Leveraging the Mainframe - Audit and Compliance requirements

Joe Anthony
Security, Risk and Compliance Product Management
jca@us.ibm.com

Agenda

- **Compliance**
- **The IBM Security Framework**
- **Security, Risk and Compliance Management**
  - People and Identity Solutions
  - Data and Information Solutions
  - Application and Process Solutions
  - Network, Server, and End-point Solutions
  - Physical Infrastructure Solutions
- **Security Landscape**

Compliance Challenges

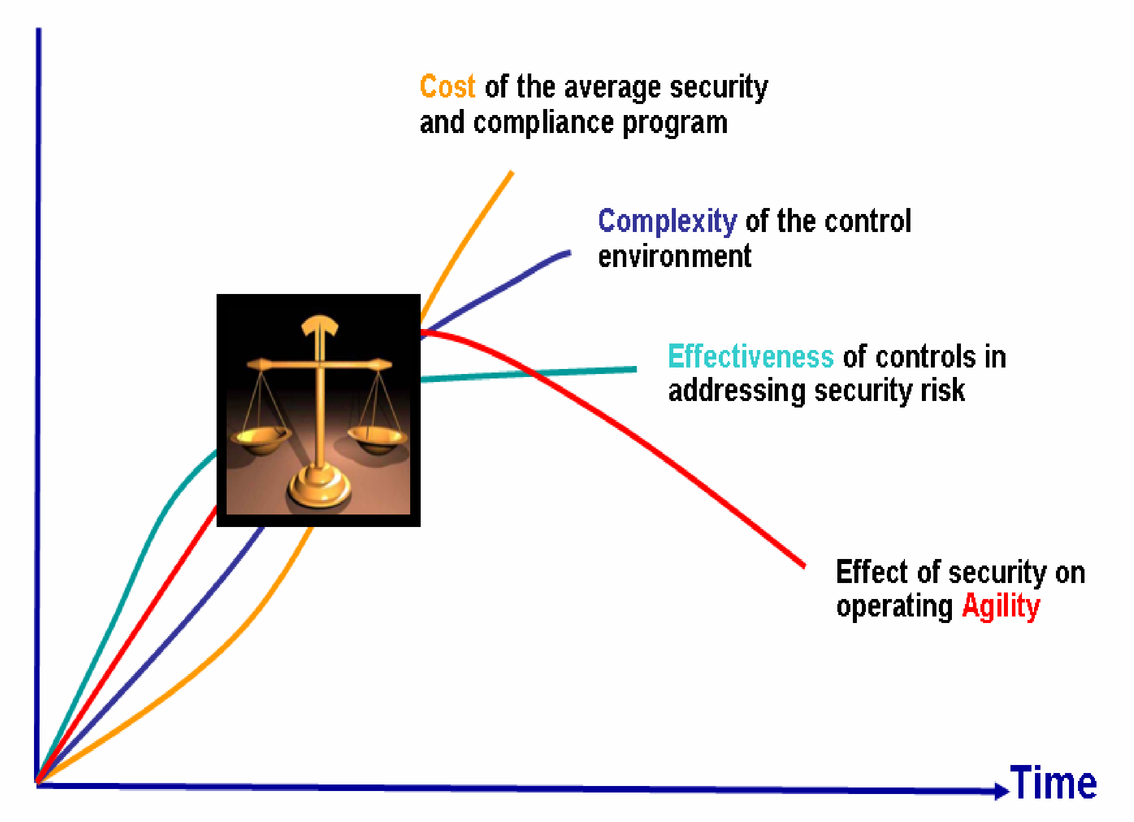
Companies face increased pressure to achieve and maintain compliance – all with limited resources, time and budget.

- **“Through 2010, public companies that do not adopt a compliance management architecture will spend 50 percent more annually than their peers to achieve Sarbanes-Oxley compliance.”**
  - Gartner Group
- **“As companies look to make SOX compliance more efficient and repeatable and improve controls reliability, technology is becoming a key enabler of these efforts…Corporate governance, including Sarbanes-Oxley, remains one of the top five priorities for North American IT organizations...”**
  - Forrester Research

The Pragmatic Approach to Risk Management

Manage Cost, Decrease Complexity, Improve Effectiveness, Assure Agility

– Focuses on finding a balance between effective security and cost



The Axiom…

Never spend $100 on a fence to protect a $10 horse

How PCI Compliance Works

- Twelve basic requirements supported by more detailed sub requirements

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

- Audits to achieve certification
- Penalties and incentives can be substantial

PCI Security Standard Council

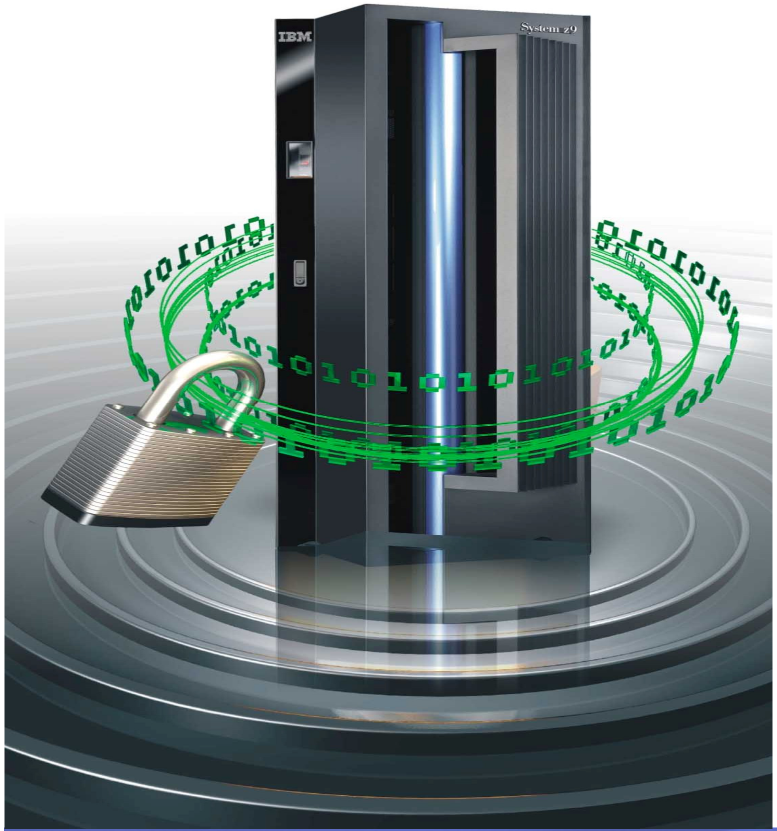
www.pcisecuritystandards.org

PCI – How System z Can Help

Mitigating the risk of security breaches

Helping to reduce the complexity and cost of enterprise security solutions

Robust security to enable consolidation

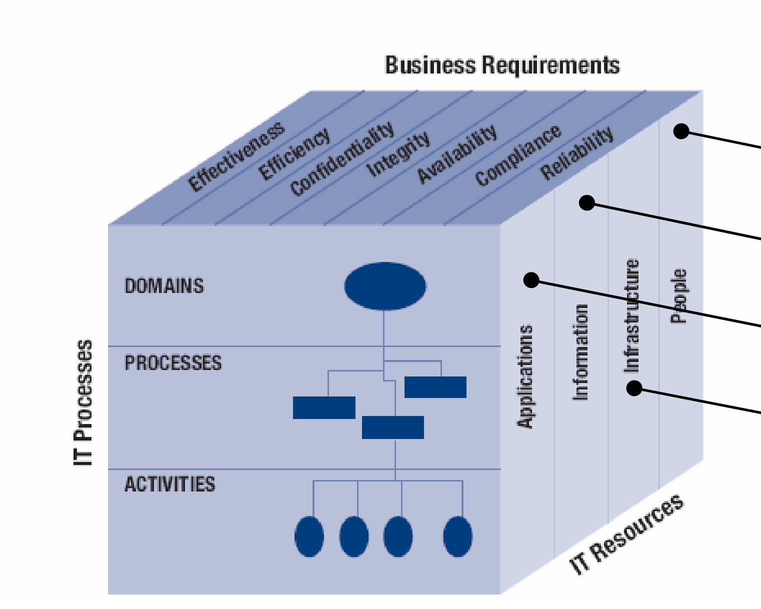


- Security-rich holistic design to help protect system from malware, viruses, and insider threats
- Highly secure network security
- System z as a central repository for sensitive data
- Minimize proliferation of sensitive data throughout enterprise
- Encryption solutions to help secure data from theft or compromise
- Leverage the mainframe security policies and processes that have been developed over many years in your enterprise
- Allowing you to address compliance needs with more confidence

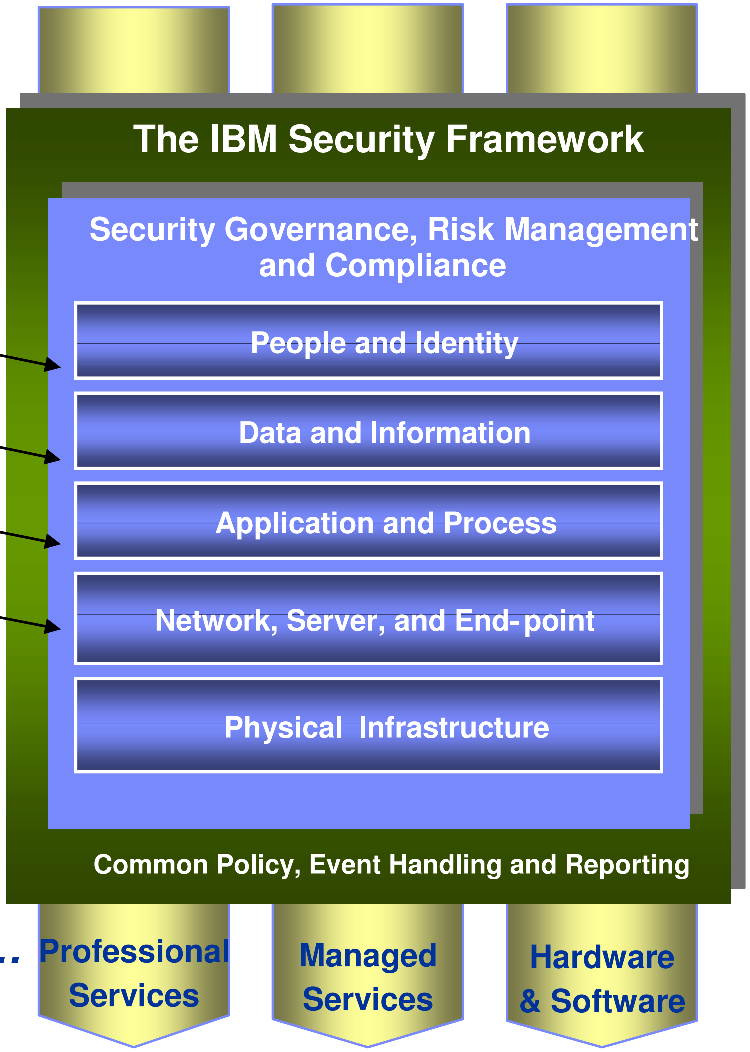
Security Landscape

Control Objectives for Information and related Technology (COBIT)

Figure 15—The COBIT Cube



Source: IT Governance Institute, Control Objectives for Information and related Technology (COBIT) 4.0.


