Journal of
Cybersecurity and Privacy

MDPI

Article

On Data Leakage Prevention Maturity: Adapting the C2M2 Framework

Jan Domnik [1,*] and Alexander Holland [2]

[1] Business Faculty, Accounting and Finance Department, Universidad Católica San Antonio de Murcia, Guadalupe de Maciascoque, 30107 Murcia, Spain
[2] Institute of IT Management and Digitization Research (IFID), FOM University of Applied Sciences, 45141 Düsseldorf, Germany; alexander.holland@fom.de
[*] Correspondence: ucam@domnik.es

Abstract: In an evolving cybersecurity landscape marked by escalating data breaches and regulatory demands, data leakage prevention (DLP) has emerged as one of several defense mechanisms. This study underscores unresolved foundational issues within DLP, revealing that it remains a significant challenge in large organizations. This highlights the necessity for a holistic approach to DLP to effectively address these persistent challenges. By developing a DLP Maturity Model, adapted from the renowned C2M2 framework, this research provides a comprehensive tool for assessing organizational DLP capabilities and pinpointing critical gaps. Applying the DLP Maturity Model within the financial sector as demonstrated through a banking scenario showcases its relevance and added value. This application illuminates the model's effectiveness in securing sensitive data and adhering to essential regulatory standards, highlighting its adaptability across various compliance landscapes. Implementing this DLP Maturity Model in a banking scenario showcases its applicability, highlighting its ability to formulate a strategy to secure sensitive data and comply with regulatory standards. This approach aligns with the concept of a continuous risk-based strategy, merging the holistic model to identify and address critical insider risks within organizations. The study addresses a specific gap in DLP research, notably the lack of a holistic framework for assessing and enhancing DLP strategies across organizations. It equips practitioners with a foundational tool to determine current DLP maturity and devise strategies for mitigating insider-driven data breach risks, thereby bolstering organizational cybersecurity resilience.

Keywords: data leakage prevention; data loss prevention; DLP; cybersecurity maturity; Maturity Model; C2M2

check for updates

Citation: Domnik, J.; Holland, A. On Data Leakage Prevention Maturity: Adapting the C2M2 Framework. *J. Cybersecur. Priv.* **2024**, *4*, 167–195. https://doi.org/10.3390/jcp4020009

Academic Editor: Georgios Kambourakis

Received: 22 February 2024
Revised: 22 March 2024
Accepted: 25 March 2024
Published: 30 March 2024

1. Introduction

The narrative of data leakage prevention (DLP) technology has unfolded rapidly yet succinctly within the cybersecurity domain [1]. Initially, up to 2005, DLP solutions were largely niche products with minimal deployment across industries. The period between 2006 and 2009 marked a significant turning point, characterized by multimillion-dollar (USD) acquisitions. Almost every major player in the IT security market acquired firms, aiming to secure a foothold in the DLP sector [2–7]. However, despite initial expectations for a widespread DLP adoption and integration into standards, the anticipated era of dominance for DLP tools did not unfold, with very few standards explicitly recommending their use. In 2019, the narrative experienced a refined shift, with the European Banking Authority (EBA) issuing updated information and communications technology (ICT) and security risk management guidelines, now adopted across numerous European nations [8], which recognized the significance of data protection yet refrained from explicitly requiring DLP. The next shift began with the broader adoption of monitoring tools and security information and event management (SIEM) systems, leading to a resurgence in DLP discussions. Contemporary standards, notably ISO/IEC 27001 and 27002 [9,10] as of

2022, now explicitly recommend the implementation of DLP tools. The discourse around the Digital Operational Resilience Act (DORA), mandating resilience for critical sectors in Europe, further exemplifies this trend, suggesting DLP's classification as essential according to the current perspective of the three European supervisory authorities (ESAs) [11].

Simultaneously, the frequency and severity of breaches continue to rise [12], which underscores the importance of holistic strategies in the field of DLP. However, there remains a discernible gap between employing discrete DLP tools and forging an overarching DLP strategy, underscoring the necessity of evolving from singular solutions to a holistic approach for DLP. This paper aims to bridge the existing gap by developing a DLP Maturity Model, specifically adapted from the C2M2 framework due to its proven reliability, industry-specific focus, and alignment with NIST methodologies. This model is designed for assessing DLP maturity, enabling target-actual comparisons and subsequently providing relevant information to support cybersecurity strategy development and decision-making regarding DLP.

The article makes several distinct contributions to the field of DLP.

- It highlights the importance of a holistic approach to DLP.
- It introduces a novel DLP Maturity Model, meticulously adapted from the C2M2.
- It details the application of this model within the financial sector, providing a comprehensive case study on its implementation in a banking scenario.

This study is structured into several key sections. Initially, it underscores the imperative for developing the DLP Maturity Model. It then delves into the essential definitions and themes underpinning DLP, setting the stage for a deeper exploration of DLP's principal components and maturity frameworks. This establishes a solid grounding in the subject. Subsequently, the paper elucidates the choice of the Cybersecurity Capability Maturity Model (C2M2) for evaluating DLP maturity and details the process of tailoring C2M2 into a bespoke DLP Maturity Model. Subsequently, theresults section (Section 3) presents the findings from the model's application in a banking context, highlighting its efficacy in identifying DLP capabilities and gaps. A key aspect of this section involves the practical application of the model, demonstrating its relevance and utility in safeguarding sensitive customer data and ensuring compliance with regulatory standards. Finally, the discussion section (Section 4) concludes by contextualizing the outcomes within the broader cybersecurity challenges, underscoring the model's contribution to enhancing organizational data protection strategies.

2. Materials and Methods

In the development of this study, the Design Science Research (DSR) methodology as outlined by vom Brocke et al. was adopted [13]. This choice was motivated by the structured and iterative approach the methodology provides, enabling a rigorous and systematic exploration of the research problem.

To organize the iterative process and its resultant outcomes, we employed the DSR grid, shown in Figure 1, also developed by vom Brocke et al. [14]. For this reason, we have structured this chapter into the six dimensions of the DSR grid: Problem, Input Knowledge, Research Process, Concepts, Solution (referred to as *Results* in this paper, see Section 3), and Output Knowledge.

2.1. Problem

In the realm of DLP, while there is a substantial body of research into DLP solutions, product comparisons, and cyber security maturity models [15], a conspicuous gap is evident in the literature: the lack of a structured DLP maturity model. This gap in both academic discourse and practical guidelines has led us to the development of a bespoke DLP Maturity Model, aimed at providing a structured approach to DLP implementation and management. This facilitates a systematic and holistic assessment of an organization's DLP capabilities, enabling the identification of areas for enhancement and strategic investment.

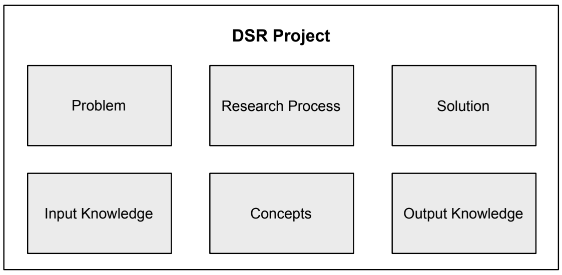


Figure 1. The DSR grid by vom Brocke et al. [14] served as both a tool for documenting activities within the DSR Methodology Process and the structure of this section.

While it is true that skilled and experienced personnel could manage several DLP measures efficiently through ad hoc practices, it is worth noting a caveat. This approach, although less resource-intensive, might not align with the structured, documented processes typically favored by regulatory bodies. Regulators often emphasize the need for structured, replicable procedures and clear documentation for compliance purposes. Hence, while an informal method might seem advantageous in terms of effort and resource allocation, its alignment with regulatory standards and compliance needs is an aspect that warrants careful consideration.

It is therefore important to understand that DLP serves not merely as a technical safeguard but also as a financial instrument, facilitating compliance and consequently averting regulatory penalties. This is particularly interesting for participants in highly regulated markets undergoing consolidation, such as the European banking sector [16]. While regulators increasingly mandate DLP requirements, to our knowledge, there exists no official framework or process dedicated to achieving a high level of DLP maturity. Often, DLP is integrated as part of a broader security solution, which, while generally beneficial, lacks detailed guidance on developing a step-by-step holistic DLP strategy. The approach by Alsuwaie et al. [17], though one of the few cited methodologies, primarily focuses on technical solutions, leaving a gap in strategic DLP planning and implementation.

2.2. Input Knowledge

This subsection delves into the foundational knowledge utilized in the development of the DLP Maturity Model.

2.2.1. DLP Definition

In alignment with the National Institute of Standards and Technology's (NIST) Special Publication 800-137 [18], DLP (also known as data loss prevention) in this article is defined as the detection and prevention of intentional and unintentional policy violations concerning data in transit, data at rest, and data in use. DLP encompasses a range of techniques and technologies designed to protect data across all stages, ensuring compliance with legal and regulatory standards. Primarily, it is a task within a security operations center (SOC), where outgoing data are scrutinized against specified rules to secure customer data and intellectual properties and to prevent reputational damage.

2.2.2. DLP Solutions

Initially, DLP strategies focused on monitoring network traffic and preventing unauthorized user activities [19]. Over time, there was a shift towards more centralized monitoring. Today's DLP solutions offer comprehensive monitoring across various data channels, encompassing web traffic, print jobs, email gateways, and file transfers to USB devices. They also incorporate advanced techniques like deep packet inspection. Both endpoint clients and centralized event collection mechanisms can be utilized together [20,21].

However, these advancements still come with challenges, notably performance limitations, e.g., when deploying sophisticated filtering rules such as advanced regular expressions to endpoint clients, which can significantly impact system performance.

In addressing the diverse landscape of DLP techniques, it is essential to distinguish between the various approaches. These techniques can be broadly classified into three categories: content-based analysis, context-based analysis, and hybrid approaches. The following provides a summary of the various approaches to DLP. For comprehensive evaluations and detailed discussions of the advantages and disadvantages associated with each DLP approach, refer to the extensive analyses in the literature, e.g., [22,23].

From the realm of data science and data mining, **content-based analysis** focuses on methods such as data fingerprinting, lexical content analysis (including rule-based systems and regular expressions), and statistical analysis. This technique [24] is adept at detecting sensitive information across various platforms, including laptops, servers, cloud storage, and outbound network traffic. Its approach is reminiscent of early spam filter technology [25]. It aims to prevent the accidental exposure of sensitive data, whether the data are static (at rest), being used (in use), or being transmitted (in transit) ([18], D-9). While effective in scenarios where sensitive data, along with potential senders and recipients, are clearly identifiable, this approach faces challenges. It often results in a high false positive rate due to several identifiable factors: the difficulty in crafting filters that account for all edge cases, the dynamic nature of DLP rules where yesterday's valid rule might flag false positives today, inconsistent data classification leading to misidentification, and evolving language and communication patterns that surpass the DLP system's rule update frequency. These limitations diminish the practicality of this method for routine business operations. Furthermore, it is vulnerable to obfuscation tactics employed by attackers, as sophisticated data alteration techniques can limit its effectiveness.

Contrastingly, **context-based analysis** eschews direct identification of sensitive content, instead analyzing the meta information associated with data or the context surrounding them [26]. This method models normal user behaviors and detects anomalous patterns, using machine learning to identify outliers. However, a significant limitation of this approach is its potential ineffectiveness in practical, everyday scenarios. For instance, it may fail to classify an email as a data leak risk based solely on metadata, without examining the content of attachments. Such scenarios include sending emails with attachments to personal addresses, where the actual content of the attachments is crucial for an accurate assessment of data leakage risk. Additionally, the effectiveness of this approach is often hampered by a lack of comprehensive training data, which are essential for accurately identifying false positive and false negative events and for refining the detection process.

Hybrid Approaches combine both content and context analysis [27–29]. This method leverages the strengths of both techniques to provide a more comprehensive solution. The hybrid approach is particularly effective in identifying sensitive content, achieving higher detection accuracy than pure context-based methods.

Therefore, content-based methods typically achieve higher accuracy but are susceptible to bypassing through data obfuscation. Context-based approaches, while often not as accurate, provide a broader scope of detection by considering user behavior and data context. Hybrid methods aim to balance these aspects, offering a more robust solution to DLP.

