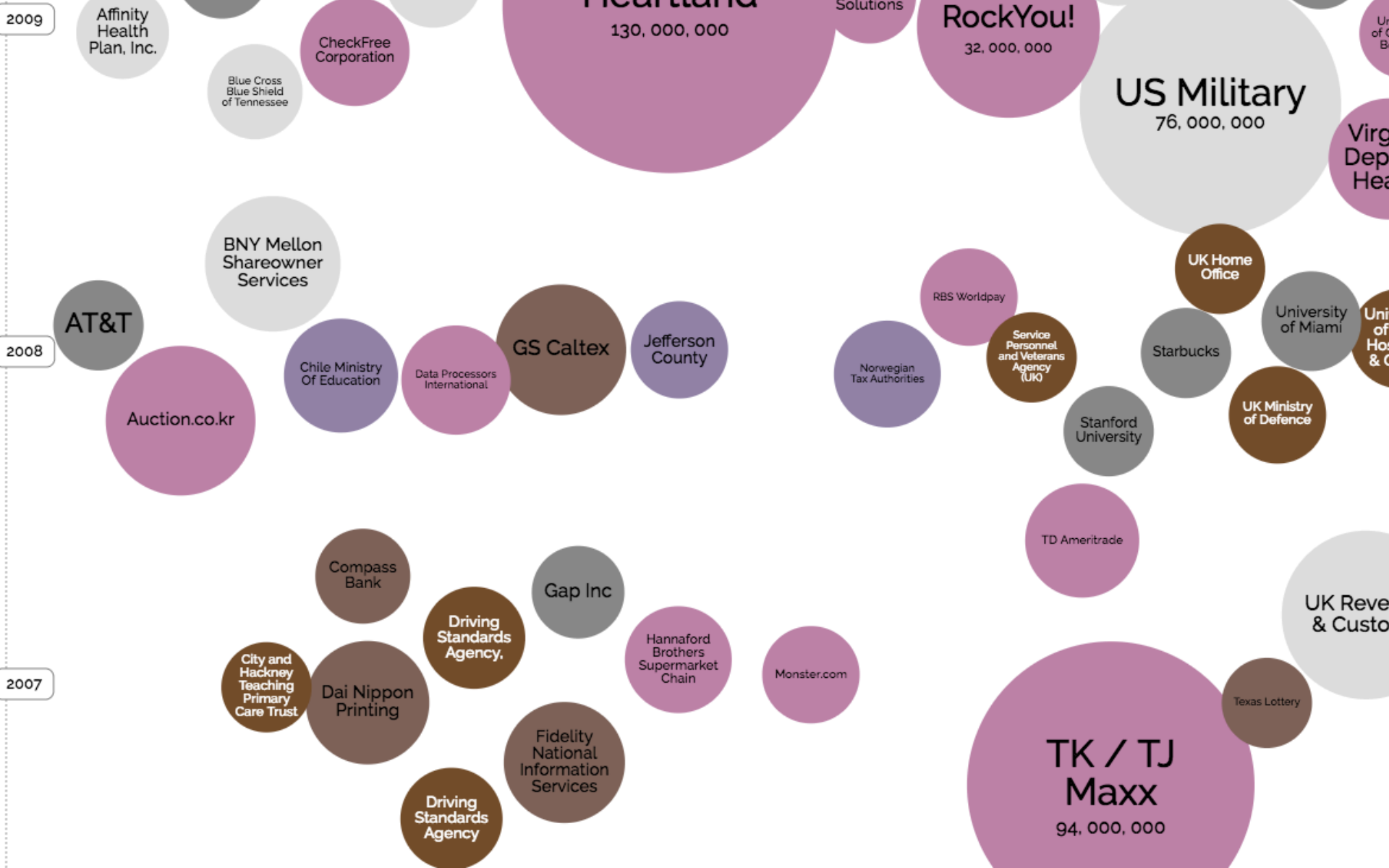
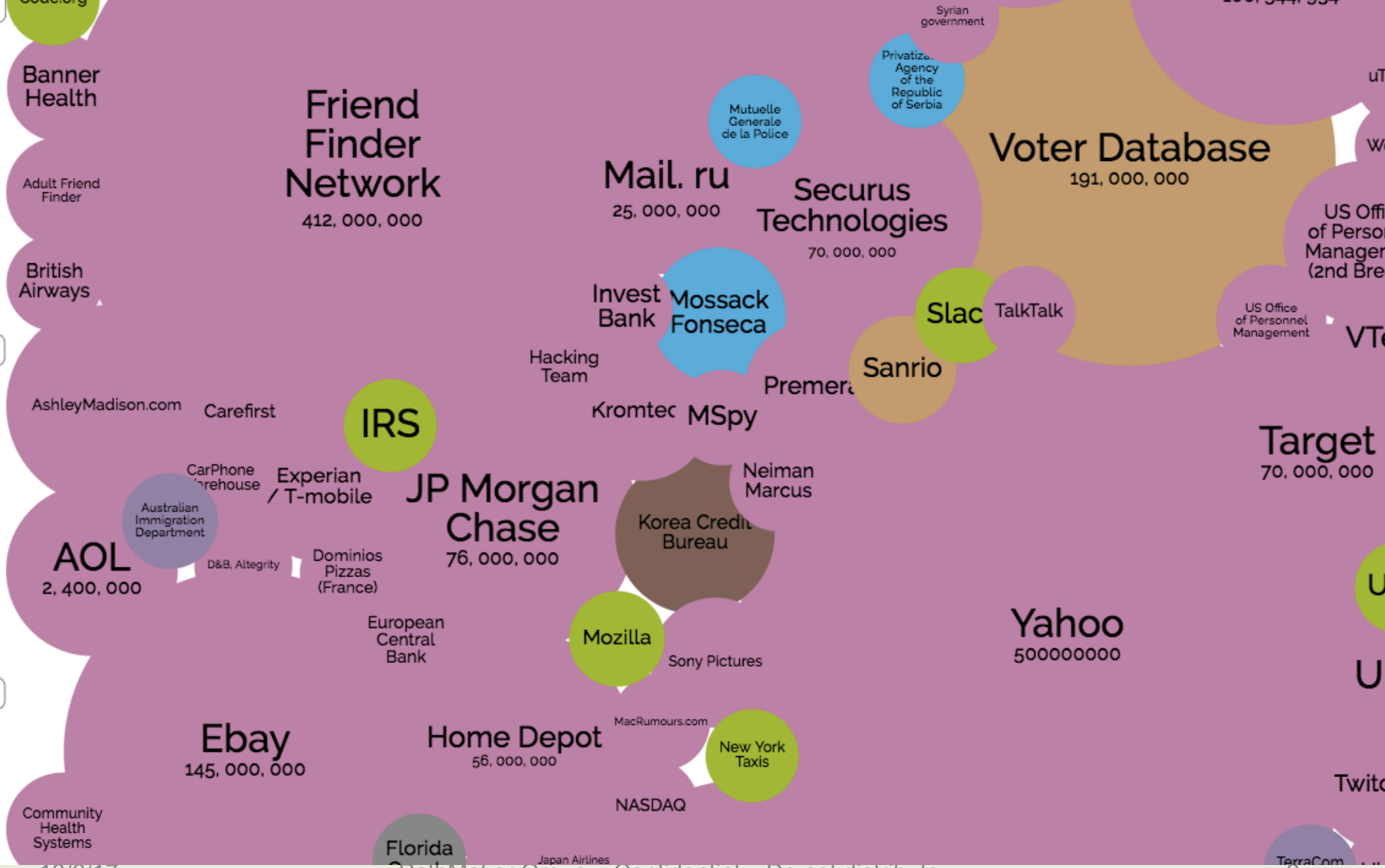
Benchmarking Identity Access Management Maturity

