THE SECURITY STANDARD

Adapting Enterprise Security to New Realities, Threats and Endpoints

September 10-11, 2012 | New York Marriott at the Brooklyn Bridge | New York City

Produced by

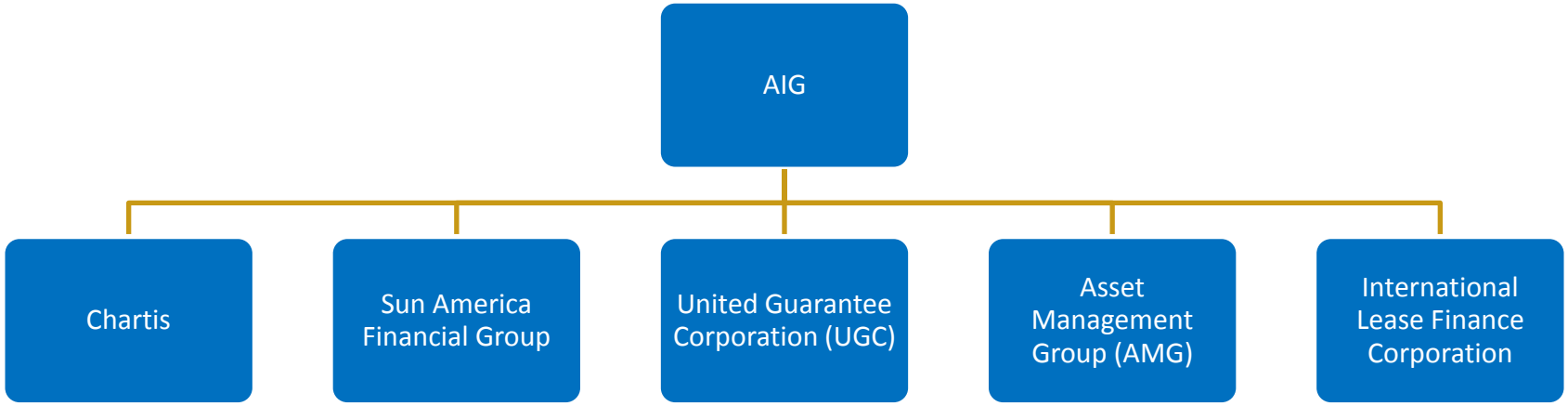
CSO

Managing Identity Through Enormous Change

Robert Mazzocchi
Vice President, Identity Management

