Information governance: A primer

Dr Ulrich Kampffmeyer, PROJECT CONSULT, Unternehmensberatung GmbH, Hamburg, Germany,
https://www.PROJECT-CONSULT.com.
Article submitted on invitation by the Associació de Professionals de l'Arxivística i la Gestió de Documents de Catalunya, to *Lligall*, January 2023 (https://arxivers.com/publicacions/revista-lligall/).

1 Introduction: Definitions and principles

Information governance is a broad term that refers to the policies, processes and practices that organisations use to manage their information assets. These assets can include anything from electronic data and documents to physical records and other types of data. Effective information governance is critical for organisations in today's digital age, as it helps ensure that information is accurate, secure and accessible to those who need it.

Information governance is a concept that refers to the overall management of information within and of an organisation. This includes the creation, storage, use and disposal of information, as well as the policies and procedures that govern these activities.

This article provides an overview of important elements, characteristics and criteria regarding information governance, with a particular focus on implementation challenges and future trends.

1.1 The term “information” and the “principles of information”

Information is an abstract concept that refers to that which has the power to inform. At the most fundamental level, information pertains to the interpretation of that which may be sensed. Any natural process that is not completely random and any observable pattern in any medium can be said to convey some amount of information.[1] In information theory, information is the knowledge that a sender conveys to a receiver via an information channel. The information can take the form of signals or code. In many cases, the information channel is a medium. For the receiver, the information leads to an increase in knowledge.

In this article, we focus on the governance of digital information.

Digital Information is only a subset of all information. Unlike analogue information objects and communication, digital information is a special form of representation for processed and recorded information. It conveys information in a more continuous form. Digital information may be analogue

[1] ANDERSON, J. B.; JOHNNESSON, R. *Understanding Information Transmission*. Piscataway: Ieee Press, 1996. ISBN 9780471711209.

information that has been transformed or “digital-born” information, the latter being the result of electronic processes or manual data entry.

One definition of digital information is as follows:

Digital information
Digital information is a sequence of symbols from a finite set of possibilities. The set of symbols is called an alphabet, and the symbols themselves are called characters. The characters are represented in a computer by a unique sequence of bits (binary digits).[2]

At its most basic level, information is any data that has been collected, processed or stored by an organisation. This can include anything from customer information and financial records to internal communications and business plans. Information management, on the other hand, is the practice of organising, storing and accessing this information in a way that allows an organisation to make the most of its data assets. Digital information is based on digital data, but they are not synonymous.

Table 1 lists the ten basic principles that apply to information[3] and make information governance a necessity:

The principles of information ***Los principios de la información***		
	English	**Spanish**
1	Information is an asset	La información es un activo
2	Information has purpose	La información tiene una finalidad
3	Information has sources and targets	La información tiene fuentes y objetivos
4	Information has deadlines	La información tiene plazos
5	Information has consumers	La información tiene consumidores
6	Information carries obligations	La información conlleva obligaciones
7	Information carries risks	La información conlleva riesgos
8	Information has many forms	La información tiene muchas formas
9	Information is not immortal	La información no es inmortal
10	Information demands accountability	La información exige responsabilidades

Table 1. The principles of information by Chris Walker and adopted by Ulrich Kampffmeyer, 2013

[2] FARNSWORTH, N. R.; THOMPSON, B. S. *The Nature of Mathematical Modeling*. Cambridge University Press, 2006.
[3] WALKER, C.; KAMPFFMEYER, U. "Information Governance - Grundsätze, Bedeutung und Prinzipien”. *PROJECT CONSULT Newsletter 20131022*, [online], 2013. <https://bit.ly/3vKnUVy>

1.2 The term “governance” and the principles of governance

Governance takes shape in various forms in companies as well as in other organisations. Governance is derived from the Latin *gubernator*, meaning “helmsman”, and is related to the conferral of the role of controller, administrator, governor. Transferred, governance stands for control. When the term "control" is used in Anglo-Saxon, it means active control rather than subsequent control. At the management level, corporate governance is the task of transparent, responsible management and control. Governance, in general, refers to the processes and structures that organisations use to make decisions and manage their operations. In the context of information, governance involves setting policies and guidelines for how information is collected, stored, accessed and used within an organisation. This includes everything from establishing protocols for data security and privacy to creating processes for managing and sharing information across different departments and teams.

In companies, organisations and public administrative institutions, the term governance is initially found at a higher management level as "corporate governance". Corporate governance is often regulated by laws and other requirements.

One definition of general governance is as follows:

General governance
Governance is the process of making and enforcing decisions within an organization or society. It is the process of interactions through the laws, social norms, power (social and political) or language as structured in communication of an organized society over a social system (family, social group, formal or informal organization, a territory under a jurisdiction or across territories). It is done by the government of a state, by a market, or by a network. It is the process of choosing the right course among the actors involved in a collective problem that leads to the creation, reinforcement, or reproduction of acceptable conduct and social order. Good governance is characterised by transparency, accountability, participation, and responsiveness.[4]

[4]BEVIR, Mark (2012). Governance: A very short introduction. Oxford, UK: Oxford University Press. ISBN 9780191646294; HUFTY, Marc (2011). "Investigating Policy Processes: The Governance Analytical Framework (GAF). In: WIESMANN, U., HURNI, H., –24

With respect to the focus of this article, we also need to look at the definition of digital governance or governance of digital objects. One definition of governance with respect of digital governance is as follows:

Digital governance
Digital governance refers to the policies, procedures, and practices that are put in place to ensure the secure, effective, and efficient creation, use, management, and disposal of digital information and systems within an organisation or society. It involves the development and implementation of strategies, standards, and frameworks for decision-making, accountability, and oversight related to the use of digital technologies and information, as well as the effective management of risks and challenges associated with the adoption and use of these technologies.[5]

Digital governance does not take analogue media and analogue communication into account. However, it is possible to digitally manage at least the information about analogue media and communication by keeping the metadata in electronic systems and referencing the analogue objects. In this way, digital governance can also manage analogue information together with digital data combined across all areas.

[5] KOVACICH, G. L.; BONI, W. C. *Digital Governance: The Intersection of Technology and Public Sector Management*. CRC Press, 2015.

The following table lists the ten principles that apply to general good governance:

The principles of governance[6] *Los principios de gobernanza*		
	English	**Spanish**
1	Transparency: Decisions and actions should be open and accountable to the public.	Transparencia: Las decisiones y acciones deben ser abiertas y responsables ante el público.
2	Responsibility: Those who make decisions or wield power should be accountable for their actions.	Responsabilidad: Quienes toman decisiones o ejercen el poder deben rendir cuentas de sus actos.
3	Fairness: All stakeholders should be treated equally and impartially.	Equidad: Todas las partes interesadas deben ser tratadas con igualdad e imparcialidad.
4	Participation: All stakeholders should have an opportunity to have their voices heard and to be involved in decision-making processes.	Participación: Todas las partes interesadas deben tener la oportunidad de hacer oír su voz y participar en los procesos de toma de decisiones.
5	Consensus-oriented: Decisions should be based on a broad consensus of stakeholders rather than the interests of a few individuals or groups.	Orientación al consenso: Las decisiones deben basarse en un amplio consenso de las partes interesadas y no en los intereses de unos pocos individuos o grupos.
6	Responsiveness: Governance systems should be responsive to the needs and aspirations of stakeholders.	Capacidad de respuesta: Los sistemas de gobernanza deben responder a las necesidades y aspiraciones de las partes interesadas.
7	Rule of law: Governance systems should operate within a framework of laws and regulations that are transparent, fair, and consistent.	Estado de derecho: Los sistemas de gobernanza deben funcionar dentro de un marco de leyes y reglamentos transparentes, justos y coherentes.
8	Ethical: Governance systems should operate with integrity and in accordance with ethical principles.	Ética: Los sistemas de gobernanza deben funcionar con integridad y de acuerdo con principios éticos.
9	Efficient: Governance systems should use resources efficiently and effectively.	Eficacia: Los sistemas de gobernanza deben utilizar los recursos de forma eficiente y eficaz.
10	Sustainable: Governance systems should be designed to be sustainable over the long term.	Sostenibles: Los sistemas de gobernanza deben diseñarse para ser sostenibles a largo plazo.

Table 2. The principles of general good governance

[6] KAMPFFMEYER, U. "Information Management". *PROJECT CONSULT Blog*, [online] 2016. <https://bit.ly/2PyJIly>

1.3 The term "information management" and the "principles of information management"

Information Management usually refers to electronic information, therefore, management in this context stands for the handling, ordering, organisation, provision, use, securing, protection and preservation of information in electronic format. Different definitions of information management (IM) exist, and ISO standards use these different definitions depending on the context (e.g. ISO 17799, ISO 27001, ISO 27701).

