ARMA INTERNATIONAL Swiss Chapter

Newsletter 2021-01

Welcome to the ARMA Swiss Chapter News

Dear Information Governance Professional,

Even though it's the most discussed topic we won't talk about COVID-19. However, we will not miss wishing you all the best for 2021 and above everything else "Stay healthy!".

Information Governance is as important as it was, and it would be wonderful to see it on more companies' top priorities for 2021. In Switzerland, the updated Data Privacy Law will soon be enacted and, without a strong information governance in place, there is little chance to become compliant.

In the deep-dive topic of this newsletter we would like to initiate a discussion about what criteria to apply when deciding to keep or not to keep information. The dilemma between over-retention, complying with data privacy regulations, reducing storage costs and ensuring destruction holds are observed, is a constant challenge for all people in charge of information governance. Enjoy the reading!

We are looking forward to having you as active participant in the Swiss Chapter contributing to the discussions around Information Governance,

Board of ARMA Swiss Chapter

Next Events (final dates will be communicated in due course)

- *25 March 2021, virtual meeting (including General Assembly)*
- *24 June 2021*
- *30 September 2021*
- *16 December 2021*

Contact us! Visit our Website!

info-pro@armachapter.ch
http://www.armachapter.ch
Twitter: @armaswisschap

All Newsletters are published and accessible on the website.

Hot Topics from the Chapter

- ***ARMA Swiss Chapter-only Membership***

  It entitles the member to join all chapter events and receiving news and collateral materials issued by the chapter. It does not include any services granted by ARMA International. The yearly fee is CHF 50.00. If you are interested in becoming a local member, please apply online on the ARMA Swiss Chapter Membership page.

- ***Quarterly Meetings and General Assembly***

  Depending on the rules to be followed we will decide for each of the quarterly meetings whether it will be physical or virtual. As a member you'll be notified via e-mail.

- ***ARMA International and European Region***

  The ARMA Swiss Chapter board is, together with representatives from the UK, in contact with ARMA International head quarter to collect information about the strategy and plans on how the ARMA European region would be supported and developed.

- ***ARMA annual conference 2021***

  Nothing has been published on www.arma.org yet.

Deep Dive and Knowledge Transfer

To keep or not to keep?

How to make a sound decision on what to keep and what to dispose?

by Guy Rom, LL. B, member of the ARMA Swiss chapter board

Neither legal and regulatory obligations nor cost should be the only drivers for information governance!

In many organizations the predominant driver for establishing Information Governance is to become and stay compliant with laws and regulations. Of course, this newsletter does not aim at suggesting being non-compliant. However, similar as you would reduce your speed when driving your car on a non-familiar country road at a rainy night, you may want to base your decisions about how strictly laws and regulations are being followed in Information Governance on the risk you are prepared to carry e.g., when deciding whether to keep information longer than required by law. But it may as well be that you would decide to shorten the retention period after having weighed the risks against the benefits.

Laws and regulations shall not be the only drivers when implementing Information Governance. There are other important reasons to keep information, e.g., product liability, business processes, product development, business continuity.

This newsletter aims at showing an approach on how to evaluate the organization's information to come to an educated decision about what to keep for how long, and ultimately, to create a retention schedule.

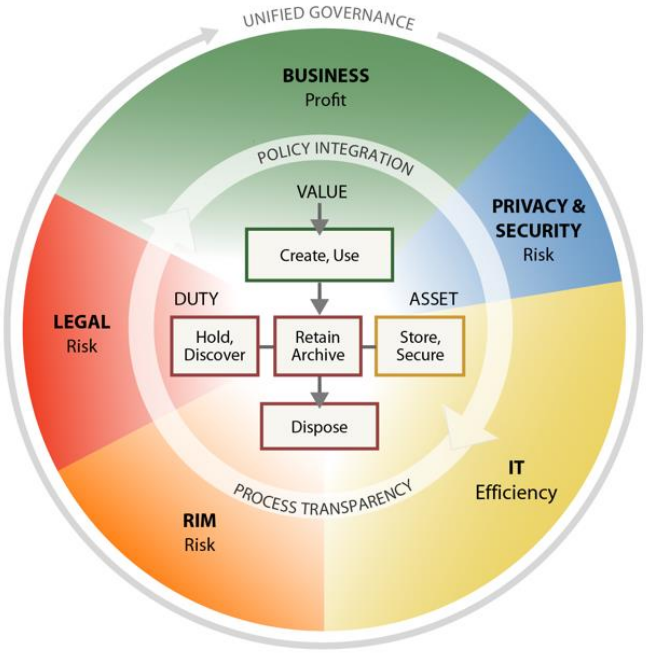
Information Governance Reference Model as navigator

