The Business Case for IAM

By André Koot

To comment on this article, please visit our GitHub repository and submit an issue.

Table of Contents

Abstract

Businesses are under enormous pressure to deliver their products and services in ways that profit the company. Areas that do not directly bring in funding are often moved lower in priority, resulting in a competition for resources that can see internal projects in areas such as IAM struggle to succeed. Projects that move to the top of the priority pile in this competition are ones that provide a compelling business case. This article focuses on how to develop a positive business case for your IAM programs.

Introduction

Identity and Access Management (IAM) is often seen as one of many expenses that must be controlled within an organization. Businesses need to see the benefits of an IAM program before they are willing to invest in IAM programs. This circular demand can leave IAM improvements stuck in a never-ending game of catch-up. Businesses fail to see the strategic value in a solid IAM program until they see tactical improvements directly attributed to IAM services.

A solid business case helps break this deadlock by providing different perspectives on the overall Return On Investment (ROI) that IAM can bring to an organization. The best business cases include:

- the concept of the quantitative versus the qualitative components of the business case for IAM;
- the perspective from different IAM domains (e.g., internally facing IAM requirements from the enterprise, externally facing IAM requirements from the customers, cybersecurity requirements); and
- the recognition of the different strategic and operational requirements for both IT and the business.

Of course, different companies will respond better to different types of business cases. Some will be driven purely by the finances, while others will respond better by putting IAM in context with other services in an organization. Some may instead be primarily driven by the regulatory requirements governing their specific business operations (e.g., finance industry regulations).

Terminology

Term	Definition
Attribute-Based Access Control (ABAC)	Attribute-Based Access Control is a pattern of access control involving dynamic definitions of permissions based on information (“attributes” or “claims”), such as job code, department, or group membership.
Business to Business (B2B)	Business to Business processes in the field of IAM involve business partner access to company resources using some form of remote access (e.g., federated access).
Business to Consumer (B2C)	Business to Consumer processes in the field of IAM are customer or consumer access to company resources. In B2C, consumers manage their own identity in a CIAM. The company still manages access to the resources, using ABAC or PBAC methods for access control
Business to Employee (B2E)	Business to Employee, also called workforce IAM, includes managing identities and accounts for employees and contractors following an identity lifecycle.
Consumer Identity and	Consumer Identity and Access Management, or Customer Identity and Access Management, involves providing access to

Access Management (CIAM)	company resources through a digital identity managed by the customer.
Identity Governance and Administration (IGA)	Identity Governance and Administration is a discipline focusing on identity life cycle management and access control from an administrative perspective.
Joiner, Mover, and Leaver (JML)	The joiner/mover/leaver lifecycle of an employee identity considers three stages in the life cycle: joining the organization, moving within the organization, and leaving the organization.
Policy-Based Access Control (PBAC)	Policy-Based Access Control is a pattern of access control involving dynamic definitions of access permissions based on attributes (as in ABAC) and context for authorized access.
Privileged Access Management (PAM)	Privileged Access Management is a mechanism for managing temporary access for accounts with high-risk permissions. PAM often involves check-out and check-in of a credential generated for a single use.
Role-Based Access Control (RBAC)	Role-Based Access Control involves using roles at run-time to govern control access. It is a pattern of access control involving sets of static, manual definitions of permissions assigned to "roles," which can be consistently and repeatedly associated with users with common access needs.
Return on Investment (ROI)	Return on Investment is the economic measure of value of an investment, using costs, revenues, interest rates, and lifecycle as parameters.
Sunk cost	Expenses that have already been made in the past and that are unrecoverable.

Acronyms

C-level	Chief Executive Level, including Chief Executive Officer, Chief Financial Officer, Chief Information Officer, etc.
BC/DR	Business Continuity/Disaster Recovery
CI/CD	Continuous Integration/Continuous Deployment
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resources
IAM	Identity and Access Management
IT	Information Technology
ROI	Return on Investment
SSO	Single Sign-On
Y2K	Year 2000
ZTA	Zero Trust Authorization

Starting an IAM program

When working in IAM, the question often arises as to whether the costs and investments of an IAM program are worthwhile. Organizations generally ask for a financial business case since that is a traditional way to argue for an investment decision. It takes significant effort to convince decision-makers to look beyond the financial viewpoint.