As illustrated, the domain of DLP techniques presents a diverse array of approaches. However, it is important to recognize that each method, while effective in certain contexts, also has its limitations.

2.2.3. Persistent Challenges in DLP

Theoretical perspectives position DLP as a crucial component of a comprehensive cybersecurity risk mitigation strategy. In practice, however, the implementation of DLP systems is associated with substantial costs, not only in initial deployment but also in continuous configuration and maintenance ([30], p. 218). Although the primary focus of this article is on the technical aspects of DLP, it is imperative to acknowledge that DLP encompasses a broader spectrum of issues. These additional considerations, vital for a holistic approach to DLP, have been extensively explored in the literature [31,32]. This multifaceted nature of DLP underscores the need for an integrated strategy that extends beyond mere technical solutions to include organizational, procedural, and human factors.

At first, identifying accurate true positive events for DLP alarms is a complex and non-trivial task. It demands a comprehensive understanding of the organization's unique context, including its various departments and operations. This process often requires an experienced DLP analyst to meticulously define a range of exceptional cases, which can be extensive and intricate. Their expertise is crucial in finely tuning DLP systems to effectively distinguish between legitimate and malicious data transactions, thereby ensuring both security and efficiency.

Secondly, the task of establishing effective thresholds to minimize false positives in DLP systems presents a significant challenge, arguably more complex than defining true positives. Security teams are often caught in a difficult balancing act: on one hand, they can set less sophisticated filters, which, while reducing the number of false positives, run the risk of missing genuine threats (a high-risk appetite). On the other hand, they face the Base-Rate Fallacy [33], a well-documented phenomenon in intrusion detection systems that is equally relevant to DLP. This fallacy highlights the difficulty in accurately detecting rare events in a sea of non-events, leading to a high volume of false positives.

Configuring an efficient DLP rule set for identifying both true and false positive events is a complex and nuanced process, especially in varied email-based scenarios. For instance, consider the case where employees send sensitive documents to personal email addresses. While this might initially appear as a straightforward true positive, the reality can be more complex. Many organizations, aiming to save on postal costs, routinely send encrypted emails to employees' personal addresses or have documents sent to business emails which are then forwarded or printed out. Further complicating matters, specific sectors like banking might regularly send sensitive, encrypted data to clients, such as wealthy private customers requesting encrypted Excel files. Additionally, human resources departments frequently exchange sensitive information with a large and diverse pool of applicants.

While technological solutions exist for these scenarios—like exact data matching for identifying large volumes of sensitive data, OCR for text recognition in scanned documents, allow-lists for different departments, and encryption gateways and deep packet inspection for analyzing encrypted traffic—the maintenance and continuous adjustment of a DLP rule set to accurately differentiate between legitimate and illegitimate data transfers is immensely challenging. The effort required to effectively manage, investigate, and handle both true and false positives in such dynamic environments can be substantial, reflecting the intricate balance between robust data protection and operational practicality.

In current practice, managing the complexities of DLP policies typically requires considerable effort, with most organizations facing a trade-off. Either they accept a higher risk of false negatives or adopt a conservative approach that leads to numerous false positives, necessitating significant investment in DLP. This situation highlights the need for more efficient DLP strategies that can balance these challenges effectively.

2.2.4. Impact of Large Language Models on DLP and Future Trends

The limitations of traditional DLP methods in large corporate settings are recognized and understood [1,22,34,35]. Extensive research has addressed specific aspects of DLP (among others [28,36–39]), yet a comprehensive solution to its complex practical challenges remains elusive. This gap underscores a significant opportunity for future exploration into the potential of large language models (LLMs) to revolutionize DLP strategies in dynamic business contexts. While recent studies have explored the use of LLMs in detecting phishing attacks [40], there is a notable absence of research on applying LLMs to DLP.

The prospective utility of LLMs in DLP remains speculative, yet their emerging capabilities suggest significant untapped potential. The current absence of LLMs from established DLP maturity frameworks is defensible, considering the technology's incipient stage of development and application in this domain. Nevertheless, the prospective integration of LLMs promises to be transformative, potentially streamlining DLP operations and reducing costs. In the preliminary phase, organizations might explore the support of LLMs to augment DLP analysts' capabilities in sophisticated data interpretation, which could lower the financial and logistical thresholds for attaining advanced DLP maturity. Close observation of these developments is imperative, as they may assist organizations in attaining elevated DLP maturity levels with diminished financial outlay.

2.3. Literature Research

A well-executed literature review should elucidate the subject matter, offering a comprehensive understanding of the topic at hand. Such an effective review establishes a solid groundwork, crucial for the progression of knowledge within the field, underscoring the pivotal role of literature reviews in academic research [41]. Furthermore, the essence of a literature review is unmistakably defined by the necessity to exclude a vast array of works during the search process ([42], p. 114), highlighting the discerning nature of scholarly research.

To construct a Maturity Model for the field of DLP, an in-depth understanding of DLP was indispensable. This constituted the initial phase of our literature research, aiming to lay a foundational comprehension that would underpin the entire model development process. Subsequently, the second phase of our literature exploration focused on identifying frameworks capable of assessing the maturity of a DLP infrastructure.

2.3.1. DLP Literature Review

A meticulous literature review was conducted with the primary objective of obtaining a profound understanding of DLP. This deep comprehension is essential for the development of a DLP Maturity Model, as it lays the groundwork for identifying and integrating the critical elements that define the maturity of DLP practices and technologies.

DLP represents a mature area of inquiry, characterized by a significant accumulation of research. This existing body of work necessitates a structured approach to literature review, as advocated by Webster and Watson [41].

The initial step in this structured approach involved querying knowledge databases using specific search terms, as detailed in Table 1. This process ensured that the literature review was comprehensive and aligned with our research objectives. Following this initial step, our focus was directed towards grasping the broader landscape of DLP, rather than delving into niche topics. With the aim of ensuring that the review encapsulated widely recognized and influential studies, we made a deliberate decision to exclude results that had five or fewer citations. This criterion was applied to concentrate our efforts on contributions that have garnered academic attention and have thus played a substantial role in shaping the understanding of the DLP domain.

Subsequently, we undertook the task of removing duplicates, thus refining our collection of sources. This step was critical for maintaining the quality and relevance of the literature under review, enabling a focused examination of the field that supports the construction of a robust DLP Maturity Model. We imposed several additional constraints to align more closely with our research focus and to ensure the relevance and quality of the sources considered. Firstly, we opted to exclude studies related to blockchain technologies. Despite the growing interest in this area, there is a discernible absence of practical, implementable proof-of-concept projects within the entire cybersecurity domain utilizing this technology. Furthermore, we disregarded ideas and theories presented without a prototype and those of a purely speculative nature. Additionally, any literature that did not demonstrate relevance for the practical application of DLP was omitted. This included highly technical works that delved into specifics such as highly sophisticated exfiltration techniques. Lastly, topics centered on key management, access management, and digital rights management (DRM) were also set aside. While these areas are crucial to the broader field of information and access management (IAM), they do not directly address the nuances of detecting policy violations.

Table 1. Knowledge databases queried.

	Web of Science	**IEEE Xplore**	**Science Direct**	**Wiley**
Search Term	"Data Leakage Prevention" OR "Data Loss Prevention" OR "Information Leakage Prevention" OR "Data Leakage Detection"	"Data Leakage Prevention" OR "Data Loss Prevention" OR "Information Leakage Prevention" OR "Data Leakage Detection"	("Data Leakage Prevention") OR ("Data Loss Prevention") OR ("Information Leakage Prevention") OR ("Data Leakage Detection")	"Data Leakage Prevention", "Data Loss Prevention", "Information Leakage Prevention", "Data Leakage Detection"
Search Fields/Topics	Topic Information Security, IT Security, Awareness	Information Leakage, Information Security, Data Leakage Prevention	Title, Abstract or Author-Specified Keywords	Title or Abstract
Additional Requirements	Articles, Proceeding Papers, Review Articles, Conference Papers	Conferences, Journals	Research Articles, Review Articles	-
Hits	164	107	27	1
Hits with >5 citations	44	31	16	1

Through these judicious exclusions, our literature review concentrated on sources that offer substantive contributions to the understanding and advancement of DLP, ensuring that our research is both comprehensive and focused. After applying these criteria, 51 papers were reviewed.

In line with best practices in conducting literature reviews [41,43], a backward search was conducted, yielding over 900 additional papers. The same stringent criteria previously outlined were applied to these findings. Ultimately, this rigorous selection process culminated in a consolidated corpus of 128 papers, forming the foundation upon which the insights presented in this work are based.

Initial attempts to organize the findings within a Concept Matrix (as proposed by [41,43]) were not conducive to selecting an appropriate maturity framework. Therefore, we shifted our strategy to employ a concept graph, a method supported by both Wolfswinkel et al. [44] and Webster and Watson. [45], to better synthesize and visualize the research outcomes. Figure 2 shows this process, providing a comprehensive visual summary of the knowledge synthesized.

2.3.2. Selection of an Appropriate Maturity Model

In contrast to the initial DLP focus, our intention was not to compile an exhaustive theoretical overview of potential frameworks. Instead, the aim was to glean a comprehensive survey of well-established frameworks within the domain. Adhering to the methodology proposed by vom Brocke et al. [46], a sequential search for representative literature using a keyword-based approach was conducted. This strategy enabled the identification of frameworks that have been recognized for their applicability and effectiveness in organizational cybersecurity contexts.

A multitude of papers have been identified comparing various maturity models, such as [47–49]. Systematic literature reviews in the field were also examined, including the work of Rabii et al. [15].

The outcome of the literature research reveals that, while frameworks such as the NIST CSF 2.0 and the ISO/IEC 27002 standard [10] can be employed as maturity frameworks, they are not purpose-specific to maturity assessments. Frameworks with substantial practical application in industry, including ISO 21827 [50], C2M2, CMMI, and CMMC, have been recognized for their utility and adoption in the field.

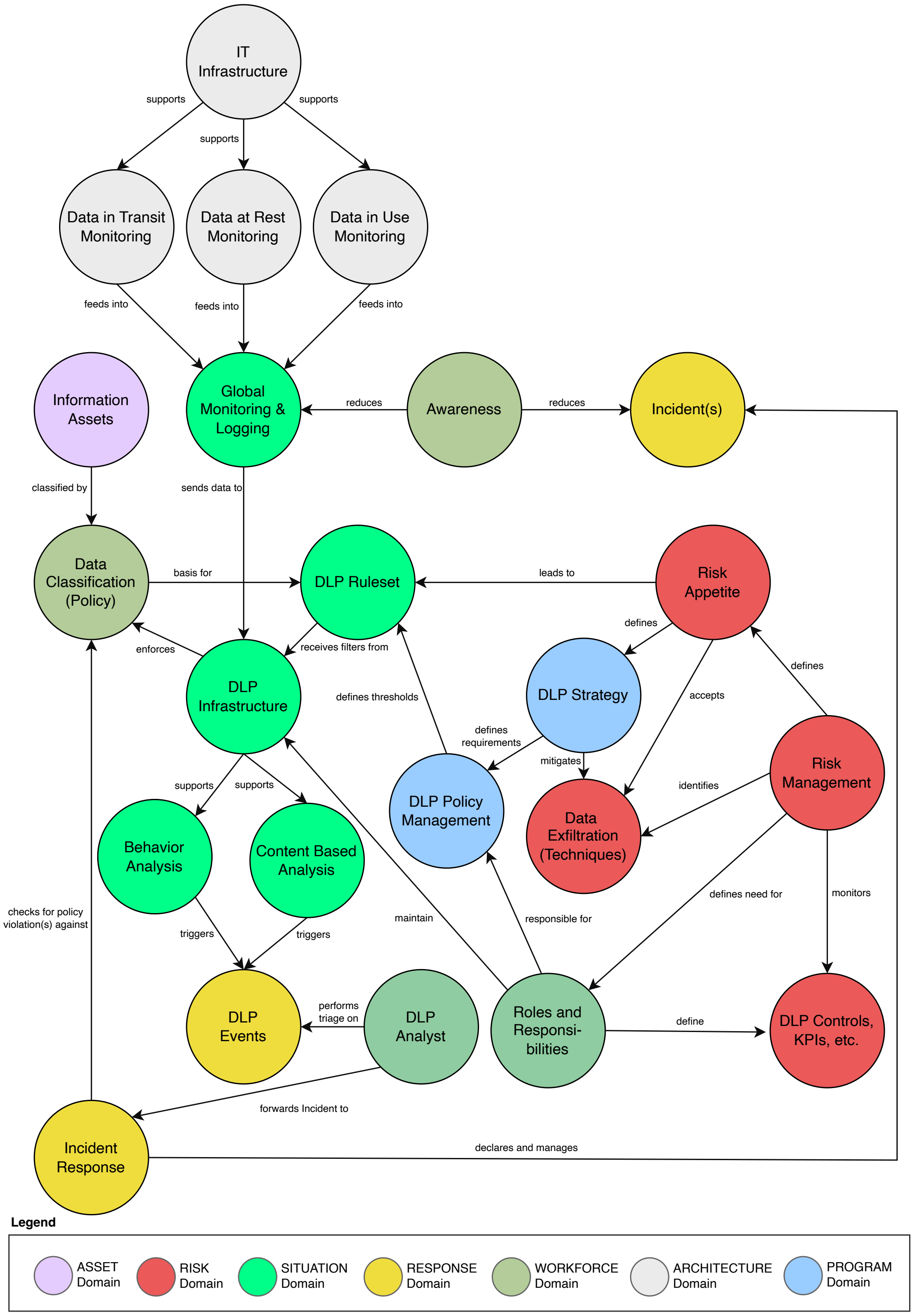


Figure 2. Conceptual visualization of knowledge synthesis from DLP literature review. The color-coding of individual nodes was not derived from the literature review but was applied subsequently to indicate the selection of corresponding objectives from the Maturity Model.

