SearchFinancialSecurity.com
INFORMATION SECURITY
FINANCIAL INFORMATION SECURITY DECISIONS

The Evolving Value Proposition and Impact of Identity Management

David Sherry, CISSP CISM
VP – Enterprise Identity & Access Mgmt
Citizens Financial Group

Presentation Overview

- **About Citizens Financial**
- **A quick poll**
- **What is Identity Management?** ***("IdM")***
- **The Citizens Case Study**
- **To role or not to role?**
- **Think enterprise: Framework and governance**
- **Service offerings and Compliance**
- **Key points to success and some cautions**
- **Changing mindsets, and the future**

About Citizens Financial Group

- Citizens Financial is owned by RBS Group
- Financial holding company (11 areas)
- 7th-largest U.S. commercial bank
- $180 billion in assets
- Headquartered in Providence, R.I.
- More than 1,600 branches in 13 states
- Approximately 3,100 ATMs
- 27,000 employees in over 30 states

Who’s Doing What?

May I have a show of hands?

Original Marketing Drivers for IdM *

- Legacy access concerns
- Multiple ID possibilities
- Multiple repositories with no reconciliation
- Difficulties in auditing
- Lack of scalability
- Outdated processes
- Lack of automation
- Convoluted processing
- Inaccurate account creation
- Downtime from processing SLA’s

** Responses culled from numerous on-line sources in 2003*

Why the need at Citizens?

- Projected growth
- Legacy access concerns
- Lack of scalability / outdated processes
- Multiple repositories with no reconciliation

- A focus on straight-through processing
- Inefficiencies and productivity concerns

- Ease of auditing growing in importance
- Regulatory Compliance

One View of Identity Management

What is identity management to Citizens?

The automated management of a colleague's access across multiple disparate systems using a centralized administrative application, with ease of provisioning, modification and deprovisioning.

Identity Management Benefits

- Provisioning and management of users
- Easily accessible audit trail of system accounts
- Delegated administration
- Automated approval processes
- Reduced paperwork
- Password synchronization

"Providing the right people with the right access at the right time"

Drivers

InfoSec presented a two-fold justification to get funding for IdM in 2003:

- **Strategic – InfoSec in its current state would be a hindrance to growth and acquisition. An IdM solution would provide efficient acquisition on-boarding, as well as a reduced staffing model and sustainable process for exponential growth.**

- **Tactical – InfoSec is relying on manual, paper-based processing for provisioning, modification and deprovisioning, with audit issues, legacy access and accuracy concerns. An IdM solution would dramatically increase speed, accuracy and compliance.**

Challenges to Beginning the Program

- Political
- Technological
- Process
- Compliance
- Service levels

Challenges to the Value Proposition

- Costs
- Undervalued benefit
- Prioritization
- Complexity

What IS the Value Proposition?

- Hard-core savings
- Administrative gain
- Soft savings
- Integrated security
- Integrated compliance support

Spotlight on IdM…circa 2008

- 2003 and earlier
  - An IT issue (provisioning, access, legacy accounts, efficiencies, automation, accuracy, etc.)
- 2006 and 2007
  - A business issue (federation, convergence, compliance, etc.)
- 2008 and beyond
  - The spotlight is on IdM brighter than ever
  - Regulatory oversight, public concerns over ID theft, the maturation of federation solutions, increased use of web SSO, etc.

An Evolving and Shifting Focus

- **From purely operational to strategic**
- **From purely tactical to an enabler**
- **From purely a technology to a compliance engine**

Vendors – then and now

- Nine, to five, to four, to two . . .
  - BMC: Control-SA
  - IBM: Tivoli Identity Manager
- Now. . . The major leagues, and the supporting minor leagues:
  - IBM, Oracle, Sun, Novell, CA . . .
  - Courion Corp., BMC, Symark Software, Identity Engines Inc. . .
  - And over 50 others who identify with this space

A Note of Caution About Vendors

- **The vendor’s view: A “project”**
- **What they want: A “sale”**
- **How they do it: A “demo”**

Roles: Should you, what, and how?

- Define and establish a success criteria
  - Base level
  - Organizational level
  - Role-based (or granular) level
- Establish your methods in advance
  - Top down (lifestyle, conceptual)
  - Bottom up (tactical and real world, but changing)
  - Hybrid
- Decide your role engineering process
  - Self-development
  - Automated
  - Manual
  - Observance
- Other role considerations:
  - Repositories
  - Certification
  - Attestation
  - Lifecycle

Think Enterprise . . .

