Tivoli software

IT Governance, Risk Management and Security

Juan Francisco Garcia
Tivoli Brand Manager
IBM Software Group, francisco.garcia@mx1.ibm.com

Agenda

- Introduction
- A Business Perspective on Governance, Risk Management & Security
- IBM's Security Governance Approach
- Summary

The world is riskier than it used to be…

Massive insider breach at DuPont
February 15, 2007
By: Larry Greeenemeier

TJX data breach: At 45.6M card numbers, it's the biggest ever
March 29, 2007
By: Jaikumar Vijayan

COMPUTERWORLD

Black Friday Turns Servers Dark at Walmart, Macy's
November 25, 2006
By: Evan Schuman

eWEEK

Blackberry outage widespread
February 14, 2007
By Marcia Walton

CNN

Bill would punish retailers for leaks of personal data
February 22, 2007
By Joseph Pereira

THE WALL STREET JOURNAL.

What is at risk?

- Your Brand
- Intellectual Property
- Legal and Regulatory Exposures
- Your Customer Information
- Customer Confidence
- Cost of Remediation
- Business Disruption
- Your Job

Business Challenges

Acquisitions and mergers

Cyber Fraud

Need to streamline linkages with partners and suppliers

Privileged User Audit

Security Audit and Compliance Requirements (PCI, SOX, etc.)

Legacy system integration

New standards and regulations

Need for a consolidated view of information and applications

More demands for personalized service

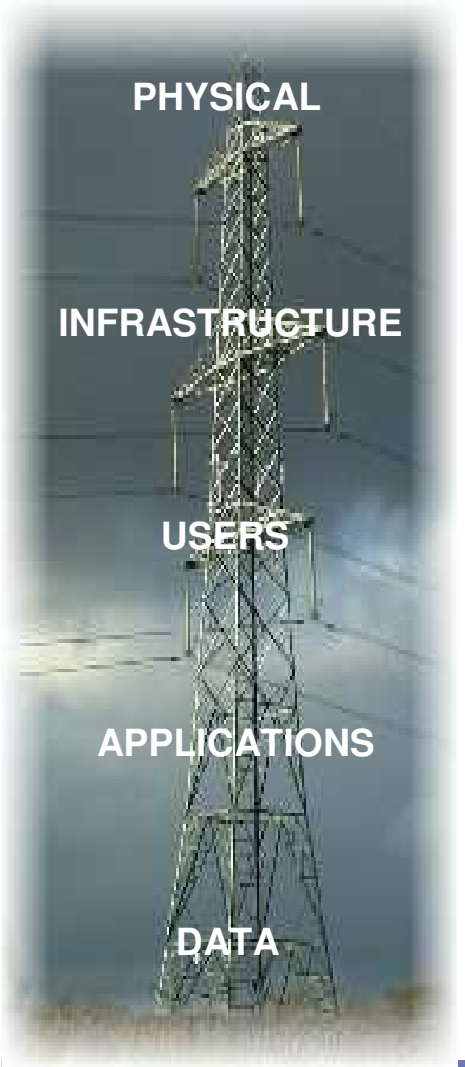
Protect security and privacy of critical assets

Improve operational efficiency – manage costs

Seamless access to infrastructure – anytime/anyplace

Increasing volume of data

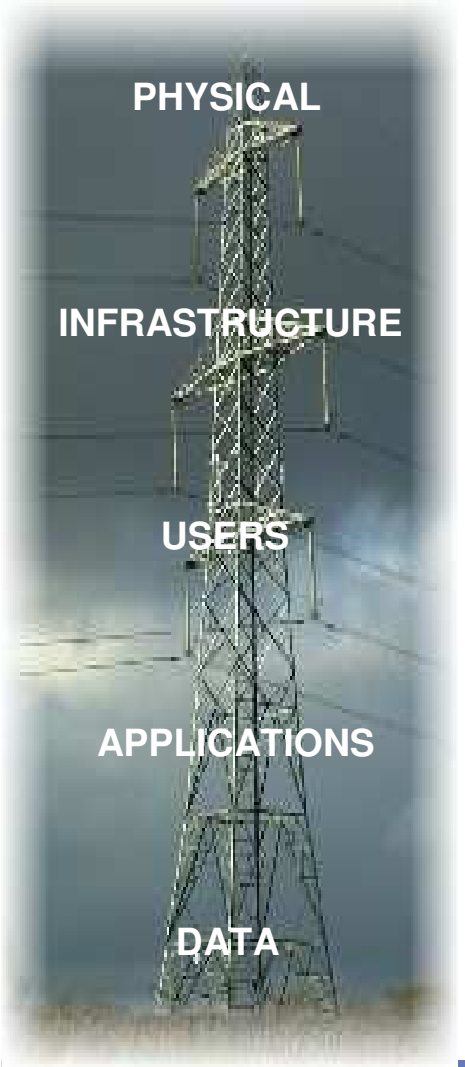
Business Challenges – The Simple View



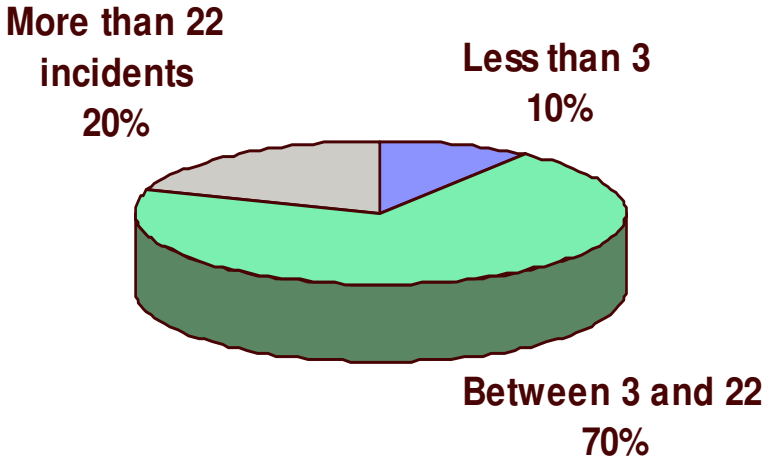
1. Can I protect against internal and external security threats? (IT Security)

2. Can I protect my business initiatives? (Line of Business)
   - Who can come in?
   - What can they do?
   - Can I easily prove it to an auditor?