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

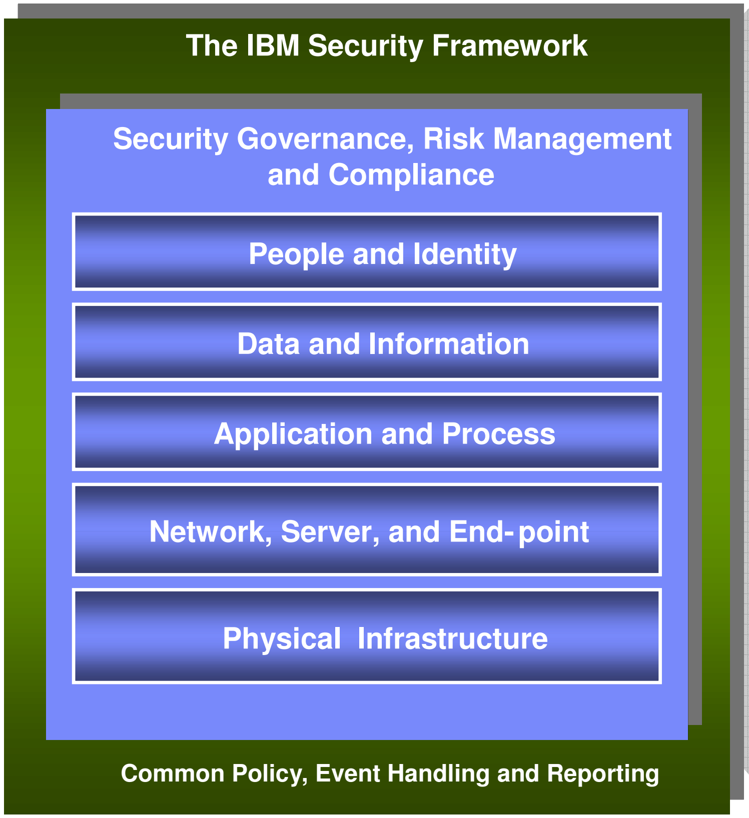
Common Policy, Event Handling and Reporting

Delivered by… Professional Services | Managed Services | Hardware & Software

Security, Risk and Compliance Management

Enabling collaboration while mitigating risk

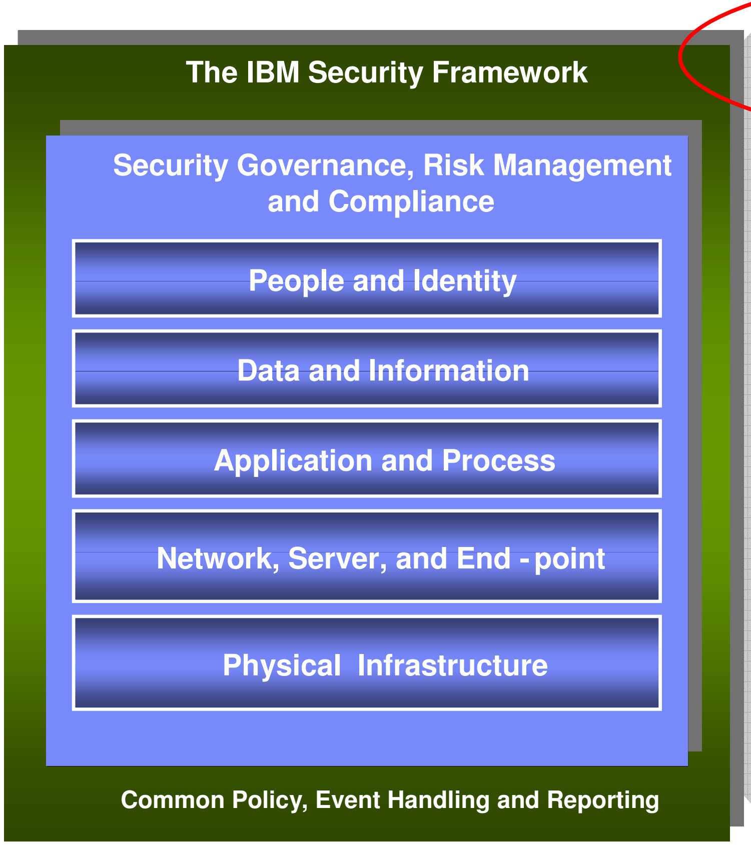
- **IBM delivers:**
  - Timely **visibility** into business continuity risks and compliance posture
  - More effective **control** over utilization of sensitive business assets
  - Efficient **automation** of the identification and remediation of vulnerabilities and the addressing of compliance mandates


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, Risk and Compliance Management

Enabling collaboration while mitigating risk


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

IBM Security Solutions

- 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

Tivoli Compliance Insight Manager

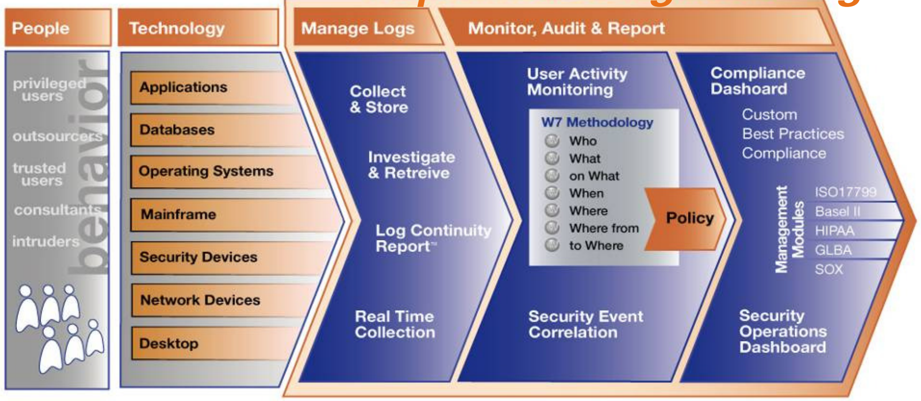
Monitoring and Assessing Compliance:

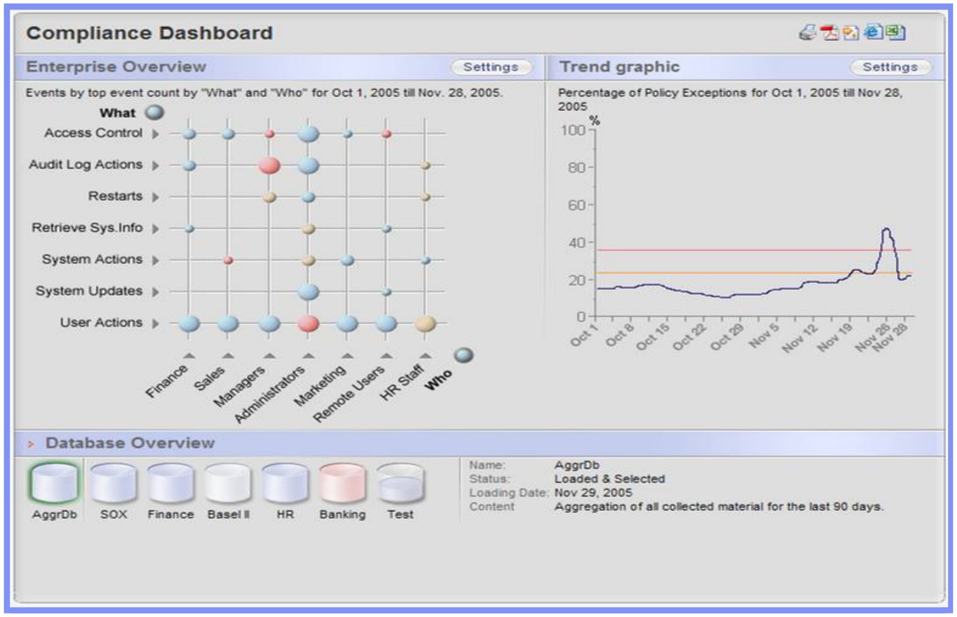
Tivoli Compliance Insight Manager provides an enterprise security compliance dashboard with in-depth privileged user **monitoring** capabilities, all powered by a comprehensive log and audit trail collection capability

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**

Tivoli Compliance Insight Manager





Compliance Dashboard

Enterprise Overview

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

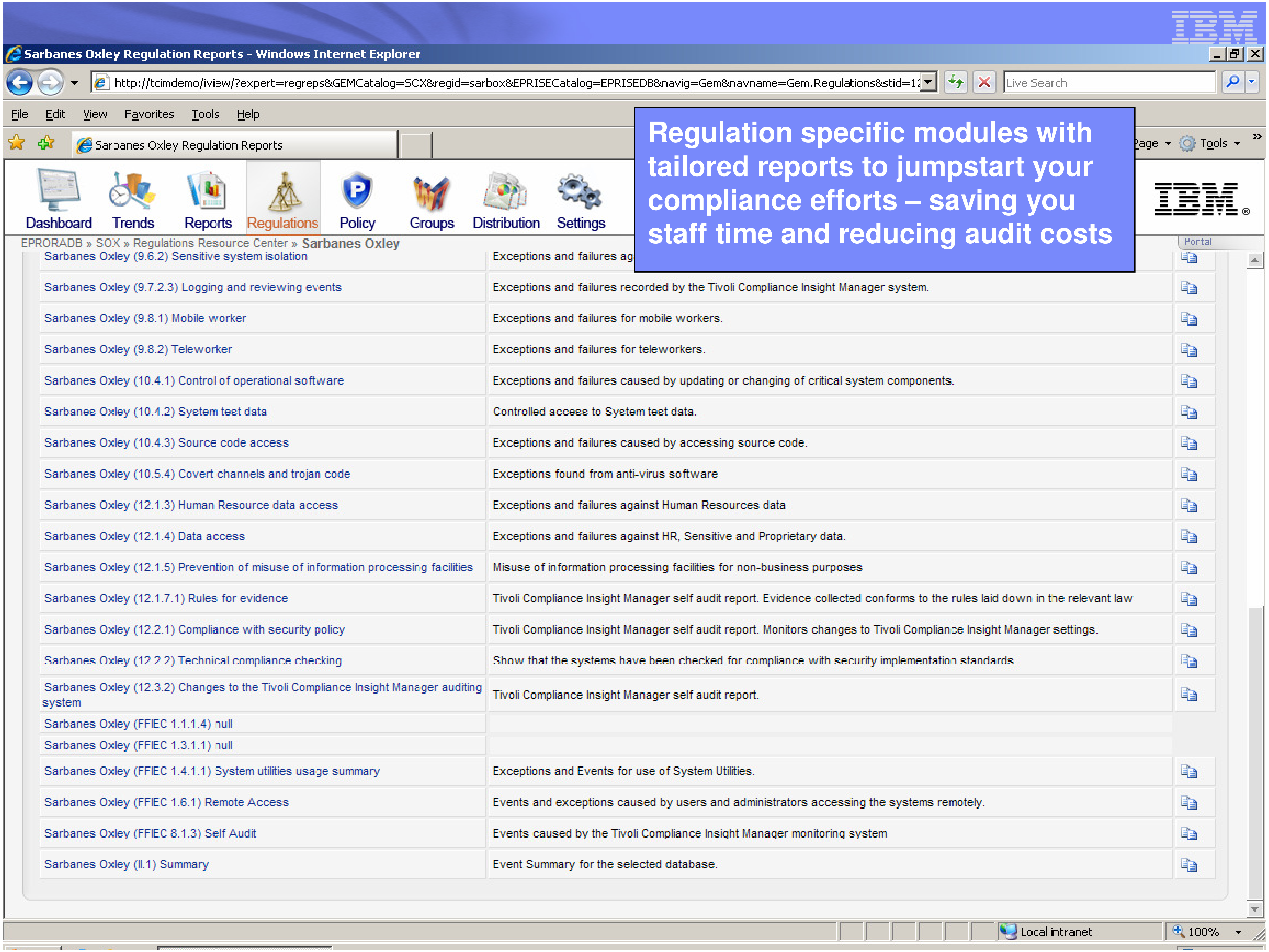
Trend graphic

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.

Regulation specific modules with tailored reports to jumpstart your compliance efforts – saving you staff time and reducing audit costs


Sarbanes Oxley Regulation Reports - Windows Internet Explorer
http://tcimdemo/iview/?expert=regreps&GEMCatalog=SOX&regid=sarbox&EPRISECatalog=EPRISEDB&navig=Gem&navname=Gem.Regulations&stid=1
Live Search
File Edit View Favorites Tools Help
Sarbanes Oxley Regulation Reports
Page Tools
Dashboard
Trends
Reports
Regulations
Policy
Groups
Distribution
Settings
IBM
Portal
Local intranet
100%

EPRORADB » SOX » Regulations Resource Center » Sarbanes Oxley

Sarbanes Oxley (9.6.2) Sensitive system isolation	Exceptions and failures ag
Sarbanes Oxley (9.7.2.3) Logging and reviewing events	Exceptions and failures recorded by the Tivoli Compliance Insight Manager system.
Sarbanes Oxley (9.8.1) Mobile worker	Exceptions and failures for mobile workers.
Sarbanes Oxley (9.8.2) Teleworker	Exceptions and failures for teleworkers.
Sarbanes Oxley (10.4.1) Control of operational software	Exceptions and failures caused by updating or changing of critical system components.
Sarbanes Oxley (10.4.2) System test data	Controlled access to System test data.
Sarbanes Oxley (10.4.3) Source code access	Exceptions and failures caused by accessing source code.
Sarbanes Oxley (10.5.4) Covert channels and trojan code	Exceptions found from anti-virus software
Sarbanes Oxley (12.1.3) Human Resource data access	Exceptions and failures against Human Resources data
Sarbanes Oxley (12.1.4) Data access	Exceptions and failures against HR, Sensitive and Proprietary data.
Sarbanes Oxley (12.1.5) Prevention of misuse of information processing facilities	Misuse of information processing facilities for non-business purposes
Sarbanes Oxley (12.1.7.1) Rules for evidence	Tivoli Compliance Insight Manager self audit report. Evidence collected conforms to the rules laid down in the relevant law
Sarbanes Oxley (12.2.1) Compliance with security policy	Tivoli Compliance Insight Manager self audit report. Monitors changes to Tivoli Compliance Insight Manager settings.
Sarbanes Oxley (12.2.2) Technical compliance checking	Show that the systems have been checked for compliance with security implementation standards
Sarbanes Oxley (12.3.2) Changes to the Tivoli Compliance Insight Manager auditing system	Tivoli Compliance Insight Manager self audit report.
Sarbanes Oxley (FFIEC 1.1.1.4) null	
Sarbanes Oxley (FFIEC 1.3.1.1) null	
Sarbanes Oxley (FFIEC 1.4.1.1) System utilities usage summary	Exceptions and Events for use of System Utilities.
Sarbanes Oxley (FFIEC 1.6.1) Remote Access	Events and exceptions caused by users and administrators accessing the systems remotely.
Sarbanes Oxley (FFIEC 8.1.3) Self Audit	Events caused by the Tivoli Compliance Insight Manager monitoring system
Sarbanes Oxley (II.1) Summary	Event Summary for the selected database.

