C21 - Leveraging an Identity Management Foundation to Sustain Compliance

Mick Coady

September 21, 2009 – September 23, 2009

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

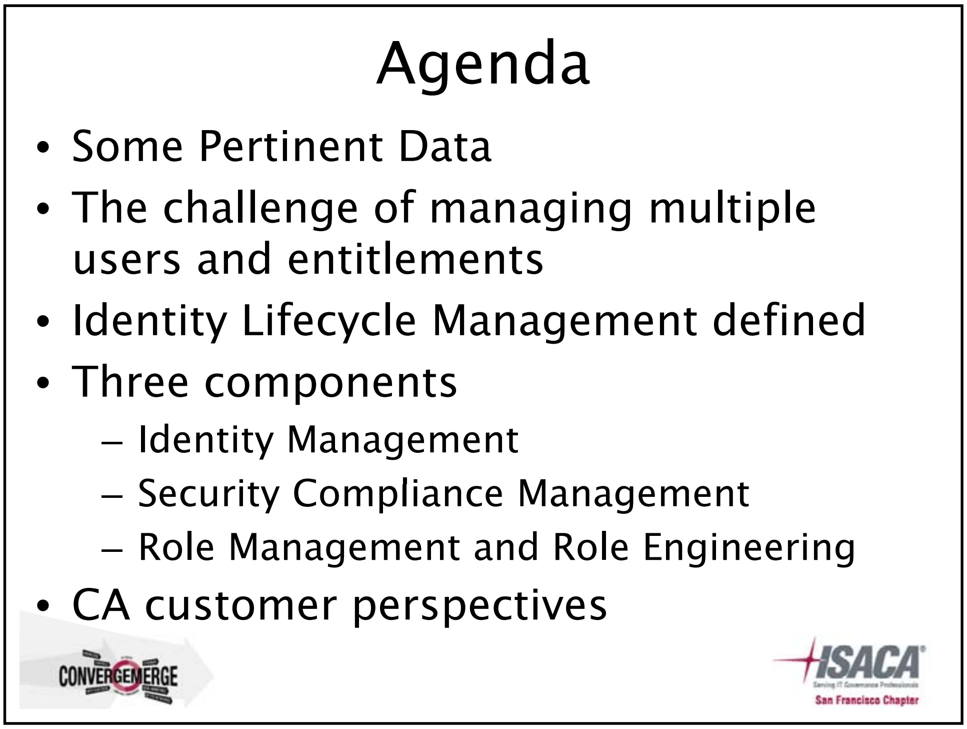
Leveraging an Identity Management Foundation to Sustain Compliance

Michael Coady
Vice President, Solution Strategy
Security Business Unit

KNOWLEDGE
CONTROLS
SF ISACA
STRONGER
CONVERGEMERGE
WITH YOUR PEERS
2009 FALL CONFERENCE
MORE MARKETABLE
BETTER NETWORKED

September 21, 2009 – September 23, 2009

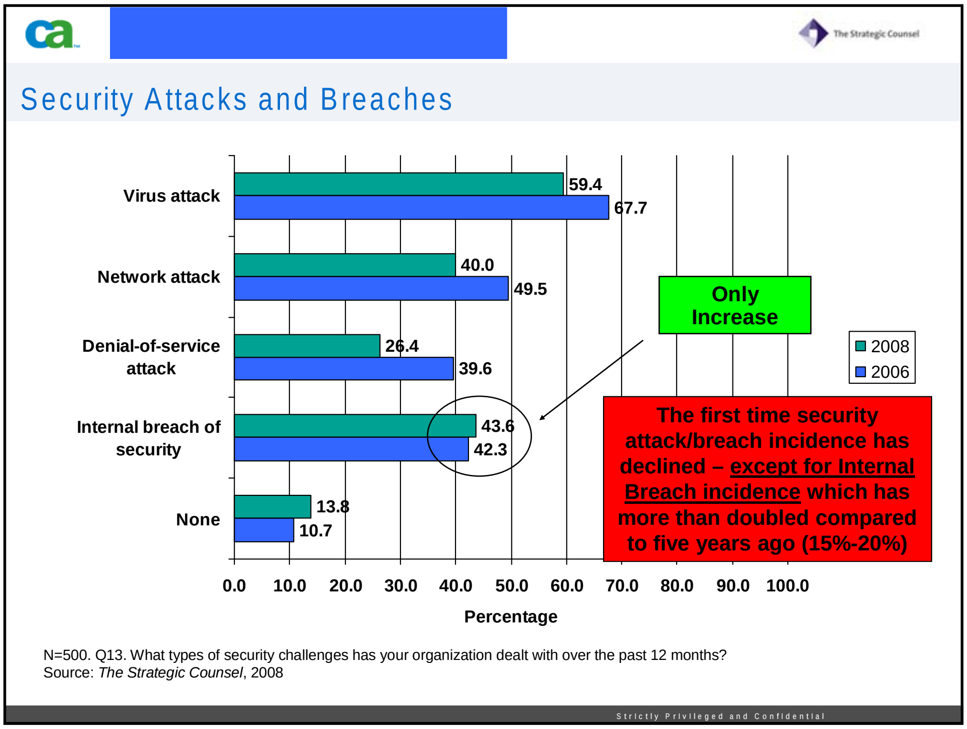
ISACA
Serving IT Governance Professionals
San Francisco Chapter



Agenda

- Some Pertinent Data
- The challenge of managing multiple users and entitlements
- Identity Lifecycle Management defined
- Three components
  - Identity Management
  - Security Compliance Management
  - Role Management and Role Engineering
- CA customer perspectives

CONVERGEMERGE
ISACA
Serving IT Governance Professionals
San Francisco Chapter



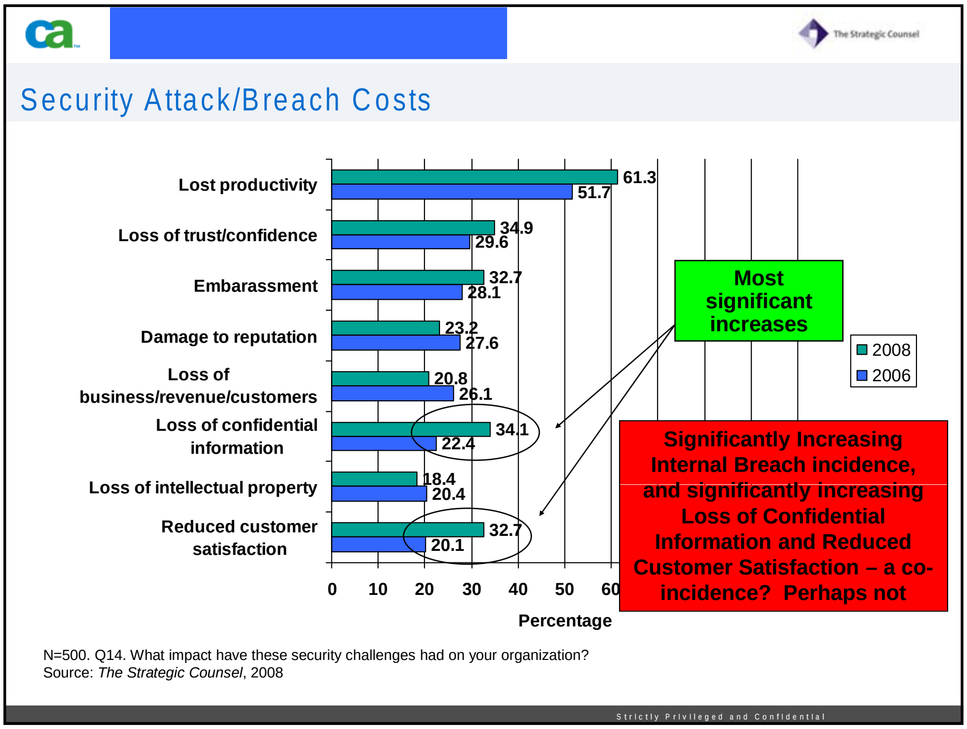
Security Attacks and Breaches

Only Increase

The first time security attack/breach incidence has declined – <u>except for Internal Breach incidence</u> which has more than doubled compared to five years ago (15%-20%)

N=500. Q13. What types of security challenges has your organization dealt with over the past 12 months?
Source: *The Strategic Counsel*, 2008

Strictly Privileged and Confidential



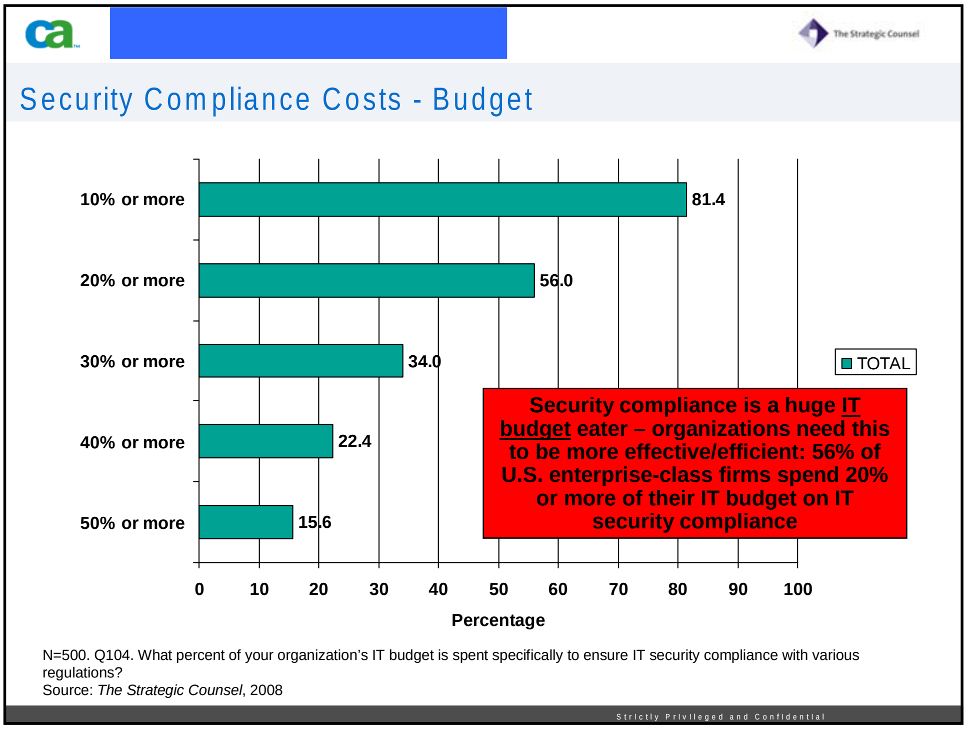
Security Attack/Breach Costs

Most significant increases

Significantly Increasing Internal Breach incidence, and significantly increasing Loss of Confidential Information and Reduced Customer Satisfaction – a co-incidence? Perhaps not

