How to Take Your IG Program to the Next Level with Continuous Auditing and Analytics

Introduction

Information governance (IG) is not a once and done effort. IG is an ***overarching*** and ***coordinating*** strategy for all organizational information from the moment it enters an organization ***throughout*** its life. (See ARMA's definition of IG). Unfortunately, information-related efforts are often executed in silos or as point-in-time/one-off efforts — an arguably more tactical approach.

IG, however, is a ***strategic*** approach to handling information. This paper will explore how **continuous auditing and analytics** can be part of an effective information strategy and IG program and how, by identifying policy deviations and data inconsistencies ***in real time***, it can help take your IG program to the next level. This approach can reduce the costs, financial and otherwise, of information becoming non-compliant, and can save time, money, and other resources by focusing stakeholder attention on exceptions requiring human intervention.

This paper will discuss:

- Why a siloed or point-in-time/one-off approach is a problem, including some common examples of this approach.
- What is meant by continuous auditing and analytics?
- How details gathered during two common IG-projects can be leveraged to develop the business rules necessary to help build a continuous approach.
- How continuous auditing and analytics can be used to monitor and improve compliance, identify and correct data inconsistencies in real time, improve efficiency, reduce the need for one-off cleanup efforts, and gain insight into your data.

Information Governance: Is the overarching and coordinating strategy for all organizational information. It establishes the authorities, supports, processes, capabilities, structures, and infrastructure to enable information to be a useful asset and reduced liability to an organization, based on that organization's specific business requirements and risk tolerance.

— ARMA Guide to the Information Profession

The Problem: Siloed & Point-in Time/One-Off Approaches to Information

So-called "siloing" is an all too familiar challenge to the effective governance of organizational information. Commonly, information-related actions can be siloed in different departments or functions of an organization, with one area of the business not knowing what the other is doing — leading to inconsistent or duplicative efforts or worse — serious compliance issues. Information-related actions can also be temporally isolated from one another through point-in-time/one-off efforts — needing to be redone at a future date when the problems they were intended to correct reoccur. Let's look at a few examples.

Have you encountered any of the following kinds of scenarios within your organization?

- **Example 1:** You just updated your policies and procedures and trained your employees regarding the handling of certain sensitive information (e.g., PII, social security numbers, credit card numbers, other sensitive information, etc.). But employees may not have fully understood the policy or, at any rate, are not complying. Perhaps, they are putting sensitive information into a non-compliant location, using it in a form it doesn't belong (e.g., unredacted/non-anonymized), or processing it in an inappropriate way (e.g., emailing sensitive, non-encrypted data).

- **Example 2:** You have just undertaken a massive data remediation project, cleaning up file shares and other data stores — removing R.O.T, moving sensitive files to compliant locations, properly classifying them, and applying appropriate security measures, etc. But people have resorted to the same bad habits that necessitated the cleanup in the first place. Now, your information is once again out of compliance, and you face a costly redo of the cleanup in the future.

- **Example 3:** You have just performed a data reconciliation as part of a routine, periodic reconciliation (a monthly, quarterly, yearly financial reconciliation, for example) or a one-off cleanup effort. But the same types of errors and inconsistencies are still cropping up. It's time for your periodic review again — a time-consuming, largely manual process perhaps involving countless hours of investigating the causes of errors, correcting them, and backing them out of systems. Or, as above, you face a redo of a major data cleanup.

If you have encountered these or similar scenarios, your organization may be guilty of taking a siloed or point-in-time/one-off approach to its information. This approach to information-related decisions and actions tends to be a more tactical than truly strategic approach to information.

- What if you could identify and correct policy deviations as they occurred?
- What if you could keep your information compliant, your stores tidy, and avoid a costly redo of the remediation in the future?
- What if you could catch and clean up errors and inconsistencies in real time, improve the quality and reliability of your information, and reduce the burden of manual reconciliation?

Continuous auditing and analytics can help you achieve all these goals, and more. It can help shift your approach to information from ***tactical*** to ***strategic*** as is the purpose of IG which is meant to be an overarching and coordinating strategy for all organizational information. By giving you clear, actionable insights into your information ***in real time***, continuous auditing and analytics helps you breakdown silos and realize the benefits of a truly strategic, lifecycle-approach to your organization's information.