Keith Squires, President and CEO

October 2017


2009
Affinity Health Plan, Inc.
Blue Cross Blue Shield of Tennessee
CheckFree Corporation
Heartland
130, 000, 000
Solutions
RockYou!
32, 000, 000
US Military
76, 000, 000
Virg
Dep
Hea
2008
BNY Mellon Shareowner Services
AT&T
Auction.co.kr
Chile Ministry Of Education
Data Processors International
GS Caltex
Jefferson County
RBS Worldpay
Norwegian Tax Authorities
Service Personnel and Veterans Agency (UK)
UK Home Office
Starbucks
University of Miami
Stanford University
UK Ministry of Defence
TD Ameritrade
2007
Compass Bank
Gap Inc
Driving Standards Agency.
City and Hackney Teaching Primary Care Trust
Dai Nippon Printing
Hannaford Brothers Supermarket Chain
Monster.com
Fidelity National Information Services
Driving Standards Agency
Texas Lottery
TK / TJ Maxx
94, 000, 000
UK Reve
& Custo


2016
2015
2014
Banner Health
Adult Friend Finder
British Airways
AshleyMadison.com
Carefirst
CarPhone Warehouse
Australian Immigration Department
AOL
2, 400, 000
D&B, Altegrity
Dominios Pizzas (France)
Experian / T-mobile
IRS
JP Morgan Chase
76, 000, 000
European Central Bank
Ebay
145, 000, 000
Community Health Systems
Florida
Friend Finder Network
412, 000, 000
Mail. ru
25, 000, 000
Mutuelle Generale de la Police
Hacking Team
Invest Bank
Mossack Fonseca
Kromtec
MSpy
Premera
Securus Technologies
70, 000, 000
Syrian government
Privatiza... Agency of the Republic of Serbia
Voter Database
191, 000, 000
Slac
TalkTalk
Sanrio
US Office of Personnel Management
US Offi... of Perso... Manager... (2nd Bre...
VT...
Target
70, 000, 000
Neiman Marcus
Korea Credit Bureau
Mozilla
Sony Pictures
Yahoo
500000000
U...
Home Depot
56, 000, 000
MacRumours.com
New York Taxis
NASDAQ
Twitc...
Japan Airlines
TerraCom

"***Identity*** has been at the heart of most every breach in the past two years. Many of these breaches have involved someone gaining access by using compromised identity, then changing their identity once inside the network to ratchet up access to data and systems by taking over a privileged account and in the process gaining unlimited access to the network, to systems and to data."

-- Richard Kneeley, PwC US Managing Director, Cyber security and Privacy, The Global State of Information Security Survey 2017