Most IAM programs are started to solve one of three enterprise problems:

- Operations management (HR, IT)
    - for increasing employee efficiency, enhancing data quality, and cost-effectiveness[i]
- Enterprise, IT, or security architecture
    - for aligning with current best practices such as new controls for API access, support for Zero Trust, and supporting multi-factor authentication along with resolving issues of technology debt
    - for realizing newly defined strategic business initiatives, such as implementing a Consumer IAM (CIAM) strategy for revenue generation, improving customer services, and easing digital transformation[ii]
- Chief Executive Level (C-level)
    - for responding to audit findings in a management letter or directives from a supervisory agency or as the result of a security incident or data breach[iii]

Regardless of where the IAM program starts, a lot of money will be required from multiple cost centers before the program is complete. It often takes several budget cycles and significant organizational commitment to realize an effective IAM initiative. The program's sponsors must be prepared to make a business case to justify the organizational effort and the financial costs. Even if the C-level initiates the IAM efforts, a business case must often remind all stakeholders why this initiative is critical to the organization.

So, what elements of IAM investments can be identified that make an investment worthwhile?

This article looks at the business case for IAM from different perspectives.

- The first viewpoint is based on the difference between a business case's quantitative and qualitative components.
    - Quantitative means an objective calculation of the financial costs and benefits of an investment
    - Qualitative means that the costs and benefits of an investment cannot be calculated objectively, but the components have value for the business or bring additional trouble.
- A second viewpoint looks at IAM from different domains: B2E (i.e., Workforce IAM, Identity Governance and Administration (IGA)), B2C and B2B (i.e., CIAM), and Privileged Access Management (PAM).

- The third viewpoint is the organizational viewpoint: strategic, tactical, and operational reasons for implementing IAM.

There is no easy, complete formula for calculating the ROI of an investment in IAM. But at least these views can help to convince the stakeholders to look beyond the purely financial impact of IAM.

The Added Value of IAM

Preventing Negative Impacts

IAM strengthens businesses in many ways, from supporting business continuity to protecting business resources and reputation. For example, there are many reasons to consider IAM as a method for Business Continuity and Disaster Recovery (BC/DR). As organizations grow, access to resources becomes a liability: access to resources becomes more challenging overall, and delegating tasks and responsibilities becomes a bigger problem. If an organization is not in control of its data, including information on who may access that data, its ability to function in the case of significant business interruption is at risk. Even in a disaster, maintaining a record of who has in the past and can in the future access systems and data is critical.

Possibly the most famous example of a disaster directly related to a poorly managed and enforced IAM program is that of the Enron scandal in the late 1990s.[iv] In IAM terms, the scandal was partly a result of executives circumventing management controls, possibly because of the lack of fitting access controls. The best practice of Segregation of Duties was circumvented by greed, organizational culture, and practices.

At the same time, investments in IAM suffer from the prevention paradox. Investing in IAM rarely brings immediate, visible improvements. Finding the benefits (in terms of concrete cost savings) may be hard to achieve. Would the effects be the same with fewer costs and efforts of the IAM investment? It may seem like the Y2K crisis all over again.[v]

Supporting Positive Impacts

Of course, not every organization suffers from the same malicious drivers as Enron did. Still, that case highlights the need for access control from the perspectives of business continuity, governance, and compliance. To be in control, the need for managing identities and especially the management of authorizations is demonstrated by this case and many others.

But there are more reasons for investing in IAM. In many organizations, the need for IAM comes from the need for efficiency and high data quality. Manually creating identities for personnel and adding and revoking authorizations is inefficient, while the manual execution of these tasks can result in a lack of data quality. Automating the process can provide higher quality with less expensive results.

