Volume XXII, Issue (1) (2026) 79-85

International May Conference on Strategic Management

DOI: 10.5937/IMCSM26079B *Original Research*

INTEGRATION OF INFORMATION MANAGEMENT AND CYBERSECURITY AT THE GOVERNANCE LEVEL THE ILGM CONCEPTUAL MODEL BASED ON THE INFORMATION LIFECYCLE (7RS)

Ghenadie Belinschi *

Academy of Economic Studies of Moldova, Doctoral School, Doctoral Programme 521.03 Economics and Management (Business and Professional Practice), Republic of Moldova

Abstract: Information and data constitute an independent managerial resource in the digital economy, while cyber incidents affect the IT environment, financial performance, reputation, and organizations' ability to meet their obligations. In practice, information management (governing data flows, data quality, and information lifecycle processes) and cybersecurity (ensuring confidentiality, integrity, and availability) often evolve separately. This separation creates "silos" of responsibility and reduces the controllability of digitalization. This paper proposes a conceptual governance model that integrates information management and cybersecurity into a single management framework for the value of information and its associated risks. The model is grounded in the information lifecycle "7Rs" (reading, recognition, reinterpretation, reviewing, release, restructuring, retrieval). An ILGM (Information Lifecycle Governance Matrix) is constructed for each lifecycle stage using the following structure: "information task – typical cyber risks (C/I/A) – managerial controls – responsibility." The paper demonstrates how the matrix can be applied as an instrument for building a risk-oriented governance system and how it can be linked to the risk register and an "information system passport." The model provides a basis for subsequent quantitative research on effectiveness (SV/ROSI) and on innovation dynamics (I–E–T).

Keywords: Information management, cybersecurity, information lifecycle, ROSI, risk management.

1. INTRODUCTION

The rise of digitalization has led to a situation in which the quality of managerial decision-making is increasingly identified with the quality of information flows, information systems, and data-handling policies and procedures. At the same time, cybersecurity has

* *Corresponding author*: ghenadie.belinschi@ase.md

Ghenadie Belinschi, ORCID: 0009-0009-3361-9890

evolved from a supporting IT function into a systemic resilience factor: incidents can disrupt business continuity, generate direct financial losses, and entail legal consequences. A distinctive feature of security investments is the probabilistic nature of their effect—protective measures "pay off" primarily by reducing expected losses rather than by delivering a guaranteed increase in revenue (Beissel, 2016, pp. 109–110).

In the European context, the regulatory environment increases the burden on governance. Requirements for data processing and protection (e.g., the GDPR), together with obligations for cyber-risk management and operational resilience (e.g., NIS2 and DORA), increasingly compel organizations to formalize policies, processes, and roles, and to implement demonstrable control practices (Regulation (EU) 2016/679; Regulation (EU) 2022/2554; Regulation (EU) 2022/2555). Taken together, these conditions underscore the critical importance of integrating data governance and cyber-risk management into a unified decision-making system.

The primary managerial challenge lies not only in selecting "technical protection measures" but in establishing a coordinated governance system—processes, roles, policies, and control mechanisms that integrate information management with cyber-risk management. The multifactorial nature of cyberspace and the interdependence of infrastructures mean that narrowly "local" or "national" approaches often result in fragmented practices and, consequently, increased systemic vulnerabilities (Munk, 2015, p. 150).

The purpose of this paper is to propose a conceptual model for integrating information management and cybersecurity at the governance level, grounded in the "7Rs" information lifecycle. The model is intended to structure responsibilities and controls across the information pathway—creation, use, storage, and reuse—and to establish a shared language for interaction among business, IT, and information security.

2. THEORETICAL FOUNDATIONS: INFORMATION MANAGEMENT AND CYBERSECURITY AS A SINGLE GOVERNANCE FRAMEWORK

In Organizing Knowledge, a useful distinction is drawn between three levels:

- information processing as the day-to-day activity of participants in the "knowledge economy";
- information management as managing information "on behalf of others" within an organization or community;
- knowledge management as a higher-level function aimed at transforming tacit knowledge into shared knowledge in pursuit of common goals (Rowley & Farrow, 2000, p. 34). This distinction helps separate the operational use of IT from the management layer in which access rules, information quality, and information value become central.

