Pulse2011

Tivoli Security Information & Event Management

How businesses are successfully employing SIEM technologies with Audit and Compliance Best Practices to ensure continuous compliance while maintaining actionable visibility into and control over their security and compliance posture.

Pete Stevenson, Manager Worldwide Security SWAT Team, Advanced Technology Group

Pulse2011

GRC, Security Audit, and Compliance

How businesses are successfully employing GRC and SIEM technologies to help mitigate risk, simplify business governance and ensure continuous compliance while maintaining actionable visibility into and control over their security and compliance posture.

Pete Stevenson, Manager Worldwide Security SWAT Team, Advanced Technology Group

Trademarks and disclaimers

© Copyright IBM Australia Limited 2011 ABN 79 000 024 733 © Copyright IBM Corporation 2011 All Rights Reserved.
TRADEMARKS: IBM, the IBM logos, ibm.com, Smarter Planet and the planet icon are trademarks of IBM Corp registered in many jurisdictions worldwide. Other company, product and services marks may be trademarks or services marks of others. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

© 2011 IBM Corporation

Is the smarter planet secure?

The planet is getting
instrumented, interconnected and intelligent.

New possibilities.
New complexities.
New risks...

"We have seen more change in the last 10 years than in the previous 90."

Ad J. Scheepbouwer, CEO, KPN Telecom

Critical Infrastructure Protection

Privacy and Identity

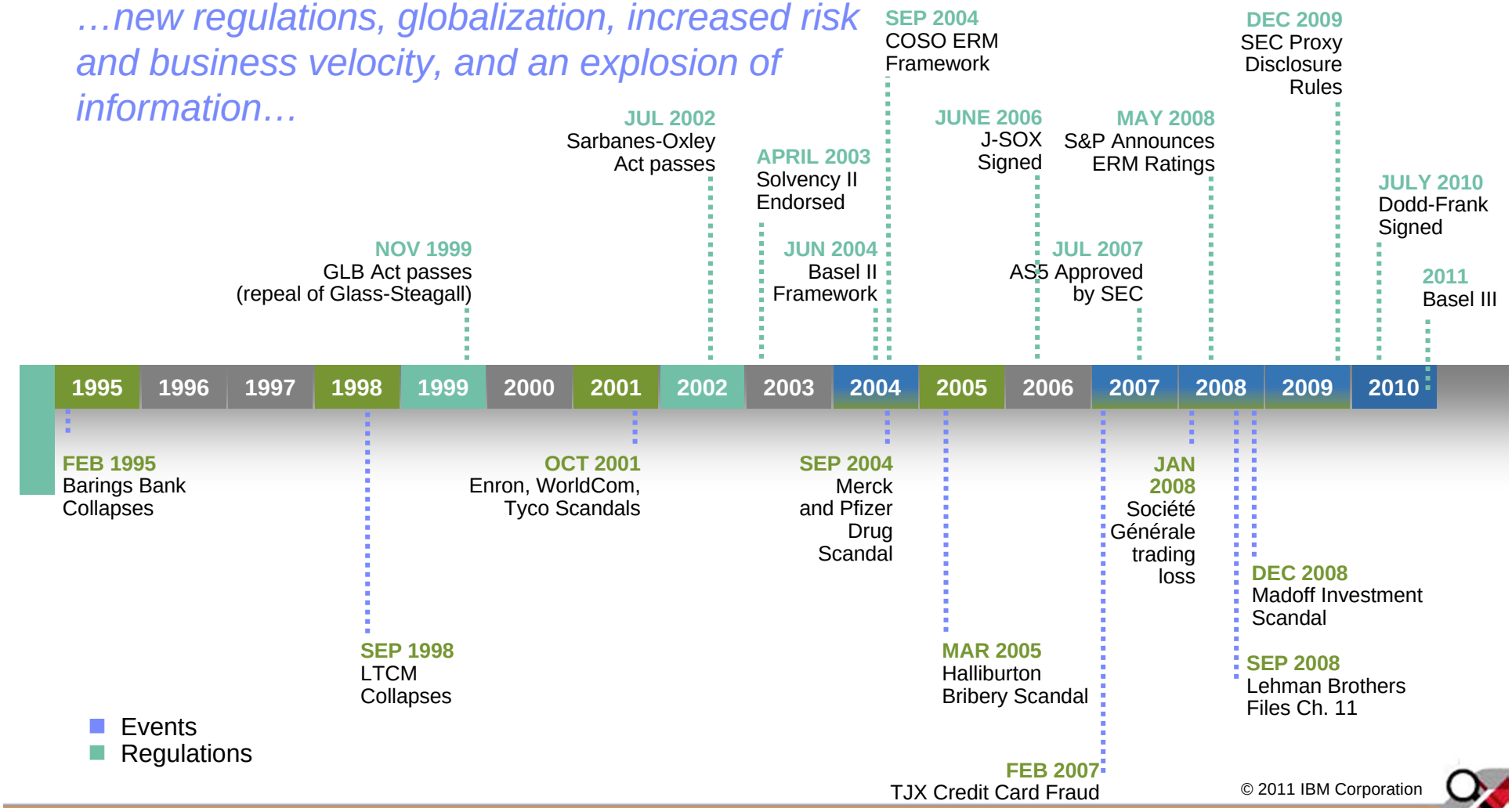
New and Emerging Threats

Cloud Security

© 2011 IBM Corporation

Managing Risk has never been a bigger challenge than in today's business environment

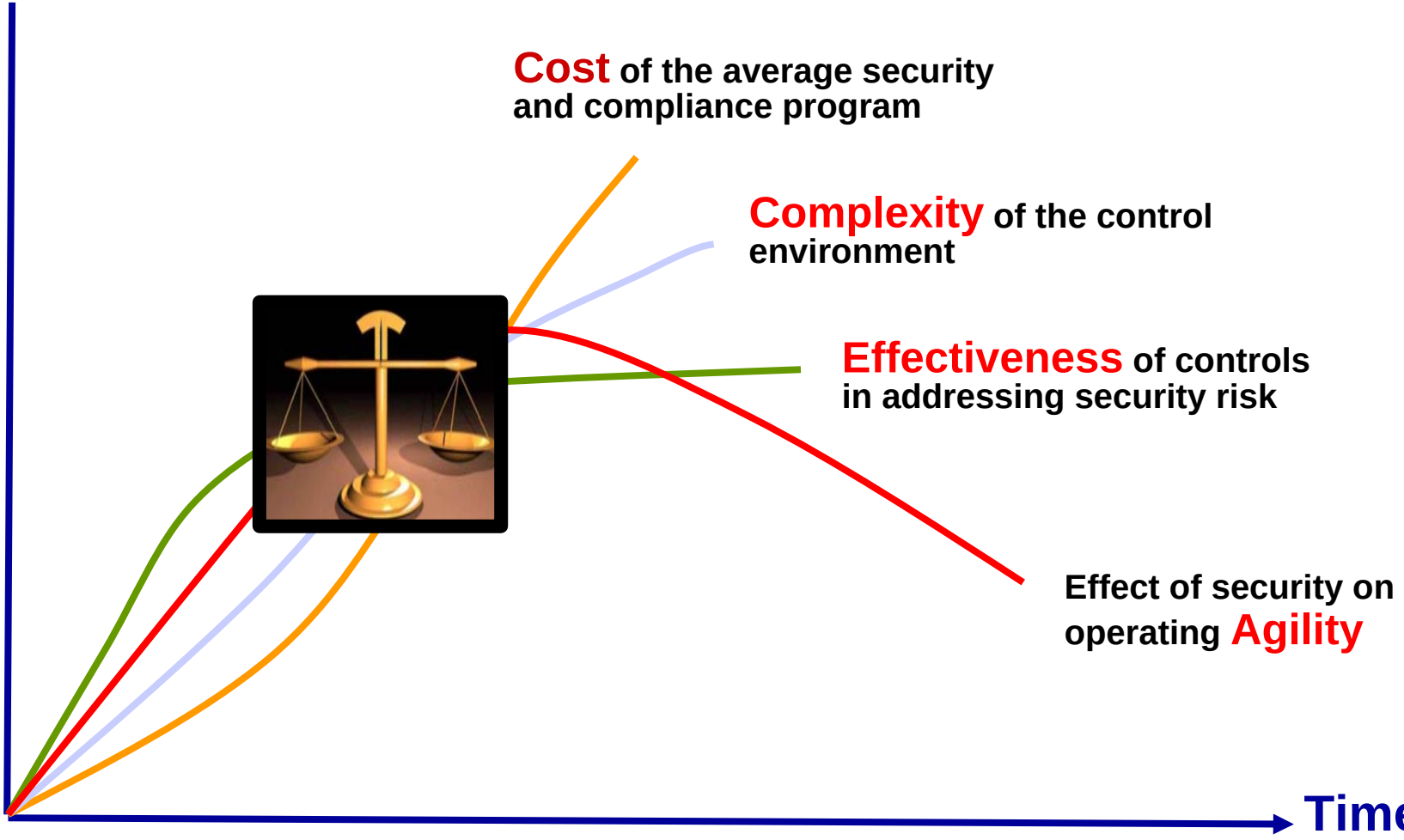
…new regulations, globalization, increased risk and business velocity, and an explosion of information…



