SCATTERED IDENTITIES- A GOVERNANCE NIGHTMARE!

Nachiketa Sharma, Ramana Kapavarapu

Nachiketa Sharma: nachiketa_sharma@rediffmail.com
Ramana Kapavarapu: ramkaps@gmail.com

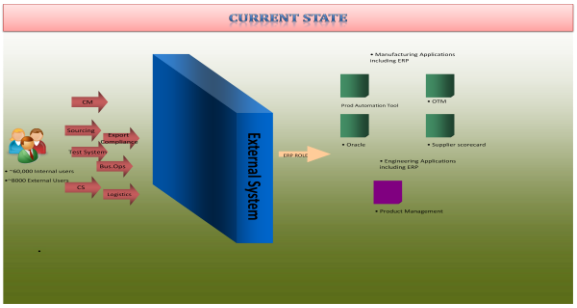
I. ABSTRACT

This study is aimed at describing the result of collaboration between a hi tech manufacturer and its partners to develop an identity management architecture. The fundamental goal of this architecture is flexible on-boarding which can in turn support quarterly quoting processes. Enabling smooth accessibility to forms, templates, and process documents. This will also increase direct communication of partners with suppliers via e-mail. Enhancing file exchange, archive and storage capabilities are other objectives. This study will help in creating a backbone and framework for next generation collaboration capabilities (ex. Instant messaging, Video on Demand). The transaction time will be reduced by providing access to the right set of tools and systems in one click and enhance security framework for all the data exchanges.

Key Words: Enterprise Security, SCM, IT Governance, Risk and Compliance, Hi Tech Manufacturing, Management Consulting

I. BACKGROUND

A hi-Tech manufacturer based out of US has numerous systems across its supply chain. Over the years, this company has acquired various competitors which resulted into myriad home grown, heterogeneous systems. Almost every supply chain process intersects with various systems.For instance, most of the manufacturing in this organization was done by a contract manufacturer, henceforth referred to as "CM". Personnel from Cam's facility access various data and processes from hi tech manufacturer's systems. Today, these accesses within the EARP and other legacy systems do not have a well defined framework. Multiple personnel have same set of identities which cut across various business functions, like planning, manufacturing, costing and logistics. Shown below is a pictorial representation of the Processes deployed across various systems.



I. PROBLEM STATEMENT

The organization under study had 20,000 Internal Users and another 1000 external partners. The supply chain comprises of approximately 60 different set of applications. In addition to these applications, the presence of ERP complicates the system landscape. Today, all the 1000 external partners get access to the systems, irrespective of the activity they perform and the role they play within their organization. Identities and roles of the users are not defined. Even within the global sourcing group, client is unable to hide the standard cost of the product and award pricing during quoting process. In addition to all this chaos, SOX poses another challenge. The process to revoke the user access is not in line with SOX mandate.All in all a nightmare for identities from an IT governance perspective. Today the external partners have to cherry pick an application from an ocean of application silos. Irrespective of the role of the partner logging into the system, he/she has to decide the application best suited for his/her needs. This involves manual discretion and more often than not leads to sheer waste of time and energy.

Key Drivers:

Establish standard processes and controls that are commensurate with the priorities for different types of intellectual asset data. Define and communicate security requirements that external third-parties need to comply with. These should, at a minimum, include:

- Type of data that needs to be protected
- Specific protection requirements (e.g., Client's data is segmented from other customers' data,

DOI: 10.5176_2010-2283_1.2.62

©2011 GSTF

only users working on Client's account have access to Client's data, etc.)

- User access monitoring and reporting

II. Methodology

To alleviate the above mentioned challenges, following solutions are proposed:

1. Create an IT governance framework to handle various identity management processes
2. Align various identities and roles with governance framework
3. Create new roles of external partners.
4. Create an exhaustive role repository.

Approach:

A multi pronged approach was followed to segregate various external partners dealing with the client. Most of the business was carried out via contract manufacturers and tier 2, component suppliers. It was felt that even before roles could be created, we had to have a detailed list of all supply chain processes each of contract manufacturer and component suppliers follow. These processes were broken down into the following phases

Plan: All systems and business processes within Supply Chain Planning function of supply chain were studied. Since, it's a contract manufacturing scenario; today the client shares its forecast details with its suppliers. In addition to it, the suppliers access demand planning tools to view backlog information. All these tools need identity based accesses. A rationalized list of roles was formed.

