.1. Theoretical and practical contributions

Firstly, our study contributes by bridging the gap between regulation and information security as presented by Dlamini et al. (2009) Secondly, our study introduces a statistical method to analyze the GDPR penalty cases and provides previously

unreported findings about information security failures and their respective solutions. Thirdly, our work expands on previous work by Ruohonen and Hjerppe (2022) and Presthus and Sønslien (2021) by further exploring early GDPR violations and sanctions from the year 2020.

From a practical perspective, our study provides input to the study of Vaibhav (2022) by providing data-driven performance measurement metrics to decision-making in information security governance. The results of our study are useful for organizations which aspire to manage information security more effectively in order to prevent the most typical and expensive information security failures by applying controls based on their importance and correlation. Organizations, as well as auditors implementing and assuring the ISO 27,001, may use our results as a guideline whereby ISO 27,001 controls should be applied and verified first in sequential order based on their impact and interdependence.

5.2. Limitations and future directions

There are three limitations in our study. Firstly, the quality of the GDPR penalty case reports written by the different supervisory authorities in each EU member county varies. The analyzed 81 penalty case reports do not always follow the same structure, and their length and level of precision differ. In some of the cases, the supervisory authority scrutinized the information security failures at a very detailed level. However, in other cases, the descriptions are comparatively limited; thus, it is possible that in these cases the underlying information security failure root causes were left undefined by the supervisory authority. In our study, however, only information security failures which were explicitly addressed in the penalty case reports were analyzed.

Secondly, the data source of our study, the GDPR Enforcement Tracker, may not be completely up to date. It is possible there were more than 81 GDPR penalty cases issued in the year 2020, which were not yet included in the database when this study was conducted. Additionally, organizations which were issued with a GDPR penalty may have lodged a court appeal, which may eventually alter the original supervisory authority decisions.

Thirdly, the penalty calculations of our study are not definitive. Even though all the 81 analyzed GDPR penalty cases can be categorized in the penalty type "insufficient technical and organizational measures to ensure information security," there were 25 cases which also included references to other GDPR articles, outside of the requirements considering information security. If a GDPR penalty is issued to an organization, the supervisory authorities administer penalties as a whole and do not separate the penalty amounts to address a specific article.

GDPR penalty cases are a fruitful and transparent ground to explore information security failures, their impacts, and respective solutions based on control frameworks. We encourage further research which would analyze GDPR penalty cases with the statistical methods we applied in our study with further versions of the ISO/IEC 27,001 as well as with other similar standardization frameworks. It would also be constructive to analyze the readiness of organizations toward information security compliance with case study methods to generate more research hypotheses.

From a broader perspective, researchers and information security practitioners at other institutions are encouraged to use this study as a motivation to popularize the assessed and ranked information security controls in order to effectively manage the complex and challenging information security risks within organizational IT-GRC driven ISMS frameworks.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

M. Suorsa http://orcid.org/0000-0002-1649-4223
P. Helo http://orcid.org/0000-0002-0501-2727

References

Akhlaghpour, S., Hassandoust, F., Fatehi, F., Burton-Jones, A., & Hynd, A. (2021). Learning from enforcement cases to manage GDPR risks. *MIS Quarterly Executive*, *20*(3), 199–218. https://doi.org/10.17705/2msqe.00049

Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for

cybersecurity auditing. *Information Security Journal: A Global Perspective*, *30*(4), 189–204. https://doi.org/10.1080/19393555.2020.1834649

Anass, R., Assoul, S., Ouazzani, T. K., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. *Information and Computer Security*, *28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

Barrett, C. (2020). Emerging trends from the first year of EU GDPR enforcement. *Scitech Lawyer*, *16*(3), 22–35.

Bashofi, I., & Salman, M. (2022), Cybersecurity maturity assessment design using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002, *2022 IEEE International Conference on Cybernetics and Computational Intelligence* pp. 58–62, https://doi.org/10.1109/CyberneticsCom55287.2022.9865640.