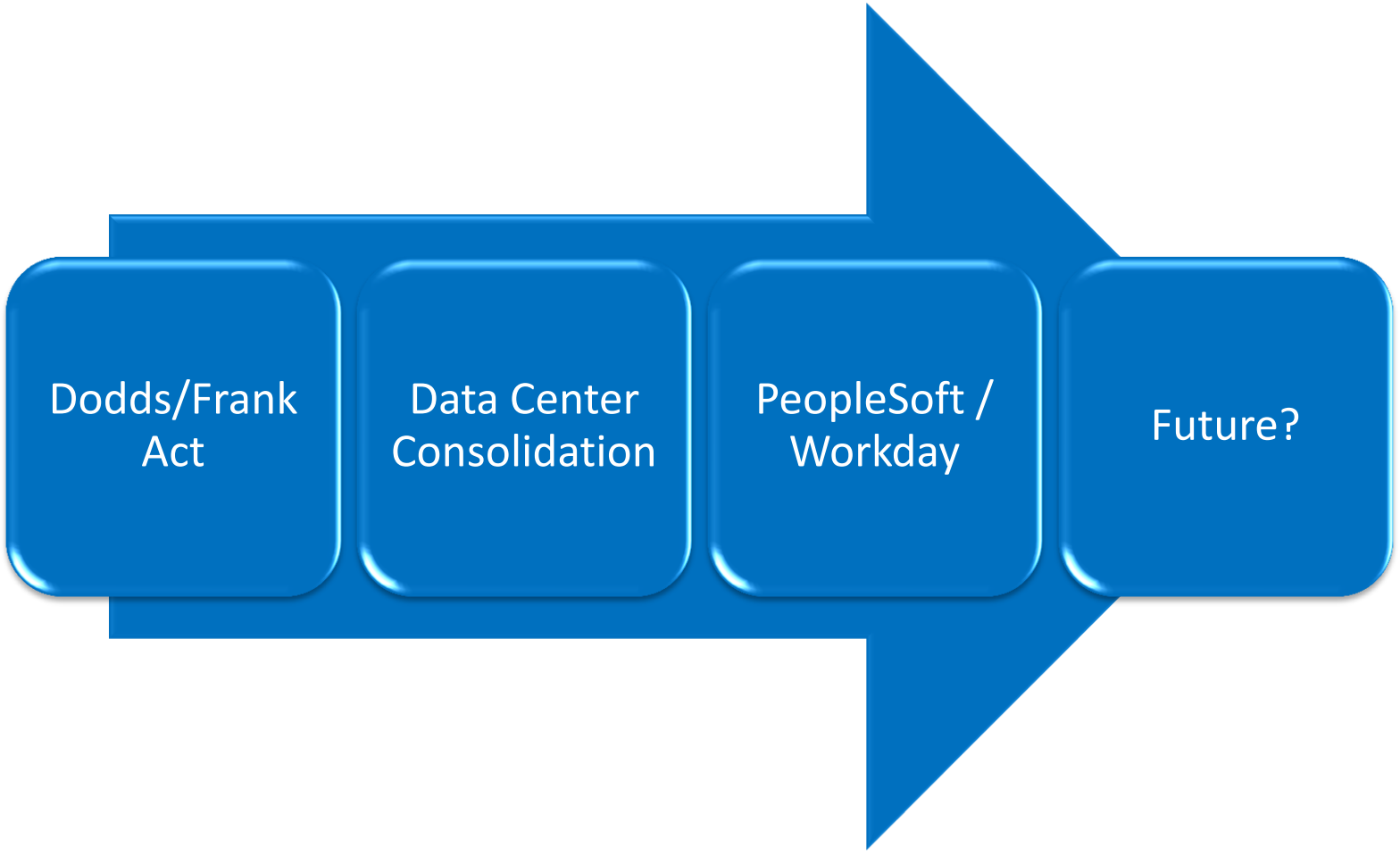
AIG
IT Security, Risk & Compliance (ITSRC)

Company Background



- Leading international insurance organization
- Services 60 million customers in 130 countries and jurisdictions
- Employs 64,000 people globally
- Decentralized Business Units - Regional Structure and In Country Model

