applied sciences

MDPI

Article

Classification of Data and Information in the AI Era: Towards Compliance and Efficient Data Management

John Lindström [1,*], Peter Boström [2], Andreas Sikström [3] and Karl Andersson [1]

[1] Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, 971 88 Lulea, Sweden; karl.andersson@ltu.se
[2] Nordic Information Control AB, Kungsgatan 37 8tr, 111 56 Stockholm, Sweden; peter.bostrom@nord-ic.com
[3] Xolaris Civil Security AB, Sundsbacken 6, 972 42 Lulea, Sweden; andreas.sikstrom@xolaris.se
* Correspondence: john.lindstrom@ltu.se; Tel.: +46-920-491000

Abstract

In the era of increasing application of artificial intelligence (AI) and machine learning (ML) tools and services, AI agents, and agentic AI within organizations on data originating from multiple sources, it is becoming necessary for organizations to address compliance and efficient data management in an efficient and sustainable manner to remain competitive. The results of the case study are an evaluated and improved data management framework, applicable to many types of organizations; this framework includes AI/ML-guided classification of data and the addition of adequate cybersecurity and quality measures prior to using the data and information in AI/ML-based tools or services, AI agents, or agentic AI solutions. This paper highlights the need for a new or improved AI policy and suggests that organizations update or improve their strategy and processes to reap the benefits while avoiding exposure of confidential matters and non-compliance. The framework and its process, identify–protect/secure–prevent, can have significant practical potential and be useful for many organizations, such as universities, public entities, and companies, that possess large amounts of unclassified data. One of the organizations that was part of the evaluation was able to quickly classify more than 10 TB of data, and another was further able to delete/remove about 90% of its data, which was irrelevant and, to a large extent, unknown (i.e., dark data), enabling a transition to new infrastructure with significant cost savings, achieving compliance, and improving data management efficiency at the same time.

Keywords: artificial intelligence (AI); availability; confidentiality; compliance; cost; cybersecurity; data classification; data management framework; efficiency; integrity; machine learning (ML); optimize; quality; usability

Academic Editor: Sheng-Tzong Cheng

Received: 31 August 2026
Revised: 16 October 2026
Accepted: 19 October 2026
Published: 21 October 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

This case study investigates how compliance (with cybersecurity standards, internal/external requirements, and legal/regulatory requirements) and efficient data management in public and private sector organizations can be achieved. The starting point for many organizations is that they have a lot of data and information that have been accumulated over years, without having implemented a strategy comprising proper data classification and long-term data management. This is further accentuated by the recent use of artificial intelligence (AI) agents, data-driven applications, or agentic AI, which can

access an organization's data, documents, emails, etc., often without clear operational boundaries and access limitations [1–3].

Data classification schemes can be very simple or advanced depending on whether the organization is active within critical parts of society, defense, etc., classifying data in terms of confidentiality, integrity, and availability (cf. ISO 27001/2 and 38505 [4–6], NIST Cybersecurity Framework 2.0, SP 800-53 and SP 800-60 [7–9]). Regarding confidentiality, common schemes may have, from lowest to highest, three classes, such as public/open, internal, and confidential, or five classes, such as public/open, business, internal, confidential, and strictly confidential/top secret. Furthermore, NIST SP 1800-39 [10] addresses classification of unstructured data and categories such as synthetic, privacy-, health-, and payment-related data (credit card numbers, etc.) and how to handle such data in operations/processing, storage, and communications. In practice, tagging data/information (e.g., attaching a label of internal or confidential) commonly requires one or more tools (Examples of tagging tools are Microsoft's Sensitivity Labeling, Google's Classification Labels, and Amazon's AWS Resource Tags), depending on what types of data an organization uses. Furthermore, tagging is complex within databases or information systems unless there is built-in support. This paper will address the confidentiality, integrity, and availability aspects of data classification, with a slight emphasis on confidentiality. The various classes have an impact on how access, authorization, and cybersecurity/protection levels should be set up. It will also discuss proactive planning for access and migration/moving of data to another setup (or provider).

Long-term management of data should be efficient, as there is often a large cost associated with managing large quantities of data; moreover, users should be able to find what data they need instead of just obtaining new data and adding that to the growing set of accumulated data. There is also a risk that over time, the unused part of the data set accumulates without any perceived value creation from it. More data, accumulated over time without order and classification, is also a risk for lower/sliding data quality and duplicate data. Further, making backups of data is rather straightforward, but restoring data is costly and may take a lot more time (depending on setup and agreements). Therefore, backing up data that is not used anymore may become a serious issue, for instance, if many organizations need to restore data at the same time from an external cloud data center provider due to a cyber incident. Thus, the confidentiality, integrity, and availability of data can also be seen from a long-term data preservation perspective: accessible/available, not changed by unauthorized persons or entities (such as agentic AI or AI agents), and usable (where quality is intact, and retention/deletion is continuously upheld (cf. ISO 14721 [11])).

This paper examines how to achieve compliance and efficient data management over time when starting to use various AI/ML tools or agents and risk exposing sensitive data/information through AI/ML-guided classification of data and AI policy enforcement. Furthermore, the purpose of the paper is to shed light on how to obtain a return on investment (ROI) from any data accumulation-related investments or actions made on a long-term basis.

2. Related Work

This section provides a brief overview of the paper's three main topics: classification of data, compliance, and data management.

2.1. Classification of Data

The introduction covered several standards related to the classification of data and various recommended protection/management schemes. Here, this continues with

categories of data, legal/regulatory implications (particularly within the European Union (EU)), and the use of AI/ML for classification.