2.4. Concepts

In the following, pivotal concepts underpinning the study are delineated. They describe the selection of the C2M2 and the creation of the DLP Maturity Framework.

2.4.1. Selection of a Suitable Maturity Framework

Leveraging an existing model proved advantageous due to its well-established nature, reducing the likelihood of overlooking crucial aspects. Established models not only come with extensive literature and practical examples but also with supporting tools for implementation and documentation, thus offering a solid foundation for a DLP Maturity Model.

After careful comparison, as detailed in Table 2, we selected the Cybersecurity Capability Maturity Model (C2M2). This model was chosen for its synergistic alignment with the methodologies of NIST and its own comprehensive scope.

Table 2. Comparison of maturity frameworks.

	C2M2	ISO/IEC 21827	CMMC	CMMI
Update Frequency	Regular updates to align with evolving cybersecurity threats.	Last updated in 2008.	Regularly updated.	Regularly updated.
Industry Focus	Broad and adaptable to different sectors, making it suitable for a wide range of industries.	Broad and adaptable to different sectors, making it suitable for a wide range of industries.	Primarily for U.S. Department of Defense contractors, limiting broader applicability.	Broad but restricted due to accessibility.
Standards Compatibility	Highly compatible with NIST's methodologies, ensuring a comprehensive and synergistic approach.	Compatible with the ISO ISMS approach.	Oriented towards suppliers and their cybersecurity maturity.	Unknown due to limited accessibility.
Proven Track Record	Well-established with a proven track record of reliability and effectiveness in various sectors.	Lacks extensive scientific implementation experiments due to its last update in 2008.	Track record for third-party security audits.	Maturity levels from this framework are well-established. The rest has restricted applicability due to limited accessibility. Further materials have a restricted applicability due to limited accessibility.

While considering other models, C2M2 emerged as the most fitting due to several factors. ISO/IEC 21827 [50], though significant, is somewhat dated, having not been updated since 2008. The Cybersecurity Maturity Model Certification (CMMC), heavily oriented towards the U.S. Department of Defense, presents limitations in a broader industrial context. In contrast, ISACA's CMMI, not being publicly accessible, restricts its applicability. The popularity and well-established nature of C2M2, as indicated in [49], offer a proven track record of reliability and effectiveness crucial for a robust DLP maturity framework.

Moreover, the absence of extensive scientific implementation experiments for many models, noted in [15], necessitated a choice that best aligns with DLP's unique demands. The historical reliability and experience offered by C2M2, coupled with its adaptability to specific sector needs, make it a suitable model for this purpose. The adaptation of general models to specific cybersecurity challenges, such as incident management as mentioned in [51], further reinforces the practical and academic viability of tailoring C2M2 for DLP.

In summary, the selection of C2M2 for DLP in critical infrastructures is justified by its industry-specific focus, detailed cybersecurity practices, modular structure, and compatibility with other standards. Its practical orientation, implementation focus, and proven track record make C2M2 an ideal choice for organizations seeking a robust, adaptable, and effective approach to data leakage prevention.

2.4.2. Adopting the C2M2

In the C2M2, maturity indicator levels (MILs) delineate the maturity of cybersecurity practices across a spectrum. The MILs serve as a yardstick to:

- Define the organization's current state of DLP maturity.
- Determine the future, more mature state the organization aspires to reach, effectively guiding a gap analysis between the current and target cybersecurity postures.
- Identify specific capabilities and improvements needed to advance to that future state, providing a roadmap of actionable steps for progression.

MIL0 indicates no implemented practices, while MIL1 represents initial, potentially ad hoc efforts. MIL2 shows practices that are documented and resourced, becoming more refined than MIL1. MIL3 signifies advanced practices that are policy-driven and evaluated for effectiveness, an enhancement over MIL2. Furthermore, MIL3 institutionalizes a culture of continuous improvement, where activities are systematically tracked and quantifiably assessed, enabling both the immediate evaluation of DLP effectiveness and the long-term enhancement of the information security strategy.

The MILs are adapted for the DLP Maturity Model to provide an analogous structured assessment for DLP practices. As shown in Figure 3, these levels were integrated to define the progression from non-existent DLP measures (MIL0) through to a mature state of advanced DLP practices.

MILs are not merely a measure of adherence to standards but are indicative of an evolutionary growth in managing and safeguarding sensitive data. They enable organizations to set realistic goals and prioritize efforts to enhance their DLP maturity, all while offering a framework to benchmark against industry peers.

Aiming for MIL2 is recommended for robust cybersecurity, while MIL3 is the mark of excellence and should be pursued as part of a risk-based approach.

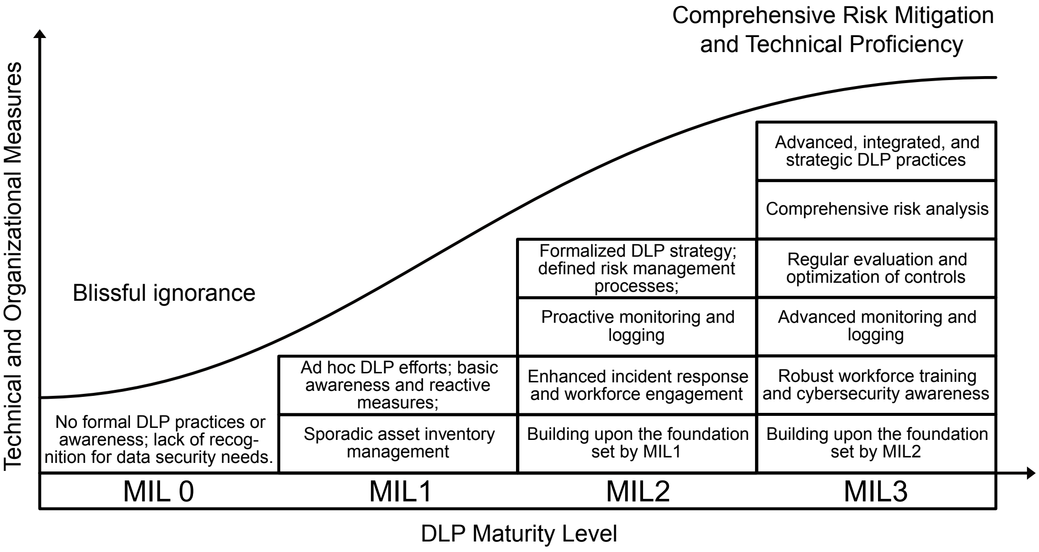

Comprehensive Risk Mitigation
and Technical Proficiency
Technical and Organizational Measures
Blissful ignorance
No formal DLP practices or awareness; lack of recognition for data security needs.
Ad hoc DLP efforts; basic awareness and reactive measures;
Sporadic asset inventory management
Formalized DLP strategy; defined risk management processes;
Proactive monitoring and logging
Enhanced incident response and workforce engagement
Building upon the foundation set by MIL1
Advanced, integrated, and strategic DLP practices
Comprehensive risk analysis
Regular evaluation and optimization of controls
Advanced monitoring and logging
Robust workforce training and cybersecurity awareness
Building upon the foundation set by MIL2
MIL 0
MIL1
MIL2
MIL3
DLP Maturity Level

Figure 3. Authors' synoptic depiction of DLP Maturity Framework progression.

In both the C2M2 and the adapted DLP Maturity Model, there are domains that categorize high-level aspects. Within these domains, there are specific objectives that represent targeted goals. The described MILs are used to assess the attainment of these objectives.

The adaptation of the C2M2 to a DLP Maturity Model involved a meticulous, three-step process, ensuring that each domain aligned with the specific nuances of DLP.

Step 1: Domain Relevance Assessment. Domains in the context of the C2M2 model refer to specific areas of focus within the broader scope of cybersecurity. Each domain of the C2M2 model was rigorously evaluated for its applicability to DLP. This evaluation led to strategic decisions on the inclusion or exclusion of certain domains, as detailed in Table 3.

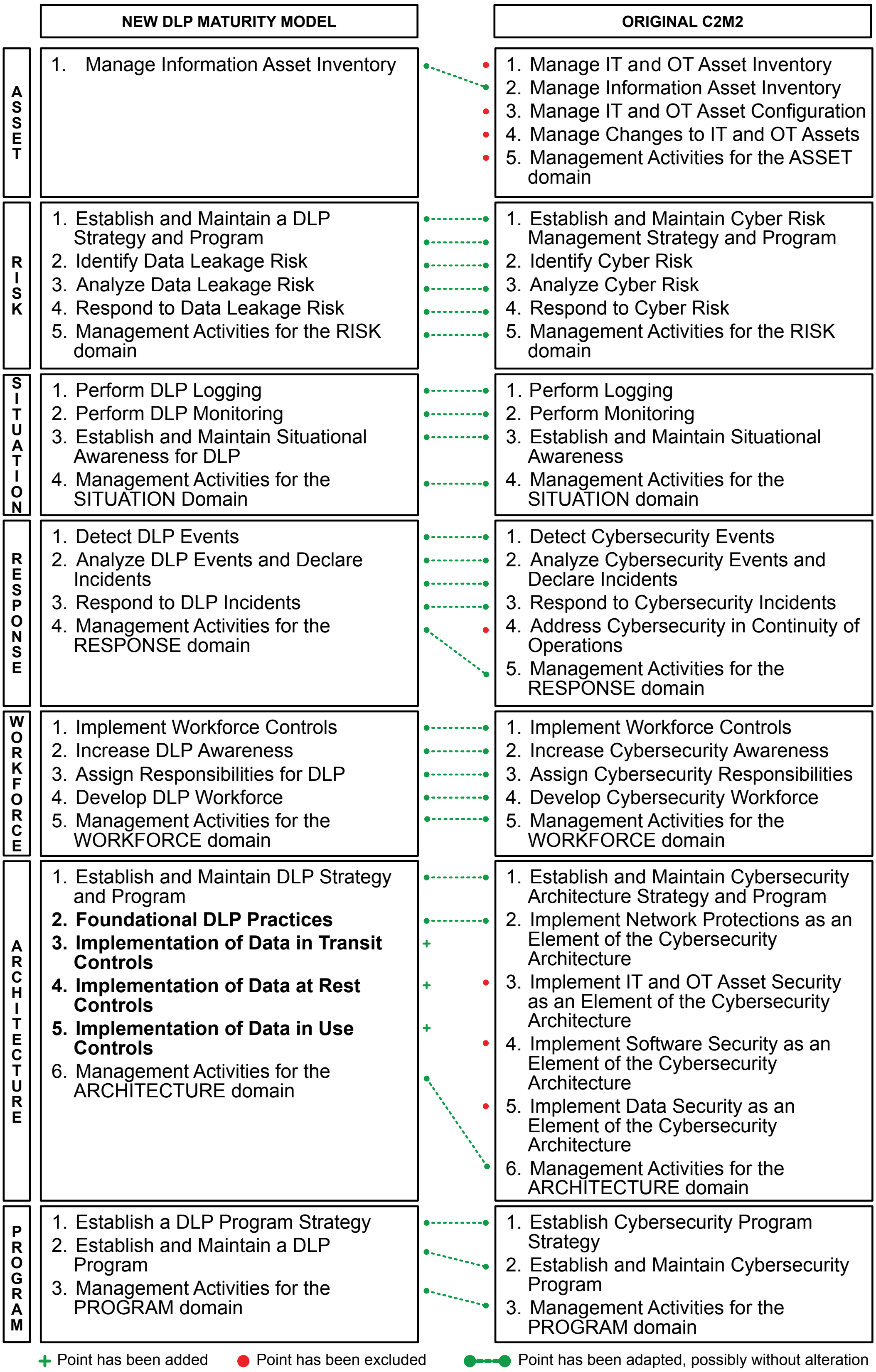
Our evaluation revealed that no additional domains needed to be incorporated into the DLP Maturity Model. This is due to the C2M2 already encompassing a comprehensive breadth of cybersecurity aspects, adequately covering the scope required for an effective DLP Maturity Model.

