



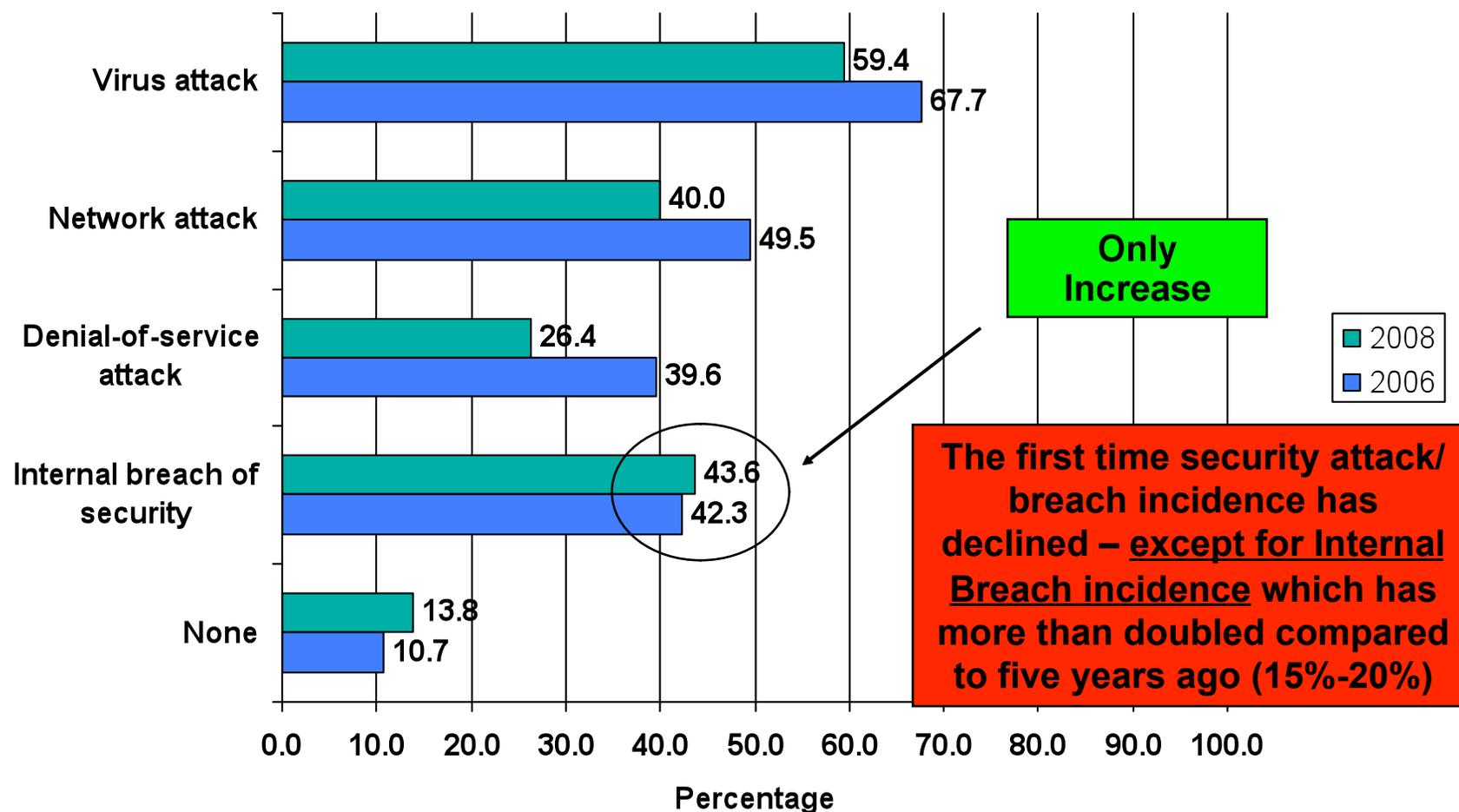
Leveraging an Identity Management Foundation to Sustain Compliance

