Four Rules for a Compelling IAM Business Case

Refreshed 9 November 2020, Published 12 February 2018 - ID G00310324 - 14 min read

FOUNDATIONAL This research is reviewed periodically for accuracy.

By Analysts Kevin Kampman, Brian Iverson

Initiatives: Identity and Access Management and Fraud Detection

Security and risk management leaders responsible for IAM often struggle to obtain adequate funding for investments in IAM capabilities. IAM leaders must provide a persuasive business case that demonstrates alignment of the program with business needs and provides metrics to define success.

More on This Topic

This is part of an in-depth collection of research. See the collection:

- Guide to Initiating and Running an Effective IAM Program

Overview

Key Challenges

Security and risk management leaders responsible for identity and access management:

- Have been challenged to convince leadership that their program's activities will support desired business outcomes.
- Are too focused on technology and narrow business drivers, such as cost and efficiency, and fail to emphasize the broad impact that identity and access management (IAM) can have on the business.
- Find themselves trying to justify program funding based solely on return on investment (ROI) claims, while ROI for IAM projects is often speculative.
- Use metrics that fail to help leadership understand the case for change.
- Tend to underestimate the complexity and risk for IAM projects, undermining credibility with leadership and jeopardizing future funding.

Recommendations

Security and risk management leaders responsible for identity and access management programs should:

- Demonstrate that the IAM program's scope, objectives and priorities reflect a working consensus among stakeholders by involving them in the development and approval of the program vision.
- Align all IAM program objectives with business drivers, and articulate them in terms understandable to the business by removing acronyms and technical terms and replacing them with commonly understood terminology.
- Define clearly articulated risk metrics that align with KPIs/KRIs to make the case for change, and make clear the terms under which success will be measured based on these metrics.
- Communicate the risks facing program execution, and demonstrate a commitment to managing risks based on how program initiatives are planned.

Strategic Planning Assumptions

Through 2021, IAM programs with complete and well-articulated business cases will secure more than 200% more investment than programs that do not.

Through 2021, 90% of IAM programs that maintain effective business cases will see priority projects funded beyond the first year, compared with 25% of programs that do not.

Introduction

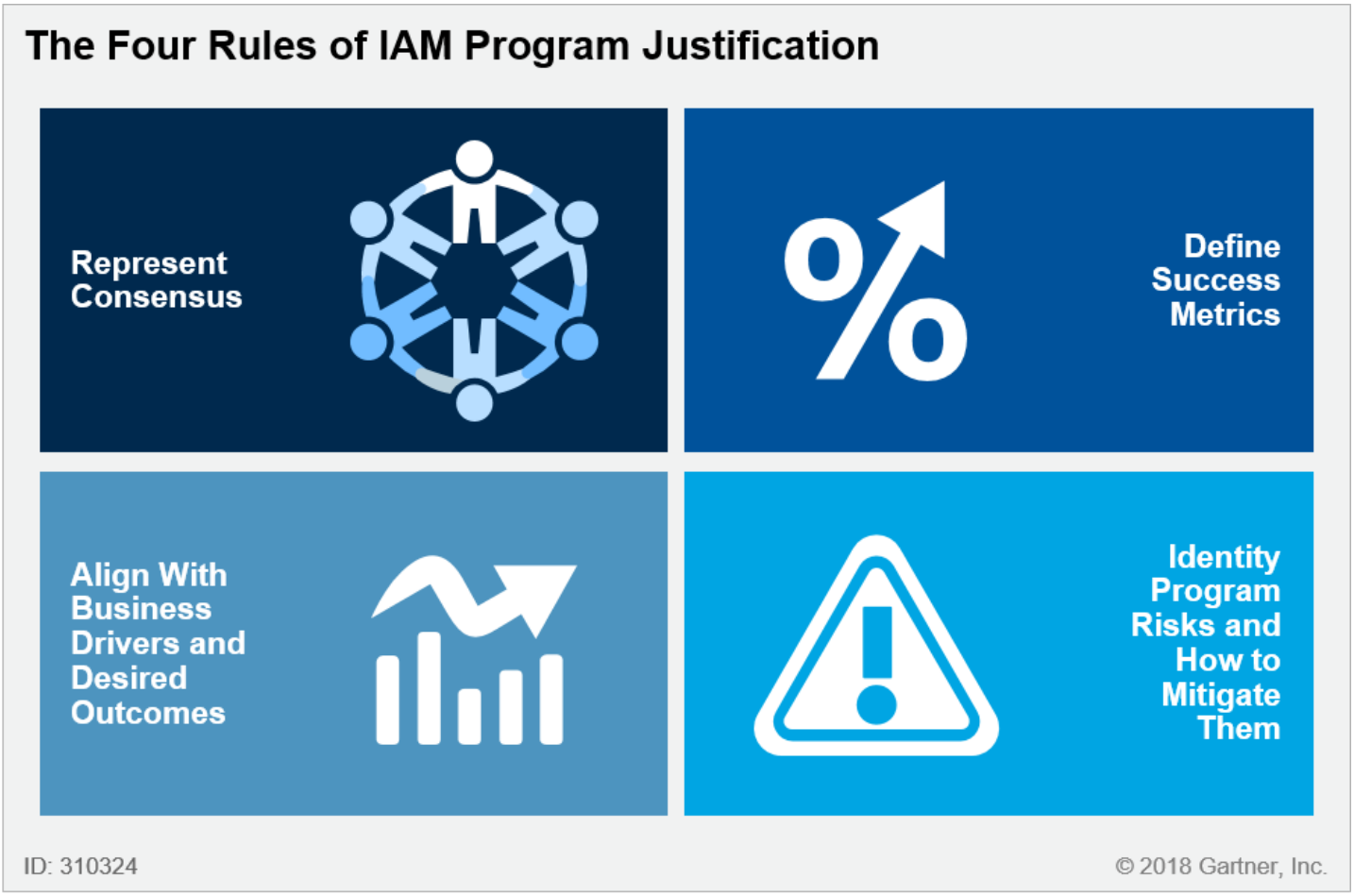
The business case is one of four key artifacts of an IAM program. Its purpose is to make the case for funding the organization's IAM strategy, which requires resources for projects as well as head count for ongoing operations. This funding is a foundation for a successful IAM program.