Step 2: Objective Analysis. The objectives within each selected domain were then scrutinized. In this process, objectives were aligned with the elements depicted in the concept graph (Figure 2). Those directly corresponding to a node within the graph were retained. Conversely, objectives lacking relevance to the elements depicted in the concept graph were discarded, ensuring that the framework's focus remained tightly aligned with DLP concerns. This alignment led to the addition of specific, DLP-relevant technical details within certain domains, notably within the ARCHITECTURE domain, to address any identified gaps. The meticulous mapping of objectives to the concept graph, distinguishable by different colored nodes in Figure 2, underscores our methodical approach to refining the framework for DLP applicability. Figure 4 illustrates the process and the adjustments made in detail.

Step 3: MILs Adjustment and Enhancement. A critical examination of the MILs within each objective followed. This involved tailoring each level (MIL1 to MIL3) to reflect the DLP context. The process included supplementing additional points to ensure a DLP-specific focus, especially in domains like ARCHITECTURE, where technical solutions are paramount. In this endeavor, among others, ISACAA's best practices for DLP [52] were used as a reference, supplemented by professional judgment, to determine the appropriate placement of these enhancements within the MIL structure. These adaptations can be found in Appendix A.1.

Table 3. Evaluation of C2M2 domains for applicability to the DLP Maturity Model.

Domain	Analytical Justification for DLP Relevance	DLP Related
ASSET	Asset management's crucial role in identifying and protecting sensitive data-bearing assets forms a foundational component of comprehensive DLP strategies.	Yes
THREAT	This domain, while pivotal in threat and vulnerability identification, does not engage directly with DLP's specific operational methodologies.	No
RISK	Integral for establishing a risk mitigation framework, it indirectly supports DLP by identifying and assessing risks pertinent to data leakage.	Yes
ACCESS	In the context of policy breach via data exfiltration, the domain's direct involvement in operational DLP processes is considered minimal.	No
SITUATION	This domain's emphasis on operational security and threat intelligence monitoring is vital for the early detection of potential data exfiltration, aligning with DLP objectives.	Yes
RESPONSE	Its focus on responding to cybersecurity incidents, including data breaches, aligns this domain closely with the reactive component of DLP.	Yes
THIRD PARTIES	The management of third-party risk is essential for comprehensive data security but does not intrinsically involve the operational specifics of data leakage prevention. This premise is based on the assumption that policies of an organization are uniformly applicable to both internal and external systems.	No
WORKFORCE	The development of a cybersecurity-aware culture and skilled personnel supports DLP through enhanced adherence to data security protocols.	Yes
ARCHITECTURE	This domain is directly aligned with DLP, encompassing the implementation of specific controls, including data exfiltration prevention mechanisms.	Yes
PROGRAM	Provides strategic oversight and governance for cybersecurity initiatives, including DLP, ensuring comprehensive management of cybersecurity risks.	Yes



NEW DLP MATURITY MODEL

ORIGINAL C2M2

ASSET

1. Manage Information Asset Inventory

1. Manage IT and OT Asset Inventory
2. Manage Information Asset Inventory
3. Manage IT and OT Asset Configuration
4. Manage Changes to IT and OT Assets
5. Management Activities for the ASSET domain

RISK

1. Establish and Maintain a DLP Strategy and Program
2. Identify Data Leakage Risk
3. Analyze Data Leakage Risk
4. Respond to Data Leakage Risk
5. Management Activities for the RISK domain

1. Establish and Maintain Cyber Risk Management Strategy and Program
2. Identify Cyber Risk
3. Analyze Cyber Risk
4. Respond to Cyber Risk
5. Management Activities for the RISK domain

SITUATION

1. Perform DLP Logging
2. Perform DLP Monitoring
3. Establish and Maintain Situational Awareness for DLP
4. Management Activities for the SITUATION Domain

1. Perform Logging
2. Perform Monitoring
3. Establish and Maintain Situational Awareness
4. Management Activities for the SITUATION domain

RESPONSE

1. Detect DLP Events
2. Analyze DLP Events and Declare Incidents
3. Respond to DLP Incidents
4. Management Activities for the RESPONSE domain

1. Detect Cybersecurity Events
2. Analyze Cybersecurity Events and Declare Incidents
3. Respond to Cybersecurity Incidents
4. Address Cybersecurity in Continuity of Operations
5. Management Activities for the RESPONSE domain

WORKFORCE

1. Implement Workforce Controls
2. Increase DLP Awareness
3. Assign Responsibilities for DLP
4. Develop DLP Workforce
5. Management Activities for the WORKFORCE domain

1. Implement Workforce Controls
2. Increase Cybersecurity Awareness
3. Assign Cybersecurity Responsibilities
4. Develop Cybersecurity Workforce
5. Management Activities for the WORKFORCE domain

ARCHITECTURE

1. Establish and Maintain DLP Strategy and Program
2. **Foundational DLP Practices**
3. **Implementation of Data in Transit Controls**
4. **Implementation of Data at Rest Controls**
5. **Implementation of Data in Use Controls**
6. Management Activities for the ARCHITECTURE domain

1. Establish and Maintain Cybersecurity Architecture Strategy and Program
2. Implement Network Protections as an Element of the Cybersecurity Architecture
3. Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture
4. Implement Software Security as an Element of the Cybersecurity Architecture
5. Implement Data Security as an Element of the Cybersecurity Architecture
6. Management Activities for the ARCHITECTURE domain

PROGRAM

1. Establish a DLP Program Strategy
2. Establish and Maintain a DLP Program
3. Management Activities for the PROGRAM domain

1. Establish Cybersecurity Program Strategy
2. Establish and Maintain Cybersecurity Program
3. Management Activities for the PROGRAM domain

+ Point has been added ● Point has been excluded ●--● Point has been adapted, possibly without alteration

Figure 4. DLP Maturity Model, constructed on the foundation of the C2M2.

2.5. Output Knowledge

To adhere to the constraints of this paper's scope, the objectives have been relegated to Appendix A.1. These can now be employed to conduct a DLP Maturity Assessment.

3. Results

This section describes the results of implementing the DLP Maturity Model in a banking environment, emphasizing the completion of our work and the practical outcomes derived from applying the model. In the banking context, DLP plays a pivotal role in safeguarding sensitive customer information, as well as in meeting compliance standards. This case study serves to illustrate the structured application of the DLP Maturity Model in evaluating and enhancing the institution's current DLP practices. It also provides a methodical approach for assessing the maturity level of these practices and gauging the bank's overall capability to prevent data leakage.

The analysis results in a comparative review between the current state and desired targets of DLP practices. This comparison then informs further actions within the bank's risk-based cybersecurity strategy, ensuring continuous improvement and alignment with regulatory requirements and best practices in data protection.

The implementation and evaluation of the DLP Maturity Model follows the structured approach outlined in the C2M2.

It should be taken into consideration that high-quality outcomes may be achieved with experienced and talented personnel even if practices are ad hoc.

3.1. Practical Implementation and Evaluation: Performing a Self-Evaluation

In the self-evaluation process utilizing our adapted DLP Maturity Model, each domain is assessed sequentially. Within each domain, objectives are evaluated individually. For every objective, the achievement of each MIL is contingent upon the responses given to the practices within that MIL and all preceding MILs.

A practice is considered *Fully Implemented* (FI) when it is complete and *Largely Implemented* (LI) when it is complete with some opportunities for improvement noted. Conversely, a practice is marked as *Partially Implemented* (PI) if incomplete with multiple improvement opportunities and *Not Implemented* (NI) if the practice is not performed at all by the organization. To achieve a particular MIL, all practices in that MIL, as well as those in all preceding MILs, must receive responses of either FI or LI. For instance, achieving MIL2 requires that all practices in both MIL1 and MIL2 are rated as either FI or LI. This stringent criterion ensures that each level of maturity is thoroughly and accurately assessed, reflecting a true picture of the organization's DLP capabilities.

3.1.1. Case Study: Implementing the Self-Evaluation in the SITUATION Domain

The process of self-evaluation is exemplified through the SITUATION domain, chosen for its comprehensive coverage of diverse DLP-related topics. This analysis utilizes the Objectives of the SITUATION domain, detailed in Appendix A.1.3, encompassing:

- Perform DLP Logging;
- Perform DLP Monitoring;
- Establish and Maintain Situational Awareness for DLP;
- Management of Activities in the SITUATION Domain.

In the Perform DLP Logging scenario, as detailed in Table 4, the assessed bank showcases robust capabilities. This is primarily attributed to the integrated use of SIEM and DLP systems, which facilitate immediate and effective logging. For MIL2 and MIL3 requirements, the status is Largely Implemented, a strategic decision based on the financial impracticality of achieving 100% client coverage. This was deemed disproportionate to the risk mitigation achieved. The risk of a few machines not reporting to SIEM was, therefore, an accepted compromise. The outcome was the achievement of at least Largely Implemented status across all MIL stages, so the bank reached MIL3. This outcome is visually represented in Figure 5, particularly at point 3.1 Perform DLP Logging, indicating a peak at MIL3.

Table 4. Assessment Outcome: The bank achieves MIL3 in this objective, as evidenced by the comprehensive implementation of objectives across MIL1, MIL2, and MIL3, with each objective meeting at least a Largely Implemented status.

Objective 3.1: Perform DLP Logging			
MIL		**Description**	**Outcome**
MIL1	a	Logging occurs for sensitive data, at least in an ad hoc manner.	**FI**
MIL2	b	Logging is implemented for assets that contain sensitive data.	**LI**
	c	Logging requirements are established.	**LI**
	d	Logging requirements are set for network and host monitoring (e.g., web proxies, e-mail gateways, print-monitoring on endpoint-clients).	**LI**
	e	Log data are aggregated and accessible for DLP analysts.	**LI**
MIL3	f	Logging is enforced for assets with higher data leakage risk priorities (e.g., for data at rest and data in use).	**LI**

For the *Perform DLP Monitoring* objective, as outlined in Table 5, the bank's evaluation reveals that objectives at MIL1 and MIL2 levels are at least *Largely Implemented*, ensuring these levels are met. However, structural constraints impede the adjustment of the DLP rule set. Due to potential extensive impacts on IT operations and the absence of a dedicated test infrastructure, any changes would require high-level management risk acceptance. Consequently, this aspect is classified as *Not Implemented*. Furthermore, regular reviews of the DLP rule set are not conducted; only ad hoc corrections are made when absolutely necessary, warranting a classification of *Partially Implemented*. Given that not all objectives at MIL3 are at least *Fully or Largely Implemented*, the bank's performance in this area is assessed as MIL2.

Table 5. Assessment Outcome: The bank achieves MIL2 in this objective, as evidenced by the comprehensive implementation of objectives (Fully Implemented, Largely Implemented) across MIL1 and MIL2 but not MIL3.

