What makes you special?

IT Governance and Compliance Solutions for System Management

Marc van Zadelhoff
IBM Tivoli Business Development

IBM Governance and Risk Management
Business alignment, visibility and control

CIO’s Top Priorities Are to Deliver

Business Agility/Innovation While Retaining a Resilient Business

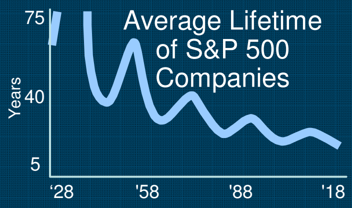
Complexity

Increased complexity makes change much harder

Compliance

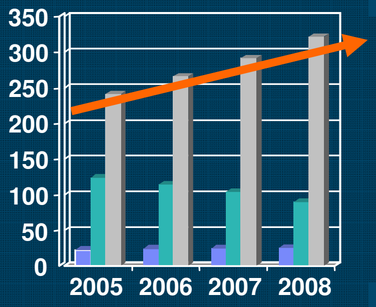
Changing regulatory environment requires security, privacy and ongoing audit capabilities

Change



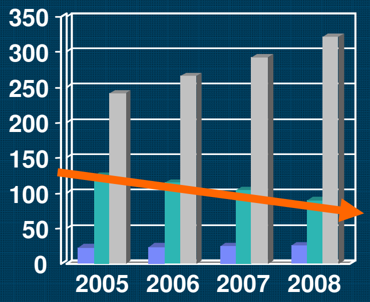
Increased competitive pressure while IT has an increasing role in every business process

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

CIOs with effective IT governance…

Enhance business performance

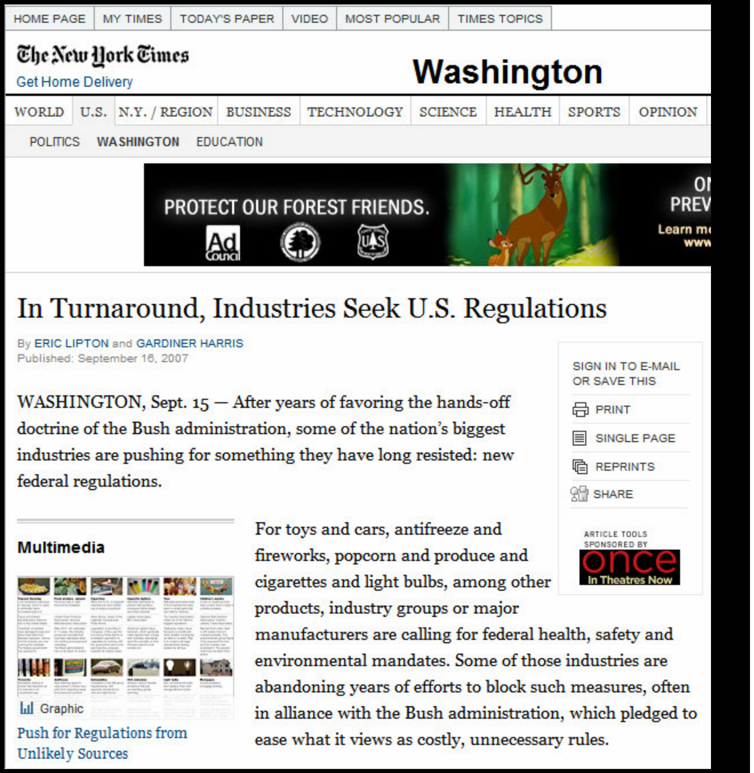
- *Maintain visibility of end to end service to help ensure service quality*
- *Improve time to value and manage costs of strategic initiatives*

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*



In Turnaround, Industries Seek U.S. Regulations

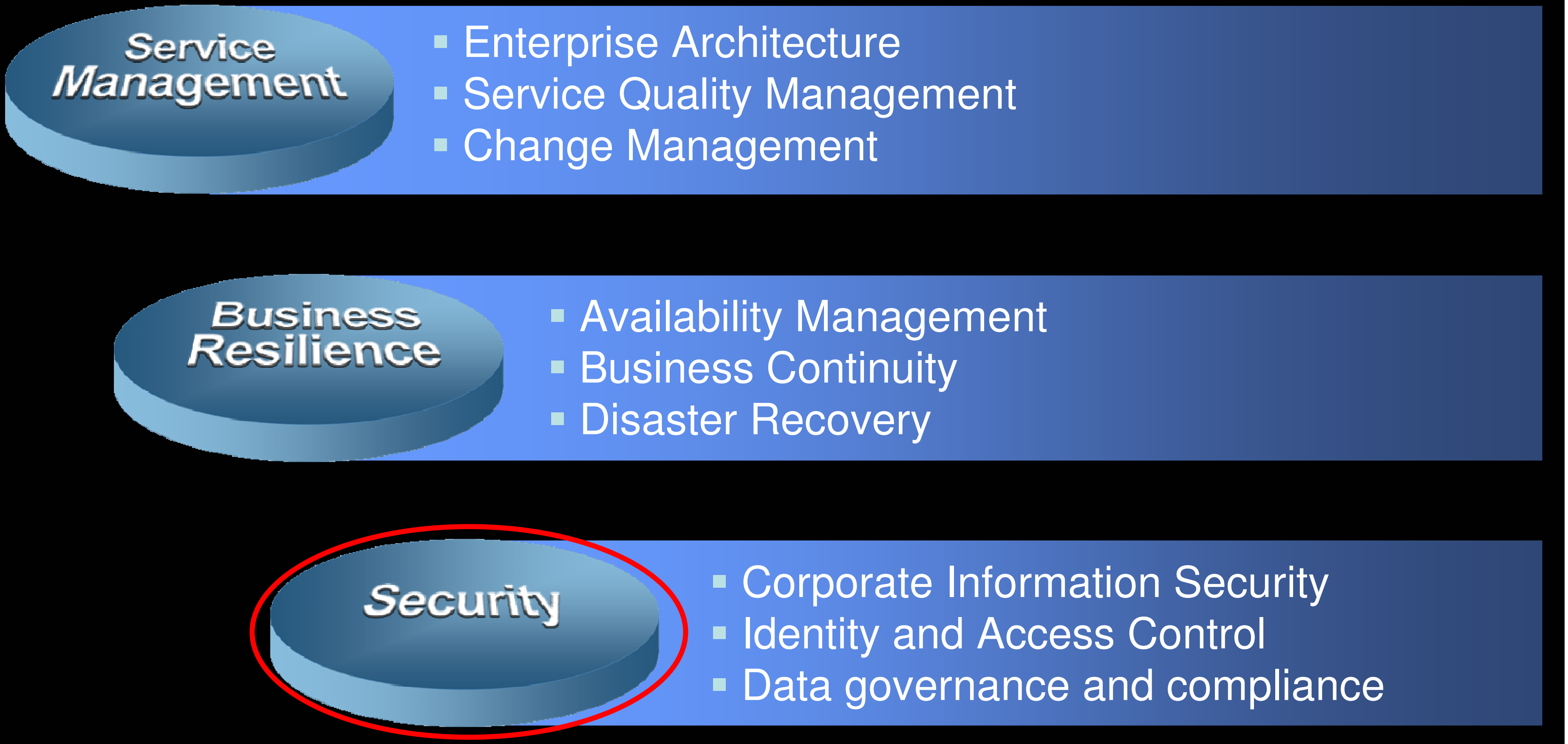
By ERIC LIPTON and GARDINER HARRIS
Published: September 16, 2007

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.

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



Service Management

- Enterprise Architecture
- Service Quality Management
- Change Management

Business Resilience

- Availability Management
- Business Continuity
- Disaster Recovery

Security

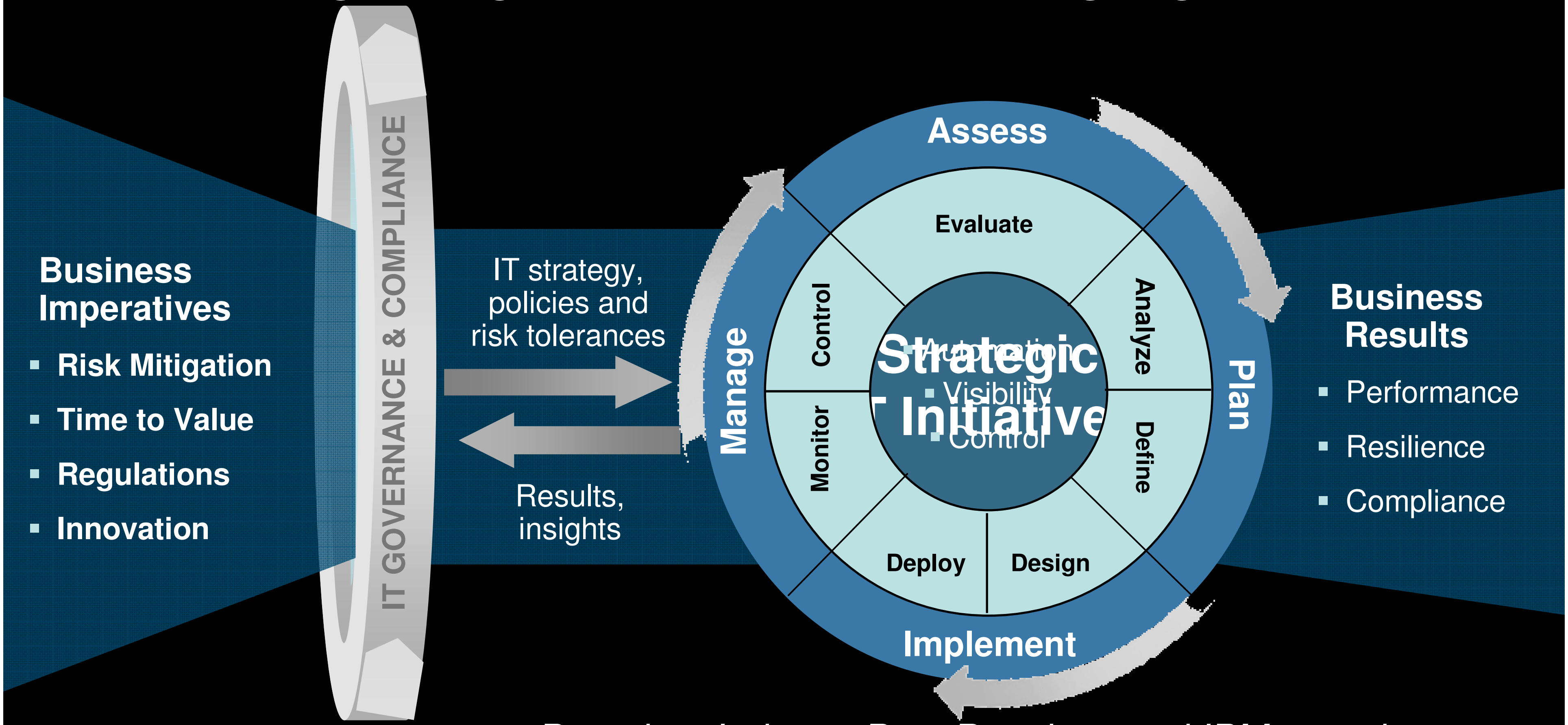
- Corporate Information Security
- Identity and Access Control
- Data governance and compliance

