How Identity and Access Management can enable Business Outcomes and Enterprise Security

Suresh Chandra Bose, Ganesh Bose
Srikanth, Thanjavur Ravindran

SureshChandra.GaneshBose@cognizant.com
Srikanth.ThanjavurRavindran@cognizant.com

©2014, Cognizant Technology Solutions
**Biography**

*Suresh Chandra Bose, Ganesh Bose* is a Manager Consulting at Cognizant Business Consulting practice. Suresh is based out of Austin, Texas and has been in the IT Industry for more than 16 years with vast Consulting experience in various industries and executed Strategic initiatives for various Fortune 100 companies in the areas of PMO, PPM, Process Consulting, Program Management, TMMI assessment/implementation, Organization Strategy, Test Consulting and CIO/Governance Dashboard/Metrics for various clients across the globe.

[SureshChandra.GaneshBose@cognizant.com](mailto:SureshChandra.GaneshBose@cognizant.com)

*Srikant Thanjavur Ravindran* is a Senior Consultant with Cognizant’s Business Consulting practice. Ravindran has diverse global experience with multiple Fortune 500 companies within the technology, telecommunications, oil & gas domains. His specialties include IT transformation, IT Strategy, ITSM, IT governance, risk management, information security, service delivery and infrastructure program management. He has published papers on topics such as BYOD, Identity and Access Management and IT Service Management at prestigious forums like ISACA and ITSMF.

[Srikant.ThanjavurRavindran@cognizant.com](mailto:Srikant.ThanjavurRavindran@cognizant.com)
## Contents

- What is IAM
- Introduction and Evolution into Identity Governance
- Industry Voices
- Key considerations for success in IAM
- Business case for automation of IAM
- Business & IT benefits
- Illustrating and augmenting through measures and Identity intelligence
- Q&A
In today’s consumer driven enterprises, infrastructures are **remote and distributed** while business and IT operations are pervasive through **mobile and virtual technology**.

Customer collaboration and Communication on **social platforms** and **service models** such as *(Bring Your Own Device) BYOD* and *(Bring Your Own Application) BYOA* have broadened the security perimeter and increased the risk exposure points.

In this scenario, the need for an identity and access management (IAM) solution has become paramount and is a top agenda item for most chief information officers (CIOs). In this session we will discuss key focus areas to **establish holistic IAM solutions** such as

- effective governance
- automated role management
- authentication
- user profiling
- integration

SMAC: social media analytics cloud; Texty, can we list these in bullets? Alternatively, you can bold and highlight certain words making them bigger so that it appears as a story summary but also looks like a wordle. Provided an example.
Looks ok. Can we introduce some animation so that the 1st para appears and then disappears, similarly for each of the subsequent sections (2nd para and bullets)
Animation would be good. When talking, emphasize on threat intelligence and access analytics and how it can enable relevant user activity monitoring and access management. Conversely talk about geo tagging and hackactive regions briefly when talking about monitoring.
Talk only about policy management, password mgmt, SSO and authentication (2 factor)
Talk about entitlements, provisioning, self service, password mgmt, user authentication, privileges mgmt, RBAC, device identification, geo tagging, transaction analysis and pattern recognition only.
Looks good. Can tie monitoring and analytics back to policy / rule repository and how real time findings can be compared with policies for anomalies.
Key considerations for success in IAM - Access Certification and Governance

Access Certification and Governance

- Automates discovery, analysis and management of user access rights
- Employs Least Privilege Access Principle (i.e. users are given access to only what is required to perform their job function)
- Facilitates periodic review and re-certification of access by business managers and data owners
- Ensures manual or automated remedial action to rectify access rights exceptions inconsistent with policy or regulatory requirements
- Demonstrates compliance with applicable regulations or business policies
- Enables multi-factor authentication such as biometrics for sensitive data or PI (personally identifiable information)

- Analyze data and identify Business rules
- Collection of access information and other data
- Work with business owners
- Analyze data from applications and identify Application access information

- Define Certification/ remediation strategy
- Define implementation plan
- Obtain Business sign-off

- Analyze data and identify Business rules
- Business Access Certification
- Privileged Access Certification
- Generic Account Certification
- Administrative Account Certification

- Certification: Sign-on certification and changes
- Remediation: Interface to change systems
- Validation: Follow-up to check that remediation has occurred
- Reporting: Audit, Process Progress, Coverage, Impact, centralized warehouse
Key considerations for success in IAM - Single Sign On (SSO)

