Use Outcome-Driven Metrics to Drive Value for Identity and Access Management

Published 2 June 2023 - ID G00784955 - 10 min read

By Analyst(s): Rebecca Archambault, Paul Proctor, David Collinson

Initiatives: Identity and Access Management and Fraud Detection; Build and Optimize Cybersecurity Programs

Organizations often find it difficult to determine the security and business value directly related to IAM investments. Security and risk management leaders responsible for IAM can use outcome-driven metrics to guide IAM investments, deliver business value and achieve a stronger security posture.

Overview

Key Findings

- Security or information technology leaders are usually responsible for identity and access management (IAM) investment decisions. These leaders typically focus on security and risk mitigation, but do not understand the wider business value that a modern IAM system can generate.
- IAM metrics are often technical and inward looking, and are not typically aligned to support business outcomes.
- The IAM program is often not involved with business-driven initiatives, impacting the IAM team's ability to actively engage them in priority discussions.

Recommendations

Security and risk management (SRM) leaders responsible for IAM should:

- Communicate the value of IAM investments by using outcome-driven metrics (ODMs) that can measure the business value of IAM investments including but not limited to security risk management improvements.
- Create a business context for investment by using ODMs to align IAM investments with business outcomes.

- Provide visibility into your IAM program using outcome-driven metrics. This allows for transparency and enables ongoing communication to set priorities and enable better business decisions.

Strategic Planning Assumption

By 2025, a 50% reduction in time to remove access will result in 20% fewer audit findings related to departing and/or transferring workforce members.

Introduction

As per Gartner's latest forecast, the identity and access management market worldwide is expected to grow from US$15.87 billion in 2021 to US$32.42 billion in 2027. [1] Organizations are becoming more aware of the foundational role that identity plays within their larger security architecture and how IAM impacts their business. It will become more common for IAM leaders to be asked about the value that they can get from their IAM investments.

The value of IAM is often viewed through a security lens. Credential misuse was involved in 40% of security breaches in 2021, making identity threat detection and response (ITDR) a top cybersecurity priority for 2022 and beyond. See Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response for more information.

Unfortunately, investment in IAM does not always result in better security or improved business outcomes. The best way to prove value is with metrics that focus on organizational risk and how IAM can enable the wider vision and strategy. Gartner recommends using IAM protection levels as a means to start the discussion, along with outcome-driven metrics (ODMs).

SRM leaders who are responsible for IAM should follow a three-step approach to make sure their metrics will deliver security and business outcomes:

1. Use ODMs to measure IAM protection levels.

2. Align ODMs to business strategies.

3. Incorporate ODMs into IAM programs for visibility and to guide IAM investment.

Analysis

Use Outcome-Driven Metrics to Measure IAM Protection Levels

IAM Investment decisions are often made in a vacuum, with organizations taking a tactical approach to solve a specific problem. This has resulted in technical debt and limits an organization's ability to build an identity fabric that supports identity-first security.

Gartner recommends using a combination of protection-level agreements and ODMs to answer the question of value.

