«Mindset Information Governance»

Information Governance
Swiss Infosec AG, Sursee

October 2022, Version 1.00

October 2022, Swiss Infosec AG, RZ
Version 1.0, K_SIAG_Mindset_Information_Governance_en_00.docx

Swiss Infosec AG
Centralstrasse 8A
6210 Sursee

Tel +41 41 984 12 12
infosec@infosec.ch
www.infosec.ch

Beratung & Schulung
Informationssicherheit
Datenschutz
IT-Sicherheit
Krisenmanagement
BCM

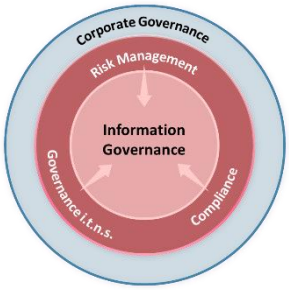
Luzern
Bern
Zürich
Berlin

«Mindset Information Governance»

Information governance: opportunity and challenge in one

Many organisations manage their information and digital data not as well as they could: data is sometimes duplicated, data cannot be found or can only be found with difficulty, accessibility according to level and function is not guaranteed, data stored in different locations contradict each other, employees cannot assess whether the data is up to date, employees do not trust the data or legally prescribed deletions cannot be carried out. This is where the "Mindset Information Governance" comes in handy, a thought and organisational approach for the appropriate implementation of information governance within the company.

Against the backdrop of information super-inflation, advancing digitalisation and the increasing value of "good" information, the "information governance mindset" quite rightly calls for a holistic approach to managing and processing information.



Impact of GRC on information governance as part of corporate governance.

Information governance aims to manage and optimise the processing[i] of information across the organisation based on policies, guidelines and directives. Information governance is a holistic approach to managing corporate information through defined processes, roles, controls and metrics, all of which consistently treat information as a valuable business asset.

Information governance provides the framework for the secure, confidential and legally compliant handling of information, which enables the respective company and its authorised employees to process information in a targeted, efficient and effective manner in accordance with its confidentiality, availability and integrity requirements for the best possible fulfilment of tasks and achievement of economically optimal results. Information governance is therefore also concerned, for example, with the economic efficiency of information processing, with the user-friendliness of the procedures used to process the information and also with the question of which employees should have access to which information.

Information governance represents a strategy for maximising the value of the information processed in the company and for minimising the resources, costs and risks associated with the processing of this information. In this context, the company's information is regarded as both value- and cost-bearing. Accordingly, requirements for control, monitoring and coordination are demanded at the highest management level.

Information governance can also be seen as the process of managing the security and usability of the information handled by the respective organisation, based on binding specifications for the handling of information. Information governance also ensures the consistency, reliability, trustworthiness and prevention of misuse of the information processed.

Information governance as part of corporate governance

The term governance comes from the French governer, "to administer, to lead, to educate", often translated as leadership, and generally refers to the control and regulation system in the sense of structures (organisational structure and process organisation) of an organisation.

Corporate governance is the legal and factual framework for the management and supervision of companies for the benefit of all relevant stakeholders. This regulatory framework is largely determined by the legislator, any regulators and the owners (shareholders). The concrete design is the responsibility of the board of directors and the company management. The company-specific corporate governance system consists of the totality of all relevant laws, guidelines, codes, declarations of intent, corporate mission

