IBM

What makes you special?

IT Governance and Compliance Solutions for System Management

IBM Governance and Risk Management

Business alignment, visibility and control

Agenda

- Compliance
- Audit Management
- Risk Management & IT Governance
- IBM Customers' Stories
- Summary

CIO's Top Priorities Are to Deliver

Business Agility/Innovation While Retaining a Resilient Business

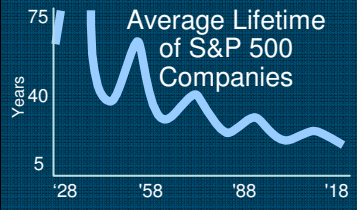
Complexity

Increased complexity makes change much harder

Compliance

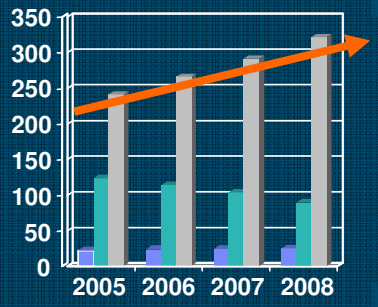
Changing regulatory environment requires security, privacy and ongoing audit capabilities

Change



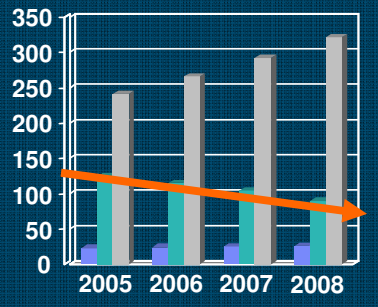
Increased competitive pressure while IT has an increasing role in every business process

Rising Cost of Operations



The cost of operations continues to increase at 10% CAGR … twice the rate of the IT budget

Inability to Innovate



Increased focus on development project spend due to higher % of costs going to keeping the lights on … creates a dual focus of doing the right thing and doing things well

What is Compliance?

- Compliance
  - Acting according to certain accepted standards
    - Princeton University WordNet
      http://wordnet.princeton.edu/perl/webwn?s=compliance
- Regulatory Compliance
  - The combined set of organizational capabilities, processes, supporting infrastructure and tools, data and information, and operational and financial controls required to satisfy the requirements set forth by all applicable regulatory agencies

Key Regulations Affecting IT and Compliance

Privacy Regulations

- 1999 Gramm-Leach-Bliley Act (GLBA) US
- 2000 PIPEDA Canada
- 2000 COPPA and CIPA US
- 2003 California Individual Privacy (SB1386) California
- 2006 **PCI DSS** v1.1 Industry
- 1987 Computer Security Act US
- 1995 EU Data Protection Directive EU
- 1996 **HIPAA** US
- 1997 Personal Health Information Act Canada
- 1998 Data Protection Act UK

Financial Integrity and Solvency Regulations

- 2005 8th Company Law Directive (Euro SOX) EU
- 2006 Financial Instruments and Exchange Law (J-SOX) Japan
- 2012 Solvency II EU
- 2002 **Sarbanes-Oxley** Act US
- 2002 Corporate Law Economic Reform Program Australia
- 2003 Basel II EU

Other Regulations

- 2006 **Federal Rules of Evidence** US
- 2001 USA PATRIOT Act US

Consequences for lack of compliance

- Financial Risk
  - Merchant banks may pass on substantial fines
  - Up to $500,000 per incident from Visa alone
  - Civil liability and cost of providing ID theft protection

- Compliance Risk
  - Exposure to Level 1 validation requirements
- Operational Risk
  - Visa-imposed operational restrictions
  - Potential loss of card processing privileges

Common Compliance Problem Areas

- Lack of encryption for emails and messaging
- Lack of encryption for data at rest
- Lack of knowledge where all the data is at rest
- Lack of segregation of duties
- Lack of adequate access controls (generic, default and shared IDs)
- Lack of network segregation
- Back end operation networks often break the isolation of PCI networks
- Too many firewall rules with no business justification
- Insufficient documented policies and procedures
- Un-patched systems
- Storing sensitive magnetic stripe data

Gartner

Recent Gartner Findings on PCI Compliance

- Cost comparison
  - Data Breaches ~ $300/user
  - Data Protection ~ $16/user
  - It's cheaper to do the right thing!