Objective 3.2: Perform DLP Monitoring			
MIL		**Description**	**Outcome**
MIL1	a	Log data or alerts from the monitoring infrastructure are reviewed, at least in an ad hoc manner.	**FI**
MIL2	b	Requirements for DLP monitoring are established and maintained.	**LI**
	c	Enhanced rule sets are configured to trigger alerts when a potential data leakage attempt is discovered.	**LI**
	d	Monitoring activities are aligned with the organization's risk-based security approach.	**LI**
MIL3	e	Enhanced monitoring is enforced for assets with higher data leakage risk priorities.	**LI**
	f	The DLP rule set undergoes periodic evaluation and updates, integrating insights from incident responses and false-positive alert assessments.	**PI**
	g	Adjustments to the DLP rule set can be executed on short notice if required.	**NI**

In the assessment process, as illustrated in Tables 6 and 7, a consistent methodology was applied. It was observed that the MIL1 level in both instances was deemed not applicable, thus defaulting to achieved status. The criteria for MIL2 were confidently met. However, certain objectives at the MIL3 level were either not achieved or only partially fulfilled. Consequently, both tables reflect an attainment of only the MIL2 level.

Table 6. Assessment Outcome: The bank achieves MIL2 in this objective, as evidenced by the comprehensive implementation of objectives (Fully Implemented, Largely Implemented) across MIL1 and MIL2 but not MIL3.

Objective 3.3: Establish and Maintain Situational Awareness for DLP			
MIL		**Description**	**Outcome**
MIL1		No practice at MIL1.	**-**
MIL2	a	Methods for communicating the current state of DLP are established and maintained.	**FI**
	b	KPIs relevant to DLP are collected for operational state awareness.	**LI**
MIL3	c	KPIs and thresholds for the rule sets are established and harmonized with leadership and stakeholder requirements.	**NI**
	d	Internal data crucial for DLP activities (e.g., employee terminations) are methodically collected and processed, leading to (ad hoc) modifications in the rule set as necessary.	**NI**
	e	Predefined operational states, such as Triage and Incident Escalation, are meticulously documented and activated in response to incoming alerts.	**FI**

Table 7. Assessment Outcome: The bank achieves MIL2 in this objective, as evidenced by the comprehensive implementation of objectives (Fully Implemented, Largely Implemented) across MIL1 and MIL2 but not MIL3.

Objective 3.4: Management of Activities in the SITUATION Domain			
MIL		**Description**	**Outcome**
MIL1		No practice at MIL1.	**-**
MIL2	a	Documented procedures are established, followed, and maintained for activities in the SITUATION domain.	**FI**
	b	Adequate resources (people, funding, and tools) are provided to support activities from the SITUATION domain.	**LI**
MIL3	c	Up-to-date policies define requirements for activities from the SITUATION domain.	**PI**
	d	Responsibility, accountability, and authority for the performance of activities in the SITUATION domain are assigned to personnel.	**PI**
	e	Personnel performing activities in the SITUATION domain have skills and knowledge needed to perform their assigned responsibilities.	**FI**
	f	The effectiveness of activities in the SITUATION domain is regularly evaluated and tracked.	**FI**

The achieved MILs across the four tables are traceable in Figure 5, specifically detailed under objectives 3.1 to 3.4. This visualization aids in comprehending the MIL outcomes in a consolidated and clear manner.

Finally, an overarching assessment was conducted for each domain across all tables, establishing a comprehensive MIL for each domain. This was achieved by first aggregating all MIL1 objectives from the four tables. The outcome showed that two objectives were *fully implemented*, while two were not applicable, reflecting the *No practice at MIL1* status.

For MIL2, a cumulative count across all four tables yielded 11 objectives, with nine being *fully implemented* and two *largely implemented*, indicating that MIL2 was at least achieved.

When considering MIL3, all 11 objectives from the four tables were tallied. The results were three *fully implemented*, two *largely implemented*, three *partially implemented*, and three *not implemented* objectives. Due to the presence of *partially implemented* and *not implemented* ratings, MIL3 was not attained.

Therefore, the domain-wide MIL for the entire SITUATION domain was determined to be Level 2. This comprehensive assessment can be visualized in the management dashboard shown in Figure 6 under the SITUATION domain.

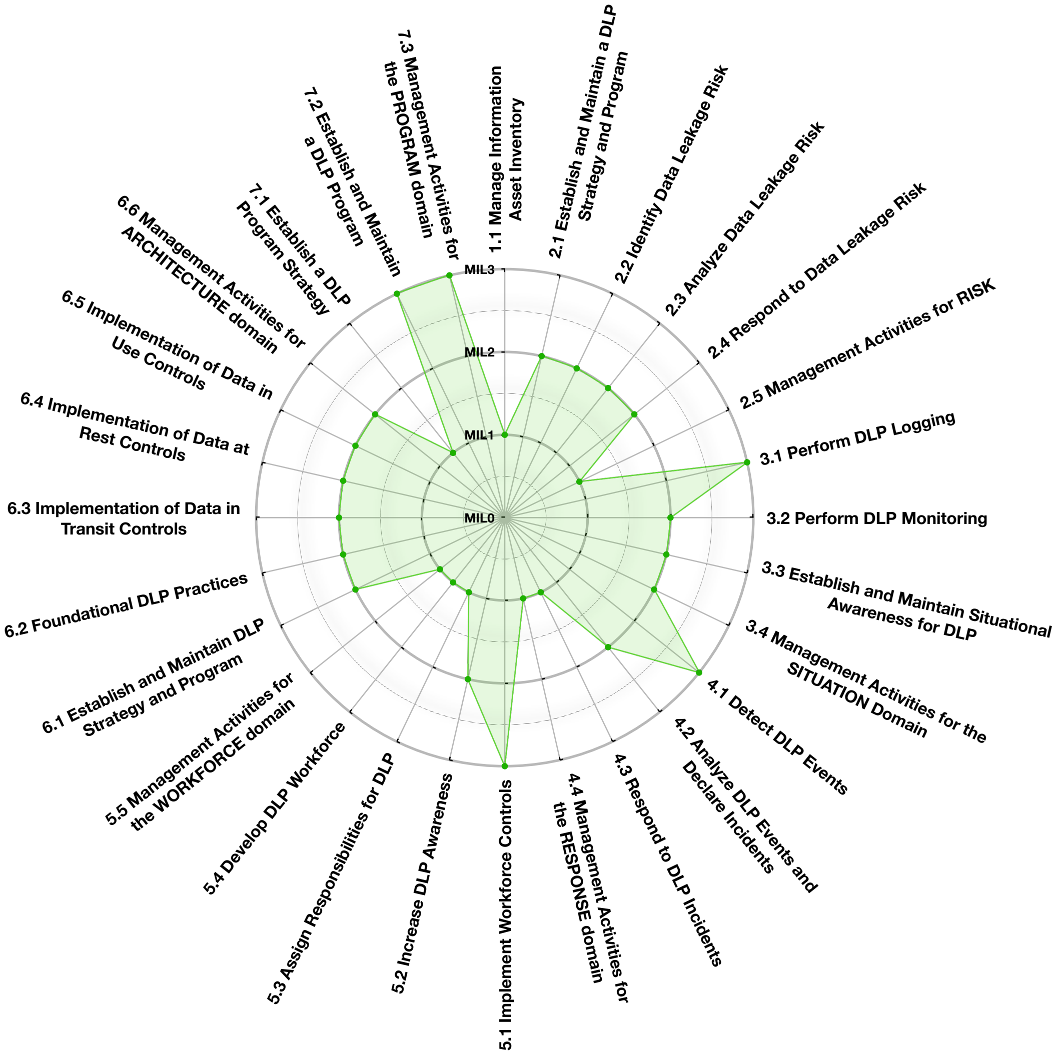


Figure 5. Summary of the self-evaluation's outcome per objective.

3.1.2. Synthesizing Outcomes across Domains

The detailed outcomes of our use case are visually presented in a management dashboard in Figure 6. This illustration provides an in-depth view of the results obtained from applying all domains from the DLP Maturity Model in our specific scenario.

3.2. Analyze Results

After self-evaluation, the organization will thoroughly analyze the results to pinpoint significant gaps in its DLP practices, adopting a risk-based approach. A detailed fulfillment of each objective might lead to an overload of information on a top-management level, so a management summary like the one provided in Figure 5 will suffice, providing a concise overview of the key findings.

It is crucial to acknowledge that attaining the highest level of maturity, MIL3—Fully Implemented, is not always necessary or optimal for every organization. Due to the fact that the necessity of reaching MIL3 should be carefully weighed against the potential risks and the specific context, the organization should tailor its DLP maturity goals to align with its own risk appetite and business objectives. This leads to the formation of a target profile, which represents the desired capability level across the various domains, ensuring a balanced and effective approach to DLP that is customized to the organization's specific needs and circumstances.

3.3. Prioritize, Plan, and Implement

After analyzing the result, the organization must undertake the crucial steps of prioritizing, planning, and implementing actions to achieve the desired maturity levels. This process begins with prioritizing actions based on several factors: the impact of the identified gaps on business objectives, the relevance of supported business functions, the costs associated with implementing necessary practices, and the availability of resources. This prioritization process should be guided by both the organization's immediate needs and its long-term strategic goals, ensuring that efforts are directed towards areas of greatest impact and value.

Upon formulating these plans, the next critical phase is their implementation. This phase demands focused efforts to operationalize the strategies laid out in the plans. Implementation might involve deploying new technologies, revising policies, conducting training programs, or other actions as dictated by the plan.

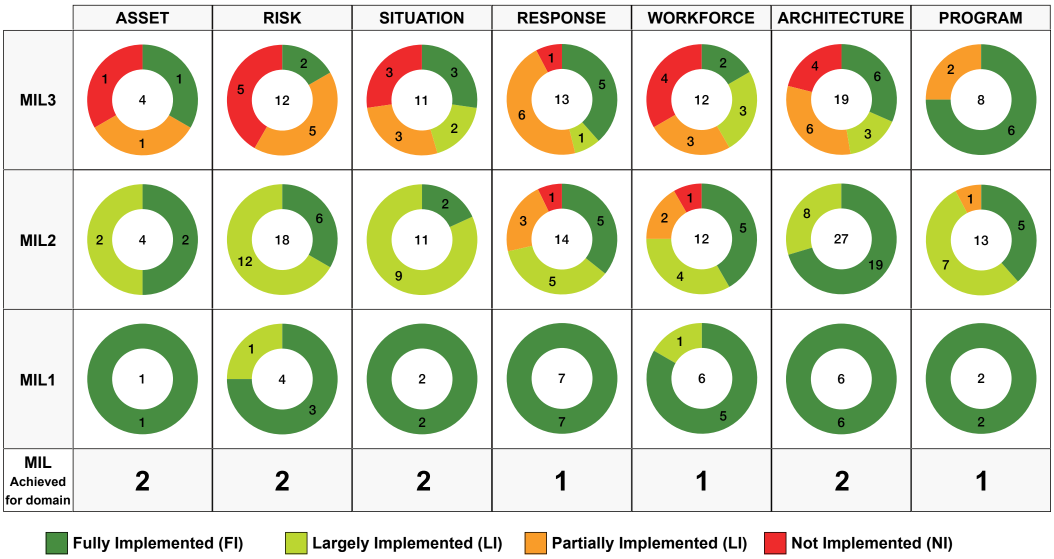


Figure 6. Detailed outcomes as a management dashboard after the self-evaluation on the domain level, inspired by the HTML-based Self-Evaluation Tool [53].

3.4. Continuous Improvement

Regular reviews and reevaluations are an integral part for continuous improvement. These periodic assessments ensure that the organization's DLP practices are not only aligned with the current business, technology, and threat landscapes but also adaptable to their evolution over time. By continuously monitoring the effectiveness of implemented practices and being responsive to changing circumstances, organizations can maintain a robust and effective DLP posture that consistently aligns with their evolving business objectives and risk profiles.

4. Discussion

4.1. Limitations

This paper acknowledges certain limitations inherent in the field of DLP. Firstly, the challenge of evidence-based security in cybersecurity [54], particularly in practical contexts, is notable. DLP frameworks and organizational strategies, typically shrouded in confidentiality, pose a barrier to developing an evidence-based approach. This lack of transparent evidence may hinder the continuous evolution and validation of DLP practices. Secondly, while the DLP Maturity Model addresses a broad spectrum of potential threats, it may not fully encompass data leakage by highly-obfuscated cyberattacks, like [55–57].

