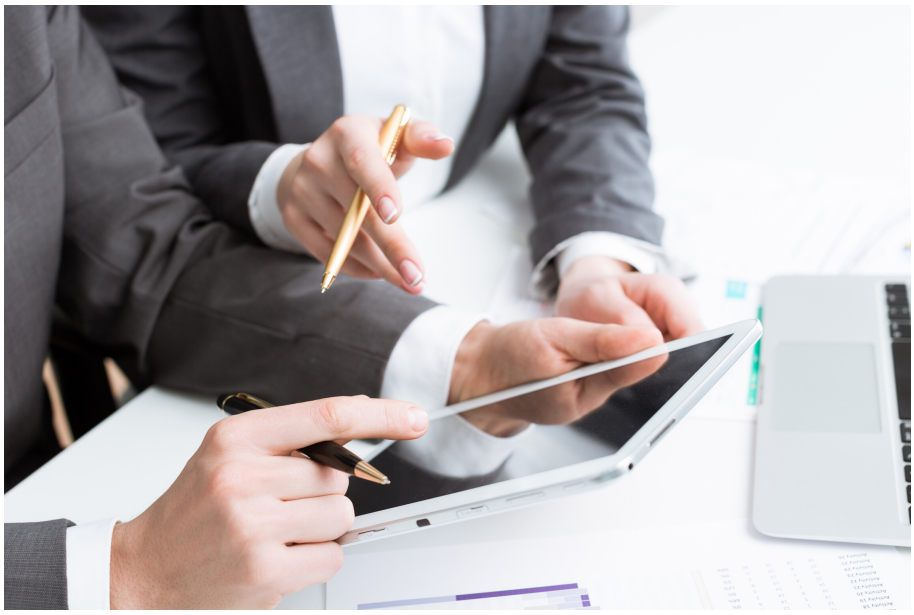
The Challenge of Balancing Information Access Demands and Risk Management Throughout the Information Lifecycle



As consumers, we have become accustomed to having information on just about everything available at our fingertips. That expectation has carried over into the workplace, too, where our employees, customers, and business partners alike have an increasing expectation *and need* for near-instantaneous access to information. Balancing these access needs against the requirements to manage information compliantly and to make sure it does not fall into the wrong hands can be a challenge, and it is a challenge that must be managed *throughout the information lifecycle.*

This article explores some of the consequences of information getting into the wrong hands or not getting into the right hands at the right time and in the right form. It examines some of the factors that make managing risk and access demands a challenge. For a more in-depth discussion of these topics, as well as some steps to consider when implementing an approach to ensure appropriate information access throughout the information lifecycle, download the free ARMA International white paper developed in conjunction with Hyland, *How to Balance Information Access Demands and Risk Management Throughout the Information Lifecycle*, or view the webinar by the same name.

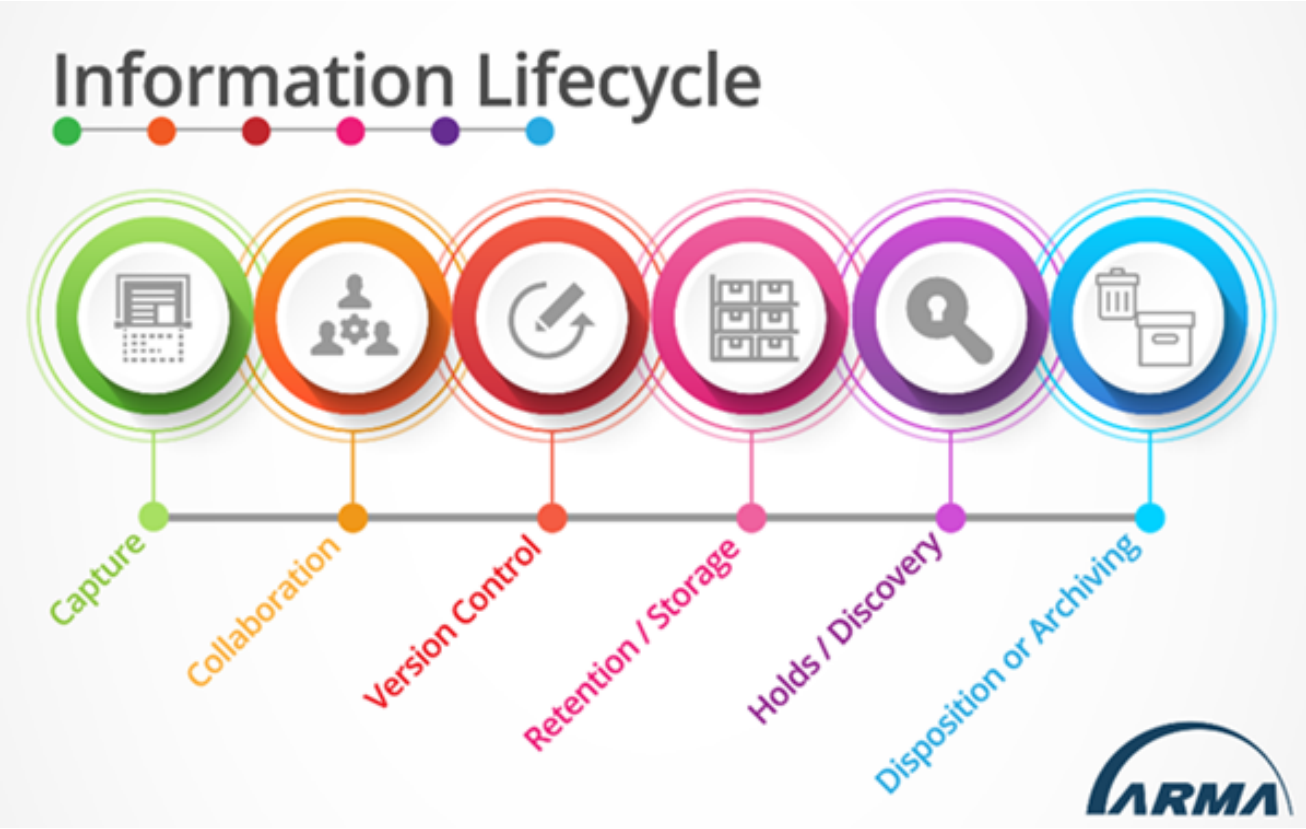
The Consequences of Information Getting into the Wrong Hands

