Insights on governance, risk and compliance

May 2013

Identity and access management

Beyond compliance

Ernst & Young

Quality In Everything We Do

Contents

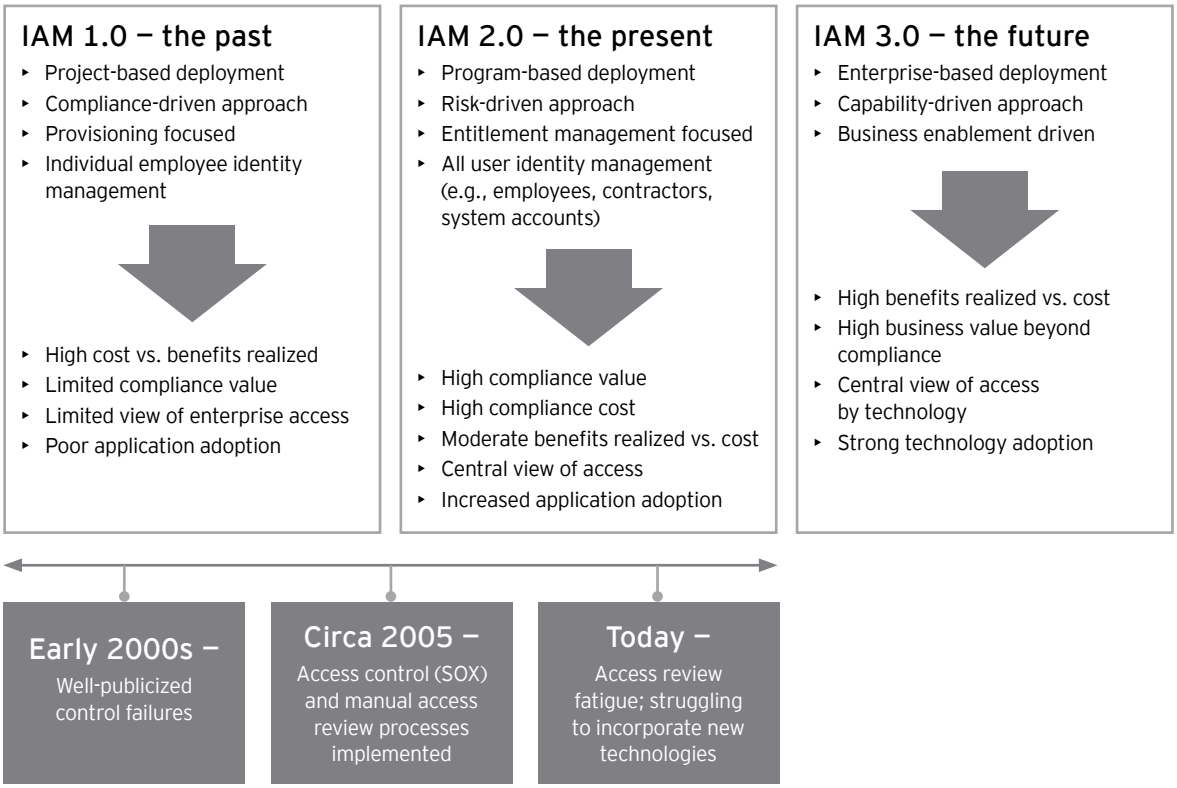
Evolution of IAM – moving beyond compliance

Identity and access management (IAM) is the discipline for managing access to enterprise resources. It is a foundational element of any information security program and one of the security areas that users interact with the most.

In the past, IAM was focused on establishing capabilities to support access management and access-related compliance needs. The solutions were often focused on provisioning technology and were poorly adopted; they also resulted in high costs and realized limited value. Organizations often struggled to meet compliance demands during this period, and the solutions were deployed to manage very few applications and systems. Centralized, standardized, automated identity management services designed to reduce risk, cost, improve operational efficiency continued to be elusive.

Many organizations now understand, or meet, their compliance requirements. While compliance is still a key driver in IAM initiatives, IAM is evolving into a risk-based program with capabilities focused on entitlement management and enforcement of logical access controls. Organizations are starting to achieve benefits from their IAM costs but are still challenged with managing time-intensive processes such as manual approval, provisioning and access review. Identity administration functions continue to be delivered in organizational silos resulting in users with excessive access, inefficient processes and higher cost of provisioning and de-provisioning.

As IAM continues to evolve, organizations will look to broader, enterprise-based solutions that are adaptable to new usage trends such as mobile and cloud computing. IAM capabilities will continue to leverage technologies to realize higher benefits versus the costs incurred. User demand will continue to drive the discipline to transform from a compliance-based program into a true business enabler (e.g., IAM is a key component for rolling out B2E and B2C applications that will drive operational efficiencies and improve the user experience) while helping to reduce risks created by emerging technologies and threats. To help reach the goal of an enabler that reduces risks, this IAM-focused paper explains life cycle phases, relevant IT trends, a capability maturity model, key considerations for transformation, tools and how to get started.



IAM life cycle phases

The management of identity and access permissions can be viewed as multiple stages.

The IAM life cycle diagram illustrates the stages that users proceed through when joining a business workforce and obtaining access to the tools and assets necessary to do their job. The IAM life cycle also includes stages to ensure that employees maintain appropriate access as they move within the organization with access being revoked or changed when they separate or change roles.

An IAM program requires a well-defined strategy and governance model to guide all the life cycle phases.

User access request and approve

Definition objective:

- Gaining access to the applications, systems and data required to be productive.

Common challenges:

- Processes differ by location, business unit and resource.
- Approvers have insufficient context of user access needs – do users really need access to private or confidential data.
- Users find it difficult to request required access.

Reconcile

Definition objective:

- Enforcing that access within the system, matching approved access levels.

Common challenges:

- Actual rights on systems exceed access levels that were originally approved/provisioned.
- There is no single authoritative identity repository for employees/non-employees.