I&AM Business Drivers

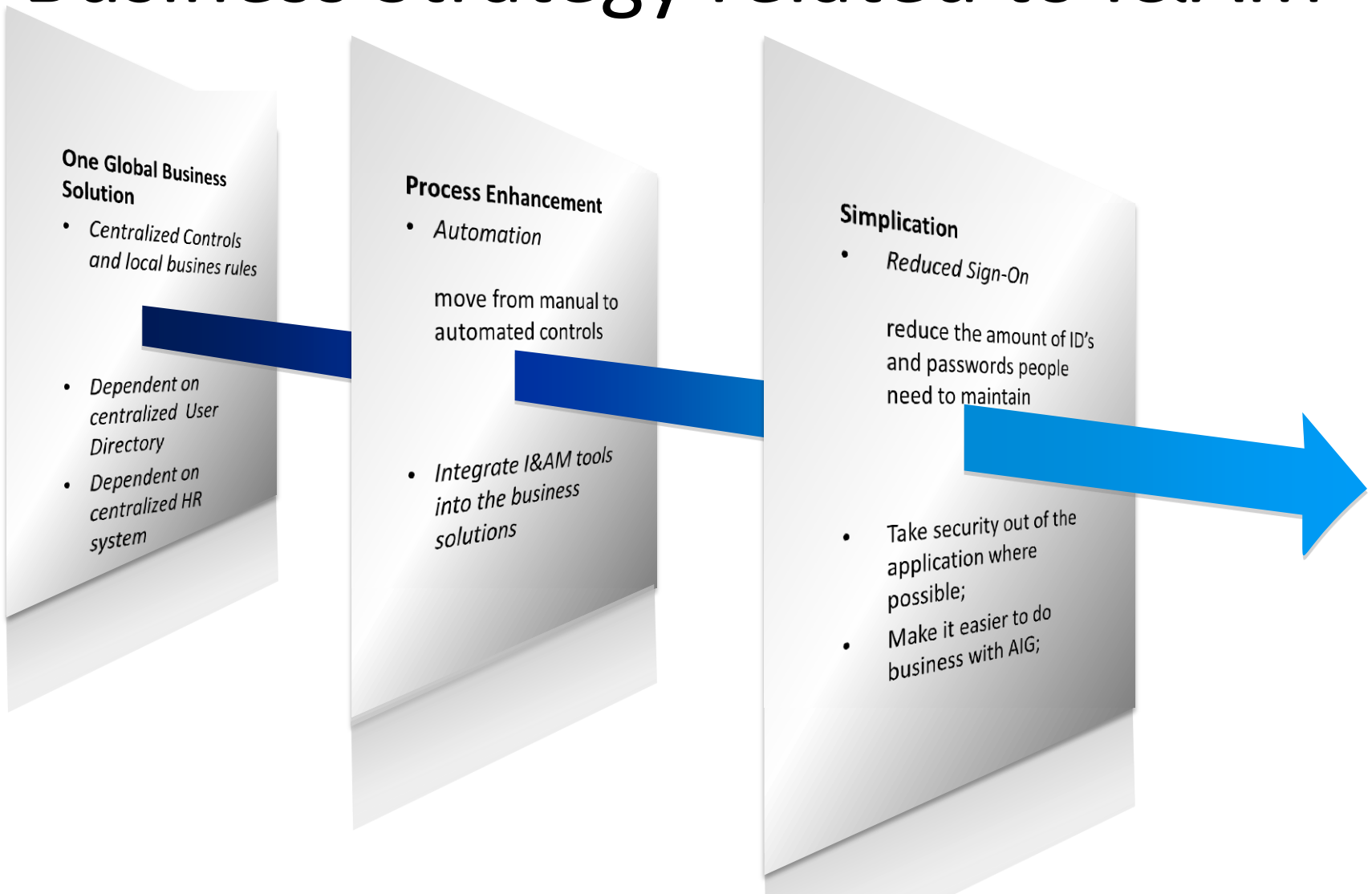


I&AM Business Challenges

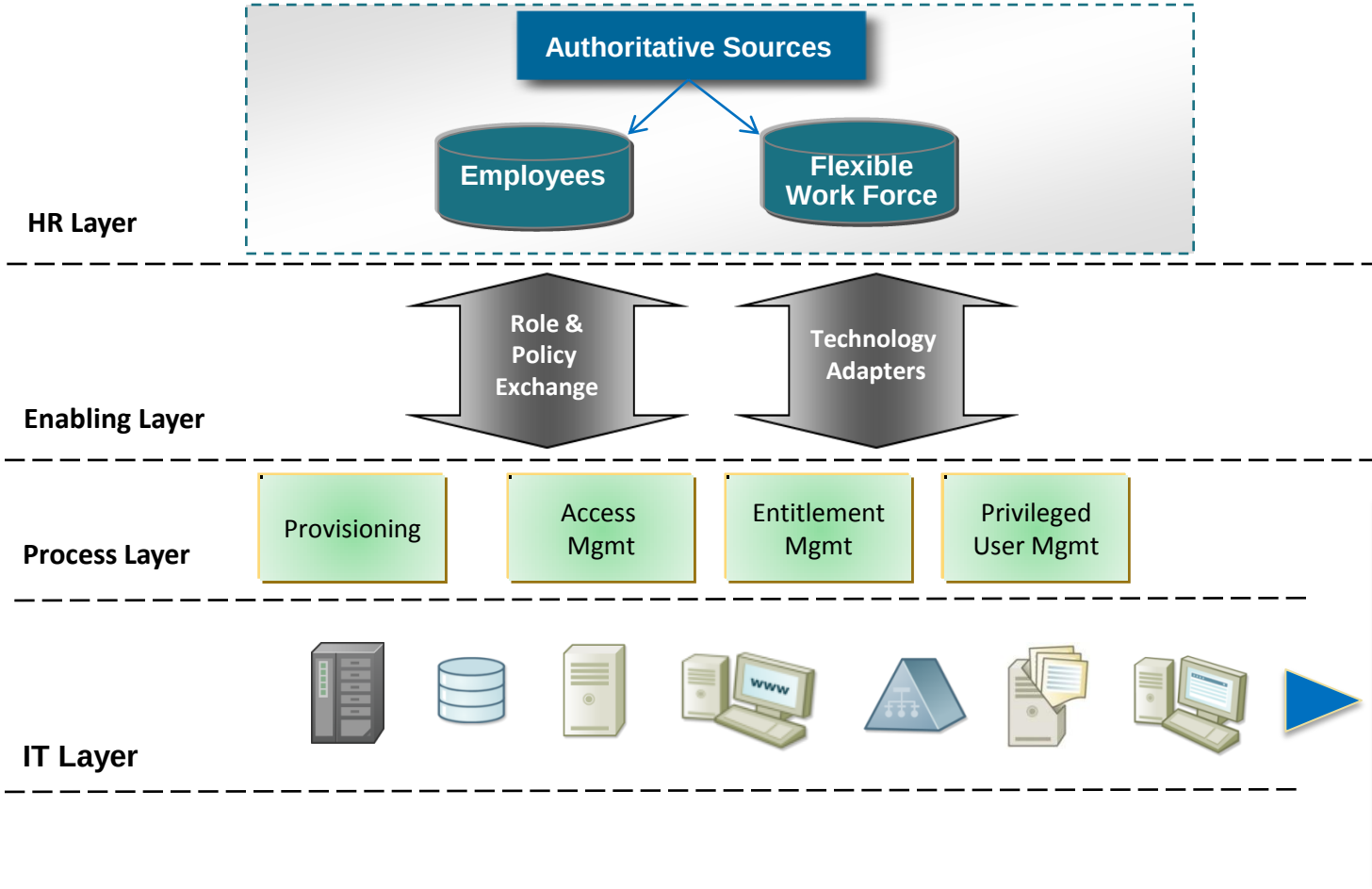
Decentralized Organization Structure (4300+ legal entities):

1. *IT Decentralized*
   - *Average number of ID and passwords was 15 per employee!*
   - *Each business unit thinks their I&AM solution is the best*
2. *No centralized HR*
   - *No authoritative sources for identity information*
   - *No manager hierarchy (organization chart)*
3. *Divestured 24 companies in 24 months*