Michael Coady
Worldwide Vice President
Security Business Unit

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

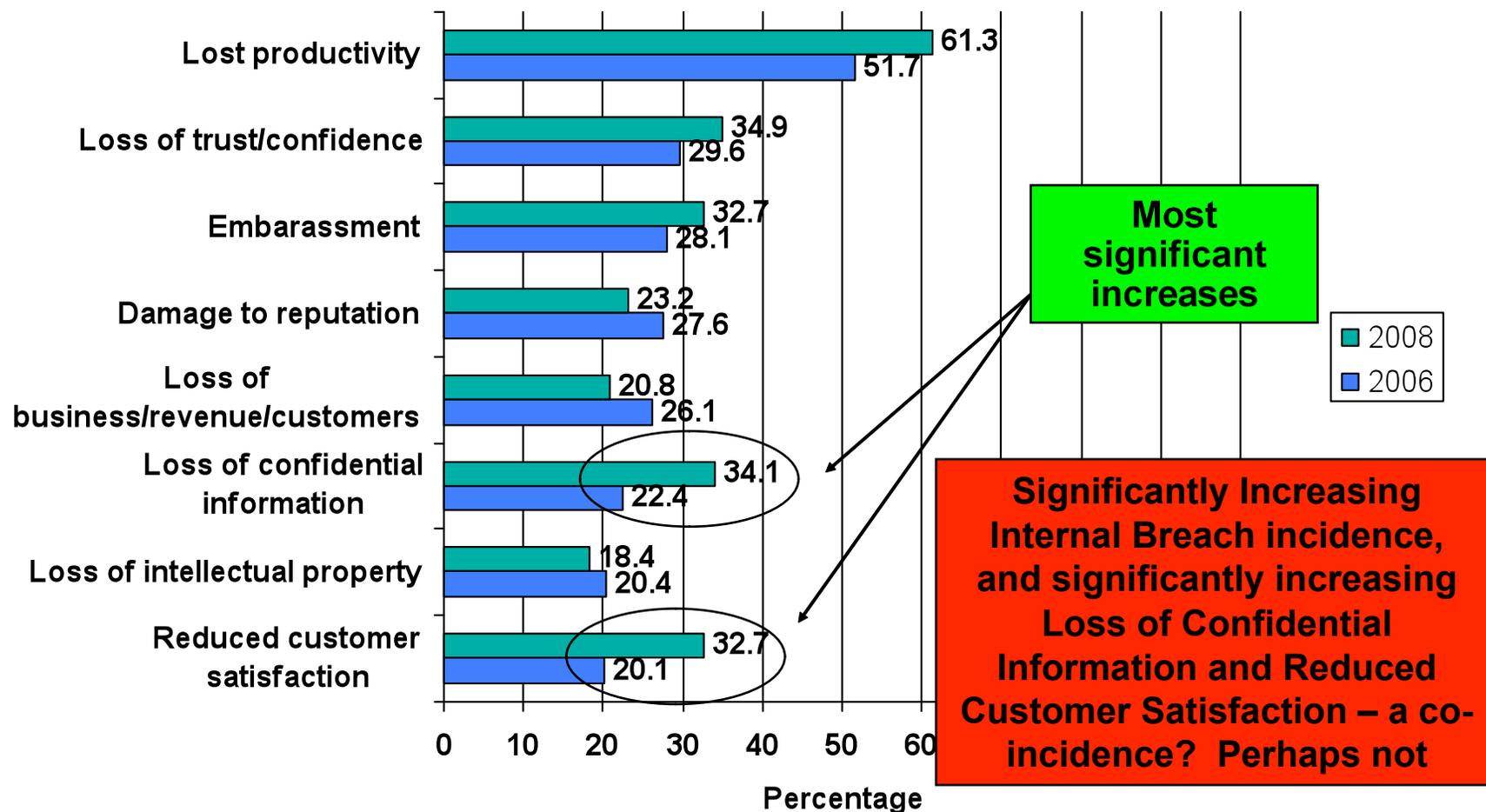
Security Attacks and Breaches



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



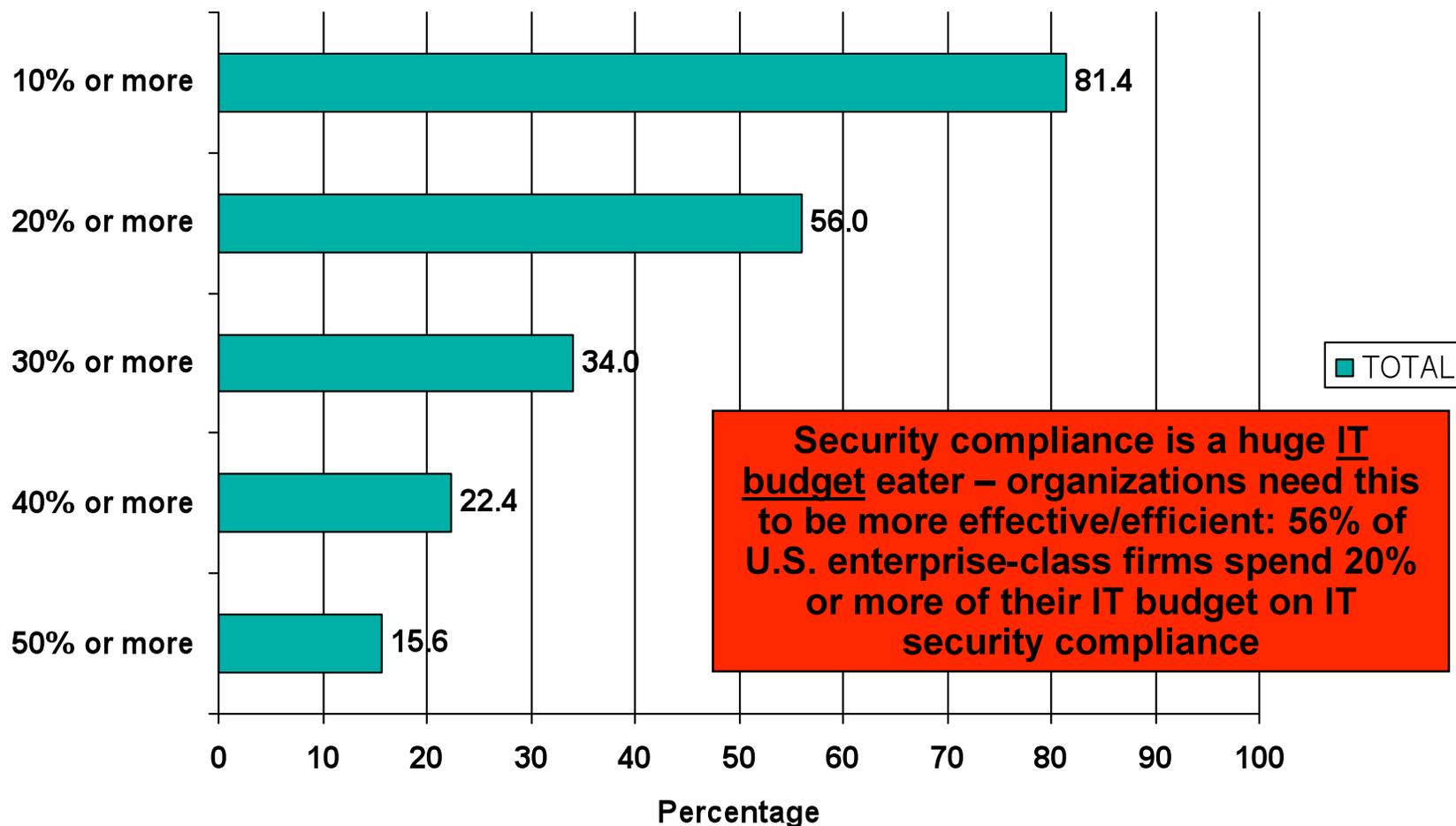
Security Attack/Breach Costs



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



Security Compliance Costs - Budget

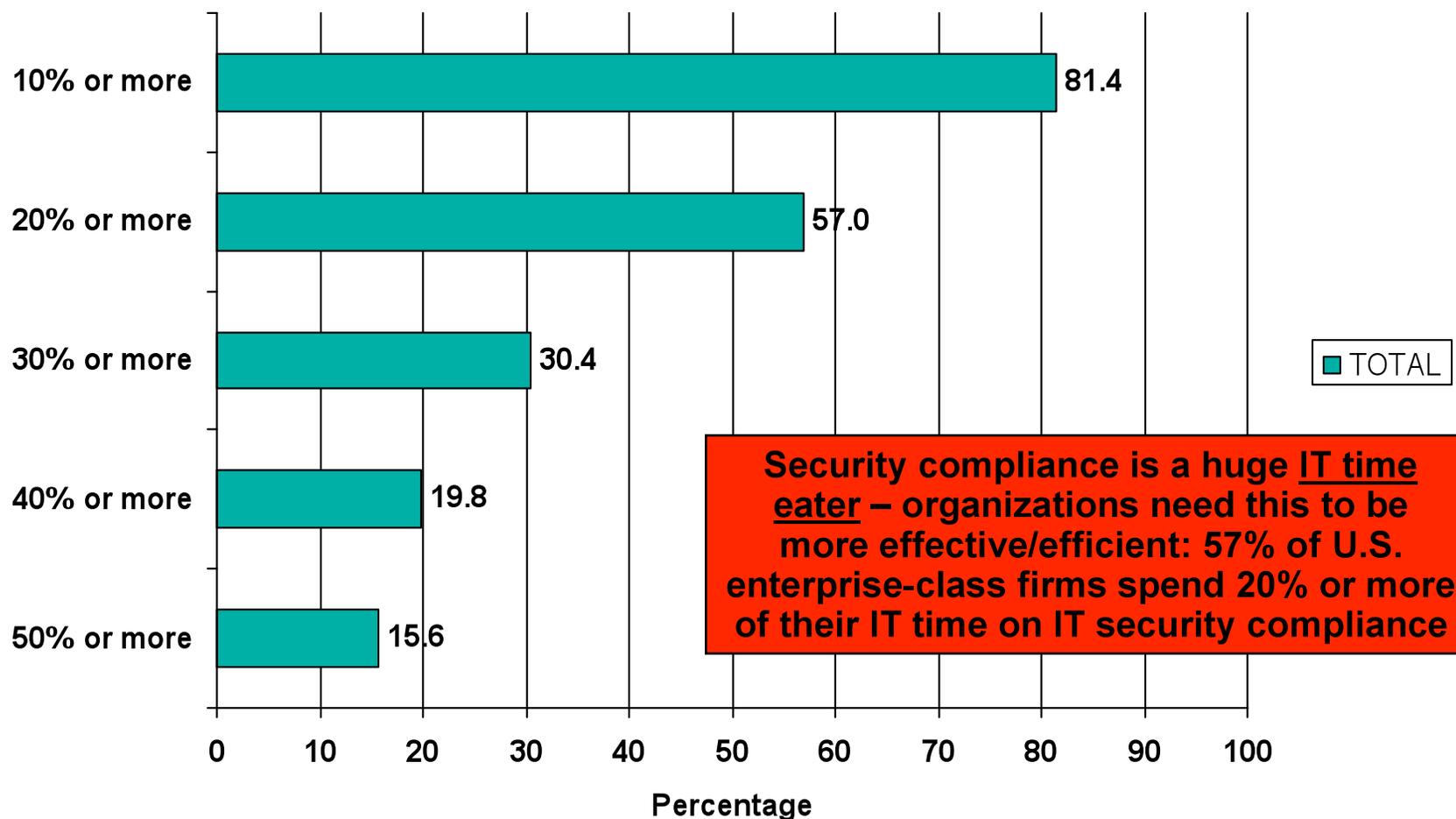


N=500. Q104. What percent of your organization's IT budget is spent specifically to ensure IT security compliance with various regulations?