- Any IdM Solution is truly enterprise wide
- Manage the business lines to think “process change”
- Sell the benefits of compliance and risk mitigation
- Ensure that your a strategy combines adherence to standards and security, but is also rooted in clear business goals
- Integrate smoothly with an overall User Access Program
- Be inclusive!

- One document can help you in this regard:
  - The Identity Management Framework

Capability Maturity Model – User Access

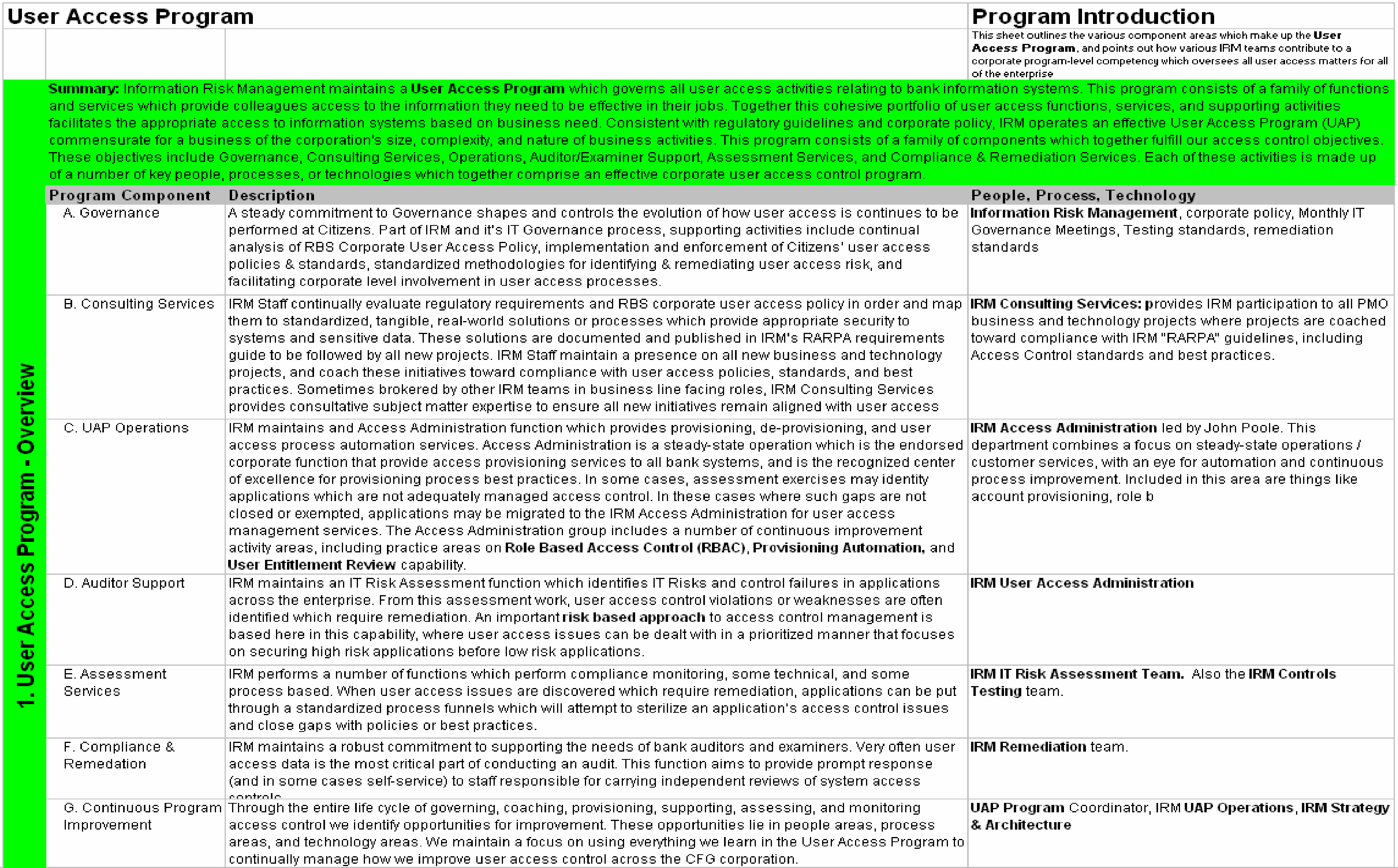
Developing → Established → Optimized

	Level 1 Ad-hoc processes / Detective remediation and manual clean-up	Level 2 Standardized and repeatable processes	Level 3 Simplified & automated processes	Level 4 Integrated compliance into existing business processes
People / Strategy / Governance	• Capability is performed by local groups – minimal integration exists. • Capability is not viewed by management as a priority. • No formal training or communication plan.	• Capability is centralized. • Centrally governed function to gather and analyze access-related information.	• Established enterprise governance model and ownership responsibilities. • Integrated management of Information Governance, Risk, and Compliance.	• Capability integrates with other business value-creating activities. • Delegated administrated capabilities for business lines and self-service for end users
Process	• Access assigned via paper-based access request forms and email. • Clean-up tasks are point-in-time detective controls and resource intensive.	• Capability is designed, in-place, and documented. • Manual exceptions checks such as segregation of duties as part of re-certification.	• Defined enterprise roles / profiles that map access to business processes and job functions. • Formalized role/profile engineering and consolidation procedures.	• Enterprise-wide workflow and policies to accommodate to include job changes. • Business translation of user access & exceptions to business/application owners (eg. cross-platform segregation of duties.
Technology	• Minimal use of technology as a tool to support capability. • Technology solutions in place are disparate and non-standardized.	• Centralized interface for submitting access requests that are processed manually. • Standardized tools to assist in information gathering and analysis.	