How to establish IAM metrics within the Zero Trust framework

EY
Building a better working world

Government agencies are implementing Zero Trust plans mandated by President Biden's Executive Order on Improving the Nation's Cybersecurity and the Office of Management and Budget (OMB) memorandum M-22-09. Zero Trust programs require the need to effectively measure identity and access management (IAM). To build or enhance an IAM metrics program, we recommend the following steps:

Linking IAM metrics to organizational goals

An effective IAM metrics program needs to link specific IAM key performance indicators (KPIs) to broader IAM and organizational goals. As shown in the figure below, we will reference the Zero Trust M-22-09 Identity strategic goal: "Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks."

01

Identify strategic goals: Start by identifying the strategic goals of the IAM program. IAM strategic goals should align with the broader objectives of the organization, such as enhancing security, improving user experience and achieving regulatory compliance. Examples of strategic goals for IAM could include reducing the risk of unauthorized access, streamlining user provisioning processes or enhancing identity governance.

02

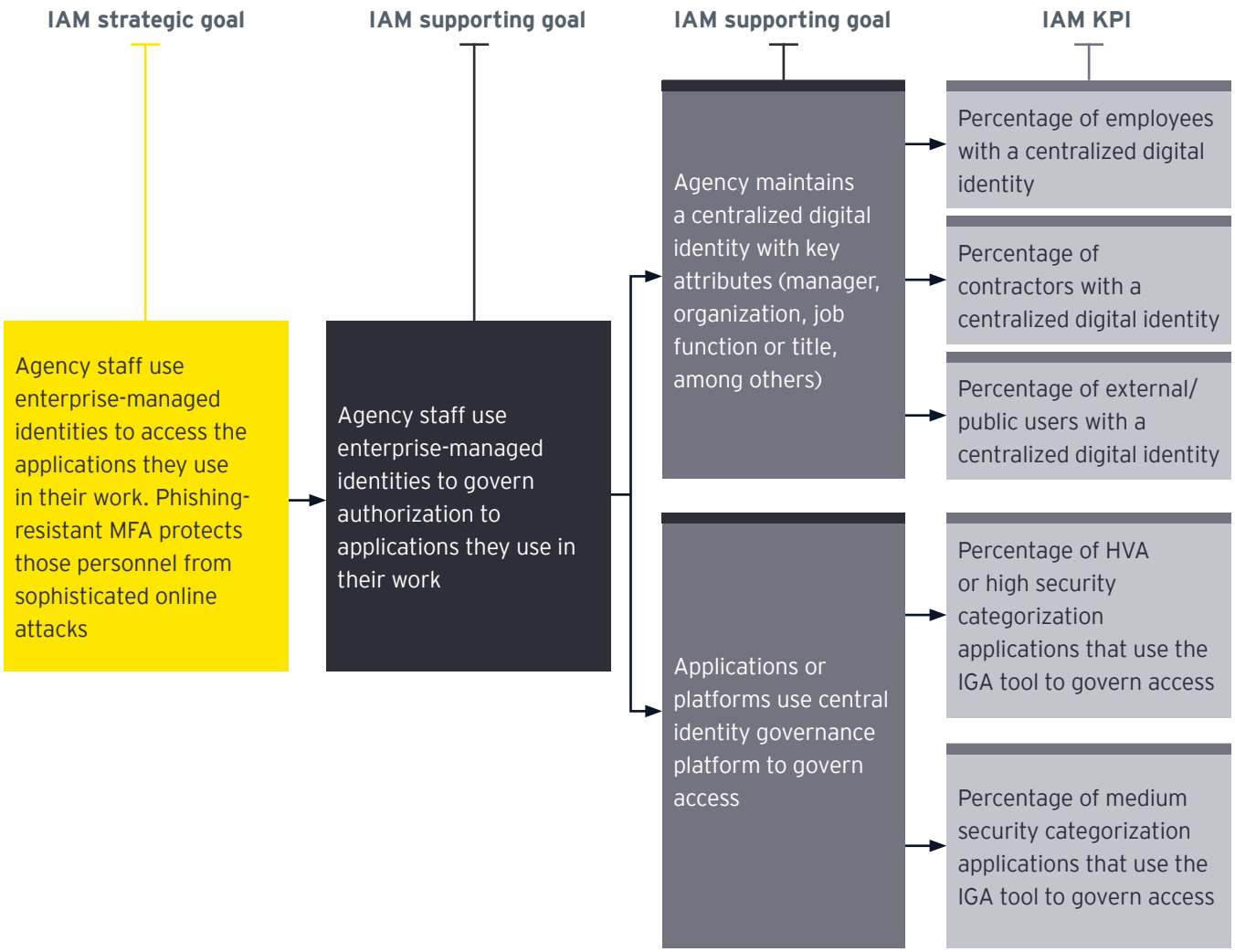
Define supporting goals: Once strategic goals are identified, then define supporting goals. These supporting goals represent specific areas or aspects that contribute to achieving the strategic objectives. For instance, if the strategic goal is to reduce the risk of unauthorized access, supporting goals could include strengthening authentication mechanisms, implementing role-based access controls or enhancing privileged access management.