- Encryption is key but if you can't encrypt data at rest, consider the following compensatory controls:
  - Narrow segmentation of cardholder data surrounded by strong access controls
    - Identity and Access Management
  - Database activity monitoring
    - Security Information and Event Management
  - Outsourcing
    - Managed Security Services

Source: "Data Breaches and PCI Compliance — Which Costs More?" Gartner Compliance & Risk Management Summit, Avivah Litan, May 2007

PCI DSS Requirements "The Digital Dozen"

Build and Maintain a Secure Network	
1.	Install and maintain a firewall configuration to protect cardholder data
2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	
3.	Protect stored cardholder data
4.	Encrypt transmission of cardholder data sent across open, public networks
Maintain a Vulnerability Management Program	
5.	Use and regularly update anti-virus software
6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	
7.	Restrict access to cardholder data by business need-to-know
8.	Assign a unique ID to each person with computer access
9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	
10.	Track and monitor all access to network resources and cardholder data
11.	Regularly test security systems and processes
Maintain an Information Security Policy	
12.	Maintain a policy that addresses information security – Connected Entities and Contracts

Being out of compliance

InfoWorld
HOME | NEWS | TEST CENTER | OPINIONS

Lawsuit filed over CardSystems data breach

Class action suit says company was negligent in maintaining consumer credit data

By Robert McMillan, IDG News Service
June 28, 2005

SAN FRANCISCO - A class action lawsuit has been filed in California over the CardSystems Solutions security breach, which may have exposed as many as 40 million credit-card numbers to fraud.

The New York Times

68,000 MasterCard Accounts Are at High Risk in Breach

By ERIC DASH (NYT) 489 words
Late Edition - Final , Section 1 , Page 22 , Column 1

The New York Times

CardSystems Sets Plan to Comply With Security Standards

By ERIC DASH (NYT) 537 words
Late Edition - Final , Section C , Page 4 , Column 3

The Register

Visa cuts CardSystems over security breach

By John Leyden (john.leyden at theregister.co.uk)
Published Tuesday 19th July 2005 16:33 GMT

Visa USA has dumped a card processing firm blamed for a security breach affecting anything up to 40m credit card numbers from MasterCard, Visa and card issuers.

c|net NEWS.COM
TECH NEWS FIRST

FRONT PAGE | ENTERPRISE SOFTWARE | ENTERPRISE HARDWARE | SECURITY

CardSystems says it faces 'imminent extinction'

REUTERS

Published: July 22, 2005, 5:44 AM PDT

U.S. payment-processing company CardSystems Solutions said Thursday it faces "imminent extinction" after revealing last month a massive credit card data security breach.

Card Systems Solutions

- May 2005
- 40 Million Account Numbers Accessed
  - Card Systems was a third-party processor of payment data
  - Its primary customers were Card Associations and FIs

  - Routinely handled account and transaction data
  - The network in the Tuscon, AZ office was hacked
  - FBI notified
  - Consumers subsequently notified according to state data breach notification laws

What Happened ??

- Common vulnerability exploited
  - A hacker accessed a central database
    - Installed a script that captured transaction data
  - According to MasterCard:
    - MC fraud monitoring systems detected a large amount of fraudulent activity for a number of card holders
    - Working with a member bank, began forensic investigation
    - The trail led directly to Card Systems
  - According to Card Systems:
    - CS IDS system detected an intruder on May 22
    - On May 23, CS contacted the FBI
    - With the approval of law enforcement, VISA, MasterCard, and other organizations were subsequently notified
  - Data Exposed
    - 20 million VISA-branded cards
    - 13.9 million MasterCard-branded cards
    - American Express, Discover, JBC, etc. affected
    - Major financial institutions issuing branded cards impacted

What does PCI say?