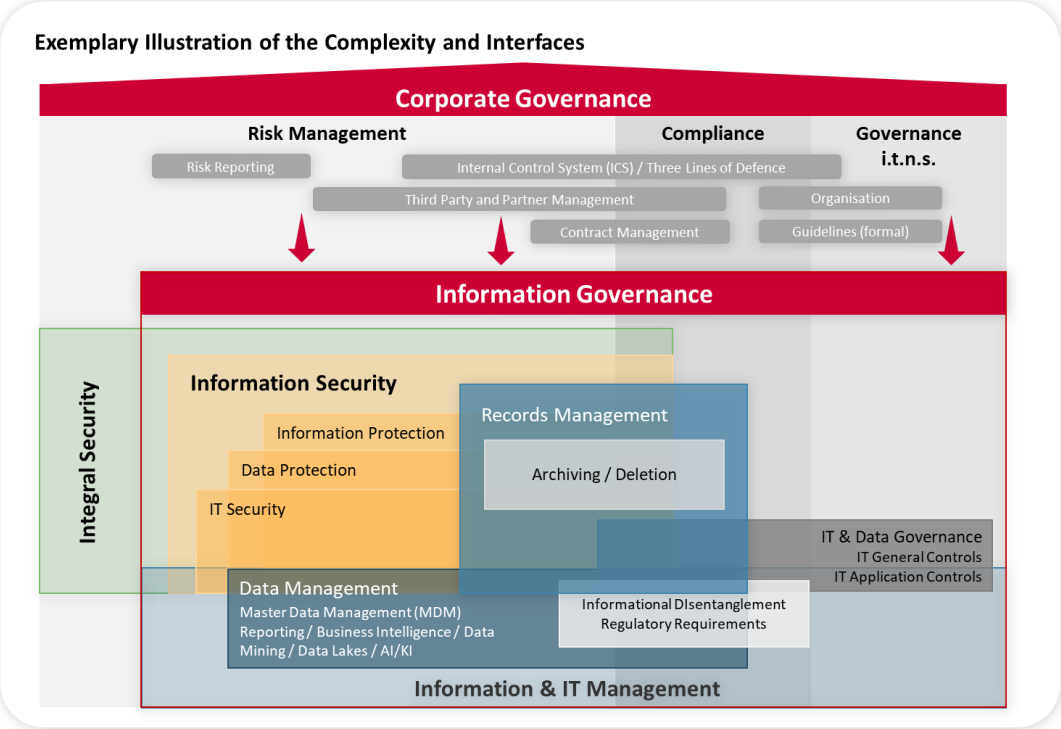
statement and the practice of corporate management and supervision.

Corporate governance is very complex and includes mandatory and optional measures: observing laws and regulations (compliance), following recognised standards and recommendations, and developing and following one's own corporate guidelines. Another aspect of corporate governance is the design and implementation of management and control structures. Good corporate governance ensures responsible, qualified, transparent management geared towards long-term success and is thus intended to serve the organisation itself, its owners, but also external stakeholders (financiers, sales and procurement markets, society, citizens) (source Wikipedia).

The abbreviation GRC has generally developed for the three sub-areas of corporate governance: Governance, Risk and Compliance (see for example Swiss GRC AG).

Information governance is in ourview an important and strategic part of corporate governance. Information governance must not and cannot be part of IT governance. Assigning information governance to IT governance would further strengthen the false belief that IT is responsible for a company's information. Responsibility for a company's information belongs in the business and in the line. This is also one of the main goals of information governance: to clearly regulate the responsibilities for a company's information.

The more extensive the processing of information is in absolute (volume) or relative (proportion) terms within an organisation, the more important and urgent it is to actively address the opportunities and challenges associated with information governance.



Information Governance - Overview of Topics: The "Mindset Information Governance" does not represent a target picture, but rather an exemplary localisation and representation of the areas or projects frequently encountered in corporate practice, some of which operate as isolated solutions. The diagram is intended to show the complexity of the issues involved in information governance and their interfaces. We would be happy to support you in identifying, locating and evaluating the sub-areas of information governance that actually exist in your company.

Information governance issues

Information governance is thematically linked to the processing of information or to information in and of itself. In terms of terminology, information governance thus goes much further than, for example, IT governance or data governance, which focus exclusively on digitally stored or processed data and represent a sub-area of information governance.

Integral security, understood as the bundling of all security sub-areas of a company, only partially overlaps with information governance. On the one hand, not all security sub-areas deal with information as the central object of protection in information governance. Nevertheless, all security sub-areas must comply with or support the procedural requirements of corporate governance or the areas of governance, risk and compliance. This includes, in particular, any procedural requirements regarding the

management of risks, such as the categorisation of risks or damage and probability of occurrence.

Here, another great opportunity of the "Information Governance" mindset becomes visible. The clear allocation of a topic to information governance opens up the possibility of implementing the requirements and procedures of the GRC area more directly and efficiently. This is often associated with stronger support for the line functions that are more experienced in these procedures.

All activities in the area of **information security** are directly related to information governance. Information security should achieve appropriate **c**onfidentiality, **a**vailability and **i**ntegrity of the information processed and the functions, systems and processes used to process it. Public administrations in particular, such as the federal administration, supplement the protection goals of information security with the term "traceability". The overlapping areas of **data protection** (processing of personal data), **IT security** (digital processing or digital instruments) and **information protection** (confidentiality of proprietary information, "classified" information) form part of information security according to doctrine and practice.

According to doctrine, **data protection** also represents a sub-area of information security. However, due to the increasing density of regulations and the associated rising risks in the area of data protection, this area has become independent in many places. An assignment of data protection to the topic of information governance would be desirable. This would also provide a corresponding organisational proximity to the areas of records management, information security and compliance.