- Employs identity federation for securely sharing digital identities with customers, partners and remote users across platforms
- Captures identities and record audit trails for web services transactions
- Externalizes entitlement logic from applications and achieves centralized security avoiding need for building security into individual applications thereby reducing complexity
- Enables secure delivery of service and cost effective online collaboration

Good with content listed. Advice is to stay at this level and not talk about SAML and other methods.
### Business & IT benefits

**Business benefits**
- Increased business user agility and improved business user productivity
- Improved compliance due to proper and periodic enforcement of controls
- Increased reliability due to predictable lead times and consistent quality
- Improved user experience
- Secure collaboration with customers, partners and employees

**IT benefits**
- Reduced labor and overhead costs
- Faster provisioning
- Multi-level Authentication combined with global Password policy models & seamless application integration for authorization
- Improved visibility and control over use of IT
- Enhanced logical access controls

Good with content listed
<table>
<thead>
<tr>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>While IAM is a complex initiative to identify measures for, analytics and measurements can go a long way in helping the organization achieve their business objectives. Types of metrics that can be measured are:</td>
</tr>
<tr>
<td>- Metrics that contribute to achieving customer outcomes and influencing them</td>
</tr>
<tr>
<td>- Metrics that impact financial performance and</td>
</tr>
<tr>
<td>- Metrics that monitor compliance</td>
</tr>
<tr>
<td>- These can be monitored at multiple levels such as strategic, tactical and operational to obtain a top-down 360 degree view</td>
</tr>
</tbody>
</table>
Illustrating and augmenting through measures - Identity intelligence

Analytic Reports

Identity intelligence should comprise of analytics on identity related status and trends. Some of the reports that could be generated for analysis are:

- Ambiguities in entitlements, user profiles, accounts and roles mapped to licensing
- Privileged user access and zombie accounts (accounts that remain active after user has switched roles or left the organization)
- DLP monitoring logs on sensitive transactions (financial statements, memos) and ambiguities in identities and entitlement level authentication
- Historical access information on transactions / events monitored
- Threats such as DDoS and APT can be monitored and reported upon and analyzed to enhance security capabilities
- Monitoring logs of privileged user accounts, as they would be vital for forensic analysis
- Access attempts from hackactive regions monitored using geotagging
Summary

Through the earlier sections we have established why IAM is no longer a debatable option but a definite need for organizations wanting to
• align themselves better through agile and flexible IT models
• save costs
• improve performance against compliance standards
• secure their information
• stay ahead of competitors

An effective IAM strategy coupled with innovative and best in class technologies with the above mentioned capabilities can be a true enabler of business process innovation and help in recognizing the maximum value of investments.

In a competitive business environment where business services are increasingly being delivered over collaborative and social platforms, IAM can prove to be a key enabler of differentiation in
• enterprise risk management
• compliance initiatives
• customer alignment
• relationship management
• reduced TCO
• increased productivity
• improved security

Let’s try and bulletize or use wordle format as in the summary slide
Let’s try and bulletize or use wordle format as in the summary slide
Questions?
GRACIAS

THANK YOU

BOLZİN MERCİ

Cognizant Technology Solutions
500 Genome Park Drive
Danvers, MA 01923-1583
Ph: 978-851-0293
Fax: 978-851-0293
Tel: 1-888-327-3277
Web: http://www.cognizant.com

All rights reserved. The information contained herein is subject to change without notice.

©2014, Cognizant Technology Solutions
<table>
<thead>
<tr>
<th>Glossary</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYOD - Bring Your Own Device</td>
</tr>
<tr>
<td>BYOA - Bring Your Own Application</td>
</tr>
<tr>
<td>IAM - Identity and Access Management</td>
</tr>
<tr>
<td>CIO - Chief Information Officer</td>
</tr>
<tr>
<td>ROI - Return On Investment</td>
</tr>
<tr>
<td>SaaS - Software as a Service</td>
</tr>
<tr>
<td>LOB - Line of Businesses</td>
</tr>
<tr>
<td>SoD - Segregation of Duties</td>
</tr>
<tr>
<td>PII - Personally Identifiable Information</td>
</tr>
<tr>
<td>SSO - Single Sign On</td>
</tr>
<tr>
<td>DLP - Data Loss Prevention</td>
</tr>
<tr>
<td>DDoS - Distributed Denial of Service</td>
</tr>
<tr>
<td>APT - Advanced Persistent Threats</td>
</tr>
<tr>
<td>TCO - Total cost of ownership</td>
</tr>
<tr>
<td>IT – Information Technology</td>
</tr>
<tr>
<td>IP - intellectual property</td>
</tr>
</tbody>
</table>
References