N=500. Q14. What impact have these security challenges had on your organization?
Source: *The Strategic Counsel*, 2008

Strictly Privileged and Confidential

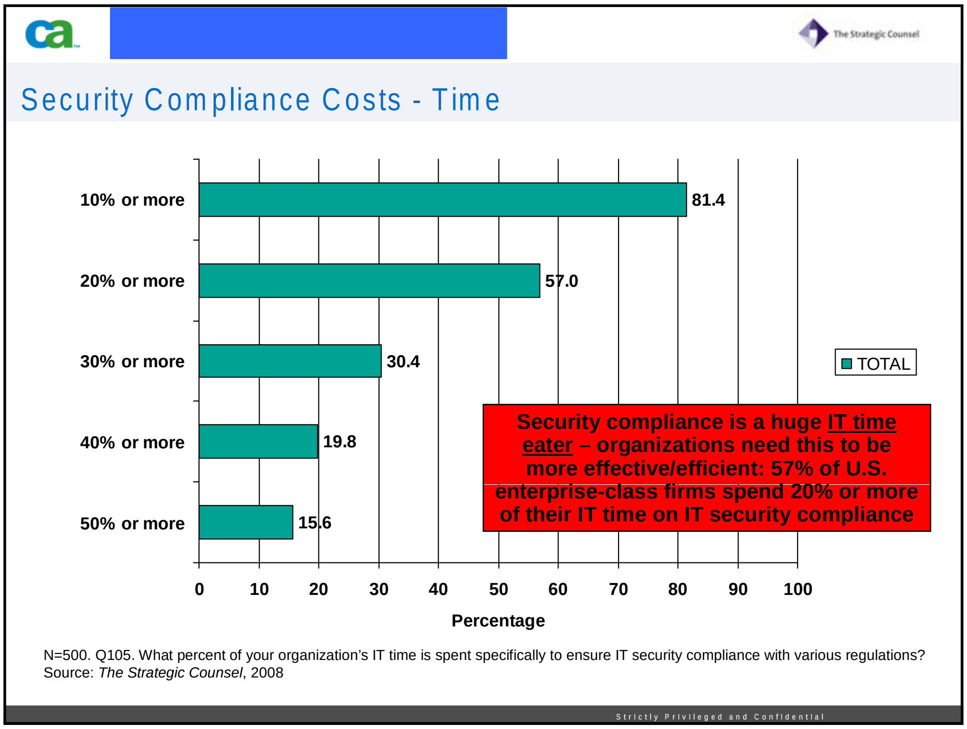


Security Compliance Costs - Budget

Security compliance is a huge <u>IT budget</u> eater – organizations need this to be more effective/efficient: 56% of U.S. enterprise-class firms spend 20% or more of their IT budget on IT security compliance

N=500. Q104. What percent of your organization's IT budget is spent specifically to ensure IT security compliance with various regulations?
Source: *The Strategic Counsel*, 2008

Strictly Privileged and Confidential



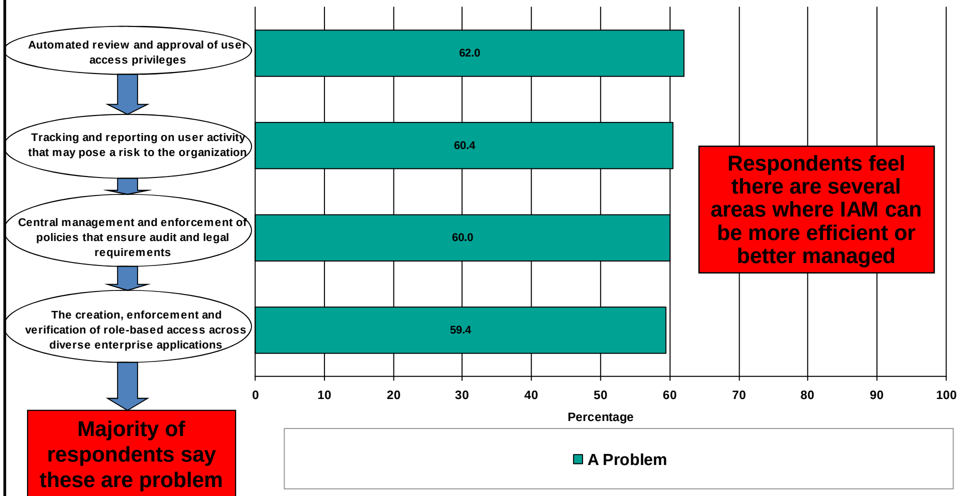
Security Compliance Costs - Time

Security compliance is a huge <u>IT time eater</u> – organizations need this to be more effective/efficient: 57% of U.S. enterprise-class firms spend 20% or more of their IT time on IT security compliance

N=500. Q105. What percent of your organization's IT time is spent specifically to ensure IT security compliance with various regulations?
Source: *The Strategic Counsel*, 2008

Strictly Privileged and Confidential

IAM Issues and Problems



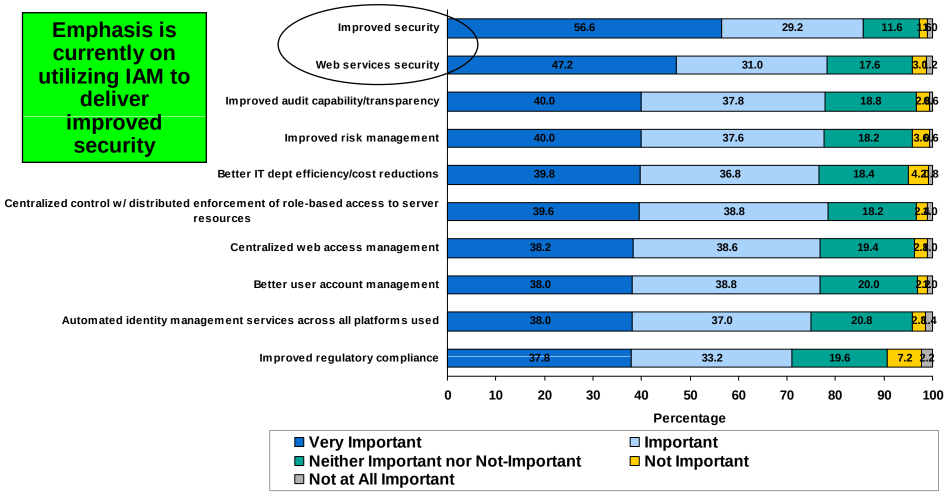
Respondents feel there are several areas where IAM can be more efficient or better managed

Majority of respondents say these are problem areas

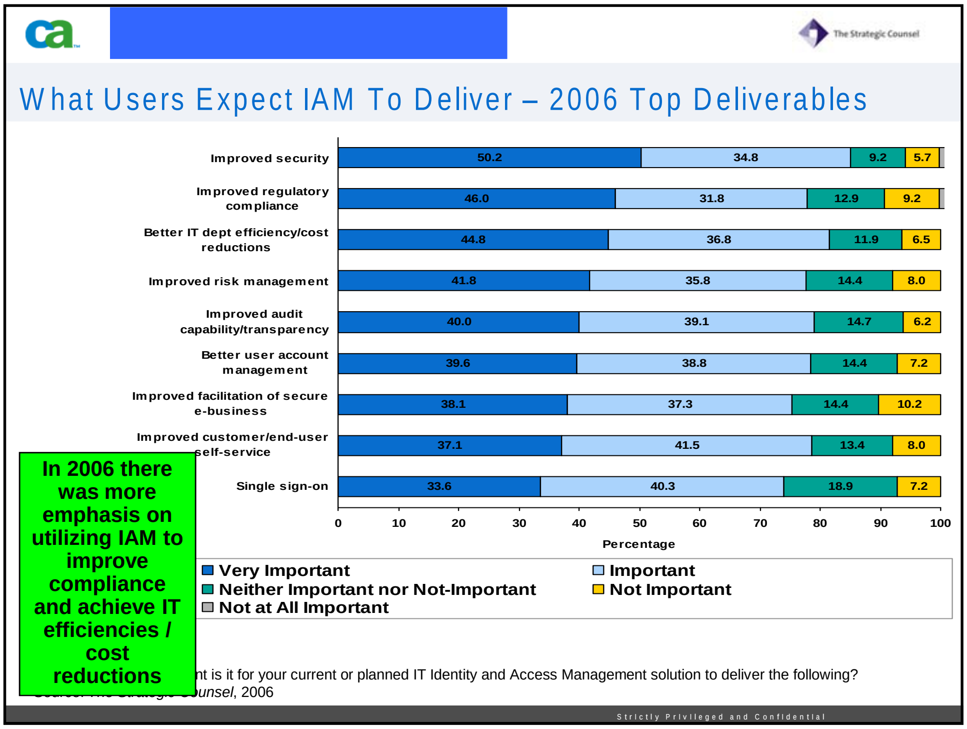
N=500. Q101. Are any of the following problem areas for your organization…?
Source: *The Strategic Counsel*, 2008