• Department and application-centric workflow and approvals and as part of user life-cycle. • De-provisioning based on user events and inactivity. • Automated exception checks such as segregation of duties. • Capability performance data is collected, monitored, and reported to management	• Automated lifecycle events based on triggers from authoritative data sources • On-demand compliance monitoring and IdM services dashboard. • Automated re-certification processes and runtime controls that prevent and remediate control gaps.

User Access Program (UAP)

- **An IdM solution should seamlessly integrate with a corporation's overall user access methodology, as one component of the strategy to fulfill access control objectives.**
- **A UAP may include Governance, Consulting Services, Operations, Auditor/Examiner Support, Assessment & Remediation Services, and Continuous Improvement.**
- **IdM will be both "operational" and "continuous improvement":**
  - Examples:
  - Access Request Automation
  - Provisioning Automation
  - Intelligent Role Engineering
  - Role Management Lifecycle

User Access Program (UAP)



User Access Program

Program Introduction

This sheet outlines the various component areas which make up the **User Access Program**, and points out how various IRM teams contribute to a corporate program-level competency which oversees all user access matters for all of the enterprise

1. User Access Program - Overview

Summary: Information Risk Management maintains a **User Access Program** which governs all user access activities relating to bank information systems. This program consists of a family of functions and services which provide colleagues access to the information they need to be effective in their jobs. Together this cohesive portfolio of user access functions, services, and supporting activities facilitates the appropriate access to information systems based on business need. Consistent with regulatory guidelines and corporate policy, IRM operates an effective User Access Program (UAP) commensurate for a business of the corporation's size, complexity, and nature of business activities. This program consists of a family of components which together fulfill our access control objectives. These objectives include Governance, Consulting Services, Operations, Auditor/Examiner Support, Assessment Services, and Compliance & Remediation Services. Each of these activities is made up of a number of key people, processes, or technologies which together comprise an effective corporate user access control program.