IBM Health Checker for z/OS

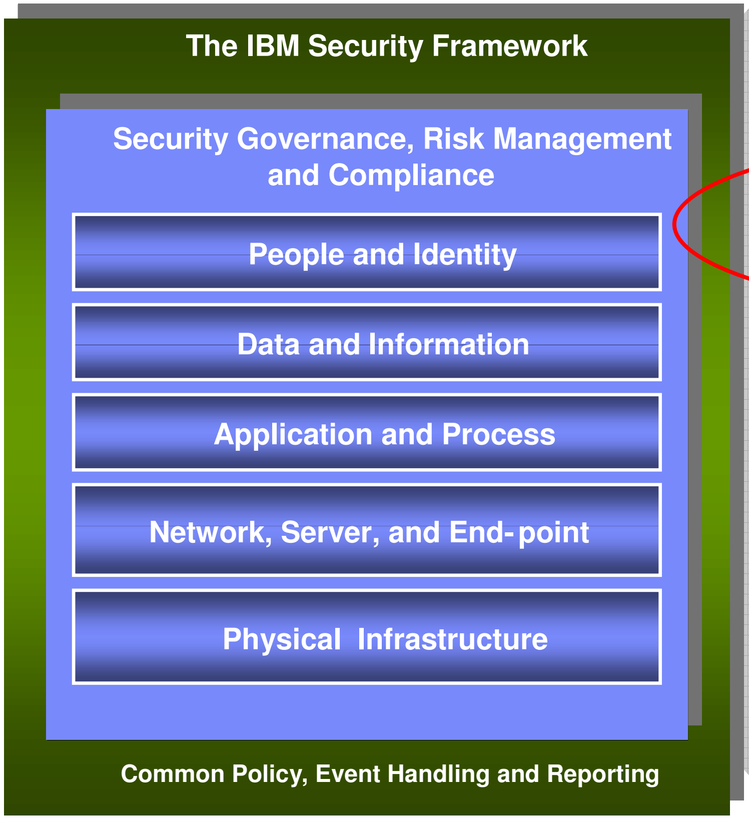
Identifies potential configuration problems

Identifies changes in configuration values that occur over the life of an IPL before they can cause damage

- **Health checker consists of:**
  - A framework to manage registration, scheduling, processing, reporting of health checks
  - Checking mechanism that evaluates settings
  - Extensible - authored by IBM, ISVs, or users.
- **Health Checker Framework improvements:**
  - Support for defining new checks in Parmlib
- **More health checks:**
  - GRS
  - Communications Server
  - DFSMS
- **z/OS Communications Server GUI improvements:**
  - Support for QoS and IDS policy configuration
  - Configure IPSec, AT - TLS, QoS, and IDS policy via a consistent user interface

Security, Risk and Compliance Management

Enabling collaboration while mitigating risk



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

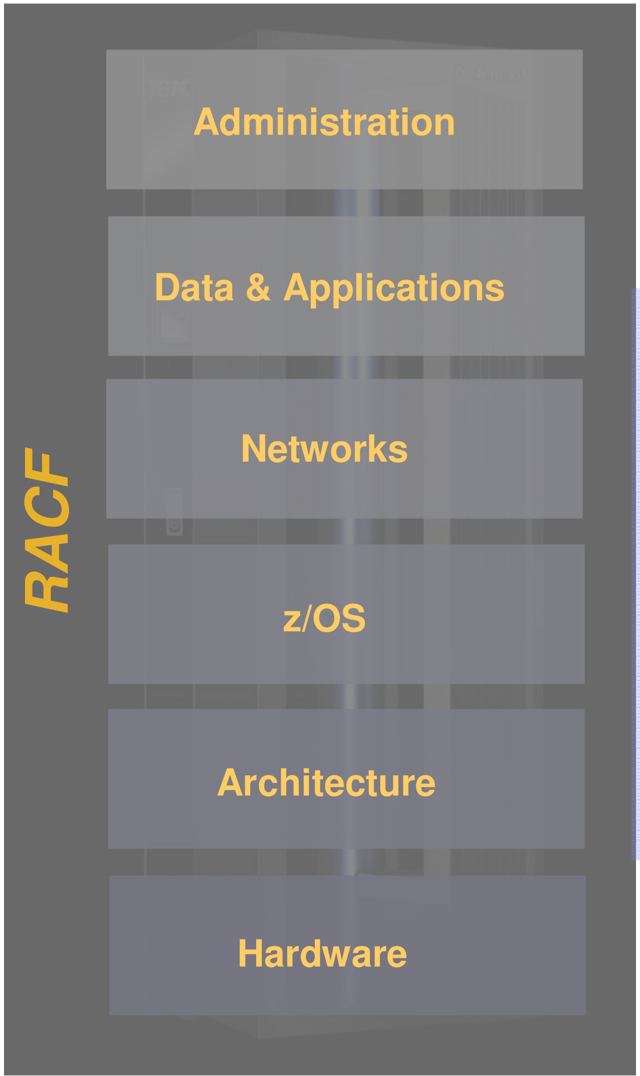
Common Policy, Event Handling and Reporting

IBM Security Solutions

- **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

Resource Access Control Facility (RACF)

The backbone of mainframe security



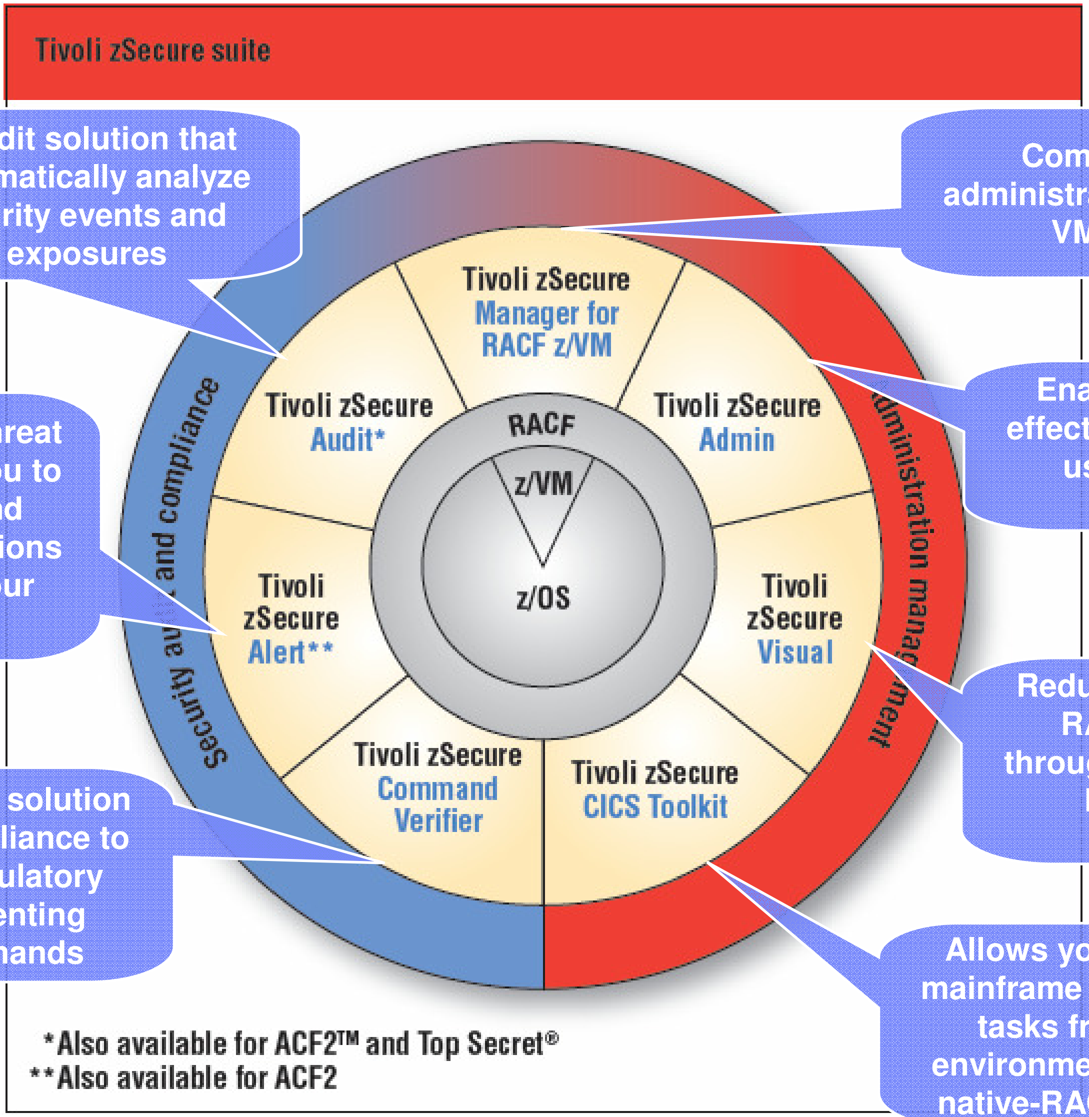
Authentication
Authorization
Administration
Auditing

Enables application and database security without modifying applications

Can reduce security complexity and expense:

- **Central security process that is easy to apply to new workloads or as user base increases**
- **Tracks activity to address audit and compliance requirements**

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

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 allowing you to monitor intruders and identify mis-configurations that could hamper your compliance efforts

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

Note: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

Tivoli Identity Manager for z/OS

Policy Based Identity Management

Provision users across the enterprise

Value of Tivoli Identity Manager

- Automated, policy-based identity management
- Provides workflow for automating the approval process
- Allows for self service enrollment and password management
- Keeps an audit of user management operations
- Reports on out-of-policy changes

Identity information and management are mission-critical

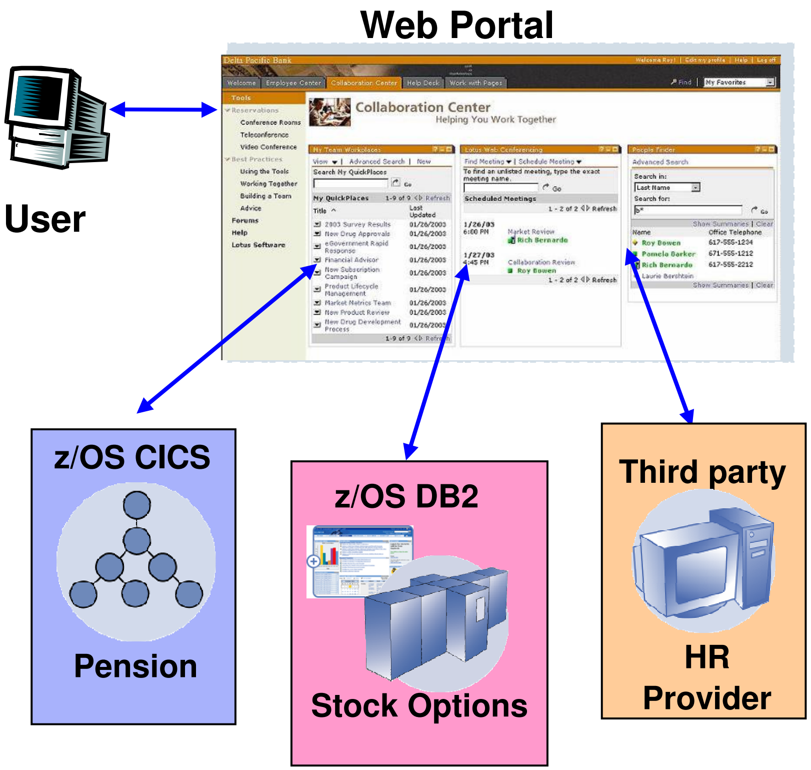
Advantages of TIM on z/OS

- Highly available and resilient
- Highly secure
- Scalable
- Integrates with z/OS RACF
- Complements Tivoli zSecure

A single hub for provisioning users

Tivoli Federated Identity Manager for z/OS

- Security integration for web services that use z/OS CICS or other z/OS subsystems
- Protect z/OS-hosted web services using z/OS security services
- Preserve identity of the requesting user for access control and audits
- Use z/OS auditing to assist regulatory compliance
- Improve integration and simplify the user experience