What Is Continuous Auditing and Analytics?

Continuous auditing and analytics is a methodology — an approach to handling organizational information. It is a full lifecycle-approach essential to governing your information well because it informs you about the state of your information in ***real time*** (e.g., what it is, where it is, how it is being handled, whether there are discrepancies, etc.) so you can take appropriate actions against it at all points throughout the information lifecycle. While continuous auditing and analytics isn't a particular set of tech tools organized in a specific way, as a practical matter, effectively leveraging technology is an integral part of this approach given today's information volume and technology environment complexity. To understand what we mean by continuous auditing and analytics, let's begin by parsing the words.

First, continuous auditing and analytics is a ***continuous*** approach. That is, it isn't performed at a point-in-time but is on-going, in real time. For example, rather than reviewing accounts on some periodic basis (e.g., monthly, quarterly, yearly), information is reviewed continuously as it is created and captured and as it lives in various systems in your technology environment throughout its lifecycle. By ***auditing***, we simply mean the review of the information. To continue the accounts reconciliation example, an invoice arrives with some amount on it; its corresponding P.O. also has an amount listed. By auditing here, we mean reviewing the invoice and the P.O. to determine what they say. And finally, we are at the last part, of the methodology, analytics. By ***analytics*** we mean performing some sort of analysis on the information based on what you learned during the review and applying the appropriate business rules to determine what to do with it. Does the invoice amount match that on the P.O. or is there only a negligible difference? If yes, to either of these questions, then the invoice might simply move on to accounts payable. If the discrepancy is too large, however, it must be resolved.

Even this relatively simple example of reconciling an invoice with a P.O. begins to show the value of this approach. By moving the identification of

the discrepancy ***upstream*** in the process, the error is caught in real time and corrected before the invoice moves downstream to accounts payable and possibly gets paid in error. Investigating the sources of discrepancies, backing data out of systems, and chasing down money paid out can be time-consuming efforts.

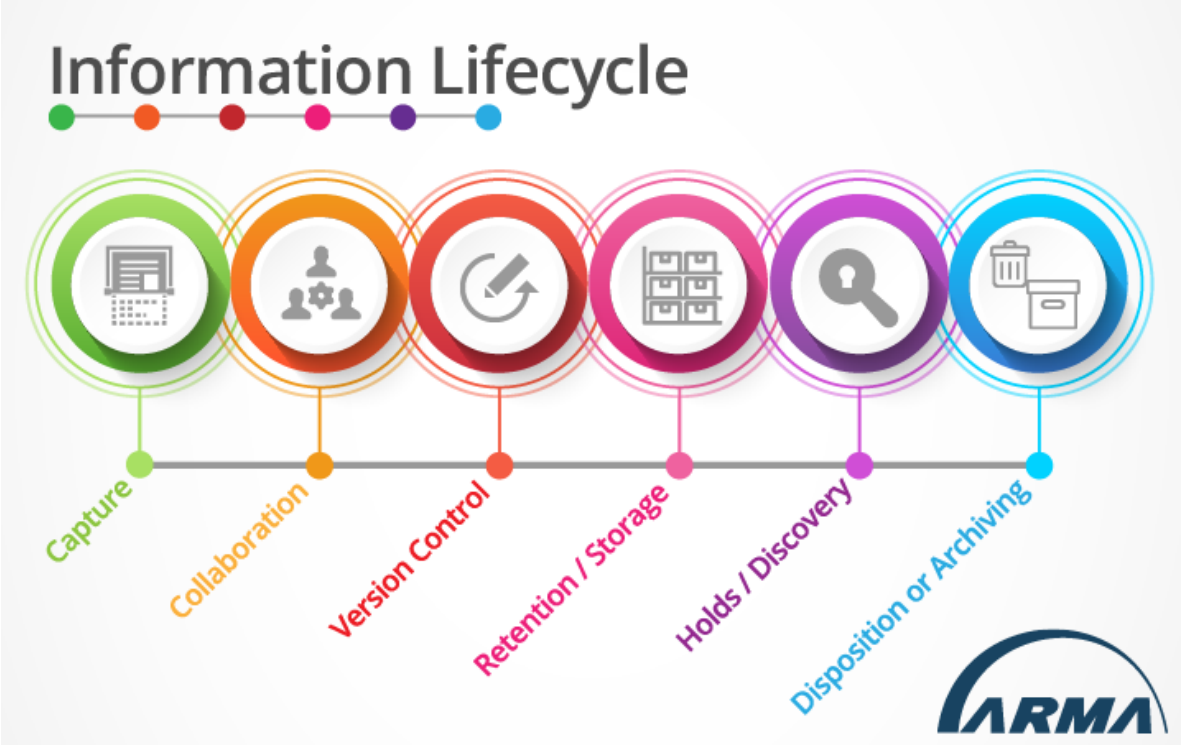
Theoretically, in an extremely simple information environment, one might be able to achieve something close to a continuous auditing and analytics approach without the assistance of technology. With enough personnel, information might be able to be manually marshalled through an organization and checked for accuracy and compliance along the way. The sheer volume of information with which even small organizations contend, makes this approach impracticable. Add to that the complexity of information ecosystems, with a myriad of applications, systems, and storage locations, and it becomes readily apparent that technology must be leveraged to achieve a continuous auditing and analytics approach.[1] It simply isn't possible for human beings to manually assess all of an organization's information throughout its lifecycle to ensure that information is in the right hands, in the right form, at the right time.