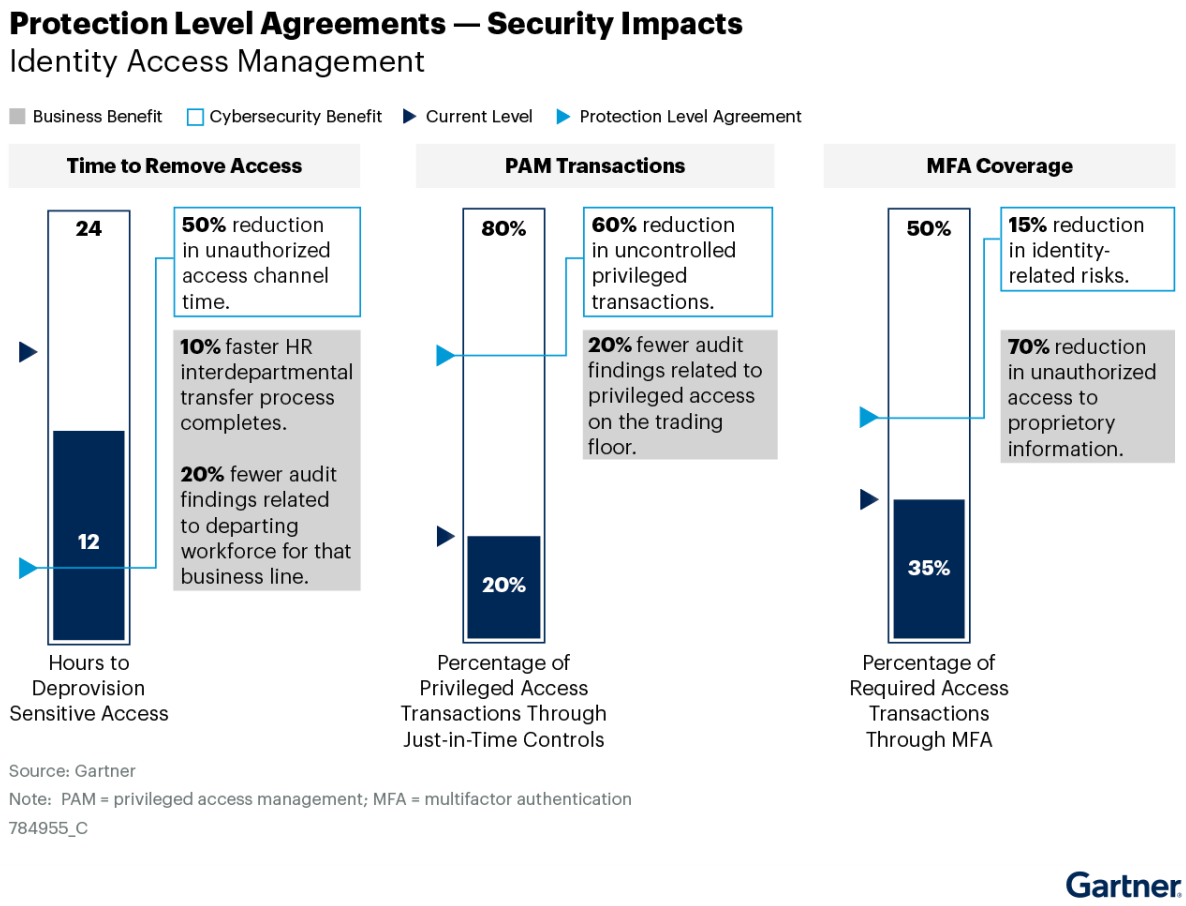
What Is a Protection-Level Agreement?

A protection-level agreement (PLA) is a construct to facilitate cybersecurity decisions between executives and IT and security decision makers. PLAs are business decisions to invest in measurable levels of protection at a defined cost.

Why ODMs?

- They measure cybersecurity outcomes achieved by specific investments. They are constructed by aligning what is measured to the desired protection outcome of the investment. In this manner, ODMs simultaneously reflect protection levels and value for investment.
- ODMs help to understand current state versus desired state in the form of validating agreed-upon protection levels. When an ODM improves, the organization is measurably better protected. When the ODM is worse, the organization is measurably less protected.
- They act as value levers for cybersecurity investment. ODMs support direct investment to achieve different outcomes. Organizations can increase their investment to improve protection levels, or save money and accept lower protection levels.

Figure 1: Protection Level Agreements — Security Impacts



As shown in Figure 1 above, Gartner recommends you to start by benchmarking three primary protection level ODMs for IAM (see Table 1 for more examples):

- **Time to remove access.** It should be measured in hours for the workforce. If you decrease the number of hours it takes to deprovision sensitive access, this will provide a risk reduction that directly impacts unauthorized access. The business benefits, in the example of a position transfer or a promotion, are that the process will complete more quickly and that the business line will have less audit findings relating to the departing workforce.