Source: *The Strategic Counsel*, 2008

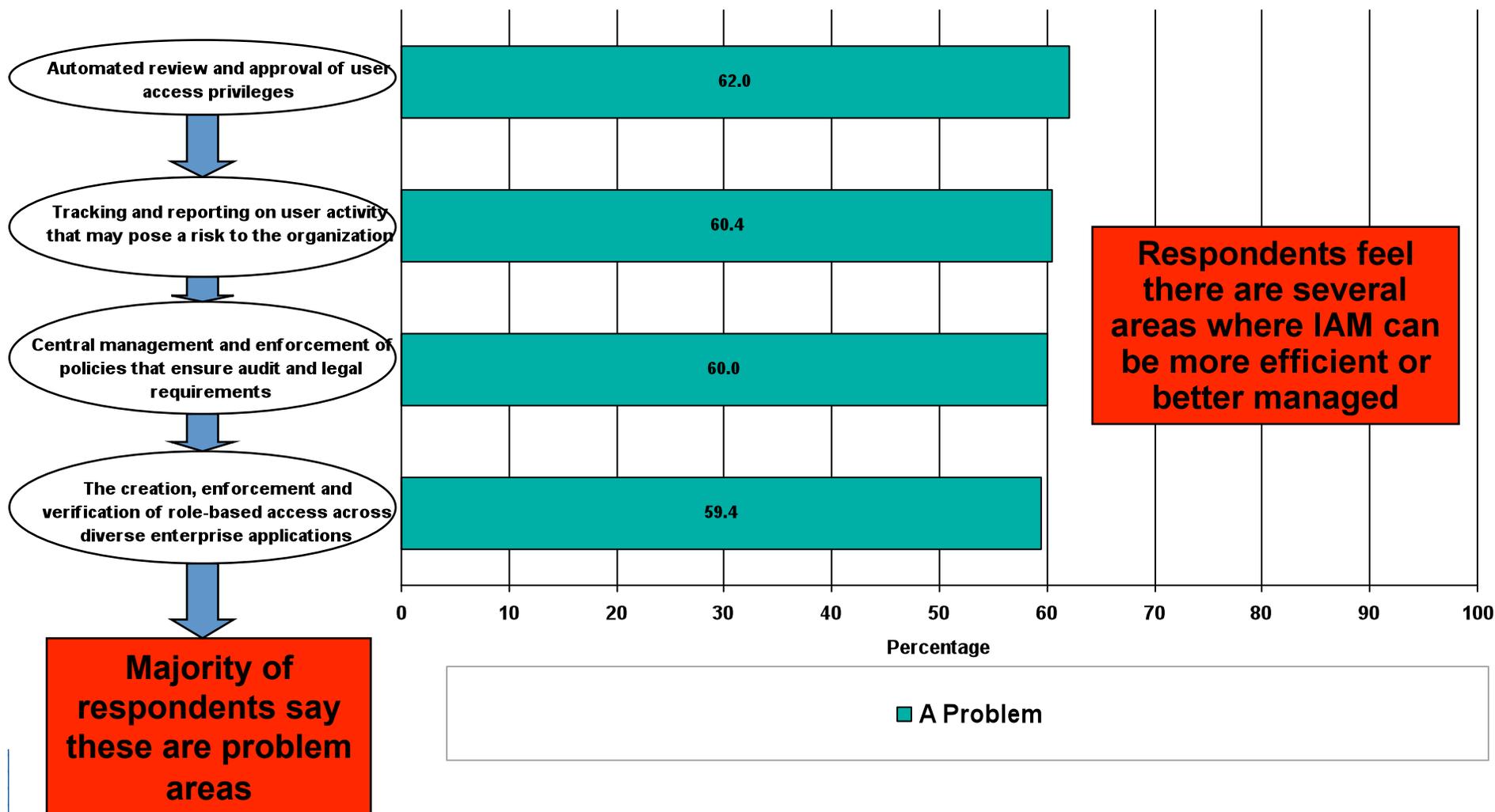


Security Compliance Costs - Time



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

IAM Issues and Problems

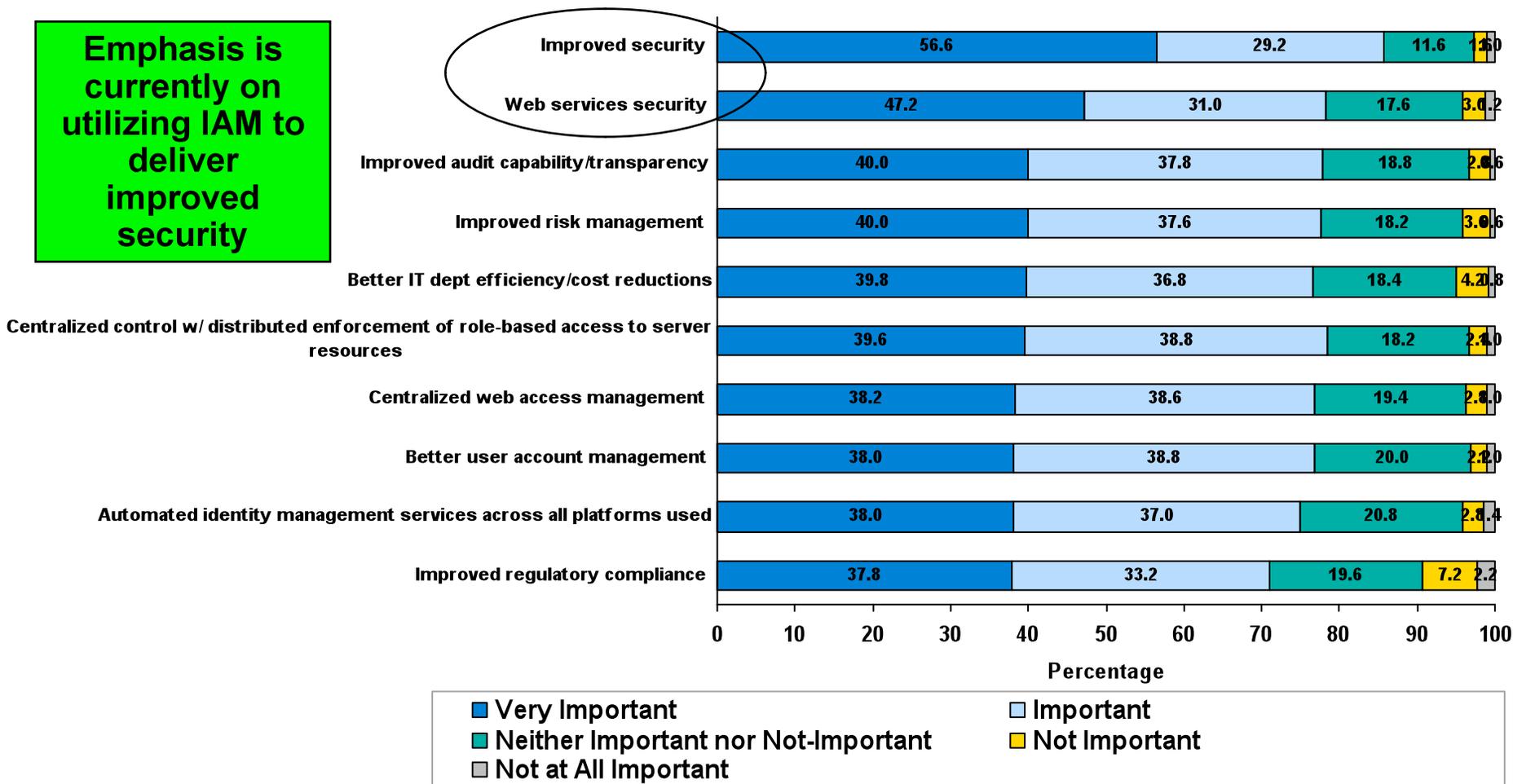


N=500. Q101. Are any of the following problem areas for your organization...?
 Source: *The Strategic Counsel*, 2008



What Users Expect IAM To Deliver – 2008 Top Deliverables

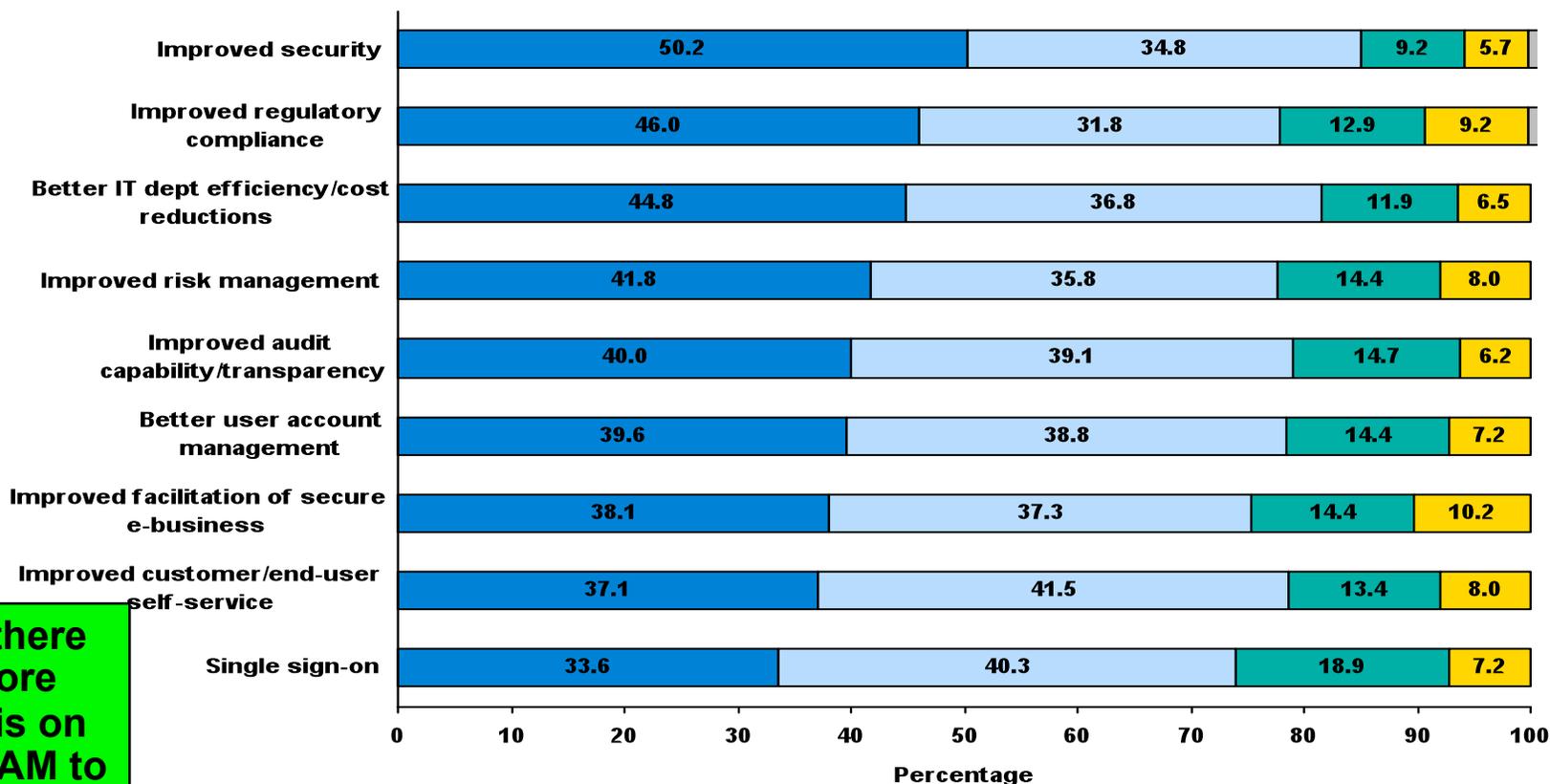
Emphasis is currently on utilizing IAM to deliver improved security



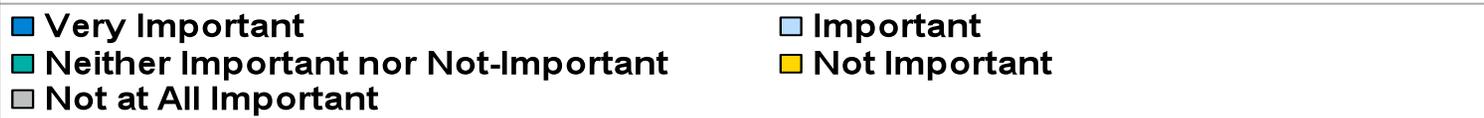
N=500. Q7. How important is it for your current or planned IT Identity and Access Management solution to deliver the following?
Source: *The Strategic Counsel*, 2008



What Users Expect IAM To Deliver – 2006 Top Deliverables



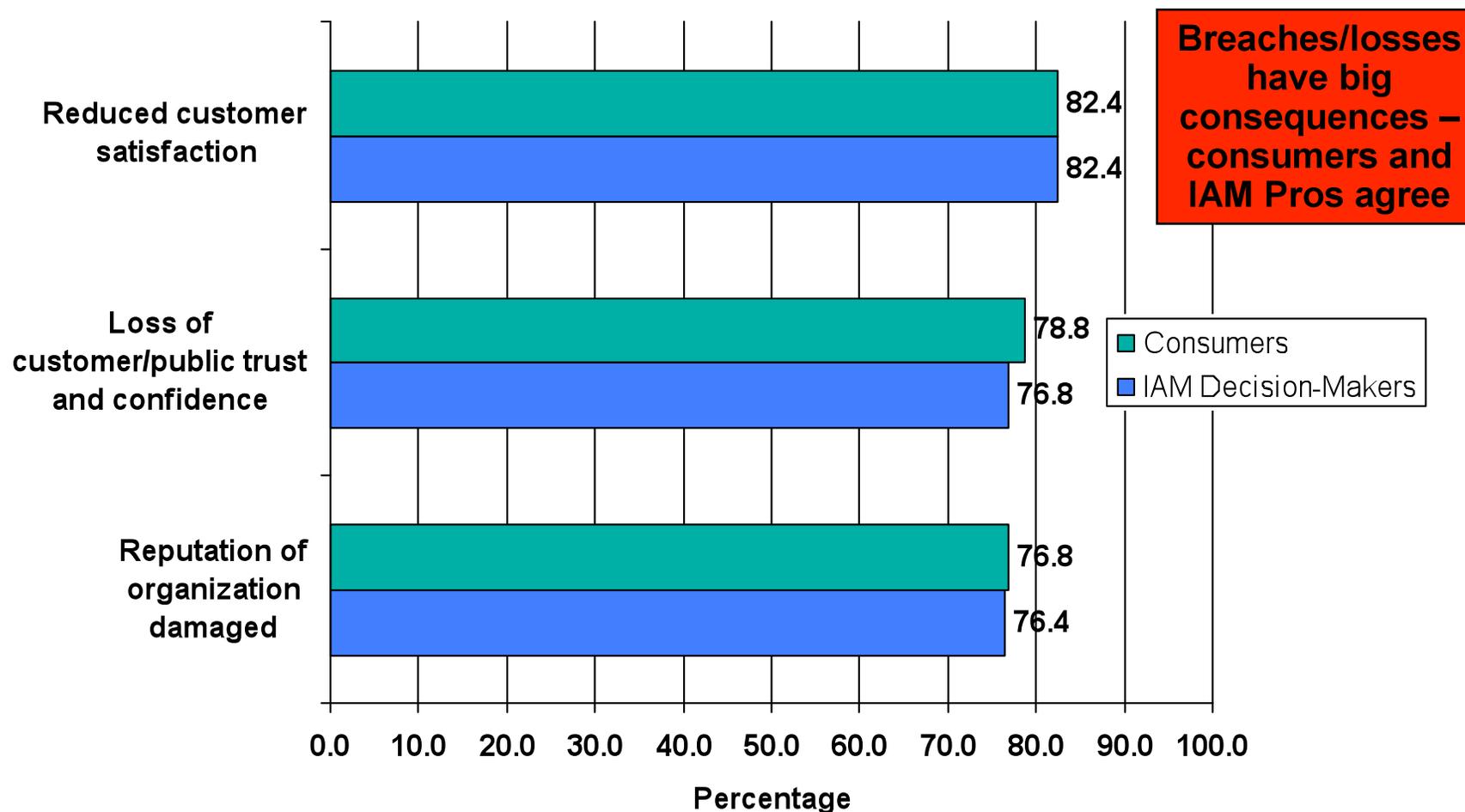
In 2006 there was more emphasis on utilizing IAM to improve compliance and achieve IT efficiencies / cost reductions