Make: Once actual demand is placed by the customers, the sales order is dropped to shop floor for manufacturing. During the manufacturing cycle, contract manufacturers have to access Actual BOM configurations along with compliance data. All these details are present on an internal system. All engineering and manufacturing subsidiary system acts as an appendage to the ERP system.

Source: The global sourcing group of the client is involved on various quoting processes with suppliers. Supplier exchange big files via FTP during quoting process.

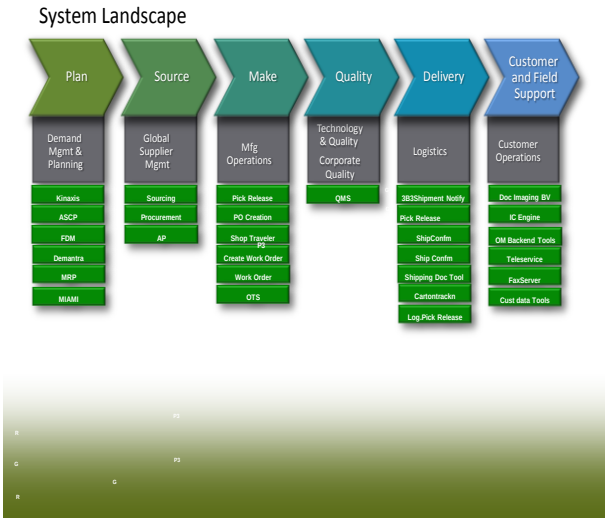
Deliver: 3PL partners access freight systems to make payments to freight provider. This again is routed via client's internal systems.

Creation of Tracks:

These processes were studied in separate tracks, namely

1. Contract Manufacturers Track
2. Component Suppliers Track
3. 3PL Partner Track
4. OEM/ODM Suppliers Track

Upon studying all the as-is processes of these partners, a comprehensive process list was created. Following is an exhibit of the system landscape present in the client's IT ecosystem.



Discussion & Principles:

The description of the components and their interaction contained in this document should provide an understanding of the identity management architecture and how it works. However, there are important questions that lie between the lines of this description, such as:

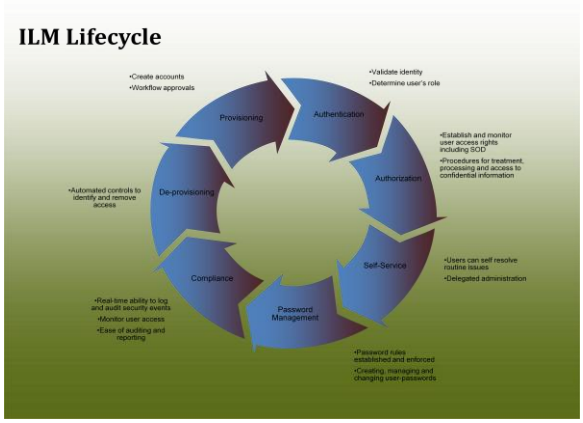
Why was ILM architecture selected? How is it different from other approaches? What are the advantages of this architecture?

©2011 GSTF

To address these questions, it may be more useful to review the underlying principles of the architecture.

- The architecture must be user-centric.
- The architecture must assist users in protecting privacy, and limit the amount of exposed personal information to the minimum required
- The architecture must be forward-looking, providing a target for existing systems to migrate towards.
- The components of the architecture must be as loosely coupled as possible to allow the identity management system to scale.
- The architecture must support and promote implementations based on open standards.
- The architecture must provide the flexibility to meet a broad range of identity-aware applications.
- The architecture must address high priority issues such as identity theft, identity proliferation, and inconsistent representation of identity across multiple government services.

Following diagram clearly depicts the lifecycle of this whole study:

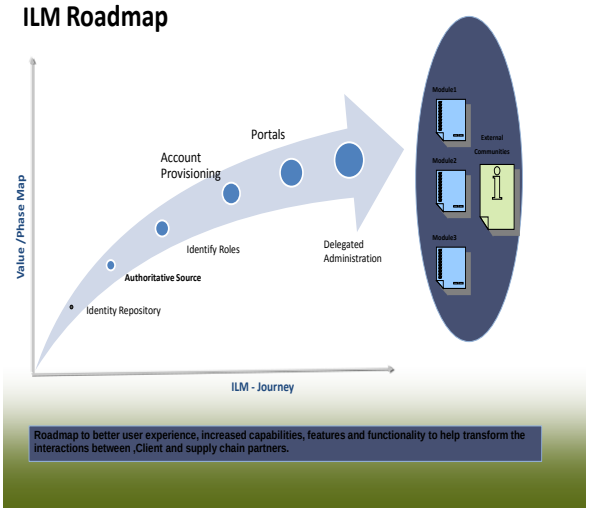


ROADMAP:

Study involved creating As-Is Process maps of each of the track for contract manufacturers and component suppliers. Following were the key processes for these partners.

