WAVESTONE

IDENTITY AND ACCESS GOVERNANCE

FINALLY PROVIDING IDENTITY MANAGEMENT EYES AND EARS ON THE GROUND?

There can be no mistaking the fact that an Identity and Access Management (IAM) project is more than a simple IT project. It should be considered a true business transformation programme covering organisational design, business processes, human and IT resources.

Successfully addressing IAM can bring many benefits but its implementation often faces many challenges. Could Identity and Access Governance (IAG) provide the answer and assure the success of IAM projects?

WHAT CAUSES THE FAILURE OF IAM PROJECTS? WHAT IS THE RELEVANCE OF IAG?

Two major causes of such failures can be identified. Firstly, there is often a mismatch between the objectives of an IAM project and the resources allocated to meet it. This is often due to a specific set of reasons: lack of governance and cross-sponsoring, a strategic vision only encompassing medium-term business challenges, an overzealous desire for implementation and improvement over time.

Secondly, a lack of metrics and simple tools exposes the reality behind authorisation and the benefits or even the appropriateness of the choices made. It is this second issue that IAG must address. In addition, IAG must provide operational indicators to effectively co-opt the appropriate management and business line staff.

AUTHORS

PATRICK MARACHE
patrick.marache@wavestone.com

FLORIAN POUCHET
florian.pouchet@wavestone.com

WHAT IS IAG? WHAT FUNCTIONALITY CAN BE EXPECTED?

In simple terms, IAG (also referred to as Identity & Access Intelligence, Identity Analytics & Intelligence or Governance Risk & Compliance) provides a more detailed view of the data behind, and wider use of, IAM.

IAG is thus regarded as a type of "control tower", fuelled as much by quality policies and internal controls as by IAM and application data. Beyond controlling identity and access, IAG must also provide the means for advanced analysis, in addition to facilitating the implementation and tracking of remediation actions.

> « What is not measured is not improving. »
>
> E. DEMING

An IAG solution will therefore import all accounts and entitlements in order to compare them with business policies. By cross-checking against organisational frameworks, a more structured assessment of gaps and risks can be conducted.

IAG must therefore permit (as shown in the diagram):

- The consideration of all rules and enterprise business controls (toxic combinations of power, limited access to certain groups, certain timeslots ...);
- The correlation and presentation of operational IAM data and each application with respect to its policies;
- The organisation and tracking of remediation actions that are required to close identified gaps.

IAG therefore functions as a crucial component in ensuring the proper use of IAM systems and corrects relevant data to improve the perceived quality of the IAM service.

Furthermore, IAG provides a solid basis for a view of the current situation and raises awareness of the efforts that need to be made to maintain quality and assurance standards.

IN WHICH CONTEXTS IS IAG RELEVANT?

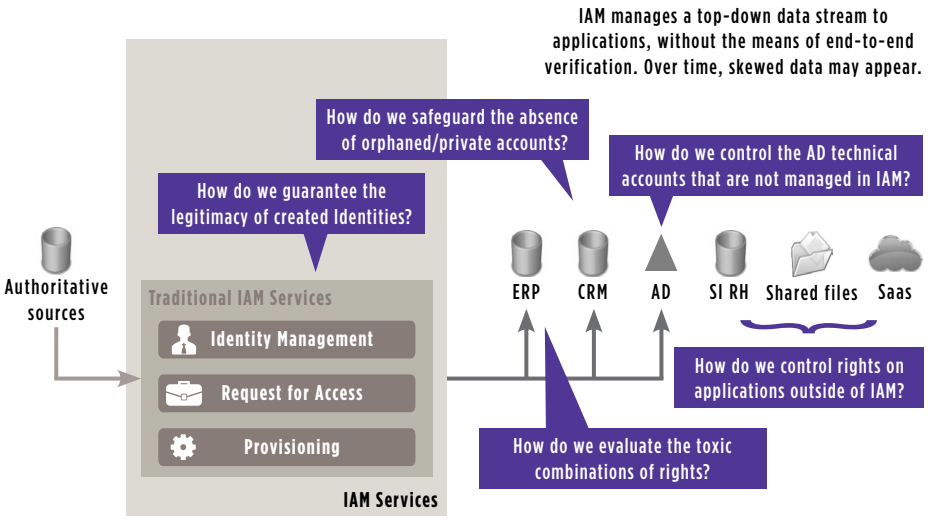
An IAG approach is equally useful for organisations that do not commit to an IAM approach as for those that have already begun to implement one.

For the former, IAG allows organisations to adopt a more operational approach, providing a more direct and immediate view of the current set of accounts and application rights.