- In General: Build and Maintain a Secure Network, Protect Cardholder Data and …
- Requirement 3: Protect stored cardholder data
  - . . . methods for minimizing risk include not storing cardholder data unless absolutely necessary . . .
  - 3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.
  - 3.2 Do not store sensitive authentication data subsequent to authorization (even if encrypted).
  - 3.2.1 Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.
- Requirement 6: Develop and maintain secure systems and applications
  - Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses.
  - 6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.
  - 6.3 Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.

Card Systems' Common Problems??

- Lack of encryption for emails and messaging
- Lack of encryption for data at rest
- Lack of knowledge where all the data is at rest
- Lack of segregation of duties
- Lack of adequate access controls (generic, default and shared IDs)
- Lack of network segregation
- Back end operation networks often break the isolation of PCI networks
- Too many firewall rules with no business justification
- Insufficient documented policies and procedures
- Un-patched systems
- Storing sensitive magnetic stripe data

One other example: Chipotle Mexican Grill

- August 2004
  - Theft of patrons' credit card numbers added up to 2000+ incidents of fraud
  - Chipotle was liable for $1.4 million
  - Discovered that software was retaining Track 2 data, and Internet gateways were not secured
  - To correct situation
    - Fixed software problems
    - Set aside $4 million to cover liabilities
      - Fraudulent charges
      - Card replacement
      - Monitoring expenses
      - Card association fines

Chipotle's Common Problems??

- Lack of encryption for emails and messaging
- Lack of encryption for data at rest
- Lack of knowledge where all the data is at rest
- Lack of segregation of duties
- Lack of adequate access controls (generic, default and shared IDs)
- Lack of network segregation
- Back end operation networks often break the isolation of PCI networks
- Too many firewall rules with no business justification
- Insufficient documented policies and procedures
- Un-patched systems
- Storing sensitive magnetic stripe data

Agenda

- Compliance
- Audit Management
- Risk Management & IT Governance
- IBM Customers' Stories
- Summary

What is Audit Management?

- Audit
  - **An evaluation of a person, organization, system, process, project or product.**
    - Wikipedia
- Audit Management
  - **Oversees the internal audit staff, establishes internal audit programs, identify inherent risks of the business and assess the overall effectiveness of controls in place relating to the company's information technology operations.**

Where Organizations Fail Audits

PCI Requirement	% Failure
Requirement 3: Protect stored data.	79%
Requirement 11: Regularly test security systems and processes.	74%
Requirement 8: Assign a unique ID to each person with computer access.	71%
Requirement 10: Track and monitor all access to network resources and cardholder data.	71%
Requirement 1: Install and maintain a firewall configuration to protect data.	66%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.	62%
Requirement 12: Maintain a policy that addresses information security.	60%
Requirement 9: Restrict physical access to cardholder data.	59%
Requirement 6: Develop and maintain secure systems and applications.	56%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.	45%

Source: VeriSign sample of 112 assessments, where 30 ultimately passed and 82 did not

Questions auditors might ask:

RACF	z/OS Communications Server	Data and Network Encryption Options	Tivoli zSecure suite	DB2 Audit Management Expert	Tivoli Compliance Insight Manager	Tivoli Identity Manager	Tivoli Federated Identity Mgr
How do you prevent unauthorized access?	*Do you know if anyone attempted an attack on the mainframe?*	*How do you know your private customer data is encrypted?*	*Do you know if administrators are abusing privileges?*	*Can your DB2 auditors get at the information they need?*	*Are you reporting consistently across the enterprise?*	*How do you know only authorized users are given user accounts?*	*How do you protect your Web services applications?*

Platform Infrastructure ⟷ **Data Privacy** ⟷ **Compliance and Audit** ⟷ **Extended Enterprise**

*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business.

Agenda

- Compliance
- Audit Management
- Risk Management & IT Governance
- IBM Customers' Stories
- Summary

What is Risk Management?