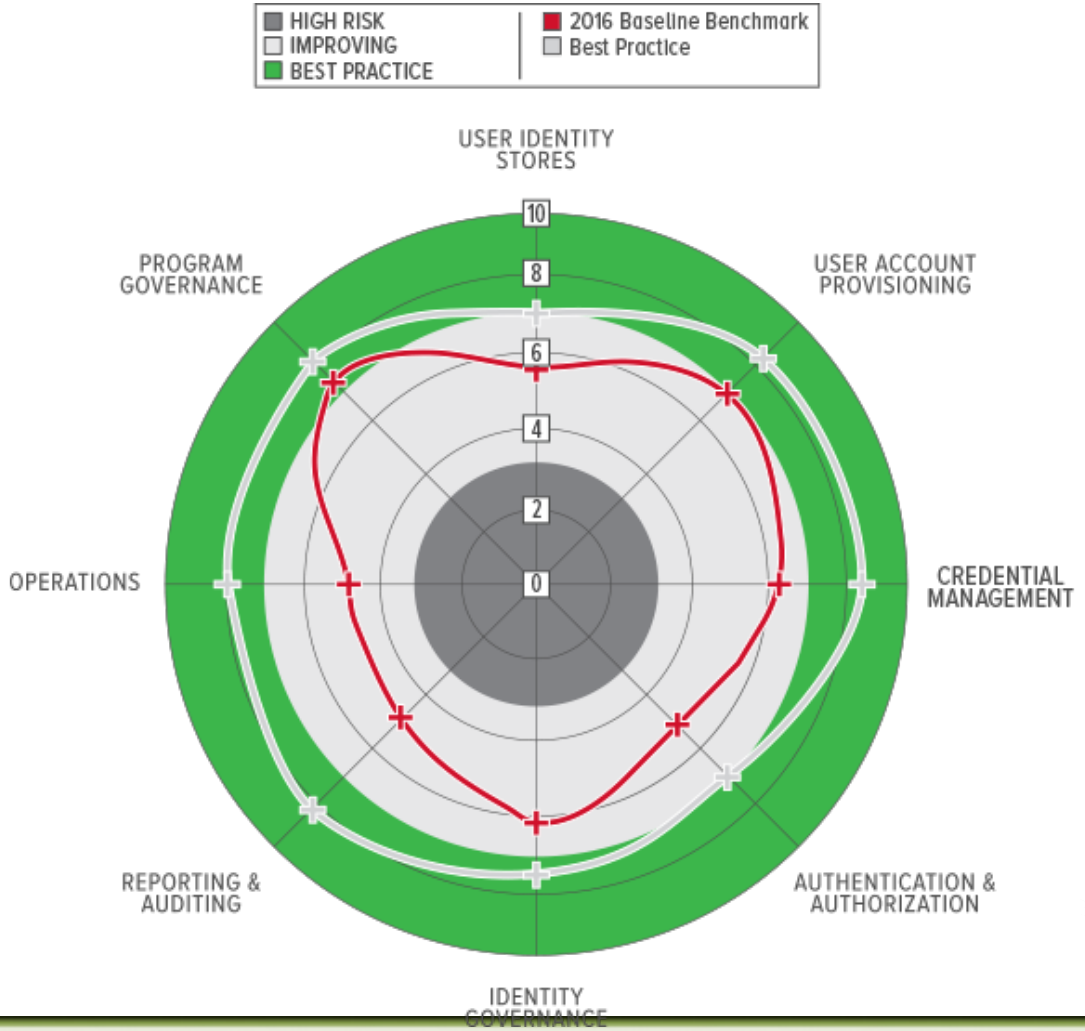

USER IDENTITY STORES
USER ACCOUNT PROVISIONING
CREDENTIAL MANAGEMENT
AUTHENTICATION & AUTHORIZATION
IDENTITY GOVERNANCE
REPORTING AND AUDITING
OPERATIONS
PROGRAM GOVERNANCE
IAM MAP™

PATHMAKER GROUP

At risk?

Improving?

Best practice?



CMM approach to scoring

Maturity model

A maturity model can be viewed as ***a set of structured levels*** that describe how well the behaviors, practices and processes of an organization can reliably and sustainably ***produce required outcomes***.

A maturity model can be ***used as a benchmark for comparison*** and as an aid to understanding - for example, for comparative assessment of different organizations where there is something in common that can be used as a basis for comparison.

Level 1 - Initial (Chaotic)

It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, ***uncontrolled and reactive*** manner by users or events. This provides a chaotic or ***unstable environment*** for the processes.

Level 2 - Repeatable

It is characteristic of processes at this level that ***some processes are repeatable***, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3 - Defined

It is characteristic of processes at this level that there are sets of defined and documented ***standard processes established*** and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.