- **Privileged access management (PAM).** PAM deployments should be benchmarked as the ratio of "always-on" privileged access versus privileged access granted on an infrequent and temporary just-in-time (JIT) and just-enough-privilege (JEP) basis. If fewer people have permanent privileged access, and most of this access is controlled with PAM tools that implement JIT and JEP processes, you can see some risk mitigations in the form of less impact attributable to production changes, audit findings and threat exposure.

- **Multi Factor authentication (MFA) coverage** for both workforce (ex. remote access scenario) and customers (security with less friction, and stronger assurance levels which could protect proprietary information). The ODM for MFA coverage measures the percentage of deployed applications that require MFA. MFA and privileged access have multiple dimensions that can be explored to define other ODMs. For example, scripts that embed machine account passwords can be measured and prioritized for remediation, limiting risk exposure.

These ODMs are defined in The Gartner Cybersecurity Business Value Benchmark, First Generation. Many more ODMs are defined in Tool: Catalog of Business-Aligned Outcome-Driven Metrics for Risk and Security.

Table 1 below lists additional ODMs that measure business alignment with the value of IAM investment.

Table 1: IAM Outcome-Driven Metric Examples

(Enlarged table in Appendix)

Metric Category	Metric	Calculation	Example
Friction — Workforce	Consistent experience across channels	% apps that are onboarded to the IAM system with consistency of experience across channels	Managers can approve access or expenses via their mobile phones as the experience is the same via laptops.
Friction — Customer	Consistent experience across channels	% apps configured via customer identity and access management (CIAM) for consistent user experience	Customers can move from chat to customer service without repeating the experience.
Productivity — Workforce	Single sign-on (SSO)	% apps configured for SSO	Employees are free to move from one application to another without reentering credentials.
Productivity — Improving the new joiner process	Birthright roles are defined.	% of access authorized by birthright rules vs. requiring manual access request and approval	New employees have the access they need to be productive on Day 1.
Efficiency — Risk reduction	Automation of provisioning process	% of access fulfilled using automated processes vs. manual access provisioning	Workforce access is quicker as provisioning and automated, and risk is reduced by automating deprovisioning processes.
Revenue — Customer	360-degree view of the customer	CIAM integration across CRM and master data management (MDM) systems which hold valuable customer insights	Provide new product or service suggestions based on behaviors.
Staffing optimization — Reducing volume of customer service calls and tickets	Offer more self-service options for customers	% of CIAM self-service capabilities deployment	Reduction in call volume and tickets generated to customer service.
Staffing optimization — Reducing help desk calls and tickets from workforce	Offer more self-service options for password reset and profile preferences	% of applications onboarded to IAM systems with password and profile self-service enabled	Reductions in call volume and tickets generated to the help desk and faster problem resolution for the workforce.