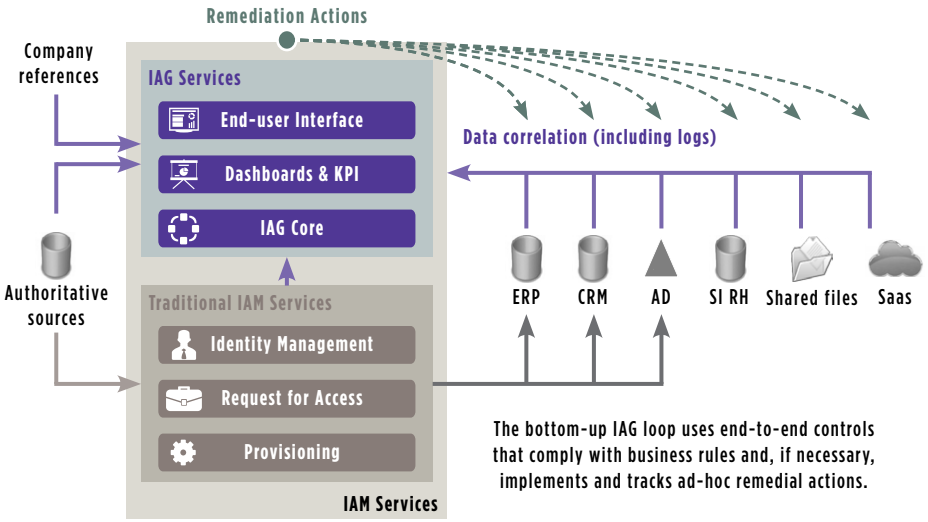
This bottom-up approach enables specific analysis to be performed which can be supported by examples. Business lines can take a simplified view of affairs and all components are brought together in the formulation of a more structured approach.

For organisations that have already begun to implement an IAM approach, numerous initiatives are hindered by an absence of use and quality monitoring indicators. This harms the «perceived quality» of the IAM service and is at its most detrimental in suspected cases of fault and during the associated investigation phases. IAG serves as a response to this lack of visibility.

Traditional IAM Services



IAG Services positionning



HOW DOES ONE ADAPT TO AND TAKE FULL ADVANTAGE OF THE PROJECT APPROACH?

In order to fully capitalise on IAG, the project approach should be adapted to its context.

It is possible to define four types of approach according to organisational objectives (managing risk or achieving operational efficiency) and the chosen analytical perspective (predefined rules or data analysis).

IAG projects often combine several approaches. Nevertheless, it is essential to not lose sight of the initial objectives. Let us consider a summary of these different approaches.

The "regaining control of the current situation" approach

This approach aims to substantiate the operational efficiency of IAM in comparison with predefined rules such as username format, naming convention of accounts or actual rights.

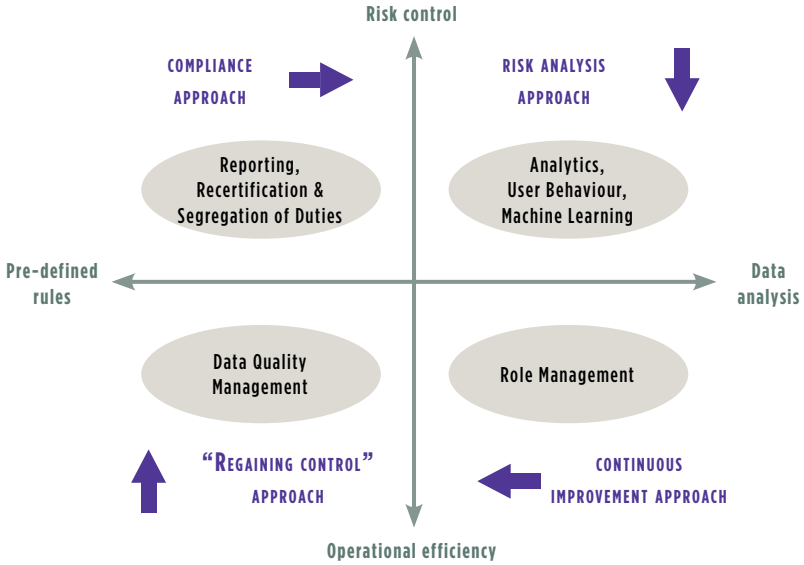
It is a data quality development process that compares actual data (accounts in applications) and the reference framework governing IAM (list of authorisation requests).

For organisations that do not adopt IAM services, this approach can ensure the successful completion of manual operations as well as detect and correct possible gaps that are introduced over time. Examples of this include:

- Typing errors in usernames,
- The erroneous allocation of rights;
- The non-deletion of an account in the event of a user leaving the organisation.