Organizations will also find benefits in improving their user experience. Developing single sign-on (SSO) services and self-service access requests improves not just the efficiency of the process but also the user's satisfaction. The continuing development of external access and the move toward API access led to the need for IAM-related programs.

These lines of reasoning, while valid, may be too far away from daily operations and immediate, visible improvements in efficiency. Businesses and boards experience the need for short-term insight as well as long-term improvements before they make further investments. In other words, companies need a specific and complete business case for IAM.

Different Dimensions of IAM Business Case

Quantitative versus Qualitative Business Case

A simple formula for calculating the ROI looks thus:

$$ROI = NetReturnonInvestment\ /Cost\ of Investment * 100\%$$

(see Guide to calculating ROI)

The simple formula can be used to calculate if an investment is anything good, financially speaking. Suppose you want to invest 1 million and later sell the investment for 1.1 million, resulting in a profit of 100,000; the ROI would then be (1,100000 – 1,000,000) / 1,000,000 * 100% = 10%

Of course, the calculation would be a little more complex for projects. It is unlikely that you would invest 1 million in IAM and later sell the investment, making a profit. This simple formula also hides the fact that indirect returns are both critical for the overall measure of ROI and extremely hard to quantify.

First, let's look at the distinction between the quantitative business case and the qualitative business case.

- The *Quantitative Business Case* is all about money. It is about calculating the costs and benefits objectively, at least as much as possible. This enumeration is relevant for managers to calculate all investments in an organization to prioritize investments. To a lesser degree, the business case can be input for a cash flow analysis. In this article, we classify topics as objectively quantifiable, but just like in risk management, some entries cannot be calculated objectively. For example, the risk of penalties does not result in an absolute value. It is an approximation of the cost of the risk. The cost of the risk could be calculated as the chance of discovery of the non-compliance times the potential maximal amount of a fine.

That means that, just like any approximation, it has to be taken with a grain of salt.

- For most governance, risk, and compliance managers, the *Qualitative Business Case* will be the preferred justification for investments in IAM solutions. The entries in the overview below may not be objectively quantifiable, but that does not mean that they should not be considered when prioritizing investments.
- An interesting example of a financial business case is the situation of banks and insurance companies who have to undergo a stress test to find if they can survive a financial crisis. The capital requirements are higher or lower depending on the risk level. High capital requirements impact the money-making capabilities; a high reserve is a lot of unused capital. These rules and regulations have been defined in the EU Basel IV and Solvency 2 regulations, which have also been adopted by the Federal Reserve in the US.[vi]
  If a bank has sufficient assurance about authorizations because of adequate access control, then data quality will be better, and risk (uncertainty about access) and capital requirements will be lower, resulting in a significant impact on revenue creation capabilities.

The Business Case for Different IAM domains: IGA, PAM, and CIAM

Another view is that the business case for different types of IAM-related programs may have different focal points because they focus on different things. For example:

- Identity Governance & Administration (IGA), which focuses on the internal account and authorization management for employees and contractors with enterprise access, has a root cause in automation, efficiency of performing JML processes, and assigning and revoking roles. While IGA investment decisions will benefit from a quantitative approach to the business case, a purely quantitative approach will not be enough to make the case. Costs and benefits will probably lie in different cost centers that measure success in different ways (e.g., in improved efficiency, in lower risk to security, in regulatory compliance). So, unless the business case is calculated companywide, the business case will be negative.
- Privileged Access Management (PAM) is all about managing risks of critical authorizations and remote access for internal accounts with broad access to sensitive resources. Its focus lies in governance and compliance. In this case, the business case is more likely to start off with a qualitative focus and miss out on some of the critical quantitative aspects that will strengthen the argument. The business case will be qualitative at first sight, but a secondary point of view may be limiting the risk of penalties and fines from laws and regulations.
- CIAM (used for B2C and B2B connections and also applicable for IoT and OT access) focuses on self-service identity management of consumers or customers. That moves convenience and consumer appreciation into a competitive advantage. The quantitative approach may not be sufficient; business continuity may be at risk for lack of investment.