Review and certify

Definition objective:

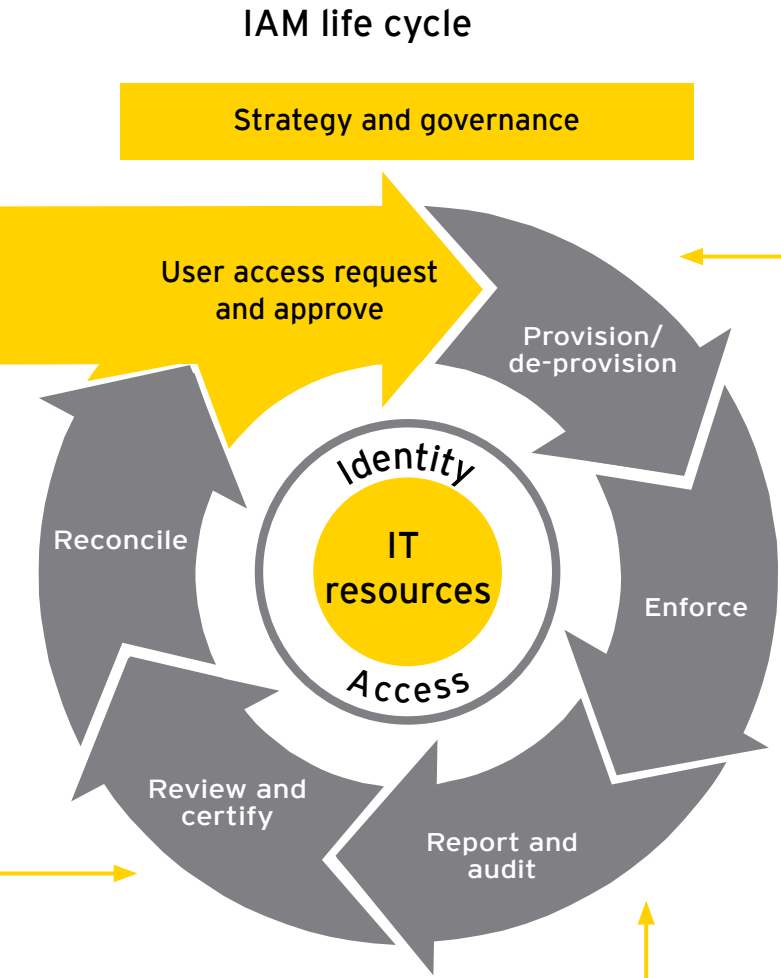
- Reviewing user access periodically to realign it with job function or role.

Common challenges:

- Processes are manual and differ by location, business unit and resource.
- Reviewers must complete multiple, redundant and granular access reviews.
- Reviewers have insufficient context of user access needs.

Governance should align the IAM program with both business objectives and the risk landscape. When solutions are focused on the business unit, they often fail to support the entire enterprise requirements and increase the cost of IAM. Typical pitfalls include the difficulty of managing access consistently across the enterprise and the increased complexity (which also drives up the cost) of incorporating new technologies into the existing IAM processes. Finally, it is essential to actively educate users about the policies behind IAM to support governance objectives, thus allowing IAM to quickly adapt to new trends.

IAM life cycle



Provision/de-provision

Definition objective:

- Granting users appropriate entitlements and access in a timely manner.
- Revoking access in a timely manner when no longer required due to termination or transfer.

Common challenges

- Time lines to grant/remove access are excessive.
- Inefficient and error-prone manual provisioning processes are used.
- Access profile cloning occurs inappropriately.
- Ad hoc job role to access profile mappings exist.
- Inappropriate access may not be de-provisioned.

Enforce

Definition objective:

- Enforcing user access to applications and systems using authentication and authorization.
- Enforcing compliance with access management policies and requirements.

Common challenges:

- Applications do not support central access management solutions (directories, web single sign-on).
- Access management policies do not exist.
- Role/rule-based access is used inconsistently.
- Segregation of duties (toxic combinations) is not enforced

Report and audit

Definition objective:

- Defining business-relevant key performance indicators (KPIs) and metrics.
- Auditing user access.

Common challenges

- KPIs/metrics do not exist or do not align with business-driven success criteria (e.g., reduce risk by removing terminated user access on the day of termination).
- Audits are labor intensive.

IAM and IT trends

Consumer demand is driving the corporate IT environment. Business demands for IT are changing rapidly — so too are the demands on IAM — resulting in the requirement to adopt emerging technologies (e.g., mobile and cloud computing, data loss prevention, and social media) earlier and more quickly.

IAM is a key element in enabling the use of these technologies and achieving business objectives, further emphasizing the need for IAM to grow beyond a mere compliance solution into a valued business tool.

Mobile computing

As today's workforce becomes more mobile, many organizations are adopting a bring your own device (BYOD) approach to provide remote access to email, sensitive or privacy-related data, and business applications. Consumer demand for mobile computing is also driving organizations to develop mobile applications to be used by customers to access their products. IAM is a strong enabler of mobile computing (both for business to employee and business to consumer) and serves as a foundational component in mobile computing security.

Here are a few ways IAM can help an organization implement a more secure mobile computing program:

- Security safeguards normally in place for external connections to a network may be disabled or implemented at a reduced level because the business may not have control over management of these devices (especially in a BYOD model). As a result, it is critical that authentication mechanisms are implemented to confirm that the user of the device is authorized to access sensitive resources.
- Mobile devices allow company personnel to access critical applications (including privacy-related data) any time and from anywhere. If a device is lost or stolen, the detection of compromised devices should not be left solely to user reporting. Device and user authentication attempts can help to detect a compromised device and reduce potential incidents of fraud.
- Access controls should be designed with usability in mind; without this, users may circumvent overly restrictive and inconvenient controls, resulting in potential data loss incidents. A common example is someone forwarding personally identifiable or confidential information unencrypted to a personal email account in order to access it outside of the office.

The proliferation of mobile devices (e.g., smartphones, tablets) and a strong consumer demand has driven organizations to adopt a BYOD model. This new reality has blurred the boundaries between home and office by providing constant access to email, sensitive data and even business applications enabling financial transactions.