Similar as in earlier newsletters the Information Governance Reference Model (IGRM) can be used as guide to evaluate the topic in detail and from many angles:

Regarding the specific information the model differentiates between

- *Duty: Legal obligation for specific information*
- *Value: Utility or business purpose of specific information*
- *Asset: Specific container of information*

In addition, we have the various stakeholders and interest groups with their main drivers "profit", "risk" and "efficiency» covered. And not to be left out is the information lifecycle in the center of the model, always in focus when making decisions about how to handle information from "cradle to grave".



Information Governance Reference Model © 2012 / v3.0 / www.edrm.net

Decisions are required all along the information lifecycle by the stakeholders in charge

Phase in Lifecycle	***Aspects influencing decision to keep or not to keep (not conclusive, but meant to initiate further analysis)***	***Stakeholders involved ****
Create / Receive	*Two cases have to be differentiated:* *a) Known type of information (similar information was received or created before):* *Classifying information according to retention schedule and application of defined and agreed retention rules including stricter rules if classified as record.* *b) Unknown type of information (first time in organization), e.g. created in a new process, related to a new product or received for the first time from outside of the organization:* *Deciding about classification and what retention rules must be applied. Decision about classification as record (incurring stricter controls) or information if such differentiation is made.* *Any information which cannot be classified must only be kept for a short period (e.g. maximum of 12 months) and be disposed of as soon as possible, ideally in an automated way.*	*Business*
Use	*a) Evaluation of business need to determine whether the information is still required in an active business process. E.g., the information could have been updated, a draft version of a document could have changed into a final document. Where the former version has no value as evidence it should be disposed of as soon as possible.* *b) Creation of copies should be prevented and, if it cannot be avoided, be controlled to ensure no duplicates are kept unmanaged. Working copies are to be marked as such and be disposed of as soon as possible, ideally in an automated process.* *In case confidential information or personal data is included, special measures, e.g. as required by GDPR, are to be applied.*	*Business / Privacy & Security*
Hold / Discover	*a) Legal is in charge to maintain an up-to-date list of information which is in scope of destruction hold. A hold may have been issued related to an anticipated or ongoing legal matter or based on laws and regulations (e.g. in the financial industry in Switzerland for dormant accounts).* *b) Information has to be organized in a way allowing to efficiently hold information, i.e. it must be able to efficiently identify all information objects in scope of a hold instruction.* *c) A decision per information type about "hold by copy" or "hold in place" must be made upfront. Processes and systems must be designed and implemented to support the decision made.*	*Legal*
Retain / Store / Secure	*a) Every type of information identified to be retained has to be evaluated and categorized e.g. regarding data protection, information security, access control, number of concurrent users, cross-border restrictions, immutability of storage device.* *b) From an IT operation's perspective, the technology used and the related costs and ecological impacts like energy consumption, would be in focus. Rarely accessed information should be identified and handled differently from information which is looked up daily or even more frequently.* *Business Continuity Management (BCM) including periodic backups of IT systems must not be considered as substitute for having information governance implemented.*	*RIM / IT*