This means that the business drivers for these domains are different and that the business case will contain other components.

Strategic, Tactical, and Operational Viewpoints

The third way of looking at the concept of the business case is the organization's viewpoint. In traditional organizational theory models (e.g., the Anthony triangle[vii]), we can identify the strategic, tactical, and operational layers. And if we follow up on these separate layers, there are also strategic, tactical, and operational considerations for implementing IAM:

Strategic

This topic is all about implementing business governance of Access, putting the business in control of IAM, and taking IAM out of the realm of IT. The underlying principles are:

- Governance Risk and Compliance: to be able to show that the organization is in control, to be compliant with laws and regulations, and to prevent 'Enron' issues.
- Competitor initiatives, competitive advantage: either to follow industry best practices (for example, a competitor implemented IGA) or to lead the market (for example, by implementing a leading CIAM platform).

These issues can also be seen as qualitative components in the business case.

Tactical

The tactical drivers may include enhancing business processes and information flows, structuring the organization to be more agile, and supporting merger and acquisition processes. But another driver could be to reduce technical debt that prevents innovation and agility. Older identity management solutions that are end-of-support or do not scale well to the cloud should be replaced.

The tactical components can be both quantitative and qualitative.

Operational

Operational considerations are related to the effectiveness and efficiency of people, processes, and technology. The automation of manual processes, increasing efficiency through self-service activities, and improving user experience are relevant topics for the business case.

These manual processes can be automated:

- User account management - In the JML processes, the workflow and the lifecycle can be automated based on transactions in the source system for identities (HR, student management, customer relationship management (CRM), etc.). For example, when Role-Based Access Control (RBAC) is implemented, granting and revoking of roles can also be automated. So, user and account management, as well as role management, can be automated, resulting in less manual work, faster processing, better data quality, and cost savings.

- Password reset – establishing a self-service mechanism for password resets increases user satisfaction and customer service efficiency.
- Reporting, certification, and attestation processes - these can be automated, resulting in more transparency.
- Data processing disclosure - Informing customers about the processing of their data can be automated in CIAM portals.
- Single Sign-on (SSO) – SSO enhances user convenience and reduces all kinds of service desk-related calls.
- Automated logging and auditing – Automated logging will facilitate security operations and forensic readiness.

Many of the operational issues can be regarded and calculated as quantitative components in the business case.

One Invalid View

One argument for not investing in IAM is the notion that an organization may have already invested heavily in IAM solutions, resulting in capital expenses that have not yet been written off.

This is not how an organization should react to an identified need for change. Costs based on decisions in the past should not be used in future decision processes; past decisions would lead to lock-in or in-agility for keeping up with the old choices. This kind of reasoning is referred to as the 'sunk cost fallacy' where people as well as organizations often continue with an action even as the costs outweigh the benefits.[viii] A useful counterargument to combat this fallacy is that, in hindsight, individuals would make different decisions for their organization.

Overview of Business Case Topics

This section offers an overview of the different components of the business case for IAM. It is by no means a complete overview, but it gives an indication of arguments for convincing anyone of the positive effects of investing in an IAM program. The tables suggest both the quantitative and the qualitative components of the business case for each of the three example domains: IGA, CIAM, and PAM. These examples can act as templates for other domains; practitioners will need to adapt the specifics to suit their own organizations and use cases. The strategic, tactical, and operational components can be recognized as components in the qualitative and quantitative columns of the tables.

The first table shows the components of the business case for Identity Governance and Administration (automating JML and implementing RBAC). In this table, both positive (green background) and negative (red background) components of both the quantitative aspects (left column) and qualitative aspects (right column) of the business case are explained.

The consecutive tables show comparable topics for both CIAM programs and PAM programs.

The negative financial components (investments, licenses, costs) are comparable for all three domains.

A basic cost savings formula is shown for some of the financial and quantitative components as guidance. It will, however, be meaningless without a good explanation of the benefits.