**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

Assess · **Plan** · **Implement** · **Manage**

Evaluate · **Analyze** · **Define** · **Design** · **Deploy** · **Monitor** · **Control**

Strategic IT Initiative

- Automation
- Visibility
- Control

Business Results

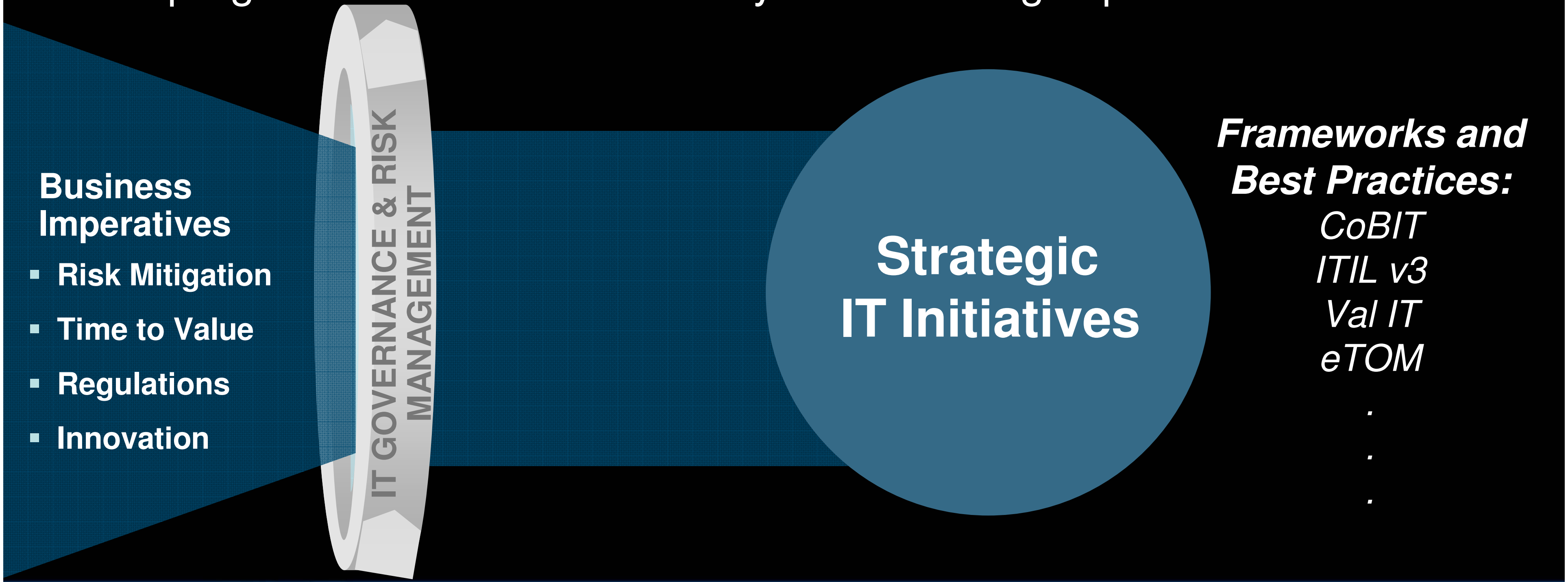
- Performance
- Resilience
- Compliance

Based on Industry Best Practices and IBM experience

5 Steps to Good Governance

1. Standardize on a process for applying IT governance and risk management —helps ensure you have the supporting implementation expertise and technology to make it actionable

2. Choose one IT initiative that makes sense – you don’t need to tackle IT governance and risk management generally—focus on specific programs or initiatives as catalysts for making improvements



Business Imperatives

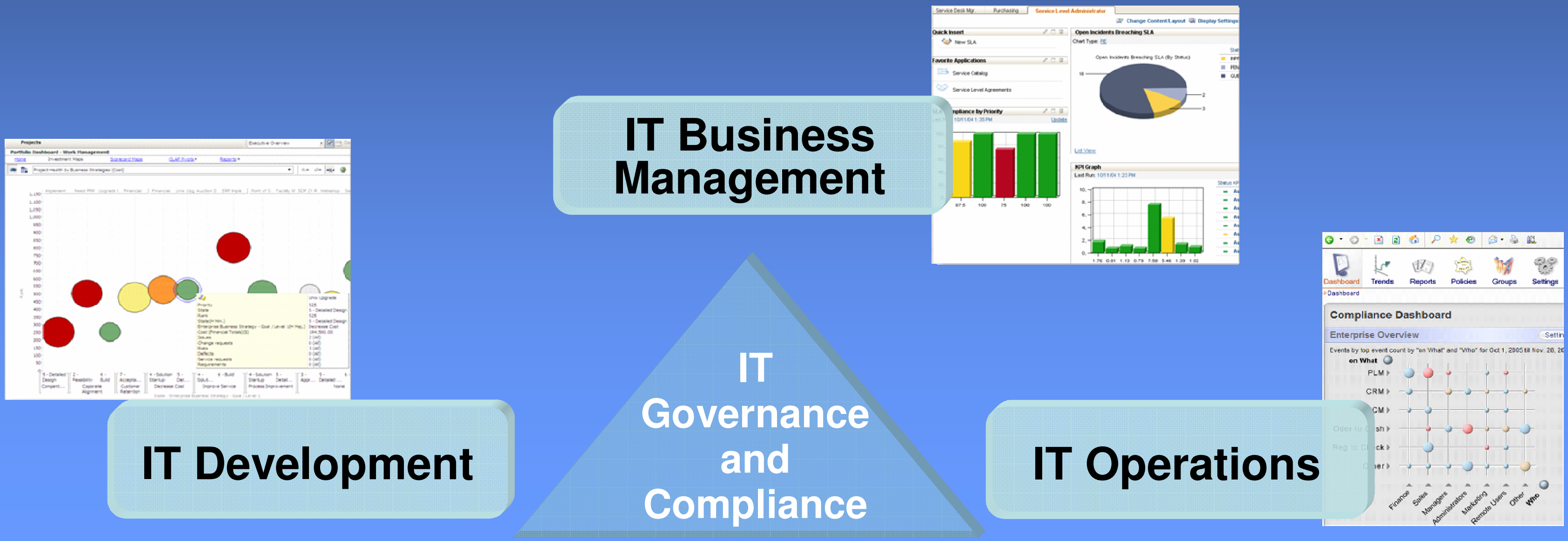
- **Risk Mitigation**
- **Time to Value**
- **Regulations**
- **Innovation**

Frameworks and Best Practices:
CoBIT
ITIL v3
Val IT
eTOM
.
.
.

5 Steps to Good Governance

Implement 'Audit Ready' Visibility and Control

3. Establish key dashboards for visibility across IT silos to monitor and measure project outcomes relative to objectives, policies and risk tolerances
4. Implement fine-grain process and management controls and automate where possible to help eliminate human error and improve process consistency
5. Underpin your enterprise architecture with a standards-based data integration and data sharing platform that spans development and operations processes with common workflow and policy integration



IT Business Management

IT Governance and Compliance

IT Development

IT Operations

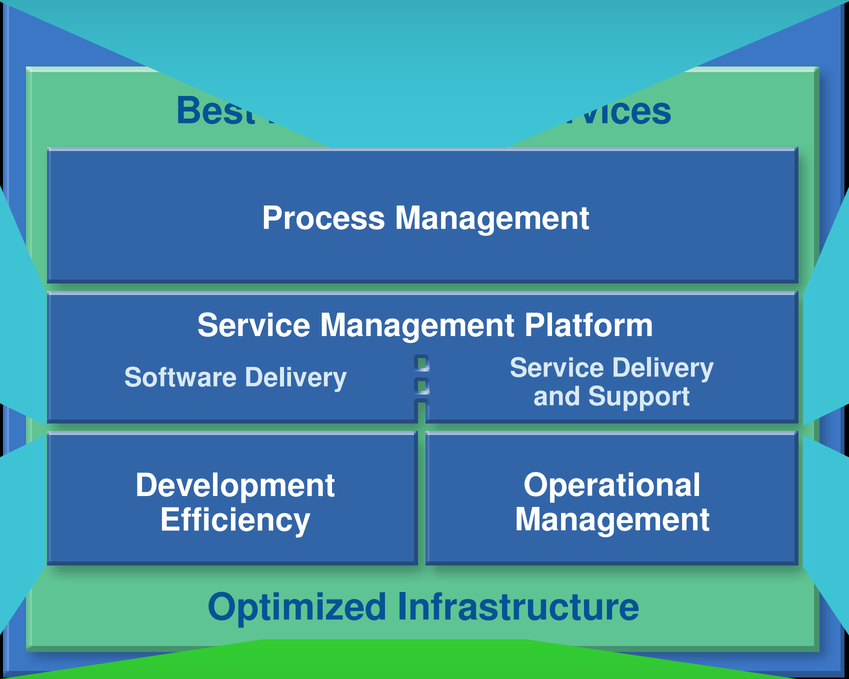
IBM's Approach to Service Management

Architected to Clarify Prioritization and Improve Efficiency

Enable service priority and leverage best practices: Process management supports organization automation and alignment with business goals