Archiving, understood as the legally compliant storage of information objects according to internal and external specifications, is often assigned to information security. One of the reasons for this is that the mechanisms for achieving the legally required protection from falsification of the archived material are very well known in the area of IT security. Archiving, however, is 'only' the second last step (before deletion) in the higher-level records management process. Records management in and of itself is not part of information security. In practice, this leads to difficulties in classifying **records management**. As mentioned above, deletion is the last step in the records management process. However, it is precisely this deletion that is now all too often demanded by data protection - independently of an existing records management - and implemented in individual cases. In order to achieve reliable and beneficial deletion processes, the author believes that it is urgently necessary to establish and implement appropriate records management processes. Deletion concepts must not remain islands of data protection.

With regard to archiving, records management and data protection, information governance offers an opportunity. The topics can be assigned more directly, clearly and comprehensively. This results in good and level-appropriate solutions.

Goals of information governance using the example of a medium-sized company

Maximise the value of the organisation's own resources by ensuring that data is kept secure and confidential, properly and lawfully obtained, accurately and reliably recorded, effectively and ethically used, and appropriately and lawfully shared and disclosed.
The following measures are implemented to protect information assets from all threats, whether internal or external, intentional or negligent:

- The information is protected from unauthorised access.
- The confidentiality of the information is guaranteed.
- The integrity of the information is preserved.
- The information is supported by data of the highest quality.
- The regulatory and legal requirements are met.
- Business continuity plans are created, maintained and tested.
- Information security training is provided for all employees; and
- All actual or suspected breaches of information security are reported to and investigated by the Information Governance Officer.

Implementation of the "Information Governance Mindset"

When developing the specifications in the area of information governance, at least the following points are to be regulated or referenced:

- Definition of the principles and guidelines applicable in the area of information governance
- Ensure close, also formalised, cooperation between Risk Management, IT, Legal and Compliance, Records Management, Integral Security, Information Security and Data Protection with the objectives: Minimising information risks and maximising the value of information
- Clarification of tasks/competences/responsibilities regarding the following functions: Governance, Risk, Compliance, Information Governance, Information Security, Data Protection, IT Security, Information Protection, Records Management, Archiving, Data Governance, etc. Creation and maintenance of appropriate guidelines in these areas
- Establishment of records management, including data protection-compliant archiving and deletion/disposal

- Information access policy that specifies exactly who may access information/data of which areas/categories under which circumstances and how this access is to be protected as a minimum
- Policy on the secure use of information, which specifies precisely which security measures the user must comply with when processing information
- Policy on the use of processing systems (internal, external, cloud, site, etc.) depending on areas/categories

Advantages of information governance at a glance

- Reduction of the risks associated with the creation, use and disclosure of corporate data
- Reduction of legal risks associated with unmanaged or inconsistently managed information
- Higher productivity through data sharing
- Simplified legal compliance: The implementation of legal requirements is massively simplified by the order in the information and data, their categorisation and classification.
- Permitted storage locations are clearly defined and can be adequately protected, redundancies are reduced
- Information protection measures are defined, can be reviewed and continuously optimised
- Additional security measures can be implemented in a targeted, risk-based manner based on classification/need for protection
- Simplified access to up-to-date and trustworthy information
- Due to clear access specifications, decision-making processes regarding user access can be massively shortened
- Due to the limited retention period, administration and storage costs can be reduced

Conclusion

The topics covered by the "Mindset Information Governance" are often scattered in the companies and assigned to different areas. In many cases, the topics are incompletely addressed and/or the interaction of the topics is not ensured.
The above diagram, the "Mindset Information Governance", clearly shows the complexity and the multitude of interfaces. For the most part, these are topics that overlap and are finely interwoven with each other and accordingly require close coordination within the company.
The company's internal information governance should define overarching principles and principles in the sense of a bracket function and support their coordinated, seamless, step-by-step implementation across all topics. The interaction of important subject areas should be ensured. In this way, redundancies, resources and efforts can be reduced.
In practice, the responsibility for creating and maintaining information governance often lies with the top finance and compliance executives (CFO and CCO) and their teams.

We recommend that you address the "Mindset Information Governance" in an appropriately composed expert committee under the leadership of a C-level position with a analysis of the status quo and an action plan - with regard to the value of your information sooner rather than later.

[i] The definition of "processing" according to Art. 5 d nFADP (SR 235.1), applicable from 1 September 2023: any handling of personal data, regardless of the means and procedures used, in particular the obtaining, storing, keeping, using, modifying, disclosing, archiving, deleting or destroying of data.