Brenner, J. (2007). ISO 27001 risk management and compliance. *Risk Management*, *54*(24), 28–29. 26.

Calder, A., & Gerard, L. (2013). The ISO/IEC 27001 family of information security standards. In *ISO 27001/ISO 27002, a pocket guide* (pp. 12–14). IT Governance Ltd.

Card, A. J. (2016). The problem with '5 whys'. *BMJ Quality & Safety*, *26*(8), 671–677. https://doi.org/10.1136/bmjqs-2016-005849

Chapple, M., Stewart, J. M., & Gibson, D. (2018). Security governance through principles and policies. In J. T. Parker, B. Sipes, & D. Seidl (Eds.), *Certified information systems security professional official study guide* (pp. 1–48). Sybex.

Cornock, M. (2018). General data protection regulation (GDPR) and implications for research. *Maturitas*, *111*, A1–A2. https://doi.org/10.1016/j.maturitas.2018.01.017

Craddock, P. (2022). Comparing past GDPR fines to future ones under EDPB's guidelines, and making a GDPR fine calculator. *Computer Law Review International*, *23*(5), 136–140. https://doi.org/10.9785/cri-2022-230503

Degli-Esposti, S., & Ferrándiz, E. M. (2021). After the GDPR: Cybersecurity is the elephant in the artificial intelligence room. *European Business Law Review*, *32*(1), 1–24. https://doi.org/10.54648/eulr2021001

Deva, P. M., & Suchithra, M. C. (2020). The personal data protection bill, 2018: India's regulatory journey towards a comprehensive data protection law. *International Journal of Law and Information Technology*, *28*(1), 1–19. https://doi.org/10.1093/ijlit/eaaa003

Dharmalingam, R., Shivasankarappa, A., & Neelamegam, A. (2018). A novel approach for optimizing governance, risk management and compliance for enterprise information security using DEMATEL and FoM. *Procedia Computer Science*, *134*, 365–370. https://doi.org/10.1016/j.procs.2018.07.197

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO/IEC27001: 2013 and ISO/IEC27002: 2013 to GDPR compliance controls. *Information and Computer Security*, *28*(4), 645–662. https://doi.org/10.1108/ICS-01-2020-0004

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*(3–4), 189–198. https://doi.org/10.1016/j.cose.2008.11.007

Doggett, M. A. (2005). Root cause analysis: A framework for tool selection. *Quality Management Journal*, *12*(4), 34–45. https://doi.org/10.1080/10686967.2005.11919269

EDPB. (2022). *Guidelines 04/2022 on the calculation of administrative fines under the GDPR*. European Data Protection Board. https://edpb.europa.eu/system/files/202205/edpb_guidelines_042022_calculationofadministrativefines_en.pdf

Garrison, C., & Hamilton, C. (2019). A comparative analysis of the EU GDPR to the US's breach notifications. *Information & Communications Technology Law*, *28*(1), 99–114. https://doi.org/10.1080/13600834.2019.1571473

GDPR enforcement Tracker. *CMS*. https://www.enforcementtracker.com

Geko, M., & Tjoa, S. (2018). An ontology capturing the interdependence of the General data protection Regulation (GDPR) and information security. *CECC 2018: Proceedings of the Central European Cybersecurity Conference 2018*, 1–6 https://doi.org/10.1145/3277570.3277590

Gerber, M., & von Solms, R. (2008). Information security requirements – interpreting the legal aspects. *Computers and Security*, *27*(5–6), 124–135. https://doi.org/10.1016/j.cose.2008.07.009

Higashizawa, N., & Aihara, Y. (2017). Data privacy protection of personal information versus usage of big data: Introduction of the recent amendment to the act on the protection of personal information (Japan). *Defense Counsel Journal*, *84*(4), 1–15. 84.