What is it for your current or planned IT Identity and Access Management solution to deliver the following?
The Strategic Counsel, 2006



Consumer and IAM Decision-Maker Security and Privacy Confidence

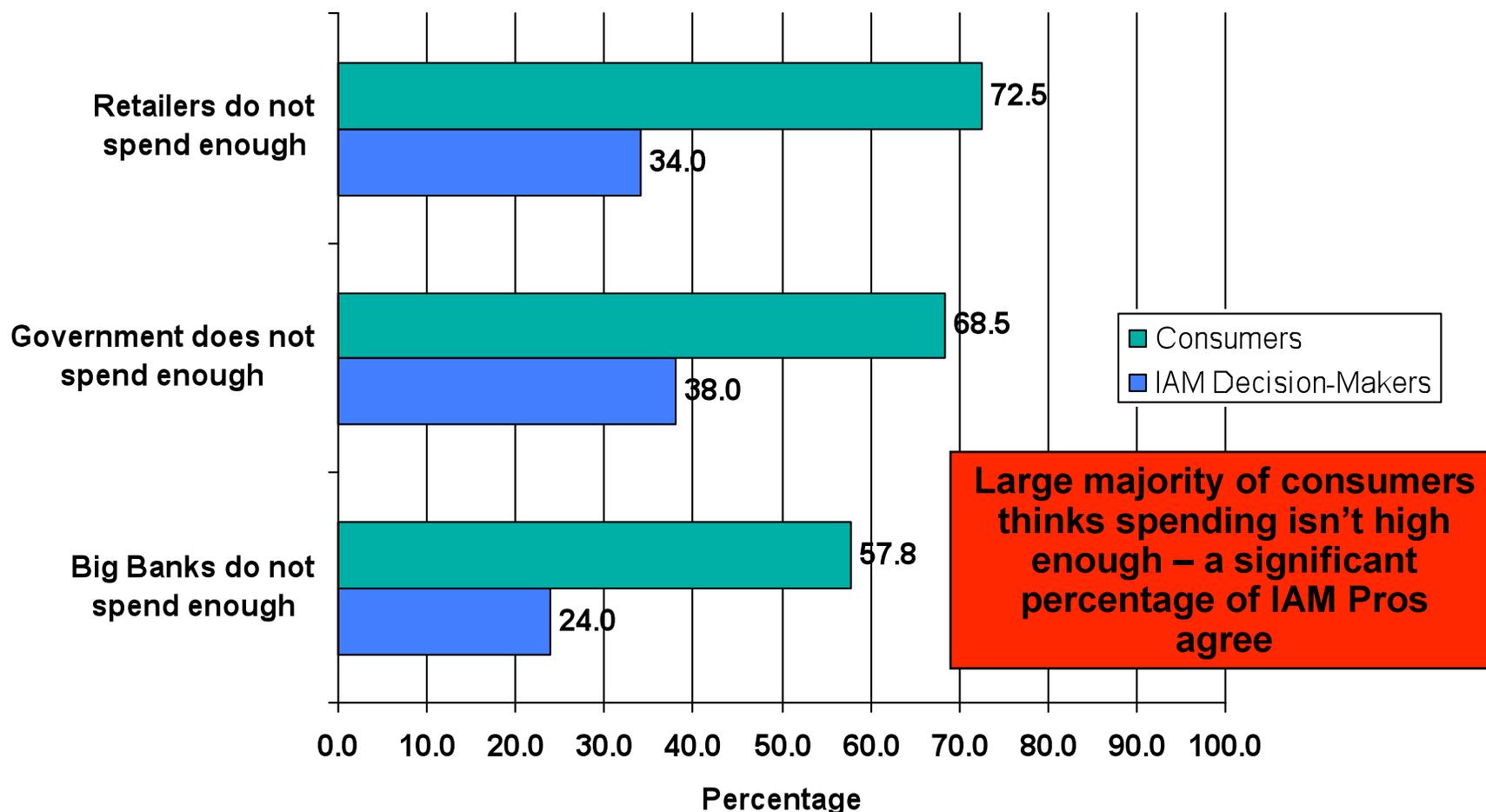


N=400. Q6. What is the impact of major security or privacy breaches for you?

N=500 Q17. If your organization suffered a loss of customer or transaction data, what impact would it have?

Source: *The Strategic Counsel*, 2008

Consumer and IAM Decision-Maker Security and Privacy Confidence



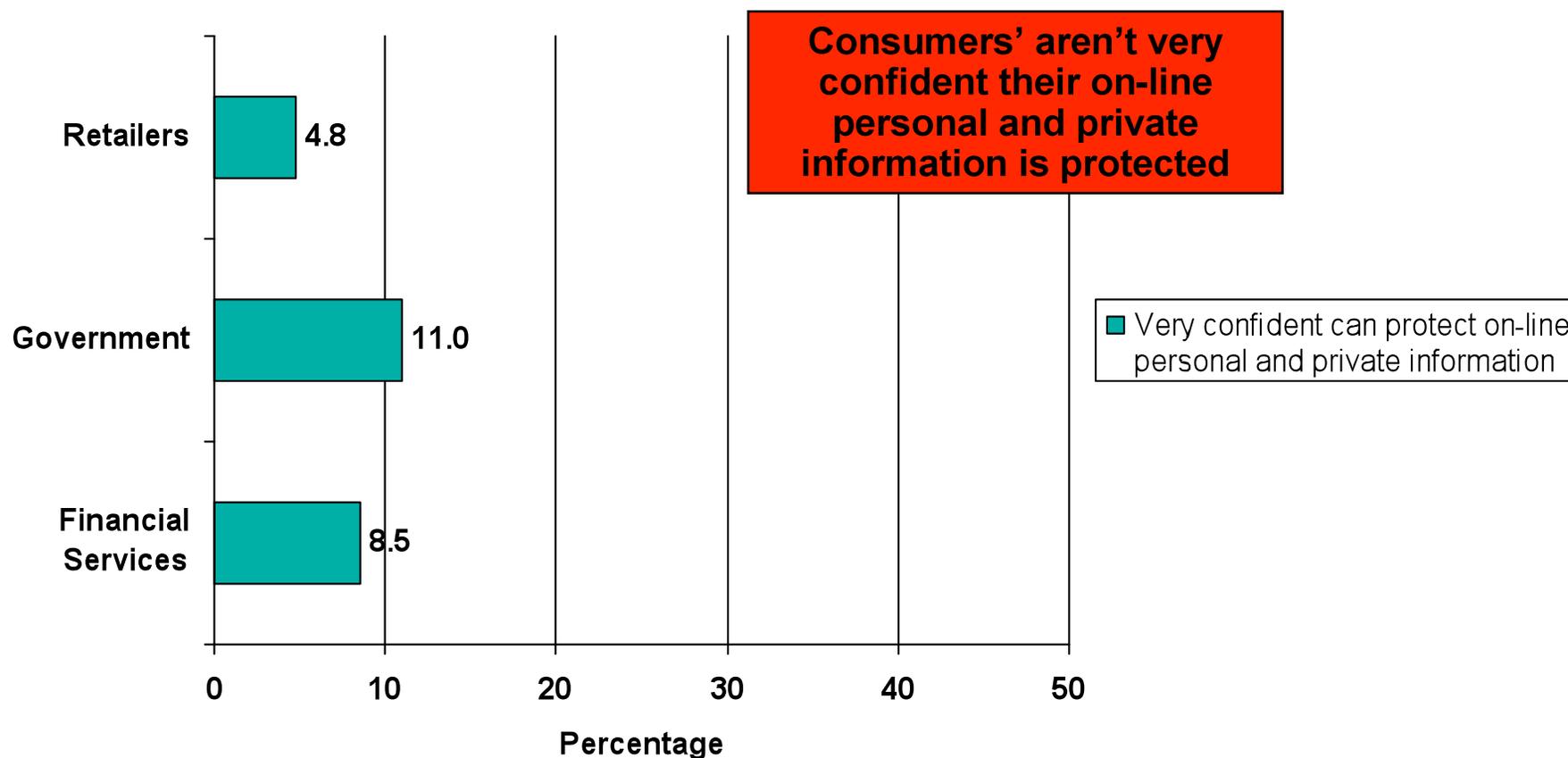
N=400. Q8-Q10. Do you think _____ spends enough on on-line security and privacy?