Delta Pacific Bank

Welcome Roy! | Edit my profile | Help | Log off

Welcome | Employee Center | Collaboration Center | Help Desk | Work with Pages

Find | My Favorites

Tools

Reservations
Conference Rooms
Teleconference
Video Conference
Best Practices
Using the Tools
Working Together
Building a Team
Advice
Forums
Help
Lotus Software

Collaboration Center
Helping You Work Together

My Team Workplaces

View | Advanced Search | New

Search My QuickPlaces Go

My QuickPlaces 1-9 of 9 Refresh

Title	Last Updated
2003 Survey Results	01/26/2003
New Drug Approvals	01/26/2003
eGovernment Rapid Response	01/26/2003
Financial Advisor	01/26/2003
New Subscription Campaign	01/26/2003
Product Lifecycle Management	01/26/2003
Market Metrics Team	01/26/2003
New Product Review	01/26/2003
New Drug Development Process	01/26/2003

1-9 of 9 Refresh

Lotus Web Conferencing

Find Meeting | Schedule Meeting

To find an unlisted meeting, type the exact meeting name. Go

Scheduled Meetings 1 - 2 of 2 Refresh

1/26/03 6:00 PM	Market Review Rich Bernardo
1/27/03 4:45 PM	Collaboration Review Roy Bowen

1 - 2 of 2 Refresh

People Finder

Advanced Search

Search in: Last Name

Search for: b* Go

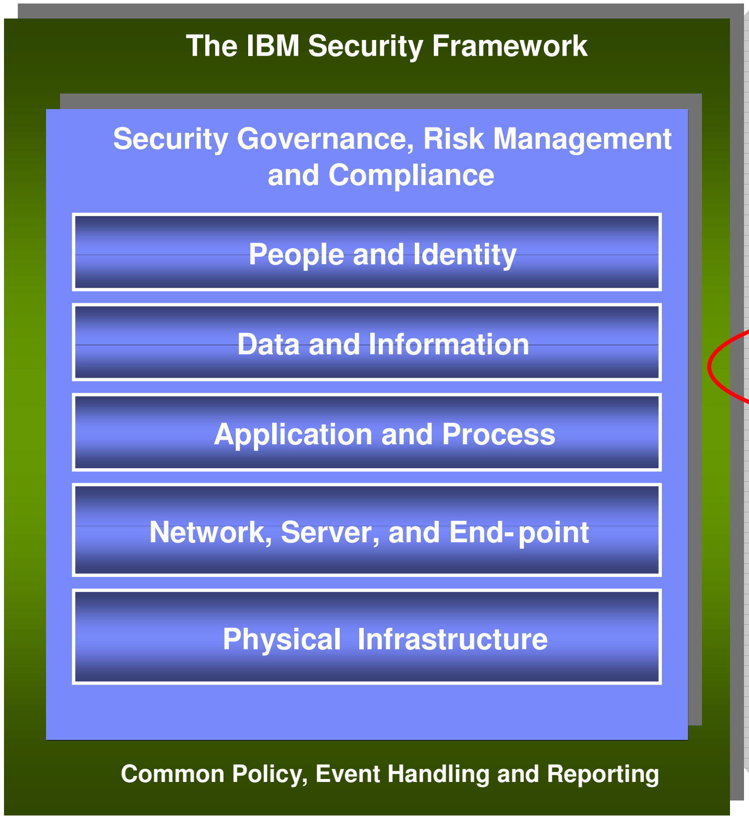
Show Summaries | Clear

Name	Office Telephone
Roy Bowen	617-555-1234
Pamela Barker	671-555-1212
Rich Bernardo	617-555-2212
Laurie Bershtein	

Show Summaries | Clear

Security, Risk and Compliance Management

Enabling collaboration while mitigating risk


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

IBM Security Solutions

- **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

DB2, IMS and IBM Data Encryption on System z

Protecting sensitive and confidential data

Key Database Capabilities

- **Provides access control to DB2/IMS resources via DB2/IMS / RACF Interface including:**
  - Resource (plan/package/table) authorization
  - Role based security (with DB2 v9, IMS v9/10 and RACF 1.8)
    - Network Trusted Context
    - Database Roles
  - MLS - Row Level Security (with DB2 v8, IMS v9/10 and RACF 1.7)
- **Provides encryption support via SQL in V8**
- **Provides trace facility performance and functionality improvements**

Key Encryption Capabilities

- **Provides a single tool for encrypting both IMS and DB2 data**
- **Can be customized at the IMS segment level and at the row level for DB2.**
- **Uses hardware encryption for the fastest possible encryption**
- **Runs as an EDITPROC**
- **Supports either clear key or secure key**
- **Exploits zSeries and S/390 Crypto Hardware features, which results in low overhead encryption/decryption**
- **Data is protected using encryption algorithms approved by the U.S. National Institute of Science and Technology**

DB2 Audit Management Expert / IMS Audit Management Expert

Value

- Helps maintain data compliance required by government and industry regulations.
- Frees up valuable IT staff resources by allowing auditors to participate in data auditing activities with less DBA involvement.
- Does not require auditors to be privileged users on the system they are auditing so database security is preserved,
- Eliminates the manual auditing processes that can be time consuming and error prone.
- Does not require auditors to log into DB2/IMS and does not permit them to directly manipulate any DB2/IMS resource
- Where a significant auditing exposure is suspected, DB2 Audit Management Expert allows an authorized auditor to investigate the exposure by reviewing what data has been changed in the system.

Key Capabilities

- Selectively audits inserts, updates, deletes, and reads of DB2 and IMS systems
- Provides views of all reported activity on specific DB2 objects (such as read and change)
- Collects trace data in an audit repository, and then views, analyzes and generates reports on the data
- Supports an easy to use interface for both auditors, DBAs, and security administrators to work together to deliver accurate data for use in audit activity
- Offers a user-friendly administration interface that enables AME administrators to easily define AME entities such as users, groups and collection criteria.

Optim Data Solution

Software solution for application-aware database archiving, test data management and data masking critical to an organization's Enterprise Data Governance strategy.

Value

- Reduce risk associated with security breaches and protect the privacy of client & employee information
- Reduces operating costs related to Data Governance
- Secures and protects sensitive information
- Cost effectively manages storage costs related to data retention requirement

Key Capabilities

- **Database archiving** - manage and maintain application aware archives of business data for both packaged and custom database applications.
  - Provide fine grained control over which data is archived by applying user defined business rules
  - Help analysts assess how archives should be tiered to ensure decision makers can access the right business data objects at the right time.
- **Test data management** - Streamline total application testing and hardening processes with comprehensive capabilities for creating referentially-intact, right-sized test databases, quickly refreshing test environments and automating comparison of test results against baseline data
- **Data privacy** – Contextual, application-aware data masking capabilities enable organizations to substitute sensitive data with realistic and fully functional masked data, thereby protecting confidentiality, safeguarding customer loyalty and supporting compliance with privacy initiatives.

IBM Tivoli Key Lifecycle Manager v1.0

- **Transparent storage encryption key serving**
  - IBM encrypting tape – TS1120, TS1130, LTO gen 4
  - IBM encrypting disk *
  - Client reference implementation

- **Lifecycle functions simplify operation**
  - Notification of certificate expiry
  - Automated rotation of certificates
  - Automated rotation of groups of keys

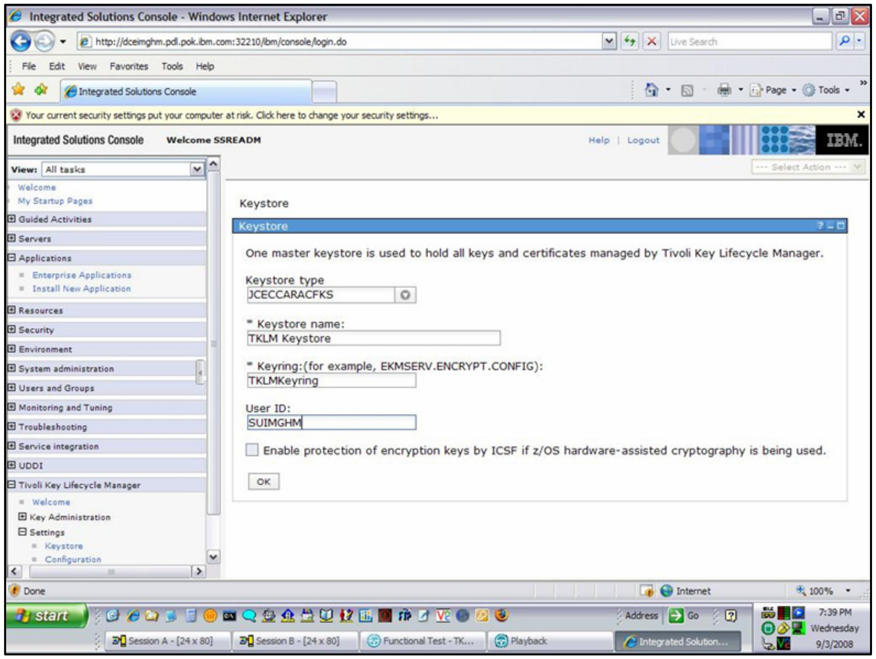
- **Designed to be easy to use**
  - Provide a Graphical User Interface
    - Initial configuration wizards

- **Easy backup and restore of TKLM files**
  - One button operation

- **Installer to simplify installation experience**
  - Simple to use install
  - Silent install option available

- **Highly secure**
  - Supports System z Hardware Security Module (HSM)

- **Platforms for v1**
  - z/OS 1.9 *
  - AIX 5.3 64 bit
  - Red Hat AS 4.0 x86 - 32 bit
  - Suse Linux 9.0 and 10 x86 - 32 bit
  - Solaris 10 Sparc -64 bit.
  - Windows Server 2003 - 32 bit.



Integrated Solutions Console - Windows Internet Explorer

http://dceimghm.pdl.pok.ibm.com:32210/ibm/console/login.do

Your current security settings put your computer at risk. Click here to change your security settings...

Integrated Solutions Console Welcome SSREADM

Keystore

One master keystore is used to hold all keys and certificates managed by Tivoli Key Lifecycle Manager.

Keystore type: JCECCARACFKS

* Keystore name: TKLM Keystore

* Keyring:(for example, EKMSERV.ENCRYPT.CONFIG): TKLMKeyring

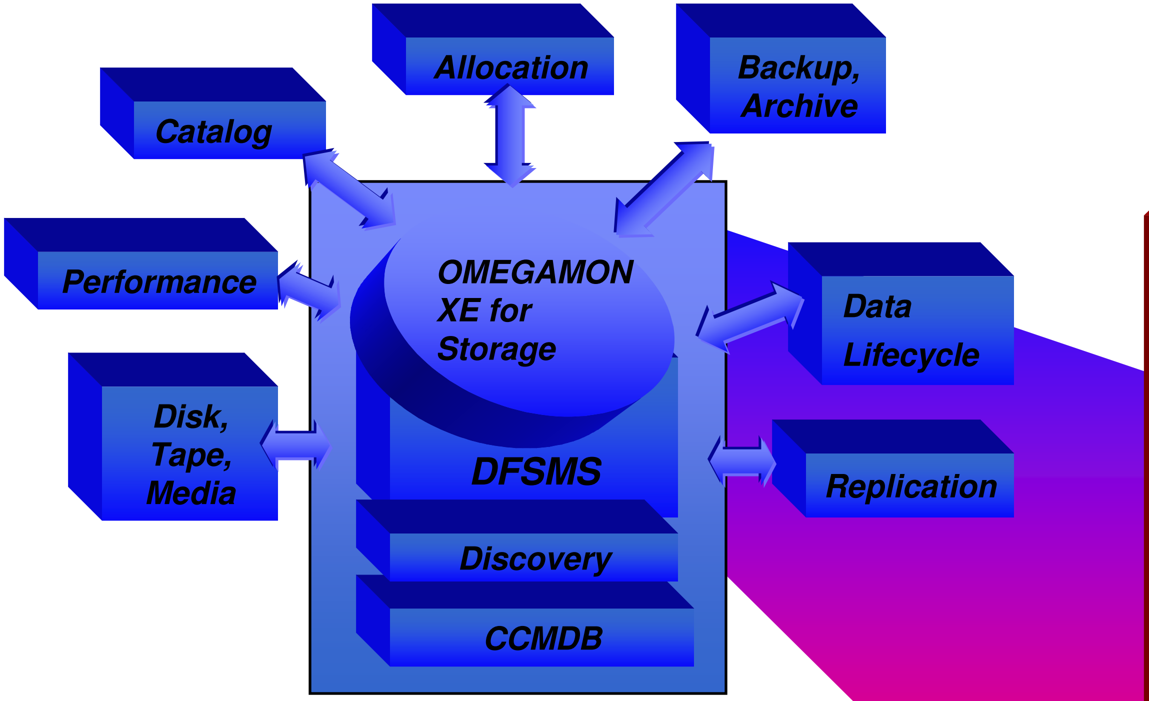
User ID: SUIMGHM

☐ Enable protection of encryption keys by ICSF if z/OS hardware-assisted cryptography is being used.