- Risk Management
  - is the human activity which integrates recognition of risk, risk assessment, developing strategies to manage it, and mitigation of risk using managerial resources.
    - Wikipedia
- Risk Management Strategies
  - Transferring the risk to another party
  - Avoiding the risk
  - Reducing the negative effect of the risk
  - Accepting some or all of the consequences of a particular risk.
    - Wikipedia

Common Denominator: Risk Management

- Regulatory compliance initiatives involve reducing the risk of adverse events
  - Sarbanes Oxley compliance initiatives require reducing the risk that the financial reporting processes, systems and data lack integrity and accuracy
  - PCI Data Security Standard compliance initiatives require reducing the risk that cardholder data will be subject to inappropriate access or theft
- Common steps for Risk Management cross many regulations
  - Evaluation of control environment
  - Risk assessment
  - Control testing
  - Remediation
  - Ongoing Monitoring

What is IT Governance?

- Governance
  - Specifying the decision rights and accountability framework to encourage desirable behavior
    - Weill and Ross
- IT Governance
  - The process of overseeing and organizing IT and IT resources, in pursuit of an enterprise's mission and goals, in an effort both to deliver corporate value and mitigate corporate risk.
  - A mechanism, put in place to ensure compliance with the rules and regulations by which an IT Department operates.
- Data Governance
  - The people, processes and procedures required to create a consistent, enterprise view of an organization's data in order to:
    - Increase consistency & confidence in decision making
    - Decrease the risk of regulatory fines
    - Improve data security
    - Maximize the income generation potential of data

CIOs with effective IT governance and risk management…

Enhance business performance

- *Maintain visibility of end to end service to help ensure service quality*
- *Improve time to value and manage costs of strategic initiatives*

Improve business resilience

- *Reduce risks and protect confidential intellectual property*
- *Minimize and control impact of planned and unplanned disruptions*

Achieve compliance

- *Create alignment with internal and external policies and regulations*
- *Effectively prioritize and get more value from IT investments*


HOME PAGE | MY TIMES | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS

The New York Times
Get Home Delivery

Washington

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

POLITICS | WASHINGTON | EDUCATION

PROTECT OUR FOREST FRIENDS.

Ad Council

In Turnaround, Industries Seek U.S. Regulations

By ERIC LIPTON and GARDINER HARRIS
Published: September 16, 2007

SIGN IN TO E-MAIL OR SAVE THIS
PRINT
SINGLE PAGE
REPRINTS
SHARE

ARTICLE TOOLS SPONSORED BY once In Theatres Now

WASHINGTON, Sept. 15 — After years of favoring the hands-off doctrine of the Bush administration, some of the nation's biggest industries are pushing for something they have long resisted: new federal regulations.

