




Enabling Business through Agile Identity Management (or From Taming the Beast to Enabling the Business)


Enabling Business Outline

- 
- Corporate Profile/History
 - The Identity Beast
 - Taming the Beast
 - Enabling the Business
 - Efficient Access Management
 - Transparent Access Controls
 - Transparent and Consistent Compliance
 - Rapid and Compliant Merger Integration – The NCF Story
 - Transparent Compliance
 - Continuous Improvement


Corporate Profile

- 
- SunTrust Banks, Inc – now rated as 7th largest Bank in U.S. - recent merger – National Commerce Financial
 - History of a decentralized family of independent companies – 28 separate companies before “One Bank”
 - Established a single charter in 2001- ranked in top 10
 - The entire spectrum of Banking – Commercial, Retail, Trust & Investment, Venture, Insurance, Mortgage, etc.
 - Now has about 33,000 employees

The Identity Beast

- 
- Decentralized Security & Access Management
 - Determining who had access rights was time consuming
 - Modeling users was the standard practice
 - Service level was poor – took eight days for full access
 - Complex Technological Environment – “One of Everything”
 - RACF, Top Secret, NT, NDS, E55, E2K, Platform, CA, Home Grown and Legacy Apps, ACAPS, Internal Security Tables, etc
 - Eight distinctly different business units and user needs
 - Over 28,000+ users (employees and contractors)
 - Approximately 1000 (part time) security admin = 60 FTEs

The Beast

- 
- All this in an ever changing environment
 - New applications/revisions every month
 - Everything is *being* migrated to RACF, AD, E2K
 - Growing number of outsourced vendors and ASPs
 - Request were difficult on the user and administrator
 - Access Modeling was the norm
 - Manager did not know what employees had or needed
 - Attestation of access not practical

The Beast




A grid of eight pages of highly redacted and obscured text, likely a technical document or report. The pages are arranged in two rows of four. Each page contains a mix of blue, red, and black text, with significant portions obscured by yellow and black redaction boxes. The text is dense and appears to be a mix of headers, body text, and tables. The pages are labeled with '00-00100' and a small 'c' in the bottom left corner of each page.

Taming the Beast

- Identifying what each Security Admin did
- Collapsing Admin Duties in a structured way
 - Phased approach over a period about 18 months
 - Consolidated ISS offices
 - Consolidated Platform Security
 - Consolidated Major Application Security
 - Incorporated into a Central Security Organization
- Began the Role Definition process – low hanging fruit
- Began automating provisioning (running parallel)

Taming the Beast

- 
- Business Drivers for Automated Identity Management
 - Password call volume Reduction
 - Enhancement to Role Based Access Control
 - Immediate and complete user termination
 - Potential to automate compliance controls
 - Providing better service levels
 - Consolidation hurt some service levels
 - Head count too high without automation

Taming the Beast

➤ Challenges


- Political – resistant to change, fiefdoms, etc
- Technological – infrastructure, legacy systems
- Process- Role definition is hard
- Compliance – ensured that existing controls were not weakened during transition
- Service level – during transition would suffer
 - Drove an aggressive timeline



Taming the Beast

- Implementing Auto Provisioning through Role Based Access Control – eliminate modeling users
- Goal was 60-70% of access in roles by end of 4Q04:
 - 100% automation desired but not realistic
 - 100% perceived-automation required
 - Difference between basic access roles and functional roles
RBAC – goal was for functional – attribute level roles
 - End user is manager
 - Supports our “attestation” requirements
- Defined what provided the biggest bang for the buck and went after that first

Taming the Beast

- 
- Developed a self service portal – defined roles and rules
 - Able to provision with very little information
 - Behind the scenes discovers required technical information
 - Through role knows what access to give
 - Uses an organizing principle of communities to know where/what to provision at the local level
 - Provides a funneling effect to achieve granularity
 - Used the system to provision our largest population of users (Retail Branches) and groups with highest turnover
 - Continued role definition and maintenance for the rest of the Bank



From This


The image displays eight panels arranged in a 2x4 grid, each containing a different type of data visualization or table. The panels are labeled with '00-00100' and a small 'c' in the bottom left corner.