What Users Expect IAM To Deliver – 2008 Top Deliverables

Emphasis is currently on utilizing IAM to deliver improved security



N=500. Q7. How important is it for your current or planned IT Identity and Access Management solution to deliver the following?
Source: *The Strategic Counsel*, 2008



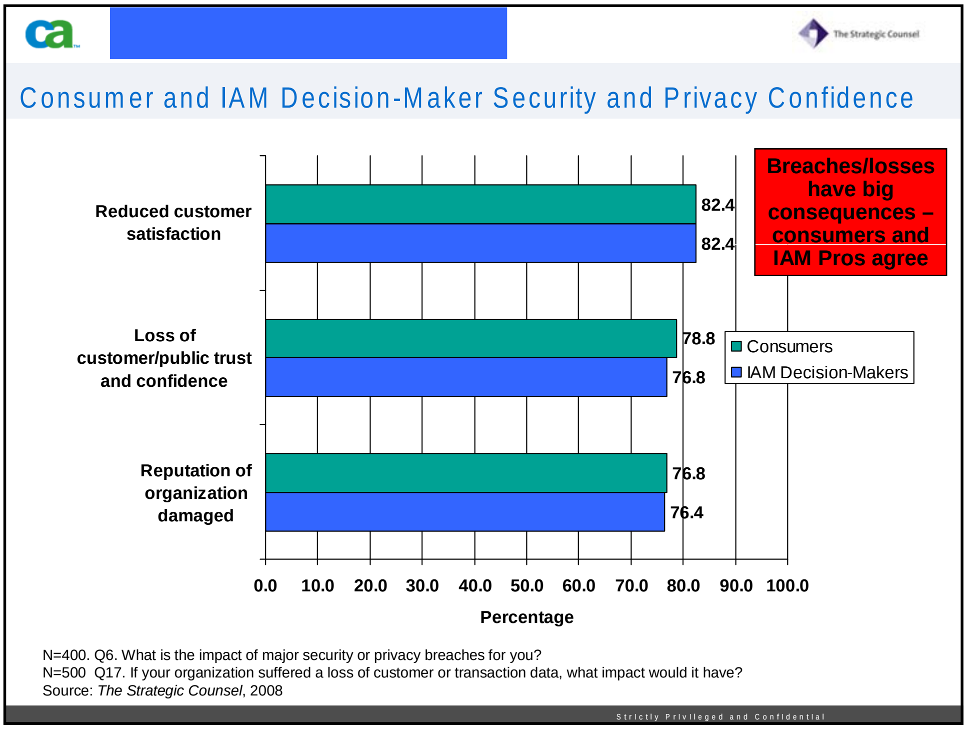
What Users Expect IAM To Deliver – 2006 Top Deliverables

In 2006 there was more emphasis on utilizing IAM to improve compliance and achieve IT efficiencies / cost reductions

nt is it for your current or planned IT Identity and Access Management solution to deliver the following?

unsel, 2006

Strictly Privileged and Confidential

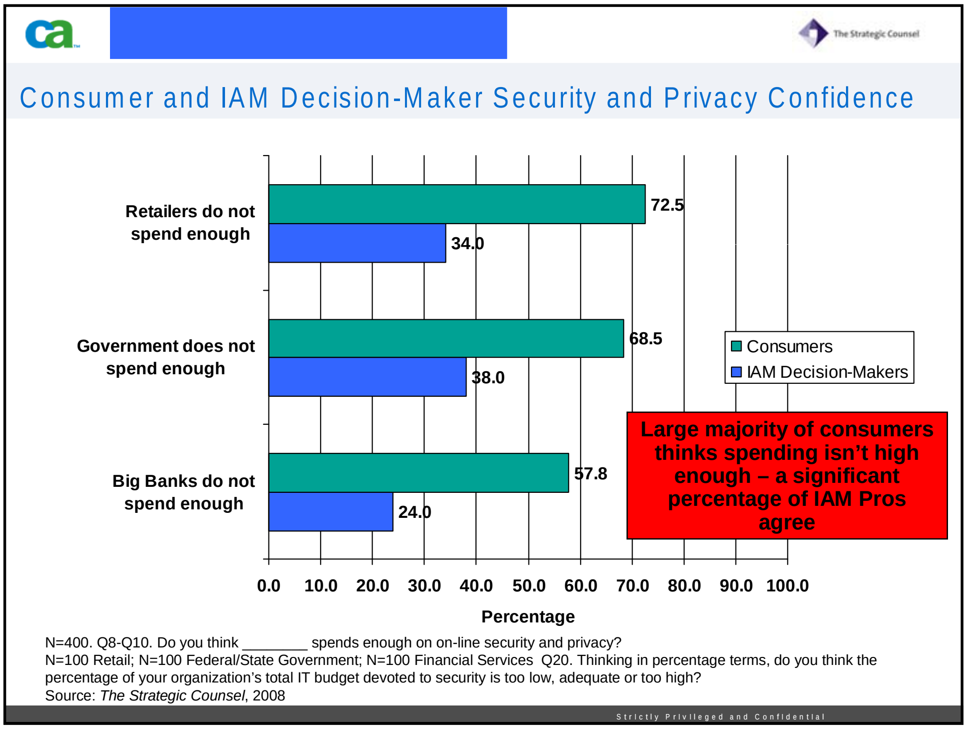


Consumer and IAM Decision-Maker Security and Privacy Confidence

Breaches/losses have big consequences – consumers and IAM Pros agree

N=400. Q6. What is the impact of major security or privacy breaches for you?
N=500 Q17. If your organization suffered a loss of customer or transaction data, what impact would it have?
Source: *The Strategic Counsel*, 2008

Strictly Privileged and Confidential

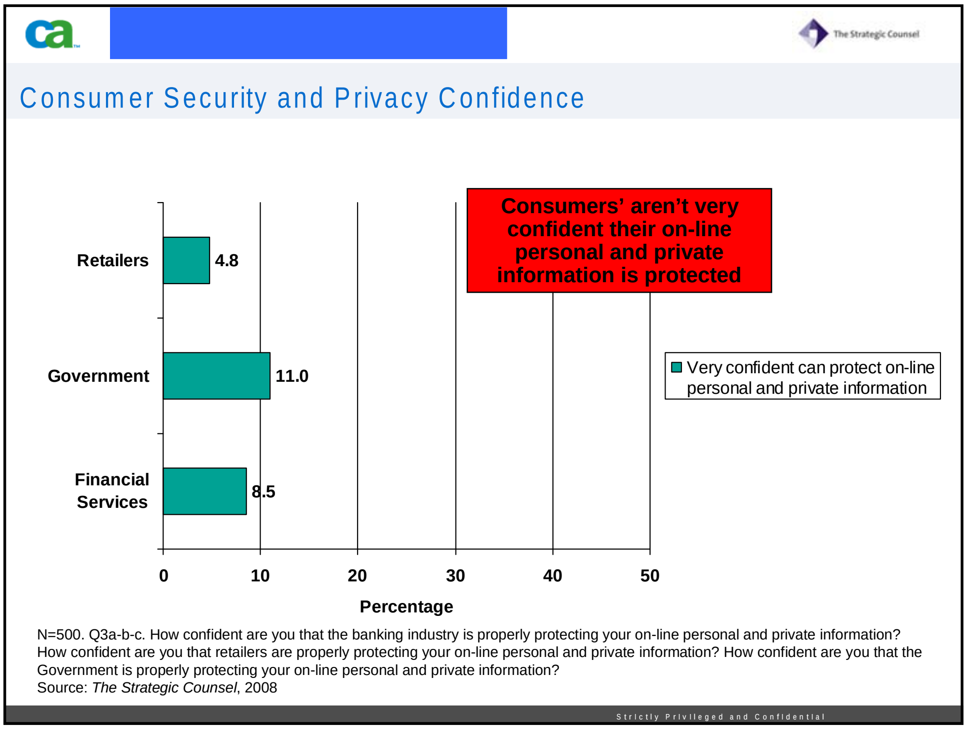


Consumer and IAM Decision-Maker Security and Privacy Confidence

Large majority of consumers thinks spending isn't high enough – a significant percentage of IAM Pros agree

N=400. Q8-Q10. Do you think ________ spends enough on on-line security and privacy?
N=100 Retail; N=100 Federal/State Government; N=100 Financial Services Q20. Thinking in percentage terms, do you think the percentage of your organization's total IT budget devoted to security is too low, adequate or too high?
Source: *The Strategic Counsel*, 2008

Strictly Privileged and Confidential

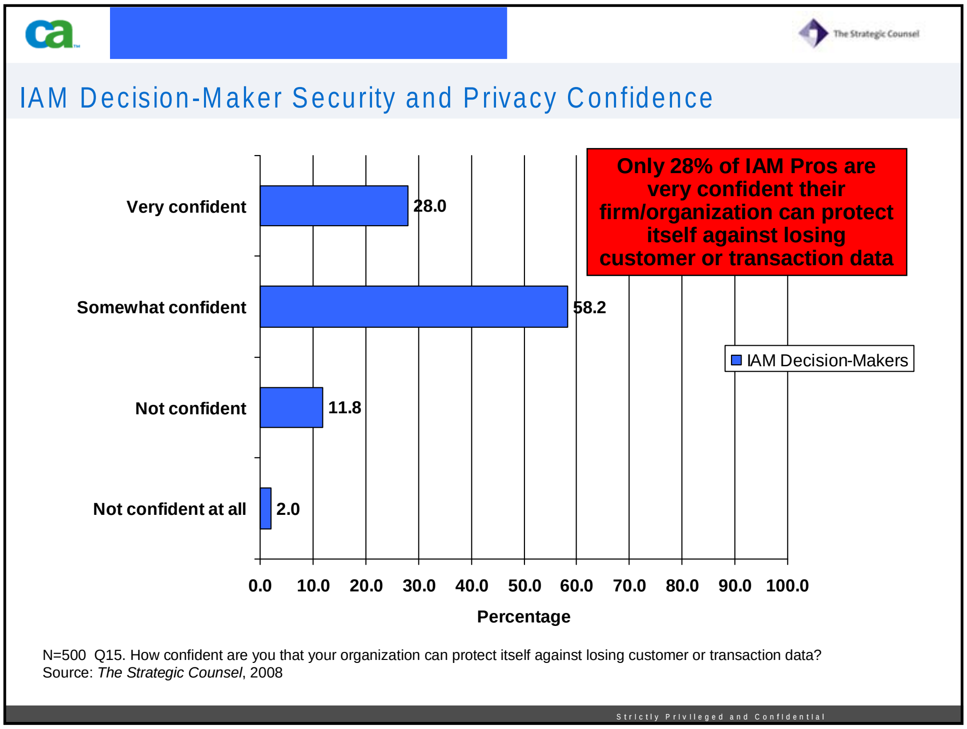


Consumer Security and Privacy Confidence

Consumers' aren't very confident their on-line personal and private information is protected