Techopedia gives the following definition:

Information management
Information management is the process of collecting, storing, managing and maintaining information in all its forms. Information management is a broad term that incorporates policies and procedures for centrally managing and sharing information among different individuals, organisations and/or information systems throughout the information life cycle.[7]

The goal of information management is to ensure that the right information is available to the right people at the right time, and that it is accurate, relevant, and secure. Information management is important in a variety of contexts, including businesses, government agencies, and other organisations, as well as in personal settings.

The principles of information management[8] ***Los principios de la gestión de la información***		
	English	**Spanish**
1	Information exchange	Intercambio de información
2	Information use	Uso de la información
3	Information provision	Suministro de información
4	Information protection	Protección de la información
5	Information organisation	Organización de la información
6	Information governance	Gobernanza de la información
7	Information distribution	Distribución de la información
8	Information evaluation	Evaluación de la información
9	Information preservation	Conservación de la información
10	Information disposal	Eliminación de la información

Table 3. The principles of information management

The term *information management* as an industry term is increasingly replacing traditional terms such as document management (DM), enterprise content management (ECM) or content services platforms (CSP). In fact, the international trade association AIIM (Association for Intelligent Information Management) goes a step further and uses the term *intelligent information management* (IIM). This is to show the influence that new technological developments such as

[7] Techopedia. "Information Management (IM)" [online]. 2017. <https://www.techopedia.com/definition/20012/information-management-im>

[8] KAMPFFMEYER, U. "Information Management". *PROJECT CONSULT Blog* [online]. 2016. <https://bit.ly/2PyJIly>

automation, artificial intelligence, machine learning, analytics and others are having.[9] Information management can subsume not only concepts such as records management, but also information governance itself as a function for controlling information. A related concept is information lifecycle management (ILM)[10] and covers the lifecycle of electronic information from creation to destruction.

1.4 The term "information governance" and the "information governance principles"

One final term is that of *information governance*, often abbreviated as InfoGov or IG.

The history of information governance can be traced back to the early days of the digital age, when organisations first began to collect and store large amounts of data. As the amount of data grew, so did the need for effective ways to manage and access it. Over time, organisations developed various practices and tools for information governance, including the use of data warehouses, data management software, and other technologies.

Information governance, then, is the combination of the information management and governance practices that organisations use to manage their information assets. This can include establishing policies and procedures for collecting, storing and accessing information, as well as implementing technologies and other tools to support these processes.

Information governance involves mastering information. In a world flooded with information, buzzwords such as big data, the growth of e-commerce, compliance and transparency requirements, discussions about confidentiality and personal data, rights in the digital world, and the pervasiveness of information available at all times via mobile devices, information governance is taking on a new dimension.

Information governance is part of the overarching strategic task. IT governance is also part of this but is by no means the same as information governance. This is important to note – IT governance is not information governance. IT governance is concerned with systems and their operation, while information governance is concerned with the information, the knowledge, the virtual, intangible assets of the company itself.[11]

[9] KAMPFFMEYER, U. "Nur Information Management oder Intelligent Information Management?". *PROJECT CONSULT Newsletter 20190615* [online]. 2019. <https://bit.ly/3WWxVuH>
[10] KAMPFFMEYER, U. "Information Lifecycle Management (ILM)". *PROJECT CONSULT Blog*, [online]. 2015. <https://bit.ly/3lytd1Z>
[11] KAMPFFMEYER, U. "Information Management & Information Governance". *PROJECT CONSULT Blog* [online]. 2013. <https://bit.ly/3QnH1y6>

Different definitions exists for information governance, one of which is that of the AIIM, which promotes intelligent information management, from 2013:

Information governance (AIIM)
The creation of a set of rules, policies, and procedures that ensures the proper handling of information from its creation to its disposal.[12]

And Wikipedia's entry in English (2022) defines information governance as follows:

Information governance (Wikipedia)
Information governance, or IG, is the overall strategy for information at an organisation. Information governance balances the risk that information presents with the value that information provides. Information governance helps with legal compliance, operational transparency, and reducing expenditures associated with legal discovery. An organisation can establish a consistent and logical framework for employees to handle data through their information governance policies and procedures. These policies guide proper behaviour regarding how organisations and their employees handle electronically stored information (ESI). Information governance encompasses more than traditional records management. It incorporates information security and protection, compliance, data governance, electronic discovery, risk management, privacy, data storage and archiving, knowledge management, business operations and management, audit, analytics, IT management, master data management, enterprise architecture, business intelligence, big data, data science, and finance.[13]

[12] Association for Intelligent Information Management (AIIM). "The Fundamentals of Information Governance" [online]. 2013. <www.AIIM.org>

[13] Wikipedia. "Information governance" [online]. <https://en.wikipedia.org/wiki/Information_governance>

The most current, official, accepted and standardised adaption of a definition is that of ISO 24143:2022, which we will discuss further in section 2:

Information governance (ISO 24143)
Information governance is a strategic framework for managing information assets across an entire organisation to support its business outcomes and obtain assurance that the risks to its information, and thereby the operational capabilities and integrity of the organisation, are adequately identified and managed. Information governance includes but is not limited to policies, processes, procedures, roles and controls put in place to meet regulatory, legal, risk and operational requirements. Information governance provides an overarching high-level framework that: • aligns all information-related activities with the mission and goals of an organisation, and its business, legal and societal obligations, • ensures a comprehensive and systematic approach to information by integrating processes relevant to directing and controlling information, • supports cooperation between stakeholders, and • creates a high-level basis for managing information regardless [of] its form, type and format, informs education, professional development of the workforce and awareness about information-related obligations, risks and possibilities.[14]

Information governance is often used as a synonym for data governance. Data governance refers to the overall management of the availability, usability, integrity and security of the data employed in an organisation. It involves establishing policies, procedures, and standards for the collection, storage, access, use and dissemination of data. Information is on a higher level than data, but both aim for the same goal.

[14] ISO 24143:2022. Information and documentation — Information Governance — Concept and principles [online]. <https://www.iso.org/standard/77915.html>

The principles of information governance *Los principios de la gobernanza de la información*		
	English	**Spanish**
1	Accountability: There should be clear lines of responsibility and accountability for the management of an organisation's data and information assets.	Rendición de cuentas: Deben existir líneas claras de responsabilidad y rendición de cuentas para la gestión de los activos de datos e información de una organización.
2	Integrity: Data and information should be accurate, complete, and reliable	Integridad: Los datos y la información deben ser precisos, completos y fiables.
3	Protection: Data and information should be protected from unauthorised access, use, or disclosure.	Protección: Los datos y la información deben estar protegidos frente al acceso, uso o divulgación no autorizados.
4	Compliance: Data and information practices should be in compliance with relevant laws, regulations, and standards.	Conformidad: Las prácticas relativas a los datos y la información deben ajustarse a las leyes, reglamentos y normas pertinentes.
5	Availability: Data and information should be readily available to authorised users when needed.	Disponibilidad: Los datos y la información deben estar fácilmente disponibles para los usuarios autorizados cuando los necesiten.
6	Retention: Data and information should be retained for as long as it is needed, and then disposed of in a secure and appropriate manner.	Conservación: Los datos y la información deben conservarse todo el tiempo que sea necesario y, a continuación, eliminarse de forma segura y adecuada.
7	Transparency: There should be transparency in the way that data and information is collected, used, and shared.	Transparencia: Debe haber transparencia en la forma en que se recopilan, utilizan y comparten los datos y la información.
8	Security: Data and information should be secure from cyber threats and other forms of unauthorised access.	Seguridad: Los datos y la información deben estar a salvo de ciberamenazas y otras formas de acceso no autorizado.
9	Privacy: Data and information should be collected, used, and shared in a manner that respects the privacy rights of individuals.	Privacidad: Los datos y la información deben recopilarse, utilizarse y compartirse de forma que se respete el derecho a la intimidad de las personas.
10	Quality: Data and information should be of high quality, with measures in place to ensure that it is accurate, complete, and up to date.	Calidad: Los datos y la información deben ser de alta calidad, con medidas que garanticen que son precisos, completos y actualizados.

Table 4. The principles of information governance

The value of information governance for organisations is clear. By implementing effective information governance practices, organisations can ensure that their data is accurate, secure and accessible to those who need it. This can help improve decision-making, reduce the risk of data breaches and increase the overall efficiency and effectiveness of the organisation. In today's digital age, information governance is more important than ever before, and organisations that fail to implement effective practices risk falling behind their competitors.

