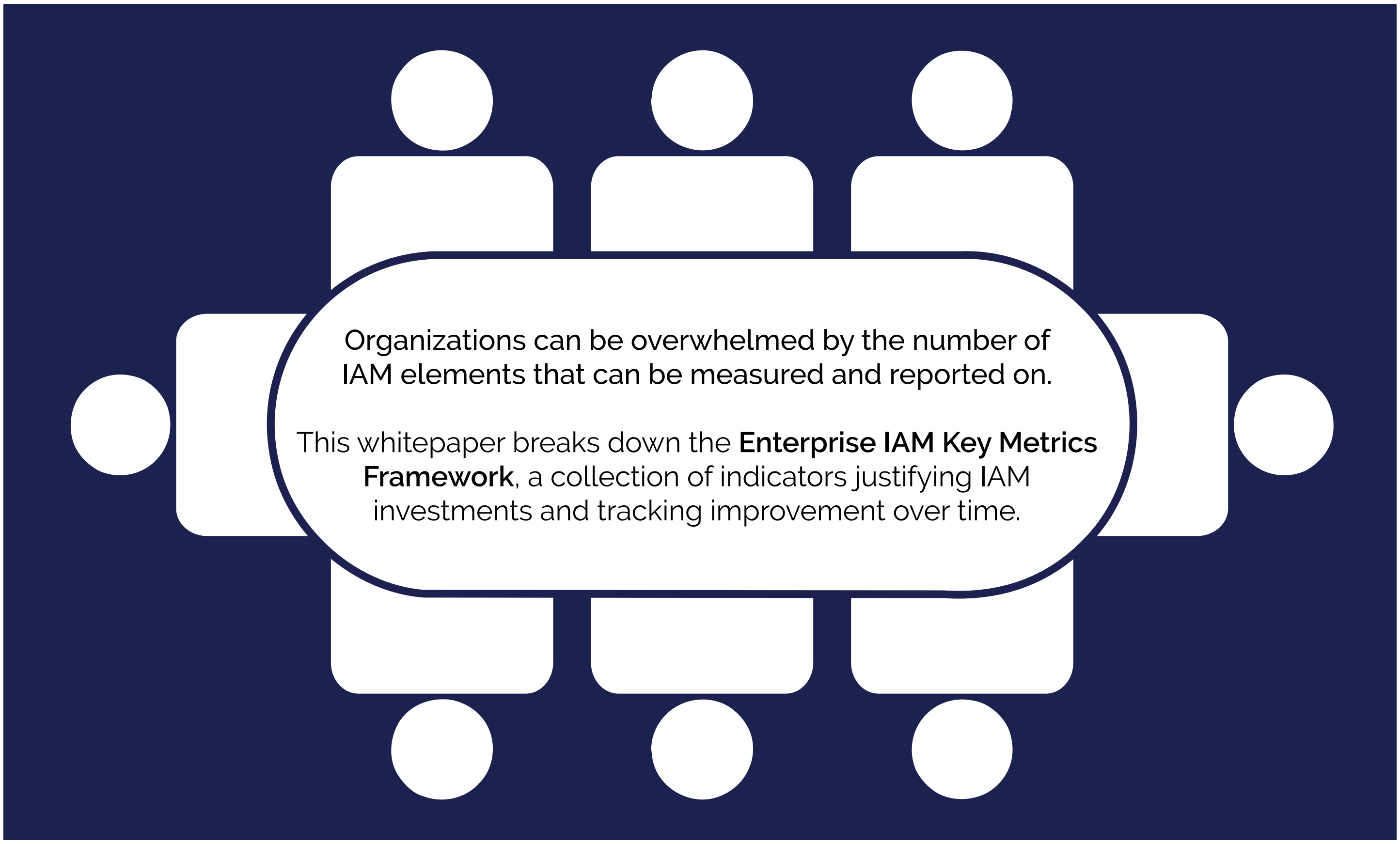
XMS SOLUTIONS

Enterprise IAM:
The Metrics that Matter

Enterprise IAM Key Metrics Framework

version 1.0
August 2016



Organizations can be overwhelmed by the number of IAM elements that can be measured and reported on.

This whitepaper breaks down the **Enterprise IAM Key Metrics Framework**, a collection of indicators justifying IAM investments and tracking improvement over time.