The Simple Answer is Typically “No, I Can’t”



Disclosures of Sensitive Business Data
(IT Policy Compliance Group, 2007)



The *Unknown People* Threat:

Jay Echouafni

Competitive DDoS

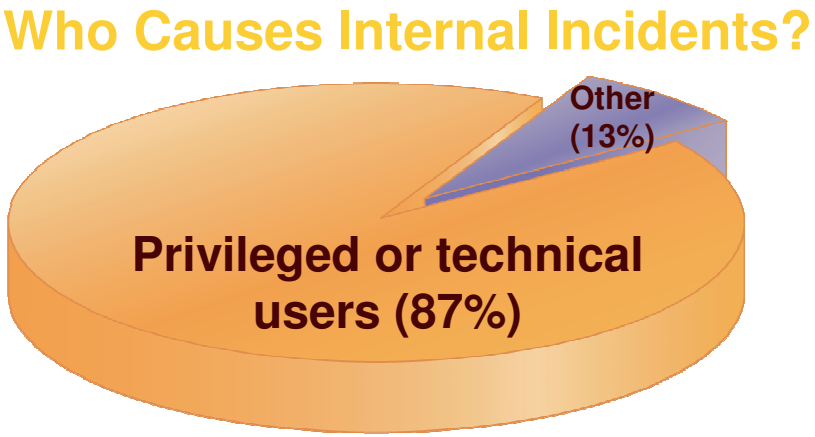
Andrew Schwarmkoff

Russian Mob Phisher

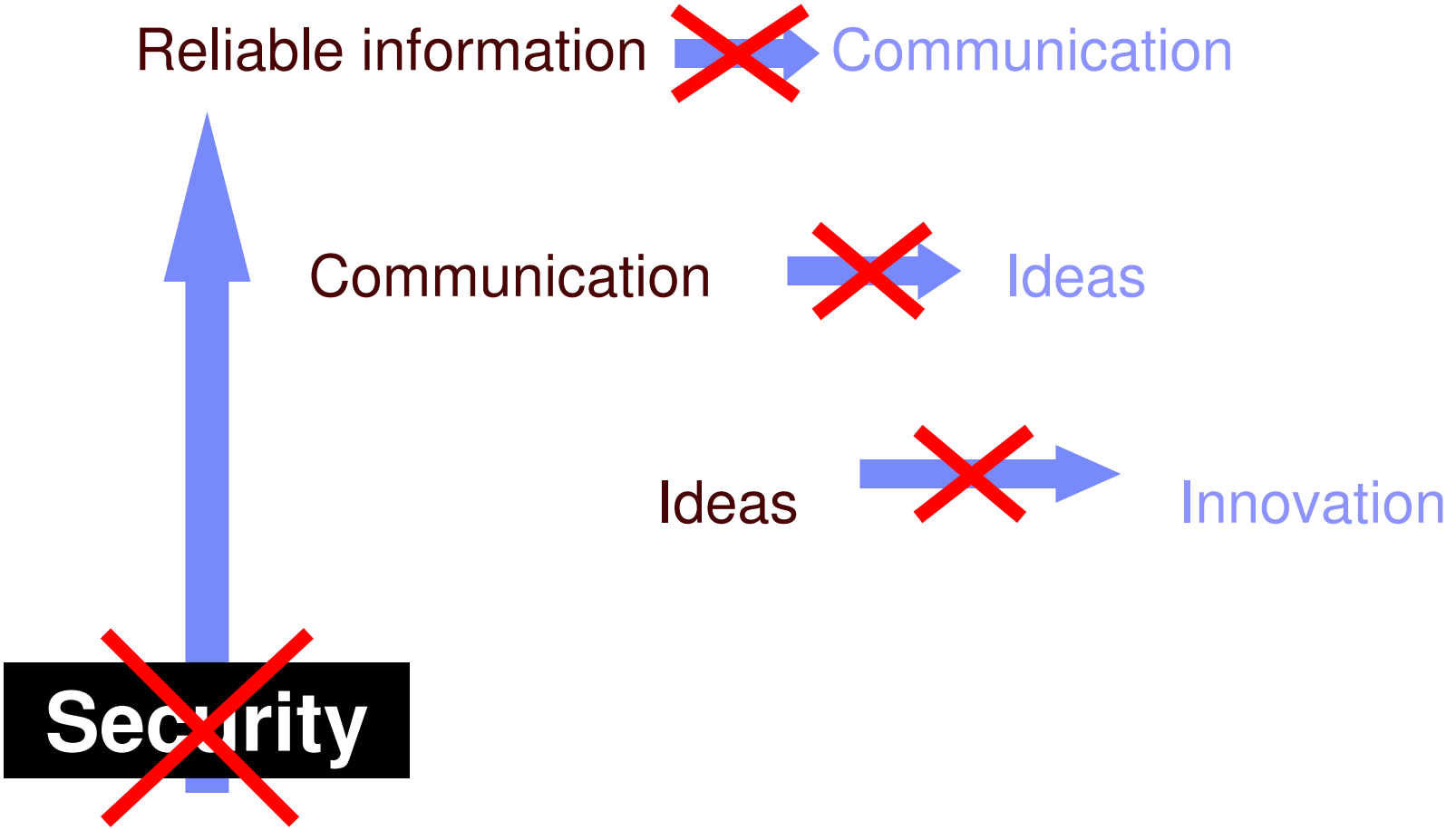
Photos from colleagues at F-Secure

Known people (un) intentionally cause great harm

- **Many are inadvertent violations of:**
  - Change management process
  - Acceptable use policy
- **Others are deliberate, due to:**
  - Revenge (84%)
  - “Negative events” (92%)
- **Regardless, too costly to ignore:**
  - Internal attacks cost 6% of gross annual revenue
  - Costing $400 billion in the US alone



Security assures delivery of reliable information



Security protects against possible liability

- Negligence is defined as the failure assert a due care (level of care that a reasonable person would have used under similar circumstance)
- Leaders who make their decisions with due care may receive protection
- Taking action to protect critical information assets is a way for leaders to demonstrate that they are acting in a reasonable manner.