Bridge silos and reduce friction: Provides a collaborative team-based software delivery platform to reduce friction

Accelerate tasks and improve effectiveness: Automate development and delivery tasks



Visibility to information & service context: Service delivery and support platform serves as the foundation for automation

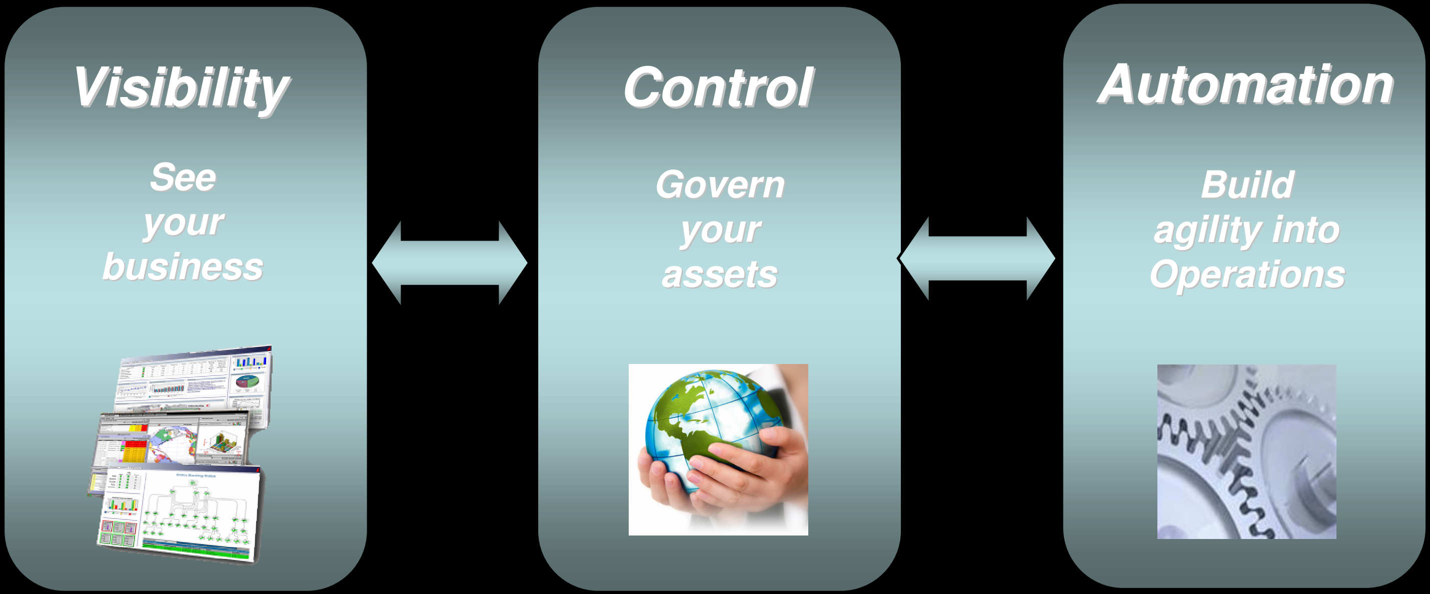
Receive service context: Operational management products deliver task level automation

Gain insight, establish best practices: Identify opportunities for added efficiency, business value and growth

Leverage flexible, reliable, available, and secure resources

IBM Service Management (ISM)

An Integrated Approach to Getting Business Results



Visibility

See your business

Control

Govern your assets

Automation

Build agility into Operations

Only IBM delivers integrated visibility across Business & IT Audiences.

e.g. Contextual LoB, Compliance, Security, Service, & Domain Dashboards

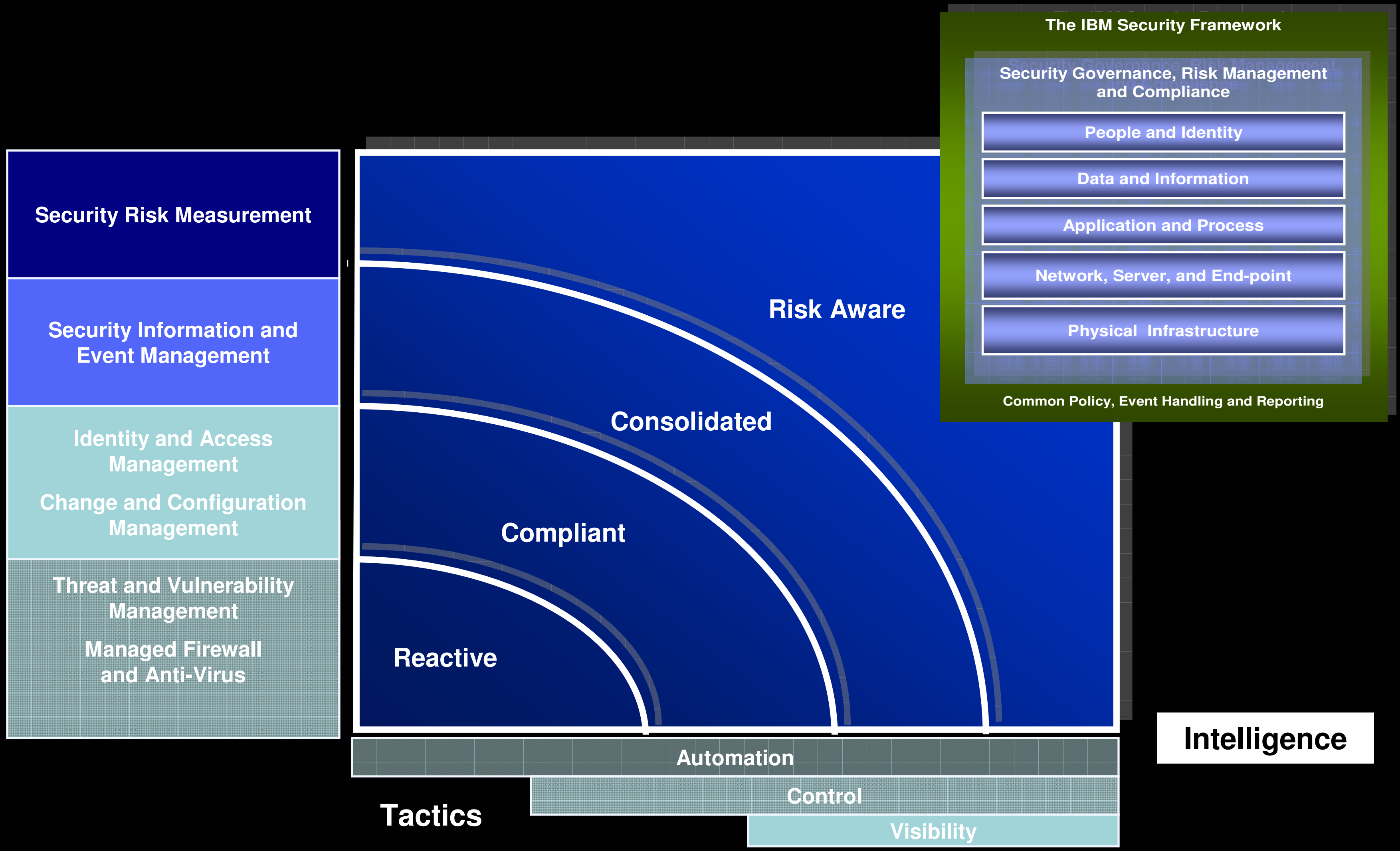
Only IBM delivers integrated control across Business & IT Assets.

e.g. EAM, IT Asset Mgmt, Change & Config, Access & Identity Mgmt, Data Mgmt.

Only IBM delivers integrated automation across Business & IT Operations.

e.g. Enterprise Ops,Service provider Ops, IT Ops, Security Ops, Storage Ops...