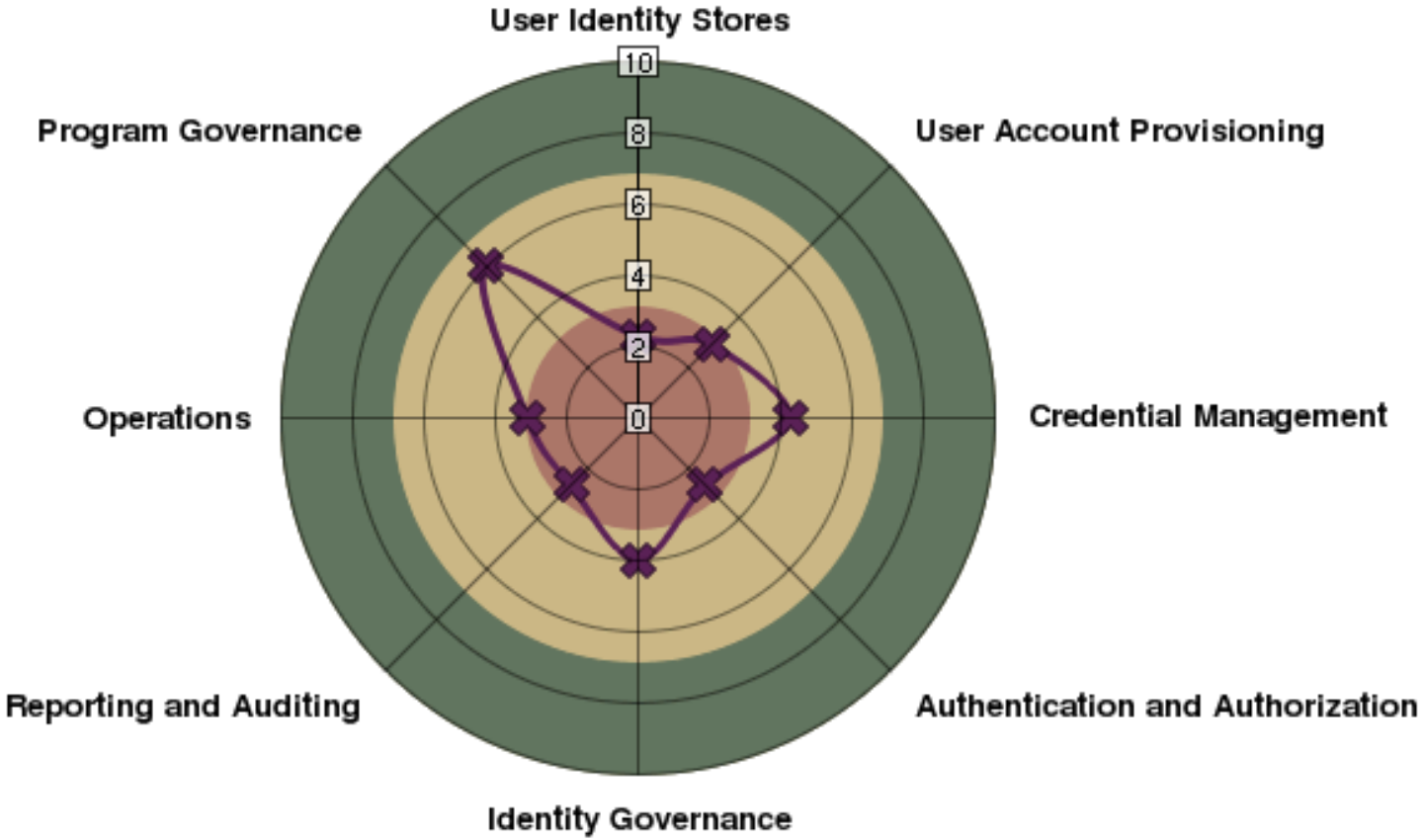
Level 4 - Managed

It is characteristic of processes at this level that, ***using process metrics, management can effectively control*** the AS-IS process. In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.