Security assures customer confidence

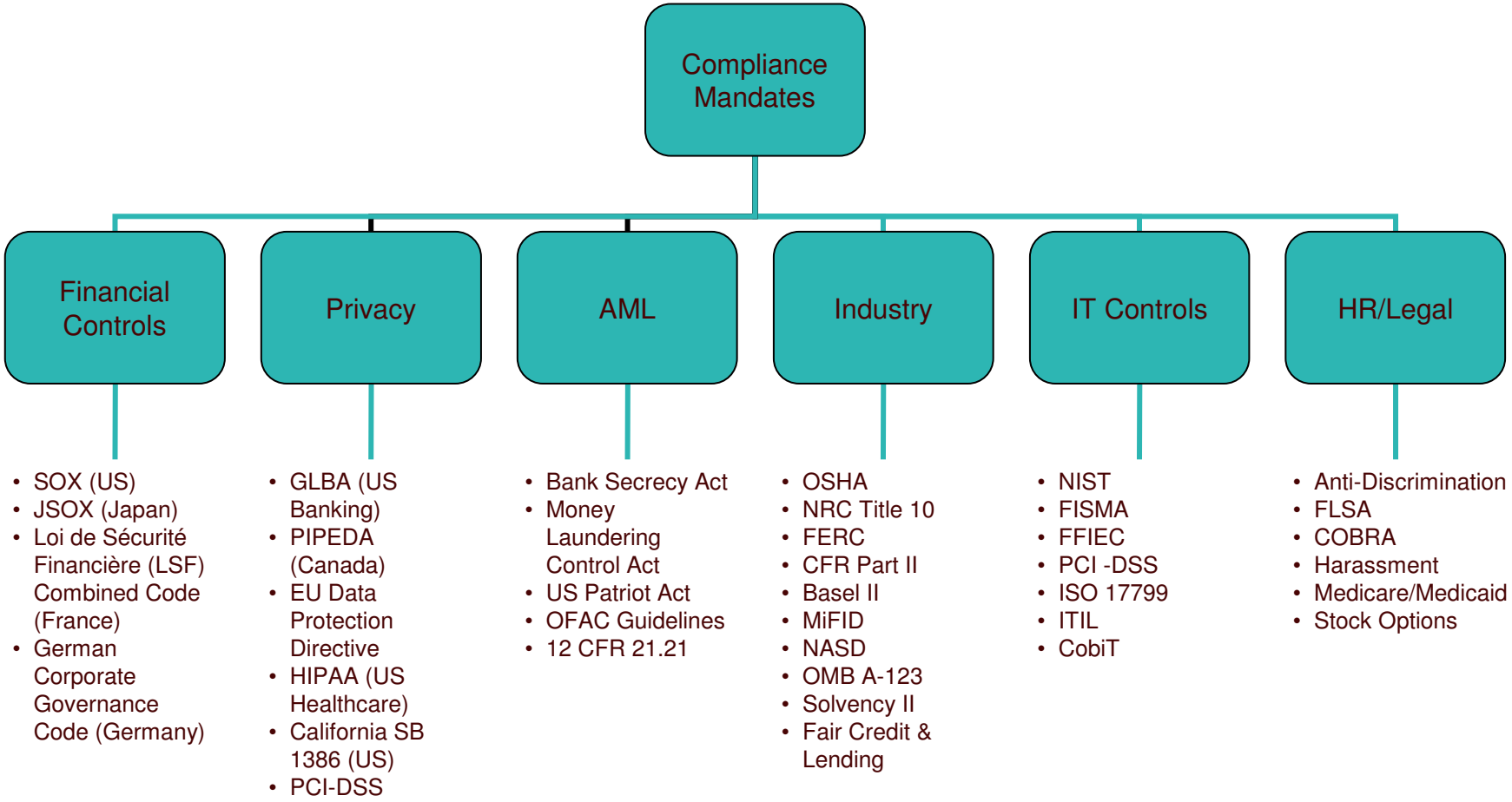
- 44% of respondents feel their information is safe when engaging in e-commerce.
- 50% avoid making purchases online because they are afraid their financial information will be stolen.
- 94% say identity theft is a serious problem.
- Only 24% say businesses are placing the right emphasis on protecting information systems and networks.

Source: Cyber Security Industry Alliance survey of consumers, 2007

1. Data security
2. Global Warming
3. Terrorism
4. Job loss
5. Disease or epidemics
6. Natural disasters

Assure brand position with recognition of trusted partner and trusted provider status