To allow these devices to access the organizations' resources quickly and efficiently, mobile devices are set up to rely on identification mechanisms that verify and/or validate the user; security safeguards normally in place for external connections to a network may be disabled or implemented at a reduced level due to these mechanisms. As a result, it is critical that even stronger authentication mechanisms are implemented to confirm the user of the device is genuine and to safely allow users access to business critical applications anytime, anywhere.

Consumer demand for mobile computing is also driving organizations to develop mobile applications that customers can use to access their products. Mobile applications may allow consumers to access or transmit sensitive information (e.g., bank account information during an online transaction, private personal information submitted through a health insurance application). However, poor controls over authentication to the application, access to the data stored on the device by the application and external connections initiated by the application could increase the likelihood of a data compromise. IAM should be incorporated into application design, pre-implementation testing and periodic vulnerability scans/tests performed after implementation.

Cloud computing

The emergence of, and demand for, cloud computing services has complicated the IAM landscape as control over access to sensitive data is difficult to maintain in such an environment. This reality has forced many organizations to operate IAM capabilities internally and to invest in integration with similar capabilities provided by their cloud service provider. The adoption of cloud computing platforms have resulted in reduced reliance on network access controls and increased reliance on logical access controls offered by IAM services.

Several distinct scenarios have emerged with the evolution of cloud computing and IAM — there is a need to securely access applications hosted on the cloud, and there is a need to manage identities in cloud-based applications, including protecting personally identifiable information (PII). Federation, role-based access (RBAC) and cloud application identity management solutions have emerged to address these requirements.

The concept of **identity as a service** (IDaaS) is also an emerging solution to this challenge and has made it possible to accelerate the realization of benefits from IAM deployments. IDaaS aims to support federated authentication, authorization and provisioning. As an alternative to on-premise IAM solutions, IDaaS allows organizations to avoid the expense of extending their own IAM capabilities to their cloud service provider but to still support secure interaction with a cloud computing environment. When using IDaaS, instead of a traditional on-premise IAM system, these capabilities are provided by a third-party-hosted service provider.

However, unless cloud computing services form an organization's sole IT infrastructure, the need for IAM capabilities to manage access to internally hosted applications will persist. The truth of this hybrid operating model is that IDaaS will need IAM agents or appliances to operate within an organization's remaining IT infrastructure to completely outsource the function. Securing these agents and their interfaces represents a new source of risk for most organizations.

Regardless of the operating model used, cloud computing creates new IAM risks that must be managed. Management of virtual servers within the cloud requires elevated rights that when compromised, may give attackers the ability to gain control of the most valuable targets in the cloud. Such rights also give attackers the ability to create sophisticated data intercept capabilities that may be difficult for cloud providers to detect in a timely manner. The risk of undetected data loss, tampering and resultant fraud can be magnified by the use of cloud computing unless equally sophisticated controls are in place. As a result, the implementation of controls over cloud computing services should account for traditional and emerging risks that are unique to the cloud.

Data loss prevention

Given recent public incidents related to data loss, data protection is top of mind for many organizations. The first line of defense in protecting data is identity and access management. Data loss prevention (DLP) is a complementary information security discipline that can be enhanced when leveraged with IAM capabilities.

IAM tools can provide identity context to DLP tools to provide better monitoring capabilities. Properly controlling access to data will reduce the likelihood of a data loss incident — fewer users with access to data results in less opportunity for data to be inadvertently or intentionally compromised by an internal or external user. In addition, DLP and IAM tools can be integrated to provide more comprehensive monitoring capabilities.

A leading practice is to use an IAM tool to provide identity information to a DLP tool that continuously monitors sensitive transactions (e.g., financial statements, internal memos) to establish an identity correlation to the events monitored. The DLP tool is then set up to monitor for data loss events related to these complex, sensitive data elements. Any events detected are also correlated against data access levels and historical access behaviors recorded by the IAM tool to detect potential fraud. These solutions could be leveraged to address insider risk and emerging threat vectors, e.g., advanced persistent threats. By utilizing identity analytics using identity (human resource) entitlement and user activity data, we can deploy more effective privileged-user monitoring solutions for forensic analysis.

Properly implemented IAM can enable an organization to handle the fast pace of emerging IT trends — as highlighted here with mobile computing, cloud computing and DLP — but to determine where an IAM program stands, we need a frame of reference or a model.

Social media

Companies look to leverage social media to interact with their customers and increase brand awareness, however there are some serious IAM risks tied to these technologies. Legal, compliance, regulatory, operational and public relations issues are at the top of the list of potential social media risks that can ultimately cause loss of customers and erosion of market share and revenue. For example, on most of the popular sites (Twitter, Facebook and LinkedIn), users are able to create company profiles and communicate on behalf of the organization through social media channels. This can create marketplace confusion because of multiple messages and different audiences, policies and practices. There have been other instances where a company's reputation has been damaged when their public-facing social media accounts had been compromised and used to distribute fake updates that spread quickly.

You should provide IAM requirements to suppliers of the social media tools and services that you use to protect your accounts from being compromised; typical requirements include adding a second factor of authentication, receiving notifications of failed login attempts and receiving notifications of attempts to authenticate from geographic regions known to be the source for frequent attacks designed to gain control of social media accounts.

In addition to protecting company-owned social media accounts, it is also important to educate employees on the importance of using discretion with social media. Revealing too much information publicly on social media can enable attackers to get information to help them with social engineering or abusing self-service password resets. Employees can also reveal confidential information about what IAM controls are in place if they are not careful about what they post.

Properly implemented IAM can help an organization to handle the fast pace of emerging IT trends — as highlighted here with mobile computing, cloud computing, DLP and social media — but to determine where an IAM program stands, we need a frame of reference or a model.

IAM and cyber crime

Cyber crime, particularly the extent of economic and reputational damage that it can cause and the role that some nation states play in sponsoring corporate espionage, is a contentious issue. Regardless of the position that a company takes on the extent or viability of such threats, a strong IAM program helps to mitigate the effectiveness of some of a cyber criminal's tools: privilege escalation, reconnaissance, remote access, social engineering and data exfiltration.

