Why metrics are the central piece of any IAM program puzzle

Many security and risk professionals find it difficult to "sell" the business benefits of a workforce identity and access management (IAM) solution to their senior leadership and other stakeholders.The rampant rise in data breaches since the onset of the pandemic is a compelling reason to consider investing in an IAM solution, or improve an existing one.

However, IAM is not only about security. Departments like Compliance and Administration often significantly impact an organization's business goals. But only with department-specific IAM metrics can you communicate value to stakeholders. Without meaningful metrics, you can't track the performance of your IAM program against the objectives you set, or determine which departments need to improve or require further investment.

In this guide, we'll look at six tenets you should keep in mind when you work with IAM metrics.

tenets you should follow while working with IAM metrics

Incorporate metrics from the beginning.

1

Often companies roll out IAM initiatives, and wait until they've collected sufficient data to identify metrics they can use to measure the effectiveness of the program. This approach often fails because it tries to define the problem based on the solution, instead of the other way round.

First define clear objectives. Then, identify metrics that will demonstrate the progress being made towards the achievement of those objectives.

Reducing the time your help desk staff spends to resolve password reset requests by N% in three months is an example of an objective. You need to then identify a metric, or a cluster of metrics, that will help you achieve this objective.

2

Learn how much your identity-related tasks are costing.

All IAM tasks have a monetary cost attached to them. Manual auditing of critical changes made to Active Directory (AD) has a cost. If employees are locked out of their accounts, the time they lose waiting for them to be unlocked by the help desk has a cost. Unless you know how much these specific tasks are costing you, you won't be able to quantify how much savings you'll get by automating them.

For instance, **our return on investment (ROI) calculator** reveals password reset requests alone cause a loss of over $35,000 for an organization with 250 employees. In this case, our ROI calculator illustrates that the company is better off automating the task rather than attempting to resolve it manually. The calculator also reveals the annual recurring ROI and also the time in which they'll be able to recover their investment in our **end-user self-service** password management tool.

Automate reporting of metrics.

3

Given the large number of data points, manual reporting is not scalable. Since it's also a time-consuming task, it will only introduce inefficiencies in the system. Analysts recommend Security and Risk (S&R) professionals automate at least 90 percent of their metrics collection and reporting.

Many security analytics and reporting tools offer intuitive dashboards that track and show data trends. Identify one that best suits your needs and budget, and automate metrics reporting as soon as you can.

4

Define acceptable thresholds, and configure alerts when they are exceeded.

By defining thresholds, you can take action only when it's necessary, as opposed to reacting to every small change. You'll save both time and resources. Consider the example of login success rates. **Cybersecurity experts** say as long as companies (irrespective of the industry they are in) have login success rates between 60-85 percent they need not panic.

However, they suggest, anything outside this range should be treated with suspicion, and is likely an indication of a credential stuffing attack.

It only makes sense to configure alerts when your login rates, or other objectives, fall below or breach the thresholds you set.

Involve only the appropriate stakeholder in the right phase.

5

IAM programs have quite a few phases: problem identification, solution ideation, stakeholder requirement research, funding, implementation, performance review, and so on. Not all stakeholders need to be involved in every phase. Discover which stakeholders are the primary decision-makers for that specific phase, and get in touch with them to understand where they can offer guidance.

For instance, when you have uncovered that your team is losing productivity because they're waiting too long for their password reset or account unlock requests to be resolved, the only stakeholder required is you.

You need to learn as much as you can about the issue and the possible solutions the industry offers. You can call it the solution ideation phase. You may decide to include another IAM professional in a similar business unit who is facing the same issue and is trying to put together a business case to resolve the problem.

However, executives who will authorize funds for the proposed IAM initiative will only need to be involved in the next phase.

6

Communicate only the applicable metrics to relevant stakeholders.

Though you'll need input only from a specific set of stakeholders based on the IAM program phase, as your IAM initiative progresses, more stakeholders will need to be involved. Your IAM initiative will move forward only when the correct person receives the correct information. Nothing more, nothing less.

Stakeholders can be placed in three broad buckets, and using these categories can be helpful when you need to prepare a stakeholder-specific pitch.

People who fund the IAM initiative: Chief information officers (CIOs), compliance officers, and CISOs fall in this bucket. In most cases, they have their own budgets and have the authority to delegate resources for an initiative.

People who help with the implementation:

Three types of stakeholders make up this bucket:

- Business process owners, such as HR functional admins, portal content managers, and others.
- System or application owners, like AD admins, vendor portal admins, and others.
- Data owners, such as database admins, AD architects, and others who manage identity data repositories.

People who rely or use IAM services: End users, including employees, vendor partners, and others.

Each of these stakeholders face different problems.

You should identify and communicate metrics that will address their specific needs.

For instance, business owners will benefit from a metric that showcases the time saved by automating user creation, deletion, and disablement. System and application owners will find a metric that demonstrates the percentage reduction in account unlock requests useful.

Only when you communicate metrics that solve specific problems, will you be able to solicit feedback and refine the metrics you need to track progress against set objectives.

The best time to strengthen your IAM was before the pandemic. The next best time is NOW.

The pandemic has put a spotlight on the dangers of not having robust and efficient IAM processes in place.

Whether you are looking to invest in an IAM solution or upgrade an existing one, the key is to put together a business case with metrics that will help you communicate value to different stakeholders, justify the need for the IAM program, and track its performance.

In the next part of this guide, **we'll look at a comprehensive list of IAM metrics** S&R professionals should track.

Write to me at **jayreddy@manageengine.com** if you would like the second part of this two-part guide on IAM metrics sent to you.