Rowley and Farrow define information management as the managerial activity of planning, organizing, directing, and controlling information in an "open" organization. They note that information management relies on information systems and IT, as well as managerial techniques (including information auditing and information mapping), to effectively manage information resources from internal and external sources in order to support decision-making and improve organizational performance (Rowley & Farrow, 2000, p. 35).

Cybersecurity, in contemporary managerial terms, focuses on preserving the core properties of information and information systems—confidentiality, integrity, and availability (CIA)—and on managing the risks of their compromise. Equally important is a clear distinction between risk and threat: risk management operates under uncertainty and emphasizes

preventive measures, whereas when a risk "mutates" into an actual threat, response and containment mechanisms are activated (Munk, 2015, pp. 93–95).

To describe cyber risk quantitatively, metrics are used that link probability and loss magnitude. In this framing, risk is expressed as the product of probability p and impact i ($r = i \cdot p$), while expected losses can be captured through the annualized loss expectancy (ALE): $ALE = i \cdot ARO$, where ARO is the annual rate of occurrence of a threat (Beissel, 2016, pp. 133–135). This logic is important for governance because it connects control measures to changes in probabilities and/or impacts, thereby providing a foundation for subsequent effectiveness metrics such as SV and ROSI.

Information management and cybersecurity can be treated as an interconnected system: the former is responsible for creating information and ensuring its usefulness as a managerial resource, while the latter is responsible for preserving its key properties under threat conditions. Integration at the governance level closes the gap between "data for the business" and "security controls" by shifting the discussion toward responsibility, risk, and managerial decision-making. This line of argument aligns with the recent evolution of framework standards: NIST CSF 2.0 places explicit emphasis on the governance function as a foundation for cyber-risk management across organizations of all types (NIST, 2024).

As the "skeleton" of integration, this paper adopts a process-cyclical view of information management—the "7Rs of information management" model. It emphasizes that information management involves both individual and organizational processes, and it describes the interaction between users and organizational mechanisms as many-to-many (Rowley & Farrow, 2000, pp. 31–33). This enables risks and controls to be linked to specific stages of information handling.

3. DATA AND METHODOLOGY

This paper is conceptual in nature and applies a literature-synthesis approach, structuring key concepts into a managerial model. The "7Rs" information lifecycle is used as the operational backbone, enabling risks and controls to be anchored to the stages of information creation, dissemination, use, and storage (Rowley & Farrow, 2000, pp. 31–33).

The output of the study is the ILGM matrix, which for each 7Rs stage specifies:

- the information task;
- typical cyber risks and scenarios in C/I/A terms;
- a set of governance controls (policies, processes, technical and organizational measures);
- responsibility, expressed through indicative roles (data/process owner, CIO/IT, CISO/information security, system owners).

The matrix is intended for both strategic and operational management: as a tool for aligning requirements for data and systems, as a basis for a risk register, and as an input for subsequent quantitative assessment of control effectiveness (via loss prevention and SV/ROSI metrics) (Beissel, 2016, pp. 96–97; 133–135).

4. PROPOSED MODEL: INFORMATION LIFECYCLE GOVERNANCE MATRIX (ILGM)

The ILGM links the 7Rs information lifecycle with typical cyber risks and managerial controls. The model logic is as follows: at each stage of information handling, specific management errors may arise (e.g., loss of context, data-quality errors, unauthorized dissemination, storage redundancy, and unavailability during recovery), which implies

corresponding risks of confidentiality, integrity, and/or availability (C/I/A) compromise. By placing controls at the relevant lifecycle stage, an organization reduces risk exposure and incident likelihood, thereby strengthening resilience (NIST, 2024; ISO/IEC 27001:2022).