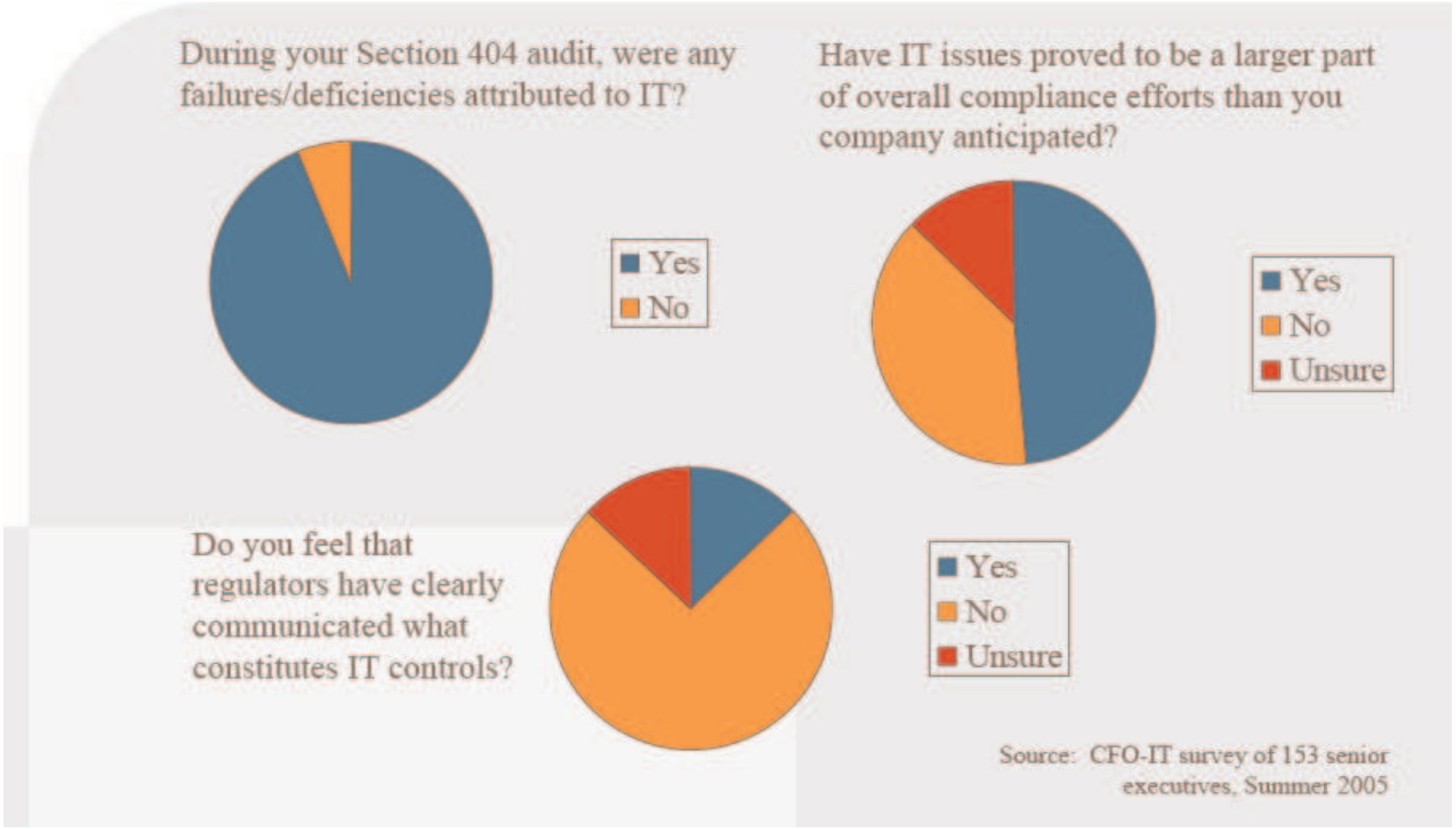
Security enables compliance



Putting Compliance into context… (for example, with Sarbanes-Oxley (SOX))

Prison Time	Offense
1 - 2 years	Escaping from prison
3 - 5 years	Kidnapping involving Ransom
10 - 20 years	**Fraudulent SOX Certification**
11 - 14 years	Second Degree Murder
20 - 25 years	Hijacking

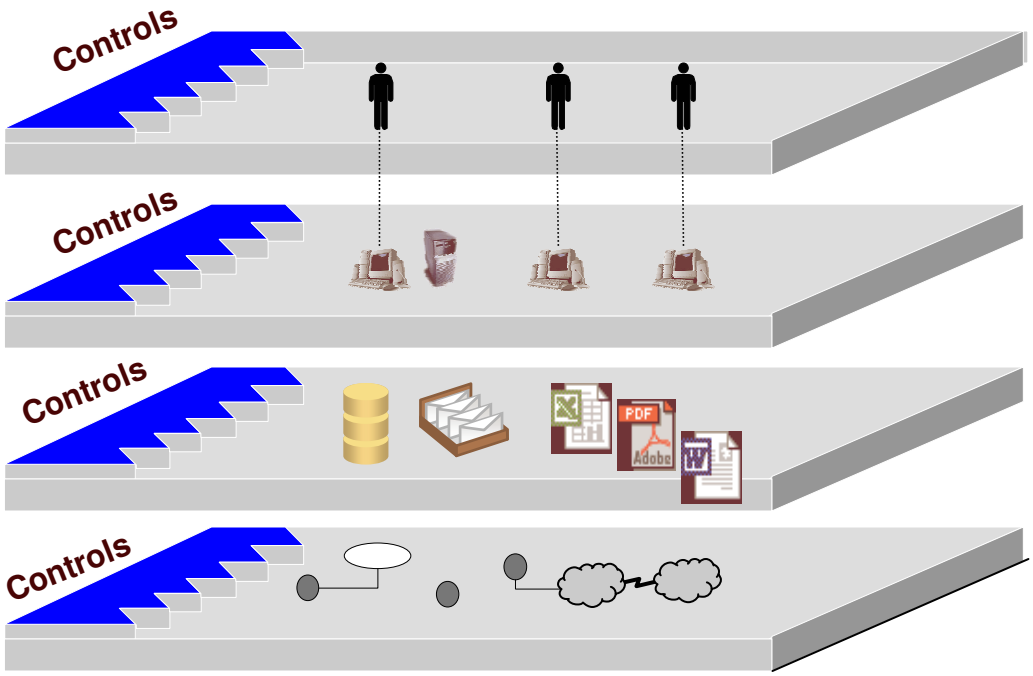
The extent to which IT control deficiencies have been identified has come as a surprise