The next section looks at two common IG scenarios — information classification and information reconciliation tasks and how what is learned in those projects can be used to build a continuous auditing and analytics approach.

1. Even small organizations can have dozens of applications, systems, and storage locations. For large organizations, the number can easily be in the 100s.

Information Lifecycle: Right Place, Right Form, at the Right Time

IG is the overarching and coordinating strategy for all organizational information (See ARMA's definition of IG above). To ***fully*** enable information to be a useful asset and reduced liability, it must be effectively governed across the organization and throughout its entire lifecycle — from the moment it enters the organization and from the moment it is created and captured (see far left side of the Information Lifecycle graphic) through final disposition by deletion or archiving. That means having the right information, in the proper form (e.g., redacted, correct, etc.), at the right place, at the right time, and conversely, making sure information is ***not*** in places or forms it shouldn't be. On one side, it is findability, reliability, and usability of the information; on the other, making sure that it is being handled in a compliant manner. Continuous audit and analytics supports more effective IG because it provides real time insights into your organization's information rather than just at points in time. It allows issues to be addressed proactively.



What Can Be Learned from Two Common IG Scenarios to Build a Continuous Auditing and Analytics Approach

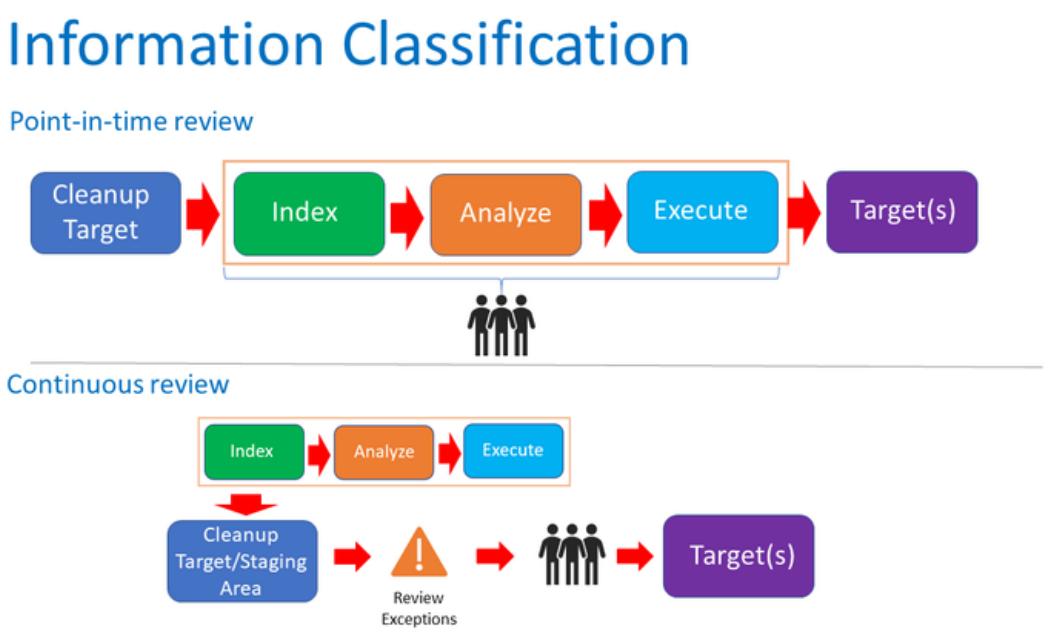
Two common tasks with which most IG professionals are likely familiar, and which are especially amenable to be improved upon with a continuous auditing and analytics approach are information classification and information reconciliation type tasks.