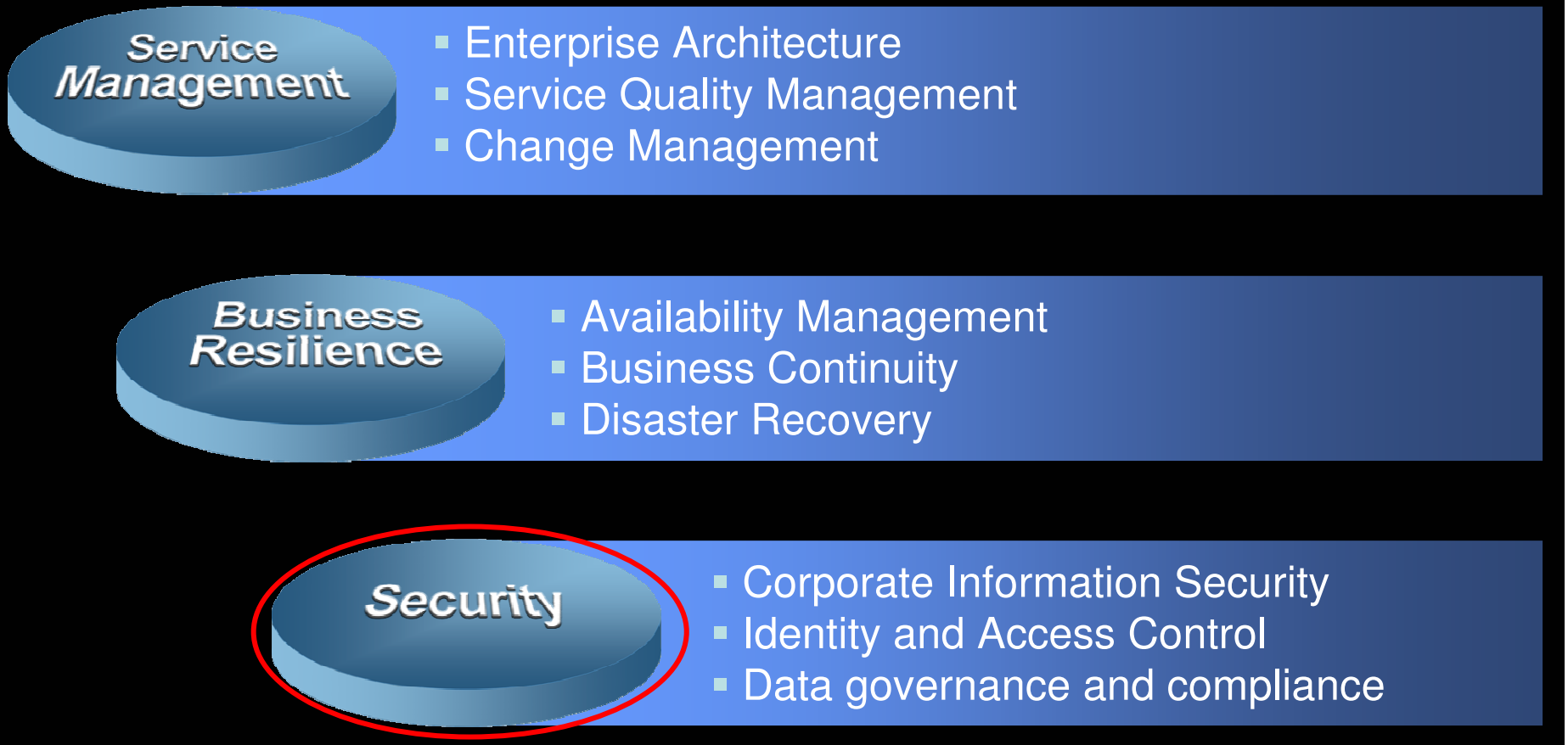
Multimedia

Graphic

Push for Regulations from Unlikely Sources

For toys and cars, antifreeze and fireworks, popcorn and produce and cigarettes and light bulbs, among other products, industry groups or major manufacturers are calling for federal health, safety and environmental mandates. Some of those industries are abandoning years of efforts to block such measures, often in alliance with the Bush administration, which pledged to ease what it views as costly, unnecessary rules.

Your Strategic IT Initiatives are the Starting Point
And Catalysts for Making Improvements



**CIO Note: Establishing an enterprise wide architecture initiative is an important project for enabling better IT governance and compliance.*