Unfortunately, many IAM leaders do not have much success when developing business cases that could allow them to secure the funding they need for investments. These efforts flounder because teams fail to persuasively demonstrate how the IAM program is relevant to the organization.

Without adequate funding throughout the program — not only in the first year, but in subsequent years as well — it is nearly impossible for an IAM program to make progress toward fulfilling the needs of stakeholders.

How can IAM leaders develop a compelling business case that improves the likelihood of adequate funding for the organization's IAM program? Figure 1 presents four rules that IAM leaders should follow to improve the persuasiveness of their IAM business cases.

Figure 1. IAM Program Justification



Source: Gartner (February 2018)

Analysis

Demonstrate That the IAM Program's Scope, Objectives and Priorities Reflect a Working Consensus Among Stakeholders

The hard work of developing the vision for an IAM program should ultimately produce a working consensus among stakeholders around the program's scope, objectives and priorities. This consensus represents political capital built by the IAM program. It is essential to reflect this in the business case to assure leadership responsible for allocating funding that IAM investments will adequately address the needs of the organization.

The business case is focused on support for funding the IAM program, so it is not necessary to replay all the elements of the vision to demonstrate the scope and nature of consensus among stakeholders. It is sufficient to summarize the most essential elements of the vision in the business case. This should include summaries, using non-IT language, of the following elements from the vision:

- Problem and/or opportunity statements
- Overview of stakeholders and their representatives
- Current state and gap analyses

- List of program objectives and priorities matched up with stakeholder needs

The mapping of program objectives to stakeholder needs is usually presented as a table, with objectives ranked in order of their relative priorities.

Knowing the audience is crucial for IAM and security and risk management leaders. When defining an IAM stakeholder, leaders should realize that practically every person involved with an organization may be a stakeholder of the IAM program in some way. IAM program stakeholders are groups of people who share similar needs with respect to the IAM program.

Due to the expansive reach of their program, IAM leaders must contend with multiple issues when attempting to craft a shared vision among stakeholders, for example:

- Stakeholders may not recognize how IAM may affect the ability to produce desirable business outcomes.
- Stakeholders may possess competing, even conflicting, needs.
- Stakeholders may have unrealistic expectations of what the IAM program can accomplish.

As covered in "A Successful IAM Program Begins With a Vision," IAM leaders can engage with stakeholders through representatives. IAM leaders have limited opportunities to select their stakeholders by manipulating the scope of their programs, but they can influence the selection of stakeholders' representatives.

Once stakeholders have been identified, leaders should seek out individuals who possess credibility within stakeholder communities and are able to interact in a collegial manner with other stakeholder representatives. These stakeholder representatives will actively participate in the shaping of the program's scope, objectives and priorities, and ultimately act as surrogates of the IAM leader when selling the IAM program to the stakeholders themselves and influencing process changes.

Dialogue should commence between individuals and groups to listen to and discuss their perspectives on IAM-related problems and opportunities. Consensus builds steadily through these interactions. Interviews can help dig below the surface of stakeholders' needs to identify surprising ways for the IAM program to potentially deliver value to the organization.