ISM – From reactive security to risk aware enterprise



Security Risk Measurement

Security Information and Event Management

Identity and Access Management

Change and Configuration Management

Threat and Vulnerability Management

Managed Firewall and Anti-Virus

Risk Aware

Consolidated

Compliant

Reactive

The IBM Security Framework

Security Governance, Risk Management and Compliance

People and Identity

Data and Information

Application and Process

Network, Server, and End-point

Physical Infrastructure

Common Policy, Event Handling and Reporting

Intelligence

Tactics

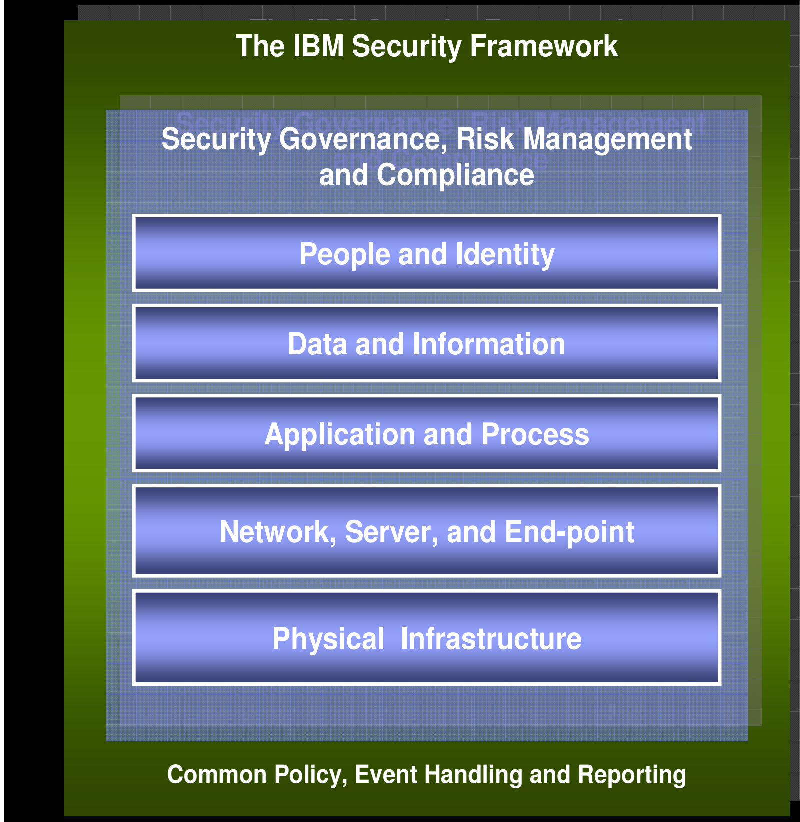
Automation

Control

Visibility

The IBM Security Framework

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


The IBM Security Framework
Security Governance, Risk Management and Compliance
People and Identity
Data and Information
Application and Process
Network, Server, and End-point
Physical Infrastructure
Common Policy, Event Handling and Reporting

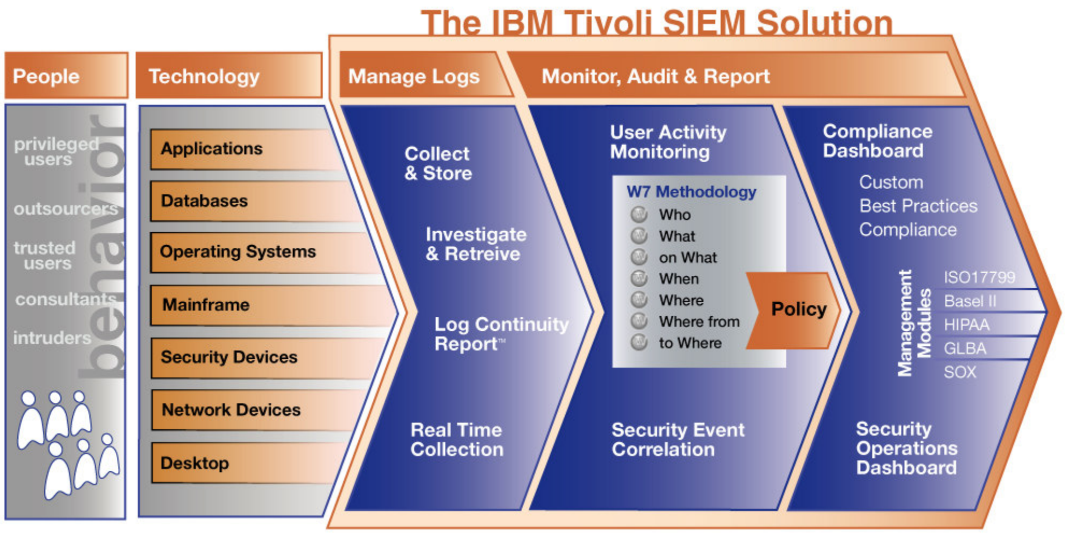
- **SECURITY COMPLIANCE**
  - Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)
- **IDENTITY & ACCESS**
  - Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets
- **DATA 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

Security Compliance

Aligning IT security to business priorities

Goals

- Proactive real-time monitoring of network & systems for compliance with security policies
- Monitor platforms from mainframe to distributed & devices
- Historical reporting to demonstrate compliance
- Clearly define & communicate potential security incidents so they can be handled correctly
- Ensure that preventive, detective and corrective measures are in place to protect information systems & technology from malware



IBM solutions

- Tivoli Security Information & Event Mgr.
- Tivoli Compliance Insight Manager
- Tivoli Security Operations Manager
- Tivoli Security Compliance Manager
- Tivoli zSecure suite

Capabilities for IBM Security & Privacy

- Tivoli Compliance Insight Manager
  - Roll-your-own compliance modules thru wizard for advanced report definition
  - Flexible automated report distribution
  - Advanced toolkit for adding new log collectors, parsers, and normalization
  - Integrates with Tivoli Identity Manager & Tivoli Access Manager for event collection and reporting
  - Agentless iSeries event collection and reporting

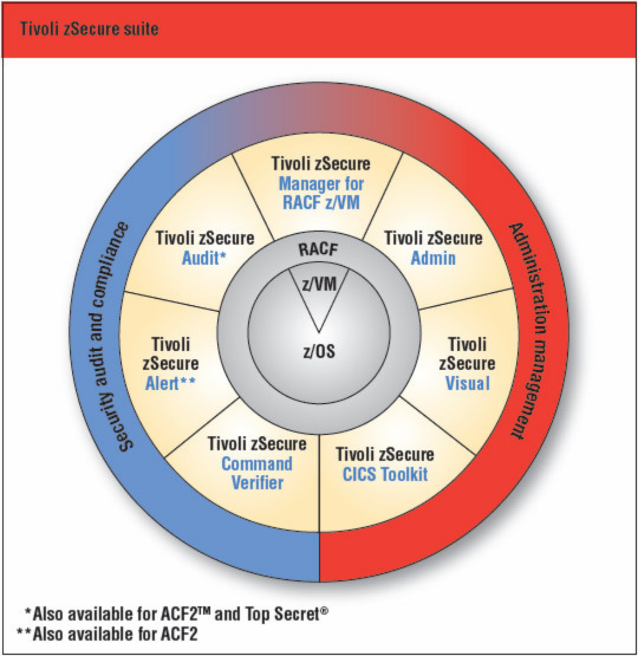
- Tivoli zSecure suite
  - Fingerprinting and modification detection of z/OS sequential datasets
  - Support for new DB2 V9 audit events
  - XML based reporting enhancements and documentation
  - New component released in Sept 2007: zSecure Manager for RACF z/VM

IBM Tivoli zSecure Suite

The Tivoli zSecure suite adds a user-friendly layer onto the mainframe that enables superior administration coupled with audit, alert and monitoring capabilities for Resource Access Control Facility (RACF)

Key Features

- The zSecure suite improves the efficiency of mainframe administration and enhances the ability for the mainframe to be the hub of enterprise security.
- Administration and provisioning:
  - zSecure Admin enhances user management
  - zSecure Visual offers a Microsoft® Windows® GUI
  - zSecure CICS Toolkit for simplified RACF security management
  - zSecure Manager for RACF z/VM provides combined audit & admin for VM environment
- Audit, monitoring and compliance:
  - zSecure Audit provides event detection, analysis & reporting and system integrity audit & analysis
  - zSecure Alert provides intrusion detection and alerting
  - zSecure Command Verifier offers automated security monitoring

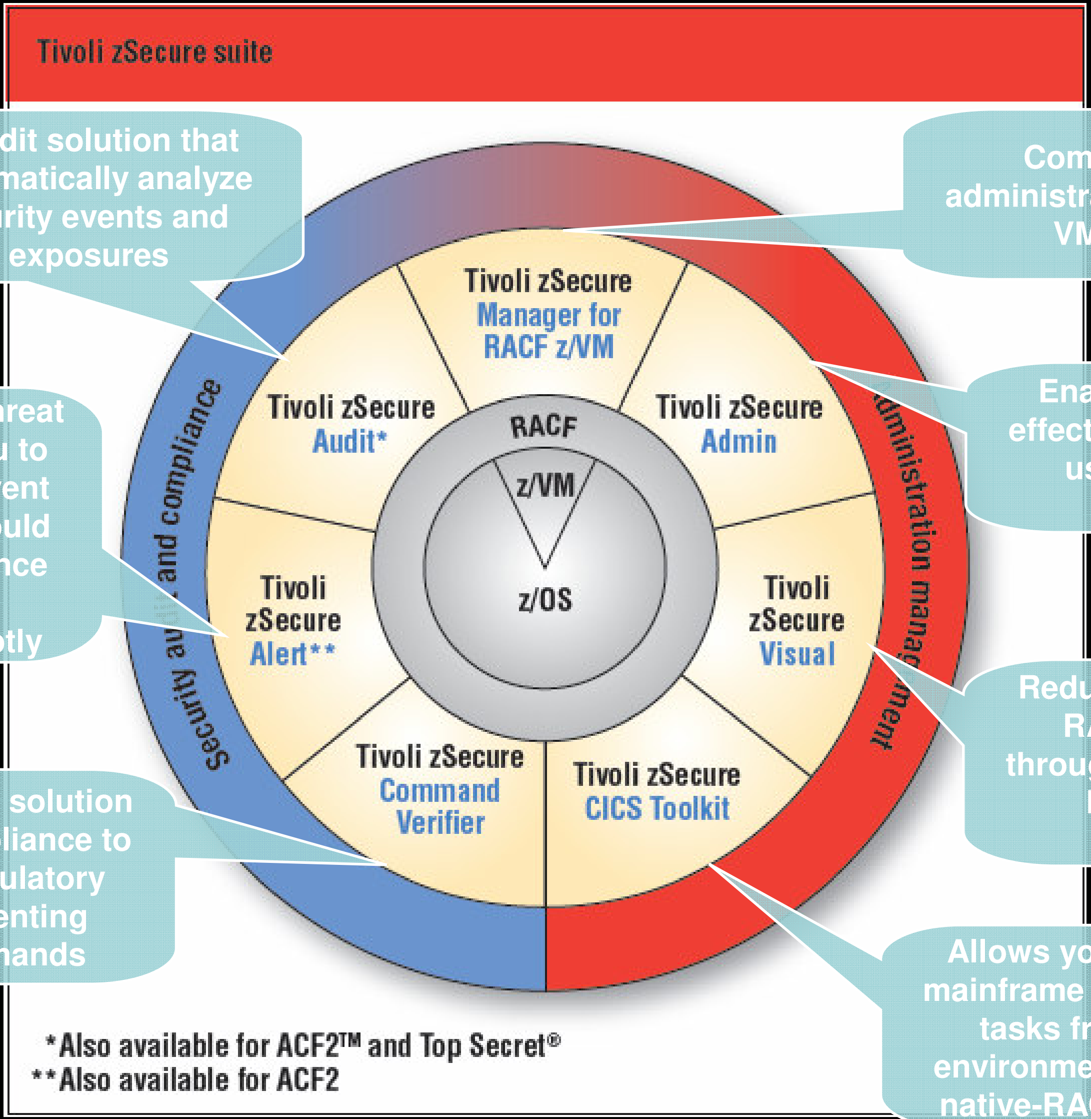

Tivoli zSecure suite
Tivoli zSecure Manager for RACF z/VM
Tivoli zSecure Audit*
Tivoli zSecure Admin
RACF
z/VM
z/OS
Tivoli zSecure Alert**
Tivoli zSecure Visual
Tivoli zSecure Command Verifier
Tivoli zSecure CICS Toolkit
Security audit and compliance
Administration management