There are special categories of data that also should be classified and may have legal/regulatory requirements beyond the normal business-related ones. Such categories may include structured or unstructured data; synthetic data; and personal-, health-, and payment-related data [1,2,9]. The scope and severity of requirements depend on the geographic region, and currently the EU seems to have the most regulated/updated and forthcoming requirements (e.g., EU GDPR (EU General Data Protection Regulation—https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng accessed on 20 July 2026), NIS2 (EU Network and Information Security Directive—https://digital-strategy.ec.europa.eu/en/policies/nis2-directive accessed on 20 July 2026), CER (EU Critical Entities Regulation—https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng accessed on 20 July 2026), DORA (EU Digital Operational Resilience Act—https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en accessed on 20 July 2026), CRA (EU Cyber Resilience Act—https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act accessed on 20 July 2026), AI Act (EU AI Act—https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai accessed on 20 July 2026), Data Act (EU Data Act—https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng accessed on 20 July 2026), Machinery Regulation (EU Machinery Regulation—https://eur-lex.europa.eu/eli/reg/2023/1230/oj/eng accessed on 20 July 2026), DMA (EU Digital Markets Act—https://digital-markets-act.ec.europa.eu/index_en accessed on 20 July 2026), and DSA (EU Digital Services Act—https://digital-strategy.ec.europa.eu/en/policies/digital-services-act accessed on 20 July 2026)). For instance, the EU stipulates in the GDPR, NIS2, and AI Act that data should be classified and that risk analysis needs to be conducted on a regular basis. The classification of data (as well as systems or services under development or in operation) is the foundation for being able to conduct a risk analysis. This is also reinforced in, for instance, the ISO/IEC 27001 (ISO/IEC 27001 Information security management systems—https://www.iso.org/standard/88435.html accessed on 24 July 2026) and 27005 (ISO/IEC 27005 Guidance on managing information security risks—https://www.iso.org/standard/80585.html accessed on 25 July 2026) standards. There are signs of slow worldwide legal/regulatory harmonization, although many regions will not harmonize due to either political or economic reasons. The industrial sector and critical infrastructures also manage a lot of data related to operations (performance of processes/services and what is produced/consumed), products (usage with wear/tear and maintenance needs, etc.), and intellectual property (recipes, drawings, methods, and know-how, etc.). The space and meteorological sectors also have special classes and categories of data. Thus, each sector and part of society has its own data classes and categories. Furthermore, Aggarwal [12] added that there is a need to be able to handle new/unseen data classes and tag such data with labels. When new/unseen data can be related to already known user activities, departments, processes, etc., this typically makes it easier and faster to classify. Hossain and Sulaiman [13] stated that it is necessary to measure the accuracy of data classification algorithms, and it may be useful to use such an evaluation metric to find an algorithm that fits an organization's needs. A natural development of the recent advances in AI and ML is that such tools are increasingly used for (automated) data classification, highlighting the need to eliminate unimportant variables and improve the accuracy, performance, and balance/imbalance of the classification [14]. In addition, Shirvan et al. [15] surveyed imbalanced data classification problems, and Amer et al. [16] investigated performance problems using k-nearest neighbor models.

Thus, classification of data requires an understanding of many aspects ranging from legal/regulatory aspects to accuracy, performance, AI/ML, and advanced mathematics.

2.2. Compliance (Related to Usage, Storage, Communications, and Processing of Data)

Compliance is a multi-faceted and complex topic as it brings together requirements from, for instance, cybersecurity standards, internal/external stakeholders, and various legal/regulatory schemas (see examples above in the sub-section on classification of data). A problem is how much of a standard creates value versus the cost to comply, and thus, how much an organization should comply. Furthermore, legal/regulatory requirements need to be honored, whereas internal/external requirements should be a business decision. Compliance is further often part of general or data governance programs in organizations, making it a top management issue.

Scope et al. [17] posited that there should be governance policies for how data should be stored and used, comprising data retention, purging requirements, and consent, which may depend on regional legal/regulatory requirements and specific regulations for sectors such as healthcare, finance, and critical infrastructure. Additional requirements can include obligations to report cyber-related data incidents to authorities and other relevant parties. Furthermore, Ladley [18] asserted that the business one is involved in should be analyzed prior to making decisions on the need for compliance and a data governance program. The analysis should include, for instance, scope, business model, federation, elements needed in a governance program, principles, policies, metrics, and critical success factors. This requires engagement, strategy, design and architecture, implementation planning, and continuous operation and change management.

Thus, as organizations and the surrounding world change at a quick pace, compliance is hard to uphold, particularly within regions such as the EU, which is experiencing a compliance nightmare with multiple new and emerging laws and regulations related to data.

2.3. Data Management

Data management needs to be efficient in terms of energy consumption, costs, and effort spent, as the lifecycle of data can get longer and more complex than anticipated. Furthermore, the cybersecurity levels related to data and the systems or services within which the data is used are essential.

General data management is an important issue in many contexts; for instance, the EU promotes the FAIR data guide, or principles, so that research data and results can be used by many others [19]. The principles are for data to be findable, accessible, interoperable, and reusable, which requires making a management plan and describing and preserving the data. Pertaining to qualitative analysis and research, Bingham [20] proposed a five-phase process for data management to obtain actionable findings and organize, sort, understand, interpret, and explain the data. This requires data to be managed on short- and long-term bases, which requires planning and strategy from the very start. Regarding data lifecycles, a lot of data is generated in the fields of smart cities, meteorology/weather, and space/earth science, as well as in large organizations. In such contexts, it is necessary to ensure consistency, granularity, interoperability, and reusability of the data collected and stored via technologies for data security and privacy [21]. Regarding data governance, Janssen et al. [22] proposed a framework with 13 design principles to organize big data for trustworthy AI/ML, enabling stewardship of data, processes, and algorithms, trusted sharing between organizations, risk-based governance, controls for systems and data, and controlled data sharing. Such design principles can be useful in long-term efficient data management contexts. Concerning special categories of data, such as within healthcare, Singh et al. [23] proposed the use of blockchain technology to achieve efficient data management where only authorized persons/entities can add, view, and use data. This is mainly related to the confidentiality and accessibility of data, but also interoperability and compliance with standards. In addition, concerning big data analytics and the use of data

warehouses or data lakes, these may need to have different data management and processing schemas depending on the 7 Vs (volume, velocity, variety/data types, volatility/variability, veracity/accuracy, visualization, and value derived from the data), according to Nambiar and Mundra [24]. Processing schemas may include batch, stream, and hybrid processing.

Thus, this requires knowledge, planning, and strategy, supported by efforts, funding, and a technical infrastructure/architecture enabling long-term data management.

2.4. Gap to Be Addressed and Potential Contribution to Standards

Currently, existing and emerging legal and regulatory developments in the EU, global information-security-related standards, and data management guides or principles require or recommend that organizations classify their data, conduct continuous risk analyses, and secure their operations on a long-term basis. However, many organizations have not done this for a long time and have a data classification debt, which may become problematic as they want to start using new or emerging AI- or ML-based tools, AI agents, or agentic AI in a secure way. Manually classifying large quantities of data, e.g., 10–100 TB or more, residing in many known and unknown disks or repositories, is a gigantic task and is likely not feasible. Furthermore, the unknown data, or dark data, organizations accumulate over time, stop using, forget about, but retain poses another great challenge, as managing this data also incurs costs. This paper addresses the gap between formal requirements, i.e., what should/must be done and how to do this in practice, and provides a framework and tools to carry this out. Furthermore, the results could potentially be used to improve or augment, for instance, the ISO/IEC 27002 (ISO/IEC 27002 Information security controls—https://www.iso.org/standard/75652.html accessed on 18 July 2026) standard (which is the implementation guide for 27001).