*Announced availability March 6, 2008 for z/OS and DS8000 support

IBM Storage Management Portfolio for System z Capabilities

Ensure rapid data recovery for compliance and auditability!



- ✓ ***Automation, Visibility, and Control of backup & recovery processes***
- ✓ ***Control use of storage devices more efficiently while governing data migration to tape, and catalog management***
- ✓ ***Audit and report on archiving – status, problems, take corrective action to ensure compliance with retention policy***
- ✓ ***Visibility to backup & recovery of both key data and key infrastructure files (e.g. ICF and Tape Catalogs)***

Infrastructure Management

- 🟥 IBM Tivoli OMEGAMON XE for Storage on z/OS
- 🟥 IBM Tivoli Advanced Catalog Managment for z/OS
- IBM Data Facility Product (DFSMSdfp)
- IBM Tivoli Tape Optimizer on z/OS
- IBM Removable Media Managers (DFSMSrmm, IRMM)
- Softek Transparent Data Migration Facilities (TDMF, LDMF)
- IBM Transactional VSAM (DFSMStvs)
- IBM Tivoli Allocation Optimizer for z/OS

Allows administrators to manage data and a broad range of devices, such as switches, tape, removable media and storage servers

Business Continuity

- IBM Data Set Services (DFSMSdss)
- IBM z/OS Global Mirror
- 🟥 IBM Backup and Restore Manager for z/VM
- 🟥 IBM Tivoli Advanced Backup and Recovery for z/OS
- IBM TotalStorage Productivity Center for Replication for System z

Minimizes operational risk by ensuring business data meets backup and recovery objectives

Lifecycle and Retention

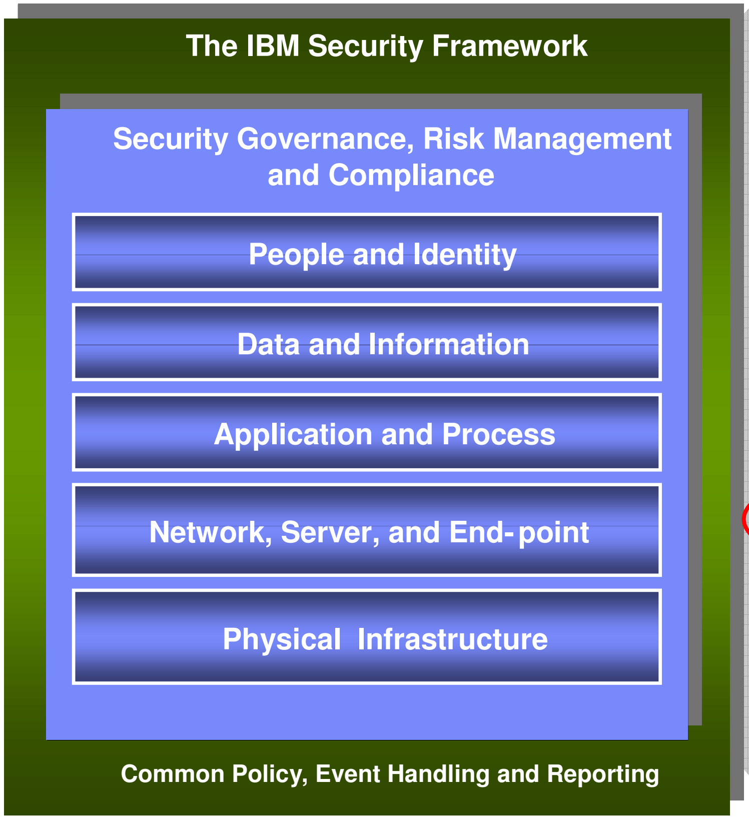
- IBM Hierarchical Storage Manager (DFSMShsm)
- 🟥 IBM Tivoli Advanced Reporting for DFSMShsm
- IBM Tivoli Automated Tape Allocation Manager for z/OS
- 🟥 IBM Archive Manager for z/VM
- 🟥 IBM Tape Manager for z/VM
- 🟥 IBM Tivoli Advanced Audit for DFSMShsm

Helps control storage growth and control costs for data requiring long retention periods.

Legend: 🟥 Solution focus includes audit and compliance

Security, Risk and Compliance Management

Enabling collaboration while mitigating risk



The IBM Security Framework

Security Governance, Risk Management and Compliance

People and Identity

Data and Information

Application and Process

Network, Server, and End-point

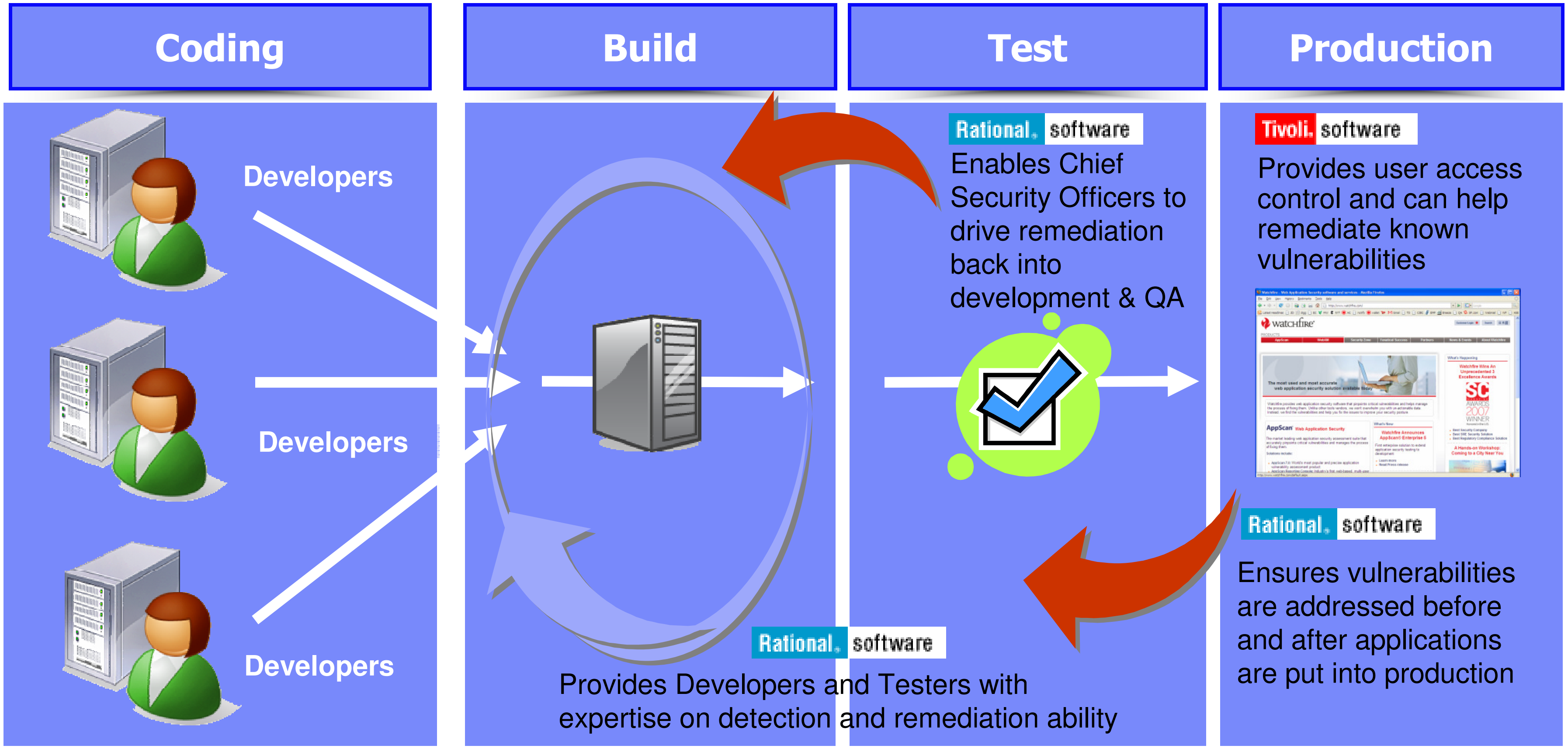
Physical Infrastructure

Common Policy, Event Handling and Reporting

IBM Security Solutions

- **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

Rational AppScan & IBM Tivoli provide security that spans the application lifecycle



Coding

Build

Test

Production

Rational software

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

Tivoli software

Provides user access control and can help remediate known vulnerabilities

Rational software

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

Rational software

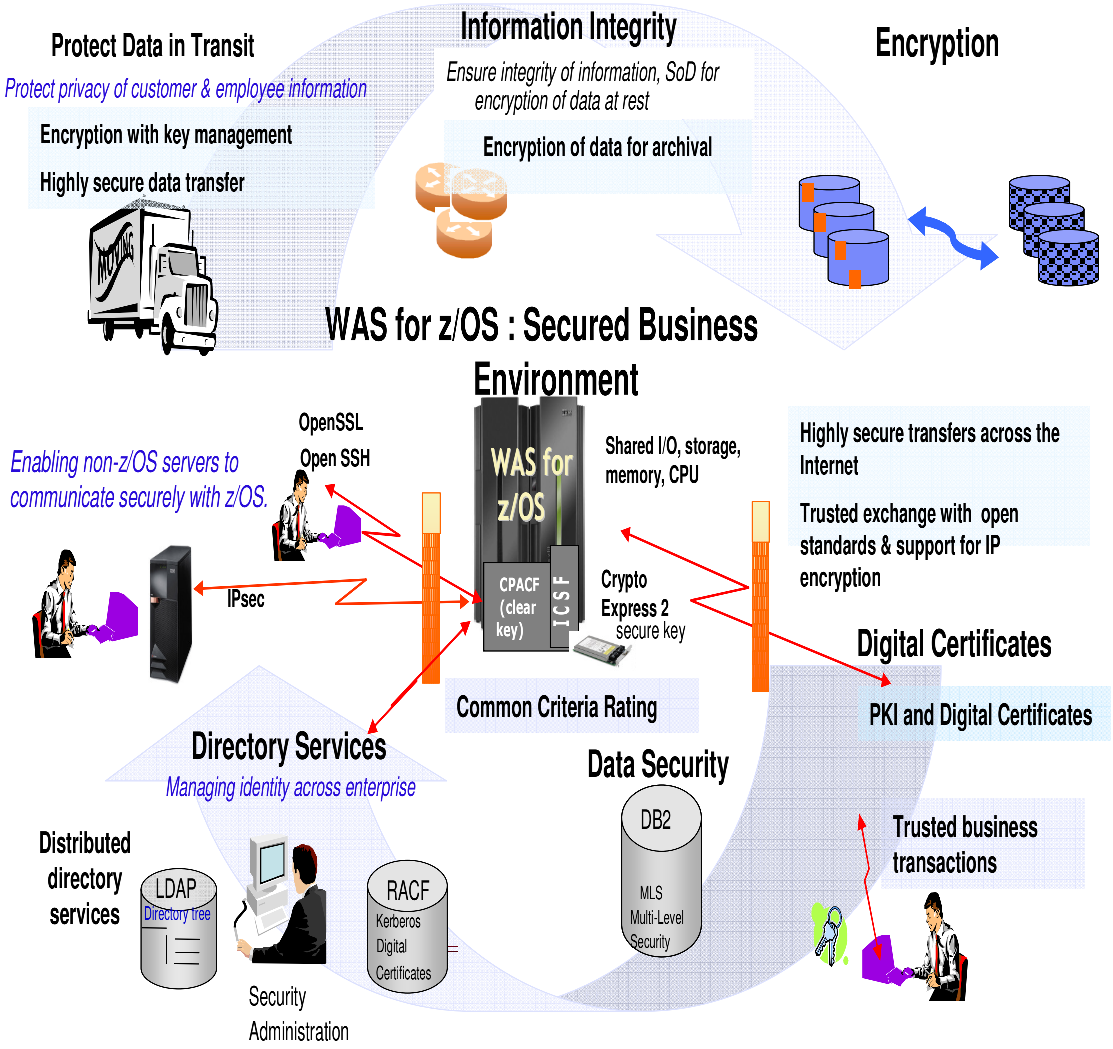
Provides Developers and Testers with expertise on detection and remediation ability

AppScan tests the application and RACF/Tivoli Access Manager secures access to them

WAS for z/OS Security Provides System and Data Integrity

WAS for z/OS v7 : Security benefits

- Tight integration of WebSphere and RACF via Security Authorization Facility (SAF)
  - Protects WAS7 Admin console using RACF and allows Applications to use their own Registry such as LDAP
- Simplified Compliance Certification and Analysis (SOX, HIPAA, etc)
- End user authentication for authorization and auditing throughout the architecture
- Security auditing records administrative actions and applications
- Kerberos Authentication And Single Sign-on



Protect Data in Transit

Protect privacy of customer & employee information

Encryption with key management

Highly secure data transfer

Information Integrity

Ensure integrity of information, SoD for encryption of data at rest

Encryption of data for archival

Encryption

WAS for z/OS : Secured Business Environment

Enabling non-z/OS servers to communicate securely with z/OS.