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

Benefits Summary

- Administration and provisioning:
  - Reduce administration time, effort and cost
  - Reduce training time needed for new administrators
- Audit, monitoring and compliance:
  - Helps to pass audits more easily
  - Can improve security posture
  - Save time and costs through improved security and incident handling
  - Can increase operational effectiveness

Introducing the IBM Tivoli zSecure Suite


Tivoli zSecure suite
Security audit and compliance
Administration management
Tivoli zSecure Manager for RACF z/VM
Tivoli zSecure Admin
Tivoli zSecure Visual
Tivoli zSecure CICS Toolkit
Tivoli zSecure Command Verifier
Tivoli zSecure Alert**
Tivoli zSecure Audit*
RACF
z/VM
z/OS

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

Compliance and audit solution that enables you to automatically analyze and report on security events and detect security exposures

Combined audit and administration for RACF in the VM environment

Real-time mainframe threat monitoring allows you to identify changes in event configurations that could hamper your compliance efforts and notify administrators promptly

Enables more efficient and effective RACF administration, using significantly less resources

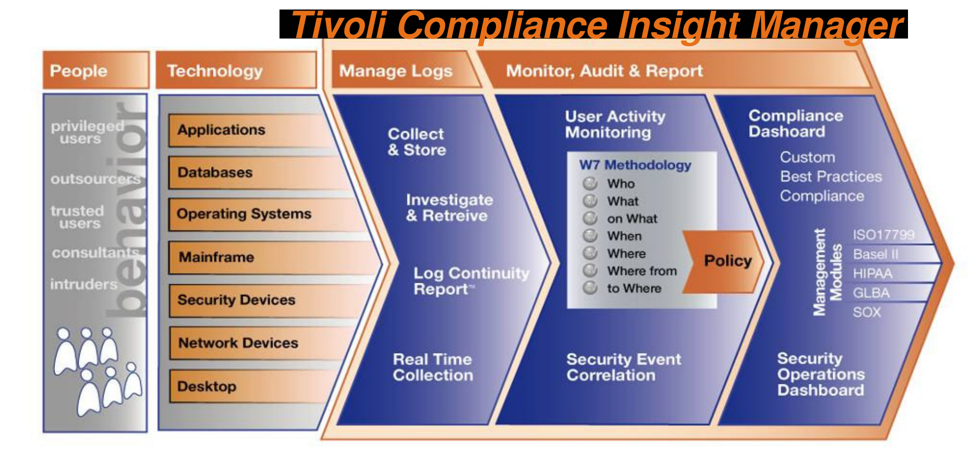
Reduces the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

Policy enforcement solution that enforces compliance to company and regulatory policies by preventing erroneous commands

Allows you to perform mainframe administrative tasks from a CICS environment, freeing up native-RACF resources

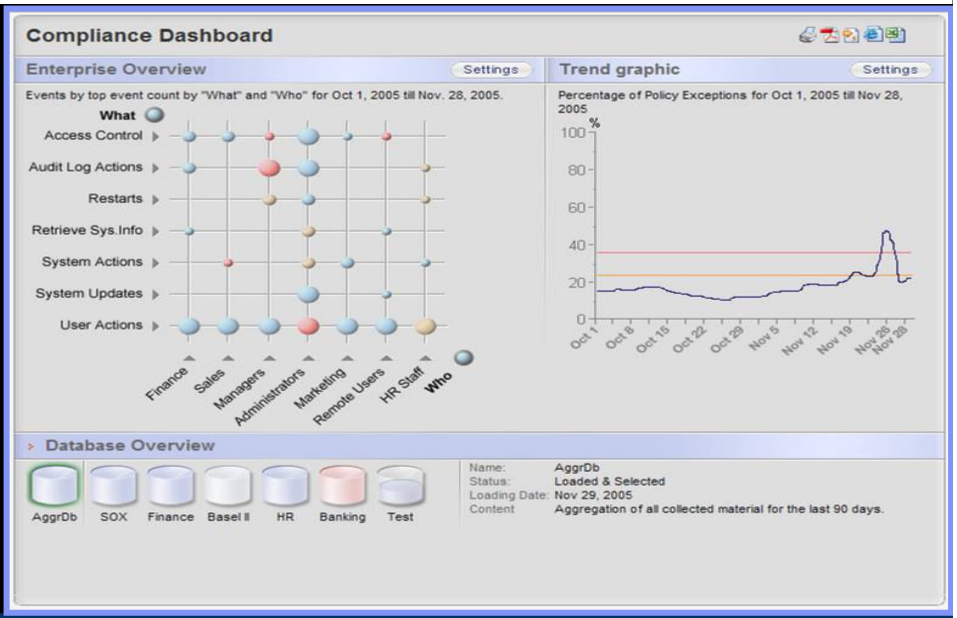
Assessing and Monitoring Compliance: Tivoli Compliance Insight Manager

Tivoli Compliance Insight Manager provides an enterprise security compliance dashboard with in-depth privileged user monitoring capabilities, all powered by a comprehensive log and audit trail collection capability



Key Features

- Compliance management modules and regulation-specific reports
- Unique ability to monitor user behavior, including PUMA (Privileged User Monitoring and Audit) reporting
- Broadest, most complete log and audit trail capture capability
- W7 log normalization translates your logs into business terms
- Easy ability to compare behavior to regulatory and company policies – auditors no longer need RACF expertise to monitor activities
- Enabler event source integrates the OS and mainframe database events into TCIM’s enterprise compliance dashboard


Compliance Dashboard

Enterprise Overview

Events by top event count by "What" and "Who" for Oct 1, 2005 till Nov. 28, 2005.

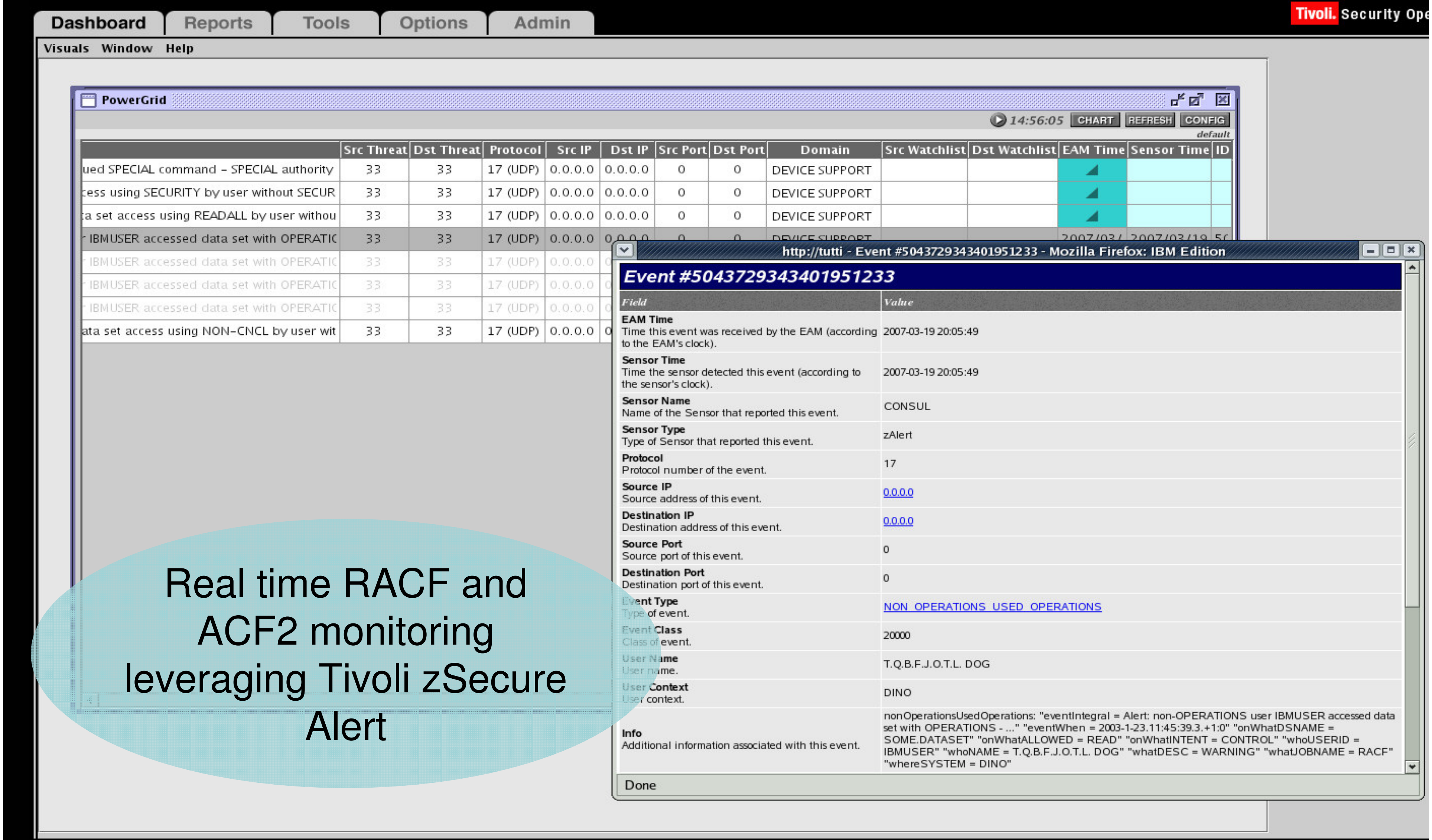
Trend graphic

Percentage of Policy Exceptions for Oct 1, 2005 till Nov 28, 2005

Database Overview

Name: AggrDb
Status: Loaded & Selected
Loading Date: Nov 29, 2005
Content Aggregation of all collected material for the last 90 days.