N=500. Q3a-b-c. How confident are you that the banking industry is properly protecting your on-line personal and private information? How confident are you that retailers are properly protecting your on-line personal and private information? How confident are you that the Government is properly protecting your on-line personal and private information?
Source: *The Strategic Counsel*, 2008

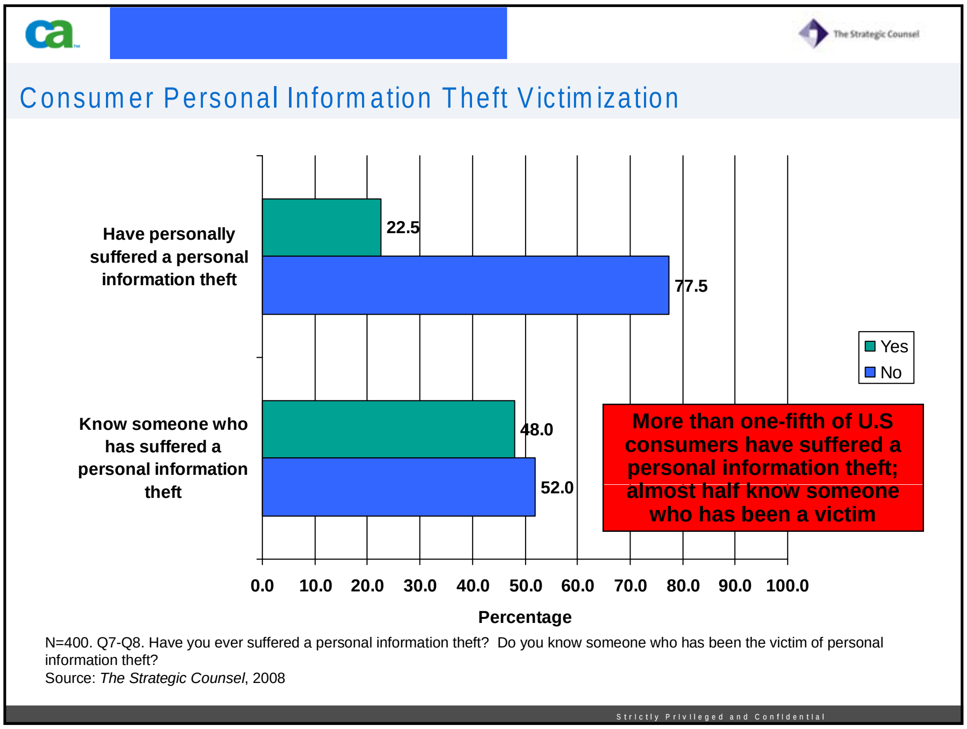
Strictly Privileged and Confidential



IAM Decision-Maker Security and Privacy Confidence

Only 28% of IAM Pros are very confident their firm/organization can protect itself against losing customer or transaction data

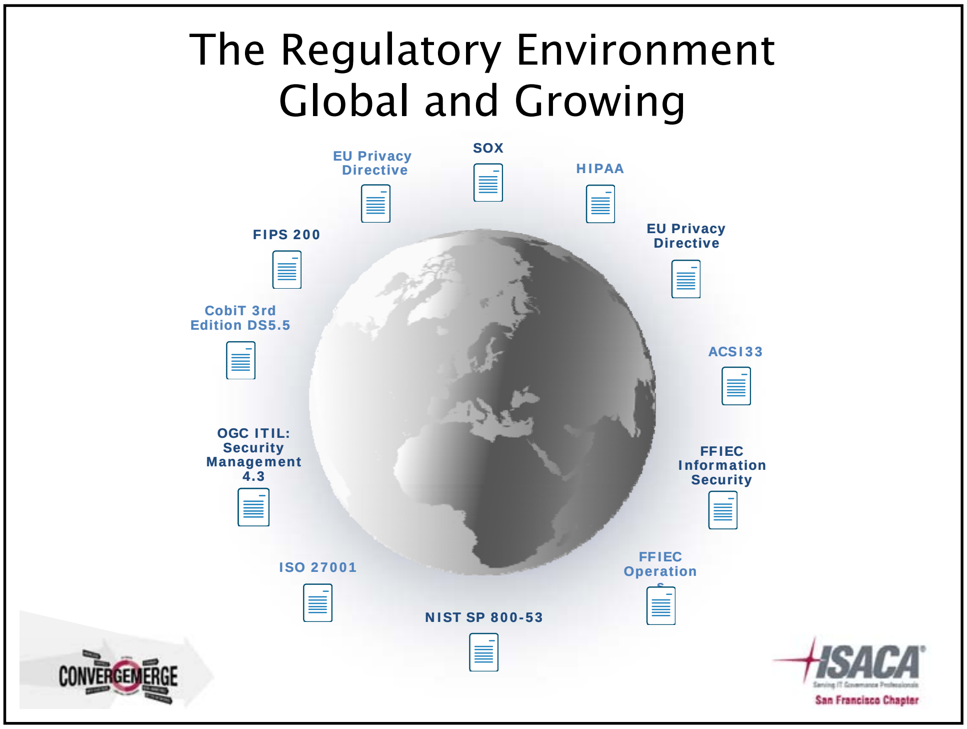
N=500 Q15. How confident are you that your organization can protect itself against losing customer or transaction data?
Source: *The Strategic Counsel*, 2008



Consumer Personal Information Theft Victimization

More than one-fifth of U.S consumers have suffered a personal information theft; almost half know someone who has been a victim

N=400. Q7-Q8. Have you ever suffered a personal information theft? Do you know someone who has been the victim of personal information theft?
Source: *The Strategic Counsel*, 2008