Business case considerations for Identity Governance and Administration programs

Quantitative Business Case: $, €, etc.	Qualitative Business Case
● Benefits: Cost reduction ○ Reducing manual tasks within the JML processes ■ Self-Service password reset ● Typically, a password ticket amounts to > $25 each. Implementing self-service password reset would save that workload. The net result will probably be less since service desk agents hardly ever are dedicated password reset employees. If, however, the service desk is outsourced, savings on out-of-pocket costs will be big. ***Formula***: saving = #password resets * (ticket price + (#minutes waiting for reset * hourly rate)) ■ Access Request management ● Automating access requests by removing them from service would save ticket costs but also the costs of manual handling of the process, both at the service desk and for application administrators and line managers. ● ***Formula***: savings = #requests * #cost per transaction (manual time * hourly rate)	● Benefits: Better Governance Risk and Compliance ○ Legal and regulatory obligations ■ Laws ● Laws and regulations result in controls that can be implemented and enforced by IAM solutions. ■ NIST / ISO standard compliance ● NIST and ISO standards and architecture patterns can be integrated with IAM solutions ■ Better compliance with Export Control regulations ○ Managerial Insight ■ Attestation, (re)certification ○ Supporting Organizational Agility ■ Mergers & Acquisitions, Due Diligence ■ Restructuring ○ Access Governance ■ Roles and rules ● By implementing roles and rules, the authorization models can be formalized and automated. This will reduce the level of ad-hoc access management and enhance the level of control of access ■ Reports

- Provisioning
  - Provisioning of accounts, roles, and authorizations will save a large amount of manual labor by system and application administrators. Using birthright roles (roles that can be granted automatically based on department or manager), the performance can be impacted even more positively. The same is true for de-provisioning.
  - ***Formula*** (per connector): saving = #accounts * $cost per transaction (manual time * hourly rate)
- Reduced costs of remediation of lack of data quality caused by manual data entry and lack of correlation between different identity repositories.
  - ***Formula***: savings = data entry *error rate* (circa 5-10%) * #accounts * $cost per transaction (manual time * hourly rate)

- Reducing Cost of Compliance
  - Attestation
    - Automating the certification process saves all manual verification of accounts and authorization. Lowering administrator efforts to create the reports and views and lowering manual verification by managers.
    - ***Formula***: savings = #reports * $cost per analysis (manual time * hourly rate)
  - Audit reports
    - IGA solutions typically have dozens of specific IAM-related reports that can be ordered from the self-service portals without assistance from the IT department or Business Intelligence experts.
  - Ownership
    - In Access Governance, multiple stakeholders are responsible for defining access decisions. By implementing roles and rules, as well as workflows, the ownership will be implemented by default. Otherwise, no access rules can be defined. Accountability will result.
- Implementing an Access Control scheme (e.g., RBAC, ABAC, PBAC, etc)
  - Popular access control schemes offer methods for defining access policies. In order to do implement these properly, IGA needs to be in place.
- Adding quality of service by moving responsibility for access control to the business from IT
  - Traditionally, IAM is a responsibility of the IT department. And that means that the 'business' is a victim of the SLA with the IT dept. By moving the responsibility and execution to the business, the burden of IT processes for the business is lowered. It does, however, imply that the burden now rests at the business level.
- User Convenience
  - Self-service
  - Faster processing, less idle time

- Auditors require reports. In some cases, they run their own reports (requiring specific authorizations, requiring additional governance) and analyze all results. Data drive audits are expensive. IGA solution can provide an auditor portal to use the available data. A process-oriented audit is more cost-efficient than a data-based audit.
- ***Formula***: savings = #reports * $cost per analysis (manual time of external auditor * hourly rate of external auditor + manual time of administrator * hourly rate of administrator)

  - Portals
    - Using the workflow, engines-based self-service portals of IGA solutions are more cost-efficient than having data scientists or IT personnel generate reports for different stakeholders.
    - ***Formula***: savings = #reports * $cost per analysis (manual time * hourly rate)