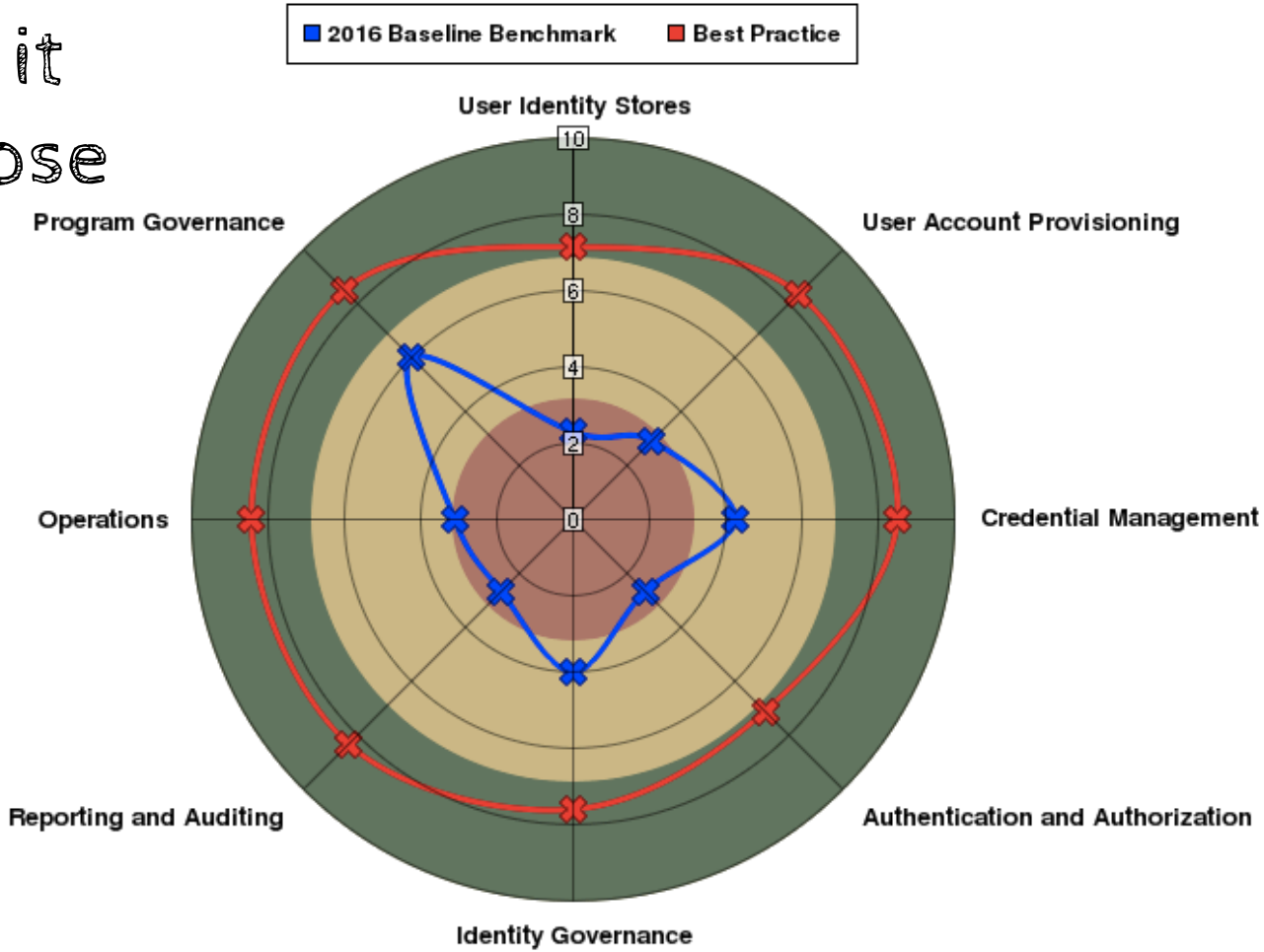
Level 5 - Optimizing

It is a characteristic of processes at this level that the ***focus is on continually improving process performance*** through both incremental and innovative technological changes/improvements.

Where is our risk?



What will it take to close gaps?



Build a Strong IAM Program by Benchmarking to Best Practice

1. Optimize existing solutions with better, simplified processes
2. Leverage investments by targeting best practices
3. Build a foundation for future growth
4. Establish a baseline with measurable progression to anchor stakeholder support
5. Show where, when and how you will invest budget dollars
6. Provide an organized, long-term view of the IAM program
7. Focus on the right order for key next steps
8. Make budgeting an orderly process, absent of surprises

8 Levers of IAM

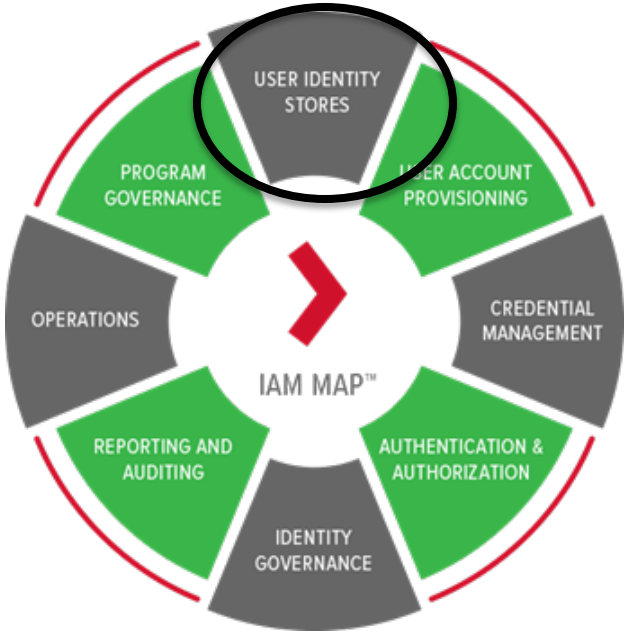
Central to the IAM MAP process is a benchmark called the '8 Levers of IAM Maturity' in an enterprise and it contains the 80 most important measures that a leader should look at to evaluate the progress of the IAM program.

By knowing where you are from poor to best in each lever at the strategic level, and each of the 80 measures at the tactical level, you can prioritize performance improvement and drive maturity up. The result is stronger overall security for your organization.

Lever 1 - User Identity Stores

How effectively and efficiently is the organization managing the number and accuracy of stores of user information across the enterprise?

Topics include attribute inventory, authoritative sources, synchronization, data consumers, redundant sources, data stewardship.



Help For Question 1 - Have you identified all of the sources of identity information and attributes within the enterprise?

Question 1 - Have you identified all of the sources of identity information and attributes within the enterprise?

Select one

- ○ Key identity stores and attributes have been identified and all consumers of user identity data have been identified and cataloged.
- ◉ All identity stores and attributes have been identified.
- ○ Key identity stores and attributes have been identified.
- ○ Identity stores have been identified but attributes have not been cataloged.
- ○ No dependable inventory of sources of identity data within our organization have been identified or a process has been started but is not completed.
- ○ No Answer

Lever 2 - User Account Provisioning

Account provisioning is the process of creating user accounts for systems and applications across the enterprise.

Topics include centralized control, workflow automation, access request, speed of account provisioning and de-provisioning, orphaned accounts, user id policy, roles, privileged accounts, service accounts.

Help For Question 6 - How well does the organization manage un-owned (orphaned) accounts?

Question 6 - How well does the organization manage un-owned (orphaned) accounts?

Select one

- ○ All orphaned accounts are easily identified and systematically removed on a timely basis.
- ◉ Orphaned accounts for most systems are identified systematically but removed manually.
- ○ Orphaned accounts for key systems are identified using a systematic process.
- ○ A process for removing orphaned accounts is being developed.
- ○ No formal process exists for removing orphaned accounts.
- ○ No Answer

Lever 3 - Credential Management

Managing passwords includes the initial creation and reset processes as well as establishing appropriate standards and policies.

Topics include password strength policies, password creation and issuance process, password management, synchronization, self-service, privileged access.

Help For Question 3 - How is the initial password/credential communicated to the new account owner?

Question 3 - How is the initial password/credential communicated to the new account owner?