In Sum: Security offers tangible benefits

~~Security~~ ⟷ ~~Trust~~ ⟷ ~~Business~~

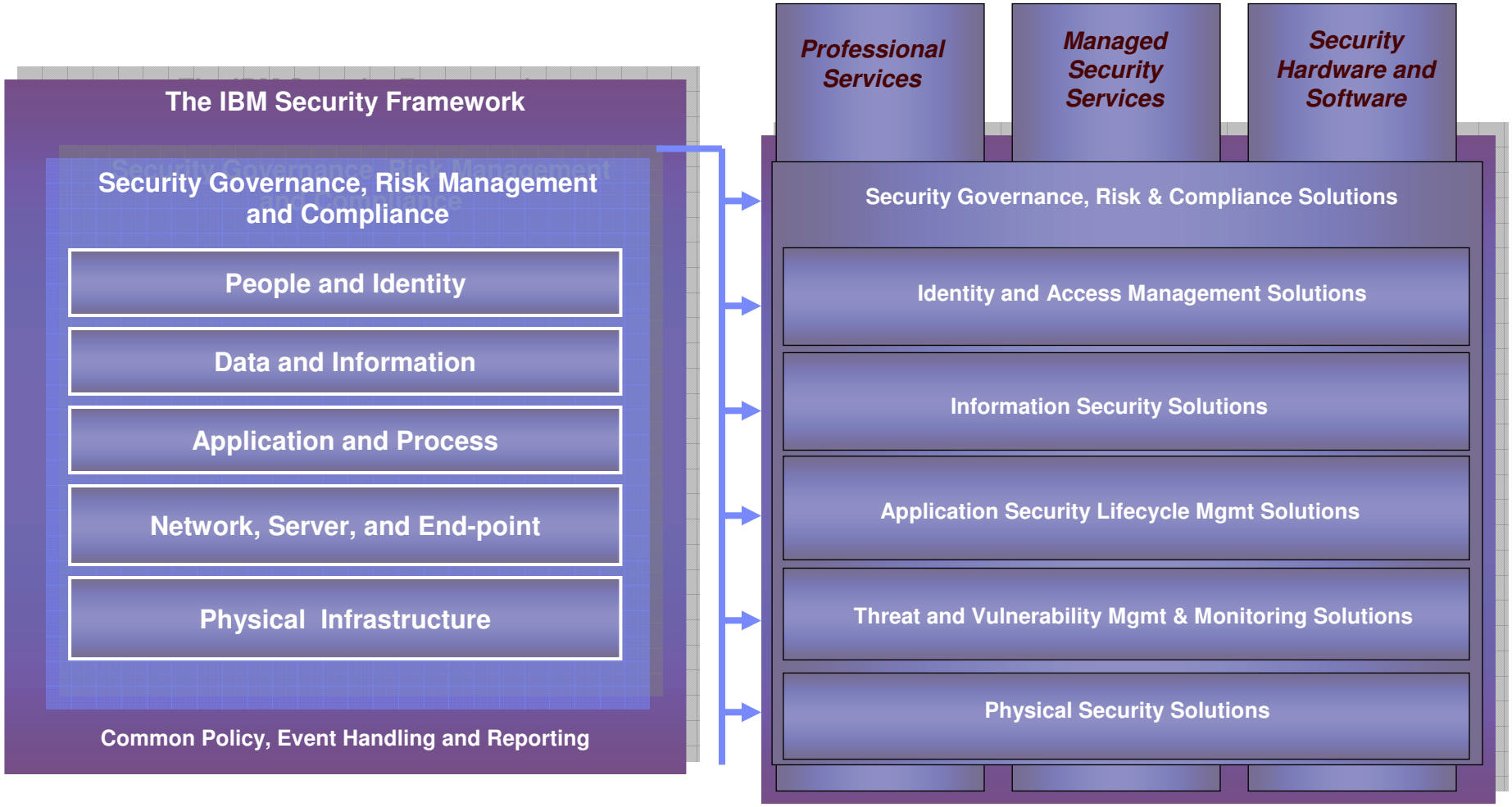
IBM's Security Governance Approach:
Designed to offer visibility, control and automation



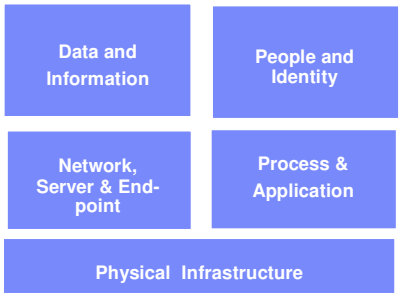
Effective Governance and Assurance

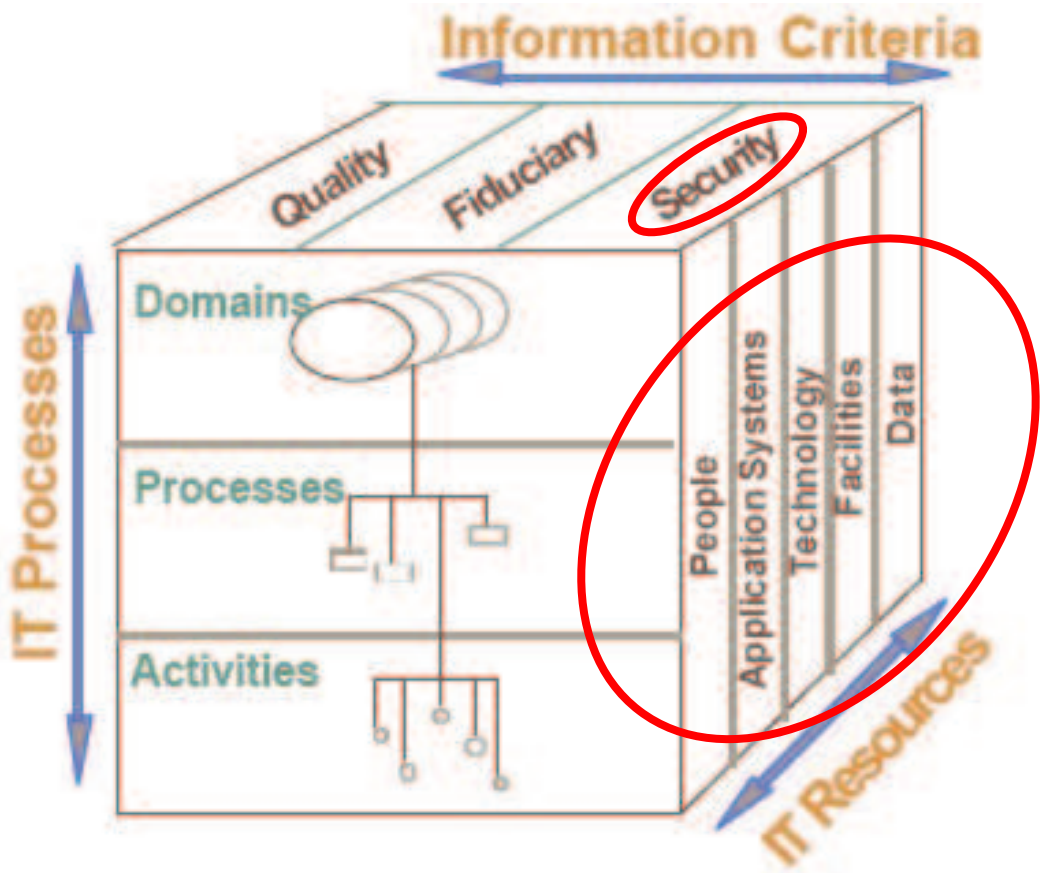
People	The right people have access to the right assets at the right time
Process	Policy and process is repeatable, measurable and effective
Information	Collaboration is enabled while data protected at rest, in motion, in use and at the endpoint
Technology	IT application and infrastructure integrity, availability and continuity is assured

IBM Security Framework



Why five IT security domains?