The Regulatory Environment Global and Growing

EU Privacy Directive

SOX

HIPAA

EU Privacy Directive

FIPS 200

CobiT 3rd Edition DS5.5

ACSI33

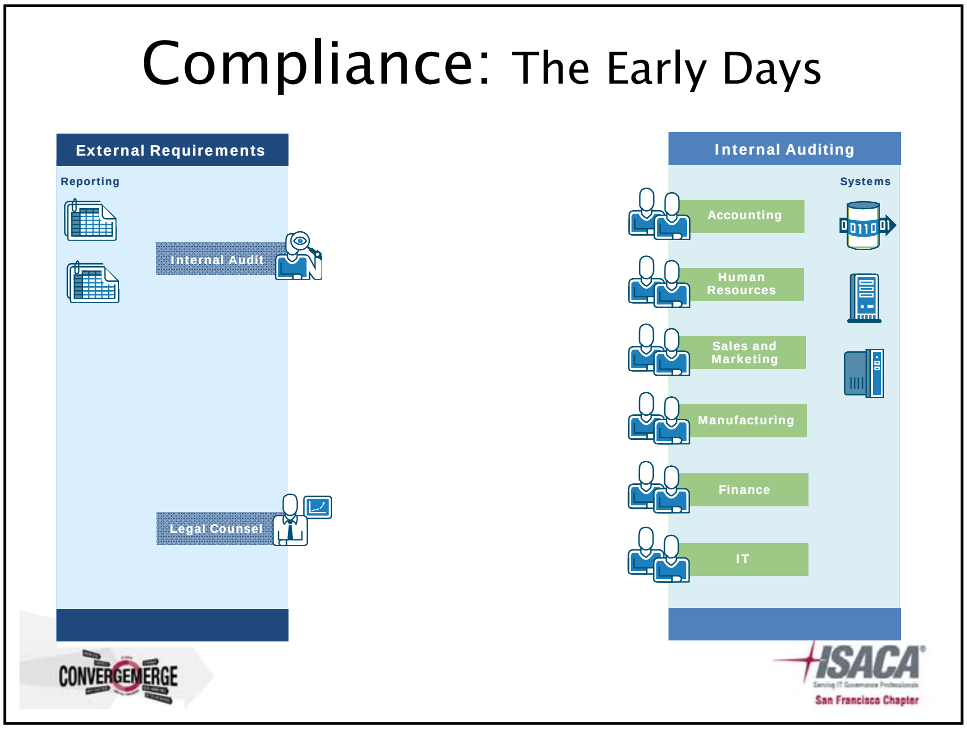
OGC ITIL: Security Management 4.3

FFIEC Information Security

ISO 27001

FFIEC Operations

NIST SP 800-53



Compliance: The Early Days

External Requirements

Reporting

Internal Audit

Legal Counsel

Internal Auditing

Systems

Accounting

Human Resources

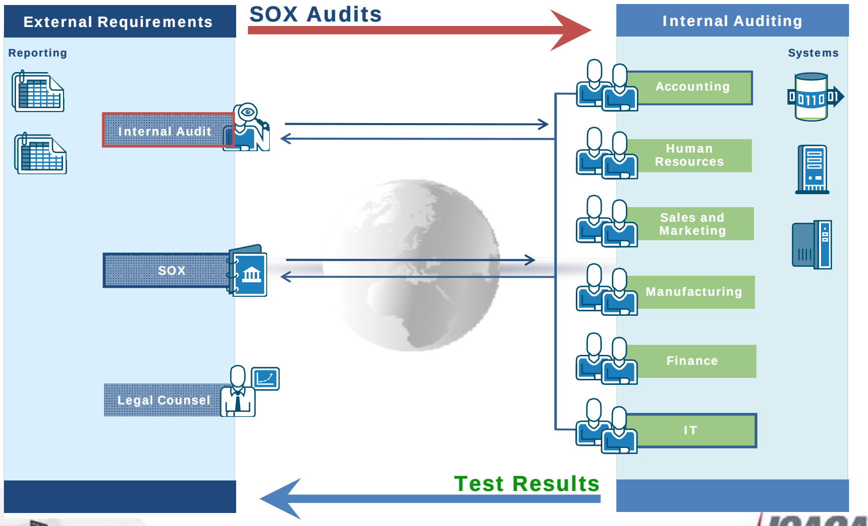
Sales and Marketing

Manufacturing

Finance

IT

Enter SOX



External Requirements

SOX Audits

Internal Auditing

Reporting

Internal Audit

SOX

Legal Counsel

Systems

Accounting

Human Resources

Sales and Marketing

Manufacturing

Finance

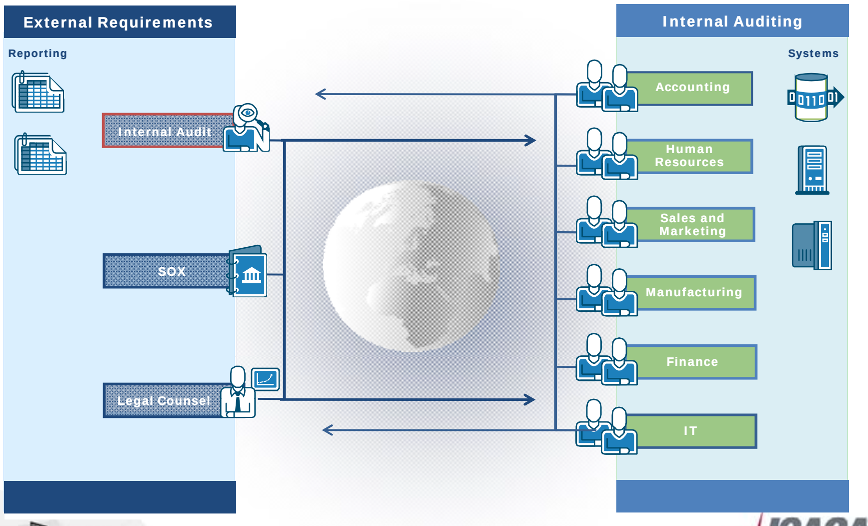
IT

Test Results

CONVERGEMERGE

ISACA Serving IT Governance Professionals San Francisco Chapter

Next Come PCI, EU Privacy Directive, Internal Policies (as well as Compliance Management)



External Requirements

Internal Auditing

Reporting

Internal Audit

SOX

Legal Counsel

Systems

Accounting

Human Resources

Sales and Marketing

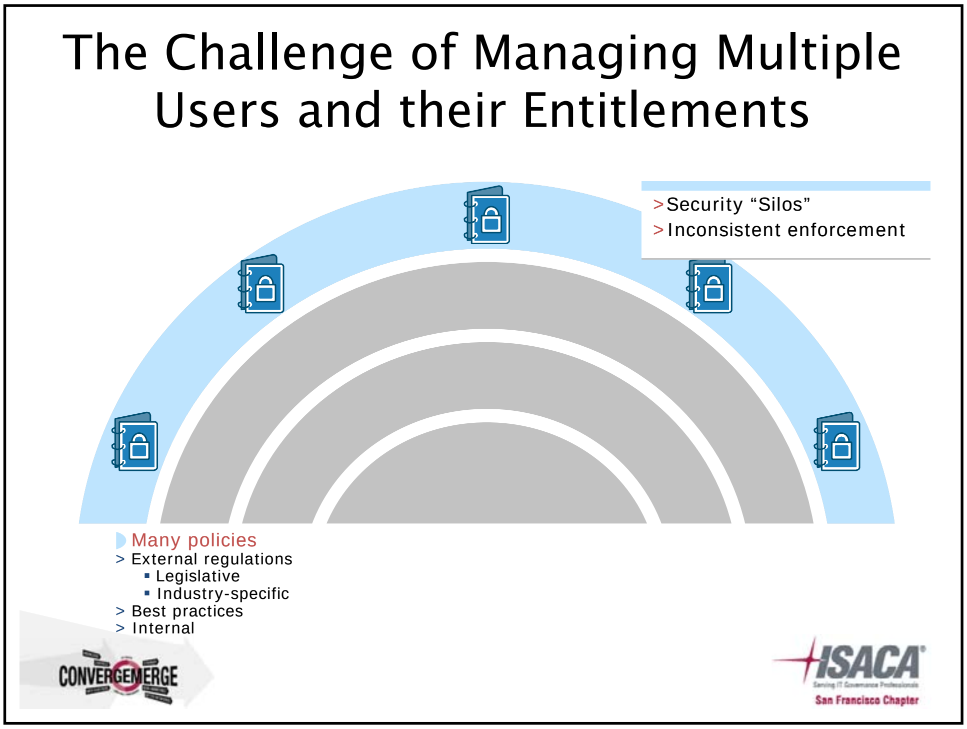
Manufacturing

Finance

IT

CONVERGEMERGE

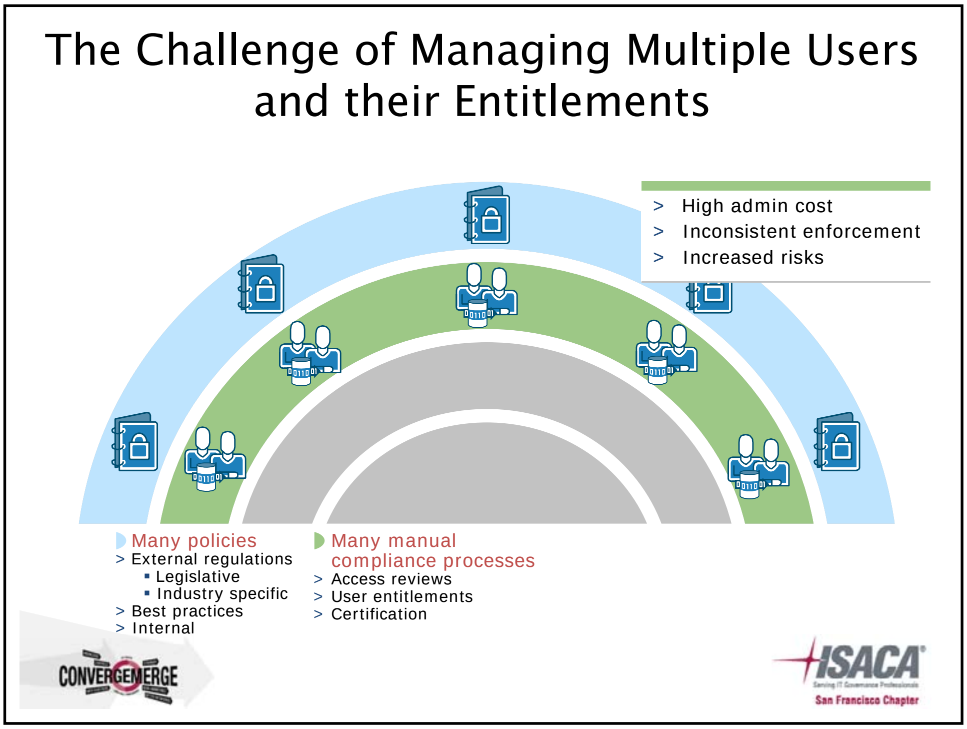
ISACA Serving IT Governance Professionals San Francisco Chapter



The Challenge of Managing Multiple Users and their Entitlements

> Security “Silos”
> Inconsistent enforcement

Many policies
> External regulations
  - Legislative
  - Industry-specific
> Best practices
> Internal



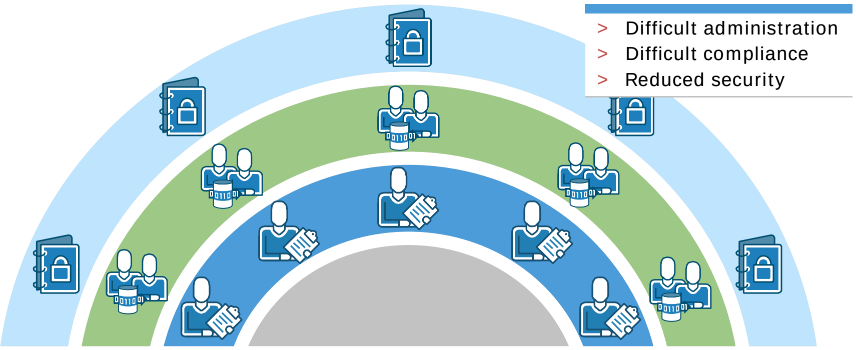
The Challenge of Managing Multiple Users and their Entitlements

> High admin cost
> Inconsistent enforcement
> Increased risks

Many policies
> External regulations
  - Legislative
  - Industry specific
> Best practices
> Internal

Many manual compliance processes
> Access reviews
> User entitlements
> Certification

The Challenge of Managing Multiple Users and their Entitlements



- Difficult administration
- Difficult compliance
- Reduced security

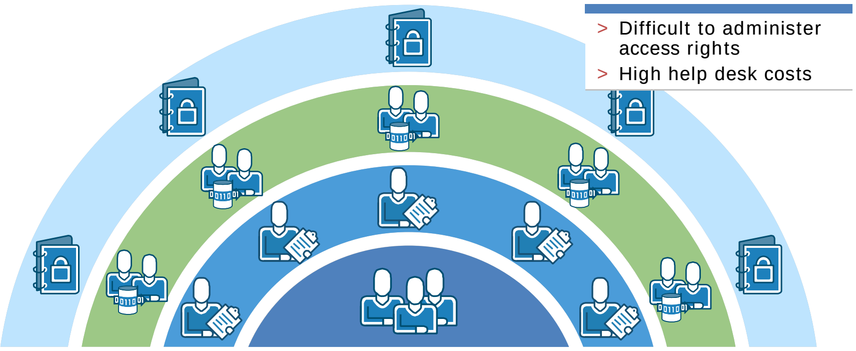
Many policies
- External regulations
  - Legislative
  - Industry specific
- Best practices
- Internal

Many manual compliance processes
- Access reviews
- User entitlements
- Certification

Many entitlements
- Mainframe
- RDBMS
- LDAP
- NOS
- ERP...