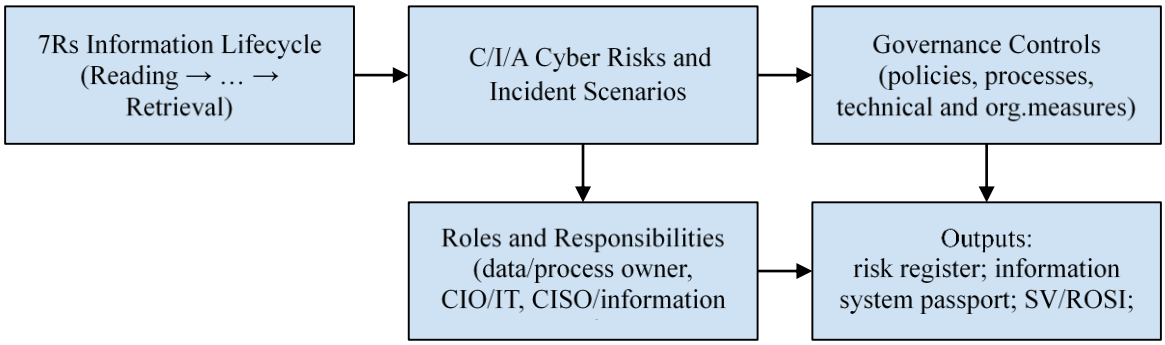


Figure 1. Conceptual Diagram of the ILGM as an Integration of the Information Lifecycle, Cyber Risks, and Governance Controls

The Table 1 presents the ILGM—a matrix that links the 7Rs stages to information tasks, typical cyber-risk scenarios, and a corresponding set of controls and responsibilities. The lifecycle stages follow the 7Rs model (Rowley & Farrow, 2000, pp. 31–33), and the grouping of control practices is aligned with the underlying logic of relevant standards and frameworks (NIST, 2024; ISO/IEC 27001:2022).

5. ILLUSTRATIVE APPLICATION: HOW TO USE ILGM IN AN ORGANIZATION

The ILGM can be used as a practical checklist for building the governance of digitalization. For example, when migrating documents and communications to cloud services, an organization faces heightened risks at the Release and Restructuring stages: leakage risk increases due to misconfigured access settings, compromised accounts, and errors in information exchange with external counterparties. The underlying logic that "access = security" is also reflected in information-management sources: access systems should be grounded in rights/permissions and supported by backup and recovery capabilities (Rowley & Farrow, 2000, p. 320)

The matrix makes it possible to define in advance which controls are mandatory (e.g., IAM/MFA, the principle of least privilege, DLP/encryption, access-rights audits, backups, and restore testing) and to assign responsibility for their implementation. From the economic logic of managerial decision-making, implementing a control is financially justified when the losses prevented (i.e., the reduction in expected loss) exceed the cost of the safeguards (Beissel, 2016, pp. 132–135).

In practice, ILGM should be linked to the risk register and to a structured description of the information system (an information system passport). The matrix specifies "what to control and at which stage," while the information system passport records "where, exactly, within the infrastructure and processes these stages are realized" (systems, data, integrations, owners). As a managerial practice, this linkage enables cyber risk to be operationalized—shifting it from a one-off assessment to a repeatable process with measurable indicators and feedback loops (Leirvik, 2023).

A high-level procedure for implementing ILGM in an organization includes:

- inventorying key information flows and systems (including cloud environments and external service providers);

- classifying data by criticality and requirements (confidentiality, integrity, availability, and regulatory constraints);
- populating the ILGM across the 7Rs stages for critical flows/systems (risks → controls → responsibilities);
- linking the identified risks and controls to the risk register and an action plan, and defining KRIs/KPIs for ongoing monitoring;
- periodically reviewing the matrix as technologies, threats, and external requirements evolve.

Table 1. ILGM: Information Lifecycle Governance Matrix (7Rs) in Relation to Cyber Risks (C/I/A)

