Identity and Access Management (IAM)
Emerging risks – a look beyond compliance
October 2013
## Agenda

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why we have to think about IAM differently</td>
<td>2</td>
</tr>
<tr>
<td>Emerging IAM solution options</td>
<td>8</td>
</tr>
<tr>
<td>Solution deployment considerations</td>
<td>12</td>
</tr>
<tr>
<td>Session summary</td>
<td>22</td>
</tr>
</tbody>
</table>
Why we have to think about IAM differently?
Traditional IAM challenges

Organizations are in the process of addressing traditional IAM challenges

Disparate, manual request, approval and deprovisioning processes

Manual and decentralized access management

Reactive and complex remediation approach for compliance

Impact to the business

- Organizations spending excessive time and money managing access
- Complex and difficult to manage legacy systems
- Difficult and time-consuming access review processes
- Users have excessive or inappropriate access
- Difficult to monitor, maintain and enforce compliance with access management policies
- Inadequate privileged access management processes

Identity and Access Management (IAM) | Emerging risk – a look beyond compliance
Key security challenges associated with IAM
Todays attacks are sophisticated

Traditional approach to access controls and signature-based detection are ineffective against modern attacks

Acquire target, sneak in, hop around
(Perimeter doesn’t help)

Get privileged access to critical assets
(Access controls and known threat signatures are ineffective)

Conduct the crime for an extended time
(Early detection and continuous monitoring matter)
Emerging threat landscape

Due to the evolving threat landscape, there is a need for improved logical access controls and solutions

- Introduction of advanced persistent threats, which proposed new risks to the business
- Compromised data can result in penalties and fines, negative brand impact and legal ramifications
- Using new platforms, such as cloud computing and mobile devices (BYOD), exposes the organization’s data to new threats, if not properly secured
- With the growth of big data, attackers have more opportunities to exploit new vulnerabilities introduced with new applications/systems within the organization
- New and emerging technologies require enhanced logical access and user activity monitoring
- Business and marketing departments are looking at using social identities. Bring your own identity (BYOI) to enhance end user experience
- BYOD and mobile device usage is leading to new device authentication requirements
# IAM technology trends

<table>
<thead>
<tr>
<th>Source</th>
<th>Quote</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gartner</td>
<td>“.. the Nexus of Forces—social, mobile, cloud and information—which is bringing new challenges and opportunities for identity and access management .. ”</td>
</tr>
<tr>
<td>Live PR</td>
<td>“Organizations are transitioning from traditional Identity (ID) management to cloud ID management..”</td>
</tr>
<tr>
<td>CIS 2013</td>
<td>“Growing socially verifiable attributes…” no more passwords , make it user friendly”</td>
</tr>
<tr>
<td>Generation Y employee</td>
<td>“Are you are seriously going to make me remember passwords for various devices and applications…”</td>
</tr>
<tr>
<td>EY</td>
<td>“ … Close-minded companies risk losing out on talented staff … ”</td>
</tr>
</tbody>
</table>
Emerging IAM solution options
IAM explained

IAM is the discipline for managing access to enterprise resources. It is a foundational element of any information security program.

IAM can be described by defining its core components:

► **Identity management**
  ► The processes and technologies collectively used to manage the life cycle of digital identities (profiles) for people, systems and services

► **Access management**
  ► The processes and technologies collectively used to manage authentication and levels of access within specific resources
IAM solutions to address emerging trends

Emerging trends require us to revisit traditional IAM solution frameworks

- Cloud applications
- On premise IDM solution
- Mobile applications
- Cloud IAM solutions
- Social, BYOI
- Identity intelligence
- Big data
- ID standards

Identity and Access Management (IAM) | Emerging risk – a look beyond compliance
### Evolution of IAM