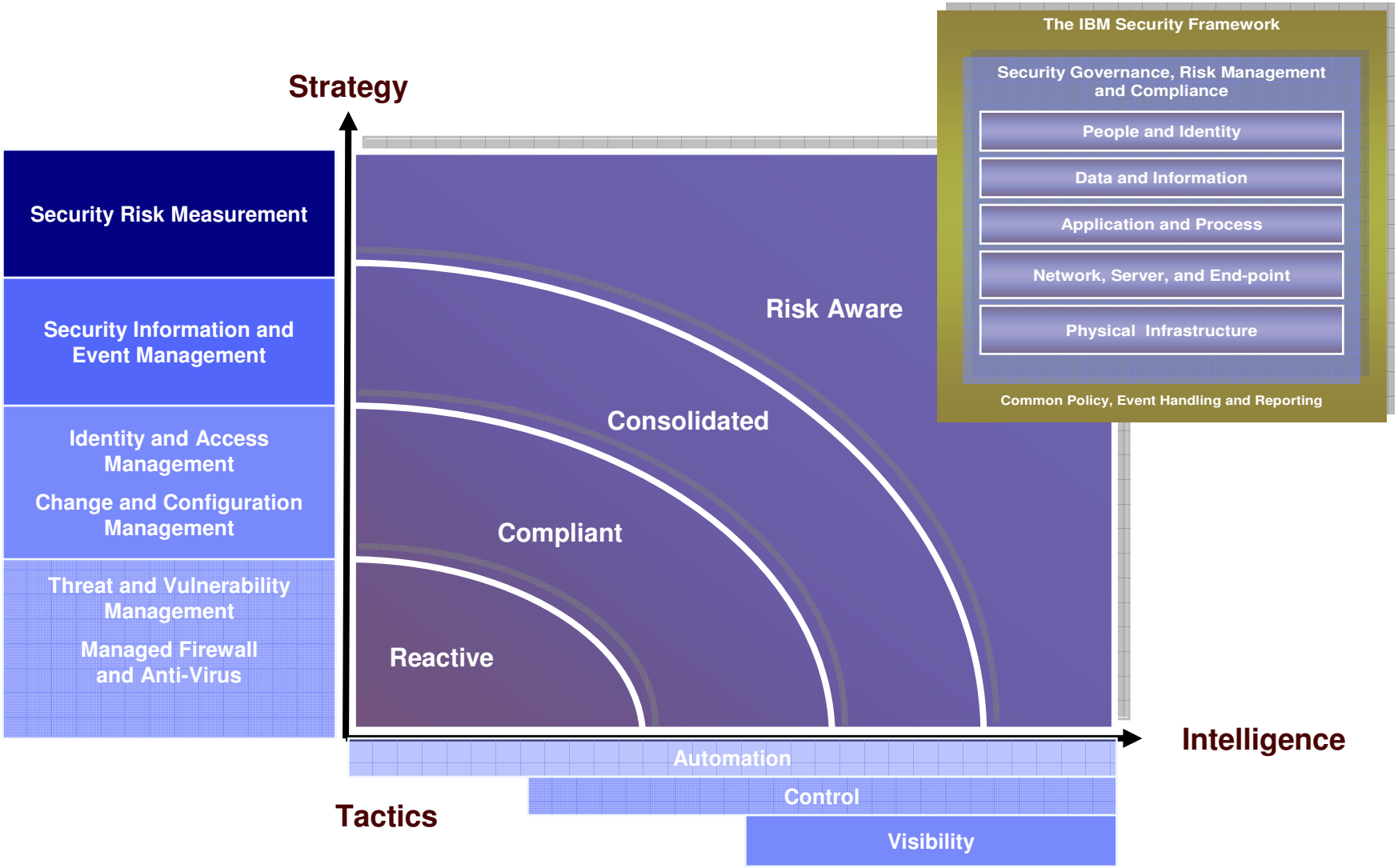




5 domains align with CobiT IT Resources

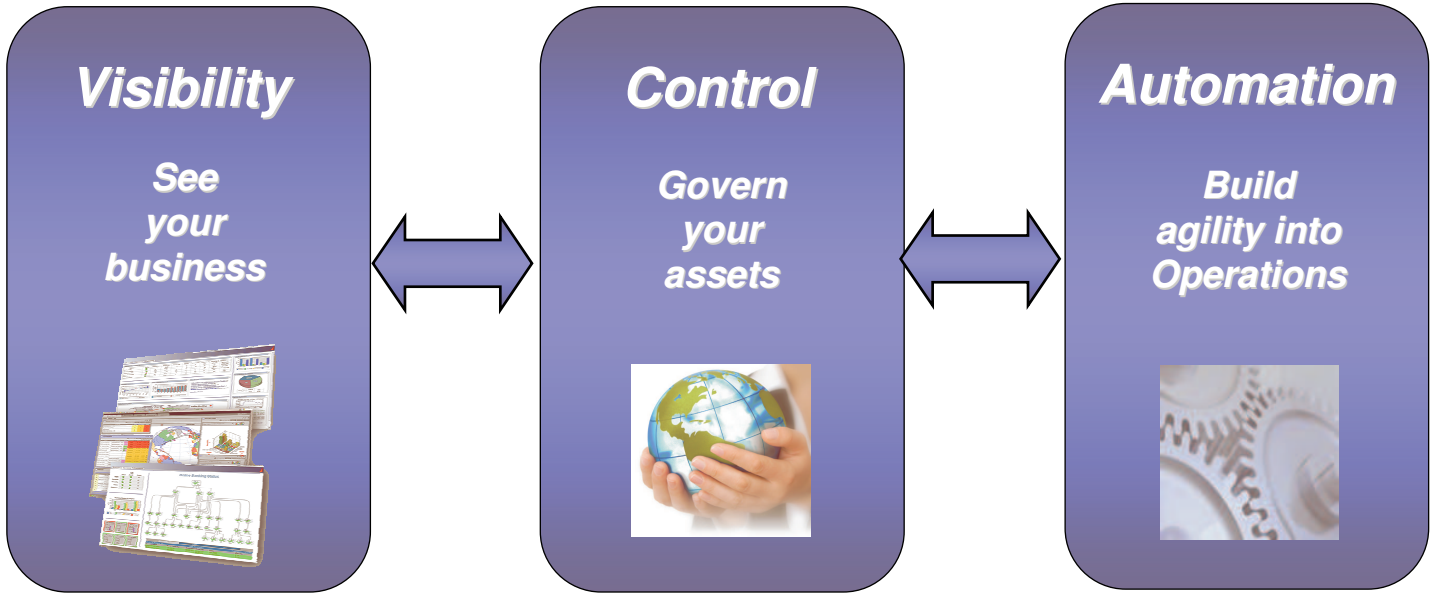
The IBM Security Framework

From Reactive Security to a Risk-Aware Enterprise



IBM Service Management

Security Addresses Top Innovation Inhibitors



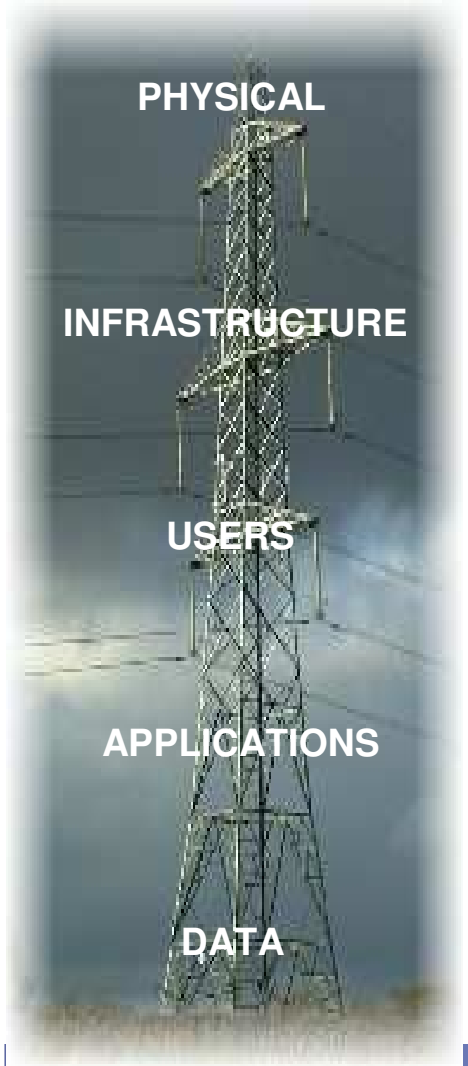
e.g. Sensitive Data Disclosure Monitoring, Alerting and Reporting

e.g. Consistent Processes for User Access to Business Applications

e.g. Automated Processes for User Account Setup, Revalidation and Removal

Major financial services firm centrally monitors and automatically generates auditor-quality SOX reports around sensitive data disclosure	Influential mutual fund company manages access to 400 applications from one policy engine, saving $24M in application development costs and ongoing administrative cost savings.	Leading retailer reduces time to setup new employee access to internal systems from 15 business days to 20 minutes (on average).

Case Studies



Service Availability

Major 401K plan provider shortens time to securely onboard and integrate new corporate clients from weeks-to-months to 3 days while centrally protecting access to critical corporate data by deploying federated identity management solution