TABLE OF CONTENTS

Enterprise IAM: The Metrics that Matter

INTRODUCTION

Metrics are critical to the success of an enterprise's IAM program, IAM initiatives and IT operations, because they enable IAM leaders, other stakeholders and decision makers to recognize the value of those efforts.

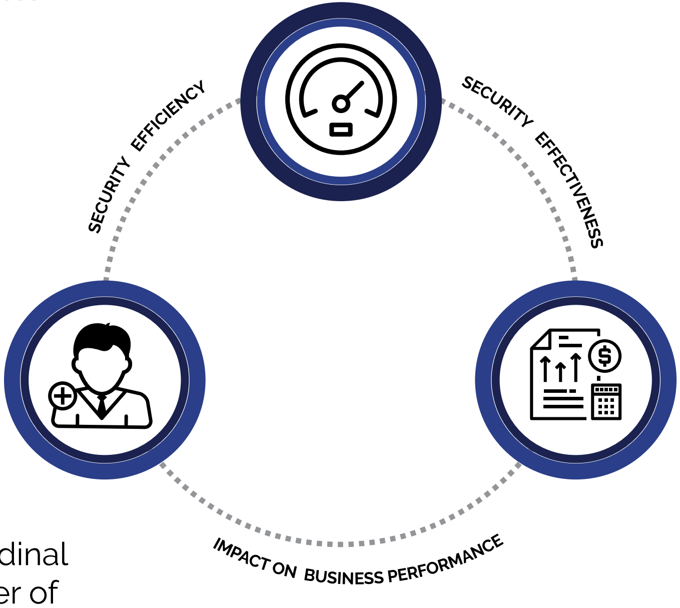
However, organizations can be overwhelmed by the number of IAM elements that can be measured and reported on. IAM leaders must focus on business-relevant metrics that demonstrate the value of their IAM activities and show improvements over time.

The Enterprise IAM Key Metrics Framework

Most enterprises are driven to pursue formal IAM due to IT efficiency, IT security and business effectiveness (such as compliance requirements), or business performance concerns.

Choosing and tracking good IAM metrics allow IAM planners, project managers, and performance managers to prove to the business that their respective IAM drivers have been addressed.

Like good information security metrics, good IAM metrics should also use action-oriented cardinal numbers (for example, ratios, such as the number of units per time period, or absolute numbers).



The Enterprise IAM Key Metrics Framework is a guide for assigning concrete, trackable metrics to IAM programs, focusing on three critical areas:

Security Efficiency
Time, Cost and Task Reduction

Security Effectiveness
Compliance and Risk Management

Business Performance
Measuring impact on users, stakeholders

Each organization will vary at some level in terms of specific activities or tasks to track, but this framework provides the foundation for developing an Enterprise Scorecard for IAM that tracks the value of the investment to IT and end users.

SECURITY EFFICIENCY

Security efficiency metrics focus on minimizing the time, money or other tangible resources required to perform administrative and operational tasks.

For example, security efficiency metrics demonstrate costs and timescales for IAM tasks and the success in reducing them. Business value here is linked to cost reduction, profitability, agility and workforce efficiency goals.

IAM metrics aimed at streamlining specific administrative and operational tasks and improving IAM performance are of particular interest to the designers and developers responsible for the IAM system itself. Examples can include:

METRIC TRACKED	VALUE
Number of Requests Processed Per Administrator	Evaluate password-related help desk calls, account lockouts, and self-service resets per month. This metric should generally trend downward, showing time saved in helpdesk support hours and increased user access and productivity.
Average Time to Provision (or de-Provision) Users	This shows how long a new user waits to get access to the resources they need to do their work. It has implicit productivity and ROI ramifications. Often, if someone doesn't get access to applications in a timely fashion, there are process issues behind the delay. This metric can flag a business process that needs to be reviewed and possibly adjusted.
Average Time to Authorize Changes	This metric can provide insight into the efficiency of an organization's approval processes. For example, if there are four people involved in approving a sales rep's access to Salesforce.com, but it takes two weeks for that approval to be granted, that's two weeks the sales rep is limited in his capacity to sell. Knowing how long it takes for approvals to be granted can help identify bottlenecks or out-of-date processes. This time should be reduced over time as processes improve.
Number of Reconciliation Exceptions	Reconciliation exceptions are typically caused be the inability of an IAM platform to reliably tie an identity to an account in a target system. This is usually the result of manual entry errors (that is, user names or unique identifiers are not matched), or worse yet, of an account created by backdoor channels. These exceptions should trend toward zero over time, reducing administrative overhead. Be sure to track error rates- specifically the Ratio of requests processed incorrectly to total number of requests, by type.
System performance (availability) expressed in comparison to Service Level Targets (SLT)	Each IAM system may have a different SLT; for example, a user provisioning system may have a lower availability target than an authentication service, because the unavailability impact is greater for authentication. This metric ensures the IAM system itself isn't a bottleneck. A good secondary metric to add here is the percent of user requests processed within a time frame prescribed by the SLA.