- Top-Left Panel:** Contains a large block of text with a red heading that reads "The Karpis Party in Africa". Below the text is a table with multiple columns and rows, some cells highlighted in yellow.
- Top-Middle-Left Panel:** Features a table with a yellow background and red text, possibly representing a schedule or a list of items.
- Top-Middle-Right Panel:** Shows a table with a grid structure, containing various numerical and text entries.
- Top-Right Panel:** Displays a complex layout with multiple tables and text blocks, including a prominent red heading.
- Bottom-Left Panel:** Contains a table with a grid structure, similar to the top-middle-right panel, but with different data.
- Bottom-Middle-Left Panel:** Shows a table with a grid structure, containing various numerical and text entries.
- Bottom-Middle-Right Panel:** Displays a table with a grid structure, containing various numerical and text entries.
- Bottom-Right Panel:** Features a table with a grid structure, containing various numerical and text entries.

To This

New Hire

All New Users Must Take and Pass AWARE (at least one hour)
Prior To Initiating an Access Request



Account Courier - Select Role - Microsoft Internet Explorer provided by SunTrust Banks, Inc.

SUNTRUST Account Provisioning

Help ✓: Required Input Field ⓘ: Numeric Field □: Read Only Field [Log Out](#)

Retail-Branch New Hire - User Information

Please enter the requested information and click "Next".

SSN: - - ✓ ⓘ

Location:

State: ⓘ ✓

City: ⓘ ✓

Address: ⓘ ✓

User Role: ⓘ ✓

Request Additional Access:

[Next](#)


Done Local intranet




From Taming the Beast to Enabling Business

ETRM Vision: “Drive better business value while maintaining regulatory and legal compliance, implement simplified and transparent access controls, and aggressively manage loss risks through embedding and monitoring of risk controls and processes”


Enabling Business

- 
- We are transforming the image of security as a roadblock to an enabler of business process (new view of brakes)
 - Embedded transparent controls allow managers to conduct business processes unimpeded and remain compliant
 - Enabling Through Efficient Access Management
 - Service levels that were 8 days are now within a day
 - Revoke is immediate vs. inconsistent and slow
 - New hire provisioning is virtually minutes in most cases
 - Manager's can initiate add, change, terminate for 69%
 - Staff to manage user access at 15 FTE vs. 60 FTE
 - Password resets at help desk reduced by 70% from original
 - Annual savings is over \$2 million


Enabling Business

- 
- Enabling through Transparent Access Controls
 - Manual process requires Managers to know access
 - Automated access only requires managers to know jobs
 - RBAC ensures the consistent enforcement of access controls
 - Enabling through Transparent and Consistent Compliance
 - Preventative and compliant controls enforced
 - Terminate is automatic based on HR action
 - Changes detected based on transfer action
 - Auditing now focuses on process vs. individual testing
 - Testing by independent auditors validated process
 - Password strength, duration and history automated


Enabling Business

- 
- Enabling through Rapid and Compliant Merger Integration – The NCF Story
 - Over 5000 employees provisioned for day one access
 - Had to have access on day one but not before legal closing
 - Manual process would have require 31 people working one week
 - During process required provisioning 3 times for most users
 - Final functional access provided through defined roles
 - Access had to be flawless and employees working on Monday after conversion weekend
 - Roles and Password solution saved the conversion
 - Compliance tool enabled the assurance of proper access

Transparent Compliance

- 
- Signed/Non Reputable Certification by Managers requires a level of technical knowledge that most business managers don't have
 - Confirmation that a manager knows and agrees that the access each employee has is the access and only the access required to do the job
 - We have a repository of access information that enables us to conduct manager attestation by presenting managers access by role and any exceptions.

Continuous Improvement

- 
- Expand Identity Management to manage Access Badges
 - Data normalization is underway
 - Provide Self Service Alarm PIN reset
 - Telephone equipment and phone numbers
 - New applications and platforms compatible at Go Live
 - New functions within company will define role in set up
 - Move authentication to AD
 - Improve Preventative controls over Detective controls
 - Automatic deletes upon termination action removes access for a population that was being missed.

Summary

- 
- Corporate Profile/History
 - The Identity Beast
 - Taming the Beast
 - Enabling the Business
 - Efficient Access Management
 - Transparent Access Controls
 - Transparent and Consistent Compliance
 - Rapid and Compliant Merger Integration – The NCF Story
 - Transparent Compliance
 - Continuous Improvement

Enabling Business



What are your
QUESTIONS?