Such sophisticated threats require a level of detection and response beyond the scope of most existing DLP solutions and might also be seen as part of SIEM or advanced anti-virus tools. This limitation suggests the need for ongoing refinement of DLP strategies to adapt to evolving and increasingly concealed cyber threats.

4.2. Further Work

Our meticulous analysis and adaptation of the C2M2 have culminated in the development of a structured approach to evaluate and enhance DLP practices across various organizational contexts. It has been demonstrated that an effective utilization of C2M2 is not only possible but also beneficial in creating a more robust DLP framework. The DLP Maturity Model's effectiveness in providing a clear, gradational assessment from initial to advanced DLP practices aligns with our research question regarding the added value of a tailored C2M2 framework in DLP. Our findings confirm that the DLP Maturity Model, built upon the adapted C2M2 framework, significantly contributes to the realm of DLP by offering a comprehensive pathway for organizations to evolve from initial, ad hoc efforts to a mature, policy-driven level of data protection. In practice, the application of this model within a banking context has underscored its utility in safeguarding sensitive data and ensuring compliance with regulatory standards. The model serves as both a current assessment tool and a guide for future enhancements in DLP practices, indicating its potential to shape organizational strategies towards a more aligned approach with broader business objectives and risk appetites.

Looking ahead, this model lays the groundwork for future research and development in DLP strategies, particularly in aligning them with evolving business needs and cybersecurity landscapes. Establishing a DLP target profile that reflects an organization's preferred capability level across multiple cybersecurity domains is a key step towards a more secure digital future.

Author Contributions: Conceptualization, J.D. and A.H.; methodology, J.D. and A.H.; investigation, J.D.; resources, J.D.; draft preparation, J.D.; writing—review and editing, A.H.; visualization, J.D.; supervision, A.H.; project administration, J.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

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

Abbreviations

The following abbreviations are used in this manuscript:

C2M2	Cybersecurity Capability Maturity Model
DORA	Digital Operational Resilience Act
DLP	Data Leakage Prevention
EBA	European Banking Authority
FI	Fully Implemented
ICT	Information and Communications Technology
LI	Largely Implemented
LLM	Large Language Model
MIL	Maturity Indicator Level
NI	Not Implemented
NIST	National Institute of Standards and Technology
PI	Partially Implemented
SIEM	Security Incident and Event Management
SOC	Security Operation Center

Appendix A

Appendix A.1. C2M2

Appendix A.1.1. Domain 1: Asset, Change, and Configuration Management (ASSET)

Table A1. Objective 1.1: Manage Information Asset Inventory.

MIL		Description
MIL1	a	Information assets that contain sensitive information are inventoried, at least in an ad hoc manner.
MIL2	b	The inventory encompasses information assets that may be susceptible to unauthorized access and compromise in incidents of data breaches.
	c	Each information asset is classified based on its sensitivity. There is a documented classification scheme in place.
	d	The criteria for categorization take into account the extent to which an asset could potentially be utilized to facilitate a data leakage incident.
	e	Information assets are sanitized or destroyed as per policies at end of life.
MIL3	f	The information asset inventory includes attributes that support DLP (e.g., asset category, backup locations, storage locations, asset owner, etc.).
	g	The information asset inventory is complete.
	h	The information asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes.

Appendix A.1.2. Domain 2: Risk Management (RISK)

Table A2. Objective 2.1: Establish and Maintain a DLP Strategy and Program.

MIL		Description
MIL1	a	The organization has a strategy for DLP, potentially managed in an ad hoc manner.
MIL2	b	A data leakage prevention strategy is established and aligned with the organization's cybersecurity strategy.
	c	The DLP strategy is maintained to perform activities according to the cyber risk management strategy.
	d	Information related to data leakage risks is communicated to relevant stakeholders.
	e	Governance for the DLP strategy is established and maintained.
	f	Senior management demonstrates visible and active sponsorship for the DLP strategy.
MIL3	g	The DLP strategy aligns with the organization's mission and objectives.
	h	The DLP strategy is coordinated with the organization's wider risk management efforts.

Table A3. Objective 2.2: Identify Data Leakage Risk.

MIL		Description
MIL1	a	Data leakage risks are identified, at least in an ad hoc manner.
MIL2	b	A defined method is used to identify data leakage risks.
	c	Stakeholders from appropriate operations and business areas participate in the identification of data leakage risks.
	d	Risks regarding data leakage are documented in a risk register or other artifact.
	e	Data leakage risks are assigned to risk owners.
	f	Risk identification activities are performed periodically and according to defined triggers, such as system changes, new projects, or external events.
MIL3	g	Risk identification activities prioritize sensitive data, as identified in the ASSET domain.
	h	Information pertaining to non-compliance, especially in systems that do not adhere to policies related to the handling of sensitive information, is utilized.

Table A4. Objective 2.3: Analyze Data Leakage Risk.

MIL		Description
MIL1	a	Data leakage risks are prioritized based on estimated impact, at least in an ad hoc manner.
MIL2	b	Defined criteria are used to prioritize data leakage risks (e.g., organizational impact, likelihood, risk appetite).
	c	A method is used to estimate impact for high data leakage risks.
	d	Defined methods are used to analyze potentially high data leakage risks.
	e	Stakeholders from relevant operations and business functions participate in the analysis of data leakage risks.
	f	Data leakage risks are removed from the risk register when no longer requiring tracking or response.
MIL3	g	Analyses of data leakage risks are updated periodically and in response to defined triggers, such as system changes, new projects, or external events.

Table A5. Objective 2.4: Respond to Data Leakage Risk.

MIL		Description
MIL1	a	Responses (such as mitigate, accept, avoid, transfer) are implemented to address data leakage risks, at least in an ad hoc manner.
MIL2	b	A method is used to select and implement responses to data leakage risks based on analysis and prioritization.
MIL3	c	DLP controls are evaluated to ensure they are effective in mitigating identified risks.
	d	KPIs from DLP activities are regularly reviewed by the leadership of the organization.
	e	Responses to data leakage risks (such as mitigate, accept, avoid, transfer) are periodically reviewed by leadership to determine whether they are still appropriate.

Table A6. Objective 2.5: Management Activities for RISK Domain.

MIL		Description
MIL1	a	No practice at MIL1.
MIL2	b	Documented procedures for activities are established and maintained.
	c	Adequate resources are allocated for activities.
MIL3	d	Policies or directives define requirements for activities.
	e	Responsibility and accountability for activities are clearly assigned.
	f	Personnel involved in DLP-related risk management possess necessary skills and knowledge.
	g	The effectiveness of activities is regularly evaluated and tracked.

Appendix A.1.3. Domain 3: Situational Awareness (SITUATION)

Table A7. Objective 3.1: Perform DLP Logging.

MIL		Description
MIL1	a	Logging occurs for sensitive data, at least in an ad hoc manner.
MIL2	b	Logging is implemented for assets that contain sensitive data.
	c	Logging requirements are established.
	d	Logging requirements are set for network and host monitoring (e.g., web proxies, e-mail gateways, print-monitoring on endpoint clients).
	e	Log data are aggregated and accessible for DLP analysts.
MIL3	f	Logging is enforced for assets with higher data leakage risk priorities (e.g., for data at rest and data in use).

Table A8. Objective 3.2: Perform DLP Monitoring.

MIL		Description
MIL1	a	Log data or alerts from the monitoring infrastructure are reviewed, at least in an ad hoc manner.
MIL2	b	Requirements for DLP monitoring are established and maintained.
	c	Enhanced rule sets are configured to trigger alerts when a potential data leakage attempt is discovered.
	d	Monitoring activities are aligned with the organization's risk-based security approach.
MIL3	e	Enhanced monitoring is enforced for assets with higher data leakage risk priorities.
	f	The DLP rule set undergoes periodic evaluation and updates, integrating insights from incident responses and false-positive alert assessments.
	g	Adjustments to the DLP rule set can be executed on short notice if required.

Table A9. Objective 3.3: Establish and Maintain Situational Awareness for DLP.

MIL		Description
MIL1		No practice at MIL1.
MIL2	a	Methods for communicating the current state of DLP are established and maintained.
	b	KPIs relevant to DLP are collected for operational state awareness.
MIL3	c	KPIs and thresholds for the rule sets are established and harmonized with leadership and stakeholder requirements.
	d	Internal data crucial for DLP activities (e.g., employee terminations) are methodically collected and processed, leading to (ad hoc) modifications in the rule set as necessary.
	e	Predefined operational states, such as Triage and Incident Escalation, are meticulously documented and activated in response to incoming alerts.

Table A10. Objective 3.4: Management of Activities in the SITUATION Domain.

MIL		Description
MIL1		No practice at MIL1.
MIL2	a	Documented procedures are established, followed, and maintained for activities in the SITUATION domain.
	b	Adequate resources (people, funding, and tools) are provided to support activities from the SITUATION domain.
MIL3	c	Up-to-date policies define requirements for activities from the SITUATION domain.
	d	Responsibility, accountability, and authority for the performance of activities in the SITUATION domain are assigned to personnel.
	e	Personnel performing activities in the SITUATION domain have skills and knowledge needed to perform their assigned responsibilities.
	f	The effectiveness of activities in the SITUATION domain is regularly evaluated and tracked.

Appendix A.1.4. Event and Incident Response, Continuity of Operations (RESPONSE)

Table A11. Objective 4.1: Detect DLP Events.

MIL		Description
MIL1	a	Detected DLP events are reported to a specified person or role and documented, at least in an ad hoc manner.
	b	Employees can report DLP events, at least in an ad hoc manner.
MIL2	c	Criteria are established to define and classify DLP events.
	d	Employees can report DLP events through predefined and communicated rules and procedures.
MIL3	e	Event information can be correlated to support incident analysis by identifying patterns and trends.
	f	DLP activities are adjusted based on identified risks and the organization's DLP threat profile.
	g	Handling of events is documented.

Table A12. Objective 4.2: Analyze DLP Events and Declare Incidents.

MIL		Description
MIL1	a	Criteria for declaring DLP incidents are established, at least in an ad hoc manner.
	b	DLP events are analyzed to support the declaration of DLP incidents, at least in an ad hoc manner.
MIL2	c	DLP incidents are classified and prioritized by an initial (and ongoing) impact assessment.
	d	DLP events undergo triage and are subsequently classified as incidents based on predetermined criteria.
	e	DLP incident declaration criteria are updated periodically and according to defined triggers, such as organizational changes, lessons learned, or newly identified threats.
	f	DLP events and incidents are systematically tracked and documented before being closed.
	g	Stakeholders are notified of DLP incidents based on predefined procedures.
MIL3	h	Criteria for the impact assessment of DLP incidents is aligned with DLP risk prioritization.
	i	DLP incidents are correlated to identify patterns and trends across incidents.

Table A13. Objective 4.3: Respond to DLP Incidents.

MIL		Description
MIL1	a	DLP incident response personnel are identified, and roles are assigned, at least in an ad hoc manner.
	b	Responses to DLP incidents are executed to limit impact and restore normal operations, at least in an ad hoc manner.
	c	Reporting of DLP incidents is performed, as appropriate, in an ad hoc manner.
MIL2	d	DLP incident response plans that address all incident life cycle phases are established and maintained.
	e	DLP incident response is executed according to defined plans and procedures.
	f	DLP incident response plans include a communications plan for stakeholders.
	g	DLP incident response plan exercises are conducted periodically.
	h	Lessons-learned activities from DLP incidents are performed, leading to corrective actions.
MIL3	i	Root-cause analysis of DLP incidents is performed, with corrective actions taken.
	j	DLP incident responses are coordinated with internal or external entities, supporting evidence collection and preservation.
	k	DLP personnel engage in continuous dialogue with vendors and DLP analysts from other organizations to identify emerging trends and new technologies promptly.
	l	DLP incident responses leverage and trigger predefined operational states.

Table A14. Objective 4.4: Management of Activities for the RESPONSE Domain.