The following techniques can help to counter these attack vectors:

- Privileged user review
- Password management
- Identity-enabled networking
- Authentication and access control
- Integration with data loss prevention (DLP) tools

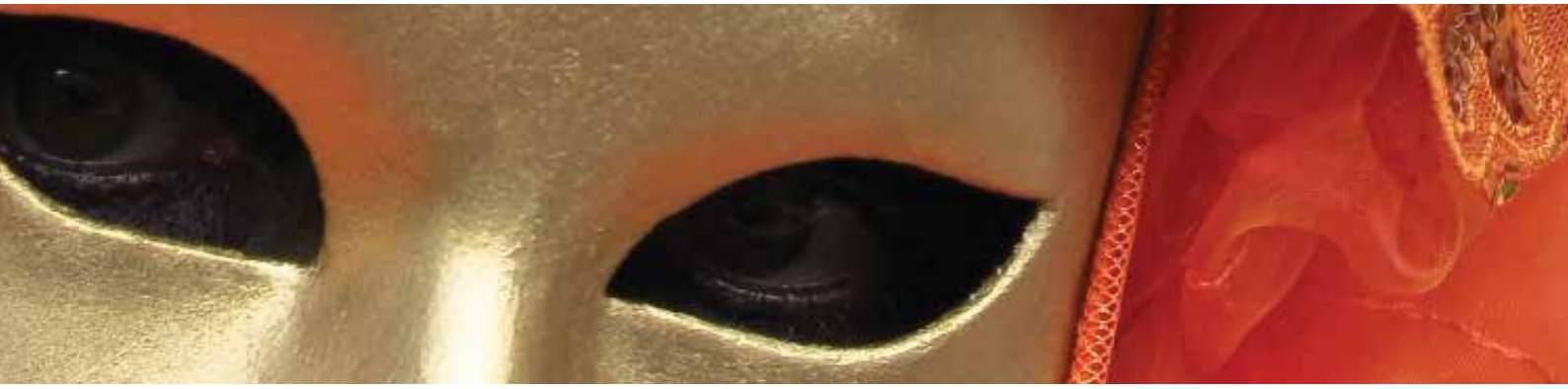
Capability maturity model

The following section outlines some of the maturity levels for the IAM life cycle phases and corresponding capabilities.

Identifying an organization's current IAM capabilities using a formal capability maturity model is the foundation for prioritizing investments to close compliance gaps (if needed) and identifying process improvements to drive cost reduction and reduce risk. Defining the desired state is fundamental to defining a strategy and road map for improvement of IAM capabilities.

Maturity level	Characteristics of capability			
	Processes	**Level of automation**	**Oversight**	**SLAs**
Optimized	When processes are automated, administrators will execute processes consistently	IT is used in an integrated way to automate procedures, providing tools to improve quality and effectiveness	Compliance with procedures is measured and action is taken where processes do not meet expectations	SLAs met or exceeded and targets are periodically reset to drive continuous process improvement
Managed	Processes are monitored for improvement opportunities and improved periodically	Automation/tools are used in a limited or fragmented manner		SLAs established and compliance is monitored/ measured
Defined	Standardized and documented	Processes are manual and time intensive	Responsibility is left to the individual to follow the process	SLAs established, but may not cover all administrators: may not be met consistently
Repeatable	Similar procedures are followed by people performing similar tasks; highly reliant on the knowledge of the individual			No SLAs established
Initial	Processes are informal and not standardized: applied on an ad hoc basis			

It is important to note that many organizations will not reach the "optimized" stage in all, or even some, of the areas of the maturity model. The level an organization should be at in the maturity model is dependent on the overall goals and strategy of the organization.



Case study — IAM in practice

Bank

Original state
Toxic access combinations existed, user provisioning processes did not address all relevant applications, and manual review processes proved ineffective and inefficient.

Challenges
Due to the number of business units impacted by the remediation efforts, there was a lack of consensus on the approach in addition to the risks of an ineffective access management environment.

Maturity-level transformation
Repeatable to managed

IAM solution
Short-term solution
Data analysis techniques were used to quickly identify segregation of duties conflicts across 800,000 entitlements (effort prioritized by application criticality).

Longer-term solution
The company implemented a standardized process for the provisioning and de-provisioning of user entitlements at the operating system, database and application levels.

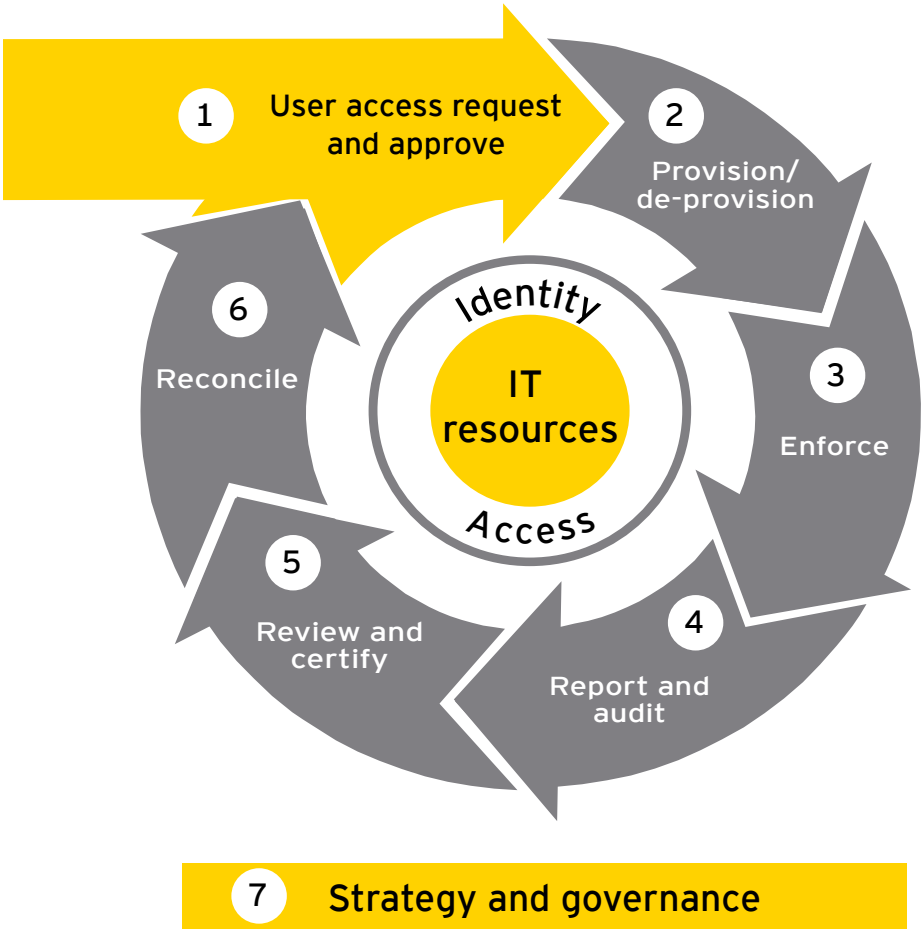
Benefits
The company developed segregation of duties remediation plans based on risk to address more than 6,000 accounts. Balance between short- and long-term solutions allowed the company to prioritize resources and funding.