1.5 GRC: governance, risk management and compliance

Information governance should be part of an overarching governance, risk management and compliance (GRC) strategy.

GRC, although the letters are often combined in a different order, offers a holistic approach that prevents the emergence of isolated solutions. Corporate governance, regulatory compliance and risk assessment increasingly go hand in hand. However, the delineation of tasks and the different perceptions of their scope lead to very different approaches.

In order to bring clarity to the relationship between the three underlying components of the GRC acronym, it is first necessary to define them individually. As we have already dealt with governance and information governance, we must now look at risk.

Risk comes from the Italian word for venture or danger, *rischio*. Risk management comprises the measures for recording, evaluating and controlling risks. The risks must be collected, processed and evaluated. Measures must be taken to avoid the risks and to comply with the relevant compliance requirements. It is the responsibility of a company's management or board of directors to determine the scope of the measures and ensure that they are complied with. Risk management is an essential component of information governance.

The term *compliance* can be interpreted as adherence to or the observance or fulfilment of certain requirements. Compliance encompasses the totality of all reasonable measures that justify the rule-compliant behaviour of a company, its organisational members and its employees with regard to all legal requirements and prohibitions. Compliance refers both to the fulfilment of external legal requirements and to the fulfilment of internal regulatory requirements. The fulfilment of compliance is another important aspect of information governance.

As is already clear from the definitions, the areas of governance, risk management and compliance cannot be viewed in isolation from one another: compliance requirements include obligations for risk management and adherence to governance guidelines. Risk management involves the assessment of compliance requirements, and corporate governance encompasses both compliance and risk management. For a long time, however, these complex tasks were seen as individual areas of work, distributed among different departments and roles, and implemented in specific solutions.
Viewed from this perspective, it becomes evident that a holistic view of the company be required. Separate consideration of governance, IT governance, compliance and information management compliance, risk management and quality management does not lead to the required transparency, traceability and consistency. For implementation in processes and in the organisation of a company or administration, a holistic view is required, in which governance provides the rules and guidelines, risk management evaluates them, and compliance ensures practical, operational implementation.

Fig. 1 GRC combine the disciplines of corporate governance, IT governance, information governance, risk management, security, data protection and compliance as an end-to-end process model.[15]
La GRC combina las disciplinas de gobierno corporativo, gobierno de TI, gobierno de la información, gestión de riesgos, seguridad, protección de datos y cumplimiento como un modelo de proceso integral.

An increasing number of laws and guidelines require organisations to be transparent in their handling of data and to separate, monitor and document business processes. Meanwhile, laws written for the paper world are being extended to the electronic world: retention and documentation requirements for electronic business records are increasing. In fact, all the legal and statutory requirements of the paper world also apply in the electronic world, yet the requirements of the IT world are often not taken into account, at least not directly, and must therefore be inferred.

Organisations are faced with the major challenge of bringing their business into line with existing and future regulations and operating effective risk management. The combination of governance, risk management and compliance, GRC, is an important step in meeting this challenge. It provides an umbrella for all measures to ensure the proper, efficient, secure and traceable use of information in an organisation.

[15] KAMPFFMEYER, U. "GRC als ganzheitlicher Ansatz". *PROJECT CONSULT Themen* [online]. 2015. <https://bit.ly/3CzRKjw>

1.6 The core of information governance: policies

Policies and rules must be documented. They must be formulated in a way that is practical and easy to understand. They must be available to all employees, who must be trained and constantly monitored for compliance. These policies and rules must be reviewed and, if necessary, adapted whenever there is a change in business activities, systems or processes. As a result, many of an information governance office's or officer's activities fall under the heading of administrative and auditing tasks.

These tasks are usually based on company guidelines and policies, which must be implemented by management for all employees. Building on the corporate governance policy is the information governance policy, which can encompass records management, compliance, information management, security, data protection and other aspects or subordinate guidelines. Each policy requires work instructions and training. Consistent implementation is the only way to achieve consistent information governance. Not everything can be managed or controlled by systems; the people in the organisation are an essential component in implementing information governance.

2 ISO 24143:2022 Information governance

ISO 24143:2022[16] is an international standard that provides organisations with guidelines on implementing effective information governance practices. The standard covers a range of topics, from the benefits of information governance to the principles that organisations should follow in order to effectively manage their information assets.

"ISO 24143:2022 Information and documentation — Information Governance — Concept and principles" is part of a larger framework, which includes standards and a range of technology areas such as data management, information management, records management, knowledge management, regulatory compliance, digital preservation, information security, enterprise architecture, data protection, open data, big data, artificial intelligence, blockchain, business processes and quality management. Information governance requires coherence and integration with relevant management system standards (MSS), such as ISO 9000 for quality management, ISO/IEC 27000 for information security and the ISO 30300 series on records management. ISO 24143:2022 makes several normative references, including other ISO standards and other documents that provide guidance on information governance. These references are important because they provide organisations with a more comprehensive view of the principles and practices that are necessary for effective information governance.

2.1 The scope of ISO 24143

The scope of ISO 24143 is to provide organisations with guidance on how to establish and maintain effective information governance practices. The standard covers a wide range of topics, including the recognition of information as a strategic asset, the integration of information governance into an

[16] ISO 24143:2022. Information and documentation — Information Governance — Concept and principles [online]. <https://www.iso.org/standard/77915.html>

organisation's governance frameworks, and the alignment of information governance with business objectives:

> *Information Governance is an integral part of the overall governance of the organisation. It identifies common high-level principles and provides a framework enabling effective and efficient cooperation of all the information-related professionals, in support of the mission of an organisation and achievement of its strategic goals.*

The cooperation of information professionals with all other units of an enterprise is an important requisite to achieve these goals. The standard also outlines fifteen principles that organisations should follow in order to implement effective information governance practices. These principles include recognising information as a corporate, strategic asset, designing information governance as a key element of corporate strategy, and integrating information governance into the organisation's governance frameworks.

In addition to these principles, ISO 24143 also recommends that organisations adopt a risk-based approach to information governance. This means that organisations should prioritise the risks associated with their information assets and develop strategies and practices to manage those risks effectively.

The standard provides organisations with a comprehensive framework for implementing effective information governance practices. By following the guidelines outlined in the standard, organisations can ensure that their information assets are well managed, secure and accessible to those who need them.

2.2 The principles of information governance

ISO 24143 standard contains a set of 15 principles of information governance[17]:

The ISO 24143 principles of information governance ***Los principios de la gobernanza de la información según ISO 24143***		
	English	**Spanish**
1	Recognising information as a corporate, strategic asset	Reconocer la información como un activo corporativo y estratégico
2	Designing Information Governance as a key element of corporate strategy	Diseñar el gobierno de la información como elemento clave de la estrategia corporativa
3	Integrating Information Governance into the organisation's governance frameworks	Integrar la gobernanza de la información en los marcos de gobernanza de la organización.
4	Securing senior management's leadership and commitment	Garantizar el liderazgo y el compromiso de la alta dirección
5	Building Information Governance in a collaborative way	Establecer la gobernanza de la información de forma colaborativa
6	Ensuring Information Governance supports legal compliance and any mandatory requirements	Garantizar que el gobierno de la información respalda el cumplimiento de la legislación y cualquier requisito obligatorio.
7	Aligning Information Governance to business objectives	Alinear el gobierno de la información con los objetivos empresariales
8	Ensuring Information Governance supports information security and privacy	Garantizar que el gobierno de la información apoya la seguridad y la privacidad de la información.
9	Ensuring Information Governance supports information quality and integrity	Garantizar que el gobierno de la información apoya la calidad y la integridad de la información.
10	Fostering a collaboration and knowledge sharing culture	Fomentar una cultura de colaboración e intercambio de conocimientos
11	Adopting a risk-based approach	Adoptar un enfoque basado en el riesgo
12	Ensuring the availability and accessibility of information to authorised stakeholder[s]	Garantizar la disponibilidad y accesibilidad de la información a las partes interesadas autorizadas.
13	Governing information throughout its information lifecycle	Gestionar la información a lo largo de todo su ciclo de vida
14	Supporting corporate culture	Apoyar la cultura corporativa
15	Supporting sustainability	Apoyar la sostenibilidad

Table 5. The 15 principles of information governance according to ISO 24143:2022

[17] ISO 24143:2022. *PROJECT CONSULT Blog*, 2022, [online]. <https://www.project-consult.com/news/iso-241432022/>

The following provides a detailed explanation of the ISO principles.