Information Classificiation

Information classification is used generally here to mean answering the question of ***what*** the information is to determine how it should be handled. For example, once it is determined ***what*** a piece of information is, it can be labeled (e.g., Is it trade secret, confidential, PII, etc.?) so that it can be assigned proper security protections (e.g., access controls or redaction). Determining what the information is guides decisions of where it belongs (e.g., Does it belong in a specific system of record or is it R.O.T. that should be deleted?).

Remediation projects are a common example of this type of information classification task (See graphic below). In this type of project, a data store needs to be cleaned up for some reason(s). For example, is the data store filled with redundant, obsolete, or trivial information (R.O.T.) that should be deleted; does it contain information that should be put in a separate repository or system of record where it can be appropriately managed and maintained; does it contain sensitive information that is being maintained in a non-compliant manner (e.g., non-redacted or without appropriate access controls)?

As shown in the graphic, in this type of project, once the target or targets to be cleaned up are identified, the information is then processed to



understand ***what*** it is. Generally, this involves indexing content and looking at the metadata. The indexed information and metadata can then be analyzed to determine what gets done with the information as determined by known business rules or ones that are elucidated during this process. For example, specific types of documents may need to be moved to their proper system of record (e.g., all contracts get moved to a contract management system), sensitive information may need to be secured (e.g., sensitive information is moved to a location where access controls can be managed or content is redacted or masked for certain viewers), or R.O.T. needs to be deleted. Technology can be leveraged during this to reduce manual efforts; this could include the use of tools that can be trained to recognize certain types of documents or extract data fields or flag sensitive information based on data patterns or words. The analysis part and final execution of the business rules against the information require lining up the appropriate stakeholders who are both familiar with the information and can approve the steps to be taken against it. The final target could be deletion, a system of record, or data lake. The specifics of the project will vary depending on the information and a specific organization's business rules, but the overarching remediation process is the same.

A problem with these types of remediation projects is that original targets of the cleanup project often become messy again, with the same

types of issues that necessitated the cleanup in the first place, and the remediation needs to be redone. This isn't an issue of tidiness alone, but is very often one of compliance, too.

Continuous auditing and analytics can be used to move the steps in the orange box (indexing, analysis, and execution) ***upstream*** to the original target of the cleanup or even in a staging area before. An information classification project like remediation provides you a lot of insights into your information, including what it is, where it is, existing compliance issues, the business rules you need to apply to remediate it, and which stakeholders in your organization need to be involved in the process as you move it upstream.