Ultimately, the determination of what makes a working consensus regarding the objectives and priorities for the program is a political decision — that is, deciding whether there is enough support, and the right kind of support, to move the program forward.

A successful IAM program recognizes changing conditions and adapts to them in ways that maintain its relevance to the organization. When evaluating the program at any point in time, it is important to keep the following questions in mind:

- Does the scope reflect a viable consensus among the program's stakeholders?
- Are the stakeholders effectively represented to discern their needs and success criteria?
- Does the current-state assessment accurately characterize the existing environment? In many cases, the "original" current state may be recast as an "initial state" so that the current-state assessment can be used to demonstrate progress.
- Can the objectives and priorities be mapped to, and from, stakeholder needs?

Align Program Objectives With Business Drivers and Desired Outcomes, and Articulate Them in Understandable Terms

Aligning the IAM program's objectives with business drivers helps establish the program's relevance for the organization and increases the likelihood of funding. This is done by linking IAM program objectives with the goals and values of the organization they support, and starts with translating goals communicated through the business strategy into IAM stories. For example, a strategic initiative for increased integration with business partners could be translated into increased collaboration as a business driver, which may then map to the objectives and needs for identity federation from the IAM vision.

Since the business strategy drives investment decisions for the overall organization, it shows where the organization intends to invest its money. Aligning IAM program objectives with business strategy serves to align IAM investments with the organization's spending priorities, increasing the likelihood of funding. The business strategy also provides helpful context for stakeholder needs, often including an explanation for why certain needs may exist.

Understanding the organization's strategic goals is essential for the IAM leader to anticipate how the business might need to adapt. For example, a strategy may set in motion new systems, retire old systems, or outline new ways of interacting with customers, partners or employees. Many of these trends can be anticipated by understanding the CIO's priorities (see "How to Justify IAM Initiatives by Aligning IAM With the CIO's Priorities"). Almost everything an organization intends to do will have an associated IAM story, and visionary IAM leaders uncover those stories in unexpected places. Perhaps existing IAM technology is a barrier to objectives, while new IAM capabilities could help achieve goals.

When positioning an IAM program as an essential requirement for the organization's needs, IAM leaders should remember to link their objectives with the organization's larger business aims. They will address a much more persuadable audience if they shape their program as a cornerstone of any effort intended to achieve business objectives.

During their interactions with stakeholders and in their preparations for the program, CIOs and CISOs should emphasize that a strong connection exists in terms of how a successful IAM program enables other areas of their business to prosper.

The importance of information security and technology risk management continues to grow, but many risk and security professionals continue to struggle with non-IT executive communication. IAM leaders should commit to speaking about IAM and security issues in terms the nontechnical audience uses and understands.

The board of directors and executive decision makers want to know that the organization is adequately protected against reasonably anticipated risk. The following steps will help to accomplish this outcome:

- Formalize the IAM program.
- Measure the IAM program's maturity.
- Use an identity risk-based approach.
- Use leading indicators of risk conditions.
- Map key risk indicators to key performance indicators.
- Link risk initiatives to corporate goals.
- Avoid operational metrics in executive communications.
- Communicate to executives, emphasizing what works and what doesn't.

Use Clearly Articulated Risk Metrics That Align With KPIs/KRIs to Make the Case for Change, and Clarify the Terms Under Which Success Will Be Measured

Effective business cases provide quantitative explanations for why investments are needed and the benefits that will be provided. ROI is usually the preferred method in organizations for making the quantitative case for investments. However, business cases that rely primarily on quantitative ROI for IAM investments are notoriously shaky and vulnerable to challenge by business leaders. Yet many security and risk management and IAM leaders still try to justify their IAM programs entirely in terms of ROI because they see no alternatives. This is a serious trap that must be avoided.

Risk metrics are the best alternative to ROI when there is a need to quantify benefits to support the case for investment. Metrics should be considered in the earliest stages of conceiving investments for the IAM program. Gartner recommends identifying metrics as part of the process of building project charters for planned IAM investments. The most compelling metrics are those that help to make the case for change without needing much additional explanation.

Not all the metrics available to the IAM program should be used for the business case — only those that are most likely to help leadership understand the case for change.

Given IAM programs' significant focus on risk management, these metrics should take the form of key risk indicators (KRIs). The business drivers discussed in the previous section will likely map to key

performance indicators (KPIs), so using KRIs in the business case helps focus attention on leading indicators of negative impact on KPIs (see "Develop Key Risk Indicators and Security Metrics That Influence Business Decision Making"). Also, make sure that leadership understands, values and supports any intangible benefits that are represented by metrics.