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



Consumer Security and Privacy Confidence

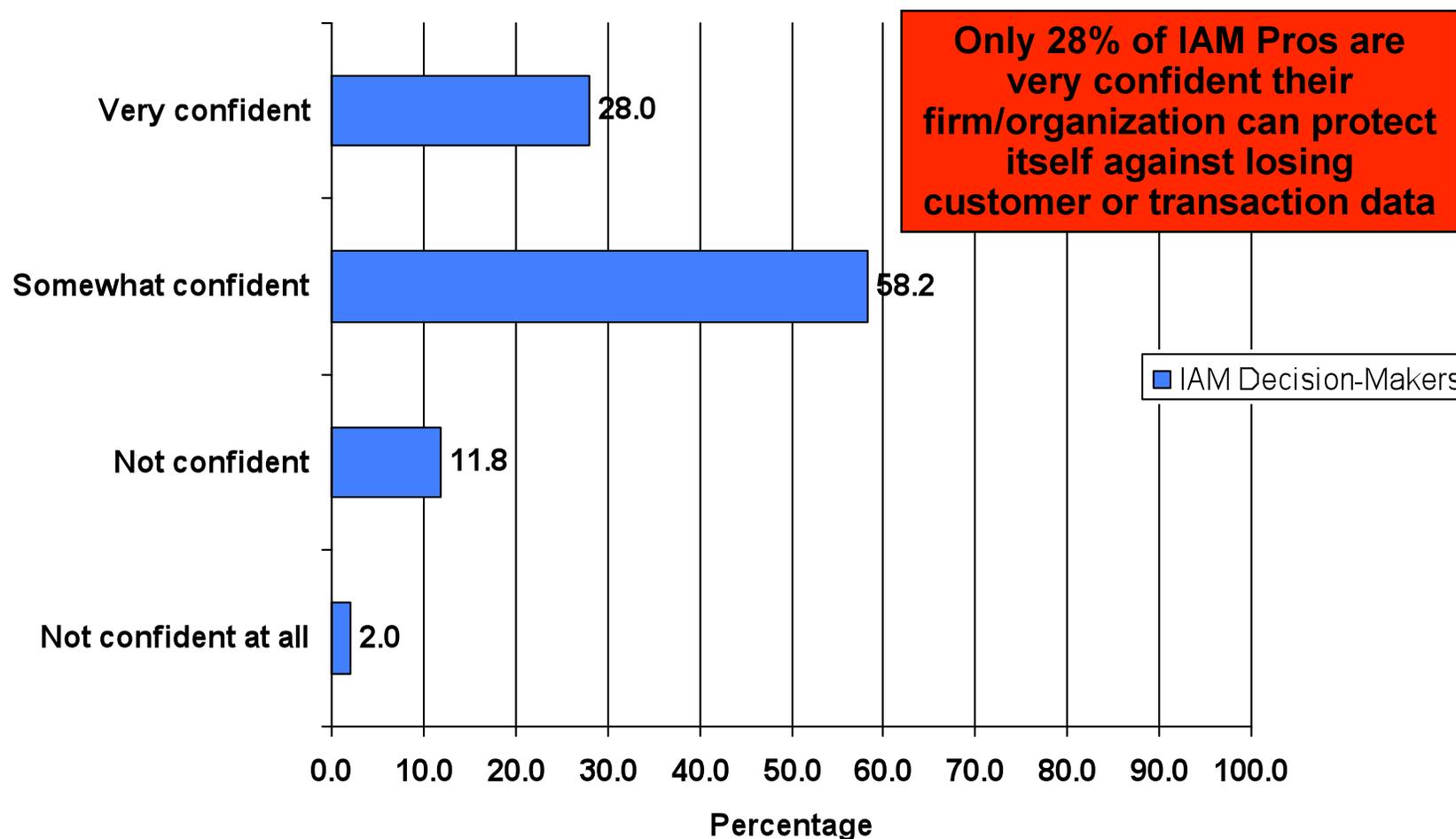


N=500. Q3a-b-c. How confident are you that the banking industry is properly protecting your on-line personal and private information? How confident are you that retailers are properly protecting your on-line personal and private information? How confident are you that the Government is properly protecting your on-line personal and private information?

Source: *The Strategic Counsel*, 2008



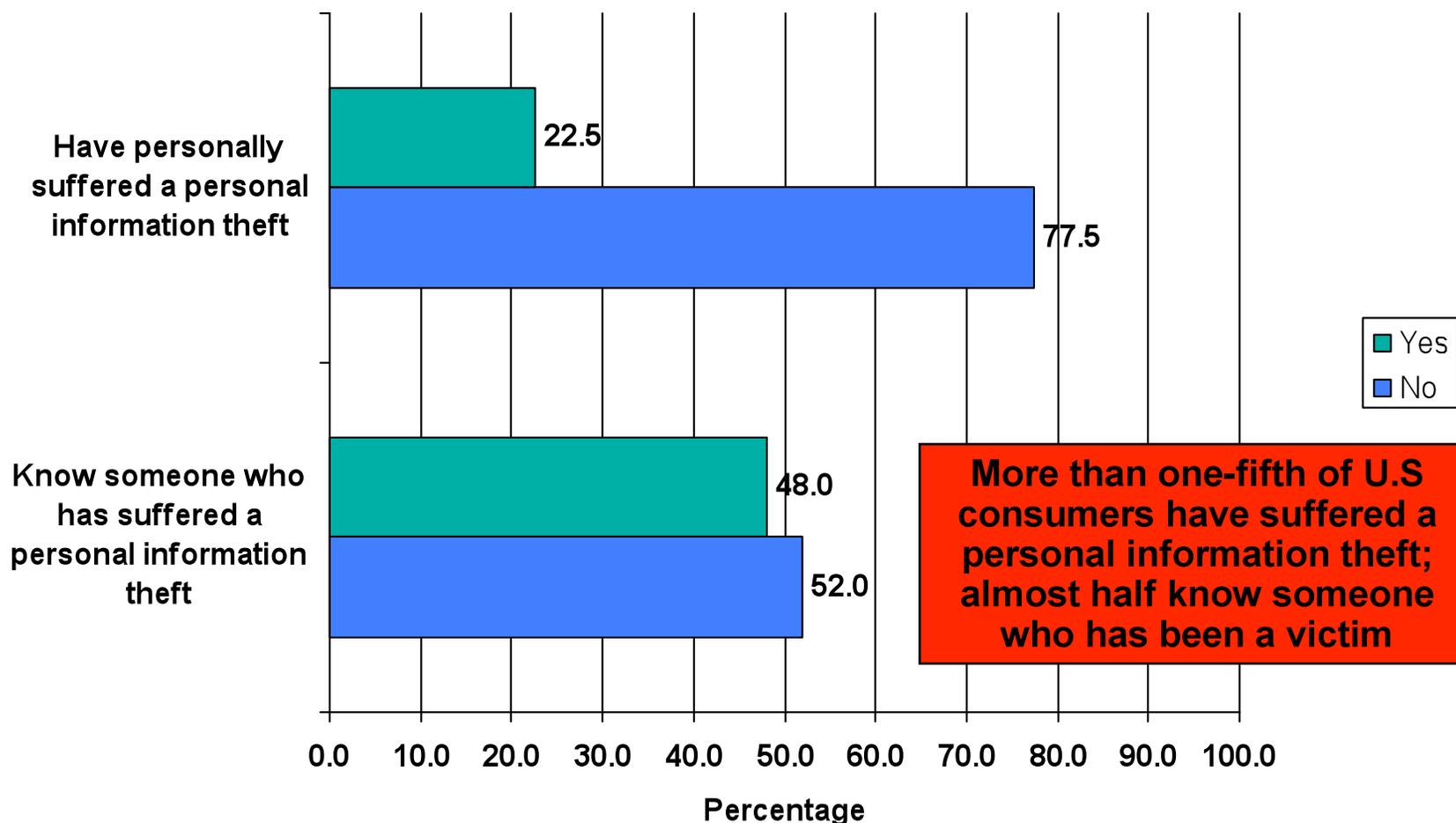
IAM Decision-Maker Security and Privacy Confidence



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



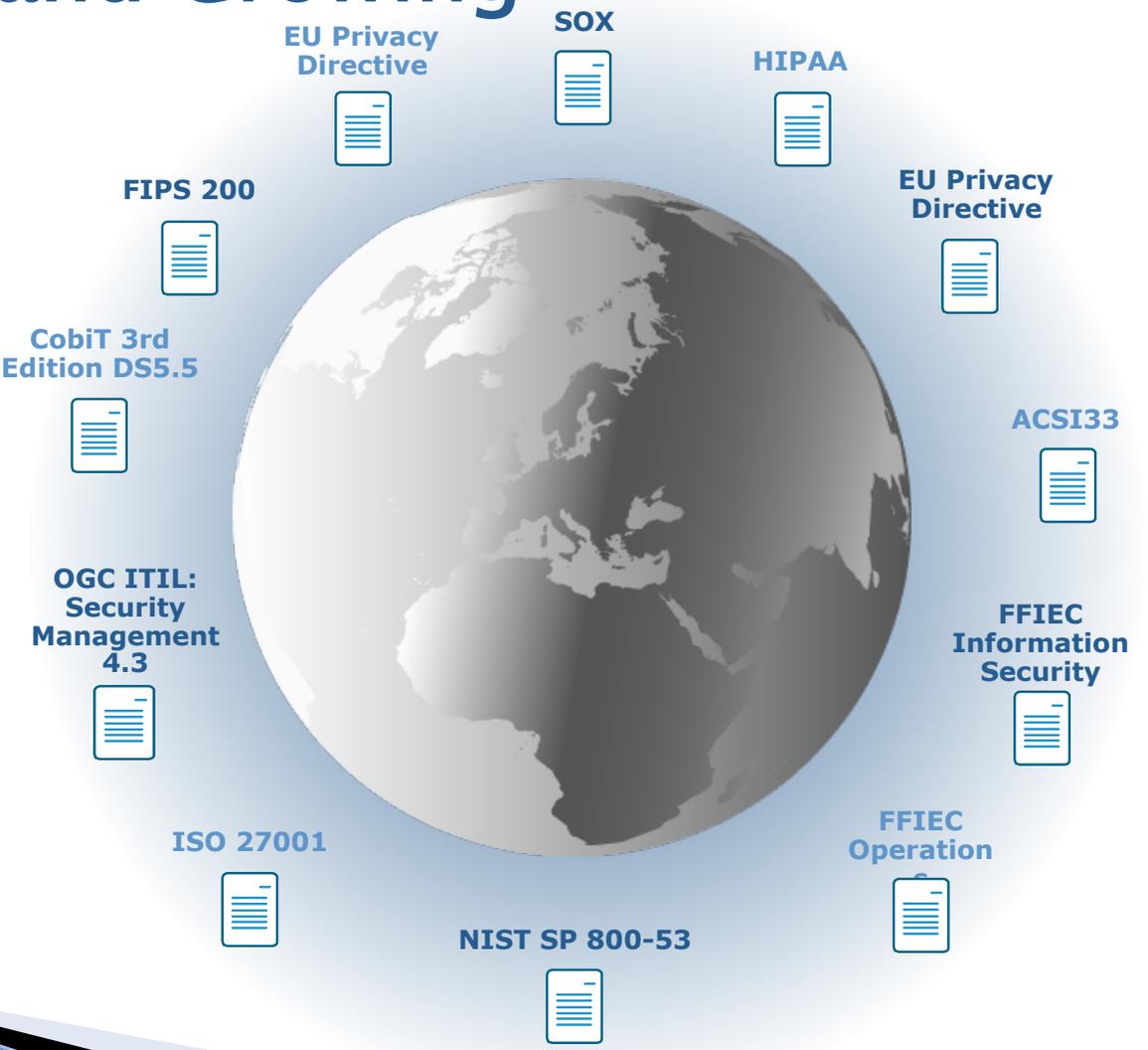
Consumer Personal Information Theft Victimization