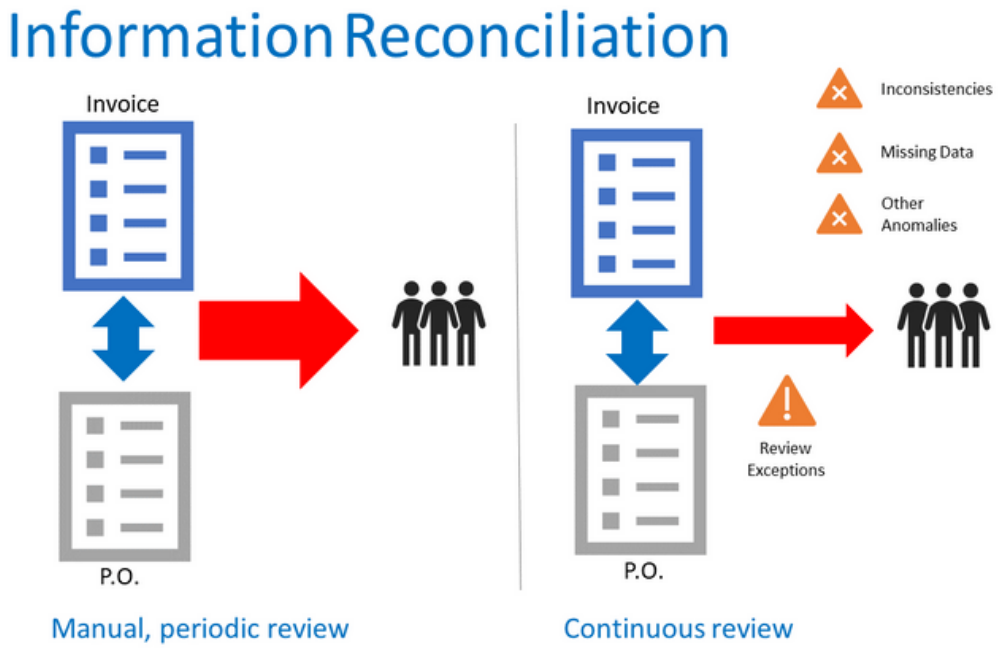
By using the same types of tools used during remediation to identify what the information is and the same business rules that determine what should be done with it, the information can be immediately processed as it is created and captured, keeping information stores clean and information compliant. If information is easily analyzed by the technology being used, it may be possible to automate some steps of execution. In other cases, human review may be needed. Exceptions requiring human intervention can be set to trigger an alert and a workflow to process them immediately before they become downstream issues. The business rules and stakeholders identified during the remediation process can be largely repurposed to establish the business rules and reviewers ***upstream***. Catching issues earlier prevents expensive redos later, keeps information compliant, and may even add efficiencies by limiting the need for human review to just the exceptions. In addition, indexing of your information can be repurposed for other uses like search or e-discovery. Take full advantage of what you learn in each of these projects to get a clearer view into your organization's information through its entire life.

IG Programs Need Both a Cleanup and Go-Forward Approach
Even if an organization is relatively new, it is likely that some of its information is out of spec or non-compliant and a cleanup of information stores may be necessary. But to avoid the costs of redoing these efforts later and the risks associated with information being out of compliance, a go-forward strategy must be married to the cleanup approach. Whichever approach you start with, cleanup or go-forward, you will almost certainly be able to repurpose the information you learned to the other side of this two-pronged approach.

Information Reconciliation

Information reconciliation tasks involve comparing information in two or more sources against one another or against a standard to identify any exceptions or errors and then correcting those discrepancies. Checking an invoice against a P.O. or checking other financial records at some fixed period are examples with which most are familiar, but there are a myriad of other tasks that could involve comparison of information across systems. Information that requires manual entry of codes (e.g., numbers and letters) is highly error prone. Exceptions that might need to be flagged include missing data, deviations of a certain amount, mismatch across systems, or errors in format.

In the case of reconciling an invoice and a P.O. (See graphic below), ideally before passing it along to accounts payable, one would compare information on the invoice to the P.O. Then, based on the organization's business rules, would either pass it along for payment or flag an exception that must be corrected. This type of reconciliation task is particularly amenable to the continuous auditing and analytics approach. The information values are known and the business rules around them can be established. A deviation in amounts below a certain threshold, for example, might not warrant processing an exception, and the invoice should just be paid.



The point is, as with the remediation project above, the rules established during the point-in-time reconciliation can be used to build out the continuous auditing and analytics approach and move the process upstream to flag exceptions as they arise, in real time.

The business rules that would require an inconsistency to be addressed during the point-in-time reconciliation can be set to trigger an alert and to create a workflow for human review only when an exception is identified. As with the remediation example, the same stakeholders who would be involved in the point-in-time reconciliation may be the same ones to review the exceptions in real time. Allowing these stakeholders to focus on the exceptions reduces the volume of information to be reviewed.