21

The Challenge of Managing Multiple Users and their Entitlements



- Difficult to administer access rights
- High help desk costs

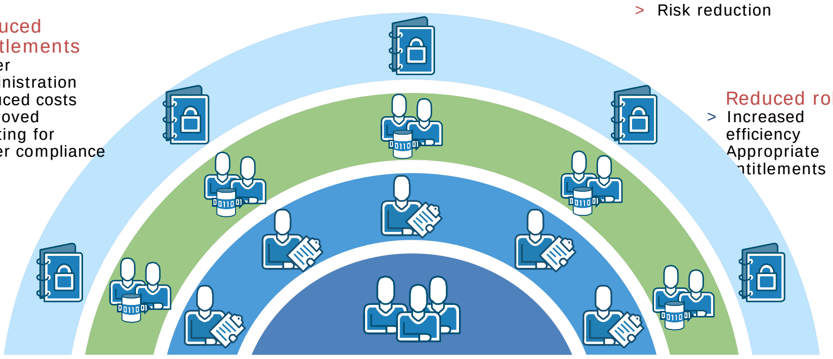
Many policies
- External regulations
  - Legislative
  - Industry specific
- Best practices
- Internal

Many manual compliance processes
- Access reviews
- User entitlements
- Certification

Many entitlements
- Mainframe
- RDBMS
- LDAP
- NOS
- ERP...

Many roles
- Many user types
- Poor role mapping
- Privilege accumulation

Identity Lifecycle Management
The Solution



Security compliance automation
- > Reduced admin costs
- > Risk reduction

Reduced entitlements
- > Easier administration
- > Reduced costs
- > Improved auditing for easier compliance

Reduced roles
- > Increased efficiency
  Appropriate ntitlements

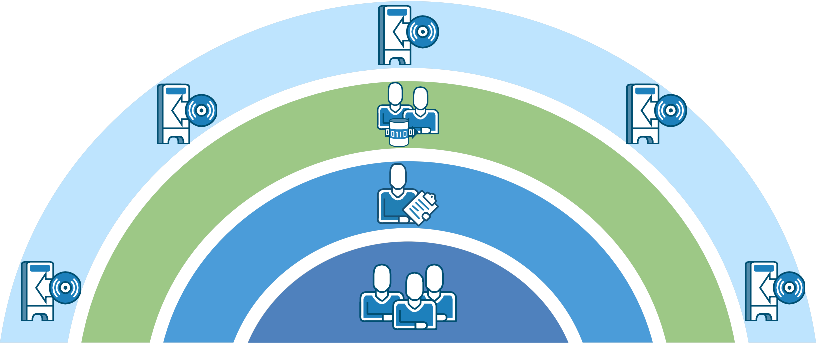
Centralized policies
- > Consistent security & enforcement

Many manual compliance processes
- > Access reviews
- > User entitlements
- > Certification

Many entitlements
- > Mainframe
- > RDBMS
- > LDAP
- > NOS
- > ERP...

Many roles
- > Many user types
- > Poor role mapping
- > Privilege accumulation

Solution to Managing Multiple Users and Entitlements
Identity Lifecycle Management



Centralized policies
- > Consistent security & enforcement

Security compliance automation
- > Reduced admin costs
- > Risk reduction

Reduced entitlements
- > Easier administration
- > Reduced costs
- > Improved auditing for easier compliance

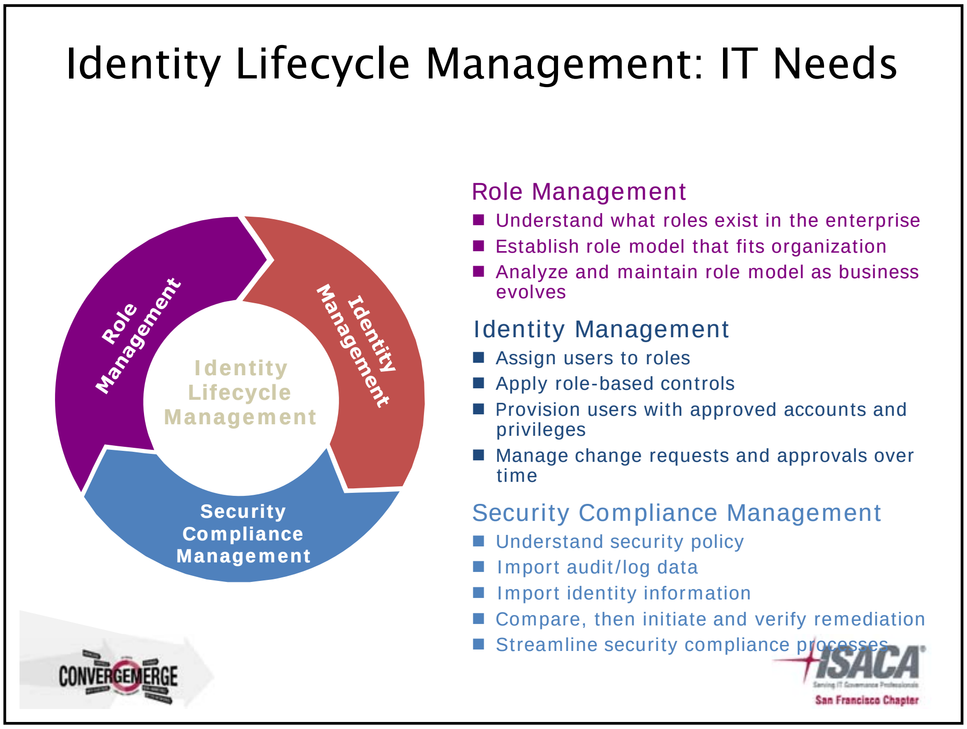
Reduced roles
- > Increased efficiency
- > Appropriate entitlements

Identity Lifecycle Management

Identity Lifecycle Management Defined

Goal: Automating identity-related processes that span the entire enterprise

- What are "identity-related" processes?
  - On-boarding/Off-boarding an employee
  - Users managing their own profiles
  - Executing proper provisioning approval processes
  - Ensuring user entitlements match functional responsibilities
  - Validating company is in compliance
  - And more…



Identity Lifecycle Management: IT Needs

Role Management
Identity Management
Security Compliance Management
Identity Lifecycle Management

Role Management

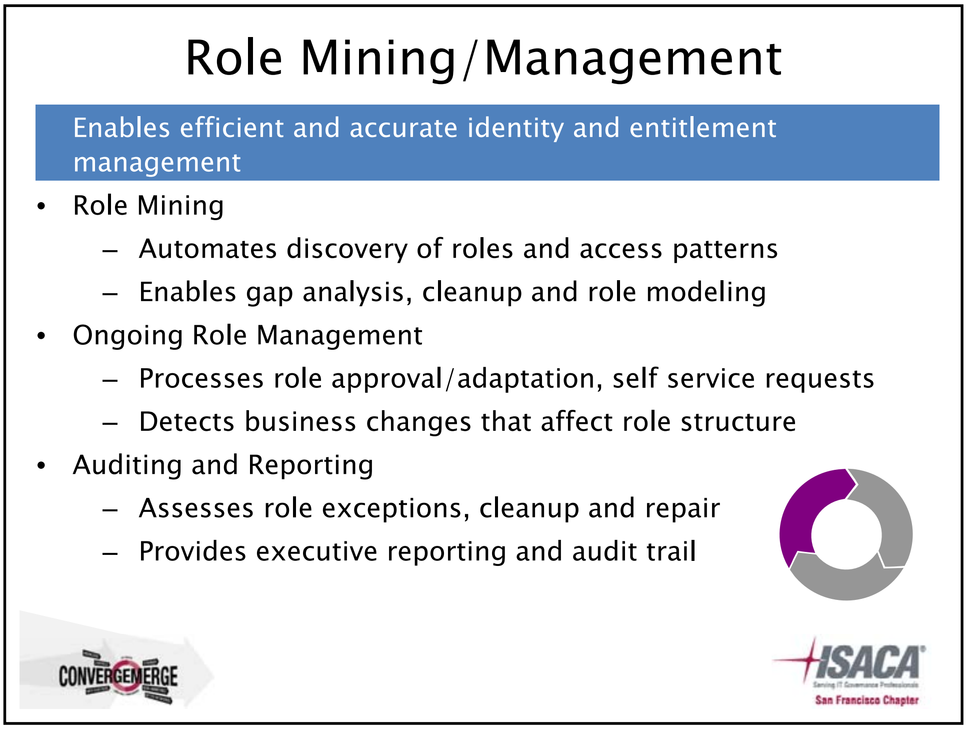
- Understand what roles exist in the enterprise
- Establish role model that fits organization
- Analyze and maintain role model as business evolves

Identity Management

- Assign users to roles
- Apply role-based controls
- Provision users with approved accounts and privileges
- Manage change requests and approvals over time