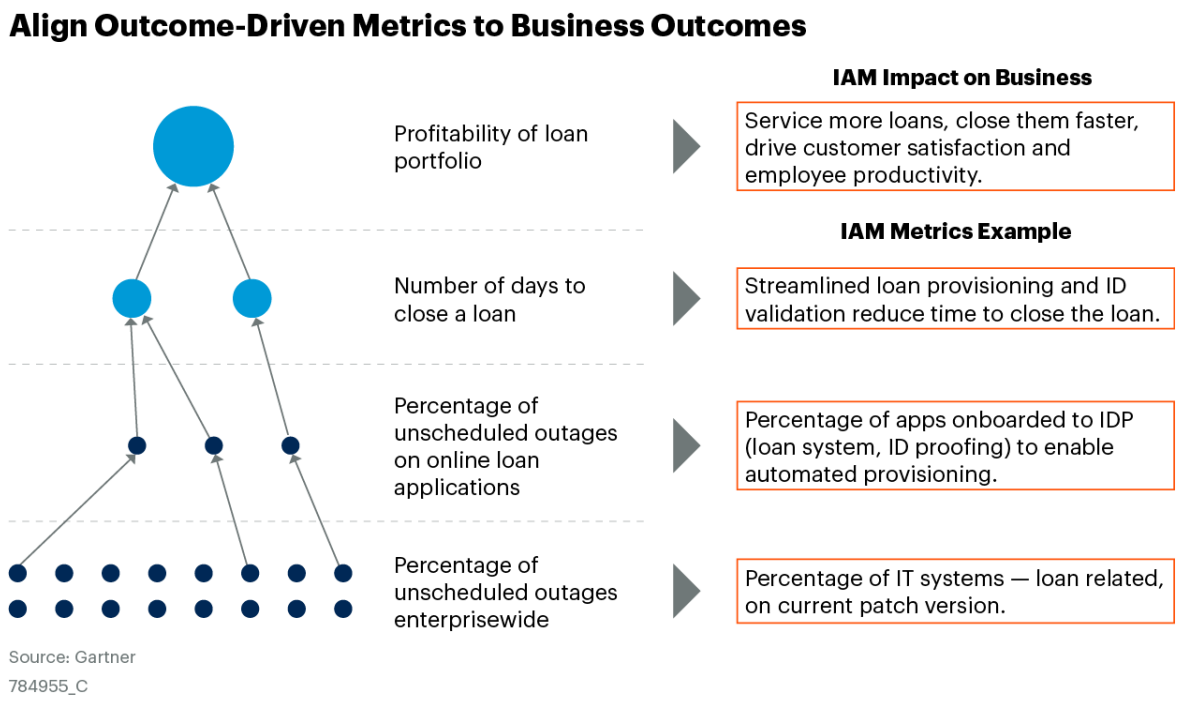
Source: Gartner

ODMs create a foundation of value measurement that can be aligned to business outcomes and a business context around IAM investment, where better-informed risk decisions can be made.

Align Outcome-Driven Metrics to Business Outcomes

Create a direct connection between IAM investment and business outcomes using ODMs. Figure 2 represents the relationship between IT operational metrics, ODMs and business outcomes through the example of an online loan origination process used by retail banks. Retail banks use the online loan origination process as a primary source of revenue to create loans for customers.

Figure 2: Align Outcome-Driven Metrics to Business Outcomes



Below the dotted line as shown in Figure 2, technology operational metrics measure different aspects of technology operation for the benefit of IT decision making such as unscheduled outage, bandwidth capacity, asset utilization and service level performance.

A small number of these operational metrics directly impact business outcomes, and this relationship is referred to as a direct line of sight. Take retail banking for example. An unscheduled outage on the technology platform supporting customer-facing online loan applications has a direct line of sight to business outcomes in the loan portfolio.

Operational metrics with a direct line of sight to business outcomes are referred to as technology ODMs. The business outcomes they support become drivers for priorities and investments in the technology while failures of the technology drive impacts to the supported business outcomes. Similarly, business ODMs are business metrics with a direct line of sight to business outcomes.

In Figure 2, the profitability of the loan portfolio (a business outcome) is dependent on the number of days it takes to close a loan from an online application (a business ODM) which is impacted by an unscheduled outage on the online loan portfolio application (a technology ODM). While some IT leaders will report that these relationships are inherently obvious, impact isn't being communicated clearly back to the business owner.

The orange text in Figure 2 illustrates the role that IAM plays in this scenario. Some questions that can be answered using this process would include:

- Has the loan application been onboarded to the access management system and has it enabled access to those who service loans in an automated way (without requiring a separate access request)?
- Is there a connection between the CIAM system and the identity proofing system? If so, can additional processes be avoided for customers?
- Are the available customer authentication mechanisms easy to use (i.e., low friction)?
- Is the new (prospective) customer registration process for this business process integrated with or reusing customer registration processes used by other parts of the business? Or is it a "one-off" process for just online loan origination?

These steps above directly impact the time it takes to close the loan, both from the workforce's and the customer's perspectives, which impacts the profitability of the loan portfolio business.