IBM Process Approach to IT Governance and Compliance

Putting policy into practice via process

"Do the right things..." ***"...and do things right"***

Business Imperatives

- **Risk Mitigation**
- **Time to Value**
- **Regulations**
- **Innovation**

IT GOVERNANCE & COMPLIANCE

IT strategy, policies and risk tolerances

Results, insights

Business Results

- Performance
- Resilience
- Compliance

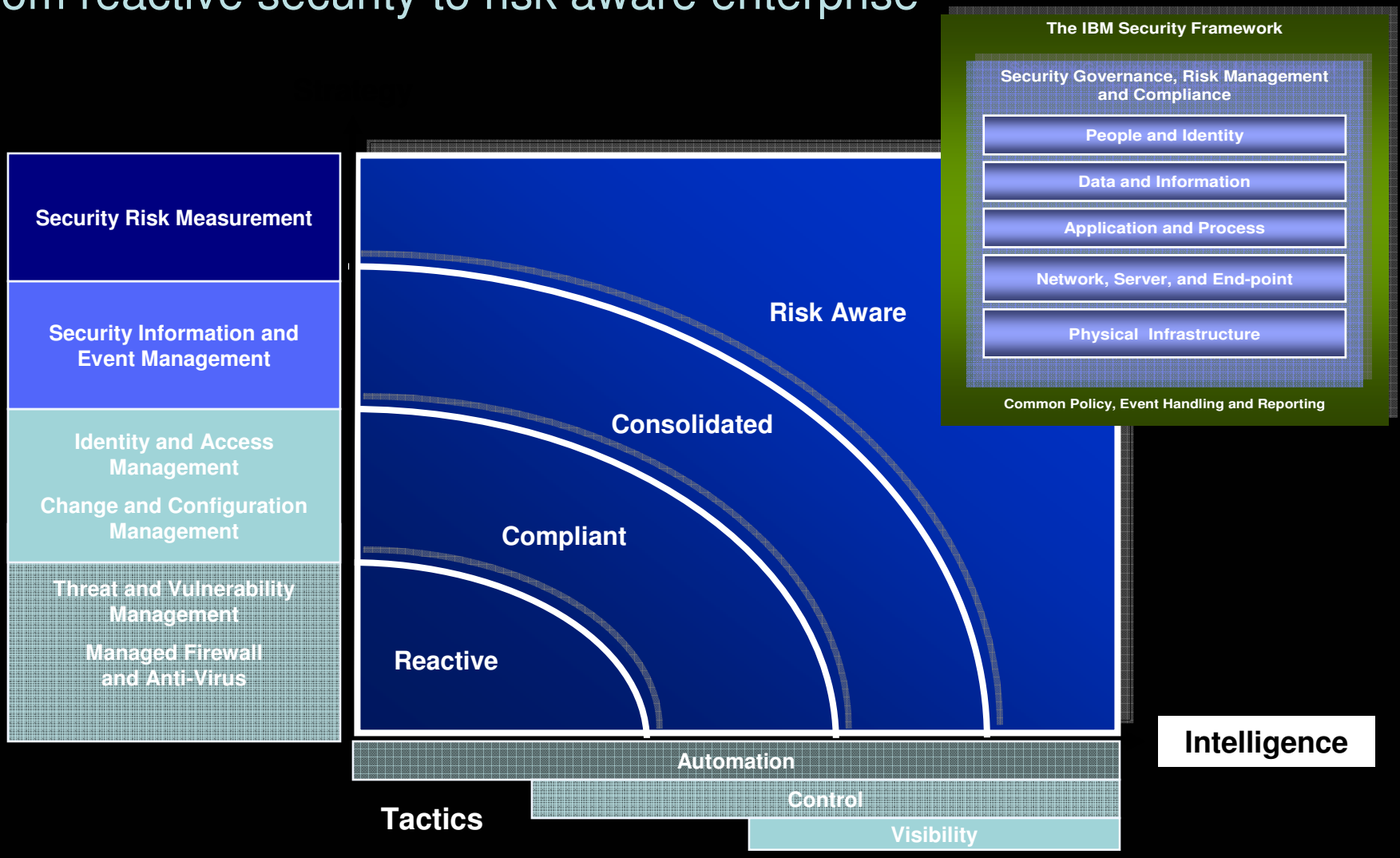
Based on Industry Best Practices and IBM experience

The IBM Security Framework

on-demand protection to stay ahead of outsider and insider threats

- **SECURITY COMPLIANCE**
  - Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)
- **IDENTITY & ACCESS**
  - Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets
- **DATA SECURITY**
  - Protect and secure your data and information assets
- **APPLICATION SECURITY**
  - Continuously manage, monitor and audit application security
- **INFRASTRUCTURE SECURITY**
  - Comprehensive threat and vulnerability management across networks, servers and end-points

IBM Security Management – From reactive security to risk aware enterprise



Agenda

- Compliance
- Audit Management
- Governance and Risk Management
- IBM Customers' Stories
- Summary

Philips International BV

Securing company assets and strengthening compliance

Challenge

- Ensure total control of global funds network
- Comply with regulations such as Sarbanes Oxley and Tabaksblat, the corporate governance code for Netherlands

Solution

- Implemented IBM Tivoli Compliance Insight Manager to protect company assets and comply with regulations

Benefits

- Total control of all data activities and traffic
- Constant control and evidence of commercial payment processes
- Established complete protection against manipulation of information

PHILIPS
sense and simplicity

"Thanks to IBM Tivoli Compliance Insight Manager, we can now validate all the treasury data published in our annual report with greater confidence than ever before."