OpenSSL

Open SSH

IPsec

WAS for z/OS

CPACF (clear key)

ICSF

Shared I/O, storage, memory, CPU

Crypto Express 2

secure key

Highly secure transfers across the Internet

Trusted exchange with open standards & support for IP encryption

Digital Certificates

PKI and Digital Certificates

Common Criteria Rating

Directory Services

Managing identity across enterprise

Data Security

Distributed directory services

LDAP

Directory tree

Security Administration

RACF

Kerberos

Digital Certificates

DB2

MLS

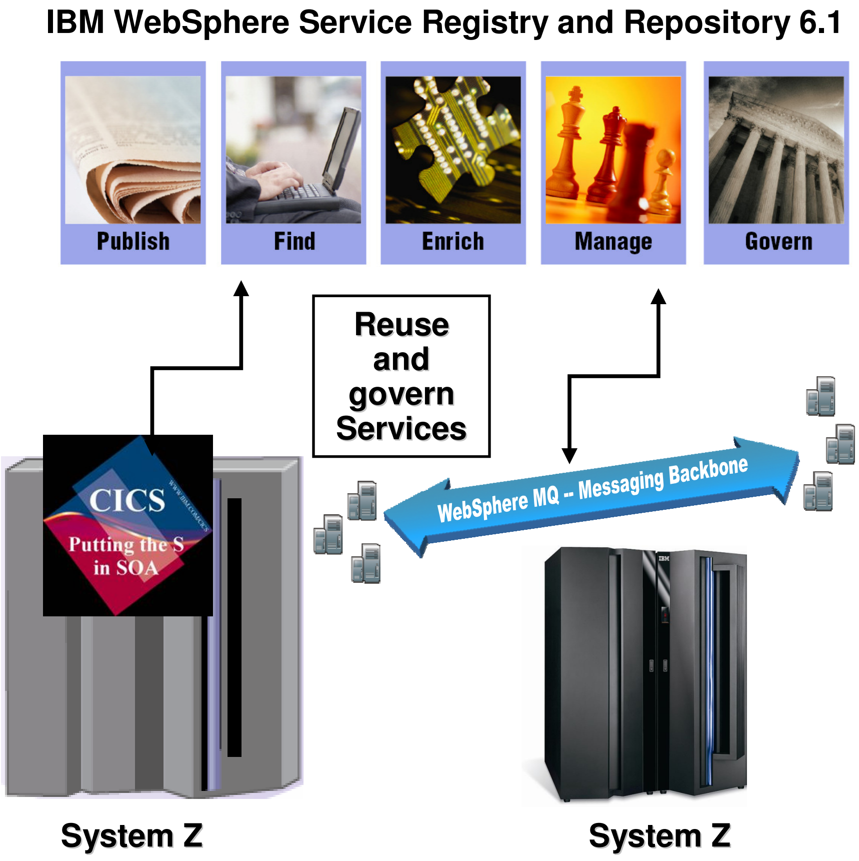
Multi-Level Security

Trusted business transactions

IBM WebSphere Service Registry and Repository (WSRR)

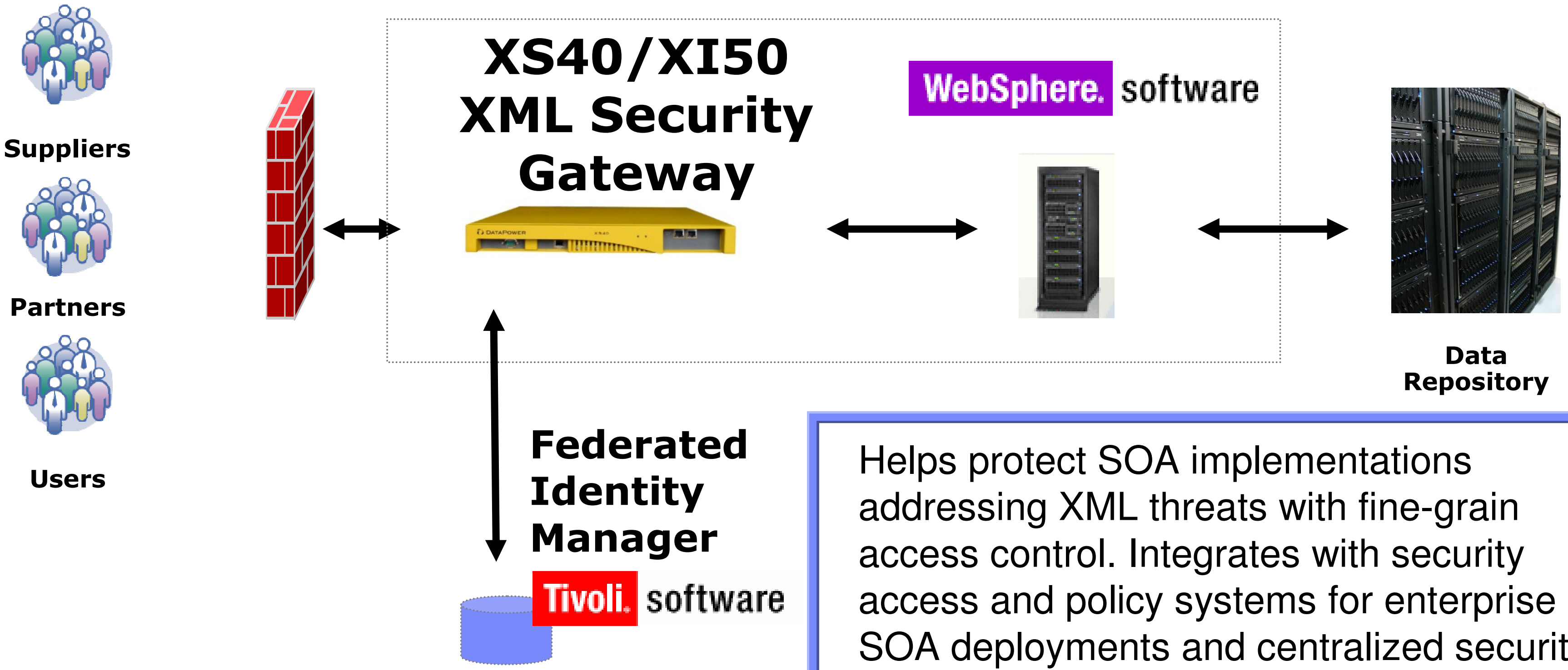
Enable governance of service-enabled CICS & MQ applications

- Raise the visibility of service-enabled CICS or MQ application by publishing it to WSRR
- Classify, describe, govern CICS or MQ service just like any other service in your SOA
- Manage the lifecycle of CICS or MQ services with versioning, approval, promotion, retirement, etc.
- Facilitate selection, invocation and monitoring of CICS or MQ services by other SOA applications
- It runs natively on zOS and zLinux


IBM WebSphere Service Registry and Repository 6.1
Publish
Find
Enrich
Manage
Govern
Reuse and govern Services
CICS
Putting the S in SOA
WebSphere MQ -- Messaging Backbone
System Z
System Z

DataPower: Defending SOA-based Environments

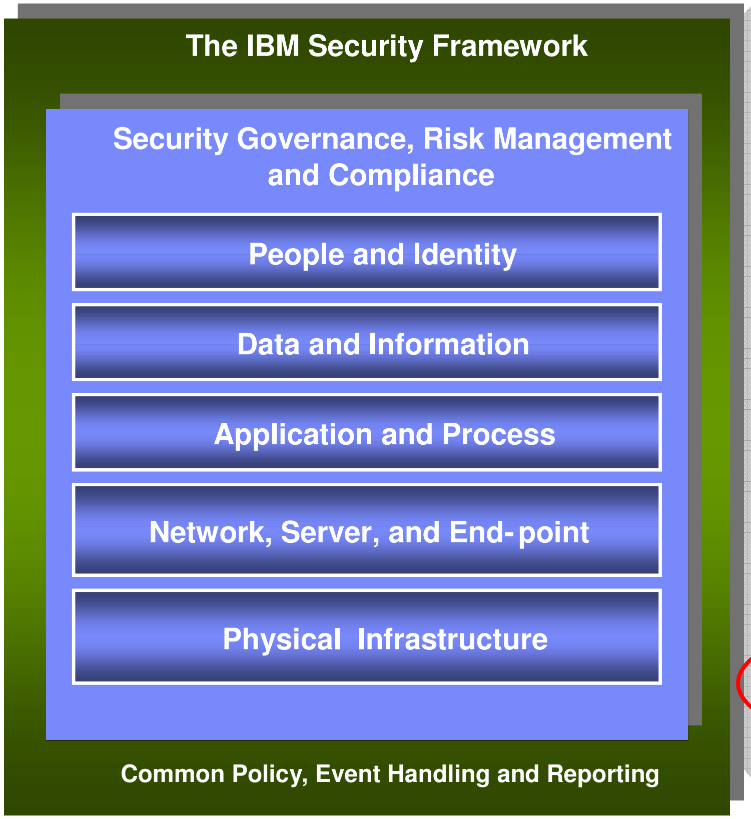
First line of defense to securely implement external web services. Secure once for many applications and aggregate user interactions.



Helps protect SOA implementations addressing XML threats with fine-grain access control. Integrates with security access and policy systems for enterprise SOA deployments and centralized security policy management

Security, Risk and Compliance Management

Enabling collaboration while mitigating risk



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

IBM Security Solutions

- **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

ISS Delivers Preemptive Security Products

- **IBM Proventia Management**
  - **Manage | Monitor | Measure**
- **IBM Proventia Network**
  - Intrusion Prevention
  - Vulnerability Management
  - Multi-Function Security
  - Behavioral Analysis
  - Mail Security
- **IBM Proventia Host**
  - Endpoint Protection
  - Server Protection
- **IBM Site Protector**

Internet Security Systems
proventia network
Intrusion Prevention System
Internet Security Systems
proventia network
Intrusion Prevention System
proventia network
proventia network

Intrusion Detection for z/OS

Communication Server for z/OS

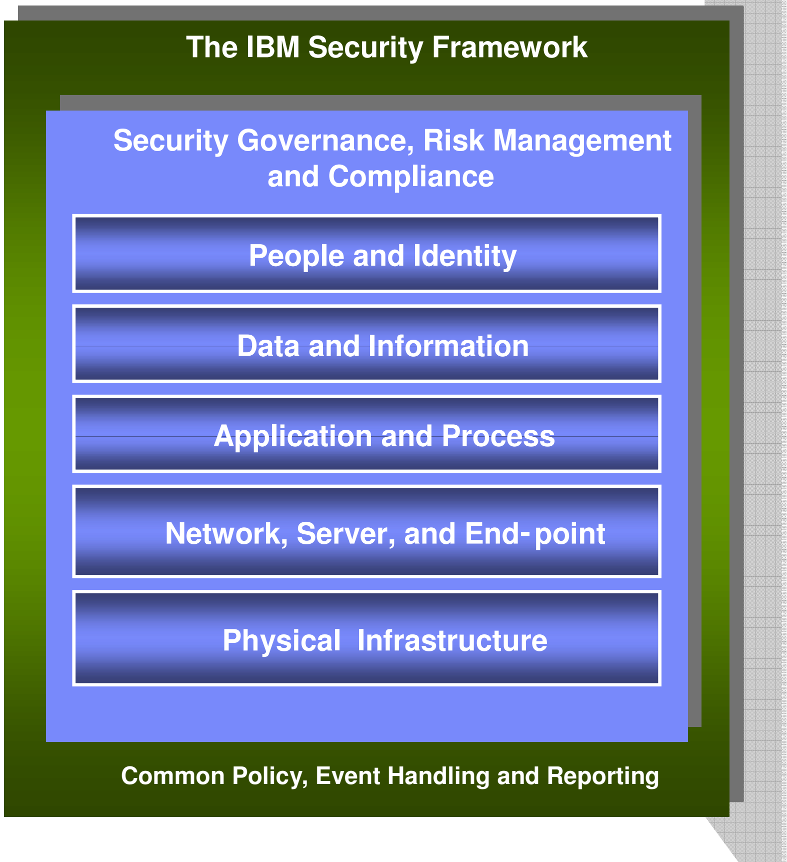
- **Offers mainframe network security**
- **Enables SNA and TCP/IP applications to communicate with partner applications and users on the same or different systems.**
- **Protects sensitive data and the operation of the TCP/IP stack on z/OS. It Provides the following services:**
  - IPSEC/ VPN
  - Intrusion Detection Services
  - TLS/SSL enablement for key applications
    - FTP client and server
    - TN3270 server
  - Kerberos5 and GSSAPI support is provided for the following applications
    - FTP client and server
    - Unix rshd server
    - Unix System Services telnet server (supports only Kerberos5)