Fast-growing county government in United States delivers real-time detection and reaction to emerging threats across 7,400 node network by deploying security information and event management solution

International energy firm reduces time to on-board new employees and partners across world-wide operations from 5 days to 10 minutes on average by deploying identity management solution for user provisioning

Operational Efficiencies

Financial services firm reduces help desk calls for password resets by 61% after deploying single sign-on technology

State government reduces help desk costs by $900,000 per year after deploying single sign-on technology, despite 5X growth in traffic

International service provider cuts out 30% of costs for help desk password management after implementing self-service password reset capability, resulting in an annual savings of at least $450,000

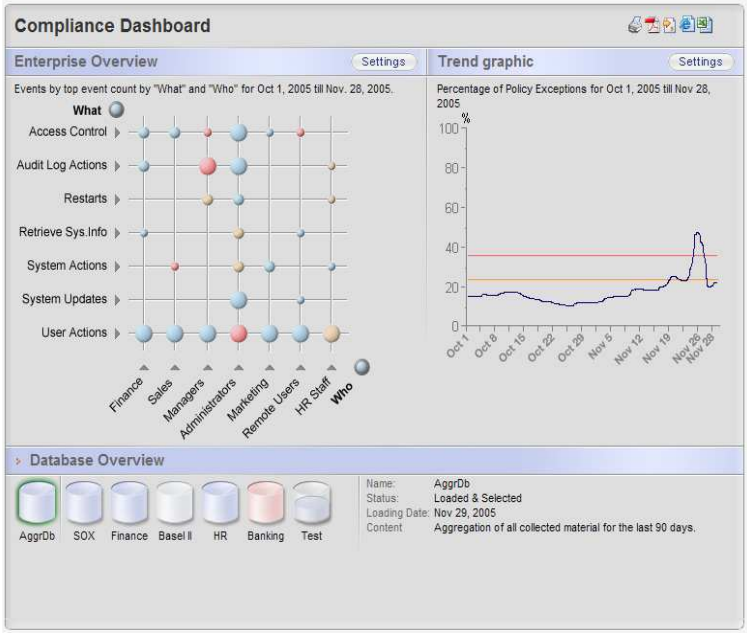
Influential mutual fund company manages access to 400 applications from one policy engine, saving $24M in application development costs and ongoing administrative cost savings.