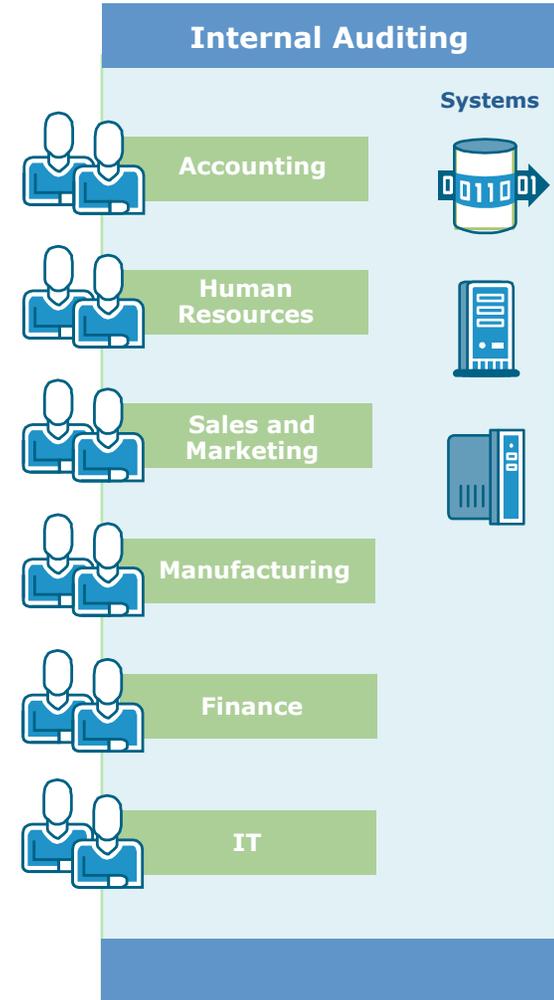
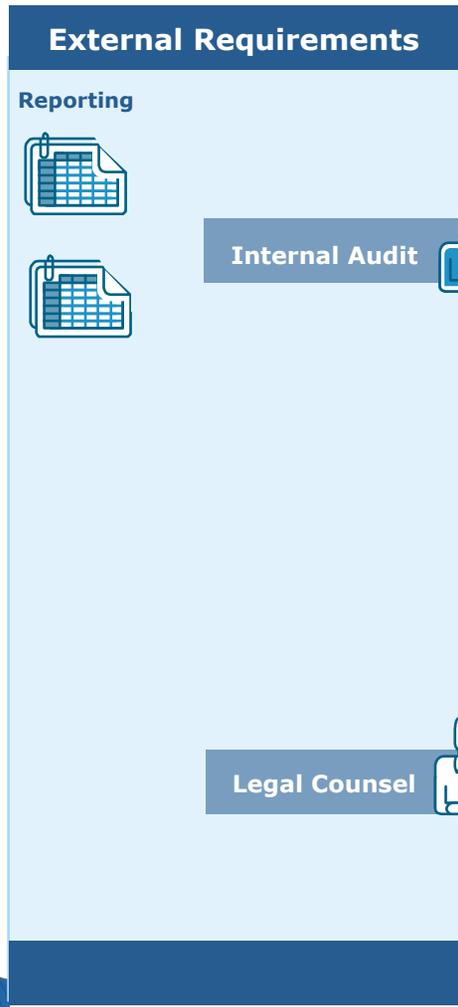
N=400. Q7-Q8. Have you ever suffered a personal information theft? Do you know someone who has been the victim of personal information theft?

Source: *The Strategic Counsel*, 2008

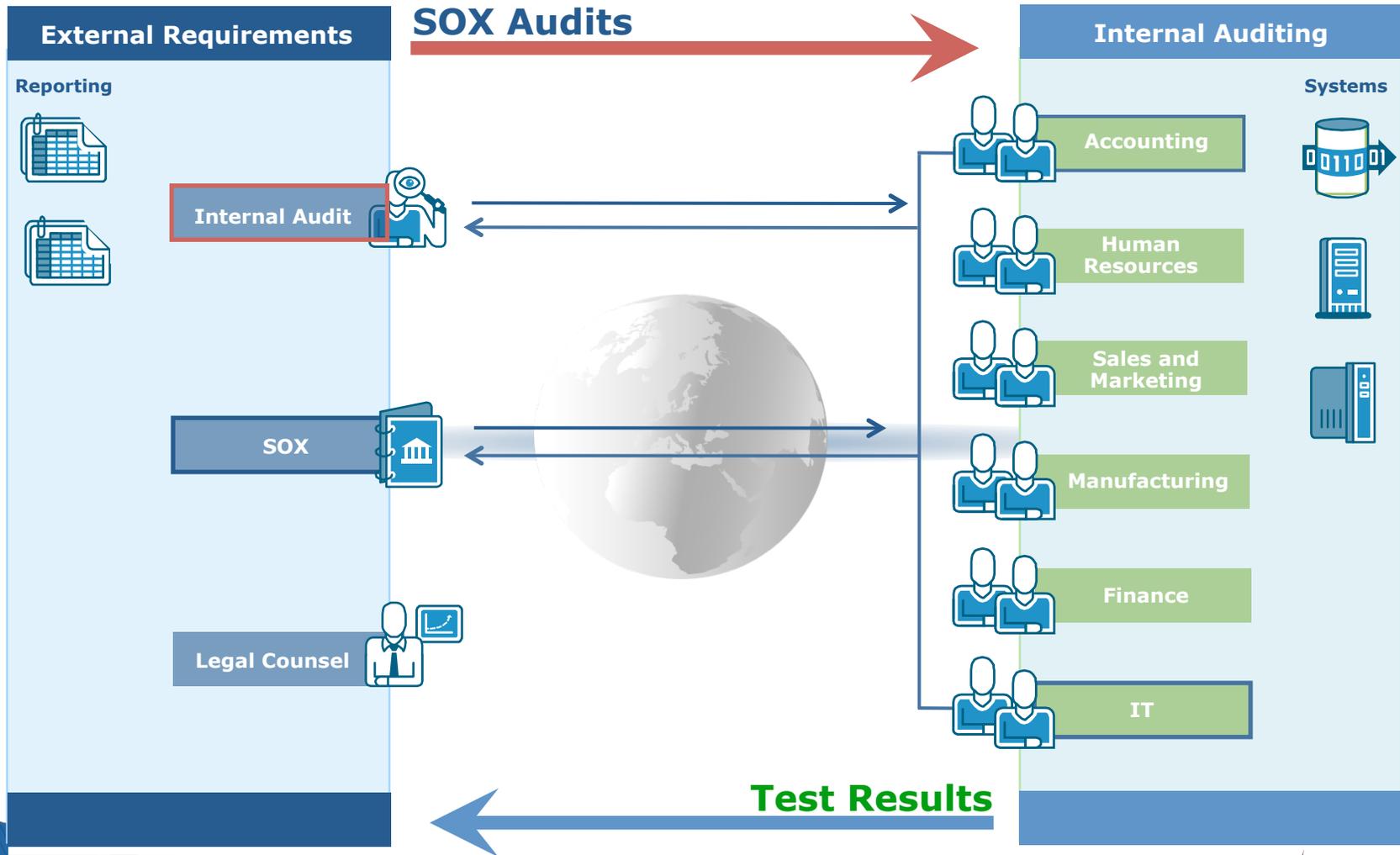
The Regulatory Environment Global and Growing