Netview for z/OS

- **Automated response to intrusion:**
  - Scans
  - Attacks
  - Traffic regulation for TCP connections and UDP receive queues
- **Send an e-mail, issue a message, generate an alert or Tivoli Enterprise Console event**
- **Issue UNIX, NetView, or z/OS commands**
  - Gather more data
  - Take action, such as close the port
- **Generate a report in response to an intrusion.**

Security, Risk and Compliance Management

Enabling collaboration while mitigating risk



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

Example IBM Security Solutions

SECURITY COMPLIANCE

- GBS Assessment Consulting
- Tivoli Compliance Insight Manager
- ISS Assessment and Managed Services
- IBM Health Checker for z/OS

IDENTITY & ACCESS

- RACF
- Tivoli zSecure Suite
- Tivoli Identity, Federated and Access Management Suite

DATA SECURITY

- DB2, IMS and IBM Data Encryption on System z
- DB2 Audit Mgmt. Expert and IMS Audit Mgmt. Expert
- Tivoli Key Lifecycle Manager
- Optim Data Solution Suite
- IBM zStorage Solutions

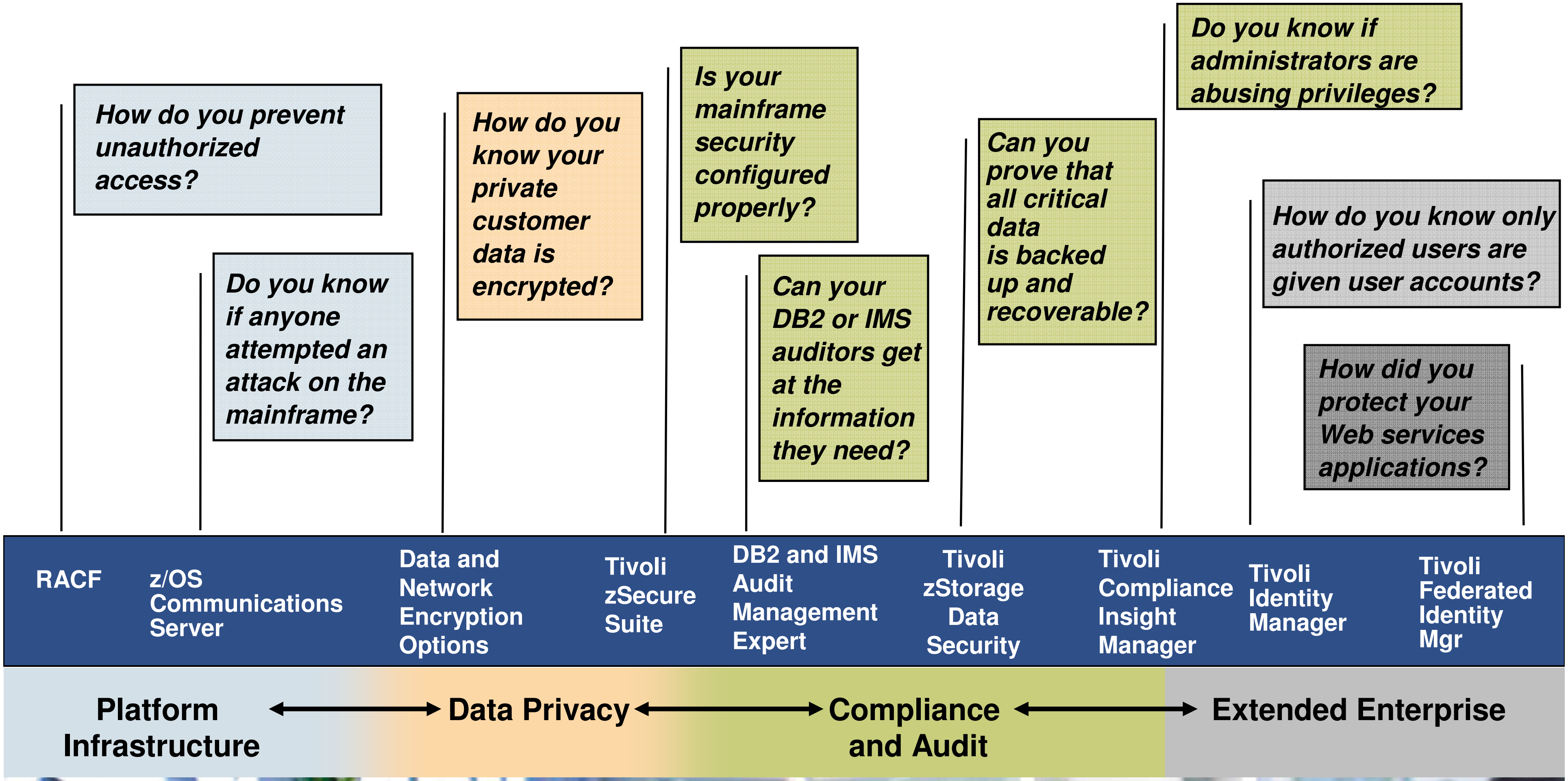
APPLICATION SECURITY

- Rational AppScan
- WebSphere DataPower
- WebSphere Service Registry and Repository
- WebSphere MQ File Transfer

• INFRASTRUCTURE SECURITY

- ISS Preemptive Security Solutions
- Tivoli Security Information and Event Management
- Intrusion Detection for z/OS

Questions auditors might ask:



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?

Is your mainframe security configured properly?

Can your DB2 or IMS auditors get at the information they need?

Can you prove that all critical data is backed up and recoverable?

Do you know if administrators are abusing privileges?

How do you know only authorized users are given user accounts?

How did you protect your Web services applications?

RACF

z/OS Communications Server

Data and Network Encryption Options

Tivoli zSecure Suite

DB2 and IMS Audit Management Expert

Tivoli zStorage Data Security

Tivoli Compliance Insight Manager

Tivoli Identity Manager

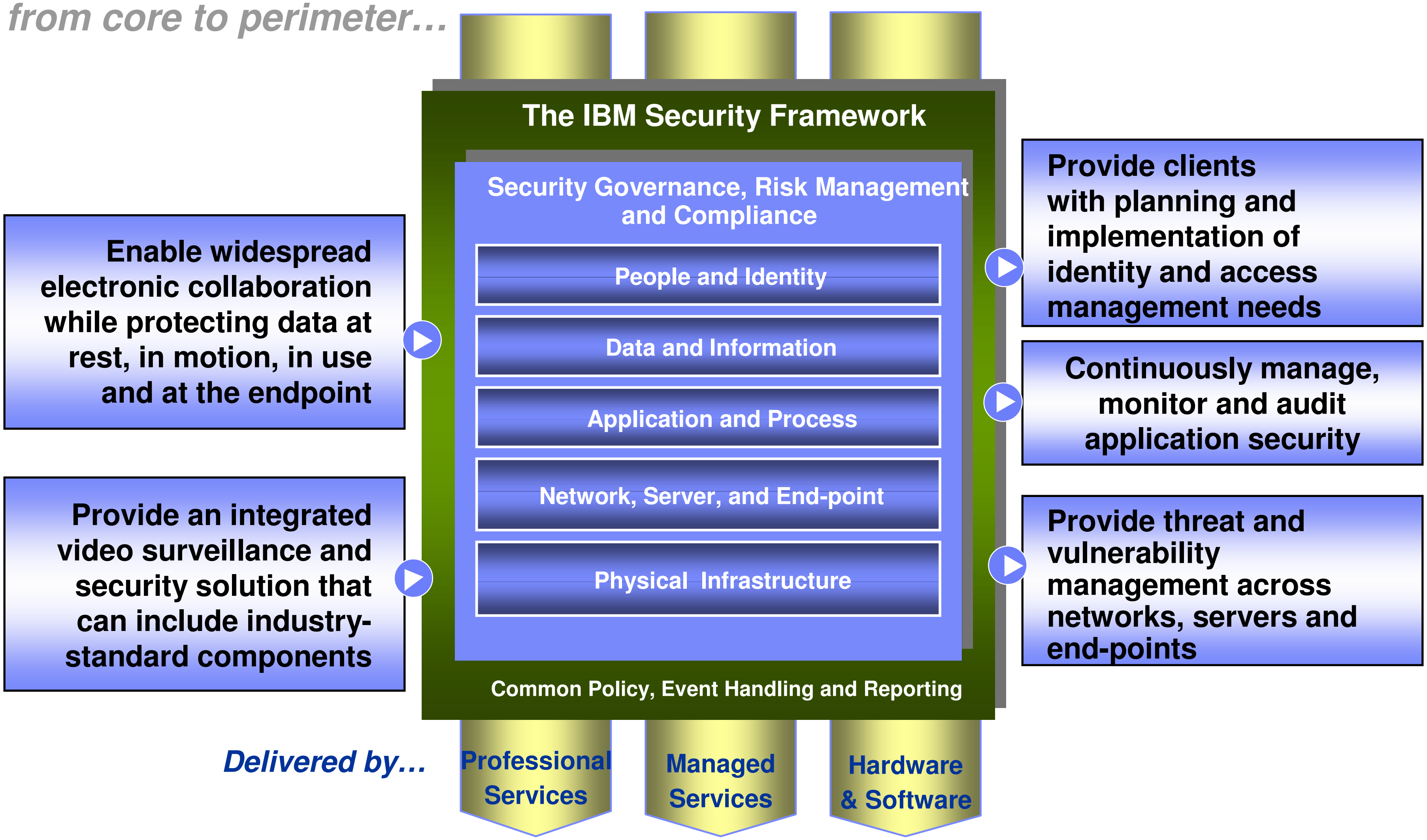
Tivoli Federated Identity Mgr

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. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

While many security companies can help you with the crisis of the day, IBM offers security solutions that address the full range of security challenges

from core to perimeter…



Enable widespread electronic collaboration while protecting data at rest, in motion, in use and at the endpoint

Provide an integrated video surveillance and security solution that can include industry-standard components

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

Provide clients with planning and implementation of identity and access management needs

Continuously manage, monitor and audit application security

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

Delivered by…

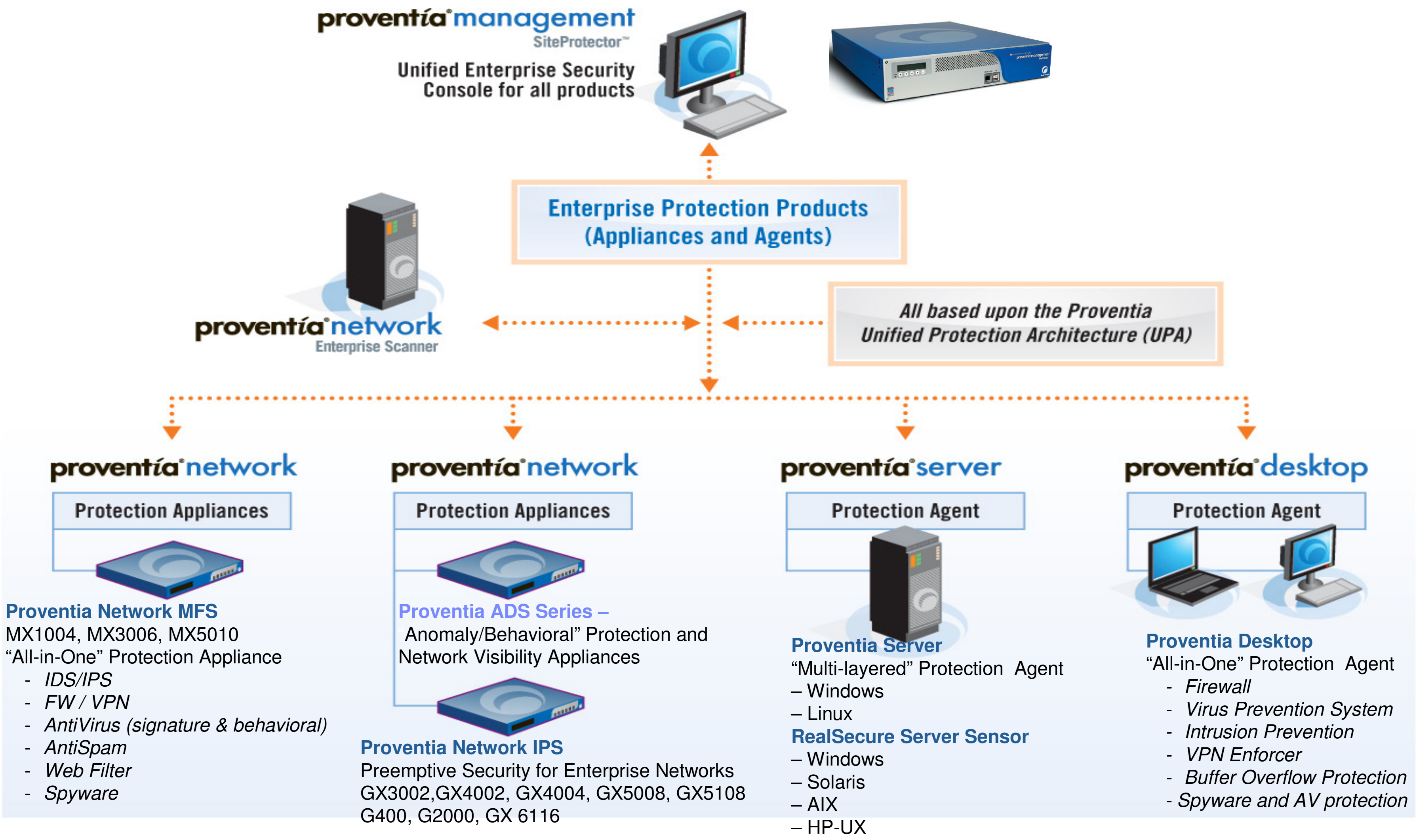
Professional Services

Managed Services

Hardware & Software

Backup

IBM ISS Enterprise Security Platform



proventia management SiteProtector™

Unified Enterprise Security Console for all products

Enterprise Protection Products (Appliances and Agents)