Integration with Tivoli Security Operations Manager



	Src Threat	Dst Threat	Protocol	Src IP	Dst IP	Src Port	Dst Port	Domain	Src Watchlist	Dst Watchlist	EAM Time	Sensor Time	ID
ued SPECIAL command - SPECIAL authority	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT			◢		
cess using SECURITY by user without SECUR	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT			◢		
a set access using READALL by user withou	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT			◢		
IBMUSER accessed data set with OPERATIC	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT			2007/03/	2007/03/19	5(
IBMUSER accessed data set with OPERATIC	33	33	17 (UDP)	0.0.0.0	0								
IBMUSER accessed data set with OPERATIC	33	33	17 (UDP)	0.0.0.0	0								
IBMUSER accessed data set with OPERATIC	33	33	17 (UDP)	0.0.0.0	0								
ata set access using NON-CNCL by user wit	33	33	17 (UDP)	0.0.0.0	0								

http://tutti - Event #5043729343401951233 - Mozilla Firefox: IBM Edition

Event #5043729343401951233

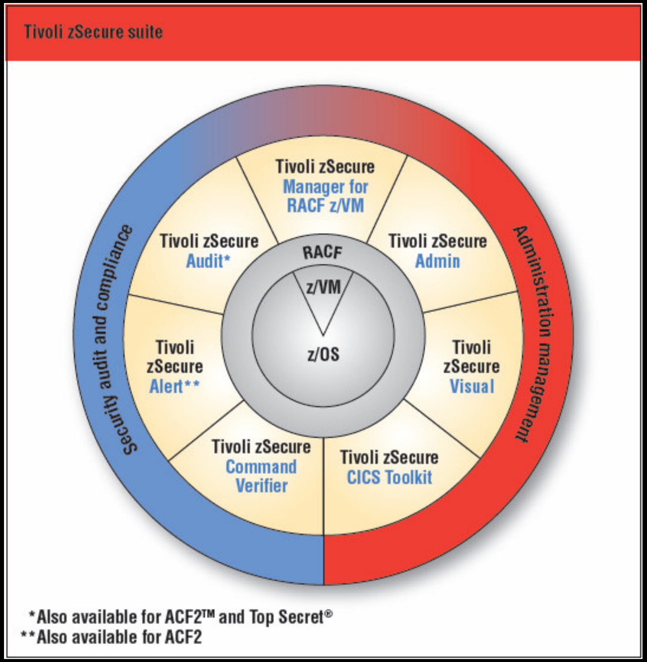
Field	*Value*
EAM Time Time this event was received by the EAM (according to the EAM's clock).	2007-03-19 20:05:49
Sensor Time Time the sensor detected this event (according to the sensor's clock).	2007-03-19 20:05:49
Sensor Name Name of the Sensor that reported this event.	CONSUL
Sensor Type Type of Sensor that reported this event.	zAlert
Protocol Protocol number of the event.	17
Source IP Source address of this event.	0.0.0.0
Destination IP Destination address of this event.	0.0.0.0
Source Port Source port of this event.	0
Destination Port Destination port of this event.	0
Event Type Type of event.	NON_OPERATIONS_USED_OPERATIONS
Event Class Class of event.	20000
User Name User name.	T.Q.B.F.J.O.T.L. DOG
User Context User context.	DINO
Info Additional information associated with this event.	nonOperationsUsedOperations: "eventIntegral = Alert: non-OPERATIONS user IBMUSER accessed data set with OPERATIONS - ..." "eventWhen = 2003-1-23.11:45:39.3.+1:0" "onWhatDSNAME = SOME.DATASET" "onWhatALLOWED = READ" "onWhatINTENT = CONTROL" "whoUSERID = IBMUSER" "whoNAME = T.Q.B.F.J.O.T.L. DOG" "whatDESC = WARNING" "whatJOBNAME = RACF" "whereSYSTEM = DINO"

Done

Real time RACF and ACF2 monitoring leveraging Tivoli zSecure Alert

A cornerstone for Tivoli's System z Security Strategy

IBM Tivoli zSecure Suite


Tivoli zSecure suite
Security audit and compliance
Administration management
Tivoli zSecure Manager for RACF z/VM
Tivoli zSecure Audit*
Tivoli zSecure Admin
Tivoli zSecure Alert**
Tivoli zSecure Visual
Tivoli zSecure Command Verifier
Tivoli zSecure CICS Toolkit
RACF
z/VM
z/OS
*Also available for ACF2™ and Top Secret®
**Also available for ACF2

Enterprise Security Monitoring and Audit Reporting

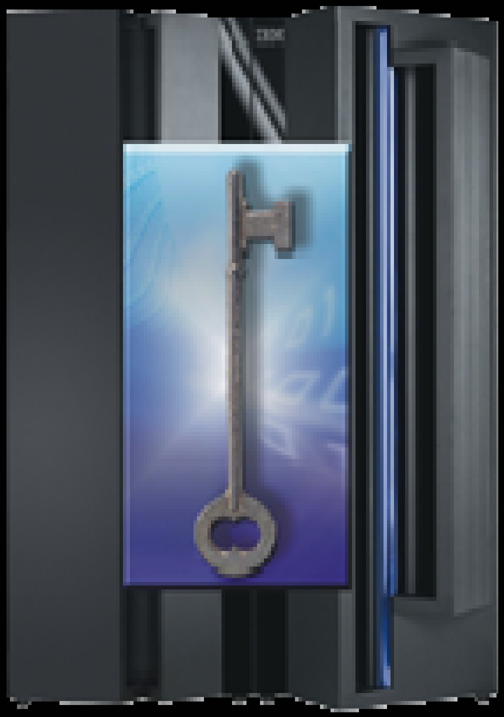
Enterprise Identity and Access Management

Tivoli Compliance Insight Manager (TCIM)	Tivoli Security Operations Manager (TSOM)	Tivoli Identity Manager (TIM) for z/OS	Tivoli Federated Identity Manager (TFIM) for z/OS	Tivoli Directory Server (TDS) for z/OS	Tivoli Directory Integrator (TDI) for z/OS

* Also available for ACF2 and Top Secret
** Also available for ACF2

Enterprise Security Hub Solution

- IBM offers the total solution for the enterprise security hub
  - Most secure and resilient hardware platform, providing reliability, availability, and scalability
  - Integrated security features in the operating system, including digital certificates and PKI
  - Data and communications encryption with support from ICSF and local key management
  - Most reliable security server
  - Most comprehensive mainframe security administration & audit
  - Comprehensive enterprise SIEM dashboard for audit and compliance management
  - Enterprise-wide identity and access management solutions in Tivoli security portfolio
  - Security, recoverability, and scalability to support centralized services offerings for SOA implementations



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*

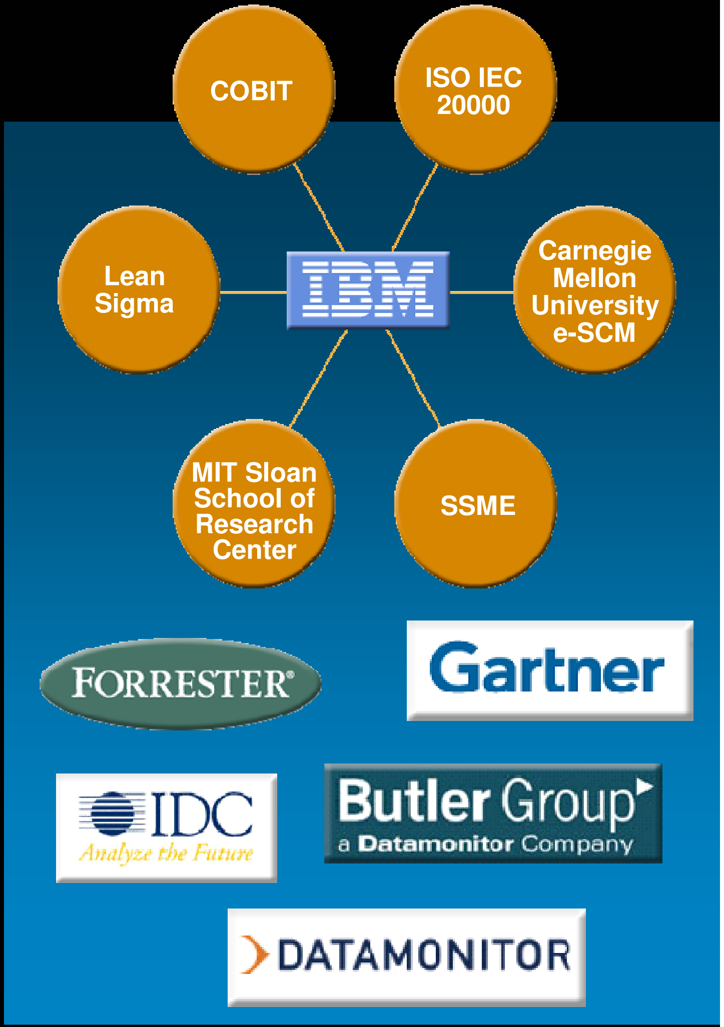
3 **Achieve compliance**

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

IBM Leadership

Around Service Management in the Market Includes …

- 25 years of thought leadership with thousands of customer engagements
  - Continued leadership in support of open standards
- IBM leadership with customers:
  - Finance: 96 of top 100 customers
  - Communications: 20 of top 20 customers
  - Healthcare: 9 of top 10 customers
  - Retail: 8 of top 10 customers
- Leadership in multiple analyst categories
  - WW operations leader five years in a row
  - Application lifecycle mgmt tools market leader
  - IT Systems Management leader



IBM

COBIT

ISO IEC 20000

Lean Sigma

Carnegie Mellon University e-SCM

MIT Sloan School of Research Center

SSME

Why IBM?