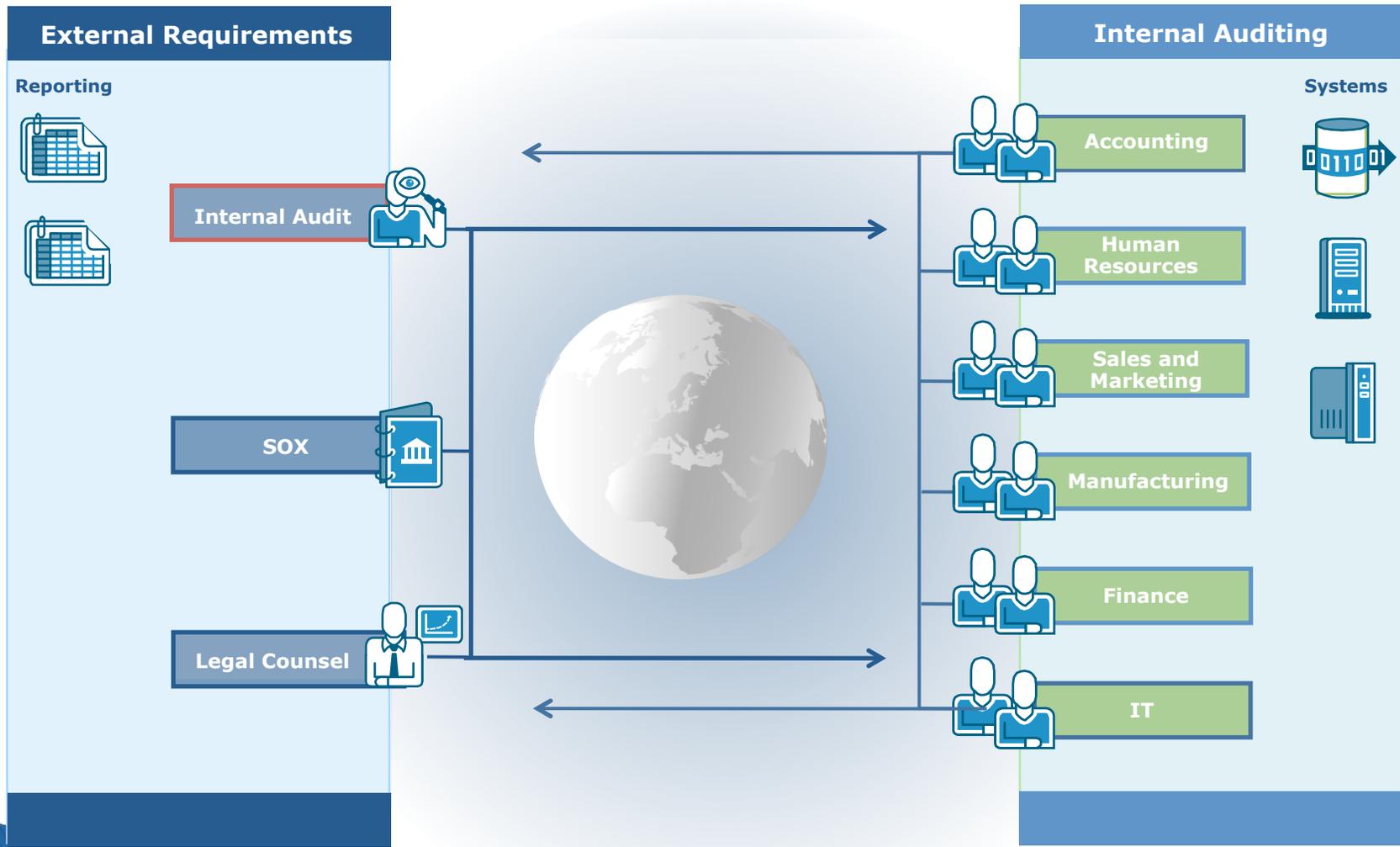
Compliance: The Early Days



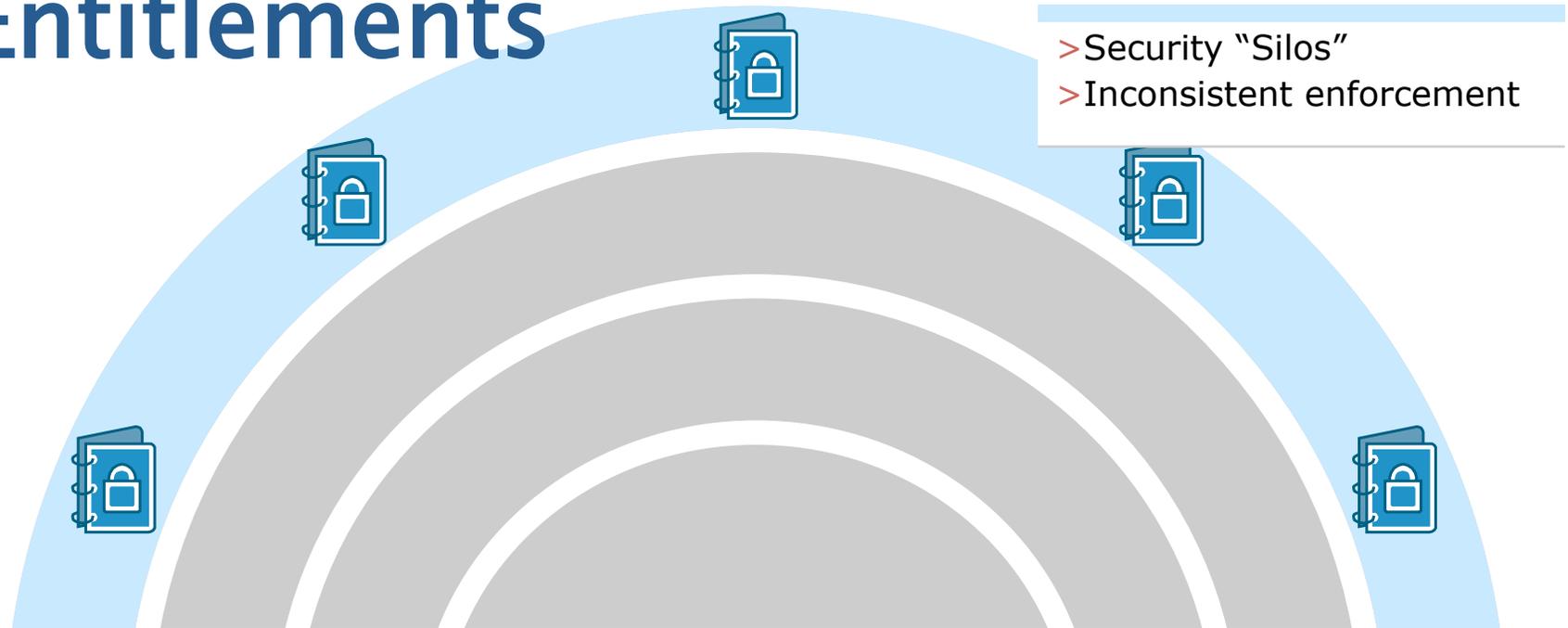
Enter SOX



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



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...

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

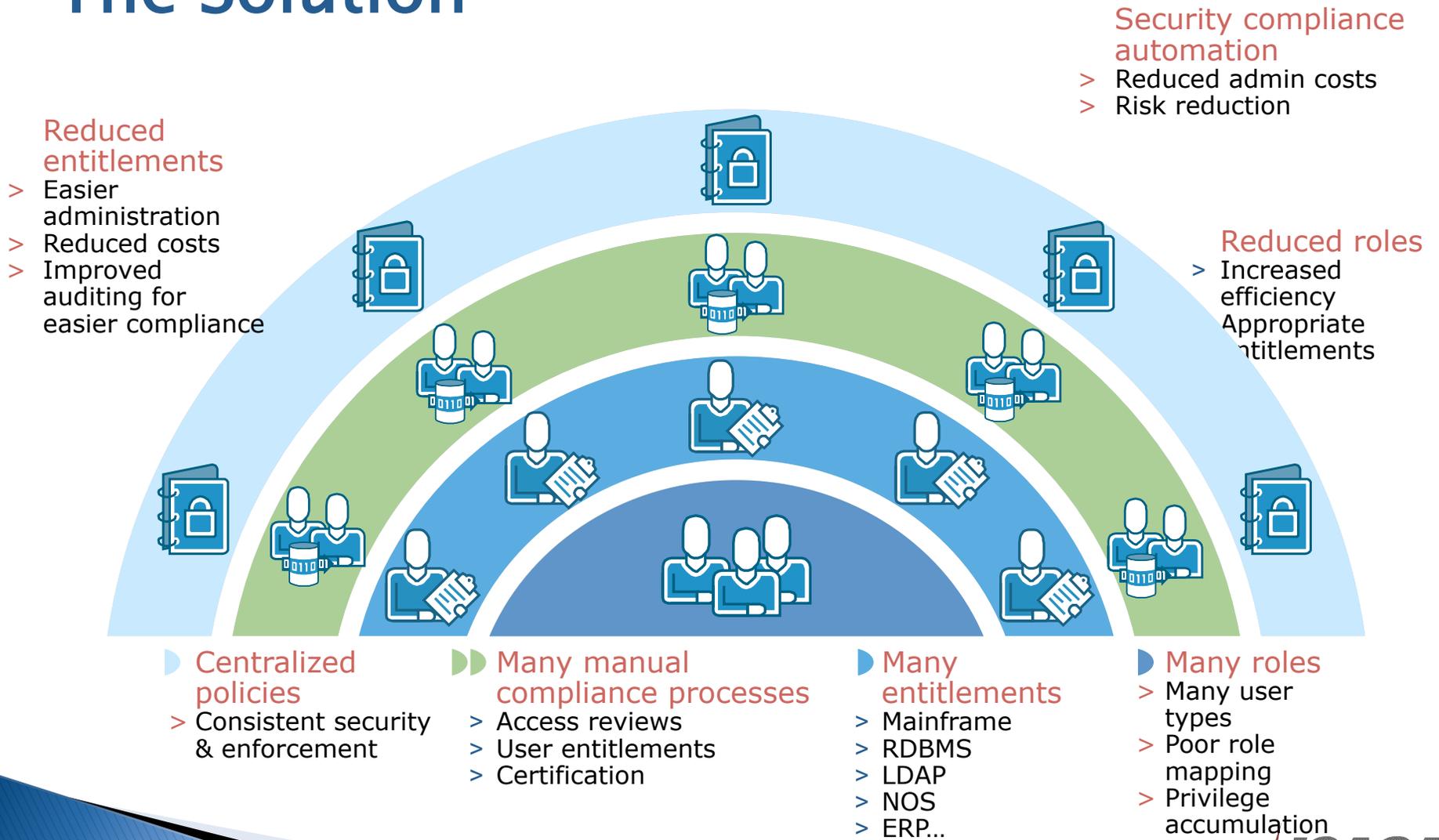
- > Mainframe
- > RDBMS
- > LDAP
- > NOS
- > ERP...