- Lower License costs
  - Software licenses are typically user-based. In manual deprovisioning processes, removing licenses is not always performed, resulting in unused licenses. When using automated workflows for Moving and Off-boarding, deprovisioning can be used to remove licenses from user accounts.
- Lower idle costs: Automation leads to faster processing
- SSO

- Reducing Technical debt
  - Replacing old technology (lack of development, end-of-support type of software) with modern solutions
  - Preparing for cloud enablement

▪ In manual (de)provisioning, the workflow will generally take much longer for transport time, waiting time, and idle time. Depending on the request type, this may be blocking personnel from performing actual work. ● Positive: Reducing the risk of fines and penalties ○ Fines and Penalties can occur when an organization is not in control and not compliant. By lowering the risk of non-compliance, the risk of fines and penalties will also be reduced. This may not be a financial business case, but lowering the risk will also be beneficial in accounting terms. Lower risks will also mean lower capital requirements, lowering the capital reserves and unused capital requirements. ○ Reduction of risk of data breaches ▪ Privacy, GDPR, HIPAA, etc. ● If there is more assurance about the granted access, and if the (re)certification/attestation is implemented in an effective way, the risk of incorrect authorizations is lower, and so the risk of fines will be lower. ▪ Risk of negative impact on Brand value ● Data breaches and security incidents can (in the short term) have a negative impact on brand value or stock value for listed companies. If the risk of data breaches is reduced, the risk of lower value is also reduced.	

○ Reducing compliance penalty risks ■ The risk of security incidents can be reduced by implementing security controls at the user level, like Segregation of Duties as required in various laws and regulations for high-risk business processes. ***Formula***: savings = (percentage of chance of discovery) * (max fine for non-compliancy) ○ Reducing Basel4 / Solvency2 cost risks ■ If financial institutions can lower their capital requirements, their costs will be reduced, and income will rise accordingly. ● Positive: Better business reputation ○ Increasing Consumer Confidence (e.g., data is kept secure, not shared with others without consent; organizations have the ability to let the consumer know who has accessed their data; consumers have the ability to opt-out, etc.)	
● Costs: Investment ○ Cost of the program, architecture, design, procurement ■ Before starting IAM programs, lots of analysis will be made, architectures and designs, and other overhead costs, like procurement and tendering costs. These costs may not be assigned to one specific project, but the costs cannot be neglected. ○ Licenses, maintenance, and support costs (the latter for open source) ■ Most IGA software solutions come from commercial	● Costs: Ways of working ○ (Sentiment of) reduced autonomy/sovereignty for impacted business units ■ If businesses are organized in some federated way, and each dept has a degree of autonomy, the implementation of a central IGA solution may feel like impacting the autonomy of a dept. This sentiment should, of course, be reduced by pointing to the configurable access policies, workflows, and reports of modern IGA solutions.

vendors. There is a limited number of open-source products.

License fees are usually based on the number of users. On-premises solutions require an investment fee with an annual maintenance or support fee.
SAAS Cloud products are usually subscription-based.

Additional costs may occur because of

- adding/developing/configuring connectors to source and target systems
- training and certification courses.

- Cost of Implementation
  - IGA solutions will be implemented by an integration partner (who also usually sells the licenses for IGA). Implementation costs can be high, depending on the level of customization. Even simple configuration changes can be hard, but custom code should be avoided as much as possible. Custom code results in lock-ins, making upgrades hard and even more expensive.
  - The cost of implementation can be high if the proposal leaves too many loose ends: ask the following default pricing for an IGA implementation, with one source system (HR), two target systems (AD + one DBMS connected system),

implementation of the JML workflow, and attestation report. Do not implement RBAC (incl. mover workflow) from the start of an IGA project; authorization management is too complex for full-fledged RBAC. Begin with just a few birthright roles and only start using RBAC when governance is in place. ○ Operational costs ▪ Additional costs of managing the IGA solution, modeling roles and workflows, performing authorization management tasks ▪ Moving decentralized (almost unidentifiable costs) JML processes to a central solution, so additional central costs, paid for by decentralized saving (this should be at least budget neutral, or could potentially lead to big cost savings, but dept versus corp makes a difference)	