Example Security Efficiency Targets can include:

- Reduce password help desk calls by 75%
- Reduce total help desk call time by 25% (less requests, shorter user authentication)
- Reduce onboarding time from 3 days to 3 hours

SECURITY EFFECTIVENESS

Security effectiveness metrics are of most benefit to risk managers, compliance and legal. Metrics for security effectiveness can demonstrate risks to critical assets and the success in mitigating those risks.

IAM metrics that can aid in mitigating IT and operational risk through IAM are of particular interest to the IAM leadership and architects, as well as other information security and risk management leaders.
Tracking these metrics helps justify the IAM investment as a risk reducer, and can help identify risk in other business process areas.

Compliance and Risk Management
Good security effectiveness metrics focus on policy exceptions and timeliness, and the accuracy of remediation. Here are some examples of specific interest to Compliance and Risk Managers.

METRIC TRACKED	VALUE
Average Number of Distinct Credentials per User	The industry average ranges from 10 to 12 unique accounts per user. Organizations should strive to bring this average down as close to one as possible. Tracking this number is a reflection of IAM program adoption and helps identify "rogue" access scenarios.
Number of Uncorrelated Accounts	These are accounts that have no owner, and occur most frequently when a change happens, such as a promotion or a termination, and that person's accounts were not transitioned properly. Too many uncorrelated accounts can lead to unnecessary risks—they are open, live accounts that can be easily hijacked for un-authorized use.
Separation of Duty Violations	Examples of separation of duty violations include developers who have admin access to production databases and traders who can submit and approve their own transactions. These are more difficult to catch and measure, given their sophistication and cross-application nature, but are also the riskiest to miss, given the potential damage that could be inflicted if they're exploited.
Number of System or Privileged Accounts Without An Owner	Also known as "orphaned" accounts. They crop up when people who had the credentials to grant them access to important resources—making them privileged users—no longer need access to those resources but never had their privileges removed.
Number of New Accounts Provisioned	This number should closely follow the number of new joiners to the organization. An effective IAM program should always account for any new user who needs to be granted access to systems and applications. If there's a discrepancy or a significant lag between the number of provisioned accounts and the total number of new joiners for a given period, that indicates inefficient processes or poor identity data.

Another area of focus for effectiveness comes at access recertification time. A high number of exceptions is expected for new applications or user sets being brought under governance, but over time this should trend toward zero.

A consistently high number of exceptions is a strong indicator of poor identity data quality (lots of users having access that they should not have), or of process problems (person requesting re-certification does not have all the information they need to complete the process.)

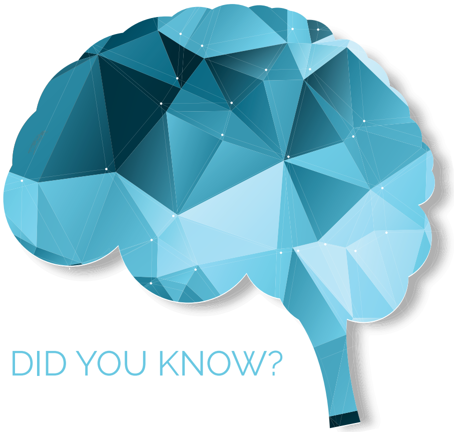
Going Deeper: Leveraging User Access Data for Process Improvement

In the event you don't see the topline metrics above improving, you can leverage IAM to go deeper, as there may be larger factors at play.

Simply automating processes for account administration can sometimes gloss over the issues that caused the original compliance or risk management problems. This results in gaps in account management that are difficult to detect, leading to a frustrating cycle of audit findings and remediation efforts that fail to address root problems.

If your organization has a number of disparate systems and processes, perhaps brought together through an M&A scenario, you may have to go deeper to expose and resolve process issues.

Here are some metrics to consider in this scenario.



By 2018, 75% of IGA products will provide process-driven effectiveness metrics that tie into key controls over user access, up from less than 10% today.