2.2.1 Recognising information as a corporate, strategic asset

Information Governance acknowledges legal, business, historical and other value of information and information assets, their essential role in business and governance, information-related benefits and risks, and the potential of information assets to become a key competitive advantage. One of the key principles of information governance is recognising information as a corporate, strategic asset. This means that organisations should view their data as an important resource that can be used to support decision-making, drive innovation and improve overall performance. By recognising the value of their information assets, organisations can take steps to protect and manage them effectively.

2.2.2 Designing Information Governance as a key element of corporate strategy

Information Governance includes all the high-level, strategic aspects of governing and controlling information, such as the provision of infrastructure and systems for processing; compliance to legal and regulatory requirements related to information; governance instruments such as policies, procedures, and standards; and people. This important principle is designing information governance as a key element of corporate strategy. This means that organisations should incorporate information governance into their overall business strategies and ensure that it is aligned with their goals and objectives. This can help organisations to better leverage their information assets and ensure that they are being used in the most effective way possible.

2.2.3 Integrating Information Governance into the organisation's governance frameworks

Information Governance forms an integral part of, and should be integrated with, all the organisation's governance frameworks and management systems. This means that organisations should ensure that their information governance practices are integrated with other governance processes and structures, such as those related to risk management, finance, data protection, compliance and security. By integrating information governance into these broader frameworks, organisations can better manage their information assets and reduce the risk of data breaches and other issues. Information Governance should be included in the integrated reporting of the organisation.

2.2.4 Securing senior management's leadership and commitment

The responsibilities of that Information Governance leader should include identifying the components of the organisation's Information Governance framework, defining the processes, procedures and driving them, unlocking potential and emergent obstacles, communicating the goals and business objectives, allocating the resources needed (team, structures, infrastructures) and keeping upper management informed on progress. Securing senior management's leadership and commitment is also essential for effective information governance. This means that organisations should ensure that their senior leaders are fully supportive of their information governance efforts and are willing to provide the necessary resources and support. By securing this leadership and commitment, organisations can better ensure the success of their information governance initiatives.

2.2.5 Building Information Governance in a collaborative way

Information Governance is understood primarily as a strategic multi-disciplinary framework that lays the foundation for cooperation and synergy between numerous information-related professions. That is why information governance should be conducted in a collaborative way. This means that organisations should involve multiple stakeholders in the development and implementation of their information governance practices. This can help to ensure that the organisation's information governance efforts are aligned with the needs and priorities of different departments and teams.

2.2.6 Ensuring Information Governance supports legal compliance and any mandatory requirements

Information Governance supports and aims for compliance with all applicable laws, regulations, mandatory and voluntary standards and codes of industry practice applicable to the organisation. Ensuring that information governance supports legal compliance, corporate standards and any other regulatory requirements is an important principle, which also requires the introduction of continuous, holistic information governance. This means that organisations should ensure that their information governance practices and processes are consistent with relevant laws and regulations. By doing so, organisations can reduce the risk of legal action and other issues related to non-compliance.

2.2.7 Aligning Information Governance to business objectives

Aligning information governance with business objectives is another important principle. This means that organisations should ensure that their information governance practices are designed to support their overall business goals and objectives. By aligning their information governance practices with their business objectives, organisations can better leverage their information assets and drive value for the organisation. Alignment should be continuously monitored and revised as the business needs and direction change. All stakeholder requirements and needs should be considered when developing the Information Governance program.

2.2.8 Ensuring Information Governance supports information security and privacy

One of the key principles of ISO 24143 is ensuring that information governance supports information security, safety and privacy. This means that organisations should have measures in place to protect sensitive information from unauthorised access, disclosure or destruction. Access controls and permissions should be established and implemented to ensure that information is only made available to those with adequate authority. This includes implementing access controls, encryption and other security measures to safeguard information.

2.2.9 Ensuring Information Governance supports information quality and integrity

Another key principle is ensuring information governance supports information quality and integrity. This means that organisations should have processes in place to ensure that the information they use is accurate, complete and reliable. This includes implementing quality control measures to validate the accuracy of information, as well as ensuring that information is kept up-to-date and relevant. The major goal is to ensure information is authentic; trustworthy; complete, consistent, reliable, relevant, easy to retrieve and use, accurate and able to demonstrate integrity.

2.2.10 Fostering a collaboration and knowledge sharing culture

Fostering a collaboration and knowledge sharing culture is another important aspect of the ISO standard. Effective and efficient Information Governance often requires the information to be treated as a corporate resource rather than an asset controlled exclusively by specific business area/function or individual. Information Governance requires a cross-functional collaboration where appropriate, to maximise information's value. This means that organisations should encourage employees to share information and collaborate with each other in order to maximise the value of the information they possess. This can be achieved through the use of collaborative tools and technologies, as well as through the creation of a culture that values the sharing of knowledge and expertise.

2.2.11 Adopting a risk-based approach

ISO 24143 also recommends adopting a risk-based approach to information governance and to implement controls for appropriate information usage in compliance with laws, policies, regulation in alignment with the organisation's risk profile. This means that organisations should assess the risks associated with their information and take appropriate measures to mitigate those risks. This includes identifying potential threats to the security, quality and integrity of information, and implementing measures to address those threats.

2.2.12 Ensuring the availability and accessibility of information to authorised stakeholder[s]

Ensuring the availability and accessibility of information to authorised stakeholders is another key principle. This means that organisations should have processes in place to ensure that the right people have access to the information they need, when they need it. This can be achieved through the implementation of access controls, as well as through the use of technologies that enable remote access to information. The Information Governance program should continuously adapt to meet the organisation's internal and external evolving needs.

2.2.13 Governing information throughout its information lifecycle

Governing information throughout its lifecycle is another important aspect of great importance which applies to the information itself but also for all rules and processes that control the lifecycle. This means that organisations should have processes in place to manage the entire lifecycle of their information, from its creation to its disposal. This includes ensuring that information is properly classified and stored, as well as implementing processes for disposing of information when it is no longer needed.

2.2.14 Supporting corporate culture

Information Governance should become embedded in the culture of the organisation and the behaviour and attitude of people working for it.. This means that organisations should align their information governance practices with their overall corporate culture and values. This includes ensuring that information governance is integrated into the organisation's policies and practices, and that it is supported by senior management. Information Governance programmes require a planned approach to adoption, change management and awareness, ensuring that all Information Governance initiatives equip employees to comply with the organisation's Information Governance requirements.

2.2.15 Supporting sustainability

Finally, ISO 24143 recommends that organisations support sustainability in their information governance practices. This means that they should consider the environmental impact of their information management practices and implement measures to reduce the use of resources and minimise waste. This means that organisations should implement information governance frameworks that are environmentally friendly and that support sustainable development.

2.3 The key benefits of ISO 24143

One of the key benefits of information governance is that it helps organisations to better manage their information assets. By implementing effective information governance practices, organisations can ensure that their data is accurate, secure and accessible to those who need it. This can help improve decision-making, reduce the risk of data breaches, and increase the overall efficiency and effectiveness of the organisation.

Overall, ISO 24143 is a valuable tool for organisations looking to implement effective information governance. By following the guidelines outlined in the standard, organisations can ensure that their information systems and practices are aligned with their corporate culture and are sustainable in the long term.

2.4 The expected impact of ISO 24143

The 15 principles go beyond previous approaches to information governance, with the risk-based approach as a special new feature. The topic of "sustainability" has also found its way into ISO 24143. The generally formulated standard can be used as a good basis for planning information governance measures and creating information governance policies.

According to Robert Smallwood,[18] the standard opens up five other new areas of application and impact:

1. **Standardisation of information governance programmes**

   It is now easier for companies to set up projects and develop strategies that address the value of information, reduce costs, define risk factors and legal requirements, and involve those responsible for information management and governance.

2. **Benchmark for private equity investors**

   The implementation of the ISO standard and the compliance it demonstrates can also serve as an incentive for investors to invest in this company. Proven compliance with requirements, proper processes and good governance in the company also promote the trust of customers, suppliers, partners, the public and investors.

3. **Broadening the market**

   More companies in the information management industry will develop and offer products and services that comply with the guidelines of ISO 24143. This will also include sector-specific model templates for information governance. However, these providers should then also commit to and implement the principles of the standard themselves.

4. **Training at universities and colleges**

   Both the standard and the guidelines derived from it can serve as a basis for lectures and seminars. On the subject of information governance, there is a considerable shortage of well-trained professionals for public authorities, companies and organisations.

5. **Extension into sustainability and corporate governance issues**

   The standard can also be helpful in establishing quality standards, ethics, resource conservation, environmental protection, data protection and other governance requirements. It can serve as a benchmark for the implementation of regulations, documentation of evidence and compliance.