For organisations that own IAM tools, this approach ensures their proper function. In this context, IAG serves as a valuable aid during investigations of faults or user complaints. Indeed, IAG stores historical data on identities and access rights. It also raises an immediate alert if an identity has been altered, the reason for the alteration and the expected consequences.

What added value can be expected from these new features?



In summary, this approach enables organisations to effectively consider the implications of non-standard events such as a company purchase and a subsequent merger of identity bases treated by IAM through a technical lot and often without controls.

The compliance approach

The objective of this approach is to provide visibility of sensitive rights and ensure their compliance with internal rules and the regulatory framework of entitlements.

It is an approach that can be implemented irrespective of the existence of an IAM solution. It involves the reconciliation of actual rights of sensitive applications for comparison against company policies.

Several actions may then be considered, including:

- The removal of suspicious rights;
- The temporary waiver of requests;
- The recertification of the entitlements at risk;
- Or, if the rule is deemed unenforceable, the implementation of the necessary means for mitigation.

It is worth noting that IAG contributes to the audit process and signals the completion of a request for authorisation. This simplifies approval and certification processes and the management of workflows significantly, where progress against exceptions can then be monitored and reported during a subsequent review campaign.

In this context, an organisation must direct the focus of its efforts to either the "stock" aligning rights that have been previously assigned, or the "flow" of new requests for access rights. Indeed, by storing historical rights, IAG identifies new allocations of rights on a daily basis and triggers an ad-hoc process.

Providing it does not interfere with previously assigned rights, an approach focusing on the "flow" should be more straightforward to implement. The requests are recent and the approvers are still employed, making it easier to understand the context and reasons for such a request. It may also serve as a first 'quick-win' for the IAG project.

The risk analysis approach

This approach is built upon capabilities in data analysis and correlation and contributes to the overall approach towards risk management, particularly fraud. The objective of risk analysis is to identify potential risks without referencing previously established rules or preconfigured patterns of fraud.

Thus, the most innovative solutions will combine Big Data, Machine Learning and UBA (User Behaviour Analytics) approaches to detect «risky behaviours», or at least, those in disregard of the most common behaviours. A specific analysis of each alert is then necessary for distinguishing genuine fraud cases from their false positives.

Such analyses can detect a network directory «sweep», a potential clue of data leakage, or even risks of collusion if, for example, purchase requests are systematically approved by the same person within the validation committee.

These features can also be used following the occurrence of fraud. The analysis of historical data in such cases can facilitate an understanding of the fraud scheme, as well as identify clues and preliminary behaviours of fraud. This will lead to alerts being raised or the implementation of additional controls to avoid reproducing such patterns of fraud.

The continuous improvement approach

The continuous improvement approach provides the option of enhanced operational efficiency. It comprises the analysis and comparison of IAM practices observed on a daily basis with the objective of improving processes and the modelling of entitlements.

This can be understood through the following examples: two simultaneously assigned access profiles that combine into a single profile; profiles owned by less than 0.1% of users that can be removed or hidden; business profiles that no longer have access and profiles owned by more than 80% of a team which could be assigned to new joiners.

How long for an IAG initiative?

- Several weeks is a sufficient timeframe for the identification of threats and major inconsistencies that entitlements can cause;
- It can take several months to correct these gaps;
- However, IAG strategies should be developed over time in order to best position identity management as a sustainable approach for improvement.

On the basis of this evidence, it is a more straightforward exercise to win the support of business and application owners with the aim of progressing towards a more pragmatic situation.

This apparently complex approach may require a higher level of organisational maturity. In practice, however, IAG solutions are flexible enough to follow an empirical approach involving regular communication with business lines.

The purpose of continuous improvement is not to encompass everything. On the contrary, it is to focus on the most commonly visible and significant cases for everyday users.

IS IAG THE MAGIC FORMULA BEHIND SUCCESSFUL IDENTITY MANAGEMENT PROJECTS?

With advanced services in analysis and reporting, IAG finally provides a means for effectively measuring the success of identity management projects. Moreover, by tailoring the approach, valuable insights can be gained about business lines and management.

The Departments in charge of internal processes, quality or internal controls have a key role to play in sponsorship, taking on responsibility for IAG initiatives and guaranteeing their longevity over expected timeframes.

Several weeks is a sufficient timeframe for the identification of threats and major inconsistencies that entitlements can cause. It can take several months to correct these gaps, however, IAG strategies should be developed over time in order to best position identity management as a sustainable approach for improvement.

WAVESTONE

www.wavestone.com

Wavestone is a consulting firm, created from the merger of Solucom and Kurt Salmon's European Business (excluding retails and consumer goods outside of France)

Wavestone's mission is to enlighten and guide their clients in the most critical decisions, drawing on functional, sectoral and technological expertise.