Select one

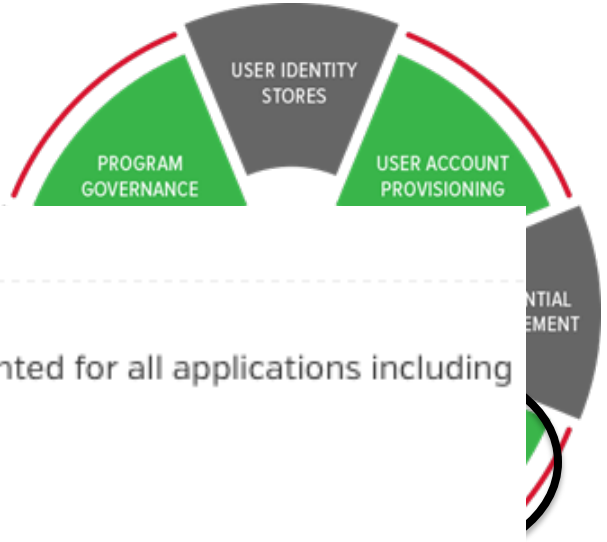
- (•) The account user either generates the credential or is the only one who receives the credential.
- ( ) The supervisor and the account user are notified automatically.
- ( ) An administrator creates the credential and the account user is notified manually.
- ( ) An administrator creates the credential and the supervisor communicates the information to the account user manually.
- ( ) No standard approach has been defined.
- ( ) No Answer

Lever 4 - Authentication and Authorization

Authentication and authorization is the process of proving who you are and that you are appropriately authorized to access information.

Topics include single sign-on, centralized authentication policy, access to cloud and mobile apps, multi-factor authentication, session management, behavioral anti-fraud analytics.

Help For Question 3 - How is access to externally hosted services managed?



Question 3 - How is access to externally hosted services managed?

Select one

- ○ A trusted authentication mechanism has been implemented for all applications including mobile applications.
- ◉ All web applications use a single login credential.
- ○ Key web applications use a single login credential.
- ○ Implementation of a common framework for external logins is in progress.
- ○ Each provider requires a separate set of login credentials.
- ○ No Answer

Lever 5 - Identity Governance

Identity Governance or role and compliance management is a set of processes that allows system owners to easily understand access rights, pro-actively manage user roles and privileges, and also satisfy possible audit and compliance requirements.

Topics include separation of duties, access certification, regulatory compliance, security policy, application risk review, transaction risk, role mining, user behavioral monitoring, role review, unstructured data governance.

Help For Question 2 - To what degree does the enterprise perform access certification?

Description

Question 2 - To what degree does the enterprise perform access certification?

Select one

- ○ An access certification process is in place for all systems with automated remediation.
- ◉ An access certification process is in place for most systems with both manual and automated remediation.
- ○ An access certification process is in place for key systems with manual remediation.
- ○ An access certification process is planned or in progress.
- ○ No access certification process is in place.
- ○ No Answer

track progress toward completion until each targeted group completes their work.

Help For Question 10 - Is the organization addressing high risk, unstructured data access concerns?

Question 10 - Is the organization addressing high risk, unstructured data access concerns?

Select one

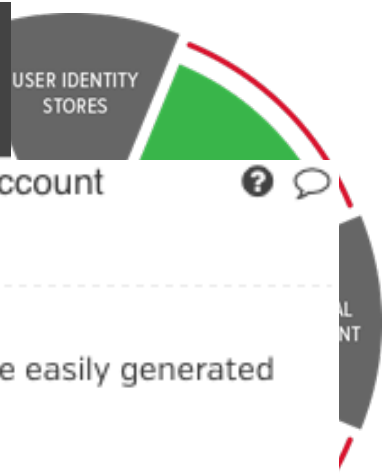
- ○ All high risk data has been identified and access is audited, monitored, and access policy violations produce alerts.
- ◉ All high risk data has been identified and access is periodically audited.
- ○ Most high risk data has been identified but access is not being audited or monitored.
- ○ A data discovery and classification process is planned or in progress.
- ○ High risk data has not been identified.
- ○ No Answer

Lever 6 - Reporting and Auditing

Fully featured IAM reporting and auditing provides a robust set of capabilities that can track all user life cycle activities, report the data for auditing and key metrics in a dynamic and flexible manner, and integrate the data into Security Intelligence tools for further correlation and analysis.

Topics include IAM reporting tools, SIEM integration, inventory reporting, account lifecycle reporting, KPIs for IAM, privileged account activity reporting, policy violations, orphan/dormant accounts, audit reporting.

Help For Question 4 - Does the organization leverage an IAM system to report all workflow or user account lifecycle activities?



Question 4 - Does the organization leverage an IAM system to report all workflow or user account lifecycle activities?

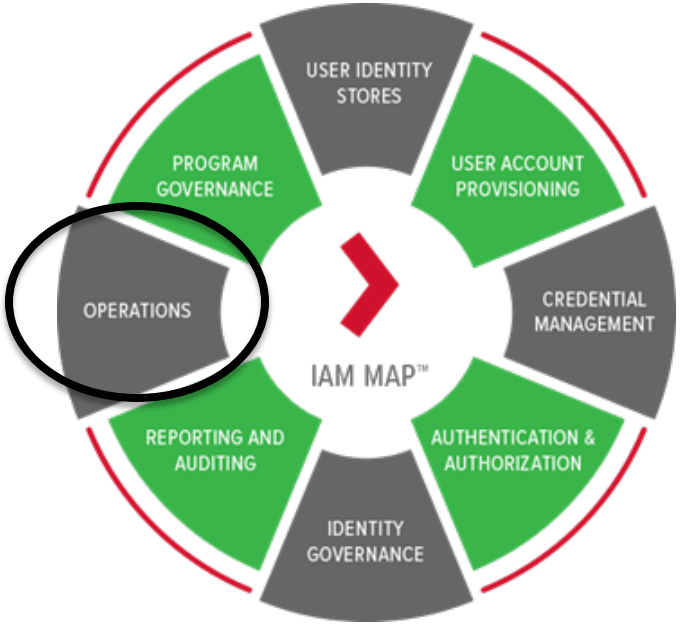
Select one

- ○ A comprehensive set of workflow and user account lifecycle reports can be easily generated including requests, approvals, password, and self-service actions.
- ◉ Most user account lifecycle reporting is generated automatically and runs on a scheduled basis.
- ○ Key user account lifecycle reporting can be generated automatically using a reporting tool.
- ○ A process to generate user account lifecycle reports using a reporting tool is planned or in progress.
- ○ Reporting on user account lifecycle events is produced manually.
- ○ No Answer