METRIC TRACKED	VALUE
Major Discretionary Entitlement Assignments	The number of entitlements where there are more direct request-based assignments than policy-based assignments. These entitlements may be candidates for refined policies or role definitions.
Average Percentage of Discretionary Assignments per Entitlement (Direct)	For every entitlement available for direct assignment through requests, the percentage of such assignments that are not consistent with policy. This can be used as a metric of role and policy health.
People Role Obsolescence	Total number of unused people roles, meaning the number of people roles that are not referenced in policy. General indicator of the health of the people role topology.
Resource Role Obsolescence	Total number of unused resource roles, meaning the number of resource roles that are not assigned to users. General indicator of the health of the resource role topology.
Uncertified Discretionary Entitlements Assignments	The number of request-based entitlements that have not been certified within a specific interval, based on the organization's preferred access certification interval. Indication of the number of discretionary entitlements that may not be subject to some type of expiration process.

BUSINESS PERFORMANCE

Business performance metrics demonstrate direct business value across a broad range of business goals, particularly those relating to accountability and transparency, but also regarding meeting other business imperatives and desirable outcomes.

Both IAM and business leaders are interested in metrics that enable better business decisions and inform business goals. For the business leadership, this is particularly true of business unit owners and other caretakers of key performance and key risk indicators.

Business performance metrics can vary greatly from organization to organization, but all start with adoption and satisfaction. Other examples can include:

METRIC TRACKED	VALUE
Service Level Effectiveness	Evaluate overall adoption, impact and satisfaction quarterly or semi-annually, depending on changes or events occurring within the business. A common equation for service-level effectiveness is: $\frac{\text{Total number of surveyed users with >=90\% satisfaction}}{\text{Total number of surveyed users}}$
New Project Velocity	How many new projects are leveraging IAM? How much time is saved per project on gaining security and compliance clearance via the IAM solution as opposed to the previous process? How much faster did the new product or feature get to end users, and how much is that increased time to users worth?
IAM Cost Management Index	Evaluate immediate and future cost savings options for IAM systems, starting with any consolidation opportunities with other internal identity management systems. Are there opportunities to stabilizing operational costs and increase service levels through managed service models?

The scale of IAM will massively increase.

Gartner projects that, by 2020, across all organizations globally, IAM will span billions of people, tens of billions of things, and tens to hundreds of trillions of relationships.

CONCLUSION

IAM initiatives must be consistently reviewed to track actual performance improvements against projections.

Discrepancies don't necessarily mean that the original proposal was flawed, because external factors might have changed. But it is possible and desirable to use metric trends throughout the initiative to guide remedial action, and the metrics themselves serve as a starting point for measuring IAM operational performance.

Customers often ask for values of metrics from other enterprises for comparison against their own IAM performance (the number of administrators is a common example). But even in similarly sized enterprises in the same vertical industry, such metrics can vary widely. The fact is that the "same" metric in different enterprises will be based on different assumptions (for example, exactly what is counted) and different dependencies (for example, the level of automation, organizational maturity and workforce turnover) and rarely form a solid basis of comparison between enterprises without laborious analysis.

The XMS Enterprise IAM Key Metrics Framework brings together the most important elements that organizations can find commonality (and the necessary flexibility) for proper cost justification and business value.

For nearly 10 years, XMS Solutions has served Enterprise IT departments worldwide. As a leader in collaboration, messaging and directory services, we saw how the distributed workforce, BYOD trends and growing demands for the cloud and data impacted our clients.

The rush of new people and things accessing collaboration systems enhanced employee productivity and customer integration- but also created new kinds of risk around scale and security. Our architects and delivery teams continued to design and deploy high-performance Microsoft collaboration platforms for Active Directory, Exchange, SharePoint and Skype for Business, scaling through the cloud, on-premise or a mix of both.

However, as more users, devices and machines required access, directory and governance policies were no longer enough. As the need for system access and user privileges scaled, compliance and security couldn't keep up. Our services have evolved with customer requirements around access, collaboration and security, focusing on identity-driven solutions that help the enterprise scale in a manageable and compliant fashion.

Our heritage in collaboration gives us a unique perspective on how systems are accessed, used and managed. Our partnerships give us the leading edge in designing, deploying and managing the best Enterprise IAM and Collaboration solutions on the market today.

Contact Us Today To Achieve Your Collaboration and IAM Goals

info@xmssolutions.com
702.940.6545