Of course, information reconciliation tasks can be much more complicated than the invoice/P.O. example. Data could be being compared across dozens of systems; exceptions could be triggered by variance above a certain dollar threshold or because of other issues, including: non-financial mismatch, missing data, errors in data pattern (e.g., the distinct XXX-XX-XXXX pattern of a SSN). Indexing tools can be pointed a various information stores to scan and compare information values, and this information across multiple systems can be presented in a single "pane of glass" view.

There are other advantages of a continuous auditing and analytics approach, too, especially for alphanumeric data (e.g., batch or part numbers). Manually entering and manually reconciling this data is prone to error and extremely time consuming. It is also the kind of work technology can do ***better***, ***cheaper***, and ***faster*** than human counterparts. Flagging just the exceptions requiring human review based on the business rules saves a great deal of time and expense. Finally, continuously monitoring information in systems also increases its reliability (for example, checking data in a data lake against source data to make sure it is accurate).

Benefits of a Continuous Auditing and Analytics Approach-Taking Your IG Program to the Next Level

Reduced Cost

The above examples have already explored how continuous auditing and analytics can reduce costs by avoiding the expense of redoing a costly remediation or reconciliation project. The approach can also save costs by removing expensive manual steps, costly errors, or fines.

Increased Efficiency/Productivity

By focusing human intervention just on exceptions, continuous auditing and analytics can also dramatically save time and increase productivity. In addition to reducing the points of human intervention, this approach can also improve efficiency because errors caught in real time are often easier to resolve than needing to reconstruct the cause of the exception well after the fact.

Improved Compliance

Continuous auditing and analytics can be used to identify instances where people are not following policies, including putting information where it doesn't belong, failing to apply appropriate security measures and controls, or processing it in non-compliant ways. This knowledge can be leveraged to identify specific individuals who might require more guidance or to improve training more, generally. Also, as discussed above, by flagging and correcting exceptions in real time, information can be kept in compliance rather than falling out of compliance between cleanup efforts.

Increased Reliability /Trustworthiness of Information

By monitoring information and correcting exceptions in real time, through continuous auditing and analytics, the information in data stores can be relied on better because it is confirmed to be trustworthy.

Repurposed Insights and Analysis

Often the indexing is performed on information for one purpose and then that same information is re-indexed for another. A continuous auditing and analytics approach can help us think differently about our organizational information that can lead us to repurpose insights gained for one purpose and use it for another. For example, indexing performed for remediation or used to set up a continuous approach upstream can be repurposed for search and e-discovery.

Taking an IG Program to the Next Level

A continuous auditing and analytics approach can also advance an IG program's maturity. By providing real time insights into information, the organization can shift from a reactive posture to a proactive or even optimizing approach to its information.

Conclusion

This paper has discussed why a siloed or point-in-time/one-off approach to information governance is a barrier to optimizing the use of organizational information and taking a truly strategic approach. Through the lens of two common IG scenarios, it has explored how the business rules and information learned about organizational information during point-in-time/one-off projects can be leveraged to move processes upstream and provide insight into our inform and address exceptions in real time. Finally, it has presented some of the benefits of using a continuous auditing and analytics approach including how this approach can advance an organization's IG maturity level.

ARMA International is the community of records management, information management, and information governance professionals who harness the benefits and reduce the risks of information.

ARMA provides resources, education, certification, and unparalleled networking opportunities. We set the standards and best practices that you leverage to address your full information lifecycle. When it comes to managing an organization's most vital asset – information – ARMA has the comprehensive resources to secure your success.

ASG Technologies is an award-winning, industry-recognized and analyst-verified global software company providing the only integrated platform and flexible end-to-end solution for the information-powered enterprise. ASG's Information Management solutions capture, manage, govern and enable companies to understand and support all types of information assets (structured and unstructured) and stay compliant. ASG's IT Systems Management solutions ensure that the systems and infrastructure supporting that information lifecycle are always available and performing as expected. ASG has over 3,500 customers worldwide in top vertical markets including Financial Services, Healthcare, Insurance and Government. Visit us at ASG.com, LinkedIn, Twitter and Facebook.