▶ Many roles

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

Identity Lifecycle Management

The Solution



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

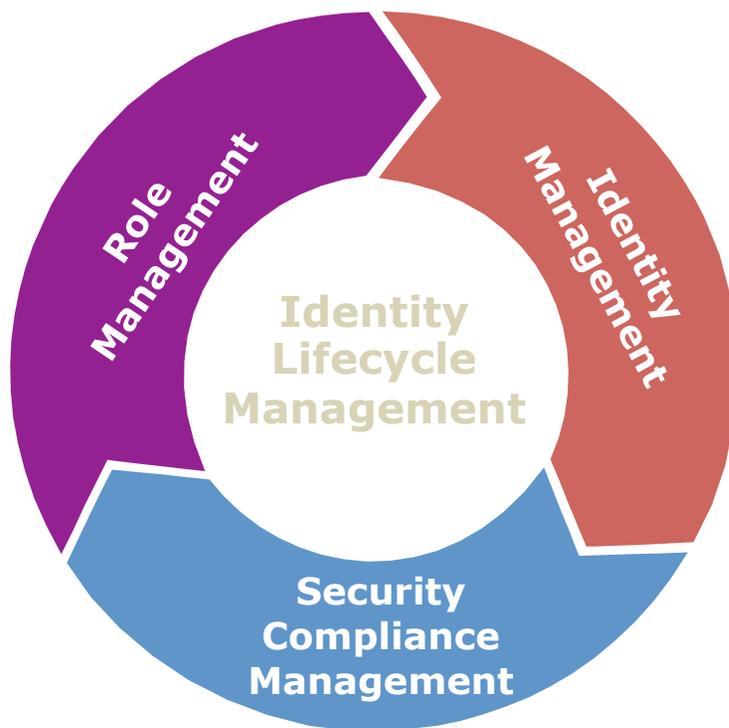
Identity Lifecycle Management

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

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

Identity Management

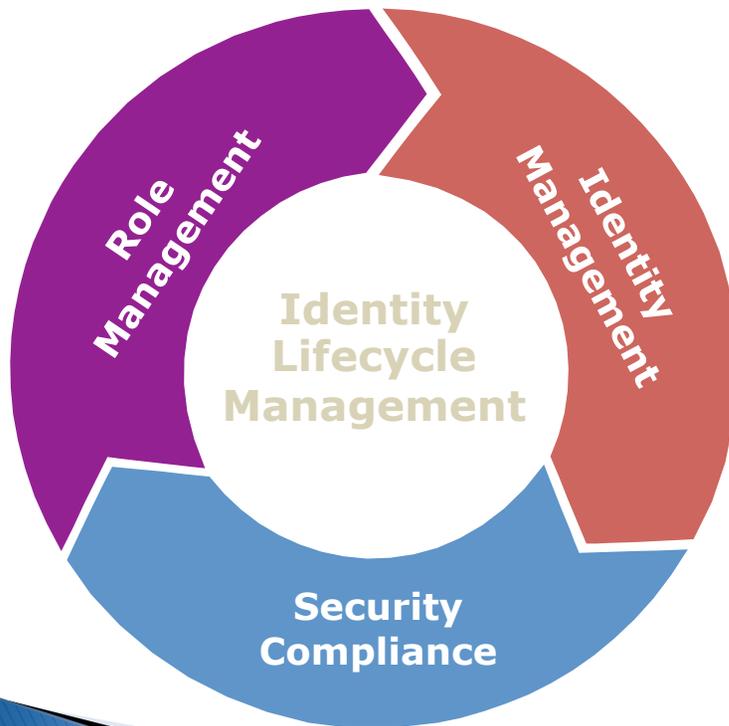
- Assign users to roles
- Apply role-based controls
- Provision users with approved accounts and privileges
- Manage change requests and approvals over time

Security Compliance Management

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

Identity Lifecycle Management: CA Approach

A complete approach: Enable users faster, reduce costs and risks, support compliance goals



Role Management

- Role discovery
- Maintain role model
- Role analysis and reporting

Identity Management

- Provisioning / De-provisioning
- User self-service
- Identity administration

Security Compliance

- Compliance reporting and dashboards
- User and role entitlement certification
- Initiate change management and validation

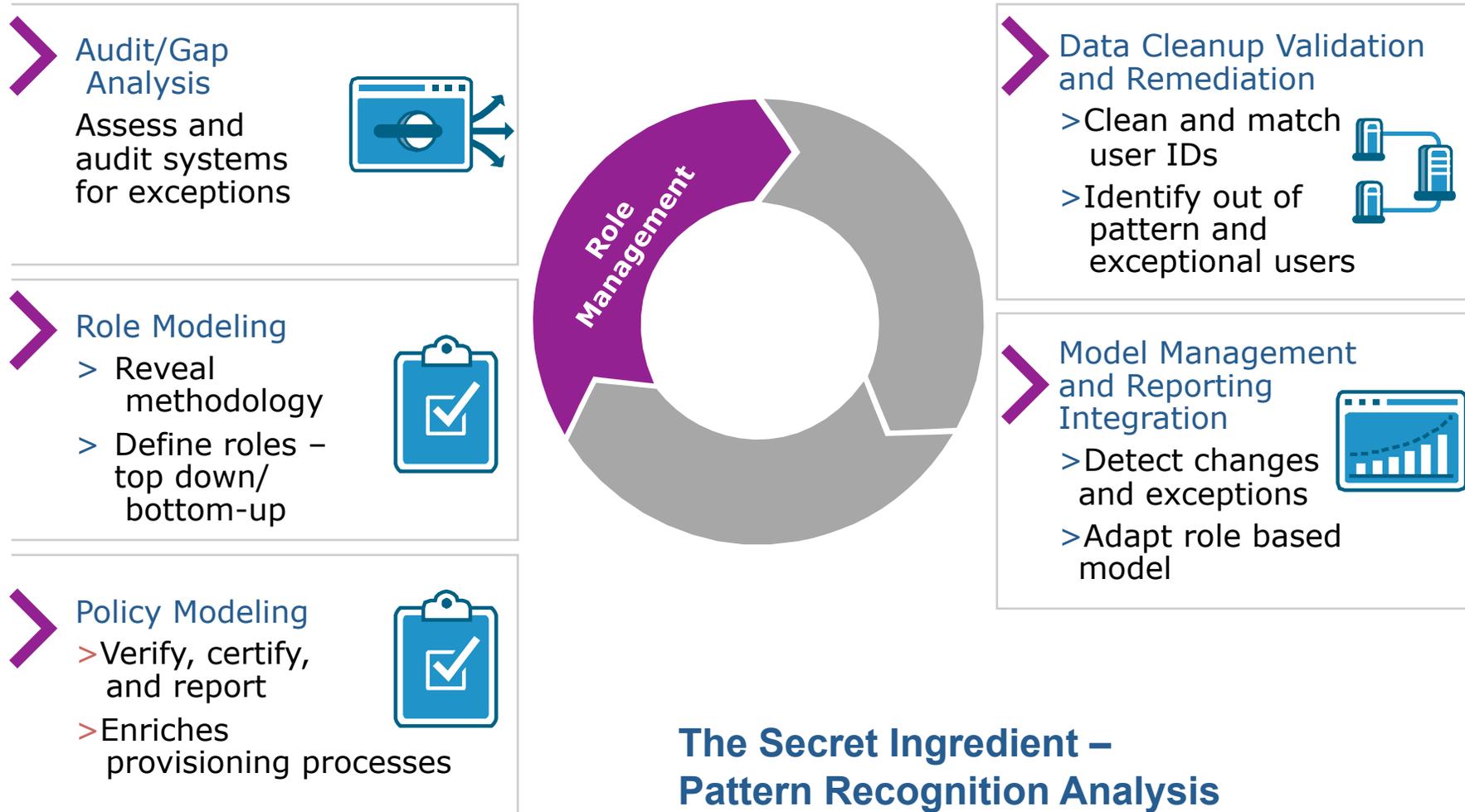
Role Mining/Management

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



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

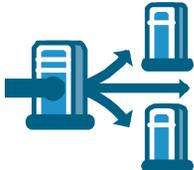


Identity Management Key Capabilities

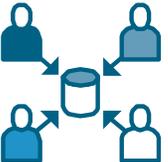
The Secret Ingredient: Modular yet Integrated

➤ **Role-based Provisioning/ De-Provisioning** 

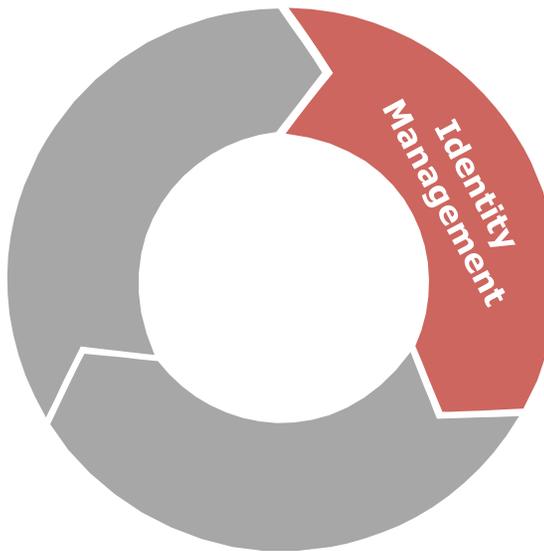
Ensure timely access and protect sensitive resources

➤ **Workflow** 

Enforce consistent and automated approval processes

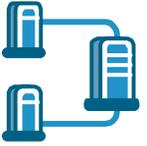
➤ **Centralized Administration** 

Establish authoritative identity source

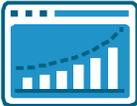


➤ **User Self-Service** 

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



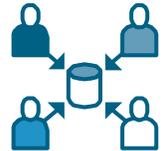
Security Compliance Key Capabilities

The Secret Ingredient: Process-centric Platform

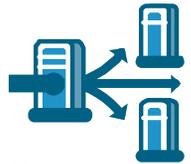
➤ Entitlement Certification
Periodic reviews of users' access, roles and applications



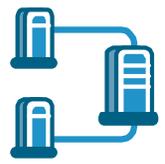
➤ Validation and Remediation
Automatically follows up on requests to verify fixes are complete



➤ Compliance Warehouse
Centralized compliance evidence warehouse



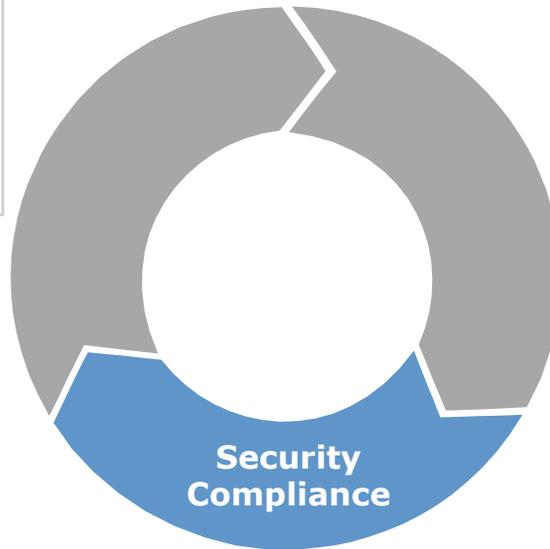
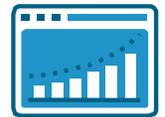
➤ Integration
IAM, GRC and Help- Desk integrations



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



➤ Reporting and Dashboards
Cross-system compliance reports and dashboards



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



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