Business Strategy related to I&AM



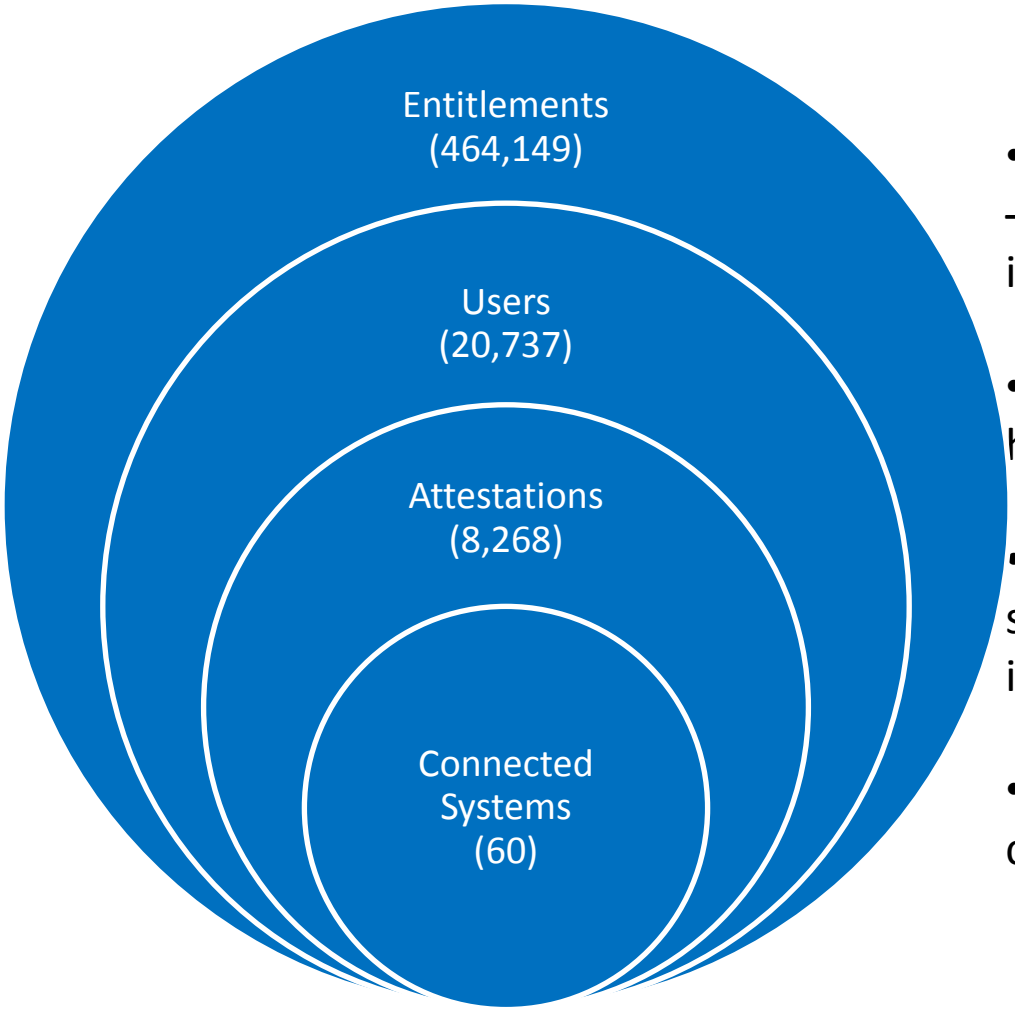
I&AM Implementation



Platform Scope:
- Active Directory
- CA Top Secret
- IBM RACF
- UNIX Privilege Access
- Radius Accounts
- DBA Access

Business Scope:
- Procurement
- Building Access
- Expense Management
- Financial Management

