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

Srikanth Thanjavur Ravindran
Suresh Chandra Bose Ganesh Bose

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

Abstract

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 disruptive 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 and integration.

Biography

Srikanth 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.

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.

Copyright Srikanth, Thanjavur Ravindran and Suresh Chandra Bose, Ganesh Bose
1 Introduction and Evolution into Identity Governance

The means of measuring business benefits of Identity and Access Management (IAM) initiatives and the ROI from IAM solution investments have been debated without much consensus in boardrooms virtually since the inception of technology. This has led to hesitation on the part of sponsors to endorse IAM undertakings leading to unrealistic deadlines, insufficient budgets and over worked staff.

During the past few years though, business agility has intensified, fueled by technologies such as cloud computing, remote infrastructures, mobility and BYOD / BYOA. IT has undergone shifts of its own due to disruptive service models in the form of multivendor outsourcing, Software as a Service (SaaS), multi-tenancy and virtual infrastructures. These shifts have increased the fear of the unknown due to organizational, customer, financial and IP data moving outside the organization’s security parameter. These changes have also given rise to a plethora of regulations with heightened penalties for noncompliance. All this has contributed to transform IAM from a process for managing access to data and systems to a governance mechanism. Some of the key objectives of IAM in today’s environment are:

- Service delivery to the business across hosted, remote, physical and virtual infrastructures
- Secure collaboration with customers, partners and employees
- Technology provision using access models spanning across web, mobile and application programming interfaces
- Role management through role definitions, user groups, identity verification, and authentication
- Compliance with regulatory requirements through personal data security, enhanced access control and privileges management
- Allow line of businesses (LOBs) to simplify access decisions based on trend analysis and save costs by rationalizing system licenses

2 Key considerations for success in IAM

![Image]

Organizations are failing at early breach detection, with more than 92% of breaches undetected by the breached organization. Situation can be improved with better threat intelligence, the addition of behavior profiling and better analytics. - Gartner Magic Quadrant for SIEM, 29 June 2014

Vendors that can provide quick integration, a wide array of supported applications, a full spectrum of IAM features, and high availability position themselves to deliver strong service and a lower total cost of ownership. - The Forrester Wave(TM): Enterprise Cloud Identity And Access Management, Q3 2012, Forrester Research, Inc.

Strong capabilities for access request management, access analytics, provisioning, access risk management, enhanced data governance, integration with Privilege Management or User Activity Monitoring are integral to Access Governance. - KuppingerCole Leadership Compass Access Governance

Figure 1: Voices In The Industry
Following are some essentials for a successful implementation of IAM:

**Figure 2: Implementation Considerations**

**Figure 3: Critical Success Factors**
2.1 Role Policy Management and Provisioning

- Provides real-time enforcement of policy/rule and role based user access to functional and data levels across all applications within an organization
- Provides centralized administration of roles/policies/rules/resources
- Serves as a central repository of role/policies/rule/resources, thus simplifying business intelligence and compliance audit data gathering efforts, and helps to create a more complete view of user access in an organization
- Supports enforcement of Segregation of Duties (SoD) preventing conflict of interest situations

2.2 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 PII (personally identifiable information)

2.3 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

Figure 4: Access Governance
- 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

2.4 Broad tenets of SSO:

- Web
- Cross Platform
- Federation
- Enterprise

![Diagram showing components of SSO](image)

Figure 5: Single Sign On

3 Business case for automation of IAM

Critical success factors for automation

![Diagram showing automation components](image)

Figure 6: Automation Components
Illustrating and augmenting through measures

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:

- Metrics that contribute to achieving customer outcomes and influencing them
- Metrics that impact financial performance and
- Metrics that monitor compliance
- These can be monitored at multiple levels such as strategic, tactical and operational to obtain a top-down 360 degree view

Figure 7: Business & IT benefits
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

5 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 and 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 and improved security.

6 Glossary

BYOD - Bring Your Own Device
BYOA - Bring Your Own Application
IAM - Identity and Access Management
CIO - Chief Information Officer
ROI - Return On Investment
SaaS - Software as a Service
LOB - Line of Businesses
SoD - Segregation of Duties
PII - Personally Identifiable Information
SSO - Single Sign On
DLP - Data Loss Prevention
DDoS - Distributed Denial of Service
APT - Advanced Persistent Threats
TCO - Total cost of ownership
IT – Information Technology
IP - intellectual property
8 References