#### Moving beyond compliance

<table>
<thead>
<tr>
<th>IAM 1.0 – the past</th>
<th>IAM 2.0 – the present</th>
<th>IAM 3.0 – the future</th>
</tr>
</thead>
<tbody>
<tr>
<td>► Project-based deployment</td>
<td>► Program-based deployment</td>
<td>► Enterprise-based deployment</td>
</tr>
<tr>
<td>► Compliance-driven approach</td>
<td>► Risk-driven approach</td>
<td>► Capability-driven approach</td>
</tr>
<tr>
<td>► Provisioning focused</td>
<td>► Entitlement management focused</td>
<td>► Business enablement driven</td>
</tr>
<tr>
<td>► Individual employee identity management</td>
<td>► All user identity management (e.g., employees, contractors, system accounts)</td>
<td>► High benefits realized vs. cost</td>
</tr>
<tr>
<td>► High cost vs. benefits realized</td>
<td>► High compliance value</td>
<td>► High business value beyond compliance</td>
</tr>
<tr>
<td>► Limited compliance value</td>
<td>► High compliance cost</td>
<td>► Central view of access by technology</td>
</tr>
<tr>
<td>► Limited view of enterprise access</td>
<td>► Moderate benefits realized vs. cost</td>
<td>► Strong technology adoption, standards based</td>
</tr>
<tr>
<td>► Poor application adoption</td>
<td>► Central view of access</td>
<td>► Leverages integrated security solutions</td>
</tr>
<tr>
<td></td>
<td>► Increased application adoption</td>
<td>► Consumer driven</td>
</tr>
</tbody>
</table>

Identity and Access Management (IAM) | Emerging risk – a look beyond compliance
Solution deployment considerations
Consideration 1: Tenets of BYOD/Mobile devices

If these tenets are not followed your BYOD program will not be successful

- Device independent – information accessible from any device
  - Platform independent
  - Ownership independent
  - Number of devices independent

- Location independent — information access from any location
  - Redefine the corporate perimeter

- Enhanced user experience — security solutions need to be user friendly
  - Security that inhibits workflow will be circumvented

- Protect the data — apply security controls as close to the data as possible
  - Avoid disrupting native user experience or reducing device functionality

- Timely innovation — rapid reaction time to changes in employee demand
  - Adapt at the speed of business
Consideration 1: Mobile IAM

**Consumerization and cost savings from the BYOD/I programs will drive the IAM solutions for mobile**

**Access provisioning**
- IT can provision and de-provision apps more easily and ensure that mobile app access for terminated employees is deactivated in a timely manner
- Seamless authentication experience without the need to type multiple user identity credentials
- Need to provision to multiple target systems, including mobile, on-premise and off-premise applications
- IT needs to make them available all in one place: a unified portal/app store
- Need to apply appropriate level of security, controls while minimizing end user impact and usability concerns

**Mobile SSO**
- Use standards-based solutions for simplifying enterprise-level mobile security through SSO
- This mobile SSO solution uses OAuth 2.0, OpenID Connect and PKI standards to leverage existing enterprise IAM investments
- Mobile SDK, which makes it simple for enterprise app developers to implement mobile SSO for iOS and Android devices
- Based on the identity of the user and the device, it determines the enterprise services available to that user on that device (e.g., using certificate-based identity improves the end-user experience, while providing IT with both higher reliability and an easier mechanism to revoke access)
Consideration 2: Understand business use cases

Factors that determine IAM implementation

- Risk reduction and security improvement
- Compliance requirements
- Improved end-user experience
- Cost containment and reduction
- User access request and approval requirements
- Provisioning and de-provisioning requirements
- Access requirements for application, databases, OS, cloud and mobile platforms
## Use case examples

<table>
<thead>
<tr>
<th>#</th>
<th>IAM services</th>
<th>Meet compliance requirement</th>
<th>Risk reduction</th>
<th>Increased efficiency and standardization</th>
<th>Improved user experience</th>
<th>Cost reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Automated provisioning</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2</td>
<td>Integrated identity access portal</td>
<td>NA</td>
<td>NA</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>3</td>
<td>Privileged access management</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>4</td>
<td>Credential management</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>5</td>
<td>Role management</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NA</td>
<td>✔</td>
</tr>
<tr>
<td>6</td>
<td>External authorization</td>
<td>NA</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NA</td>
</tr>
<tr>
<td>7</td>
<td>Shared authentication service</td>
<td>NA</td>
<td>✔</td>
<td>NA</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>8</td>
<td>Risk based authentication and ESSO</td>
<td>✔</td>
<td>✔</td>
<td>NA</td>
<td>✔</td>
<td>NA</td>
</tr>
</tbody>
</table>
## Use case examples (cont.)