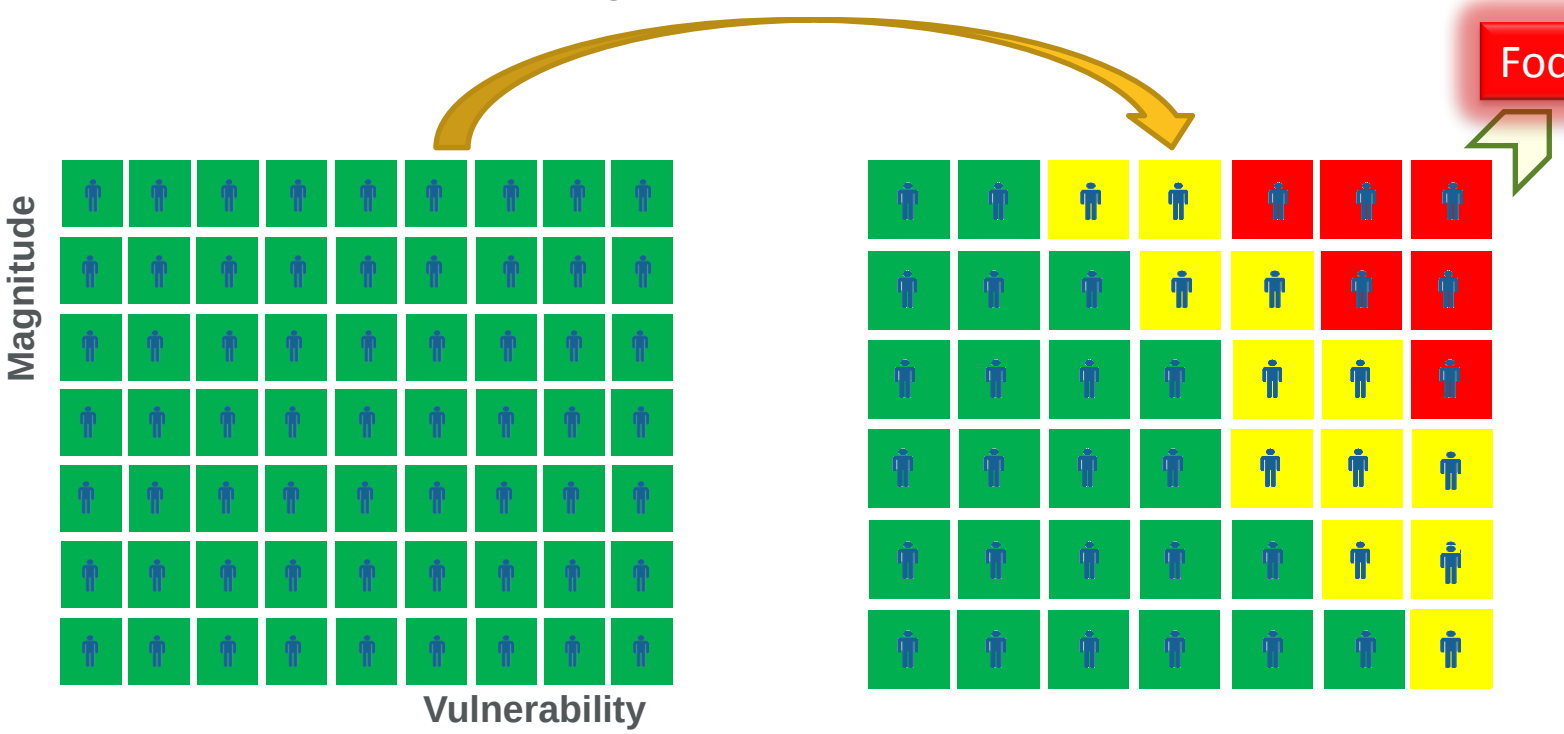
Certification Automation Implementation



- Time savings process improvements – added 50 applications – no increase in staff
- Report turn around time reduced to hours
- Lowered risk and strengthened security – immediate 20% reduction in unnecessary entitlements
- Built foundation for continual compliance – after US, went to Japan

Future Plans - A Risk-Based Approach

Without risk management, all users must be scrutinized…



Low Risk Profile

- **Read-only privileges**
- **No changes since review**
- **No policy violations**
- **No access to high risk apps**

BULK CERTIFY

Medium Risk Profile

- **Changes or new accounts**
- **Mitigated policy violations**
- **Previously approved high-risk application access**

NORMAL CERTIFICATION ROUTINE

High Risk Profile

- Orphaned accounts
- Privileged user accounts
- Active policy violations
- Aged certification status
- Pending remediations
- High risk application access (not previously approved)

SHORTER CERTIFICATION INTERVALS

Future - Risk Modeling

- Risk scoring
  - Similar to a credit rating algorithm
  - Customizable factors & weightings
- Identity risk factors
  - Business roles
  - Extra entitlements
  - Policy violations
  - Certifications/Allowed exceptions
  - Identity attributes
- Resource risk factors
  - Orphaned accounts
  - Dormant accounts
  - Duplicate accounts
  - Uncertified service-level accounts

Identify areas of risk across the organization by department, geography, etc. quickly