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, z/OS 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.

Thank You

Impact of a Breach

- Average annual loss up 80% over 2006
- Financial Fraud overtook Virus Attacks as the greatest source of losses
- Data breach-related attacks rank #1, 3, 4, and 5 as most costly incidents by dollar amount
- 43% of U.S. companies have no overall security strategy
- Employees beat hackers as the most likely security incident source
- 46% of respondents suffered a security incident

CSI Survey 2007

The GLOBAL STATE of INFORMATION SECURITY 2007

A Joint Research Project of CIO and CSO in partnership with PricewaterhouseCoopers

Just released: FBI/CSI Survey, PricewaterhouseCoopers Studies

Sources: CSI Computer Crime and Security Survey 2007; Global State of Information Security 2007

Identity & Access Management

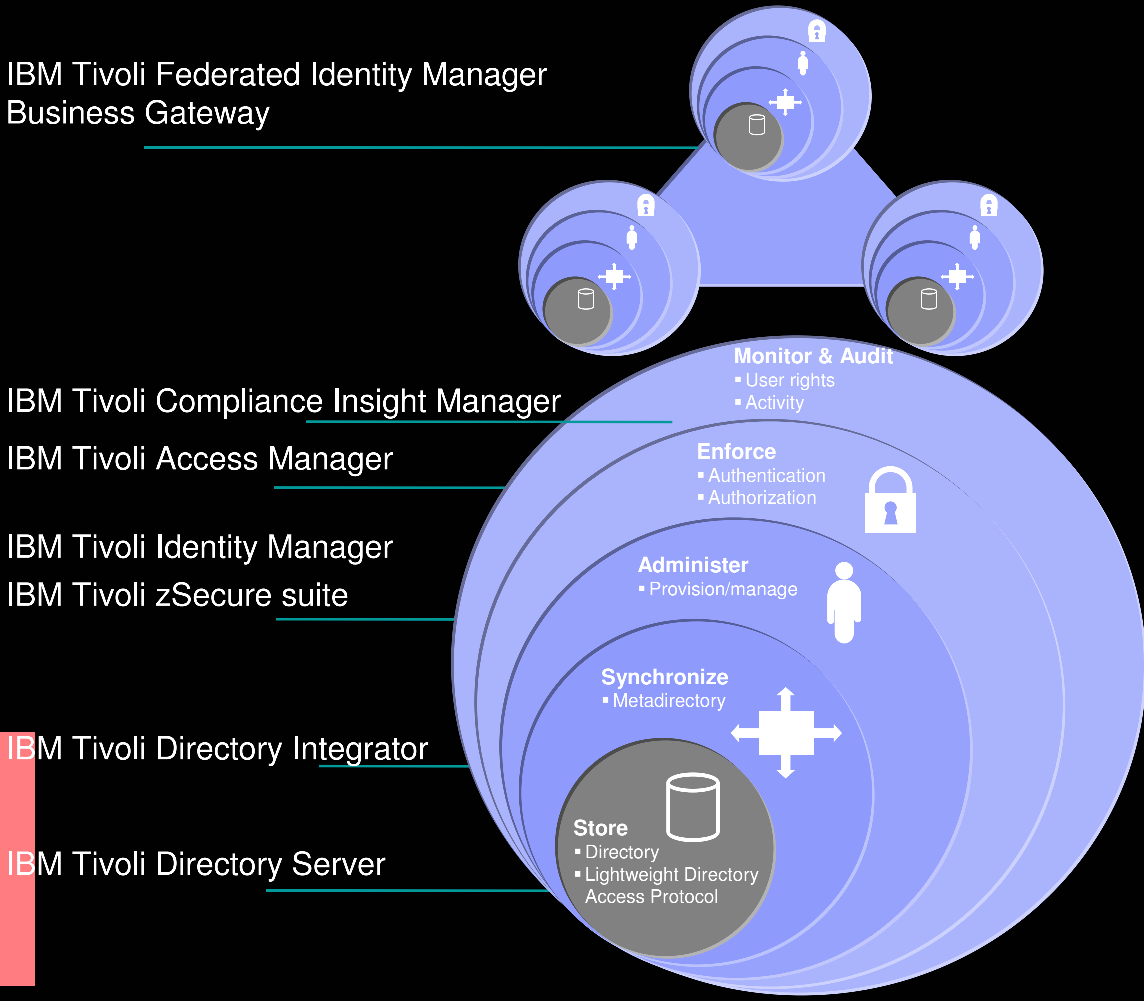
Manage users, identities, access rights, enforce & monitor user activity on all IT systems

Goals

- Enable single sign on
- Manage identity lifecycle: provision, deprovision.
- Monitor account activity: dormant accounts, irregular activity.
- Review / recertify access periodically
- Automate manually-implemented processes for controlling access to IT resources
- Centralize access policy and related internal controls
- Properly verify authenticity of all users based on potential liability

IBM solutions

- Tivoli Identity Manager
- Tivoli Access Manager
- Tivoli Federated Identity Manager
- Tivoli zSecure Suite



IBM Tivoli Federated Identity Manager
Business Gateway

IBM Tivoli Compliance Insight Manager

IBM Tivoli Access Manager

IBM Tivoli Identity Manager

IBM Tivoli zSecure suite

IBM Tivoli Directory Integrator

IBM Tivoli Directory Server

Data Security

Protecting a critical enterprise asset

Goals

- Comprehensive protection for all data and information in the enterprise – structured, unstructured and sem-structured data
- Facilitate the discovery, classification, defense, and monitoring of critical intellectual property and sensitive enterprise information in disparate information stores (databases, email, laptops, pervasive devices, etc.)

IBM solutions

- Tivoli Access Manager
- IBM FileNet P8 with Records Crawler and IBM Classification module
- Tivoli zSecure suite
- Tivoli Key Lifecycle Manager (2008)

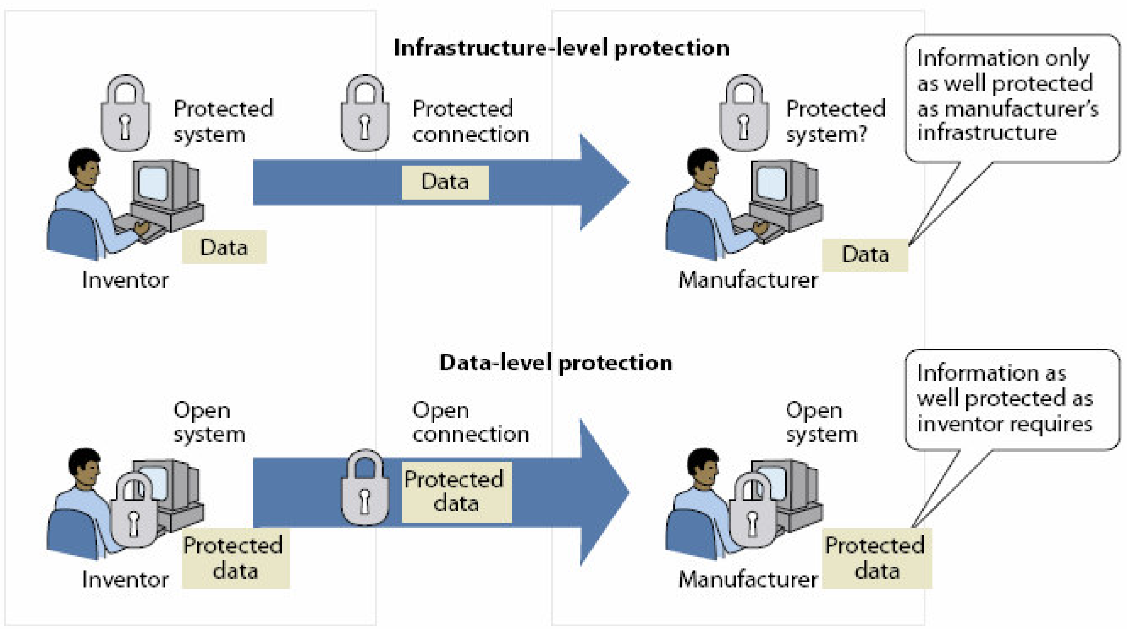
Old Security model

Defensive, threat-protection oriented

Manual, audit-based policy enforcement

Focused on securing infrastructure

Figure 1 Data-Level Protection In An Inventor-Manufacturer Relationship



39438

Source: Forrester Research, Inc.