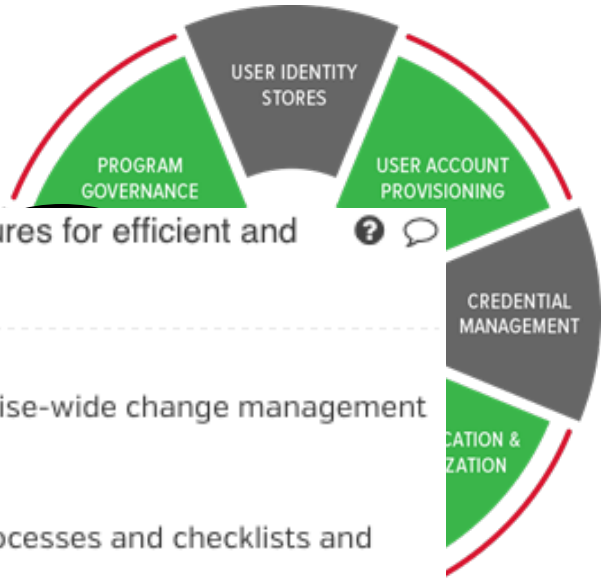
Lever 7 - Operations

A mature IAM operational model includes having a scalable, redundant architecture and infrastructure, the right on-premise vs. cloud mix, and the people and processes required to manage, operate, and support an IAM program.

Topics include operational support, outage recovery, ease of system maintenance and management, change management, root cause analysis, performance management, cloud management.



Help For Question 6 - Does the IAM support team follow standardized methods and procedures for efficient and prompt handling of all production changes?



Question 6 - Does the IAM support team follow standardized methods and procedures for efficient and prompt handling of all production changes?

Select one

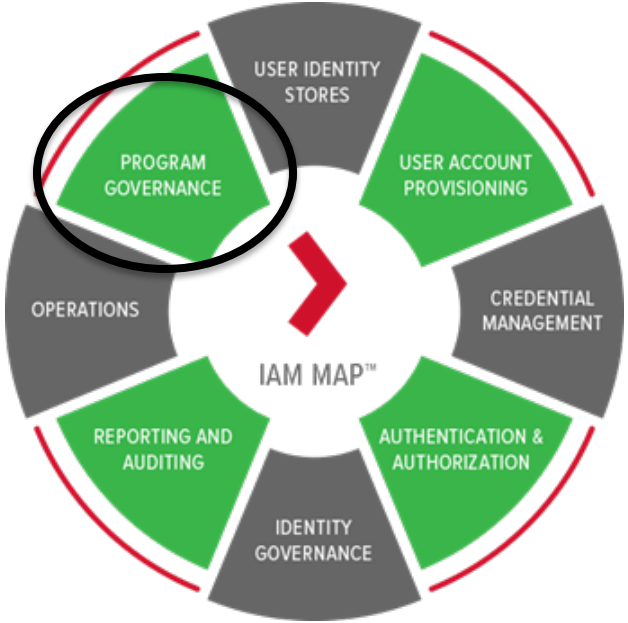
- ○ The organization, including the IAM team, follows formal, enterprise-wide change management standards and processes.
- ◉ The IAM team follows a repeatable process with standardized processes and checklists and includes management approval.
- ○ The IAM team follows a repeatable process with standardized processes and checklists.
- ○ A standardized change management approach is planned or in progress.
- ○ No standardized process is used to implement production system changes.
- ○ No Answer

of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of changes.

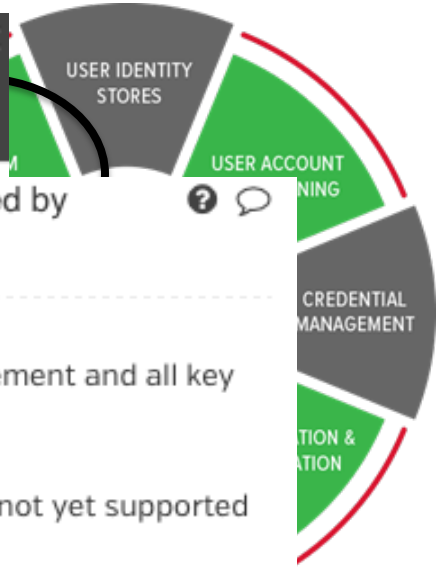
Lever 8 - Program Governance

An Identity and Access Management Governance program enables the enterprise to plan, establish, enforce and review the plans, policies, and procedures an enterprise will leverage to advance to a fully mature state.

Topics include program ownership, strategy and roadmap, steering committee, methodology, program metrics, IAM reference architecture, IAM system standards.



Help For Question 1 - Does someone in the organization "own" the IAM program and are they supported by management and stakeholders?