Transforming IAM

To keep pace with IT trends and changing business needs, and to leverage the insights from the capability maturity model, the IAM function needs to be transformed.

IAM can be a highly manual process and still be effective in meeting an organization's goals, however in these instances the cost of labor is high and will likely outweigh the cost of technology. On the other side of the spectrum, a highly automated IAM program will have a very low cost of labor but a very high cost to implement and maintain. The key is finding the balance between the cost of labor and the cost of implementation and maintenance while still meeting the organization's overall business, security and IAM goals.

Transformation methods



	Life cycle phase
1	User access request and approve
2	Provision/ de-provision
3	Enforce
4	Report and audit
5	Review and certify
6	Reconcile
7	Strategy and governance

Steps to move to defined or managed maturity levels	Potential capabilities

▸ Deploy a centralized access request and approval process to increase adherence to SLAs and compliance requirements
▸ Integrate access profiles into the centralized process to enforce consistent requests and to streamline the process
▸ Use "real-world" roles (i.e., business-centric roles) to define appropriate access profiles to increase user's and approver's understanding of the access being requested, reduce the risk of excessive access, and align access requested with real-world job functions
▸ Support user self-service access request functionality to decrease the time needed to fulfill requests
	▸ Entitlement management
	  ▸ Role mining
	  ▸ Role definition
	  ▸ Role certification
	  ▸ Segregation of duty rules
	▸ Authoritative identity source
	▸ User request portal
	▸ Job role matrix or application access matrix

Deploy an automated provisioning solution to:
▸ Enforce consistent processes and segregation of duties
▸ Eliminate the need for basic access requests so users can obtain access needed to be productive faster
▸ Enable timely access creation and removal
▸ Adjust access upon termination or role change to reduce likelihood of retention of inappropriate access
	▸ Integrated identity and access service portal
	▸ Automated account provisioning
	▸ Advanced provisioning services
	  ▸ Automated access request and approval workflow
	  ▸ Role-driven or rule-driven access assignment

▸ Increase consistency of processes
▸ Maintain sensitive identity and credential information centrally
▸ Correlate use of shared and administrative access with specific users
▸ Detect potentially inappropriate use of administrative access
▸ Enforce the use of stronger passwords for administrative accounts
▸ Develop external authorization capabilities to reduce the likelihood of compromised passwords and reduce authentication overhead for users
▸ Deploy application access matrices, and role- and rule-based access, to reduce the risk of inappropriate access and to force the continuous alignment of access granted with real-world job functions
▸ Perform segregation of duties analysis to define toxic access combinations
▸ Integrate toxic access prevention capabilities into request, approval and provisioning processes
▸ Review privileged-user access logs for reasonability, and implement behavioral analysis tools to identify outlier activities
	▸ Password management
	  ▸ Shared password management
	  ▸ Privileged password management
	▸ Centralized authentication service
	▸ Risk-based authentication
	▸ Web access management
	▸ Enterprise (single sign on (SSO)
	▸ Entitlement management
	▸ Federation
	▸ Identity-enabled networking
	▸ Privileged access management
	  ▸ Administrative access monitoring
	  ▸ Behavioral analytics

▸ Define KPIs/reports to compare performance against success criteria ▸ Implement reports to support audit evidence requests in current and future solutions ▸ Reduce level of effort to support audits and enable sustained compliance	▸ Identity audit ▸ Continuous control monitoring ▸ Identity analytics

▸ Deploy a centralized, automated access review process to eliminate redundancy
▸ Establish risk-driven review cycles to reduce the amount of access to be reviewed during any given cycle
▸ Display roles in access review reports in lieu of granular access details to increase the reviewer's understanding and to reduce the likelihood of excessive access being retained
	▸ Advanced access certification
	  ▸ Periodic access certification
	  ▸ Job change access certification

▸ Configure automated provisioning solution to automatically adjust access if not approved ▸ Exceptions resolved by automated access adjustment should trigger a user-specific off-cycle access review	▸ Access reconciliation
▸ Assess the current state using a capability maturity model ▸ Define business-focused and risk-driven future state capabilities ▸ Develop an IAM strategy and transformation road map to close gaps between current and target states ▸ Align the leadership structure of the IAM program with the organization structure to institutionalize adaptation of IAM processes to meet evolving business needs, new technologies and regulatory requirements ▸ Periodically review IAM metric reports to confirm improvement as the road map is executed	▸ Asset inventory ▸ Identity data analytics ▸ Strategy and road map ▸ IAM policy definition ▸ Policy and control framework ▸ Continuous control monitoring ▸ IAM service-level management

Key considerations when transforming IAM

Having considered coming IT trends and evaluated your capability, you decide the time is right to transform your IAM program. The success of an IAM transformation depends on the interaction of people, processes and technology.