3. Research Approach

This paper is based on a case study á la Yin [25] at Nordic Information Control AB (NIC) in Sweden. The case study approach was outlined according to Yin [25] using "a linear but iterative process" (p1) comprising planning, design, preparation, data collection, data analysis, and visualization/sharing of results. The approach was considered suitable to combine the academic state of the art with industrial knowledge and insights. The research question was *how to achieve compliance and efficient data management when using various AI/ML tools and risking exposing sensitive data/information*. This indicates that a case study methodology was appropriate. Other potential research approaches include action research or interviews. NIC is a high-tech SME with about five employees and has been active since 2021. Furthermore, NIC is a provider of advanced analytic services related to analysis of large data sets and compliance with EU legal/regulatory requirements and standards such as ISO 27001. NIC has developed an AI/ML-based tool and a data management framework and processes for this. NIC's public use cases are further used to evaluate the framework. The case study was conducted during 2025 and 2026. The case study design comprised formulating the study question and stating the study proposition: how to obtain a return on investment (ROI) from any data accumulation-related investments or actions made on a long-term basis. The unit of analysis was the organizational level (i.e., management of organizations and their operations) of the company studied. Explanation building was used to link the data to the propositions. To interpret the case study's findings, the criteria were set via rival explanations based on Patton's balanced defensive and offensive approach [26], where the researchers wanted to investigate *whether it is feasible to expect considerable improvement, ROI, and optimization of compliance and efficient data management within a couple of years*. A literature review was used to guide empirical studies and included approximately 100 papers using the Google Scholar and IEEE

search engines. Data were collected using semi-structured open-ended interviews, workshops [27–29], and additional materials from NIC (sales and strategy documents, sales presentations, and business development plans). The interviews lasted about 1 h, and the CEO and CTO were interviewed. See Appendix A for the interview questions. Interview problems and bias were minimized as much as possible by the experienced senior researcher preparing the interview questions and leading the interviews. Further limitations of the study are discussed in Section Limitations of the Case Study. The respondents were knowledgeable about the topic in question, having more than 25 years of experience in the IT software and services industry. Two workshops were also held with the CEO and CTO to collect additional data and ideas. To increase the validity, the interview respondents and workshop participants could view the recorded answers and directly corroborate/provide feedback using a TEAMS online conference window and a projected screen in a conference room. As the collected data set was small, no coding was applied. The data were analyzed using relational graphs and displayed using a table/matrix [30]. The data analyzed were used to propose improvements to NIC's data management framework (see Appendices B and C, Figures A1 and A2). Figure A1 was crafted based on the materials provided by NIC as part of the case study, and the three phases of the framework were extended using the analyzed data. Thus, triangulation was straightforward to perform. Finally, three use cases were used to evaluate NIC's framework and the proposed improvements.

Errors Recorded in NIC's AI/ML-Guided Classification of Data

The AI/ML-guided classification of data is based on NIC, and the customer can compose and compile a catalogue with classifiers related to the customer's context and operations, used to classify the data. Commonly, this is an incremental process, as the customer often does not know which types of data there are in all the repositories (including the dark data, which is unknown to the customer). The process starts with assessment scans on parts of the data, instead of the whole body of data, to save time and find out what data can/cannot be identified/classified. The assessment scans are then iterated to build up a baseline of identified data types and related classifiers. The baseline will gradually be extended into a catalogue of classifiers, which will later be continuously incremented as new types of data are created or added (i.e., discovered and classified).

Typically, based on NIC's customer cases, 30–90% of a customer's data is irrelevant, and dark data is typically considered irrelevant as well (and could be removed/erased). Thus, upon notifying the customer, a lot of the old data could be omitted from classification and either removed/erased or moved to special repositories for old/irrelevant data.

Among NIC's previous and current customer cases, the errors recorded after the initial assessment scans occurred in the Nacka municipality case (see Section Evaluation of NIC's Improved Data Management Framework Using Three Use Cases). A classifier record (or journal in Swedish) showed that not only medical records but also the staff's driving records were classified as confidential instead of as business. As this was corrected, there have not been any additional classification problems or false positives at Nacka municipality (or any of the other customers after this classifier catalogue building process is fully completed). Furthermore, there are certain types of data or files that cannot yet be classified by NIC, such as the contents of some pictures/photos if they are blurred, some stamps and watermarks, and old file formats.

Thus, the key is to build and then keep the classifier catalogue updated. The classifiers are based on regular expressions (REGEX) where compound attributes are built up. An example of this is a person's personal number/social security number, which is complemented by the context around it. Thus, an employee agreement will have the start date, salary, agreement type, title, etc. The ML-guided classification learns what the customer's

information and all types of employee records and agreements look like. The AI-guided part of the classification then helps to sort the metadata found after the scans. Additional files added to disks or repositories are automatically discovered and classified (see Section 4 for additional information on this). If classification is not possible, the data is flagged and then handled. NIC is currently improving the classification functionality and its usability to make this simpler for customers.

NIC's AI/ML-guided classification of data aims to help the customer achieve the requirements of globally applicable standards and legal/regulatory requirements. This is difficult if a customer does not know what types of data they have accumulated over many years in all disks and repositories. However, if a customer knows that they have sensitive personal data, healthcare/medical records, etc., these files can be classified and located to make sure that these are kept confidential and in the right places (and not in unprotected places). The classification does not make a customer compliant with, for instance, the ISO 27001 standard and legal/regulatory requirements, but provides a cornerstone to become compliant.