Phase in Lifecycle	**Aspects influencing decision to keep or not to keep (not conclusive, but meant to initiate further analysis)**	**Stakeholders involved ***
Archive	*An archive is a more secure and more regulated place where information (and especially records) is kept for a defined period. Access control and distinct legal or regulatory requirements which are in general wider than what would have to be applied on other storage must be observed. Where the decision to archive is based on specific triggers, these should be determined and become part of the retention schedule.* *a) Business to identify those types of information needed to perform process steps or as source for future activities and developments and to document the organization's history.* *b) Legal to provide guidance on legal and regulatory obligations which are to be followed and identify types of information which would be subject to these stricter rules.* *c) Personal data (e.g. in accordance to GDPR) has to be evaluated separately in case it shall be archived. Restrictions on how long personal data can be kept by an organization apply and, if e.g. for historical reasons, a longer retention is required than the original purpose to collect the personal data asked for, anonymization or pseudonymization may have to be considered.* *d) From an IT perspective an evaluation of the best suitable storage systems, e.g. ensuring immutability, extended access control and the longer retention period, would be required. However, this would take place not on an information type level but for the organization in general.* *Ideally the identification of types of information which shall be archived occurs in the phase "create/receive" already.*	*Business / Legal / RIM / Privacy & Security / IT*
Dispose	*Over-retaining information bears the risk of data leakage and can substantially increase the costs of discovery e.g., in the context of legal matters. In addition, it may impact the efficiency of business processes if it is not possible to easily identify the accurate information required to perform the process.* *An organization should define principles regarding defensible disposal of information and get the principles signed off by the higher management to avoid endless discussions resulting in over-retention and inconsistent application of the disposal process.* *Such principles could be:* *a) Retention schedule defines when to dispose of information. Exceptions from the retention schedule are only accepted in the context of a destruction hold instruction issued e.g. by Legal.* *b) Disposal according to the retention schedule does not require explicit sign off by business or management or the information owner.* *c) Types of information not listed in the retention schedule, i.e. which are not classified, have to be disposed of e.g. within 12 months.* *d) Disposal process is to be automated whenever technically feasible.* *e) Per type of information the method of disposal should be determined when added to the retention schedule. Available and accepted types of disposal have to be defined as applicable company standards and e.g. be based on commonly accepted standards as the "Guidelines for Media Sanitization" NIST 800-88.*	*RIM / IT*

** In the ARMA Swiss Chapter Newsletter 2018-03 we elaborated in more details on the various stakeholders and their responsibility. Please find the newsletter on the ARMA Swiss Chapter webpage.*

Organizational setup and processes

An interdisciplinary team should be in charge to perform a risk assessment on the types of information and decide what types of information would have to be kept. They would as well define how to classify the type of information and what retention rules (defined in the retention schedule) would have to be applied.

Leadership should be assumed by RIM (Records and Information Management). However, the classification process should be initiated by business representatives (information owners) when receiving or creating a new type of information. Depending on the criticality of the type of information (e.g. involving personal data or business sensitive information) further stakeholders would have to be involved in the risk assessment.

The involved stakeholders would be asked to assess every type of information by answering following questions (ranges should be used instead of exact numbers when estimating the impact):

- *What is the value of the information type considering the organization's past, presence and future?*
- *What does it cost (time, resources, effort) to keep the information?*
- *What is the potential impact (legally, financially etc.) of not having the information available?*
- *What compromise would be possible e.g., regarding the retention period or the methodology and technology of how the information is kept? Can the organization afford the compromise?*

Stakeholders would evaluate the risks by applying a standardized questionnaire and provide their risk rating (e.g. in a heatmap). Whether to keep the type of information and, if yes, for how long, should be decided based on the consolidated rating.

Risk categories to be considered are listed below. The final list of criteria and the rating scale would have to be defined considering the business context of the organization.

- *Financial risks* — *Potential costs of not keeping the type of information … or not long enough / cost savings resulting from not keeping the type of information*
- *Reputational risks* — *Potential risk if type of information is kept but should not be kept, or vice-versa*
- *Legal risks* — *Potential risk of being incurred in a lawsuit if not keeping the type of information or not keeping it long enough; probability to have to apply a destruction hold on the type of information*
- *Operational risks* — *Potential business impact if type of information is not kept and available e.g. for performing processes, developing new products or as evidence*

All types of information would have to be evaluated based on the risk catalog including, by application of a standardized rating scale, the assessment of the severity and likelihood of a potential incident. However, the more regulated the industry is, the less "room for optimization" may exist.

Based on the results a consolidated assessment would be performed by considering the various ratings. Its outcome is reflected in the retention schedule which then would be used by the organization.

The risk assessment and the resulting retention rules should be periodically reviewed. Any stakeholder should be allowed requesting changes based on their role and responsibility, e.g. by legal in case of changing laws and regulations or by business if an information type is not anymore received or created. A standardized change process led by RIM should be deployed and followed across the organization.

Having an up-to-date retention schedule which is available and known to everyone in the organization is a pre-requisite for a successful information governance. A classification must be determined by the business owners of the information and defined such that everyone involved in processing the information can find and apply the respective retention rules.

Conclusion

Keeping everything is as little a solution as keeping nothing, hence, none of both can be recommended.

However, establishing retention rules based on a risk assessment by all relevant stakeholders and considering the business value of the information can lead to get a broader support to "live" information governance and to not reduce information governance to a constant debate about costs and legal obligations.

Note/Disclaimer: *This Newsletter is the author's view only.*