Stage (7Rs)	Information task	Typical risks (C/I/A) and scenarios	Governance - controls and responsibility
Reading (reading/consumption)	Formation of information needs, access to sources, training	C: Leak when accessing external sources; I: use of unreliable data; A: uunavailability of sources	Source policy; access management; training; basic verification rules. Roles: process owner + IT + information security
Recognition (recognition of the significant)	Filtering "noise", identifying critical data and signals	I: integrity loss due to misclassification; C: incorrect sensitivity labeling; A: overload of systems/people	Data classification; data catalog; criticality rules; data-quality KRIs/KPIs. Roles: data owner + data steward + information security.
Reinterpretation	Contextualization, analytics, transforming data into decision-relevant knowledge	I: distorted conclusions due to data errors; C: leakage via analytical dashboards/data marts; A: dependency on a single tool/provider	Data-quality controls; model/version control; access control in BI; logging. Roles: process owner + analytics/IT + information security.
Reviewing (review/validation)	Verification of quality and correctness; version control	I: introduction of errors into the "source of truth"; C: leakage during review; A: process disruption when controls fail	Data-quality assurance procedures; change management; two-stage review; four-eye principle. Roles: data owner + IT + internal control.
Release (publication/dissemination)	Exchange and dissemination within the organization and with counterparties	C: leakage and excessive disclosure; I: unauthorized changes; A: channel/email disruption; account compromise	IAM/MFA; least privilege; DLP; encryption; contractual SLAs; third-party oversight. Roles: data owner + information security + legal/compliance.
Restructuring (structuring/storage)	Metadata, classification, storage, retention, archiving	C: leakage from storage/cloud; I: corruption/duplication; A: ransom ware; backup failures	Storage and retention policy; backup/recovery; segmentation; configuration control; access audit. Roles: IT (operations) + information security
Retrieval (search and retrieval)	Search and retrieval for reuse and decision-making	A: inability to recover/search; I: retrieval of outdated versions; C: access by unauthorized users	Catalogs and indexing; version control; access control; recovery tests; monitoring. Roles: IT + data owner + information security

6. DISCUSSION AND LIMITATIONS

The main contribution of this paper is that the integration of information management and cybersecurity is framed not as a "renaming of functions," but as an operationalizable governance model anchored in the information lifecycle. This facilitates cross-functional alignment of decisions and reduces the risk of "silo" optimization—where security measures are introduced without understanding information flows, or where data practices evolve without due consideration of cyber risks (Rowley & Farrow, 2000; NIST, 2024).

A key limitation of this paper is its conceptual nature: the matrix requires empirical validation (organizational case studies and cross-industry comparisons) and subsequent quantification of its effects. Within the forthcoming dissertation research, further development is expected to include:

- Formalizing the "saved value of information" (SV) metric as avoided losses and applying it to ROSI, as proposed by Beissel and adapted by the author of the present study (Beissel, 2016, pp. 96–97; 133–135);
- Embedding SV/ROSI into a dynamic I–E–T model to analyze innovation effectiveness and transitions between technological stages.

It is also important to recognize that, even after controls are implemented, residual risk remains and must be monitored, with measures reviewed regularly as technologies and threats evolve (Beissel, 2016, pp. 109–110). The ILGM can serve as a mechanism for such review because it anchors control practices to specific stages of information handling and enables tracking of risk "shifts" as the information system or external context changes.

7. CONCLUSION

This paper proposes a conceptual governance model for integrating information management and cybersecurity based on the 7Rs information lifecycle. It develops the ILGM matrix, which links lifecycle stages to typical C/I/A risks, control practices, and assigned responsibilities. The model is intended to improve the manageability of digitalization and to establish a shared language for interaction among business, IT, and information security. Further research will focus on empirical validation of the matrix and quantitative assessment of the effects of controls and innovations (SV/ROSI) within the dynamics of technological change.

REFERENCES

Beissel, S. (2016). Economic Aspects. In: Beissel, S. Cybersecurity Investments: Decision Support Under Economic Aspects of Safeguards and Breaches (pp. 79–141). Springer (Progress in IS). https://doi.org/10.1007/978-3-319-30460-1_4.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).

ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. International Organization for Standardization.

Leirvik, R. (2023). Understand, Manage, and Measure Cyber Risk®: Practical Solutions for Creating a Sustainable Cyber Program. Apress. https://doi.org/10.1007/978-1-4842-9319-5.

Munk, T. H. (2015). Cyber-security in the European Region: Anticipatory Governance and Practices (Doctoral thesis). The University of Manchester.

NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, February 26, 2024. https://doi.org/10.6028/NIST.CSWP.29.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation - GDPR).

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA).

Rowley, J. E., & Farrow, J. (2000). Organizing Knowledge: An Introduction to Managing Access to Information (3rd ed.). Gower.