IBM Security: Sum is greater than its parts

FORRESTER®		Wave: User Account Provisioning (TIM)	Leader
FORRESTER®		Wave: Enterprise Security Information Management (Consul InSight)	Leader
Gartner		MQ: User Provisioning (TIM)	Leader
Gartner		MQ: Web Access Management (TAM)	Leader
Gartner		MQ: Security Information & Event Management (TSOM, Consul InSight)	Challenger
Gartner		ISS Network Security, Firewalls and Managed Services	Leader
Gartner	#1	Marketshare: Web Access Management, Worldwide, 2005 (FIM, TAM)	Ranked #1
Gartner	#1	Marketshare : Application Security Vulnerability Scanning, 2006 (Rational AppScan)	Ranked #1
FROST & SULLIVAN	#1	Identity Management (TIM , TAM, FIM, TDI, TDS)	Ranked #1
FROST & SULLIVAN	#1	Managed Security Services (Marketshare)	Ranked #1
IDC Analyze the Future	#1	Marketshare: Identity and Access Management	Ranked #1
IDC Analyze the Future	#1	Marketshare: Application Vulnerability Assessment (Rational AppScan)	Ranked #1

Emerging Trend: Policy Visibility

- The days of “everybody has to choose the same access control engine” for cross-firm collaboration and integration are long gone
  - How can we define security policy centrally based on standards (e.g. with WS-SecurityPolicy and XACML) and push it to the enforcement points?
  - How can we effectively ensure compliance with access policy at the points of enforcement?
- **Solution:** Policy definition & provisioning, and policy audit
- Benefit: Effective deployment of security policy



Emerging Trend: Identity Protection

- How do we apply risk management as individuals, given identity is valuable, consequential, contextual and dynamic?

- How to give ourselves a say in how much risk we're willing to have with respect to our identity data, which is potentially shared across so many 'consumers'?

- **Solution**: user-controlled identity as a service
  - Like Federated Single Sign-On (FSSO), but not really – user has ultimate control as personal identity broker
  - e.g. CardSpace and Higgins (wire compatible with CardSpace but supports more protocol providers such as OpenID and HTML forms, etc.)
- Benefit: not only allows us to implement our own individual risk management preferences, but lowers risks for service providers because they don't have to store as much detailed information about us, since iCard provides needed info each time (think PCI etc.)

Summary

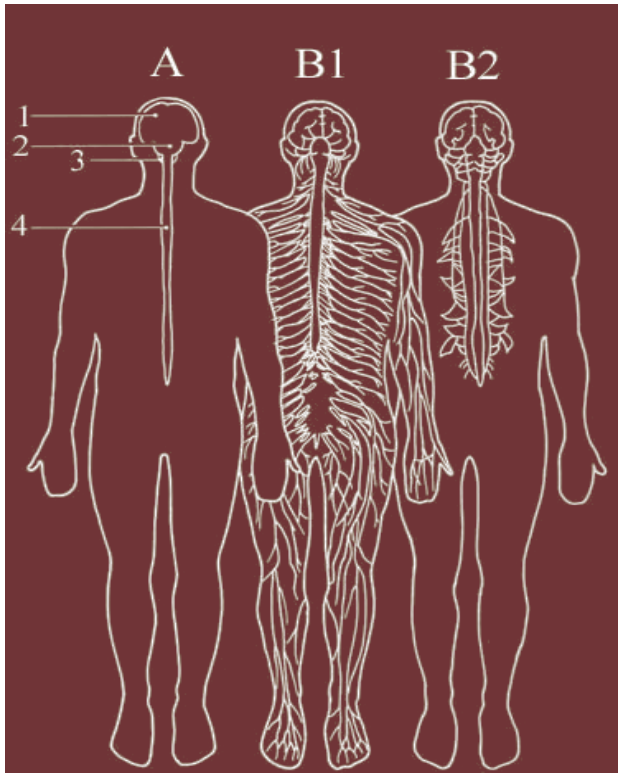
Breadth and Depth of Solution	Only vendor that delivers breadth of security and compliance capabilities to address infrastructure, applications, information, people and identities
Extensive Integration	Integrates with all types of business data (structured, semi-structured, and unstructured) for addressing information & data security needs and all major application types (web, legacy, and ESB for SOA) for securing business process
Open Standards	Open security platform and leadership in Web Services security, policy management and federated identity
Product Leadership	Analyst attested leadership in markets for user and infrastructure security and compliance software and services.
Best in class System z security	Leadership in mainframe security with RACF, zOS security, identity & access and compliance enabling clients to leverage System z as the enterprise security hub
A core element of IBM Service Management	Security integration with key ITIL processes out of the box: Incident, Problem, Change, Release, SLA, Configuration, Availability.
Breadth of Service Management offering	IBM offers full breadth of end-to-end asset and service management solutions that operate on a common web services infrastructure.

Security assures ability to transact businesses

Enable new and improved types of products and services

Enable new types of staff, customer or supplier interaction

Conduct secure transactions, ensuring customer and partner confidence and satisfaction



Common IT control deficiencies derived from SOX filings

- Improper Change Management
  - Lack of formal program change procedure
  - Lack of understanding of system configurations
  - Oversight of changes and review of change logs
- Insufficient Segregation of Duties
  - Separation of requestor, approver, implementer
  - Separation of developers and operators
- Lack of Self Assessment
  - Late implementation of controls
  - Failure to identify abnormal application transactions
  - Failure to consider automated controls
  - Ongoing testing program

Common IT control deficiencies derived from SOX filings

- Excessive Access to Systems / Databases
  - Developer / programmer access to production environment
  - Developer / programmer access to production data
  - DBA access
  - System Administrator access
- Lack of Access Controls
  - User provisioning and administration
    - Changes in responsibilities
    - Changes in organization
    - Terminations
- No documented access policies and standards
- General monitoring of the security infrastructure

Security Governance Benefits: Performance, Resilience, *Compliance*

- Ensure sustainable compliance with growing number of regulations and private sector requirements
- Enable new services and business models
- Improve existing processes
- Decreasing cost ongoing operations
- Allow effective, requirements-based collaboration among employees, partners, and customers
- Deal with increasing complexity of security

43% of CFOs think that improving governance, controls and risk management is their top challenge.

CFO Survey: Current state & future direction,
IBM Business Consulting Services

Security assures shareholder confidence

- Accurate reporting of the returns, effectiveness, and productivity of the enterprise
- Availability and reliability of services
- Demonstrated due diligence with respect to protecting against malicious attacks (internal and external) and accidents that can be anticipated
- Ensuring only authorized access to enterprise information

The positive perspective on compliance, based on recent surveys conducted by Compliance Week and CFO Magazine

- Investors are gaining increased comfort with information available to the capital markets, in other words, “confidence in the numbers”.
- Senior managers and boards of directors are more confident in the reliability of the financial reports on which they sign off.
- Business processes have been streamlined and improved.
- Control Assessments have been centralized, with responsibility moving to a newly designated “chief internal control officer.”
- More effective audit committees, codes of conduct and whistleblower channels.