4. Findings

The data collected in the case study shows that NIC's data management framework has a three-step process, with additional sub-processes or sub-steps (see Figure A1) when addressing a new customer case together with the wanted/established data classification scheme (e.g., open, confidential, and strictly confidential). This requires that it is possible to find out what data/information is where, how sensitive it is, whether it is classified and tagged or not, and whether there are deviations from policies, which will enable a comprehensive risk assessment. Furthermore, the process and AI/ML-based tool will discover what data/information is stored in different locations, systems, or services. Thus, it is necessary to understand what data/information needs protection and what data can be shared and how. NIC has an AI/ML-based tool for automatic discovery and classification of data, which, when used properly, can facilitate the secure use of other AI/ML tools, achieve data/information security and compliance, and reach efficiency/cost savings via deletion/retention of data. However, NIC's AI/ML-based tool does not copy/move or tag data with a label, and additional tagging tools are commonly needed for the types of data an organization uses. The three-step process can be described as follows:

1. **Identify**: An automated traversal of the data and information residing on disks, information systems, cloud services, and other repositories that are made available for NIC's AI/ML-based tool. The first step identifies what data and information are harmless, personal information (PI), and sensitive personal information (SPI), and then maps out the data that may be obsolete or shared with others, access rights, and whether there are any deviations from policies. Further, there may be data/information in unknown disks or repositories that needs to be investigated and put into the right X-ray category. Any critical flaws, or the 2–3 most critical ones, discovered may require immediate remedy. First, an organization's top management needs training to learn why data management is needed and how to conduct it on a long-term basis. This will then lead to the development of a potential AI policy and changes/updates to related organizational policies such as IT, information security, or human resources (HR). An AI policy can comprise how to use AI/ML responsibly, what AI/ML tools are allowed to use (internal or external), and what information can be used and accessed by such AI/ML tools.
2. **Protect/secure**: Determining classification and protection/security-related improvements and whether they can be carried out by themselves or whether help is needed. Furthermore, the organization may need training to understand why the changes/improvements are needed and how to enact them properly. To check whether the

improvements and training provide any results, they should be fine-tuned and measured to show proof. The AI policy should be activated and provide automated support when using AI/ML tools for adequate access to data/information. An analysis of the above will lead to the development of a data/information architecture and protection levels, which then need to be implemented and tested together with the AI policy.

3. **Prevent**: The AI policy should be properly tested prior to being fully implemented regarding what data/information, systems, services, repositories/databases, etc., the AI/ML tools can access and use or not. This will help to prevent and minimize incidents and optimize costs through improved organizational strategies for data management and use of AI/ML tools to improve work processes and routines. In addition, continuous improvements in data management will lead to higher efficiency. Measurements should be made on a regular basis to spur additional improvements, and if possible, all this should be extended to suppliers (to avoid incidents spilling over from them). Regular exercises should be conducted to refresh understanding and get new employees on board.

Furthermore, there are some additional questions to ask during this process (or by any organization in general):

- What data/information is used, for what, and when?
    - Is there a lot of data/information that is never used again after creation?
        - What data/information must be kept for a period due to legal/regulatory requirements?
    - Do we have a functioning deletion-and-retention scheme for data/information?
        - Is the scheme in use?
- What is the quality of the data/information?
    - Is it good enough to base decisions on?
    - Is it ensured that the right data/information is used only for authorized activities in work processes, within manual or automated (using AI/ML tools, AI agents or agentic AI) work processes?

NIC's current data management framework is outlined in Appendix B, Figure A1, and the case study's proposed improvements are indicated in Appendix C, Figure A2, outlining the proposed improvements to the framework using purple and small arrows to further indicate where they are made. The proposed improvements have not yet been implemented in the framework. The proposed improvements are listed below according to the three main process steps:

Identify

- What data/information objects are tagged or not, and which tagging tools may be required based on the types and classes of data used?
- What are the current protection/security levels for these data/information objects?
- Who should be able to access these data/information objects?
- Training for (top) management teams.
- Crafting of AI policy and changes/updates may be required in related policies accordingly.

Protect/secure

- Is the current data quality good enough to base decisions on or not?
- Do we need/want to automate work processes using AI/ML tools (or AI agents or agentic AI)?

Prevent

- Can we prevent or minimize incidents, as well as optimize costs, using automation?
- Can we estimate or pre-calculate cost savings beforehand?
- Can we also extend the framework ideas to our value chain(s)?

Evaluation of NIC's Improved Data Management Framework Using Three Use Cases

The first step is evaluating the original NIC data management framework (Figure A1) and then determining what the proposed improvements (Figure A2) can add. The proposed improvements (conceptual) below were distilled from the interviews and workshops and are to be implemented by NIC. The improvements are expected not to affect the operation of the AI/ML-based tool but will add some extra steps into the process/model when applied in real cases. The automation of work processes may take some time to implement, but that is a task for NIC's customers.

- **Nacka municipality in Sweden, use case 1**: Nacka is a municipality near the capital city Stockholm with approximately 113,000 inhabitants. Nacka wanted to securely use AI/ML tools and prevent these tools from accessing sensitive data/information. Nacka had a significant amount of unclassified data/information. NIC's AI/ML-based classification tool scanned about +10 TB and automatically tagged ~4.5 TB while continuing to help with auto-tagging documents as new ones are created. Furthermore, the tool identified irrelevant information (unused data/information and copies) for deletion/archiving. Knowing what sensitive data/information to protect and what could be used by the employees when using AI/ML tools resulted in improved cybersecurity. In addition, this provided compliance with NIS2, GDPR, and the Swedish Public Access to Information and Secrecy Act, combined with lowered costs and more efficient data management.
    - NIC's data management framework helped to solve Nacka's problems in a timely manner with lower costs, improved compliance, and improved data management efficiency. The proposed improvements could have added further focus on automation matters regarding data quality, optimizing/automatizing work processes, preventing incidents, and minimizing consequences.
- **Company in retail information, use case 2**: A company makes labels for shelves, e.g., grocery stores and warehouses, that can be centrally updated and managed. Thus, there is no longer any need to run around and manually switch labels with the product name, EAN code, price, etc. They had a more than 20-year-old on-premise IT architecture and wanted to move to a new cloud-based IT architecture. The old IT architecture comprised more than 20 years of collected and stored data, with no one knowing how much there was in total. NIC's AI/ML-based tool was used to classify and identify dark data, distinguish between different types of data/information, and determine when it was created/altered/used, which led to the deletion of about 90% of the data. This allowed the company to acquire a smaller-scale cloud-based IT architecture at a lower cost, further improving data management.
    - NIC's data management framework helped solve the company's problems, transition to a new cloud-based IT architecture, and remove a lot of data/information. The proposed improvements could have helped automate work processes, prevent incidents, and minimize consequences.
- **Company in HR data management, use case 3**: A Swedish company manages customers' HR data/information on a long-term basis in various information systems and cloud services. The problem was that their customers did not know what data/information they had shared with others, whether the data/information was sensitive, and whether the sharing was conducted in an insecure manner. NIC's AI/ML-based tool enabled the company to classify, measure, and verify the data/information, stop

sharing, enable secure sharing, and minimize any consequences of a hacker/encryption incident.