With a major data breach in the news seemingly every other week, organizations are giving more attention to the dangers of information getting into the wrong hands. Information exposures can be the result of intentional bad actors or accidents, and threats can come from outside the organization or from within. Organizations may have an obligation to report and could face a series of costly repercussions, depending on the nature and sensitivity of the information exposed. They may face consequences, including:

- Lawsuits/investigations and associated legal and other support costs
- Legal judgements, settlements, or fines
- Remediation cost to fix the problem that caused the breach
- Damage to reputation
- Lost revenue
- Loss of business opportunities

How severe the above consequences are depends upon the specifics of the case, including what and how much information was exposed as well as how the organization behaved before, during, and after the incident.

An organization that does not have a clear understanding of where its information is, in particular its especially sensitive information, cannot properly secure that information at the various stages through the information lifecycle and may find itself scrambling during a breach trying to understand just what was exposed. Risk and security needs can also change throughout information's life. For example, during information's more active phase, securely sharing it may be a major concern, whereas later in the lifecycle secure storage and eventually disposition may be the primary focus. Information can be exposed at any point from the moment it is created/captured until its ultimate disposition, and so organizations must manage the risks associated with its getting into the wrong hands – risks *that exist throughout the information lifecycle*. (See infographic of the Information Lifecycle for reference.)



An organization that does not have a clear understanding of where its information is, in particular its especially sensitive information, cannot properly secure that information at the various stages through the information lifecycle and may find itself scrambling during a breach trying to understand just what was exposed. Risk and security needs can also change throughout information's life. For example, during information's more active phase, securely sharing it may be a major concern, whereas later in the lifecycle secure storage and eventually disposition may be the primary focus. Information can be exposed at any point from the moment it is created/captured until its ultimate disposition, and so organizations must manage the risks associated with its getting into the wrong hands – risks that exist throughout the information lifecycle. (See infographic of the Information Lifecycle for reference.)

Getting the Correct Information into the Right Hand at the Time it's Needed

Like risk and information security concerns, access demands are requirements that must be addressed throughout the information lifecycle, too. Of course, those access demands are likely to change over the course of a given piece of information's life within an organization.

During the earlier phases of the lifecycle in which information's use may be more active and dynamic, issues like collaboration, sharing, mobile access, version control, etc., may be at the forefront in the minds of information users. But ready access to information, getting the correct information into the right hands when it needs to be there, applies throughout the information's entire life — until disposition through deletion (if this applies). An information user responding to an audit, inspection, or discovery request needs timely access to the right information to support the overall business objectives of the organization, too.

Challenges to Managing Risks and Access Demands

As discussed above, balancing access demands with risks and security is critical. But, striking the right balance is a challenge: the balance needs to fit a specific organization's needs and be tailored to meet its business needs, the legal and regulatory environment in which it operates, and its risk tolerance. The following are a few factors that add to this challenge:

- *Complexity of the Legal and Regulatory Environment*: Consistent application of legal and regulatory requirements is a challenge because of their volume, complexity, and variations in jurisdiction, and because they change so often.
- *Complexity of the Information Environment*: Managing information risk and access demands over the information lifecycle is further complicated by the fact that information can live and move between a myriad of applications, systems, and platforms (e.g., in a small organization there could easily be dozens; in a large organization that could number in the hundreds). Information users must navigate this complexity to find the information they need. Further, in each system (and its movement between systems), risk of inappropriate access must also be managed.
- *Volume of Information*: Handling increasing volumes of information can also add to the challenge of managing risks and access because the sheet volume can quickly outstrip the ability of information users to manually capture or classify information for these efforts.
- *Human Factors*: Human beings can further complicate managing risk and access demands, often unintentionally. If employees are not fully enabled to access information they need to do their jobs, they often resort to work arounds like using existing technology in a way that exposes information to risk (e.g., removing a document from a secured system and emailing it) or resorting to so-called "shadow IT" (e.g., uploading documents to an unsanctioned, third-party file-sharing system).

Learn More About Balancing Access Demands and Risk Throughout the Information Lifecycle

To learn more, download, *How to Balance Information Access Demands and Risk Management Throughout the Information Lifecycle,* a free white paper developed by ARMA International in conjunction with Hyland or view the webinar by the same name.