Hintze, M. (2018). Data controllers, data processors, and the growing use of connected products in the enterprise: Managing risks, understanding benefits, and complying with the GDPR. *Journal of Internet Law*, *22*(2), 17–31. https://doi.org/10.2139/ssrn.3192721

Hirvonen, P. (2022). A review of GDPR impacts on information security. *Proceedings of the 26th Pacific Asia Conference on Information Systems*, 83. https://aisel.aisnet.org/pacis2022/83

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

ISO/IEC 27001. 2013, information Technology – security techniques – information security management systems – requirements (ISO/IEC 27001: 2013). *International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)*.

ISO/IEC 27002. 2013, information Technology – security techniques – code of practice for information security controls. *International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)*.

ISO/IEC 27002. 2022, information security, cybersecurity and privacy protection – information security controls. *International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)*.

ISO/IEC 27701. 2019, security techniques — extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — requirements and guidelines. *International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)*.

Khajouei, H., Kazemi, M., & Moosavirad, S. H. (2017). Ranking information security controls by using fuzzy analytic hierarchy process. *Information Systems and eBusiness Management*, *15*(1), 1–19. https://doi.org/10.1007/s10257-016-0306-y

Lopes, M. I., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 standards as GDPR compliance facilitator. *Journal of Information Systems Engineering and Management*, *4*(2). https://doi.org/10.29333/jisem/5888

Lopez-Leyva, J. A., Kanter-Ramirez, C. A., & Morales-Martinez, J. P. (2020), Customized diagnostic tool for the security maturity level of the enterprise information based on ISO/IEC 27001, *2020 8th International Conference in Software Engineering Research and Innovation*, 147–153, https://doi.org/10.1109/CONISOFT50191.2020.00030.

Macedo, A. C. (2021). Some thoughts about the intersection between data protection and competition law: A view from Brazil. *Journal of Antitrust Enforcement*, *9*(2), 197–202. https://doi.org/10.1093/jaenfo/jnab007

Makupi, D., & Karume, S. (2019). Towards an information security maturity model for universities based on ISO 27001. *Journal of Humanities & Social Sciences*, *3*(6), 241–245. https://doi.org/10.24940/theijbm/2019/v7/i6/BM1906-038

Mayer, N., & Smet, D. D. (2017). Systematic literature review and ISO standards analysis to integrate IT governance and security risk management. *International Journal for Infonomics*, *10*(1). https://doi.org/10.20533/IJI.1742.4712.2017.0154

Monev, V. (2020). Organisational information security maturity assessment based on ISO 27001 and ISO 27002. *2020 International Conference on Information Technologies (InfoTech)*. https://doi.org/10.1109/InfoTech49733.2020.9211066

Nicho, M., Khan, S., & Rahman, M. S. M. K. (2017), Managing information security risk using integrated governance risk and compliance. *2017 International Conference on Computer and Applications (ICCA)*,Doha, United Arab Emirates.

Nungky, A. C., Ramli, K., Anak Agung, P. R., & Teddy, S. G. (2022). Information security risk assessment using situational awareness frameworks and application tools. *Risks*, *10*(8), 165. https://doi.org/10.3390/risks10080165

Osden, J., & Lubbe, S. (2009). Using information technology governance, risk (GRC) as a creator of business values - a case study. *South African Journal of Economic and Management Sciences*, *12*(1), 115–125. https://doi.org/10.4102/sajems.v12i1.264

Paciarotti, C., Mazzuto, G., & D'Ettorre, D. (2014). A revised FMEA application to the quality control management. *International Journal of Quality & Reliability Management*, *31*(7), 788–810. https://doi.org/10.1108/IJQRM-02-2013-0028

Peerally, M. F., Carr, S., Waring, J., & Dixon-Woods, M. (2016). The problem with root cause analysis. *BMJ Quality & Safety*, *26*(5), 417–422. https://doi.org/10.1136/bmjqs-2016-005511

Presthus, W., & Sønslien, K. F. (2021). An analysis of violations and sanctions following the GDPR. *International Journal of Information Systems & Project Management*, *9*(1), 38–53. https://doi.org/10.12821/ijispm090102

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, and repealing directive 95/46/EC (General data protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

Rooney, J. J., Lee, N., & Van den, H. (2004). Root cause analysis for beginners. *Quality Progress*, *37*(7), 45–53.