- NIC's data management framework helped solve the HR data company's problems in terms of knowing what sensitive data/information they had and how and to whom the data was shared. The proposed improvements could have added insight into preventing incidents and minimizing consequences.

The evaluation shows that NIC's original framework creates value within the use cases, and the value may be further extended if the proposed improvements in Figure A2 are also applied.

5. Analysis

The empirical findings concerning how to achieve compliance and efficient data management when using various AI/ML tools and risking exposure of sensitive data/information can be outlined as potential improvements to NIC's data management framework and related processes; the findings also support the use of an AI/ML-based tool to facilitate such an endeavor. Furthermore, implementing an AI policy (and updating other related policies) is of utmost importance to automating what data/information can be used by AI/ML tools so that the data is securely stored and shared. This is important for many organizations, as increased amounts of old and unclassified data necessitate retention/deletion to maintain the quality of data/information. In addition, adequate tagging (or attaching labels) of data/information objects and being able to protect/secure the sensitive parts is a large step, in addition to sharing or using sensitive data accordingly. Automating or improving work processes in organizations using AI/ML tools or other engines requires high-quality data and the use of relevant data from appropriate data classes. AI/ML tools should not be able to use/ingest data that is not authorized or from the wrong data classes. Improving and automating the management of incidents and minimizing the consequences are also key for most organizations in light of what happens every day regarding cyberattacks. In addition, the analytic findings point to the fact that for organizations to be able to have good returns on AI/ML investments, they likely need to change and update their organizational strategy and processes, including adding an AI policy.

Furthermore, if there is a need for migration to a new data architecture or a cloud IT architecture, it is necessary to determine what data should be migrated. This question is also related to compliance, protection/security level, and cost. Thus, it is important to identify the data/information being used and ensure it is of adequate quality and current, as migrating all data, including data with questionable quality, provides little value. A further question is whether only data/information of certain classes and types used within the last x number of years (unless there are legal/regulatory requirements) should be selected and whether the rest should be omitted (if such data have not been used for a long time). In addition, interoperable/migratable data formats should also be considered to avoid technical or vendor lock-ins.

Taking another step or two further, organizations could craft a tailor-made management system for IT/information security (cf. ISO 27001/2 [4,5]) using an AI tool, considering the data/information and what they do. This would constitute a data/information- and business-based approach rather than a top-down approach. Additions and fine-tuning are probably needed after the initial crafting, but the volume would likely be quite optimized compared to top-down approaches.

Regarding the research question of *how to obtain a return on investment (ROI) from any data accumulation-related investments or actions made on a long-term basis*, the results indicate that NIC's data management framework and process offer several opportunities. For instance, reduced costs, automated incident management, and minimization of

consequences from incidents are key drivers, along with high-quality classified data/information and adequate protection and access. This further enables secure use of AI agents, agentic AI, and other work process automation engines. Considering rival explanations and *whether it is feasible to expect considerable improvement, ROI, and optimization of compliance and efficient data management within a couple of years*, the findings indicate that many organizations can expect these benefits, particularly those with a lot of unclassified data/information (or dark data). Further, if there is strong pressure from regulatory/legal institutions, as in the EU, the expectations may be even higher.

In comparison with relevant standards, principles, and frameworks discussed in the Introduction and Related work sections, NIC's data management framework addresses practical matters not covered by normative standards. See Table 1 below for a high-level comparison (as well as Section 2.4).

Table 1. Comparison of NIC's framework with relevant standards, principles, and frameworks.

Standard, Principle or Framework	Classification of Data	Use of AI/ML for Automation of Work Processes, Incident Prevention, Minimization of Consequences, etc.	Mgmt of AI/ML-Related Risks and AI Policy	Mgmt of Data/Information-Related Risks and CIA (CIA—Confidentiality, Integrity, and Availability) Protection Levels	Compliance	Data Deletion/Retention Schemes	Cost/Efficiency Aspects
ISO 27001/2	Yes	No	No	Yes	Yes	Partly	No
ISO 38505	Yes	No	No	Yes	Yes	Yes	Partly
NIST SP 800-53	Yes	No	No	Yes	Yes	Partly	No
NIST SP 1800-60	Yes	No	No	Yes	Yes	No	No
FAIR	Yes	No	No	No	No	Partly	No
NIC's current framework	Yes	Partly	Yes	Yes	Yes	Partly	Yes
NIC's improved framework	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 1 indicates that NIC's improved data management framework considers aspects that others do not. However, NIC's framework is not a public framework and can be improved based on experiences from recent customer cases and related requirements. The following points briefly cover each of the columns in Table 1 with additional explanations:

- **Classification of data**: All standards, principles, and frameworks state that classification of data must/need/should be done. Furthermore, the classification is the foundation for building an information security management system and conducting risk analyses.
- **Use of AI/ML for automation of work processes, incident prevention, minimization of consequences, etc.**: This is not clearly brought up in any of the standards or principles but is an emerging practice that is part of the NIC's framework. In particular, the use of automation within incident prevention (and response) will likely get added to the standards in Table 1.
- **Management of AI/ML-related risks and AI policy**: This has not been specifically brought up in the standards but is also expected to be added to most standards,

principles, and frameworks in Table 1. Furthermore, the recent ISO/IEC 42001 and NIST AI Risk Management Framework (AI RMF) mainly concern risk management (and innovation) related to the use of AI rather than how to practically use data/information within AI/ML tools in a secure manner. These may be good to consider while crafting a potential AI policy.

- **Management of data/information-related risks and CIA protection levels**: This is addressed by all except the FAIR principles. These risks need to be addressed after the classification of data (and the actual implementation of the classification).
- **Compliance**: Compliance is a natural part of standards and frameworks addressing information security and data management or classification. However, it is not clearly brought up in the FAIR principles.
- **Data deletion/retention schemes**: There is a mix of yes, no, and partly among the standards, principles, and frameworks in Table 1. The ISO 38505 and NIC's framework with improvements cover this, whereas the ISO 27001/2, NIST SP 800-53, FAIR, and NIC's current framework only partly cover how to set up and implement data deletion/retention schemes. Data deletion/retention schemes are necessary to keep any large data repositories up to date and free of as much dark data as possible.
- **Cost/efficiency aspects**: ISO 38505 partly addresses cost/efficiency aspects, and NIC's current and improved framework fully addresses this. This is perhaps not in the interest of a standard but of great practical interest for any organization.