New security model

Securely designed from the ground up

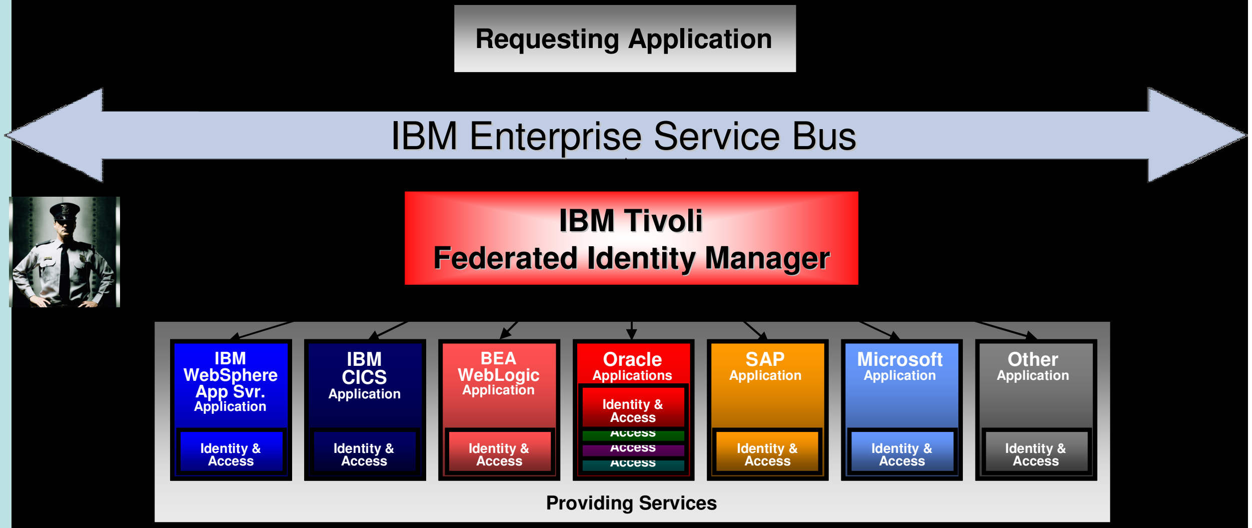
Automated policy enforcement

Focused on securing data

Application Security - SOA

Goals

- In an SOA environment, provide secure access and federate identity across these services
- Externalize core security services from the application
- Ensure security administrators make changes NOT developers.
- Ensure changes to security are auditable



IBM solutions

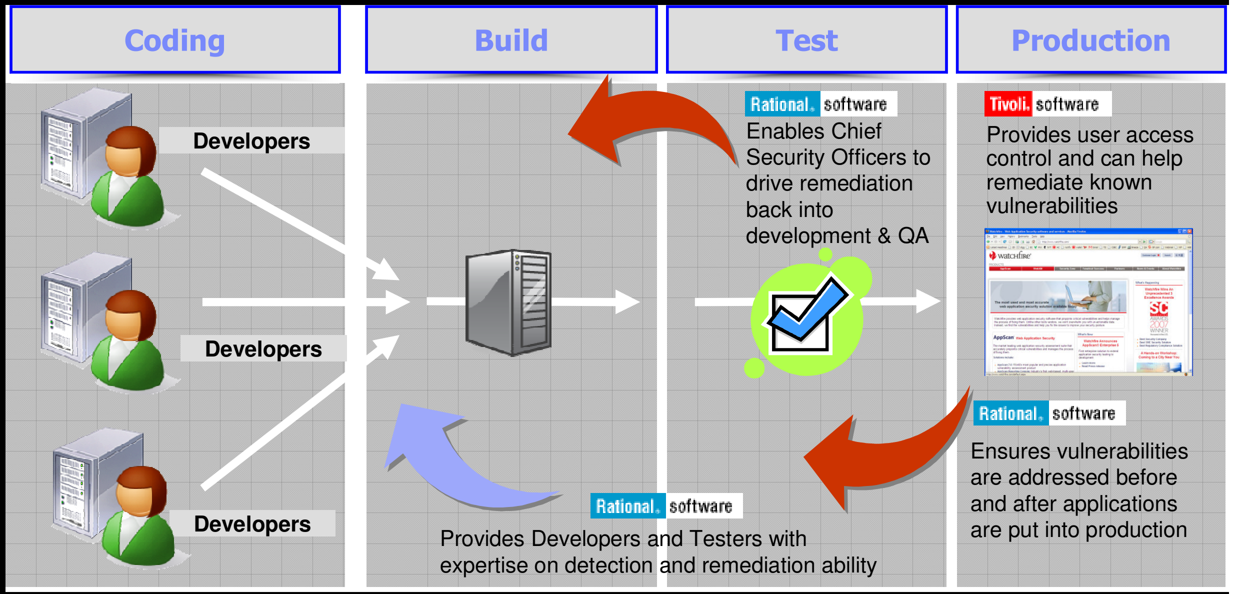
- Tivoli Federated Identity Manager
- WebSphere Enterprise Service Bus (ESB)
- WebSphere Message Broker
- WebSphere DataPower

Application Security – vulnerability management

Security policy management for an application from creation through production.

Goals

- Define application security standards and requirements
- Build security into app design and model threats
- Build and test individual and composite applications
- Configure infrastructure for application policies; deploy applications in production
- Continuously manage, monitor and audit application security



Enables Chief Security Officers to drive remediation back into development & QA

Provides user access control and can help remediate known vulnerabilities

Ensures vulnerabilities are addressed before and after applications are put into production

Provides Developers and Testers with expertise on detection and remediation ability

Rational AppScan & Tivoli provide security that spans the application lifecycle

IBM solutions

- Rational AppScan
- Tivoli Access Manager
- Tivoli Federated Identity Manager
- Tivoli Identity Manager

Infrastructure Security Management

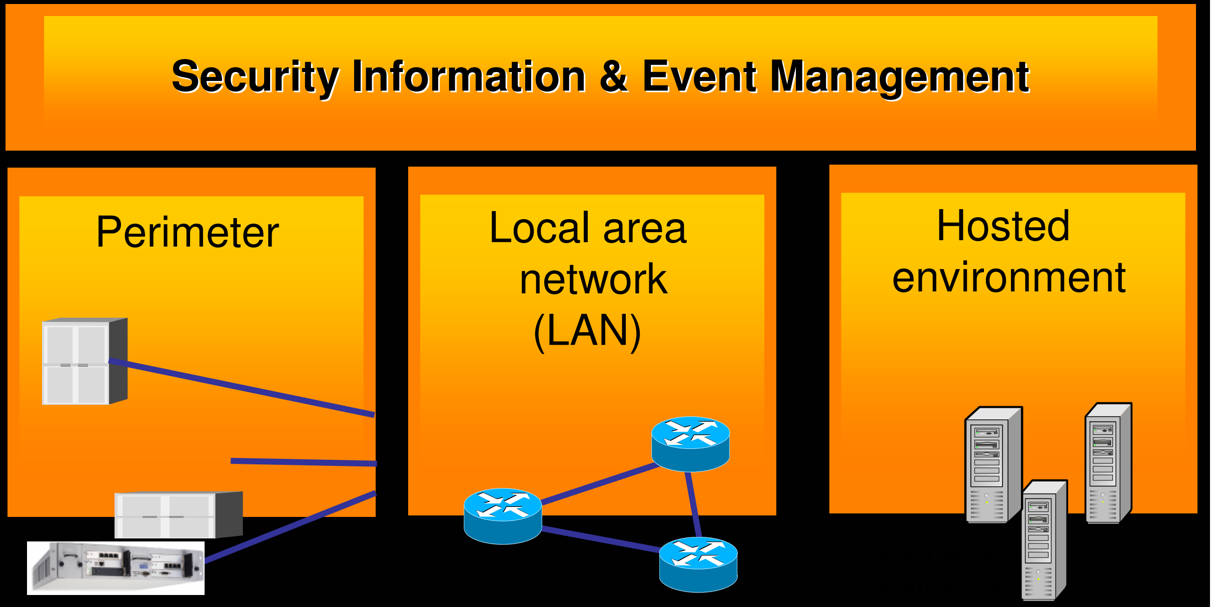
Comprehensive threat and vulnerability management across networks, servers and end-points

Goals

- Protect the enterprises through detection and management of network threats at the network core and perimeter
- Prevent intrusions and protect all endpoints and host systems
- Centrally manage and monitor security operations.
- Investigate and respond to security events

IBM solutions

- Tivoli Security Information and Event Manager
- ISS Proventia Appliances



- Intrusion prevention
- Firewall
- Universal threat management

- Intrusion prevention
- Anomaly detection service
- Vulnerability management
- Remediation
- Compliance and risk management
- Vulnerability protection service

- Host protection (server and desktop)
- Layer 4 – 7 protection (content, URL, Web)

Analyst Accolades

	Title	2006/7 Status
Gartner	ISS Network Security, Firewalls and Managed Services	Leader
FROST & SULLIVAN	Identity Management (TIM , TAM, FIM, TDI, TDS)	Leader
FORRESTER	Wave: User Account Provisioning (TIM)	Leader
FORRESTER	Wave: Enterprise Security Information Management (Consul inSight)	Leader
Gartner	MQ: User Provisioning (TIM)	Leader
Gartner	MQ: Security Information & Event Management (TSOM, Consul InSight)	Challenger
Gartner	MQ: Web Access Management (TAM)	Leader
FROST & SULLIVAN	Managed Security Services (Marketshare)	Leader
IDC *Analyze the Future*	Marketshare: Identity and Access Management	Ranked #1

Resource Center

CCR2 Newsletter Article

- http://www.ibm.com/software/tivoli/features/ccr2/ccr2-2007-09/innovative-mainframe.html

zSecure data sheets, solution sheets, and white papers

- http://www-306.ibm.com/software/tivoli/products/zsecure/

zSecure Manuals

- http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc/welcome.htm

Redbooks & Redpapers

- http://www.redbooks.ibm.com/

IBM Tivoli Security and System z Redpaper

- http://www.redbooks.ibm.com/redpieces/abstracts/redp4355.html?Open