People

- Using a risk-based and business-centric approach, consider the downstream impact on organization structure as well as on key stakeholders including IT customers (business and operations), human resources, internal audit and users, so that any IAM enhancements can progress smoothly and with minimal disruption to the business.
- Avoid confusion and contention over priorities by appointing one executive-level "program owner" who is empowered to make decisions as required, supported by committed stakeholders and executive sponsors from across the organization. IAM enhancement programs should also have a dedicated program management team that operates using an integrated plan vetted by auditors and compliance managers.
- Be proactive in establishing ongoing support by designating an experienced operational manager as the "service owner" after the enhancements have been completed.
- Place experienced staff on the program execution team as it takes a long time to become skilled in IAM methodologies, control implementation, process reengineering, stakeholder alignment, and program and change management.

Process

- Integrate process improvements into awareness campaigns designed to educate users in order to increase adoption rates.
- Document access control processes and perform periodic testing to validate that processes are being followed.
- Inform key stakeholders early (and often) that business processes will have to change to accommodate the improvement of IAM capabilities. Temper that message with the fact that IAM can simplify processes by eliminating manual, error-prone access management procedures, including access requests, approvals and reviews.

Technology

- The leading IAM products have similar capabilities and can generally meet most IAM requirements; however, these products are likely to need configuration and even customization to meet IAM requirements that are unique to your organization.
- A key activity often included in transformation programs is to redefine access profiles in terms of roles so that they can be more easily understood (using business-friendly definitions that avoid technical jargon). Activities intended to produce such role definitions will often require the use of a sophisticated, configurable role mining technology that will suggest potential access profiles.
- The definition of a business-friendly name and description for these access profiles will require a substantial amount of analysis by subject matter resources that understand your business.

When integrating people, process and technology, organizations can be inundated by technology options. The next section addresses some of the important features.

Case study — IAM in practice

Healthcare organization

Original state
The majority of the access management functions were being performed in application and business unit silos using different processes.

Challenges
Service-level and compliance requirements were difficult to meet, and the operational silos led to a lack of accountability, ownership and resolution of issues.

Maturity-level transformation
Initial to defined

IAM solution
The company established an access transformation program with relevant stakeholders, application owners, HR and IAM representatives.

The company increased adoption of centralized automated services, implemented standard processes and scaled the central infrastructure to serve the access management needs of the business community.

Benefits
The company demonstrated access control compliance, effectively reduced access-related risks, increased efficiency and reduced costs related to access management functions.

IAM tools

As they evolve their IAM programs, organizations seeking to achieve higher levels of IAM maturity commonly will use commercially available products with the features listed in this table.

Life cycle phase	Technology features
User access request and approve	▸ Web-based self-service access requests ▸ Approval processes capable of supporting risk-based approval paths, approver notifications, delegation, segregation of duties rules, and escalations for failure to approve within service-level agreements (SLAs) ▸ Preapproved, automated access requests for "Day 1" access ▸ Role-based access profiles to drive complex access provisioning downstream
Provision/ de-provision	▸ Authoritative identity source integration to detect hire, transfer and termination triggers ▸ Configurable approval, provisioning and de-provisioning workflow, including automated escalation ▸ Automated provisioning and de-provisioning of access to target systems using standard protocols or native application program interfaces (APIs) ▸ Role-based access profile support
Enforce	▸ Policy-driven access control for web applications ▸ Centralized directory services used for authentication and authorization ▸ Web services-based authentication and authorization capabilities, including SAML (Security Assertion Mark-up Language) and XACML (eXtensible Access Control Mark-up Language) ▸ Federated authentication and authorization services, which may be web-based

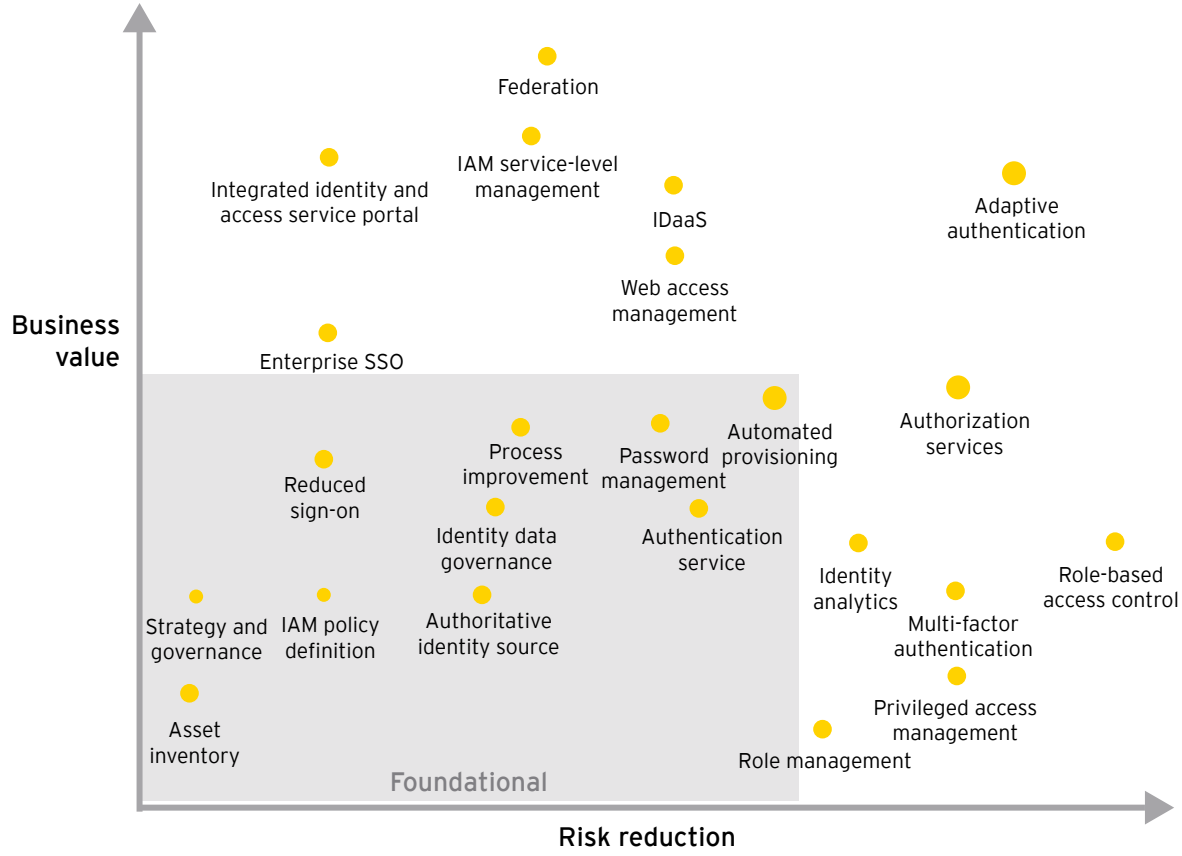
Life cycle phase	Technology features
Report and audit	▸ Identity analytics capable of identifying high-risk user access and behavior profiles, rule- and exception-based access analysis and reporting, and continuous access monitoring and reporting ▸ Generation of IAM service management metric reports.
Review and certify	▸ Configurable processes that support periodic, on-demand and user life cycle event-triggered access reviews — also referred to as attestations or certifications ▸ The capability to tag access with risk ratings to support more frequent periodic access reviews for higher risk access ▸ De-provisioning event generation to trigger revocation of access, which has been deemed inappropriate during access reviews
Reconcile	▸ Role- and rule-variance monitoring and reporting ▸ High-risk user analysis (i.e., outlier analysis, behavior profiling) ▸ Rules- and exception-based access analysis ▸ Role and rule variance monitoring
Strategy and governance	▸ Role management, including role and rule mining, role definition reviews, role ownership dispositioning in response to user life cycle events, such as transfers and terminations ▸ Governance, risk and compliance monitoring, including risk management and tracking, risk reporting dashboards, risk remediation plan tracking, data content and system configuration monitoring ▸ IAM service management dashboards supporting KPIs and metric reports generated via reporting and auditing technology