Thus, to conclude the analysis, there are ideas and frameworks available to achieve compliance and efficient data management when using various AI/ML tools and risking exposure of sensitive data/information.

Limitations of the Case Study

As the case study covered one company with a small number of respondents and a geographical/regulatory focus on Sweden and the EU, the findings may have been affected by potential selection bias in the use cases and a lack of independent benchmarking. Another limitation is that the proposed improvements have not yet been fully empirically tested.

6. Discussion and Conclusions

This paper contributes to the literature with findings regarding how to achieve compliance and efficient data management when an organization uses various AI/ML tools and risks exposing sensitive data/information. This is exemplified using a data management framework with proposed improvements (Figures A1 and A2). Further, the paper contributes to practice by highlighting the need for adequate data/information classification and tagging, combined with protection/security measures and strict access control. This is a necessity for most organizations, regardless of their size or business type. In addition, the paper's managerial contributions highlight the need for an AI policy and the importance of updating related organizational policies. To be successful in the long term, top management needs to ensure an adequate level of data quality and use automation in incident management to minimize the consequences. These measures are important for achieving compliance and efficient data management required in the future.

The paper's findings are aligned with the FAIR principles [19], Bingham's [20] proposed five-phased process to manage data, and Janssen et al.'s [22] 13 design principles. The paper's findings go a step further by striving for greater automation and the application of an AI policy to support the automation of various work processes and govern who can use, access, and share data/information in a protected/secure manner. In addition, an updated organizational strategy and processes may be needed to get a good return on

investment from AI/ML tools or services and automating work using AI agents and agentic AI. Further, the findings regarding classification and tagging of data with adequate protection/security are aligned with many of the standards and legal/regulatory requirements brought up in the Introduction. This is getting increasingly important in jurisdictions such as the EU. Automation is key to achieving compliance, reducing costs, and improving data management efficiency.

This paper highlights why it is important to classify and tag data/information and manage their whole lifecycle; otherwise, it will be very hard to keep track of what data/information is stored, accumulated, and can be shared, and how. It is also likely that the data quality will suffer if lifecycle management is poor or non-existent.

The research question, *how to achieve compliance and efficient data management when using various AI/ML tools and risking exposing sensitive data/information*, has been answered. Furthermore, AI agents and agentic AI can be included as part of the AI/ML tools, as these are expected to increasingly be used to optimize and improve/automate work processes and tasks. The findings are deemed to be highly generalizable to many contexts, business types, and organizations with different sizes and levels of complexity. Increased amounts of old and unclassified data/information result in there being more to gain.

The generalizability of NIC's framework, process, and AI/ML-based tool is deemed high when applied to larger, more complex organizational environment architectures despite being initially developed within a small enterprise context. As larger organizations typically accumulate more data and file types over time, assessment scans may take more time and effort but yield similar outcomes as smaller enterprises or organizations.

Pertaining to future research, the authors plan to dig deeper into technical and organizational challenges related to compliance and data management in the AI era. In particular, aspects related to automation and governance, risk management, and compliance (GRC) are of great interest.

In conclusion, most organizations can benefit from starting to address how they plan to create value in the future using AI/ML tools, AI agents, agentic AI, etc., particularly if their data/information are of low quality, unorganized, unclassified, and inadequately protected with security measures. This is part of being competitive and sustainable in the long term, and many changes are expected to occur in organizations over the next decade. Thus, top management and employees must prepare for these changes and act if they have not already done so.

Author Contributions: Conceptualization, J.L., P.B. and K.A.; methodology, J.L. and K.A.; software, P.B.; validation/evaluation, J.L., P.B. and A.S.; analysis, J.L., P.B. and A.S.; investigation, J.L. and P.B.; writing—original draft preparation, J.L., P.B. and A.S.; writing—review and editing, J.L. and K.A.; visualization, J.L. and P.B.; funding acquisition, J.L. and K.A. All authors have read and agreed to the published version of the manuscript.

Funding: The research was mainly funded by the companies themselves, and the endeavors of Luleå University of Technology were supported by the European Regional Development Fund with the Cybersäkerhetsnod Norr-project (no. 20366918) and Secure AI User Experience-project (no. 20379663 via Intrerreg Aurora combined with Region Norrbotten and Lapin Liitto).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: All interviewed companies have approved the data collected and the text written in this paper.

Data Availability Statement: All data collected and analyzed are available in the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

https://doi.org/10.3390/app162010425

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
ML	Machine Learning
EU	European Union
NIC	Nordic Information Control AB
CIA	Confidentiality, Integrity and Availability

Appendix A. Interview Questions

The interview questions were as follows:

1. What is the nature of the customer problem(s) that you address?
2. What types of customer organizations/companies do you address and also intend to address?
3. What customer cases have you implemented the solution(s) in?
4. How have you initially attempted to solve these customer problem(s)?
5. Are there any known issue(s) in your problem solution(s)?
6. Are there any known error rates, false positives, or other types of errors of interest?
7. What can be improved in the problem solution(s)?
8. What are your future plans for the solution(s)?
9. Anything else to add outside of the already asked questions?