When using metrics for the business case, it is helpful to show the initial (or current) state of a given metric and then forecast how IAM investments should affect the state of the metric over time. The forecasts should help convey the idea of how benefits will be treated over the course of time.

IAM metrics development and implementation is no simple matter. Different organizations have different business goals, risks and cultures, so no one set of fundamental IAM metrics exists. Standardized approaches can only provide foundational ideas, rather than a finished product because they are not tailored for the goals, risk factors and contexts of individual organizations.

As stated above, IAM leaders should know each stakeholder's interests, expectations and performance measures, and understand the decisions that each person makes every day to fulfill their business objectives. Identify each intended recipient for your IAM metrics, and why they should take notice.

As covered in "Sharpen Your Security Metrics to Make Them Relevant and Effective," leaders should take the metrics that they have and refine them, focusing on those metrics that are both relevant and that you can reasonably generate, and discarding anything else. Know what "good" and "bad" mean, and be able to articulate what decision and what action would be taken for a "bad" result, and who would be responsible for that decision and action.

IAM leaders should articulate metrics using the business language and concepts that the audience understands. Report only on what is relevant to them.

Effective metrics reporting often takes into account the characteristics of individuals to whom the metrics will be reported. Concepts, language and, indeed, areas of individual sensitivity are important. Remember, risk, IAM and security are unusual disciplines, in that they become most noticeable when there are failures. Suitable security often means a perceived lack of activity by nonsecurity practitioners, so IAM leaders must sustain the collection and demonstration of metrics that provide proof of the IAM program's success.

Communicate the Risks Facing Program Initiatives to Stakeholders

A good business case discusses the risks facing execution of the IAM program and explains how those risks are being mitigated. Leadership will be hesitant to make investments that appear risky and may lose the will for IAM after experiencing failures with previous efforts, such as long delays. The business case must be sensitive to the political situation that surrounds the IAM program. Previous failures must be acknowledged and explained, especially in terms of what is being done to avoid known pitfalls and improve the likelihood of success.

IAM leaders should be realistic when explaining benefits and demonstrate an appreciation for risk management through the structure of the IAM roadmap — the ways that projects are staged and delivered. Large initiatives that depend on big upfront investments with no visible benefits during the current budgeting cycle are too risky. IAM initiatives should be planned so that visible "wins" are delivered on a consistent basis and in short time intervals (ideally, every three to four months).

Success during the initial phases of the IAM program is critical to its ongoing viability, so IAM leaders must be modest with what they promise and plan to deliver. Many IAM initiatives have been launched with ambitious buzzword-laden schemes, such as "enterprise directories," "single sign-on (SSO)" or "role-based access control (RBAC)," only to drift toward failure or irrelevance because inflated expectations outpaced reality.

As the business case is updated and refined to secure funding beyond the first year of the IAM program, it is a good practice to reflect on the status of investments from previous rounds of funding. Both successes and failures must be acknowledged and discussed. Circumstances occasionally call for adjustments to plans inside a funding cycle. For example, funding may be shifted from one project to another because of a shift in priority. These changes, and their impacts, require explanations.

Gartner client inquiries make it clear that one of the most serious problems facing security and risk management professionals — and one that is undermining their credibility — is their inability to communicate effectively with senior executives, line-of-business managers and other key business decision makers. The result is a vicious cycle, in which poor communication results in inefficiencies and failures, which in turn diminish the perceived value of the enterprise's security and risk management initiatives.

As covered in "How to Gain Support for Your Security Awareness Program," it is paramount for the CISO to find ways to get on the influential executives' radar early to lay a good foundation for a discussion about budgeting. This applies equally to IAM leaders. From there, the IAM leader makes a strong case that positions the program as an essential component of business initiatives. An advocate will use measurable data that clearly shows the program's benefit.

IAM leaders can identify an executive advocate to help initiate communication regarding the IAM program. This should be someone with influence, and who has the most to gain from IAM initiatives.

The IAM leader should use a line-of-business-populated governance forum to ensure that budget requirements are appropriate and adequate for the attainment of corporate goals. In other words, IAM leaders should ensure that the need for the budget is understood, that it is being applied to the right problems, and that it is sufficient for what must be achieved. This approach can also provide perspective on operational obstacles and areas of obstructed or misdirected funding (see "How to Defend and Manage Your Security Budget").

Document Revision History

Four Rules for a Compelling IAM Business Case - 6 August 2015

Build an Effective Business Case for IAM - 27 January 2014

Recommended by the Authors

A Successful IAM Program Begins With a Vision

Developing Metrics for Security Operational Performance

Demonstrate Control Over User Access With IAM Effectiveness Metrics

Communicate Plans and Manage Program Risks With the IAM Roadmap