All based upon the Proventia Unified Protection Architecture (UPA)

proventia network Enterprise Scanner

proventia network

Protection Appliances

Proventia Network MFS
MX1004, MX3006, MX5010
“All-in-One” Protection Appliance

- *IDS/IPS*
- *FW / VPN*
- *AntiVirus (signature & behavioral)*
- *AntiSpam*
- *Web Filter*
- *Spyware*

proventia network

Protection Appliances

Proventia ADS Series –
Anomaly/Behavioral” Protection and Network Visibility Appliances

Proventia Network IPS
Preemptive Security for Enterprise Networks
GX3002,GX4002, GX4004, GX5008, GX5108
G400, G2000, GX 6116

proventia server

Protection Agent

Proventia Server
“Multi-layered” Protection Agent
– Windows
– Linux

RealSecure Server Sensor
– Windows
– Solaris
– AIX
– HP-UX

proventia desktop

Protection Agent

Proventia Desktop
“All-in-One” Protection Agent

- *Firewall*
- *Virus Prevention System*
- *Intrusion Prevention*
- *VPN Enforcer*
- *Buffer Overflow Protection*
- *Spyware and AV protection*

IBM ISS Professional Security Services

Assessment Services

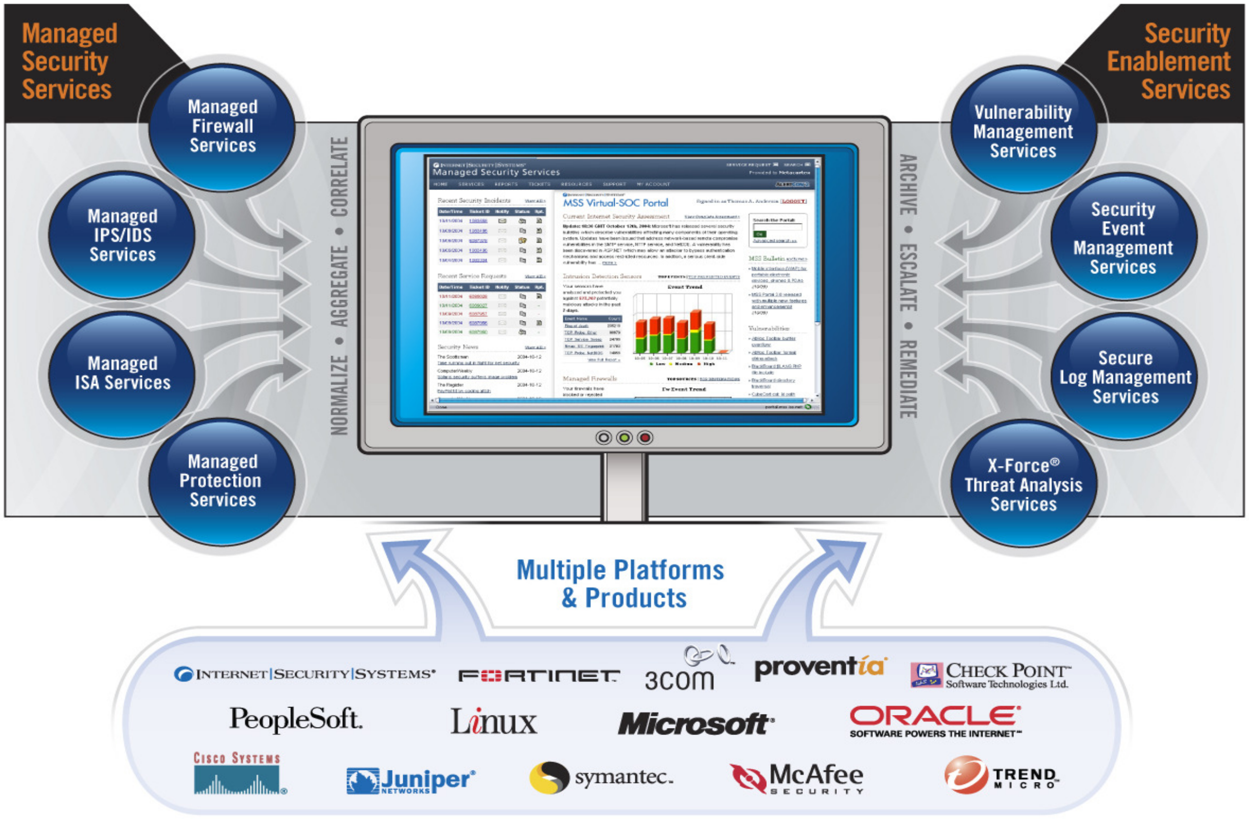
- Application Security Assessment
- Information Security Assessment
- Penetration Testing
- Wireless Network Security Assessment
- Security Testing Program
- ISO 17799 Gap Analysis
- Policy Gap Assessment
- Business Risk Assessment

- **PCI Assessments**
  - Qualified Data Security Company
- **Vertical Market Gap Assessments**
  - HIPAA
  - Gramm-Leach-Bliley
  - Sarbanes-Oxley
  - California Senate Bill No. 1386
  - SCADA
- **Emergency Response Service**
  - Subscription
  - On Demand
- **Forensic Analysis**
  - Subscription
  - On Demand
- **X-Force Threat Analysis Service**

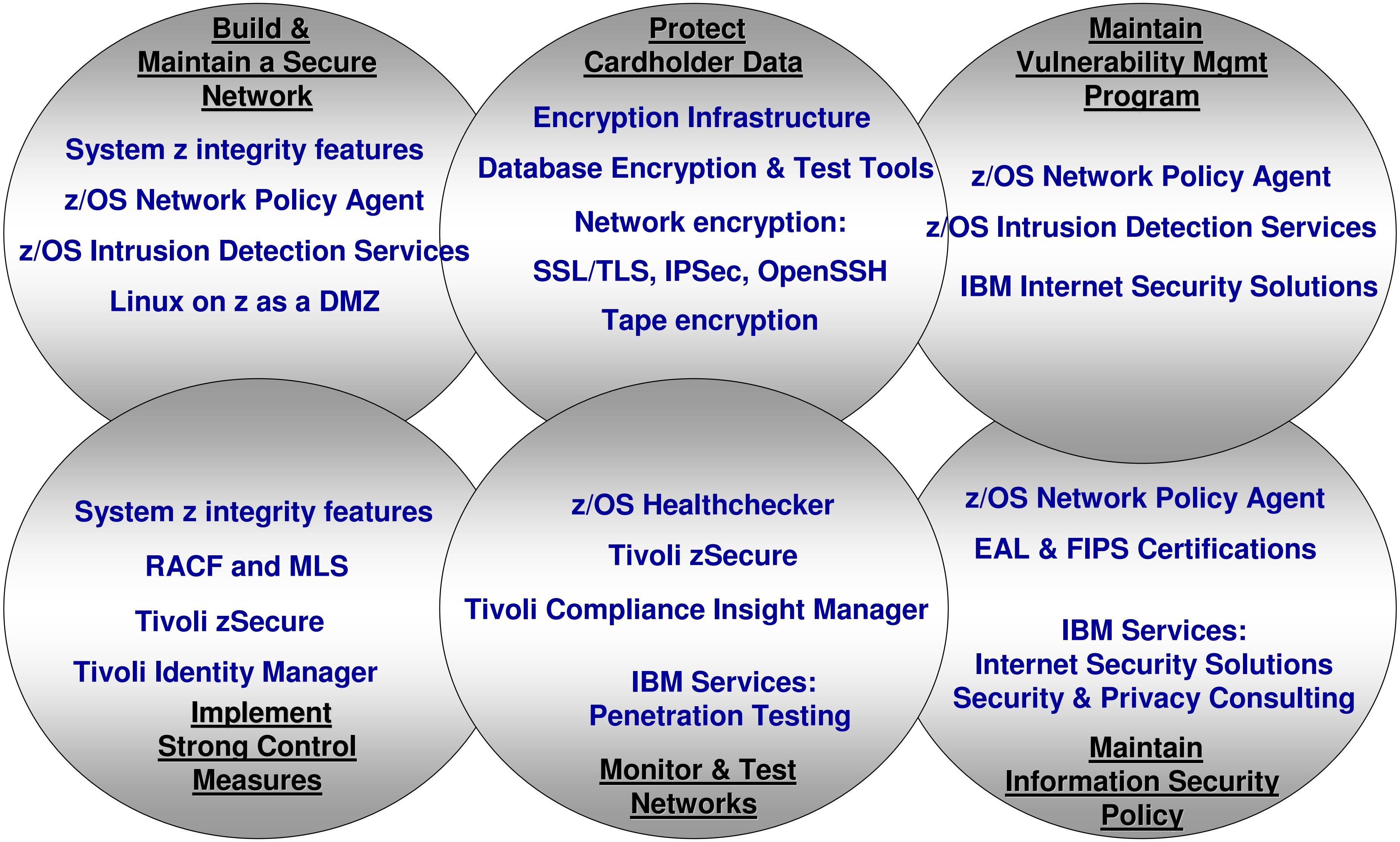
IBM ISS Managed Security Services

Breadth and depth for multiple markets

- ✓ **Fully Managed Services deliver turn key protection to the customer premise or the cloud.**
- ✓ **Security Enablement Services provide on-demand protection and security to the masses.**
- ✓ **Multiple service levels ensure organizations of all sizes present opportunity.**
- ✓ **A centralized multi-tenant web based portal provides real-time, integrated access to all services.**
- ✓ **IBM ISS Remains the *ONLY* provider of true, *GUARANTEED* protection.**


Managed Security Services
Managed Firewall Services
Managed IPS/IDS Services
Managed ISA Services
Managed Protection Services
NORMALIZE • AGGREGATE • CORRELATE
Managed Security Services
MSS Virtual-SOC Portal
ARCHIVE • ESCALATE • REMEDIATE
Security Enablement Services
Vulnerability Management Services
Security Event Management Services
Secure Log Management Services
X-Force® Threat Analysis Services
Multiple Platforms & Products
Internet Security Systems
Fortinet
3com
proventia
Check Point Software Technologies Ltd.
PeopleSoft.
Linux
Microsoft
ORACLE Software Powers the Internet
Cisco Systems
Juniper Networks
symantec.
McAfee Security
Trend Micro

Payment Card Industry Compliance– How System z can help



Build & Maintain a Secure Network

System z integrity features

z/OS Network Policy Agent

z/OS Intrusion Detection Services

Linux on z as a DMZ

Protect Cardholder Data

Encryption Infrastructure

Database Encryption & Test Tools

Network encryption:

SSL/TLS, IPSec, OpenSSH

Tape encryption

Maintain Vulnerability Mgmt Program

z/OS Network Policy Agent

z/OS Intrusion Detection Services

IBM Internet Security Solutions

System z integrity features

RACF and MLS

Tivoli zSecure

Tivoli Identity Manager

Implement Strong Control Measures

z/OS Healthchecker

Tivoli zSecure

Tivoli Compliance Insight Manager

IBM Services:
Penetration Testing

Monitor & Test Networks

z/OS Network Policy Agent

EAL & FIPS Certifications

IBM Services:
Internet Security Solutions
Security & Privacy Consulting

Maintain Information Security Policy

*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.