In any case, it is important to understand information governance and raise awareness of its importance.

[18] SMALLWOOD, R. “5 Key Ways the New ISO Information Governance Standard Can Have an Impact”, 2022, [online] <www.LinkedIn.com>.

3 Records management

Using records management and other document management technologies is an excellent way to enable effective information governance.

However, there is one major challenge – records management only covers a small amount of an organisation's total information. More valuable data and information can be found in applications and databases that independently control and archive their information. Most of the information in an organisation goes uncontrolled and unmanaged. It contains a large amount of outdated, redundant and trivial data. Information exists in multiple formats like PDFs, emails, notes, documents, spreadsheets, graphics, images, videos, audio recordings, drawings, messages and 3D-models, among others, and often these types of information objects are not suitable forlong-term archiving and digital preservation. The greatest challenge is that more and more of an organisation's data and information are kept off-site on portals, social media, partner sites, and so on. Therefore, it is necessary to have an overarching framework to manage and control all the information inside and outside an organisation. The controlled environment of records management is only one part of the overall information governance architecture.

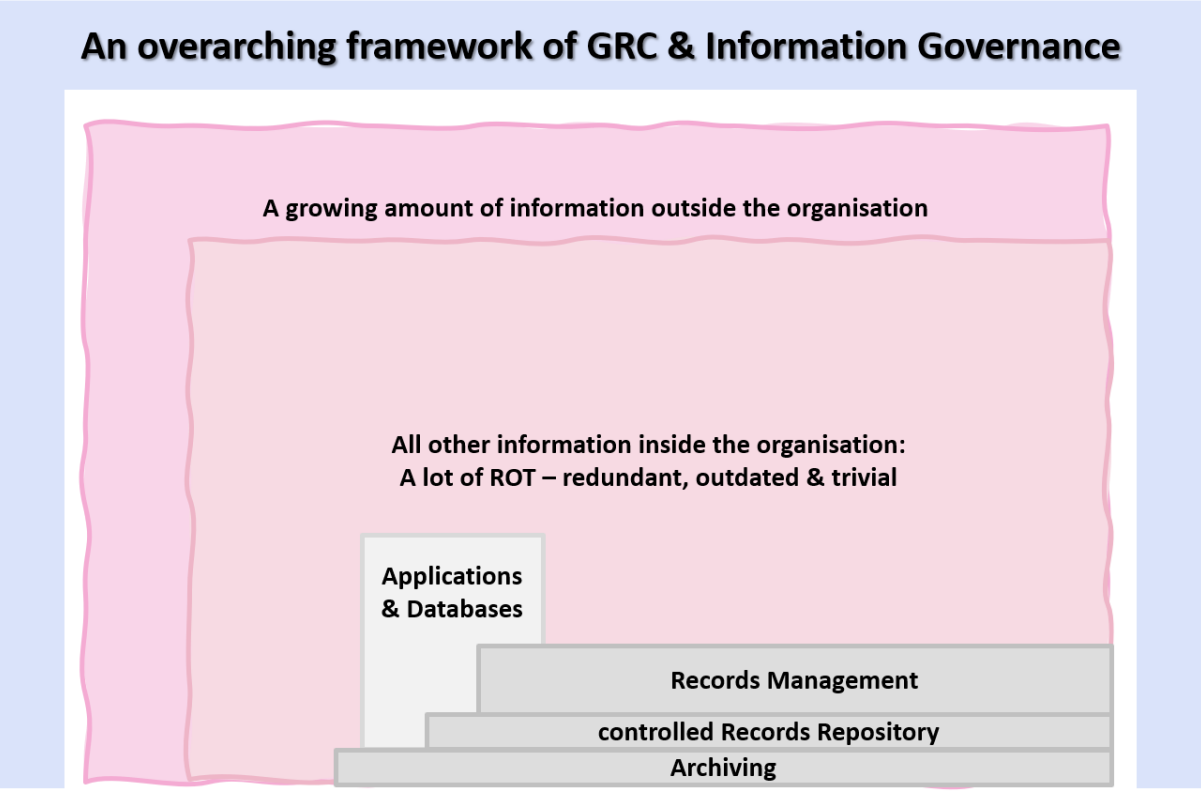

Fig. 2 An overarching framework of GRC and information governance is needed to manage and control all information inside and outside the organisation.
Se necesita un marco general de GRC y gobernanza de la información para gestionar y controlar toda la información dentro y fuera de la organización.

The principles of records management are another good way to manage the rest of an organisation's information, even if this information is not included in records or archives. ISO 15489:2016 defines records management as follows:

Records management
…field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records... [19]

ISO 15489 is very general but offers a good basis for formulating and implementing records management policies.

[19] ISO 15489-1:2016. Information and documentation — Records management — Part 1: Concepts and principles. Revised 2021. [online]. <https://www.iso.org/standard/62542.html>

The Association of Records Managers and Administrators (ARMA) provides a set of eight principles for records management known as the Generally Accepted Recordkeeping Principles (GARP), often referred to as "The Principles".[20] These are general requirements and are the basis for a framework of effective records management:

The Principles®, ARMA *Los Principios® de ARMA*		
English		**Spanish**
1	Accountability	Rendición de cuentas
2	Transparency	Transparencia
3	Integrity	Integridad
4	Protection	Protección
5	Compliance	Conformidad
6	Availability	Disponibilidad
7	Retention	Conservación
8	Disposition	Eliminación

Table 6. The eight Generally Accepted Recordkeeping Principles (GARP)

The eight principles are as follows:

1. **Principle of Accountability**

   There should be clear lines of responsibility and accountability for the management of an organisation's data and information assets. Organisations are responsible for maintaining accurate, complete and reliable records that reflect their activities and transactions. This means that they need to have clear policies and procedures in place to ensure that records are created, managed, and preserved in accordance with all relevant laws and regulations. A senior executive (or a person of comparable authority) shall oversee information management and ensure it is accessed by the appropriate individuals.

2. **Principle of Transparency**

   There should be transparency in the way that data and information is collected, used and shared. Organisations should be open and transparent in their records management practices. This means that they need to make their records easily accessible to those who are authorised to access them, and that they should provide clear information about how records are created, managed and preserved. An organisation's business processes and activities, including its information governance programme, should be documented in an open and verifiable manner, and that documentation should be available to all personnel and the appropriate stakeholders.

3. **Principle of Integrity**

[20] Association of Records Managers and Administrators (ARMA). "The Principles", [online]. https://www.arma.org/page/principles

Data and information should be accurate, complete and reliable. Records should be accurate, complete and unaltered. Organisations need to implement measures to ensure that records are not altered or tampered with, and that they are preserved in their original format. An information governance programme should be constructed so the information assets generated by or managed for the organisation have a reasonable guarantee of authenticity and reliability.

4. **Principle of Protection**

   Organisations should protect their records from damage, loss, unauthorised access and other risks. This means that they need to implement appropriate physical and electronic security measures to ensure that records are safeguarded. An information governance programme should be constructed to ensure an appropriate level of protection to information assets that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection.

5. **Principle of Compliance**

   Data and information practices should be in compliance with relevant laws, regulations, and standards. Organisations should ensure that their records management practices comply with all relevant laws and regulations. This means that they need to be aware of the legal requirements for records management, and that they should implement policies and procedures to ensure that they are compliant. An information governance programme should be constructed to comply with applicable laws, other rules by regulatory authorities and the organisation's policies.

6. **Principle of Availability**

   Data, information and records should be readily available to authorised users when needed. Organisations need to ensure that their records management systems and practices support timely and efficient access to records. An organisation should maintain its information assets in a manner that ensures their timely, efficient and accurate retrieval.

7. **Principle of Retention**

   Data and information should be retained for as long as they are needed, and then disposed of in a secure and appropriate manner. Organisations should retain records for as long as they are needed for business or legal purposes. This means that they need to develop and implement retention schedules that outline how long records should be kept, and that they should dispose of records in accordance with these schedules. An organisation should maintain its information assets for an appropriate time, taking into account its legal, regulatory, fiscal, operational and historical requirements.

8. **Principle of Disposition**

   Often forgotten, organisations should dispose of records in a secure and responsible manner when they are no longer needed. This means that they need to have policies and procedures in place to ensure that records are destroyed or otherwise disposed of in a way that protects their confidentiality and integrity. An organisation should provide secure and appropriate disposition for information assets no longer required to be maintained, in compliance with applicable laws and the organisation's policies.

Overall, the GARP provide a valuable framework for effective records management, which could be applied both to information management and to information governance. By following these principles, organisations can ensure that all information is accurate, complete and protected, and that they are managed in a way that is compliant with all relevant laws and regulations.