The business case for Privileged Access Management programs	
Quantitative Business Case	**Qualitative Business Case**
● Benefits: Cost reduction ○ Consolidation of password management solutions ▪ ***Formula***: savings = #accounts * license fee (for every password manager)	● Benefits: Governance, risk, and compliance ○ Better Governance Risk and Compliance ▪ Reducing anonymous access to critical accounts ● MFA for critical access

- Consolidation of remote access solutions
  - PAM solutions, by default, have good remote access capabilities. This may include admin login and authentication, incl. MFA, secure routing, (SSL) VPN, logging and monitoring, and session recording. Most PAM solutions can replace different remote access facilities in both IT and OT and can even replace vendor/supplier remote access. Thereby reducing the costs of multiple point solutions, including maintenance and support.
    - ***Formula***: savings = (license fee + maintenance costs) (for every password manager)
  - By using the monitored PAM solution, vendors and suppliers can manage their own access without requesting (remote) access from a service desk officer.
    - ***Formula***: savings = # remote access request * administrator rate
- Password management
  - Lower operational costs by admins to secure, rotate, and manage passwords and tokens for privileged accounts.
- Reducing compliance penalty risks
  - The risk of security incidents can be reduced by implementing a PAM solution.
    Formula: savings (percentage of chance of
    - Password rotation and vaulting
    - Session Recording
  - More insight into the usage of critical accounts
  - Connection between administration and service tickets
- User convenience
  - SSO for admins
  - Remote Access for admins
    - offering MFA for non-personal accounts
  - Remote access for vendors and suppliers
    - including risk-based session recording, MFA and monitoring and logging of events

discovery) * (max fine for non-compliance)	
• Costs: Financial • See B2E for similar costs	• Costs: Ways of working ○ (sentiment of) reduced autonomy, loss of divine powers of administrators

Business Case Considerations for Consumer Identity and Access Management Programs (B2C, B2B)	
Quantitative Business Case	**Qualitative Business Case**

• Benefits: Cost reduction
  ○ Manual tasks for JML
  ▪ Self-Service Identity Management for external identities, reducing the manual tasks connected to identity management, including password reset ***Formula***: savings = #accounts * (manual cost per task)
	• Benefits: Business agility
	  ○ A competitive advantage when building portals
	  ○ Supporting Organizational Agility
	  ▪ B2B and Remote Access
	  ○ Support innovation
	  ▪ DevOps, Continuous Integration/Continuous Deployment (CI/CD), Zero Trust Authorization (ZTA), API access
	  ○ Access Control and Access Governance
	  ▪ Policy-Based Access Control (PBAC), Attribute-Based Access Control (ABAC)

	○ User Convenience ■ Self-service ■ SSO ■ MFA ○ Scalability ■ Federative Access ■ Scalable to access APIs and microservices
● Costs: Finance ● See B2E for similar costs	● Costs: Way of working ○ (sentiment of) loss of autonomy of customers, victimization due to privacy risks

Closing Thoughts About the Business Case

As explained before, a short-term positive real quantifiable business case can hardly ever be achieved. For instance, the real benefits of automating the JML flow with RBAC will only be apparent after several years, after adding multiple target systems across multiple lines of business, thus generating more business value. When looking through one-year project glasses, the outcome will not be financially interesting enough. IAM cannot just be seen from a financial perspective; there are many more considerations to be taken into account.

Pay attention to the following:
The issue of just focusing on the financial business case is too restrictive, more so when the investing stakeholder Is not the stakeholder who benefits from the investment—as is often the case. In many cases, the IT department is the cost center funding the investment. But, as can be seen in the business case examples, other departments profit from the investment in IAM. It is therefore essential to identify all stakeholders and the advantages they gain from the investment in IAM solutions, even if these benefits are not financial.