Incorporate ODMs Into Your IAM Program

Gartner recommends a formal IAM program that stresses the importance of building value beyond security with your IAM investments (see IAM Leaders' Guide to IAM Program Management). This can be accomplished by moving out of the traditional IT and security silos, and giving key stakeholders visibility into the role that IAM plays across the organization. The program should represent a comprehensive view, including both tactical and strategic efforts that focus on security and business outcomes.

Once ODMs are included in the IAM program, tracking progress will help to inform future risk decisions, and will guide priorities. Remember that the IAM team has to support the entire organization. Ask yourself the following questions:

- Do I assign precious resources to hygiene activities associated with increased risk (i.e., assigning owners to orphan accounts, both human and machine)?
- Do I remediate dormant accounts, or tackle empty groups opposed to onboarding a new application which includes the launch of a new product?

Include ODM targets and even changes in ODM targets in your IAM program roadmap. Discuss them with your stakeholders, and prioritize them in a way that is achievable. ODMs help to explain why implementation initiatives in the roadmap are sequenced the way they are, and make clear to all stakeholders what outcomes need to be achieved by when, to demonstrate business value. Put another way, they will improve your roadmap by directly tieing the "below-the-line" IAM technical implementation work with the "above-the-line" business outcomes.

Evidence

"Identity-first security" was introduced by Gartner in early 2021 in Top Security and Risk Management Trends 2021 and is often discussed in client inquiries and vendor briefings, on which this research draws. How to represent value from IAM investments is also a frequent topic of inquiry.

[1] Forecast: Information Security and Risk Management, Worldwide, 2021-2027, 1Q23 Update

Notes

Gartner's Cybersecurity Business Value Benchmark tool is currently available for early adopters. Please see The Gartner Cybersecurity Business Value Benchmark, First Generation for more details.

Document Revision History

Four Rules for a Compelling IAM Business Case - 12 February 2018

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

Some documents may not be available as part of your current Gartner subscription.

Identity-First Security Maximizes Cybersecurity Effectiveness

4 Steps to Effectively Communicate the Business Value of IT

Quick Answer: What Is a Cybersecurity Outcome-Driven Metric?

Tool: Catalog of Business-Aligned Outcome-Driven Metrics for Risk and Security

Use Value and Cost to Treat Cybersecurity as a Business Decision

Table 1: IAM Outcome-Driven Metric Examples

Metric Category	Metric	Calculation	Example
Friction — Workforce	Consistent experience across channels	% apps that are onboarded to the IAM system with consistency of experience across channels	Managers can approve access or expenses via their mobile phones as the experience is the same via laptops.
Friction — Customer	Consistent experience across channels	% apps configured via customer identity and access management (CIAM) for consistent user experience	Customers can move from chat to customer service without repeating the experience.
Productivity — Workforce	Single sign-on (SSO)	% apps configured for SSO	Employees are free to move from one application to another without reentering credentials.
Productivity — Improving the new joiner process	Birthright roles are defined.	% of access authorized by birthright rules vs. requiring manual access request and approval	New employees have the access they need to be productive on Day 1.
Efficiency — Risk reduction	Automation of provisioning process	% of access fulfilled using automated processes vs. manual access provisioning	Workforce access is quicker as provisioning and automated, and risk is reduced by automating deprovisioning processes.

Metric Category	Metric	Calculation	Example
Revenue — Customer	360-degree view of the customer	CIAM integration across CRM and master data management (MDM) systems which hold valuable customer insights	Provide new product or service suggestions based on behaviors.
Staffing optimization — Reducing volume of customer service calls and tickets	Offer more self-service options for customers	% of CIAM self-service capabilities deployment	Reduction in call volume and tickets generated to customer service.
Staffing optimization — Reducing help desk calls and tickets from workforce	Offer more self-service options for password reset and profile preferences	% of applications onboarded to IAM systems with password and profile self-service enabled	Reductions in call volume and tickets generated to the help desk and faster problem resolution for the workforce.

Source: Gartner