https://doi.org/10.3390/app162010425

Appendix B. Figure A1

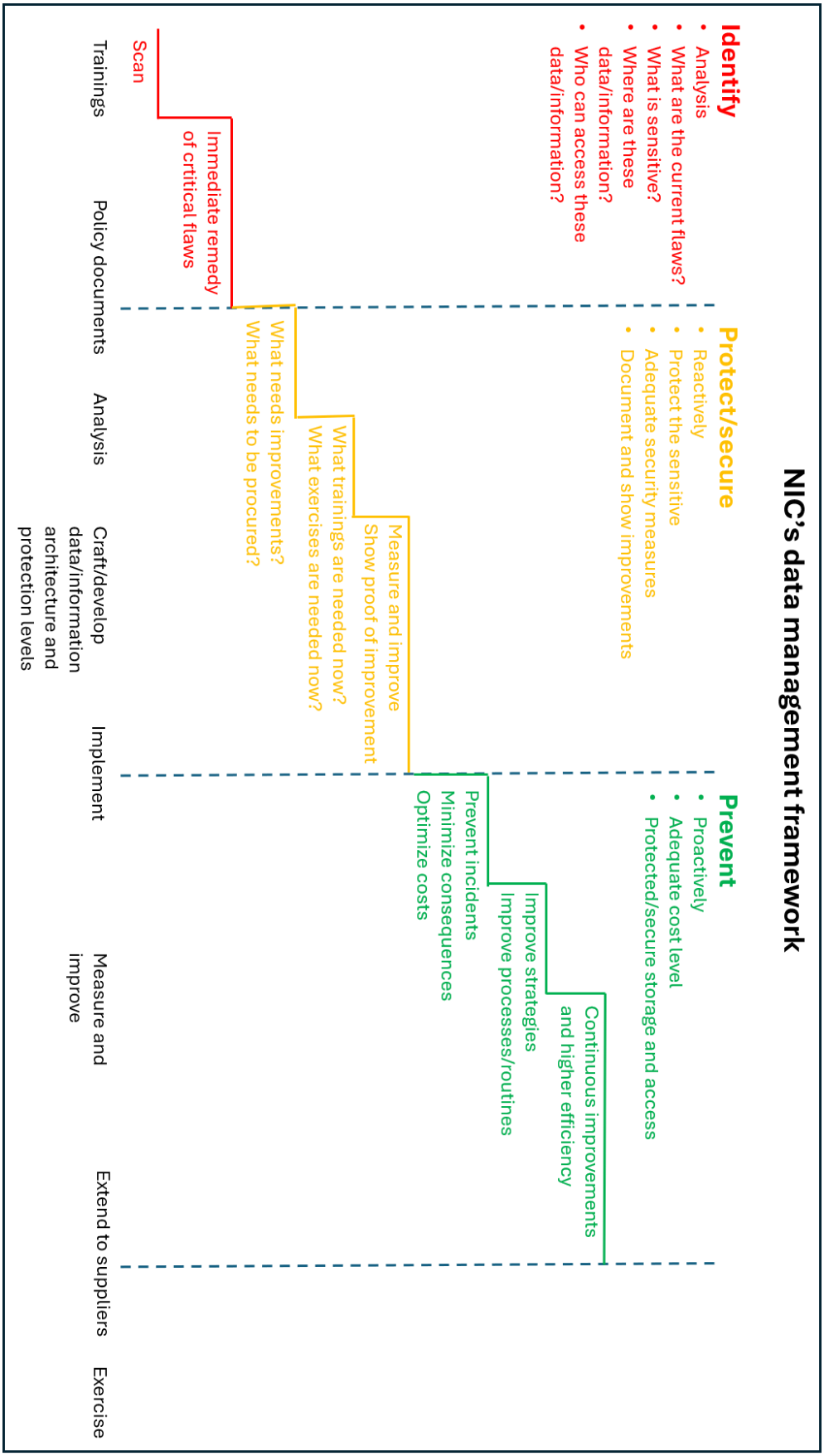

Figure A1. NIC's current data management framework.

Appendix C. Figure A2

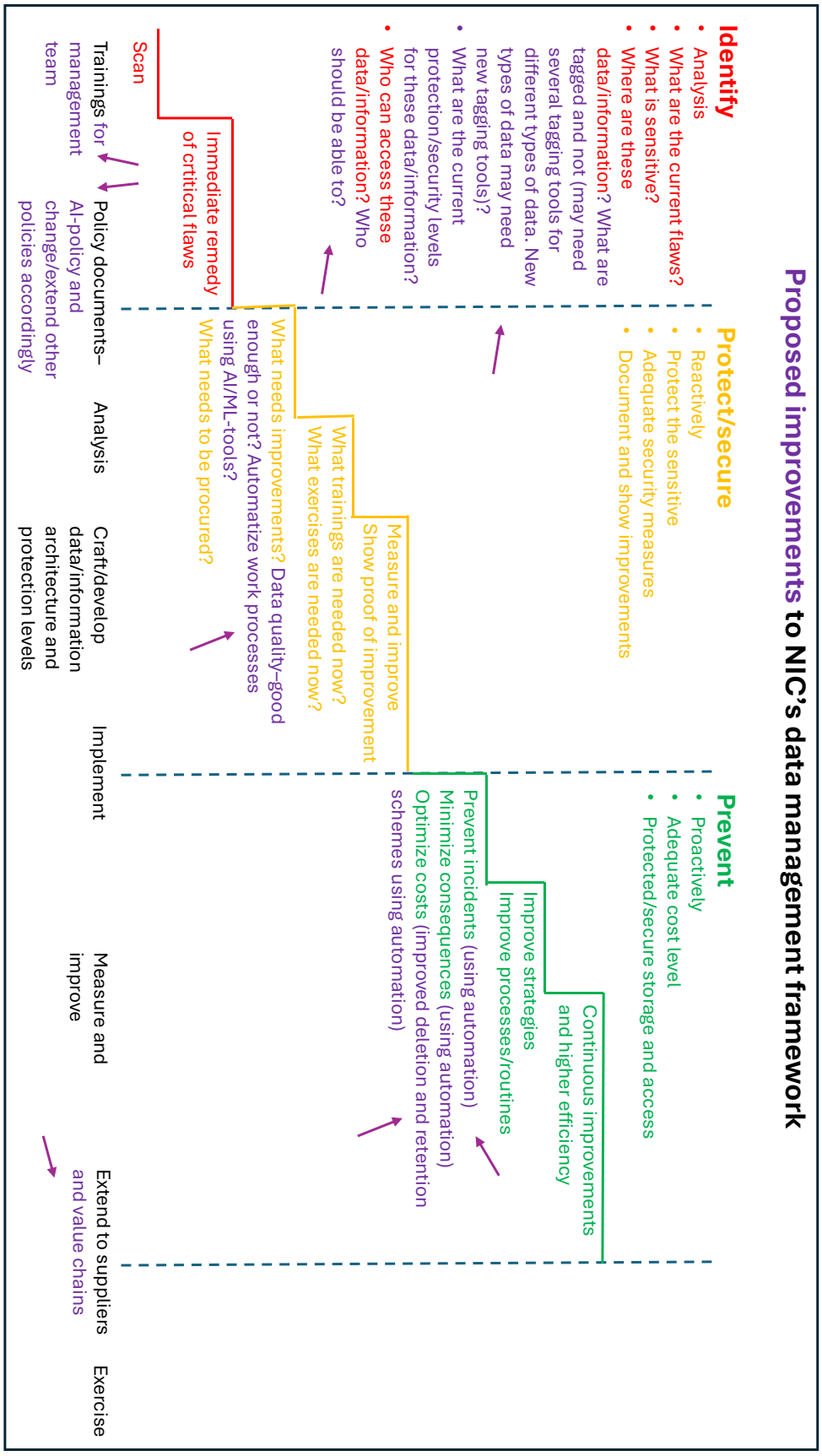

Figure A2. Proposed improvements to NIC's data management framework (in purple and indicated by small arrows as well) to be implemented by NIC.