Ruohonen, J., & Hjerppe, K. (2022). The GDPR enforcement fines at a glance. *Information Systems*, *106*, 101876. https://doi.org/10.1016/j.is.2021.101876

Saemann, M., Theis, D., Urban, T., & Degeling, M. (2022). Investigating GDPR fines in the light of data flows. *Proceedings on Privacy Enhancing Technologies*, *2022*(4), 314–331. https://doi.org/10.56553/popets-2022-0111

Sanskriti, C., & Astitwa, B. (2018). Significance of ISO/IEC 27001 in the implementation of governance, risk and compliance. *International Journal of Scientific Research in Network Security and Communication*, *6*(2), 30–33. https://doi.org/10.26438/ijsrnsc/v6i2.3033

Schlarman, S. (2009). What ITIL can teach IT-GRC. *The EDP Audit, Control, and Security Newsletter*, *40*(2), 8–18. https://doi.org/10.1080/07366980903340012

Selzer, A., Woods, D., & Böhme, R. (2021). Practitioners' corner · an economic analysis of appropriateness under article 32 GDPR. *European Data Protection Law Review*, *7*(3), 456–470. https://doi.org/10.21552/edpl/2021/3/15

Serrado, J., Pereira, R. F., Mira da Silva, M., & Scalabrin, B. I. (2020). Information security frameworks for assisting GDPR compliance in banking industry. *Digital Policy, Regulation & Governance*, *22*(3), 227–244. https://doi.org/10.1108/DPRG-02-2020-0019

Shojaie, B., Federrath, H., & Saberi, I. (2014), Evaluating the effectiveness of ISO 27001: 2013 based on annex a. *IEEE, 2014 Ninth International Conference on Availability, Reliability and Security*. https://doi.org/10.1109/ARES.2014.41

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *International Journal on Informatics Visualization*, *4*(4), 4225–4230. https://doi.org/10.30630/joiv.4.4.482

Tariq, M. T., Tayyaba, S., Ali, M. T., Safraz, M. S., De La-Hoz-Franco, E., Butt, S. A., Starcangelo, V., & Rad, D. V. (2020). Combination of AHP and TOPSIS methods for the ranking of information security controls to overcome its obstructions under fuzzy environment. *Journal of Intelligent & Fuzzy Systems*, *38*(5), 6075–6088. https://doi.org/10.3233/JIFS-179692

Thomas, I. (2020). Getting ready for the California consumer privacy act: Building on general data protection regulation preparedness. *Applied Marketing Analytics*, *5*(3), 210–222.

Vaibhav, A. (2022). Information security governance metrics: A survey and taxonomy. *Information Security Journal: A Global Perspective*, *31*(4), 466–478. https://doi.org/10.1080/19393555.2021.1922786

von Solms, B. (2006). Information security – the fourth wave. *Computers and Security*, *25*(3), 165–168. https://doi.org/10.1016/j.cose.2006.03.004

Wei, Y. C., Wu, W. C., Lai, G. H., & Chu, Y. (2020). pISRA: Privacy considered information security risk assessment model. *The Journal of Supercomputing*, *76*(3), 1468–1481. https://doi.org/10.1007/s11227-018-2371-0

Wolff, J., & Atallah, N. (2021). Early GDPR penalties: Analysis of implementation and fines through May 2020. *Journal of Information Policy*, *11*, 63–103. https://doi.org/10.5325/jinfopoli.11.2021.0063

Wright, C. (2019). Cyber security governance. In how cyber security can protect your business: A guide for all stakeholders. *IT Governance Ltd*, 21–29.

York, D., Jin, K., Song, Q., & Li, H. (2014). Practical root cause analysis using cause mapping. *Proceedings of the International MultiConference of Engineers and Computer Scientists 2014, IMECS 2014*, Hong Kong.