With the opportunities presented by the array of tools that support the people and processes needed to transform the maturity of an organization's IAM life cycle stage, it is natural to ask, "how do we get started?"

Getting started

When determining how to transform your IAM program, the diagram below illustrates the common IAM areas classified by business value and risk reduction.

The foundational areas serve as necessary building blocks for the other areas to be successful and should be implemented before other initiatives are started. The size of the circles defines the approximate level of effort of the area (i.e., bigger the circle, the higher level of effort) – this will help you to prioritize your action plan.



Key IAM capabilities

During the development of an IAM transformation plan, you should confirm that the following recommended capabilities are included:

- **Job role or application access matrices using rule mining tools**: this serves as the logical access foundation needed to embrace cloud-based and mobile applications in addition to ensuring appropriateness of access a key regulatory requirement, especially for data privacy.
- **Automated workflow-based access request and approval processes, using job role or application access matrices and segregation of duties checking**: this helps increase the consistency and efficiency of your IAM procedures and reduce the risk of inappropriate access.
- **Entitlement warehouse solution**: this accelerates the ability to address security and access management needs across a high volume of applications, host and database platforms within large organizations: it results in streamlined provisioning/access attestation and provides a centralized view of access privileges across systems.
- **Access proxy solutions, central authentication (application, host and database layers)**: this improves the end user experience and addresses key requirements around user de-provisioning.
- **Risk-based authentication solutions**: this addresses exposures related to compromise of basic authentication techniques, enables secure access for sensitive transactions (e.g., access to PII) and fulfills key regulatory requirements around multi-factor authentication.
- **Identity analytics and behavioral analysis services to integrate with DLP and security information and event management**: this helps to enable behavior-based profiling, identifies access outliers for risk-based verification and effective reduction of insider risk. Context-aware identity and access intelligence solutions are being used to identify anomalous activities/exception-based access, perform account analysis, and execute oversight and monitoring functions, helping to protect data governed by privacy regulations.
- **Data and access management process governance program, which includes HR, application owners, information security and IAM stakeholders**: this helps to confirm that the appropriate people (i.e., departments, roles) are supporting and sponsoring the IAM program — vital to the success of process and technology changes.
- **Federation solutions**: this improves end user experience and management of identities for cloud-based applications.
- **Consider emerging solutions that combine logical and physical security**: these solutions will address business risks related to critical infrastructure protection.
- **Design solution with future scalability requirements in mind**: these access transformation initiatives are impacted by negative end user experience, including performance delays; therefore, it is imperative to deploy solutions after considering future adoption and scalability requirements.

Key capabilities can focus your starting point, but why strive to transform your IAM program to higher maturity levels? How can it help drive business value?