MIL		Description
MIL1		No practice at MIL1.
MIL2	a	Documented procedures for response activities are established, followed, and maintained.
	b	Adequate resources are allocated to support activities from the RESPONSE domain.
MIL3	c	Up-to-date policies define requirements for activities from the RESPONSE domain.
	d	Responsibility and accountability for activities in the RESPONSE domain are clearly assigned.
	e	Personnel performing activities in the RESPONSE domain have skills and knowledge needed to perform their assigned responsibilities.
	f	The effectiveness of activities is regularly evaluated and tracked.

Appendix A.1.5. WORKFORCE

Table A15. Objective 5.1: Implement Workforce Controls.

MIL		Description
MIL1	a	Personnel identification is performed at hire.
MIL2	b	Personnel vetting is performed for positions with access to sensitive data.
	c	Disciplinary actions for non-compliance with DLP related policies are carried out in an ad hoc manner.
	d	Personnel are made aware of their responsibilities for protecting and using information assets.
MIL3	e	A formal accountability process, including disciplinary actions, is implemented for non-compliance with DLP related policies.

Table A16. Objective 5.2: Increase DLP Awareness.

MIL		Description
MIL1	a	Cybersecurity awareness activities incorporate DLP topics in an ad hoc manner.
MIL2	b	Cybersecurity awareness objectives, encompassing DLP topics, are established and maintained.
	c	Cybersecurity awareness objectives are aligned with the DLP threat landscape.
	d	Cybersecurity awareness activities, incorporating DLP, are conducted periodically.
MIL3	e	Cybersecurity awareness activities are customized to different job roles, with particular emphasis on DLP-related topics.
	f	Cybersecurity awareness activities specifically address DLP procedures pertinent to stakeholders, such as incident reporting and handling.
	g	The effectiveness of DLP-focused cybersecurity awareness activities is evaluated periodically, with improvements made as appropriate.

Table A17. Objective 5.3: Assign Responsibilities for DLP.

MIL		Description
MIL1	a	Cybersecurity responsibilities for DLP are identified, at least in an ad hoc manner.
	b	Cybersecurity responsibilities for DLP are assigned to specific people, at least in an ad hoc manner.
MIL2	c	Cybersecurity responsibilities for DLP are assigned to specific roles, including external service providers.
	d	Cybersecurity responsibilities for DLP are documented.
MIL3	e	Cybersecurity responsibilities and job requirements for DLP are reviewed and updated periodically based on system changes and organizational structure shifts.
	f	Assigned responsibilities for DLP are managed to ensure adequacy and redundancy of coverage, including succession planning.

Table A18. Objective 5.4: Develop DLP Workforce.

MIL		Description
MIL1	a	DLP-related content is available to personnel working with sensitive data, at least in an ad hoc manner.
	b	Gaps for DLP-related topics are identified, at least in an ad hoc manner.
MIL2	c	Gaps for DLP-related topics are addressed through training.
	d	Training for DLP-related topics is mandatory before granting access to critical information assets.
MIL3	e	The effectiveness of DLP-related training programs is evaluated periodically, with improvements made as appropriate.
	f	DLP-related training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities.

Table A19. Objective 5.5: Management of Activities for the WORKFORCE Domain.

MIL		Description
MIL1		No practice at MIL1.
MIL2	a	Documented procedures for activities within the WORKFORCE domain are established and maintained.
	b	Adequate resources are allocated to support activities in the WORKFORCE domain.
MIL3	c	Updated policies define requirements for activities within the WORKFORCE domain.
	d	Responsibility and accountability for activities in the WORKFORCE domain are clearly assigned.
	e	Personnel involved within the WORKFORCE domain possess the necessary skills and knowledge.
	f	The effectiveness of activities in the WORKFORCE domain is regularly evaluated and tracked.

Appendix A.1.6. Cybersecurity Architecture (ARCHITECTURE)

Table A20. Objective 6.1: Establish and Maintain DLP Strategy and Program.

MIL		Description
MIL1	a	The organization has a DLP strategy, potentially developed and managed in an ad hoc manner.
MIL2	b	A DLP strategy is established and maintained in alignment with the organization's cybersecurity and enterprise architecture strategies.
	c	DLP processes and infrastructure are implemented, aligning with the classification of information assets.
	d	Governance for DLP is established, including periodic reviews and an exceptions process.
	e	Visible and active senior management sponsorship for the DLP processes and infrastructure.
	f	Requirements for the organization's assets are established and maintained within the DLP processes and infrastructure.
	g	Controls for DLP are selected and implemented to meet these requirements.
MIL3	h	The DLP strategy is coherently aligned with the organization's overarching cybersecurity strategy.
	i	Conformance of the DLP controls to established DLP requirements is periodically assessed.
	j	DLP processes and infrastructure are guided by the organization's risk analysis and threat profile.

Table A21. Objective 6.2: Foundational DLP Practices.

MIL		Description
MIL1	a	No practice at MIL1.
MIL2	b	Prioritization of data leakage events, with processing based on assigned priority levels.
	c	Technical enforcement of DLP-related policies.
	d	Regular identification and mitigation of DLP-related vulnerabilities.
MIL3	e	Utilization of optical character recognition (OCR) to prevent leaks via screenshots or photographs containing sensitive data.
	f	Proactive blocking of suspicious data leakage events.
	g	Round-the-clock technical support for resolving false positives in event blocking.

Table A22. Objective 6.3: Implementation of Data in Transit Controls.

MIL		Description
MIL1	a	Implementation of basic DLP monitoring.
	b	Activation of denylisting protocols.
	c	Policy prohibition of unsecured file transfers.
MIL2	d	Monitoring of all inbound and outbound file transfers, including web uploads and email.
	e	Technical restriction or monitoring of USB ports for file storage.
	f	Technical restriction or monitoring of print systems.
	g	Requirement of risk exceptions for unmonitored data exchange methods.
	h	Technical prevention of unsecured file transfers.
	i	Application of network segmentation strategies to mitigate data breach impacts.
MIL3	j	Assurance of end-to-end encryption for sensitive data transfers.
	k	Implementation of active allowlisting.
	l	Comprehensive tracking of large file transfers, including complete workflow documentation and senior management authorization.

Table A23. Objective 6.4: Implementation of Data at Rest Controls.

MIL		Description
MIL1	a	No practices at MIL1.
MIL2	b	Active use of present data classification by DLP tools to categorize files.
	c	DLP tools enabled to scan across network shares, file servers, and user endpoints.
	d	Ability of DLP tools to scan files within cloud infrastructures.
	e	Implementation of data encryption to protect confidentiality of sensitive data and identification of unencrypted sensitive data.
	f	Enhancement of access controls to limit data access to authorized individuals.
MIL3	g	Regular execution of DAR scans.
	h	Systematic evaluation of DAR scan results, with assignment and tracking of findings and escalation as needed.
	i	Periodic audits of access logs to detect unusual or unauthorized data access.

Table A24. Objective 6.5: Implementation of Data in Use Controls.

MIL		Description
MIL1	a	Logging of alarms during attempts of privilege escalation.
	b	Application of mobile device management (MDM) for device oversight.
MIL2	c	Automatic notification to users when policy breaches are detected, issuing violation warnings.
	d	Monitoring of files written to shares.
	e	Triggering alarms and analysis for attempted privilege escalations.
	f	Refinement of MDM to provide detailed control over app permissions and data access, especially in BYOD scenarios.
	g	Utilization of data masking in environments where sensitive data are accessed, to prevent unintentional exposure.
MIL3	h	Observation of user interactions with data.
	i	Employment of user and entity behavior analytics (UEBA) for monitoring and analyzing anomalies in user data interactions.
	j	Implementation of measures to prevent physical data leakage, including controls to inhibit the taking of photos of sensitive information, such as the use of safe rooms or strict no-phone policies.

Table A25. Objective 6.6: Management of Activities for DLP in the ARCHITECTURE Domain.

MIL		Description
MIL1		No practice at MIL1.
MIL2	a	Documented procedures for activities within the ARCHITECTURE domain are established and maintained.
	b	Adequate resources are allocated to support activities in the ARCHITECTURE domain.
MIL3	c	Updated policies define requirements for activities within the ARCHITECTURE domain.
	d	Responsibility and accountability for activities in the ARCHITECTURE domain are clearly assigned.
	e	Personnel involved within the ARCHITECTURE domain possess the necessary skills and knowledge.
	f	The effectiveness of activities in the ARCHITECTURE domain is regularly evaluated and tracked.

Appendix A.1.7. Cybersecurity Program Management (PROGRAM)

Table A26. Objective 7.1: Establish a DLP Program Strategy.

MIL		Description
MIL1	a	The organization has a DLP program, potentially developed and managed in an ad hoc manner.
MIL2	b	The DLP program strategy defines goals and objectives for the organization's DLP activities.
	c	The DLP program strategy is documented and aligned with the organization's mission, strategic objectives, and risk profile for sensitive data.
	d	The DLP program strategy delineates the organization's approach to the oversight and governance of DLP activities.
	e	The DLP program strategy defines the structure and organization of the DLP program.
	f	The DLP program strategy identifies standards and guidelines relevant to DLP activities.
	g	The DLP program strategy addresses compliance requirements pertinent to DLP.
MIL3	h	The DLP program strategy is periodically revised in response to changes in business dynamics, shifts in the operating environment, and evolving threat landscapes.

Table A27. Objective 7.2: Establish and Maintain a DLP program.

MIL		Description
MIL1	a	Senior management provides support for the DLP program, potentially in an ad hoc manner.
MIL2	b	The DLP program is developed in line with the overarching cybersecurity strategy.
	c	Senior management sponsorship for the DLP program is evident and proactive.
	d	Senior management endorses the development, maintenance, and enforcement of the DLP program.
	e	A designated role with sufficient authority is responsible for the DLP program.
	f	Key stakeholders are identified and involved in the DLP program.
MIL3	g	DLP program activities are regularly reviewed for alignment with the cybersecurity program strategy.
	h	DLP activities undergo independent evaluations to ensure adherence to cybersecurity policies and procedures.
	i	The DLP program addresses and supports compliance with legal and regulatory requirements, as appropriate.

Table A28. Objective 7.3: Management of Activities for the PROGRAM Domain.

MIL		Description
MIL1		No practice at MIL1.
MIL2	a	Documented procedures for activities within the PROGRAM domain are established and maintained.
	b	Adequate resources are allocated to support activities in the PROGRAM domain.
MIL3	c	Updated policies define requirements for activities within the PROGRAM domain.
	d	Responsibility and accountability for activities in the PROGRAM domain are clearly assigned.
	e	Personnel involved within the PROGRAM domain possess the necessary skills and knowledge.
	f	The effectiveness of DLP activities in the PROGRAM domain is regularly evaluated and tracked.