A second topic that should not be ignored in the financial savings area. Many manual activities are 'hidden' costs, including when users request access, and managers review existing authorizations, approve new requests, create accounts, and grant permissions or roles. These activities disappear in the 'normal', daily tasks of employees and so often go unaccounted for. By automating these tasks, employees can focus on more valuable activities. In the financial business case, quantifying this element may be an unwanted eye-opener.

Considering a multi-faceted business case for IAM is essential for every IAM program. A business case that goes beyond financial considerations will build awareness and commitment for starting a multi-year program that adds value to long-term business continuity. Approval is nice, but do not make it depend on a financial business case only.

Acknowledgments

The author wishes to thank Robert Sherwood and IDPro Principal Editor Heather Flanagan for their reviews and assistance in writing this article, turning thoughts into words.

Additional Reading

Beattie, Andrew. 2022. "How to Calculate Return on Investment (ROI)." *Investopedia*, August. https://www.investopedia.com/articles/basics/10/guide-to-calculating-roi.asp.

Azmi, A. M. (2007). Business cases for information technology projects. Paper presented at PMI® Global Congress 2007—EMEA, Budapest, Hungary. Newtown Square, PA: Project Management Institute.

James Cook University (14th February 2020). How to Write a Business Case: Tips, Resources and Examples.

Wikipedia contributors, "Business case," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Business_case&oldid=1164376316 (accessed October 17, 2023).

Author Bio

André Koot is principal consultant at and co-founder of SonicBee, a Dutch IAM consultancy company (IDPro partner), focused on business consultancy and giving IAM training courses. He is also a member of the IDPro BoK committee and (co-)authored several articles in the BoK.

---

[i] Schueler, Chris. 2022. "Neglecting The IAM Process Is Fighting A Losing Battle To Achieve Operational Excellence." Forbes, April 8, 2022. https://www.forbes.com/sites/forbestechcouncil/2022/04/08/neglecting-the-iam-process-is-fighting-a-losing-battle-to-achieve-operational-excellence/?sh=2a6b16147977.

[ii] "Manage Technology Debt to Create Technology Wealth." Gartner. August 17, 2020. https://www.gartner.com/en/documents/3989188.

[iii] Shea, Sharon. "How IAM Systems Support Compliance." *Security*, July 2020. https://www.techtarget.com/searchsecurity/tip/Identity-management-compliance-How-IAM-systems-support-compliance.

[iv] Hayes, Adam. "What Was Enron? What Happened and Who Was Responsible." Investopedia, March 2023. https://www.investopedia.com/terms/e/enron.asp.

[v] Allen, Frederick E. 2019. "Apocalypse Then: When Y2K Didn't Lead To The End Of Civilization." *Forbes*, December 29, 2019. https://www.forbes.com/sites/frederickallen/2020/12/29/apocalypse-then-when-y2k-didnt-lead-to-the-end-of-civilization/?sh=6c4625dc475c.

[vi] "Basel IV Implementation in the EU: What Does the New Banking Package Mean for Banks?" 2022. Oxford Law Blogs. February 3, 2022. https://blogs.law.ox.ac.uk/business-law-blog/blog/2022/02/basel-iv-implementation-eu-what-does-new-banking-package-mean-banks and "Solvency II." n.d. European Insurance and Occupational Pensions Authority. https://www.eiopa.europa.eu/browse/regulation-and-policy/solvency-ii_en.

[vii] Larson, Theodore, and Daniel Friesen. n.d. "The Anthony Triangle and an Analytics Framework: Developing a Business Analytics Curriculum Conceptual Model." *CERN European Organization for Nuclear Research*. December 2020. https://doi.org/10.5281/zenodo.3996830.

[viii] "The Sunk Cost Fallacy - The Decision Lab." n.d. The Decision Lab. https://thedecisionlab.com/biases/the-sunk-cost-fallacy.