4 Challenges for information governance

Now that we have discussed all relevant definitions, principles and implications for efficient information governance, it is time to tackle the challenges of implementing and maintaining an information governance infrastructure.

The key challenges are as follows:

The key challenges for information governance ***Los principales retos de la gobernanza de la información***		
English		**Spanish**
1	Legal	Aviso jurídico
2	Compliance	Conformidad
3	Organisational	Organización
4	People	Personas
5	Implementation	Aplicación
6	Business	Empresa
7	Ethical	Ética
8	Software & technology	Software y tecnología
9	Preservation	Conservación
10	Knowledge management	Gestión del conocimiento

Table 7. Ten challenges for information governance

4.1 Legal challenges

One of the key challenges that organisations face when implementing information governance are legal challenges. In many cases, the laws and regulations governing information management are complex and constantly evolving. This means that organisations need to be aware of the legal requirements for information governance, and that they need to ensure that their information management practices are compliant with these requirements.

Laws and regulations change swiftly to adapt to the Digital Age. A good example of a flood of new laws is the Shaping Europe's Digital Future programme.[21] Until 2025 ten European initiatives will implement a dozen of new laws: Digital Services Act (DSA), Digital Market Act (DMA), European Chips Act (ECA), European Digital Identity (eIDAS), European Data Strategy, Artificial Intelligence (AI Act), European Industrial Strategy, Contributing to European Defence, Space and EU-US Trade and Technology Council.. All of these will have a great impact on information governance in Europe.

Overall, legal challenges are a significant challenge for organisations implementing information governance. Organisations need to be aware of the legal requirements for information management, and they need to ensure that their information management practices are compliant with these requirements in order to avoid penalties and fines. By addressing these legal challenges, organisations can ensure that their information management practices are effective and compliant with all relevant laws and regulations.

[21] European Commision. "Shaping Europe's Digital Future", [online] <https://digital-strategy.ec.europa.eu/en>

4.2 Compliance challenges

Another challenge that organisations face when implementing information governance are compliance requirements. More and more laws and regulations address the use of digital information. They are subject to continuous change. These can originate from laws and regulations but also organisations' internal standards. Information governance involves ensuring that information is accurate, consistent and compliant with all relevant laws and regulations. This can be a complex and time-consuming process, and organisations need to have appropriate policies and procedures in place to ensure that they are meeting these requirements. This avoids risks and possible penalties.

Compliance challenges are a significant issue for organisations, but by addressing these challenges, organisations can ensure that their information management practices are effective and support the achievement of their business objectives.

4.3 Organisational challenges

Organisations have to adapt, be able to implement information governance and react to market changes with more flexibility. In particular, information governance involves coordination and collaboration between different departments and stakeholders within an organisation. This can be challenging, especially when different departments have different priorities and objectives. Organisations need to have effective communication and collaboration processes in place to ensure that information governance is implemented effectively across the organisation.

If these organisational challenges are addressed correctly, organisations can successfully align their information governance practices with the overall strategy and objectives of the organisation so that it reaches its objectives.

4.4 People challenges

In order to implement and maintain effective information governance, organisations have to take into account existing staff and their structure, relations and behaviour. Major obstacles can arise in terms of staff attitudes, the work structure and individual beliefs within an organisation. Extensive change management programmes are needed to address these issues. The organisation must ensure that individuals within an organisation have a positive attitude towards information governance. Companies may find that certain Individuals have a negative perception of information governance or records management, such as that it is time-consuming or unnecessary, or they may come up against resistance to change, with feelings of "this never will work", or "we never did it this way". Organisations need to provide training and support to ensure that each staff member understand the value and importance of information governance, and that they are motivated to support its implementation. As such, a broad approach is needed.

In addition to human resource challenges, organisations also face social challenges when

implementing information governance. These challenges relate to the social dynamics within an organisation, and they can be difficult to address. For example, individuals within an organisation may have different priorities, beliefs and attitudes, which can make it difficult to implement information governance effectively. Organisations need to have effective communication and collaboration processes in place to ensure that individuals are able to work together to support the implementation of information governance. Organisations need to provide training and support to ensure that individuals have the necessary attitudes towards information governance and have effective communication and collaboration processes in place to support its implementation.

4.5 Implementation challenges

Any plan to implement and maintain a robust information governance programme has to consider various aspects:

- **Handling existing systems, workflows and procedures**
  There is no greenfield deployment; systems, ways of working, processes and structures already exist and have to be integrated or adapted.
- **Managing the volume and variety of information**
  The amount of information that organisations generate and store continues to grow exponentially. This makes it difficult to manage and organise this information effectively and can lead to information overload and inefficiency.
- **Ensuring information security**
  Cybersecurity threats continue to evolve and become more sophisticated, and organisations must protect their information from these threats. This requires implementing and maintaining robust security measures, such as encryption and access controls, as well as regularly training employees in information security best practices.
- **Ensuring information accessibility**
  Organisations must be able to access the information they need quickly and easily in order to make timely and informed decisions. This can be challenging, especially as the volume and variety of information grows.
- **Managing the lifecycle of information**
  The lifecycle has to be managed and controlled effectively in order to maintain the integrity and security of information. This includes properly disposing of information when it is no longer needed, as well as ensuring that information is kept up-to-date and accurate.

The implementation of an information management policy, the monitoring of compliance with this policy and the maintenance of an information governance system is a critical aspect of any organisation. By addressing this challenge head-on and in a structured manner, organisations can ensure that they have a robust and effective information governance programme in place.

4.6 Business challenges

One key business need is the need to ensure compliance with relevant regulations and standards. Organisations must comply with a variety of regulations and standards that govern the use of information. These may be general requirements like laws for commercial documentation, protection of personal rights, taxation regulations and others. There is always a selection of additional regulations for a certain industry. These regulations may create obstacles for effective business

processes, so information governance has to be implemented in a way that it does not put up roadblocks but instead facilitates an organisation’s business processes and goals. It must be easy to use and should work undetected in the background of software solutions. Failing to comply with these regulations can result in significant fines and damage to reputation, endangering business.

Correctly implemented information governance generates considerable business benefits. A strong information governance programme can help organisations improve their efficiency and productivity by making it easier to access and manage the information they need. Additionally, a robust information governance programme can help organisations protect their sensitive information from cybersecurity threats, which is critical in today's digital world. In order to realise these business benefits, organisations must have a clear set of business requirements for their information governance programme. This includes having a defined set of policies and procedures for the creation, storage, use and disposal of information, as well as the appropriate technology and resources to support these activities. Additionally, organisations must have a dedicated team of information governance professionals who are responsible for implementing and maintaining the programme and ensuring that it aligns with the organisation's business needs.

4.7 Ethical challenges

There are quite a lot of challenges when comes to automating information governance using artificial intelligence, machine learning and analytics. One of the key ethical challenges is the issue of privacy with respect to the EU General Data Protection Regulation (GDPR) and ePrivacy directive. Organisations have a responsibility to protect the personal information of their employees, customers and other stakeholders. This means that they must have clear policies and procedures in place for collecting, storing and using this information, and must ensure that these policies are in compliance with relevant regulations and standards.

Another challenge is the issue of access to information. Organisations must ensure that the information they hold is accessible to those who need it, but this can also raise ethical concerns. For example, some information may be sensitive or confidential, and may not be appropriate for certain individuals to access. This is typical of human resources data. It can also be a major issue for cloud solutions. Overall, ethical challenges are an important consideration in the field of information governance, and organisations must address these challenges in order to ensure that their information governance programme is ethical and in compliance with relevant regulations and standards.

4.8 Software and technology challenges

Software and hardware is used – on premises, in the cloud or in hybrid solutions – to create, capture, manage, provide, control and archive digital information. These can be stand-alone, integrated or a mix of heterogenous solutions. To govern all of these systems systematically is a big challenge in implementing and maintaining information governance. Implementing information governance for isolated, “island” systems makes no sense because overarching control is necessary. It is only when

all systems are under one roof in terms of the information governance approach that an organisation is truly compliant.

Software and related hardware – not the other way round – are necessary to ensure the integrity, usability, accessibility, longevity, preservation and overall management of the organisation's information. This means ensuring that the information is accurate, complete and up-to-date, and that it is protected from unauthorised modification or tampering.

To address this challenge, organisations must have the appropriate software and technology in place to manage and protect their information. This may include tools such as data quality and integrity-checking software, as well as technologies that enable the tracking and auditing of changes to the information. The same refers to the usability of the information. It must be easy for users to access and use. This may include tools such as search engines, data visualisation software and other technologies that enable users to quickly find and use the information they need. This includes good accessibility for users with disabilities that allows barrier-free access, a key concept. A major issue is ensuring information accessibility and usability over time, which we address below.