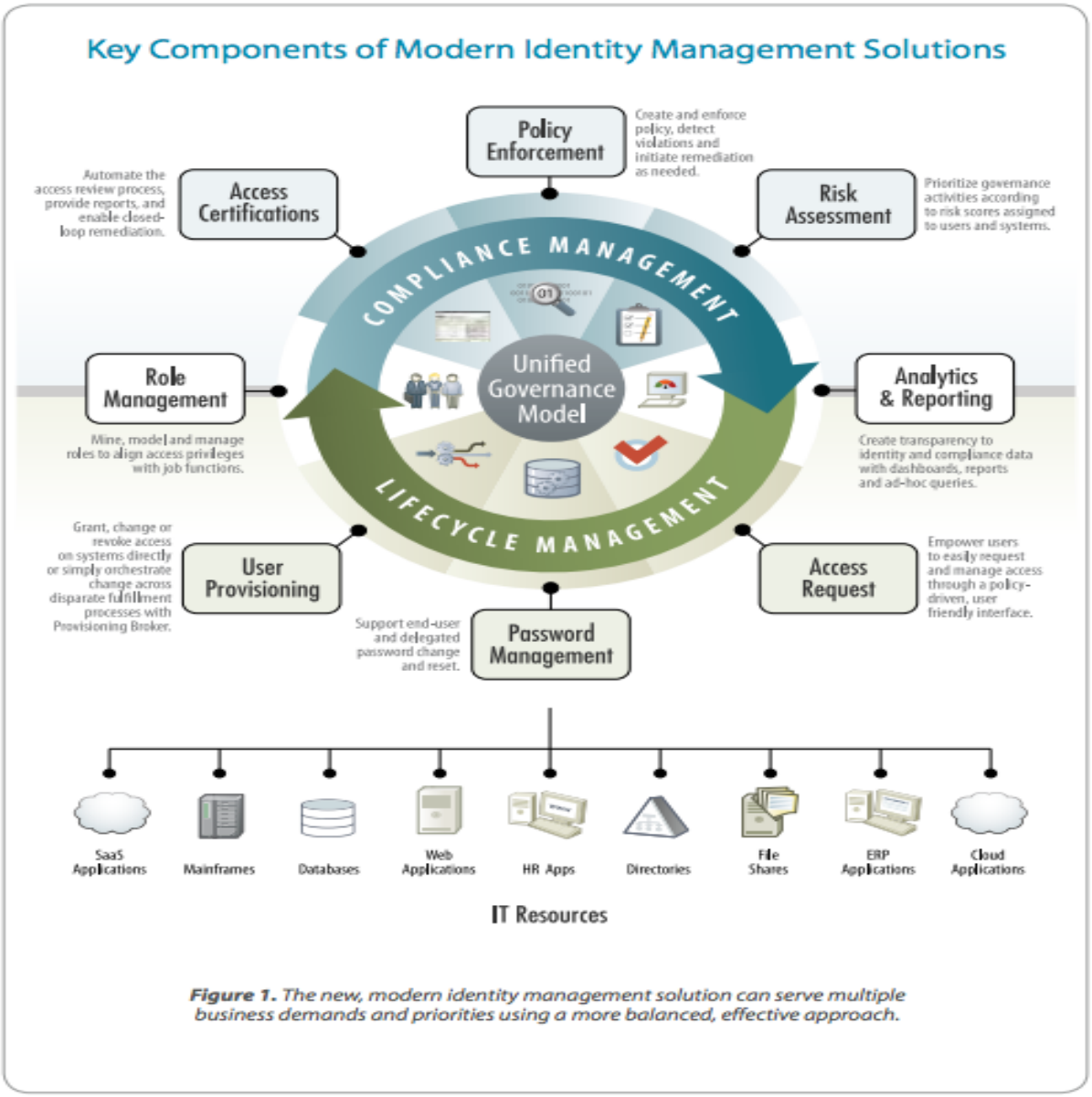


Figure 1. *The new, modern identity management solution can serve multiple business demands and priorities using a more balanced, effective approach.*

Policy Enforcement - Create and enforce policy, detect violations and initiate remediation as needed

Risk Assessment – Prioritize governance activities according to risk score assigned to users and systems

Analytics & Reporting – Create transparency to identity and compliance data with dashboards, reports and ad-hoc queries

Access Request – Empower users to easily request and manage access through a policy driven, user friendly interface

Password Management – Support end-user and delegates password change and reset

User Provisioning – Grant, change or revoke access on systems directly

Role Management – Mine, model and manage roles to align access privileges with job functions

Access Certifications – Automate the review process, provide reports and enable close loop remediation

Advice and Lessons Learned

- Get business unit champions involved early in the process
- This early buy-in is especially important for selection process & POC criteria
- Don’t compete solely on price with a home-grown solution
- Don’t make excuses
- Don’t hide if problems occur
- Maintain constant communication with HR (and their process staff)
- Smarter decisions are made when all user data is on one screen / paper and email

Advice and Lessons Learned

- Communication is key
- Leverage established processes when possible
- Look for early wins to build support
- There is no magic pill
- The only way to solve your problems and put your business on the right path is execution of fundamental business practices
- You're not in this alone

Questions

THE SECURITY STANDARD

Adapting Enterprise Security to New Realities, Threats and Endpoints

September 10-11, 2012 | New York Marriott at the Brooklyn Bridge | New York City

Produced by

CSO