References

1. Hughes, L.; Dwivedi, Y.K.; Li, K.; Appanderanda, M.; Al-Bashrawi, M.A.; Chae, I. AI Agents and Agentic Systems: Redefining Global IT Management. *J. Glob. Inf. Technol. Manag.* **2025**, *28*, 175–185.
2. Hughes, L.; Dwivedi, Y.K.; Malik, T.; Shawosh, M.; Albashrawi, M.A.; Jeon, I.; Dutot, V.; Appanderanda, M.; Crick, T.; De', R.; et al. AI Agents and Agentic Systems: A Multi-Expert Analysis. *J. Comput. Inf. Syst.* **2025**, *65*, 489–517.
3. Hofmann, P.; Urbach, N.; Lanzl, J.; Desouza, K.C. AI-enabled information systems: Teaming up with intelligent agents in networked business. *Electron Mark.* **2024**, *34*, 52.
4. *ISO/IEC 27001:2024*; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. International Standards Organization: Geneva, Switzerland, 2024. Available online: https://www.iso.org/standard/27001 (accessed on 10 June 2026).
5. *ISO/IEC 27002:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Controls, Requirements. International Standards Organization: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/75652.html (accessed on 11 June 2026).
6. ISO/IEC 38505-3:2021; Information Technology—Governance of Data. Part 3: Guidelines for Data Classification. International Standards Organization: Geneva, Switzerland, 2021. Available online: https://www.iso.org/standard/56643.html (accessed on 12 June 2026).
7. NIST. NIST Cybersecurity Framework 2.0. 2024. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (accessed on 4 July 2026).
8. NIST. NIST SP 800-53r5—Security and Privacy Controls for Information Systems and Organizations. 2020. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (accessed on 4 July 2026).
9. NIST. NIST SP 800-60r2 (Initial Working Draft, 2024)—Guide for Mapping Types of Information and Systems to Security Categories. 2024. Available online: https://csrc.nist.gov/pubs/sp/800/60/r2/iwd (accessed on 10 June 2026).
10. NIST. NIST SP 1800-39 (Initial Public Draft, 2026)—Data Classification Practices. 2026. Available online: https://csrc.nist.gov/pubs/sp/1800/39/ipd (accessed on 10 June 2026).
11. *ISO 14721:2025*; Space Data System Practices—Reference Model for an Open Archival Information System (OAIS). International Standards Organization: Geneva, Switzerland, 2025. Available online: https://www.iso.org/standard/87471.html (accessed on 10 June 2026).
12. Aggarwal, C. Data Classification. In *Data Mining*; Springer: Cham, Switzerland, 2015.
13. Hossin, M.; Sulaiman, M.N. A review of evaluation metrics for data classification evaluations. *IJDKP* **2015**, *5*, 2.
14. Chen, R-C.; Dewi, C.; Huang, S-W.; Caraka, R.E. Selecting critical features for data classification based on machine learning methods. *J. Big Data* **2020**, *7*, 52.
15. Shirvan, M.H.; Moattar, M.H.; Hosseinzadeh, M. Deep generative approaches for oversampling in imbalanced data classification problems: A comprehensive review and comparative analysis. *Appl. Soft Comput.* **2025**, *170*, 112677.
16. Amer, A.A.; Ravana, S.D.; Habeeb, R.A.A. Effective k-nearest neighbor models for data classification enhancement. *J. Big Data* **2025**, *12*, 86.
17. Scope, N.; Rasin, A.; Heart, K.; Lenard, B.; Wagner, J. The life of data in compliance management. In Proceedings of the CYBER 2021: The Sixth International Conference on Cyber-Technologies and Cyber-Systems (Part of the NexTech 2021 Congress), Barcelona, Spain, 3–7 October 2021.
18. Ladley, J. *Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program*, 2nd ed.; Academic Press: New York, NY, USA; Elsevier: London, UK, 2020.
19. Open Research Europe. FAIR Data Guide. 2022. Available online: https://horizoneuropencpportal.eu/repository/5b7fcc0e-73da-4e76-8b46-3682a36fa59b (accessed on 17 June 2026).
20. Bingham, A.J. From data management to actionable findings: A five-phase process of qualitative data analysis. *Int. J. Qual. Methods* **2023**, *22*, 1–11.
21. Gharaibeh, A.; Salahuddin, M.A.; Hussini, S.J.; Khreishah, A. Smart Cities: A Survey on Data Management, Security, and Enabling Technologies. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2456–2501.
22. Janssen, M.; Brous, P.; Estevez, E.; Barbosa, L.S.; Janowski, T. Data governance: Organizing data for trustworthy Artificial Intelligence. *Gov. Inf. Q.* **2020**, *37*, 101493.
23. Singh, S.; Kumar Sharma, S.; Mehrotra, P.; Bhatt, P.; Kaurav, M. Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives. *Mater. Today Proc.* **2022**, *62*, 5042–5046.

24. Nambiar, A.; Mundra, D. An Overview of Data Warehouse and Data Lake in Modern Enterprise Data Management. *Big Data Cogn. Comput.* **2022**, *6*, 132.
25. Yin, R.K. *Case Study Research: Design and Methods*; Sage Publications: Thousand Oaks, CA, USA, 2003.
26. Patton, M.Q. *Qualitative Evaluation and Research Methods*; SAGE Publications, Inc.: Thousand Oaks, CA, USA, 1990.
27. Fontana, A.; Frey, J. Interviewing. In *Handbook of Qualitative Research*; Denzin, N., Lincoln, Y., Eds.; Sage Publications: Thousand Oaks, CA, USA, 1994.
28. Kvale, S.; Brinkmann, S. *Interviews: Learning the Craft of Qualitative Research Interviewing*; Sage: Thousand Oaks, CA, USA, 2009.
29. Remenyi, D. *Field Methods for Academic Research: Interviews*; Academic Conferences Limited: Manchester, UK, 2012.
30. Miles, M.B.; Huberman, A.M. *An Expanded Sourcebook: Qualitative Data Analysis*; Sage: London, UK, 1994.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.