Security Compliance Management

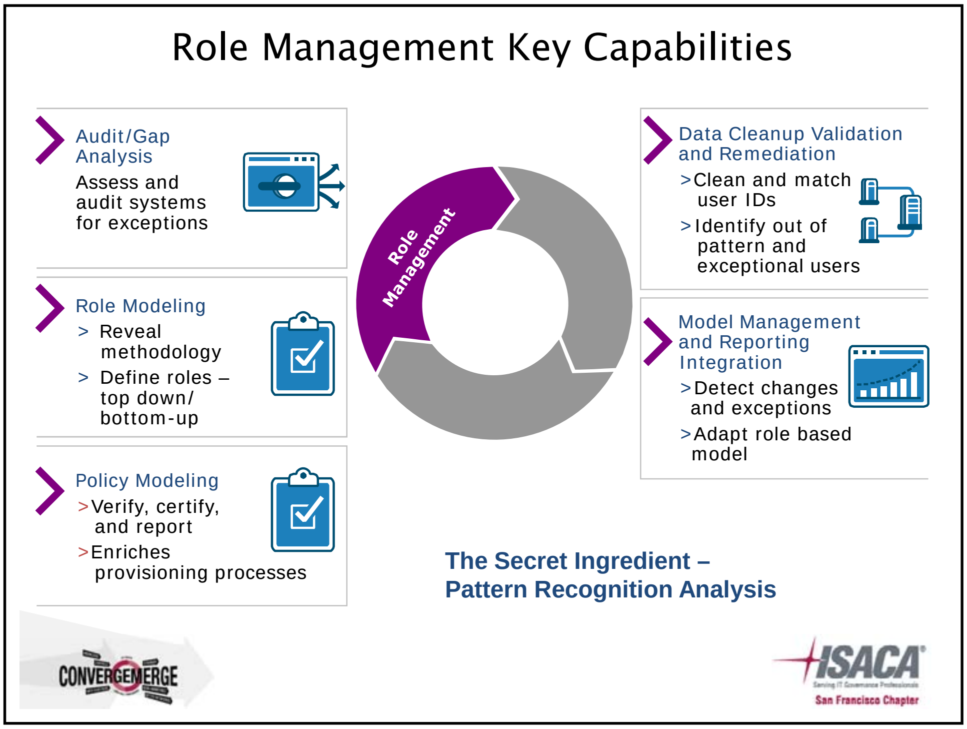
- Understand security policy
- Import audit/log data
- Import identity information
- Compare, then initiate and verify remediation
- Streamline security compliance processes



Role Mining/Management

Enables efficient and accurate identity and entitlement management

- Role Mining
  - Automates discovery of roles and access patterns
  - Enables gap analysis, cleanup and role modeling
- Ongoing Role Management
  - Processes role approval/adaptation, self service requests
  - Detects business changes that affect role structure
- Auditing and Reporting
  - Assesses role exceptions, cleanup and repair
  - Provides executive reporting and audit trail



Role Management Key Capabilities

Audit/Gap Analysis

Assess and audit systems for exceptions

Role Modeling

- Reveal methodology
- Define roles – top down/ bottom-up

Policy Modeling

- Verify, certify, and report
- Enriches provisioning processes

Role Management

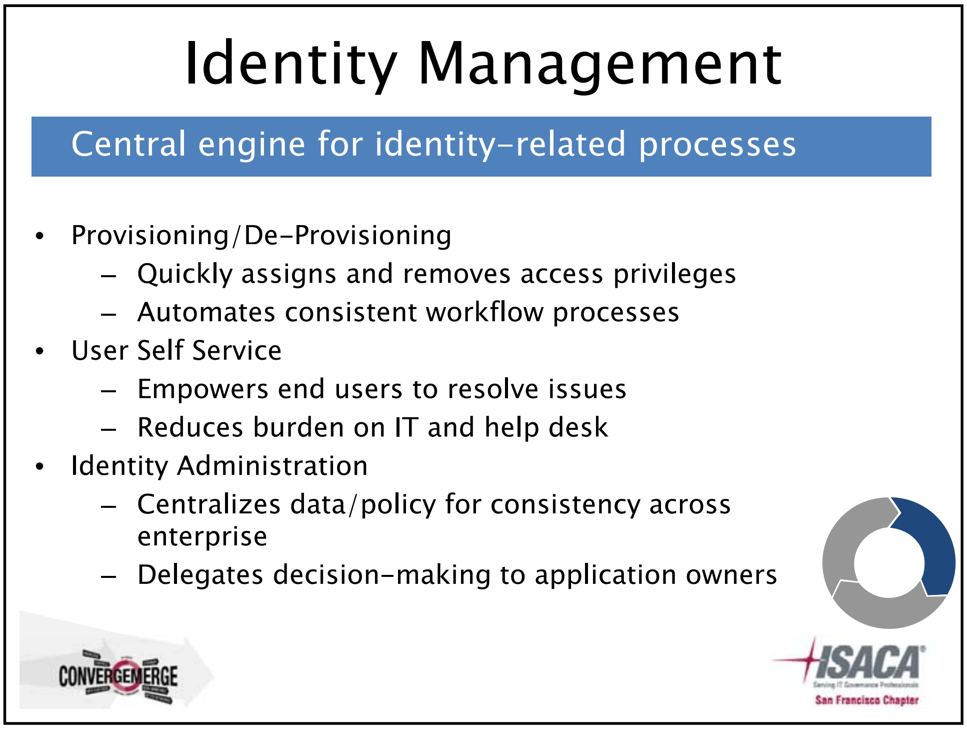
Data Cleanup Validation and Remediation

- Clean and match user IDs
- Identify out of pattern and exceptional users

Model Management and Reporting Integration

- Detect changes and exceptions
- Adapt role based model

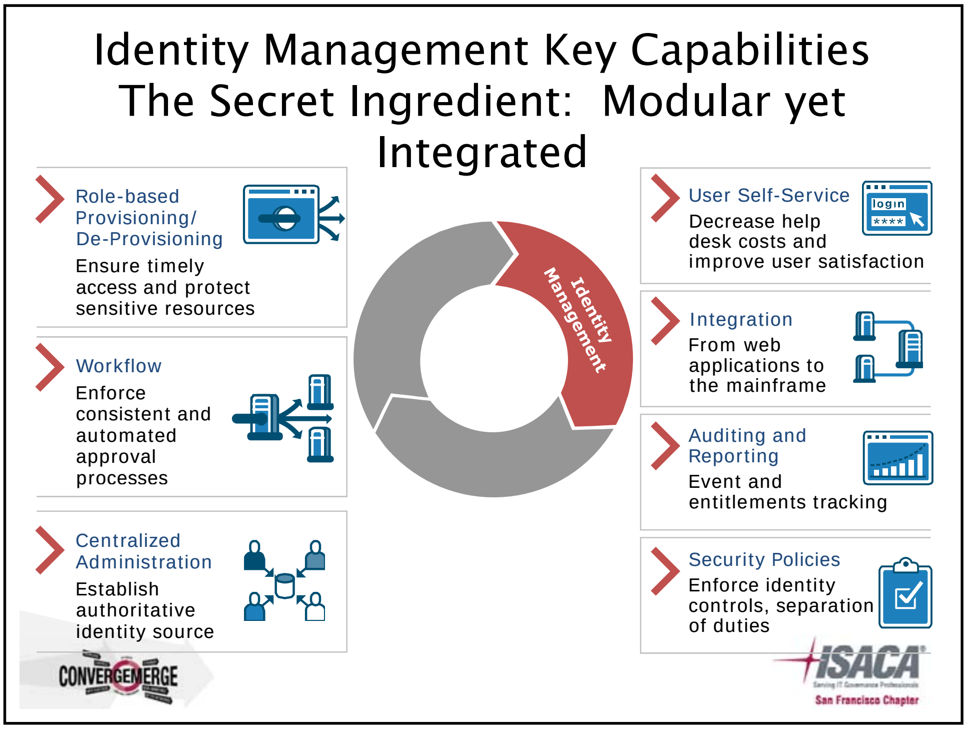
The Secret Ingredient – Pattern Recognition Analysis



Identity Management

Central engine for identity-related processes

- Provisioning/De-Provisioning
  - Quickly assigns and removes access privileges
  - Automates consistent workflow processes
- User Self Service
  - Empowers end users to resolve issues
  - Reduces burden on IT and help desk
- Identity Administration
  - Centralizes data/policy for consistency across enterprise
  - Delegates decision-making to application owners



Identity Management Key Capabilities The Secret Ingredient: Modular yet Integrated

Role-based Provisioning/ De-Provisioning
Ensure timely access and protect sensitive resources