4.9 Preservation challenges

One of the key challenges for information governance is the need to manage digital preservation and long-term archiving. In our digital age, the amount of information available is constantly growing, together with a myriad of different formats. If information is to be stored over decades, the systems, formats and metadata used to access it will be a problem if these means of access, formats and data processing capabilities are not constantly checked. Information governance policies must address the issue of technological change and anticipating necessary measures in advance. Archiving or preserving information is a key issue for compliance as well as the quest to save knowledge, so one goal of information governance is to maintain the value of information over time.

Measures may include constant migration of applications, databases and stored information objects. Obsolete formats can be transformed into long-term archival formats. Metadata can be enriched to create more value and better use information. By addressing the challenges related to digital preservation, records management and archiving, organisations can ensure that their valuable information assets are properly managed and preserved in the long term.

4.10 Knowledge management challenges

Digital information stored in an organisation’s repositories is only of value if it can be used as knowledge for business processes. Therefore, information governance and knowledge management

are closely related yet different concepts. The goals of information governance are often controlling information, restricting access, documenting the use of information, and so on. Knowledge management, on the other hand, refers to the process of creating, sharing, using, leveraging and managing the knowledge within an organisation. Knowledge is often based on unstructured information and lost in places like the C drive of a personal device. To create value through knowledge management, all of an organisation's information must be universally accessible.

Information governance has to provide and control access to information via knowledge management. It has to make sure that the information used by employees is correct, complete, up-to-date, authorised and suitable for the intended use. Information governance has to safeguard the integrity, accessibility and security of the knowledge base. The organisation must have the appropriate tools, systems and interfaces in place to combine the two poles of information governance and knowledge management.

5 The future of information governance

In this section we address three of the many major trends that are having an impact on information governance.

The future of information governance ***El futuro de la gobernanza de la información***		
	English	**Spanish**
1	Distributed systems and the cloud	Sistemas distribuidos y la nube
2	Automation	Automatización
3	Artificial intelligence, analytics and machine learning	Inteligencia artificial, análisis y aprendizaje automático

Table 8. The future of information governance

5.1 Distributed systems and the cloud

The future of information governance is closely tied to the ongoing development and adoption of distributed computing environments. In these environments, organisations have a large number of distributed systems, which can be located in the cloud, on-premise or in hybrid solutions. This can make it difficult to manage information governance effectively, as it is no longer possible to manage systems and information manually.

One of the key challenges of information governance in distributed environments is the sheer number of systems that must be managed. As organisations increasingly rely on distributed systems

to support their operations, the number of systems in use is likely to continue to grow. Another challenge in distributed environments is the diversity of systems in use. Each system may have its own unique set of policies and procedures for the creation, storage, use and disposal of information, which can make it difficult to ensure overall governance, integrity and security. Additionally, these systems may have overlapping functionalities, which can lead to confusion and inefficiency.

A third challenge is the need to use a variety of different administration tools. Each system may have its own administration tools, which can make it difficult to manage and coordinate these systems' activities. This can again lead to inefficiency and inconsistency, as different systems may have different policies and procedures for the management of information.

In the future, information governance will only be able to work sensibly if all administration tools are harmonised. The real challenge is when organisations have no way of changing SaaS administration tools or integrating these into their tool landscape. Information governance has to take into account the fast-paced changes that hardware and software infrastructure undergoes. Therefore, the goal for information governance policies is no longer to be stable and static, but flexible and easily adaptable to technological changes. This is a completely new concept for information governance policies, which need constant checks and reliable change processes of their own.

Distributed systems may lead to "distributed" information governance, where only quality, security and other basic standards remain the same.

5.2 Automation

Information governance can no longer be set up and maintained manually. Automation is key for future IG endeavours; to be "future-proof", IG must be automated.

There are different areas of process automation, and it is critical that these comply with information governance policies. Most automation processes are still manually coded and governed by predefined rules. New automation technologies are changing this paradigm.

- **Infrastructure**
  The base is always a governance infrastructure, which endows all systems of an organisation with basic features like electronic signatures, encryption, master data management, an authorisation directory, audit trails, storage, monitoring, etc. The assignment of such tools can be automated, even as a background operation invisible to the user. The task of information governance is to monitor and control the use of these services and allow the tracking of all transactions. For backbone processes it is necessary that all information governance measures be automated to keep track.
- **Capture**
  The use of these infrastructure capture processes can be automated. By scanning analogue documents and using OCR, image processing and enhancement, metadata extraction, classification and storing can easily be automated, at least partially. The same technologies can be used for emails and other office documents, with metadata extraction, classification and storing following the same rules and quality standards as scanning. Applications provide

their information readily indexed with metadata and classified. This allows us to create a universal data entry process for most types of information objects. Information governance standardises and controls these processes.

- **Workflow**
  With business process management (BPM), workflow tools evolved to become the backbone of information management software infrastructure. BPM provided rules and audit trails, which in turn helped to enable and automate effective information governance. With new tools like robotic process automation (RPA), BPM's reign over processes and information has ended, and the creation of workflows has been democratised – every user can create its own workflows. Together with ad hoc workflows in collaboration software, this has represented a great improvement for users but has been hell for information governance. Automation is needed to once again take back control of these processes. The more process management becomes automated, the more information governance will have to become automated as well.
- **Ordering and visualisation**
  Automated indexing and classification carry out the function of assigning an information object to a certain branch of a classification scheme or file plan, to a defined process or to one user or a group of users. This allows us to display information in an inbox, virtual folder or workflow as an item. The wide array of options for visualisation, prioritisation, personalisation and individualisation can only be controlled by automated software. To assure consistency and correctness, these processes require monitoring, checking and logging by information governance tools. If these processes are to be automated, information governance itself must be automated.
- **Records management**
  The declaration of records, their attribution with metadata and their classification can all be automated. Checking the accuracy and quality of this process is a major task for information governance applications. Comparison with thesauri, existing master data in applications and logic review, together with the storage process and assignment to certain workflows, are important information governance software features. Automated translation, added context information, assignment to the correct user group and enrichment of information from other sources make using records easier. All these processes for handling records are subject to strict information governance procedures and documentation.
- **Archiving**
  The process of moving records and other information to a long-term archiving repository can be completely automated when all necessary metadata are collected throughout the lifecycle of the information object. Information governance functionality must assure that archived information can no longer be changed or manipulated, secure the integrity of the information base, and provide audit trails and journals which prove the authenticity of the stored information objects. The disposition process can also be automated in a controlled information governance environment. Expanding the concept of information governance to include an overarching model for all an organisation's information, these automation tools can be used beyond the archival environment. To work with big data, these information governance tools have to be automated.

The automation of information management as an idea is playing an increasingly important role in the field of information governance. The actual automation of information, however, is lagging behind. This creates gaps in an overarching information governance concept and risks for information security and protection.

5.3 Artificial intelligence, analytics and machine learning

Artificial intelligence (AI), natural language processing, intelligent information retrieval, machine learning and analytics create new possibilities for automation and therefore have a significant impact on information governance. These technologies provide efficient tools for managing a growing amount of information while also offering a chance to improve information governance.

Access to information changes dramatically with the introduction of context-sensitive searches and chatbots. Agents will evaluate existing repositories and come up with ordering structures, classification schemes, file plans and self-organised virtual folders. Existing processes will be monitored, analysed and automatically improved, streamlined and re-created with new machine-generated processes. Retrieving information will result in the right information being automatically provided at the right time to the right addressee. Standard tasks inside the organisation, as well processes, communication and interaction with customers, business partners and the public, will be handled by intelligent software. The field of possible application scenarios is already immense. Artificial intelligence will penetrate or replace all applications.

Information governance will be forced to keep up with this development. It has to make use of these features to develop self-learning algorithms of its own to be able to control self-learning, deep learning and machine learning systems. This can no longer be done manually. Code will have to be analysed if it is compliant with the established rules of information governance policies. The execution of self-generated applications will have to be controlled by self-adapting information governance software. Audit trails will have to adapt automatically to changing environments. Looking at the previous sections of this article, there is little doubt that we have a great deal to do in regard to automation and the use of AI.