1. Forecasting Process
2. Quotation and Contract Negotiation Process
3. Sales Order Management/Picking and Shipping Process

Picture below states the whole process of creating an identity repository and taking it all the way up to provisioning and administration.



In addition to the above mentioned framework, the study involved following activities to begin with:

- CM & Component Supplier Partner Sessions
  - Identify current processes
  - Identify systems, tools accessed as part of interactions with Client
- Design Roles
- Create Identity Repository
- Create Governance Framework

STUDY REPORTS AND TEMPLATES:

The whole study centered around creating a role repository and a governance framework. Following were some of the key templates and reports created as part of this study.

Role Design Template:

- Defines User Roles
- Uses position /responsibilities as inputs but not sole driver

©2011 GSTF

Role/Responsibility Name:		Oracle Technical Name:	
Business Process:		Sub-Process:	
Role/Responsibility Description:			
Key Elements of This Role/Responsibility/Key Questions to Ask When Mapping This Role/Responsibility:			
This Role/Responsibility Should Have The Following Variations (restrictions by organization structure or cost structure component (e.g. company code, location, etc.))			
The Security Access for this Role/Responsibility is Restricted by the Following Structural Authorizations (non organization structucture components.)			
If this Role/Responsibility is Mapped to a Position, the Following Other Role/Responsibilities Must Mapped:			
If this Role/Responsibility is Mapped to a Position, the Following Other Role/Responsibilitys Must NOT Be Mapped:			
Positions and/or Functions in the Current Organization That Would Map to This Role/Responsibility			
Special Skills Required for this Role/Responsibility			
Notes and Additional Requirements			

Role-to-Content Matrices

- One Matrix per major Operational Process
- Maps Role to types of Content and /or application(s)
- Detailed but critical for complete policy definition

Level	Menu	Sub-menu	Function	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)
(1, 2, or 3)	(Name)	(Name)	(Name)											

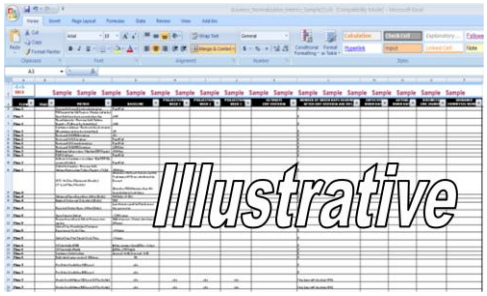
Position-to-Role Matrix

- One Matrix relates internal positions/ levels to User Roles
- Addresses indirect responsibilities

		(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)	(Responsibility)
1	Job Title										
2	Job Title										
3	Job Title										
4	Job Title										
etc.	etc.										

IM Governance Framework

- Responsibility matrix for setting, reviewing, approving, and managing access policies by role



WAY FORWARD:

A sound framework was created as part of this study. Both, the roles, Identity repository and Governance framework will be utilized to create Access Policies. This study has created a convincing reason for the customer to choose a Governance Model as the policy framework tool.

©2011 GSTF

Nachiketa Sharma is working as a Senior Consultant in US. He is a supply chain consultant with 10 Yrs of experience. He has thorough experience in SIPOC, Process Modeling, As-Is Process Mapping. He advises his clients in solving Supply Chain Challenges through various process modeling and technology deployments. He is an engineering graduate from Regional Engineering College, Trichy, India. He has completed Benchmarking, IT Portfolio Management Course from Stanford University. He is APICS SCM certified. He is also Oracle Procurement Champion & Oracle Technical Integration Champion certified by Oracle Corporation. He has worked with entire gamut of clientele in Hi-Tech, Discrete Manufacturing, Retail and Financial Services industries in US. He can be reached at nachiketa_sharma@rediffmail.com.

Ramana Kapavarapu is the Program Manager based out of U.S. He has been involved with information security, business process re-engineering and operational process improvement for that past 14 years. Over this time he has worked in many different processes such as manufacturing, financial services, health care and legal. He received his Bachelors and Masters in Industrial Engineering and also holds PMP and CISM certifications from ISACA.

©2011 GSTF