References

1. Alneyadi, S.; Sithirasenan, E.; Muthukkumarasamy, V. A Survey on Data Leakage Prevention Systems. *J. Netw. Comput. Appl.* **2016**, *62*, 137–152. [CrossRef]
2. Stiennon, R. McAfee Acquires Onigma | ZDNET. 2006. Available online: https://www.zdnet.com/article/mcafee-acquires-onigma/ (accessed on 1 February 2024).
3. Wilkens, A. McAfee Kauft Safeboot für 350 Millionen US-Dollar. 2007. Available online: https://www.heise.de/news/McAfee-kauft-Safeboot-fuer-350-Millionen-US-Dollar-183016.html (accessed on 1 February 2024).
4. Check Point Software Technologies Ltd. *Report of Foreign Private Issuer*; Check Point Software Technologies Ltd.: Tel Aviv-Yafo, Israel, 2007.
5. Wilson, T. Symantec Seals $350M Acquisition of Vontu. 2007. Available online: https://www.darkreading.com/cybersecurity-analytics/symantec-seals-350m-acquisition-of-vontu (accessed on 1 February 2024).
6. RSA the Security Division of EMC to Acquire Tablus Further Advancing Information Security Leadership. 2007. Available online: https://www.dell.com/en-us/dt/corporate/newsroom/announcements/2007/08/08092007-5267.htm (accessed on 1 February 2024).
7. Dumitru, A. No More Data Leaks!—Fidelis Pounds Hackers. 2007. Available online: https://news.softpedia.com/news/No-More-Data-Leaks-63521.shtml (accessed on 1 February 2024).
8. European Banking Authority, EBA/GL/2019/04 - Guidelines Compliance Table *Report*, **2023**, Paris, FR, April 2023. Available online: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/896720/EBA%20GL%202019%2004%20-%20CT%20GLs%20on%20ICT%20and%20security%20risk%20management.pdf (accessed on 1 February 2024).
9. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Controls. ISO Central Secretary: Geneva, Switzerland, October 2022.
10. *ISO/IEC 27002:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Controls. ISO Central Secretary: Geneva, Switzerland, February 2022.
11. Consultation Paper on Draft Regulatory Technical Standards to Further Harmonise ICT Risk Management Tools, Methods, Processes and Policies as Mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554. Joint Committee of the European Supervisory: Paris, France, 13 June 2023. Available online: https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_RTSs_ICT_risk_management_tools_methods_processes_and_policies.pdf (accessed on 1 February 2024).
12. IBM Corporation. Cost of a Data Breach Report 2023. *Report*, Armonk, NY, USA, July 2023. Available online: https://www.ibm.com/reports/data-breach (accessed on 1 February 2024).
13. Vom Brocke, J.; Hevner, A.; Maedche, A. (Eds.) Introduction to Design Science Research. In *Design Science Research. Cases*; Springer International Publishing: Cham, Switzerland, 2020; pp. 1–13. [CrossRef]
14. Vom Brocke, J.; Maedche, A. The DSR Grid: Six Core Dimensions for Effectively Planning and Communicating Design Science Research Projects. *Electron. Mark.* **2019**, *29*, 379–385. [CrossRef]
15. Rabii, A.; Assoul, S.; Ouazzani Touhami, K.; Roudies, O. Information and Cyber Security Maturity Models: A Systematic Literature Review. *Inf. Comput. Secur.* **2020**, *28*, 627–644. [CrossRef]
16. European Central Bank. Number of Stand Alone Credit Institutions. 2024. Available online: https://data.ecb.europa.eu/data/datasets/CBD2/CBD2.Q.B0._Z.47._Z._Z.A.A.R0101._Z._Z._Z._Z.LE._Z.PN (accessed on 1 February 2024).
17. Alsuwaie, M.A.; Habibnia, B.; Gladyshev, P. Data Leakage Prevention Adoption Model & DLP Maturity Level Assessment. In Proceedings of the 2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC), Rome, Italy, 12–14 November 2021; pp. 396–405. [CrossRef]

18. Dempsey, K.L.; Chawla, N.S.; Johnson, L.A.; Johnston, R.; Jones, A.C.; Orebaugh, A.D.; Scholl, M.A.; Stine, K.M. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*; Technical Report NIST SP 800-137; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011. [CrossRef]
19. Ouellet, E.; McMillan, R. Magic Quadrant for Content-Aware Data Loss Prevention *Report of Foreign Private Issuer*; Gartner Inc.: Stamford, CT, USA, August 2011. Available online: https://www.gartner.com/en/documents/1764118 (accessed on 1 February 2024).
20. Broadcom. Symantec Data Loss Prevention—Drive Total Protection of your Sensitive Data. In *Report of Foreign Private Issuer*; Broadcom Inc.: San José, CA, USA, November 2023. Available online: https://docs.broadcom.com/doc/data-loss-prevention-family-en (accessed on 1 February 2024).
21. McAfee. McAfee Total Protection for Data Loss Prevention In *Report of Foreign Private Issuer*; McAffee, LLC.: Santa Clara, CA, USA, February 2019. Available online: https://www.trellix.com/enterprise/en-us/assets/solution-briefs/sb-total-protection-for-dlp.pdf (accessed on 1 February 2024).
22. Cheng, L.; Liu, F.; Yao, D.D. Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions. *WIREs Data Min. Knowl. Discov.* **2017**, *7*, e1211. [CrossRef]
23. Swain, D.; Pattnaik, P.K.; Gupta, P.K., Eds. *Machine Learning and Information Processing: Proceedings of ICMLIP 2019*; Advances in Intelligent Systems and Computing; Springer: Singapore, 2020; Volume 1101. [CrossRef]
24. Gafny, M.; Shabtai, A.; Rokach, L.; Elovici, Y. Detecting Data Misuse by Applying Context-Based Data Linkage. In Proceedings of the 2010 ACM Workshop on Insider Threats, Chicago, IL, USA, 8 October 2010; pp. 3–12. [CrossRef]
25. Rennie, J.D.M. An Application of Machine Learning to E-Mail Filtering. In Proceedings of the KDD-2000 Text Mining Workshop Boston, Boston, MA, USA, 20–23 August 2000.
26. Faiz, M.F.; Arshad, J.; Alazab, M.; Shalaginov, A. Predicting Likelihood of Legitimate Data Loss in Email DLP. *Future Gener. Comput. Syst.* **2020**, *110*, 744–757. [CrossRef]
27. Katz, G.; Elovici, Y.; Shapira, B. CoBAn: A Context Based Model for Data Leakage Prevention. *Inf. Sci.* **2014**, *262*, 137–158. [CrossRef]
28. Costante, E.; Fauri, D.; Etalle, S.; Den Hartog, J.; Zannone, N. A Hybrid Framework for Data Loss Prevention and Detection. In Proceedings of the 2016 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, 22–26 May 2016; pp. 324–333. [CrossRef]
29. Alneyadi, S.; Sithirasenan, E.; Muthukkumarasamy, V. Adaptable N-gram Classification Model for Data Leakage Prevention. In Proceedings of the 2013 7th International Conference on Signal Processing and Communication Systems (ICSPCS), Carrara, Australia, 16–18 December 2013.
30. Stouffer, K.; Zimmerman, T.; Tang, C.; Cichonski, J.; Pease, M.; Shah, N.; Downard, W. *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 3 Discrete-Based Manufacturing System Use Case*; Technical Report NIST IR 8183A-3; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019. [CrossRef]
31. Van der Klerj, R.; Wijn, R.; Hof, T. An Application and Empirical Test of the Capability Opportunity Motivation-Behaviour Model to Data Leakage Prevention in Financial Organizations. *Comput. Secur.* **2020**, *97*, 101970. [CrossRef]
32. Hauer, B. Data and Information Leakage Prevention Within the Scope of Information Security. *IEEE Access* **2015**, *3*, 2554–2565. [CrossRef]
33. Axelsson, S. The Base-Rate Fallacy and the Difficulty of Intrusion Detection. *ACM Trans. Inf. Syst. Secur.* **2000**, *3*, 20. [CrossRef]
34. Shabtai, A.; Elovici, Y.; Rokach, L. *A Survey of Data Leakage Detection and Prevention Solutions*; SpringerBriefs in Computer Science; Springer: Boston, MA, USA, 2012. [CrossRef]
35. Alneyadi, S.; Sithirasenan, E.; Muthukkumarasamy, V. Detecting Data Semantic: A Data Leakage Prevention Approach. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; pp. 910–917. [CrossRef]
36. Shvartzshnaider, Y.; Pavlinovic, Z.; Balashankar, A.; Wies, T.; Subramanian, L.; Nissenbaum, H.; Mittal, P. VACCINE: Using Contextual Integrity For Data Leakage Detection. In Proceedings of the WWW'19: The Web Conference, San Francisco, CA, USA, 13–17 May 2019; pp. 1702–1712. [CrossRef]
37. Awad, A.; Kadry, S.; Maddodi, G.; Gill, S.; Lee, B. Data Leakage Detection Using System Call Provenance. In Proceedings of the 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS), Ostrawva, Czech Republic, 7–9 September 2016; pp. 486–491. [CrossRef]
38. Shu, X.; Zhang, J.; Yao, D.D.; Feng, W. Fast Detection of Transformed Data Leaks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 528–542. [CrossRef]
39. Gomez-Hidalgo, J.M.; Martin-Abreu, J.M.; Nieves, J.; Santos, I.; Brezo, F.; Bringas, P.G. Data Leak Prevention through Named Entity Recognition. In Proceedings of the 2010 IEEE Second International Conference on Social Computing, Minneapolis, MN, USA, 20–22 August 2010; pp. 1129–1134. [CrossRef]
40. Heiding, F.; Schneier, B.; Vishwanath, A.; Bernstein, J. Devising and Detecting Phishing: Large Language Models vs. Smaller Human Models. *arXiv* **2023**, arXiv:2308.12287. http://arxiv.org/abs/2308.12287.
41. Webster, J.; Watson, R.T. Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Q.* **2002**, *26*, xiii–xxiii.
42. Cooper, H.M. Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews. *Knowl. Soc.* **1988**, *1*, 104–126. [CrossRef]
43. Levy, Y.; Ellis, T.J. A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Sci. Int. J. Emerg. Transdiscipl.* **2006**, *9*, 181–212. [CrossRef]

44. Wolfswinkel, J.; Furtmueller, E.; Wilderom, C. Using grounded theory as a method for rigorously reviewing literature. *Eur. J. Inf. Syst.* **2013**, *9*, 45–55. [CrossRef]
45. Watson, R.T.; Webster, J. Analysing the Past to Prepare for the Future: Writing a Literature Review a Roadmap for Release 2.0. *J. Decis. Syst.* **2020**, *29*, 129–147. [CrossRef]
46. Vom Brocke, J.; Simons, A.; Riemer, K.; Niehaves, B.; Plattfaut, R.; Cleven, A. Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. *Commun. Assoc. Inf. Syst.* **2015**, *37*, 9. [CrossRef]
47. Almuhammadi, S.; Alsaleh, M. Information Security Maturity Model for Nist Cyber Security Framework. In *Proceedings of the Computer Science & Information Technology (CS & IT)*; Academy & Industry Research Collaboration Center (AIRCC): Mogappair West, Chennai, Tamil Nadu, India, 2017; pp. 51–62. [CrossRef]
48. Le, N.T.; Hoang, D.B. Can Maturity Models Support Cyber Security? In Proceedings of the 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA, 9–11 December 2016; pp. 1–7. [CrossRef]
49. Rea-Guaman, A.M.; Sanchez-Garcia, I.D.; Feliu, T.S.; Calvo-Manzano, J.A. Maturity models in cybersecurity: A systematic review. In Proceedings of the 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon, Portugal, 21–24 June 2017; pp. 1–6. [CrossRef]
50. *ISO/IEC 21827:2008*; Information technology Security techniques—Systems Security Engineering Capability Maturity Model (SSE-CMM). ISO Central Secretary: Geneva, Switzerland, October 2008.
51. Miloslavskaya, N.; Tolstaya, S. Information Security Management Maturity Models. *Procedia Comput. Sci.* **2022**, *213*, 49–57. [CrossRef]
52. Wlosinski, L.G. Data Loss Prevention—Next Steps. In *Issuer*; ISACA: Schaumburg, IL, USA, 2018. Available online: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2018/volume-1/data-loss-prevention-next-steps_joa_eng_0218 (accessed on 1 February 2024).
53. US DOE: Cybersecurity, Energy Security, and Emergency Response. C2M2 HTML-Based Tool. 2023. Available online: https://c2m2.doe.gov/c2m2-assessment (accessed on 1 February 2024).
54. Böck, H. In Search of Evidence-Based IT-Security, 2016. In 33C3 (33rd Chaos Communication Congress), 27–30 December 2016. Available online: https://media.ccc.de/v/33c3-8169-in_search_of_evidence-based_it-security (accessed on 1 February 2024).
55. Guri, M.; Hasson, O.; Kedma, G.; Elovici, Y. An Optical Covert-Channel to Leak Data through an Air-Gap. In Proceedings of the 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016; pp. 642–649. [CrossRef]
56. Guri, M.; Zadov, B.; Elovici, Y. LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED. In *Detection of Intrusions and Malware, and Vulnerability Assessment*; Polychronakis, M., Meier, M., Eds.; Springer International Publishing: Cham, Switzerland, 2017; Volume 10327, pp. 161–184. [CrossRef]
57. Guri, M.; Zadov, B.; Bykhovsky, D.; Elovici, Y. CTRL-ALT-LED: Leaking Data from Air-Gapped Computers via Keyboard LEDs. In Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), 15–19 July 2019; Volume 1, pp. 801–810. [CrossRef]

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.