<table>
<thead>
<tr>
<th>#</th>
<th>IAM services</th>
<th>Meet compliance requirement</th>
<th>Risk reduction</th>
<th>Increased efficiency and standardization</th>
<th>Improved user experience</th>
<th>Cost reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Reduced sign-on</td>
<td>NA</td>
<td>✓</td>
<td>NA</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>10</td>
<td>Identity federation</td>
<td>NA</td>
<td>✓</td>
<td>NA</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>11</td>
<td>Unique ID generation</td>
<td>NA</td>
<td>✓</td>
<td>✓</td>
<td>NA</td>
<td>✓</td>
</tr>
<tr>
<td>12</td>
<td>Authoritative source data management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>13</td>
<td>Risk based access and review certification</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>NA</td>
</tr>
<tr>
<td>14</td>
<td>Role certification</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>15</td>
<td>Privileged access monitoring</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>16</td>
<td>Identity and access intelligence</td>
<td>✓</td>
<td>✓</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>
Consideration 3: Centralized and risk-based access management

Centralized access management

- Improved end-user experience by using a single unique ID and enterprise password to access applications instead of the need to remember multiple usernames/passwords
- Upon implementation of this solution, customers can use the self-service capabilities to reset forgotten passwords
- Increase administration efficiency by automating account deprovisioning at multiple resources when a user is terminated
- Centralizing authentication will help enterprises meet regulatory compliance through timely termination/deactivation of user accounts
- Unified reporting and monitoring, security and scalability

Risk based access management

- Proactive fraud prevention
- Risk-based access management mitigates the risks with traditional authentication by using a dynamic authentication based on the risk of the transaction
- Real-time risk analysis based on contextual factors like location, device and behavioral profiling helps in proactively preventing fraud
- RBAM provides higher level of assurance that the users accessing the applications by verifying users identity before allowing access to the applications
- Provides virtual authentication features like Keypad to prevent phishing and malware threats
Consideration 4: Identity intelligence

Provides management with the ability to make intelligent decisions to improve accuracy and reduce the likelihood of inappropriate access, thus reducing risk to the client’s business.

- **Threat detection**
  - Support real-time data mining and threat detection against large data feeds
  - Automated correlation of identity and threat information across multiple internal and external sources

- **Identify riskiest access**
  - Select users with peer-group outlier analysis
  - Select users with minimal activity
  - Review and reduce this access to minimal necessary
  - Analytics for rapid, consistent and quality analysis across key sources

- **Risk-based access reviews**
  - Not all access reviewed during each access review cycle
  - Reduce number and monitor privileged users

- **Improve roles**
  - Reduce number of redundant and unused roles
  - Deep application visibility for business risk & compliance context
  - Advanced scoring and visualization for effective, efficient, continuous reporting
Consideration 5: Cloud IAM solution deployment

Speed of deployment, usability, emerging protocol standards and cost savings will drive the IAM solutions in the cloud space.

- Consider and review IAM services from the cloud, for the cloud and to the cloud.
- Use identity bridge to integrate your existing identity store (or stores if you have multiple) to handle authentication of users on cloud-based applications, consider solutions supporting SCIM (Simple Cloud Identity Management) protocol.
- Combination of on-premises identity management solution and bridges could be used to automate provisioning and de-provisioning of user accounts across applications based on policies and streamlining the process for the on-boarding and off-boarding of users.
- Ensures the business maintains both control and visibility over all user behaviors when accessing applications.
- Define application access rules and access control processes.
IAM deployment approach recommendations

Develop a strategy that is aligned to the needs of the business and considers people, processes and technology issues

► People
  ► Business-centric approach to security solutions
  ► Appoint one executive-level program owner
  ► Focus on deploying the top “essential” security controls

► Process
  ► Integrate process improvements into awareness campaigns designed to educate users to increase adoption rates
  ► Business processes will have to change to accommodate the improvement of IAM capabilities
  ► Create an inventory of applications, systems and definition of business-friendly access roles (profiles)

► Technology
  ► Avoid the “Big Bang” approach; use a risk-based, phased/iterative implementation approach to ease the integration and adoption of IAM changes
  ► Focus on refreshing your organization’s IAM strategy to accommodate AN/AZ transactions involving identities with varying levels of trust
  ► Leverage latest approaches to security solution deployment
  ► Leverage cloud-based technologies to rapidly deploy security solutions as business requirements change
Session summary
Key takeaways

Summary:

► IAM programs need to adapt to changing business and threat landscape

► Be strategic, not tactical, when planning and designing a solution

► Don’t think of IAM as an IT-only initiative, especially when it addresses business usage and regulatory requirements

► Don’t rush to buy and implement a tool without first considering the necessary business, process transformation and risk reduction requirements
Thank you

Ayan Roy
ayan.roy@ey.com
+1 949 437 0439

Kumar Chandramoulie
kumar.chandramoulie@ey.com
+1 949 437 0472
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization and may refer to one or more of the 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 ey.com.

© 2013 Ernst & Young LLP. 
All Rights Reserved.

1309-1140228 W(LA)
ED None

ey.com