Conclusion

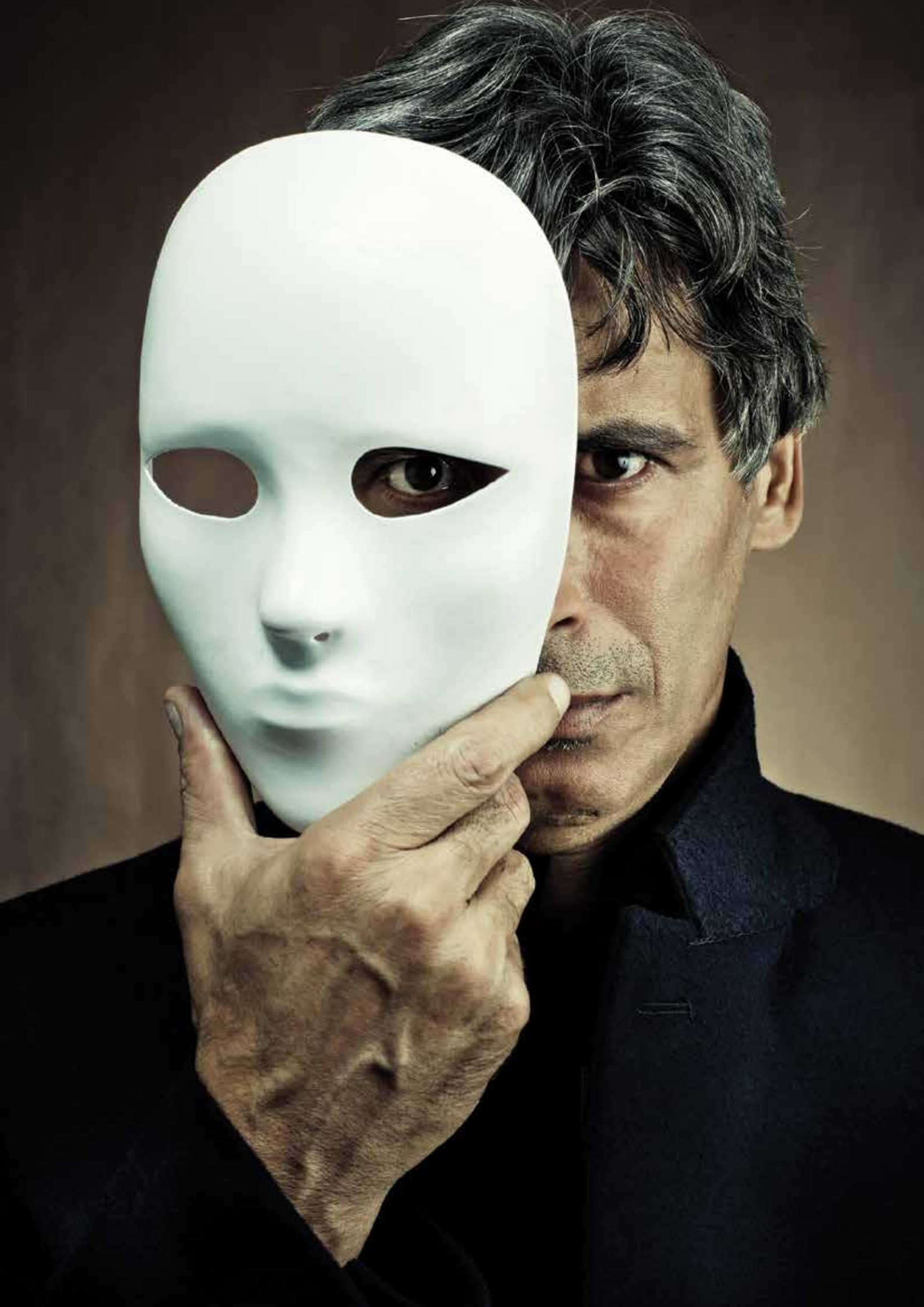
This paper examined the IAM life cycle phases; explored relevant IT trends; provided a capability maturity model; considered the people, processes and technology of transforming IAM; enumerated key features of tools; and showed how to get started.

Effective identity and access management processes are integral to driving business value — reducing risk, sustaining compliance, improving the end user experience and responding to the changing IT landscape.

Your organization should first assess your existing IAM capabilities using the capability maturity model and then develop a risk-based action plan.

Here are some guidelines for success:

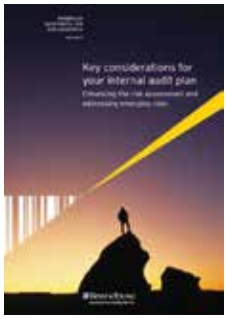
- Develop a strategy that is aligned to the needs of the business and considers people, processes and technology issues
- Don't think of IAM as an IT-only initiative, especially when it addresses business usage and regulatory requirements
- Be strategic, not tactical, when planning and designing a solution
- Because IAM is pervasive, be prepared for objections and concerns during any transformation process
- Avoid the "Big Bang" approach; use a risk-based, phased implementation approach to ease the integration and adoption of IAM changes
- Don't rush to buy and implement a tool without first considering the necessary business and process transformation requirements — tools do not guarantee enhancements in maturity
- Creating an inventory of applications, systems and definition of business-friendly access roles (profiles) are critical activities to ensure success of an IAM program and will take longer than expected
- Don't expect 100% assignment of access through roles; start with enterprise-level roles first, then move to business-unit-level roles and allow for exceptions



Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our *Insights on governance, risk and compliance* series at **www.ey.com/GRCinsights**



Key considerations for your internal audit: enhancing the risk assessment and addressing emerging risks
www.ey.com/IA_considerations

Smart control: transforming controls to reduce cost, enable growth and keep the busines safe
www.ey.com/SmartControl

Privacy trends 2013: the uphill climb continues
www.ey.com/PrivacyTrends

Fighting to close the gap: Ernst & Young's 2012 Global Information Security Survey
www.ey.com/giss2012

Ready for the challenge: integrated governance — the key to effective business continuity management
www.ey.com/IntegratedGovernance

Mobile device security: understanding vulnerabilities and managing risks
www.ey.com/MobileDeviceSecurity

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 167,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

About Ernst & Young's Advisory Services
The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 25,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

EYG no. AU1638

In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ED None

How Ernst & Young makes a difference

At Ernst & Young, our services focus on our clients' specific business needs and issues because we recognize that these are unique to that business.

Effective risk management is critical to helping modern organizations achieve their goals, and it offers the opportunity to accelerate performance while protecting against the uncertainties, barriers and pitfalls inherent in any business. Integrating sound risk management principles and practices throughout operational, financial and even cultural aspects of the organization can provide a competitive advantage in the market and drive cost-effective risk processes internally.

Our 15,000 Risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective support – wherever you are in the world. We work with you to develop an integrated, holistic approach to managing risk and can provide resources to address specific risk issues. We understand that to achieve your potential, you need tailored services as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or a member of our team listed below.

Contact details of our leaders

Global		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Randall J. Miller	+1 312 879 3536	randall.miller@ey.com
Areas		
Americas		
Michael L. Herrinton	+1 703 747 0935	michael.herrinton@ey.com
Bernard R. Wedge	+1 404 817 5120	bernard.wedge@ey.com
EMEIA		
Jonathan Blackmore	+44 20 7951 1616	jblackmore@uk.ey.com
Manuel Giralt Herrero	+34 91 572 7479	manuel.giraltherrero@es.ey.com
Asia-Pacific		
Jenny S. Chan	+86 21 2228 2602	jenny.s.chan@cn.ey.com
Rob Perry	+61 3 9288 8639	rob.perry@au.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp
Haruyoshi Yokokawa	+81 3 3503 2846	yokokawa-hrysh@shinnihon.or.jp