Using the M-22-09 Identity strategic goal above, supporting goals could be "Agency staff use enterprise-managed identities to govern authorization to applications they use in their work" and "Agency staff use phishing-resistant MFA to access Agency resources." There can be multiple layers of supporting goals, if needed.

03

Establish specific IAM KPIs: After supporting goals have been defined, establish specific IAM KPIs that measure the progress and effectiveness of the IAM program. KPIs should be specific and measurable and expressed as a proportion (percentage) so that various dimensions (departments, branches, regions, time periods, etc.) can be compared against each other. KPIs indicate the success or areas of improvement for each supporting goal. Examples of IAM KPIs could include the average time taken to provision user accounts, access policy violation rate, percentage of failed authentication attempts or MFA adoption rate.

In the example above, KPIs include "Percentage of employees with a centralized digital identity" and "Percentageof cloud resources that require phishing-resistant MFA to authenticate."



Establishing new IAM metrics programs

For agencies without a mature IAM metrics program, it is important to incorporate metrics and reporting capabilities from the beginning. Although data collection might be limited initially, describing the desired measurements and aligning them with strategic objectives guides the design of the IAM processes and technology.

In addition, IAM metrics programs can be used to align to Zero Trust frameworks. For example, the Department of Homeland Security (DHS) established a Zero Trust maturity model which defines optimal "Visibility and Analytics" maturity: *Agency maintains comprehensive visibility and situational awareness across the enterprise by performing automated analysis over user activity log types, including behavior-based analytics.*[1]

For an agency to achieve this level of maturity, it is important to design goals and metrics that will measure progress. For example, metrics related to user behavior analytics (UBA) – e.g., "percentage of critical applications that send log data to a UBA tool" – can offer insights into maturity level as well as help the organization focus efforts on identifying applications suitable for providing data to the UBA tool.

[1] Cybersecurity & Infrastructure Security Agency's CISA's Zero Trust Maturity Model v2

Enhancing existing IAM metrics programs

If an organization already has a mature IAM program, what should it do with its existing metrics? It is important to review existing metrics and question the necessity of each metric. Does the metric help monitor progress towards achieving the broader goals? More metrics does not equate to better results; understanding the purpose behind measuring something is what truly matters.

For example, measuring the percentage of uncorrelated identities can be a very effective IAM metric. A sudden increase in the number of uncorrelated identities can provide valuable insight that warrants further investigation. This metric also maps to the first supporting goal in the example above: "Maintaining a centralized digital identity."

Conclusion

By aligning strategic goals with supporting goals and KPIs, organizations can establish IAM metrics programs that focus on measuring outcomes and tracking progress toward desired objectives. This structured approach facilitates effective monitoring, evaluation and continuous improvement of the IAM program. In the ongoing effort to mature IAM within the Zero Trust framework, establishing and integrating IAM reporting and metrics is critical to success.