Gabriel van de Luitgaarden
Senior Vice President

Bancaja

Valencia, Spain

Challenge

- Minimize the risk of customer dissatisfaction and regulatory fines by managing the impact of unplanned system outages
- Reduce IT costs and improve security across the bank's two data centers

Solution

- Engage IBM Global Technology Services to provide business resilience services and two IBM eServer™ zSeries® servers in an IBM Geographically Dispersed Parallel Sysplex™ (GDPS) configuration
- Provide automated transaction monitoring with IBM Tivoli® NetView® software, and automated failover support with IBM TotalStorage® Enterprise Storage Server hardware

Benefits

- Reduced from several days to an hour and a half the time required to initiate backup support due to CPU problems
- Established automatic system recovery in the event of a disk failure
- Reduced the risk of lost revenue and regulations costs, and eliminated risk of Basel II penalties

Pay by Touch

Building a retail payment system that provides total security

Value Drivers

Pay By Touch had put together two existing capabilities — biometric recognition and electronic financial transactions — to create a groundbreaking new retail payment service. The company needed a highly scalable, secure and easy-to-integrate platform to support its rapidly growing operations.

Solution

A service-oriented architecture (SOA) approach that provides the ability to integrate IT assets and capabilities while remaining rapidly scalable as well as secure. The underlying platform is built on WebSphere and Tivoli software for process choreography, integration and high availability.

Benefits

- 25 percent reduction cost of integrating acquired companies
- 30 percent increase in the productivity of IT staff
- 15 percent reduction in total cost of ownership
- Provides secure, positive identification of shoppers
- Eliminates the possibility of credit/debit card fraud due to theft

PAY BY TOUCH™

"For customers, it [Pay by Touch] offers ease and security that just doesn't exist elsewhere—they don't have to carry cash or even a card that could be stolen. Literally, they can walk into a store empty-handed and make a purchase."

— Ryan Ross
Vice President, Business Development
Pay By Touch

Swiss Reinsurance Company

Implements comprehensive IT governance framework

Challenge

- Link IT processes and data to business strategies
- Optimize IT processes, including planning, implementing and delivering IT systems
- Optimize IT resources to capitalize on business opportunities and gain competitive advantage

Solution

- Developed IT governance framework to establish governance processes and steps to monitor regulatory compliance
- Created a process maturity model for IT governance processes

Benefits

- Better able to manage risks
- Increase in investor and shareholder confidence
- Corporate wide standardization of all IT-related risks

Swiss Re

SwissRe increases stakeholder confidence and ensures compliance by reducing IT-related risks.

Consumer Bank

Challenge

- Organization had grown through acquisitions, with no centralized governance over IT assets
- Failed external regulatory audit
- Reasons for audit failure:
  - Inadequate security and business controls over software lifecycle
  - Poor governance over software development environment

Solution

- Bank-wide configuration and change management for IT systems
- Implemented Rational ClearCase MulitSite, Rational ClearQuest, Tivoli Configuration Manager

Benefits

- Passed audit
- Compliance infrastructure well positioned the bank for Sarbanes-Oxley compliance
- Enhanced software team productivity
- Improved governance over software assets

Agenda

- Compliance
- Audit Management
- Governance and Risk Management
- IBM Customers' Stories
- Summary

Make Synchronizing Business and IT Actionable

Supporting the IT Governance and Compliance Lifecycle with Measurable Business Value

1 Enhance business performance

- *Maintain visibility of end to end service and ensure service quality*
- *Improve time to value and manage costs of strategic initiatives*

2 Improve business resilience

- *Reduce risks and protect confidential intellectual property*
- *Minimize and control impact of planned and unplanned disruptions*

3 Achieve compliance

- *Create alignment with internal and external policies and regulations*
- *Effectively prioritize and get more value from IT investments*