Workflow
Enforce consistent and automated approval processes

Centralized Administration
Establish authoritative identity source

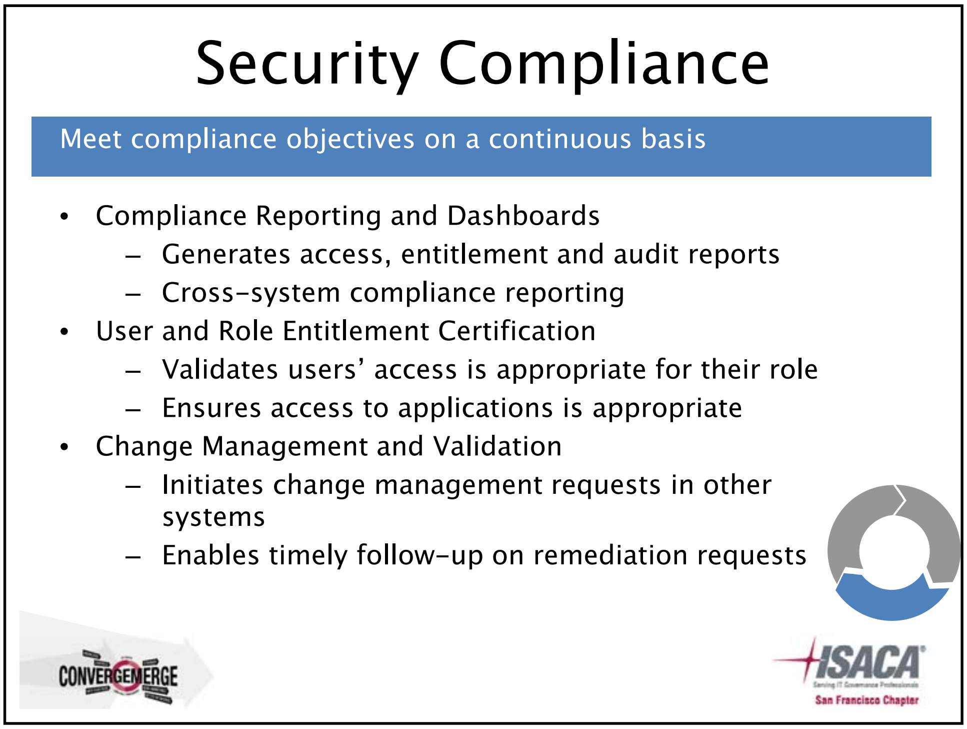
Identity Management

User Self-Service
Decrease help desk costs and improve user satisfaction

Integration
From web applications to the mainframe

Auditing and Reporting
Event and entitlements tracking

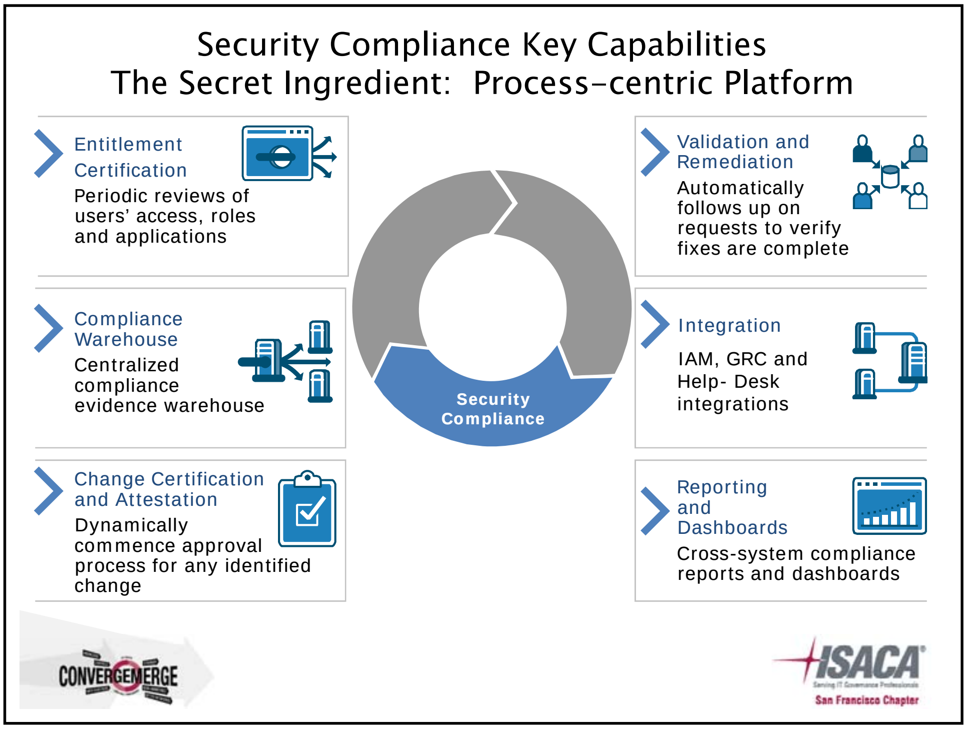
Security Policies
Enforce identity controls, separation of duties



Security Compliance

Meet compliance objectives on a continuous basis

- Compliance Reporting and Dashboards
  - Generates access, entitlement and audit reports
  - Cross-system compliance reporting
- User and Role Entitlement Certification
  - Validates users' access is appropriate for their role
  - Ensures access to applications is appropriate
- Change Management and Validation
  - Initiates change management requests in other systems
  - Enables timely follow-up on remediation requests



Security Compliance Key Capabilities
The Secret Ingredient: Process-centric Platform

Entitlement Certification
Periodic reviews of users' access, roles and applications

Compliance Warehouse
Centralized compliance evidence warehouse

Change Certification and Attestation
Dynamically commence approval process for any identified change

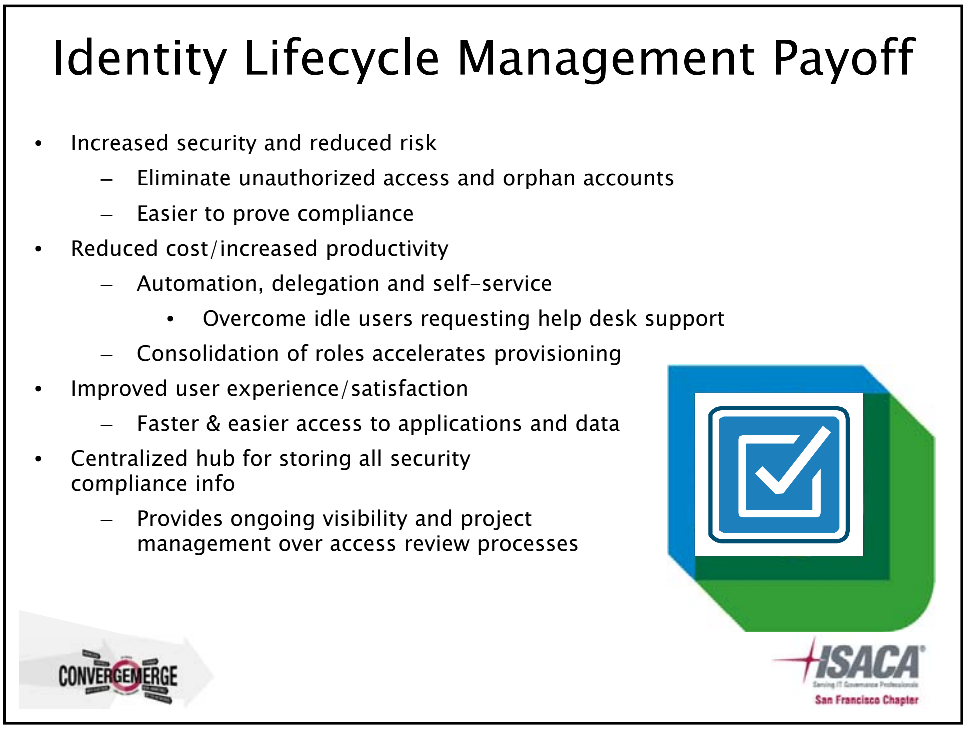
Validation and Remediation
Automatically follows up on requests to verify fixes are complete

Integration
IAM, GRC and Help- Desk integrations

Reporting and Dashboards
Cross-system compliance reports and dashboards

CONVERGEMERGE

ISACA
San Francisco Chapter



Identity Lifecycle Management Payoff

- Increased security and reduced risk
  - Eliminate unauthorized access and orphan accounts
  - Easier to prove compliance
- Reduced cost/increased productivity
  - Automation, delegation and self-service
    - Overcome idle users requesting help desk support
  - Consolidation of roles accelerates provisioning
- Improved user experience/satisfaction
  - Faster & easier access to applications and data
- Centralized hub for storing all security compliance info
  - Provides ongoing visibility and project management over access review processes

CONVERGEMERGE

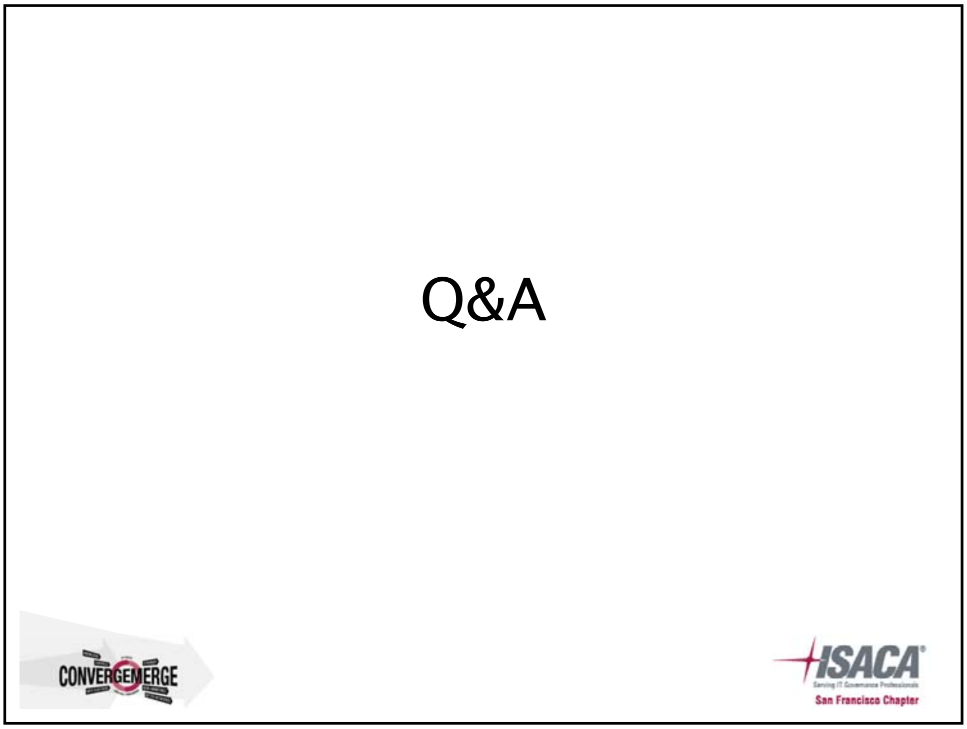
ISACA
San Francisco Chapter

Customer Successes: Identity Lifecycle Management

- Problems
  - Organizations with more roles than users
  - 10+ days to provision new employees
  - Very complex IT environments:
    - 100+ target systems, 150K roles, 200K identities
  - Man weeks to complete compliance processes such as access reviews (multiple man-weeks)
- Solutions
  - Reduce 150K roles to <5K roles
  - Provision new employees in <1 day to multiple systems
  - Complete access reviews in hours not days

Summary

- You need to streamline and automate your existing identity lifecycle management processes for:
  - Identity management
  - Role mining and management
  - Security compliance
- You need to find vendors who have a complete, integrated solution to manage the entire identity lifecycle across your enterprise



Q&A

CONVERGEMERGE

ISACA®
Serving IT Governance Professionals
San Francisco Chapter