Program Component	Description	People, Process, Technology
A. Governance	A steady commitment to Governance shapes and controls the evolution of how user access is continues to be performed at Citizens. Part of IRM and it's IT Governance process, supporting activities include continual analysis of RBS Corporate User Access Policy, implementation and enforcement of Citizens' user access policies & standards, standardized methodologies for identifying & remediating user access risk, and facilitating corporate level involvement in user access processes.	**Information Risk Management**, corporate policy, Monthly IT Governance Meetings, Testing standards, remediation standards
B. Consulting Services	IRM Staff continually evaluate regulatory requirements and RBS corporate user access policy in order and map them to standardized, tangible, real-world solutions or processes which provide appropriate security to systems and sensitive data. These solutions are documented and published in IRM's RARPA requirements guide to be followed by all new projects. IRM Staff maintain a presence on all new business and technology projects, and coach these initiatives toward compliance with user access policies, standards, and best practices. Sometimes brokered by other IRM teams in business line facing roles, IRM Consulting Services provides consultative subject matter expertise to ensure all new initiatives remain aligned with user access	**IRM Consulting Services:** provides IRM participation to all PMO business and technology projects where projects are coached toward compliance with IRM "RARPA" guidelines, including Access Control standards and best practices.
C. UAP Operations	IRM maintains and Access Administration function which provides provisioning, de-provisioning, and user access process automation services. Access Administration is a steady-state operation which is the endorsed corporate function that provide access provisioning services to all bank systems, and is the recognized center of excellence for provisioning process best practices. In some cases, assessment exercises may identity applications which are not adequately managed access control. In these cases where such gaps are not closed or exempted, applications may be migrated to the IRM Access Administration for user access management services. The Access Administration group includes a number of continuous improvement activity areas, including practice areas on **Role Based Access Control (RBAC)**, **Provisioning Automation**, and **User Entitlement Review** capability.	**IRM Access Administration** led by John Poole. This department combines a focus on steady-state operations / customer services, with an eye for automation and continuous process improvement. Included in this area are things like account provisioning, role b
D. Auditor Support	IRM maintains an IT Risk Assessment function which identifies IT Risks and control failures in applications across the enterprise. From this assessment work, user access control violations or weaknesses are often identified which require remediation. An important **risk based approach** to access control management is based here in this capability, where user access issues can be dealt with in a prioritized manner that focuses on securing high risk applications before low risk applications.	**IRM User Access Administration**
E. Assessment Services	IRM performs a number of functions which perform compliance monitoring, some technical, and some process based. When user access issues are discovered which require remediation, applications can be put through a standardized process funnels which will attempt to sterilize an application's access control issues and close gaps with policies or best practices.	**IRM IT Risk Assessment Team.** Also the **IRM Controls Testing** team.
F. Compliance & Remedation	IRM maintains a robust commitment to supporting the needs of bank auditors and examiners. Very often user access data is the most critical part of conducting an audit. This function aims to provide prompt response (and in some cases self-service) to staff responsible for carrying independent reviews of system access controls	**IRM Remediation** team.
G. Continuous Program Improvement	Through the entire life cycle of governing, coaching, provisioning, supporting, assessing, and monitoring access control we identify opportunities for improvement. These opportunities lie in people areas, process areas, and technology areas. We maintain a focus on using everything we learn in the User Access Program to continually manage how we improve user access control across the CFG corporation.	**UAP Program** Coordinator, IRM **UAP Operations**, **IRM Strategy & Architecture**

IdM as a Service Offering

- **Common drivers across technology projects**
  - *Provides consistency, uniformity, and auditability, while reducing design hurdles and roadblocks. Common drivers ensure reliability in process.*
- **Repeatable Processes / Reusable Components**
  - *reduces development costs, and defines and enforces integration standards*
- **Provides opportunities for cost-saving**
  - *decreases administrative costs for user management, and can efficiently support high growth*
- **Security as an enabler**
  - *Delegated administration allows the business line access flexibility; people get to work quicker with the agreed-upon access*
- **An unforeseen benefit**
  - *A fundamental change in mindset at Citizens - from a tactical and operational model relative to identity management, to a enabling and compliance model*

Regulatory Compliance

Regulation	Requirement	Compliance through IdM
Sarbanes-Oxley	Sections 302 and 404: • Appropriate Access Controls • Periodic Review of Access • Segregation of Duties • Sustained and Demonstrable Internal Controls	• Automated de-provisioning • Role-based access enforces segregation of duties • Automated reports • Centralized repository for access reports • Auditable changes
GLBA	Title V: • Financial institutions must protect the confidentiality and integrity of customer data • Financial institutions must protect against unauthorized access to customers personal information	• Role-based access enforces segregation of duties • Ability to track approval trails • Granular access controls • Centralized repository

Big Wins for the IdM Program:

- Conversion success
- Initial day provisioning
- Population of Outlook properties
- Compliance reports
- Delegated authority
- Support of physical access
- Governance and framework
- User Access Program driver

The Future

- Ensure new apps are integrated upon production
- Web SSO
- Enterprise SSO
- Federation
- Role entitlements
- Digital Rights Management
- Integration of privileged passwords and their use
- Cell phones, credit cards, voice mail, cubicles, hardware/software needs . . .

Key Points to Success

- Understand the business, and identify key stakeholders
- Highlight the Risk Management / Compliance aspects
- Establish a Governance Framework
- Manage expectations, maintain public relations and navigate the political landscape
- Build for one key area, but design for the enterprise
- Identify the “globally interesting data” early and receive buy in
- Show incremental progress and risk mgmt wins
- Most of all, perseverance!

Cautions

- The technology proves to be easy . . . not so the data
- Role definition is not easy . . . decide your methods in advance
- Limit your scope, and manage expectations

Closing Summary

- Identity Management’s “role” is evolving
- Identity Management’s value proposition is increasing in scope
- Look for ways to meet diverse needs with your IdM implementation
- Speak in terms of risk and capabilities, and not so much in technology
- The road is hard and filled with lessons to learn, but achievable

Questions?

Contact information:

David Sherry, CISSP CISM
VP, Enterprise Identity and Access Mgmt.
Citizens Financial Group
One Citizens Drive – ROP295
Riverside, RI 02915
401.282.3165
david.sherry@citizensbank.com