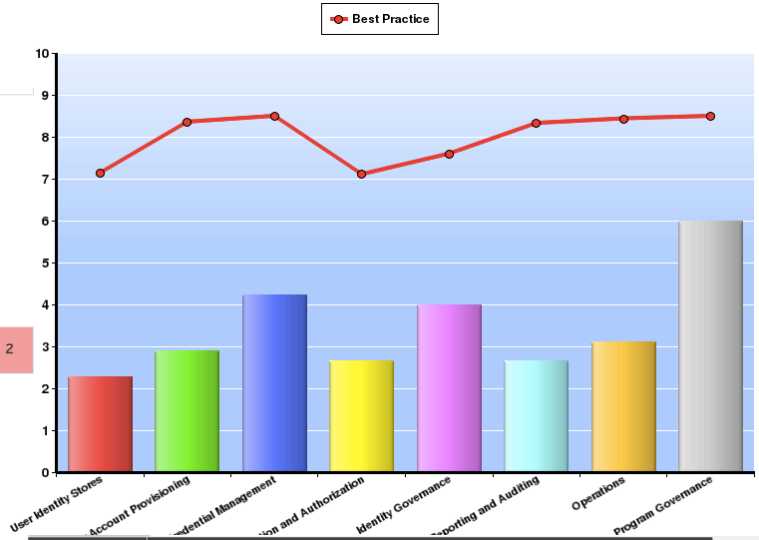
Question 1 - Does someone in the organization "own" the IAM program and are they supported by management and stakeholders?

Select one

- (●) A formal program owner is recognized and fully supported by senior management and all key stakeholders.
- ( ) There is a program owner supported by management but IAM initiatives are not yet supported throughout the enterprise.
- ( ) There is a program owner but the role is not known throughout the enterprise.
- ( ) There is an informal program owner but management or other organizational changes have challenged the effectiveness of the role.
- ( ) No program owner or champion exists.
- ( ) No Answer

IAM MAP Outputs

1) User Identity Stores	5.43	4	4	4	10	4	6	6				
2) User Account Provisioning	3.82	2	6	6	2	6	2	6	2	2	2	6
3) Credential Management	4.25	8	6	4	2	2	2	4	6			
4) Authentication and Authorization	2.89	2	2	2	2	2	8	2	2	4		
5) Identity Governance	5.2	2	6	8	10	6	6	2	8	2	2	
6) Reporting and Auditing	3.17	2	4	2	4	4	2	6	6	2	2	2	2
7) Operations	6.0	2	4	4	4	4	10	10	8	8		
8) Program Governance	5.25	4	4	6	8	4	8	4	4			



Lever	Main Benchmark	Best Practice
User Identity Stores	2.29	7.14
User Account Provisioning	2.91	8.36
Credential Management	4.25	8.5
Authentication and Authorization	2.67	7.11
Identity Governance	4.0	7.6
Reporting and Auditing	2.67	8.33
Operations	3.11	8.44
Program Governance	6.0	8.5

Lever	Question	Priorities	Timescale
2) User Account Provisioning	4) How quickly do new employees gain access to key applications and resources?	600	1 - 3 months
2) User Account Provisioning	6) How well does the organization manage un-owned (orphaned) accounts?	600	1 - 3 months
2) User Account Provisioning	10) How is the enterprise managing privileged access to applications and resources?	600	1 - 3 months
6) Reporting and Auditing	10) How does the organization identify and dispense with orphaned accounts?	525	1 - 3 months
6) Reporting and Auditing	11) How does the organization identify and dispense with dormant accounts?	525	1 - 3 months
1) User Identity Stores	1) Have you identified all of the sources of identity information and attributes within the enterprise?	500	1 - 3 months
1) User Identity Stores	2) Has the authoritative source for each user attribute been identified within the organization?	500	1 - 3 months
2) User Account Provisioning	1) To what degree has the enterprise centralized the account provisioning function?	384	3 - 6 months
6) Reporting and Auditing	3) Can the organization produce a comprehensive report of all systems, accounts, owners, and entitlements used across the enterprise?	315	6 - 12 months
7) Operations	1) Does the organization have the necessary people and skills to operate and support the IAM systems?	300	3 - 6 months
8) Program Governance	1) Does someone in the organization "own" the IAM program and are they supported by management and stakeholders?	300	1 - 3 months

Key Post Workshop Actions

1. Review heat map and take action on easier, short-term low hanging fruit (Create processes, leverage data for reporting, create application inventory, etc.)
2. Prioritize and sequence longer-term improvements using "work plan"
3. Model planned changes and review cost of risk gap closure
4. Build scope/budget and begin next major phase of work
5. Re-score IAM MAP after each major phase of work to track improvements

"Between half and two-thirds of organizations attempting to establish a truly-effective IAM program approach it in the wrong way. IAM process requirements should always precede organization and technology decisions. But currently, most IAM planning is done around clusters of technologies, rather than by addressing specific IT or business processes."

-- Earl Perkins, IAM Research Vice President at Gartner

Questions?
Download presentation at About Us/Resources

Keith Squires, PMP

President/CEO

PathMaker Group

817.704.3644

Email:

info@pathmaker-group.com

Website:

www.pathmaker-group.com

Dallas Office

635 Fritz Dr., Suite 110

Coppell, Texas 75019

Austin Office

1250 Capital of Texas Hwy S.

Building 3, Suite 400

Austin, Texas 78746

What our customers are saying . . .

"PathMaker Group is all in all just a great company. From top to bottom their people have integrity. They are personable, flexible, professional and a true partner with us. We can count on you to be there to pickup the phone at 2 am."

Chris Armstrong, BNSF Railway

"We view PathMaker Group as a true partner, as part of the team, and that matters a lot because they show concern for our business beyond just what they can get from us. They are our first option when we need help trying to solve a problem."

Mike Couvillon, Drilling Info

Over 400 IAM Projects Since 2003

Successfully Implementing IAM Since 2003