There are some additional benefits when automating information governance with AI. Process documentation will be generated automatically. AI will identify and correct errors and improve the overall quality of information. AI extraction and analysis tools will preserve the value of information. Automated tools will strengthen the implementation of information governance within the organisation. Users will no longer have to worry about compliance while working when this is supported by intelligent automation. Risks will be discovered and reported by artificial intelligence, and big data analysis will help to make use of the huge information pools. It will support compliance and the extraction of all information with relevance to certain cases. AI-based business intelligence will help to make more informed decisions and improve overall performance. AI and deep learning will simulate and test processes to improve their governance.

The impact of artificial intelligence, analytics and machine learning on information governance is complex and multifaceted. While these technologies have the potential to greatly improve the efficiency and accuracy of information management, they also bring potential challenges and risks that must be carefully considered and addressed.

In regard to future information governance principles, the use of AI, analytics and machine learning should be seen as an opportunity, not a risk. In fact, AI will lead to the creation of new principles that will redefine the scope of information governance. Other, older principles will be automated as standard and will fall into oblivion. This could be perceived as a risk in the future implementation of AI-based information governance, but the people responsible for archives, records management and information management must open their minds and welcome these changes.

6 Summary

There are many definitions and sets of principles for information, governance, information management and information governance. It all comes down to managing the increasing amount of digital information, making proper use of information and staying in control of information.

Information governance refers to the management of the availability, integrity and security of information within an organisation. It encompasses the processes, policies and practices that are put in place to ensure that information is properly collected, managed and used. Information governance is not a policy document on a shelf but is rather alive and well in day-to-day work and transactions.

The importance of information governance lies in its ability to protect the organisation from risks associated with the mishandling of information. This includes risks such as legal liabilities, loss of data and damage to reputation. By implementing effective information governance practices, organisations can ensure that their information is accurate, complete and secure, which can help to improve decision-making and protect the organisation from potential harm.

Today, it is no longer a question of whether you need an overarching information governance system – it is an absolute must. It is important to recognise that information governance is not only about systems and solutions but also people, so that they make sure to apply all information governance measures during their work day.

ISO 24143:2022 on information governance is a useful, up-to-date standard for educating about and designing, implementing and maintaining effective information governance.

There are quite a lot of challenges to information governance's implementation and maintenance – and these challenges are compounded by the progress of automation, artificial intelligence, machine learning and big data analytics. These advances in technology in no way mean we can overlook the human factor, but they are a chance to establish improved information governance. Adequately used

they help us keep track of all the new software properties, distributed and cloud environments and self-generating functionalities. It has become evident that information governance no longer can be managed manually and must itself become automated.

7 Literature

Footnotes

[1] ANDERSON, J. B.; JOHNNESSON, R. *Understanding Information Transmission*. Piscataway: Ieee Press, 1996. ISBN 9780471711209.

[2] FARNSWORTH, N. R.; THOMPSON, B. S. *The Nature of Mathematical Modeling*. Cambridge University Press, 2006.

[3] WALKER, C.; KAMPFFMEYER, U. "Information Governance - Grundsätze, Bedeutung und Prinzipien". *PROJECT CONSULT Newsletter 20131022* [online]. 2013. <https://bit.ly/3vKnUVy>

[4] BEVIR, Mark (2012). Governance: A very short introduction. Oxford, UK: Oxford University Press. ISBN 9780191646294; HUFTY, Marc (2011). "Investigating Policy Processes: The Governance Analytical Framework (GAF). In: WIESMANN, U., HURNI, H., –24.

[5] KOVACICH, G. L.; BONI, W. C. *Digital Governance: The Intersection of Technology and Public Sector Management*. CRC Press, 2015.

[6] KAMPFFMEYER, U. "Information Management". *PROJECT CONSULT Blog* [online]. 2016. <https://bit.ly/2PyJIly>

[7]Techopedia. "Information Management (IM)" [online]. 2017. <https://www.techopedia.com/definition/20012/information-management-im>

[8] KAMPFFMEYER, U. "Information Management". *PROJECT CONSULT Blog* [online]. 2016. <https://bit.ly/2PyJIly>

[9] KAMPFFMEYER, U. "Nur Information Management oder Intelligent Information Management?". *PROJECT CONSULT Newsletter 20190615* [online]. 2019,. <https://bit.ly/3WWxVuH>

[10] KAMPFFMEYER, U. "Information Lifecycle Management (ILM)". *PROJECT CONSULT Blog* [online]. 2015. <https://bit.ly/3lytd1Z>

[11] KAMPFFMEYER, U. "Information Management & Information Governance". *PROJECT CONSULT Blog* [online]. 2013. <https://bit.ly/3QnH1y6>

[12] Association for Intelligent Information Management (AIIM). "The Fundamentals of Information Governance" [online]. 2013. <www.AIIM.org>

[13] Association of Computer Science and Information Technology (IACSIT). "Information Governance: Concepts, Strategies, and Best Practices", 2014.

[14] Wikipedia. "Information governance" [online]. <https://en.wikipedia.org/wiki/Information_governance>

[15] ISO 24143:2022. Information and documentation — Information Governance — Concept and principles [online]. <https://www.iso.org/standard/77915.html>

[16] KAMPFFMEYER, U. "GRC als ganzheitlicher Ansatz". *PROJECT CONSULT Themen* [online]. 2015. <https://bit.ly/3CzRKjw>

[17] ISO 24143:2022. Information and documentation — Information Governance — Concept and principles [online]. <https://www.iso.org/standard/77915.html>

[18] ISO 24143:2022. *PROJECT CONSULT Blog* [online]. 2022. <https://www.project-consult.com/news/iso-241432022/>

[19] SMALLWOOD, R. "5 Key Ways the New ISO Information Governance Standard Can Have an Impact" [online]. 2022. <www.LinkedIn.com>.

[20] ISO 15489-1:2016. Information and documentation — Records management — Part 1: Concepts and principles [online]. Revised 2021. <https://www.iso.org/standard/62542.html>

[21] Association of Records Managers and Administrators (ARMA). "The Principles" [online]. https://www.arma.org/page/principles

[22] European Commision. "Shaping Europe's Digital Future" [online]. <https://digital-strategy.ec.europa.eu/en>

Additional literature

BLOKDYK, G. *Information governance: Deployment and Administration*. CreateSpace Independent Publishing Platform, 2017. ISBN 978-1977722324.

DE HAES, ST., VAN GREMBERGEN, W., JOSHI, A., HUYGH, T. *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organisations.* Springer; 3rd ed., 2020. ISBN 978-3030259174.

ELIN, P., RAPAPRT, M. *A Government Librarian's Guide to Information Governance and Data Privacy*. New York: Business Expert Press, 2022. ISBN 978-1637422434

ISO 24143:2022. *Information and documentation — Information Governance — Concept and principles* [online]. 2022, <https://www.iso.org/standard/77915.html>

KAMPFFMEYER, U. "Information Management Compliance". *PROJECT CONSULT Whitepaper* [online]. 2007. <https://bit.ly/3vTAfXn>

KAMPFFMEYER, U. "Information Governance". *PROJECT CONSULT* [online]. 2013. <https://d-nb.info/1267861622/34>

SAFFADY, W. *Information Governance: Concepts, Requirements, Technologies.* Overland Park: ARMA International, 2017. ISBN 978-1936654765

SMALLWOOD, R.F. *Information Governance - Concepts, Strategies and Best Practices*. Hoboken: Wiley, 2nd ed., 2019. ISBN 978-1119491446

WILDHABER, B. (Ed.) et. al*. Information Governance: A Practical Guide - How to regain control over your information*. 2017. ISBN 978-3952443033

Ulrich Kampffmeyer

Ulrich Kampffmeyer (born 1952) holds a PhD, a magister artium, a diploma in prehistory and informatics, and a master in information technology. He is founder and managing director of the German consultancy PROJECT CONSULT Unternehmensberatung Dr. Ulrich Kampffmeyer GmbH, in Hamburg (https://www.PROJECT-CONSULT.com). He has been working in the field of information management, electronic archiving, records management, information governance and enterprise content management for 40 years. He has worked on pattern recognition, expert systems, image processing and software for prehistoric and early historical research at research institutions (FhG IITB) and universities (Kiel). A strategy advisor for over 30 years, he has been involved in numerous implementation projects for information management and information governance. He has been a member of various standardisation groups such as MoReq and is internationally known as a keynote speaker.

His curriculum can be found on the German Wikipedia: https://de.wikipedia.org/wiki/Ulrich_Kampffmeyer.

In the German blog on his website he covers current topics regarding information management and governance (https://www.project-consult.com/blog-news-newsletter-diskussion-discussion-project-consult-unternehmensberatung/).

In his public knowledge base, "Essentials" (https://project-consult.theum.com/essentials/index.htm), he offers information and publications from his 30 years of activity as a consultant.