© 2011 IBM Corporation

The CSO/CISO/CCO Challenge:

Manage Cost, Decrease Complexity, Improve Effectiveness, Assure Agility



© 2011 IBM Corporation

Traditional approaches to risk management and security do not work effectively…

Point Products

Point Problems

Fragmented policy and process

Complexity

Redundant Costs

Resource Inefficiency

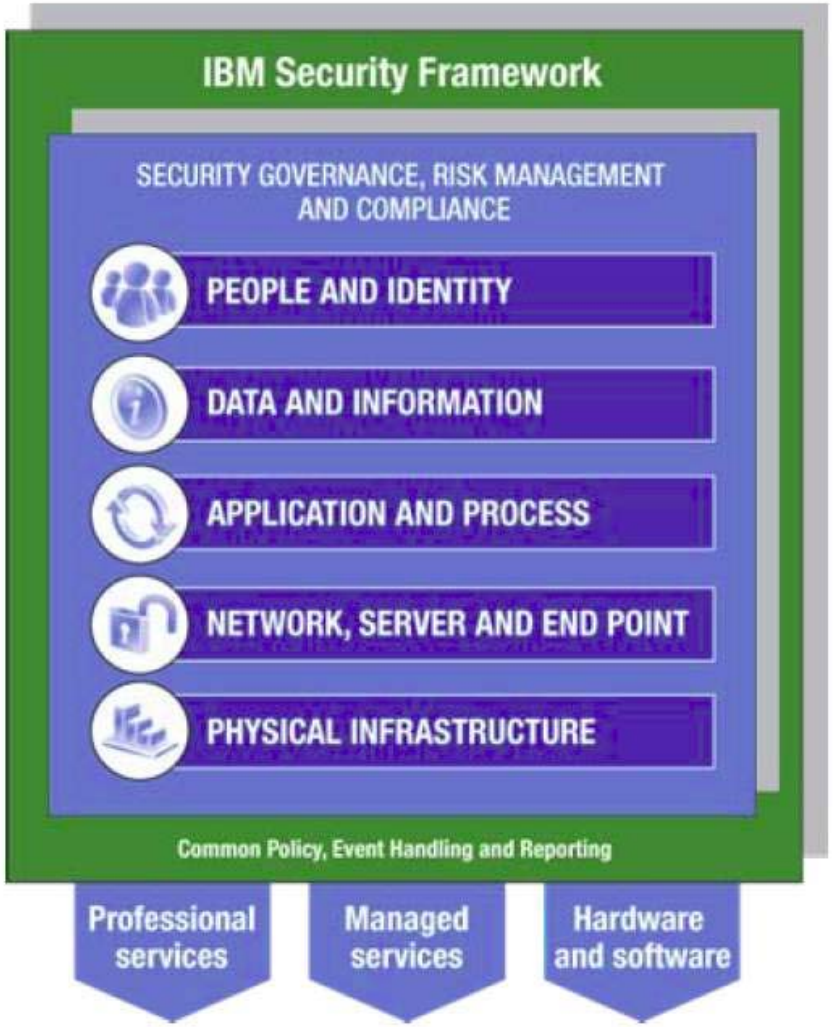
Silos of Data

- An alternative approach is required to solve the risk/security puzzle
- Need an approach based on delivering business value through integrated solutions built into standard operations

IBM'S integrated approach enables enterprises to:

- **start addressing their most pressing challenge**
- **extend to other focus areas as needed**

A new approach to Security

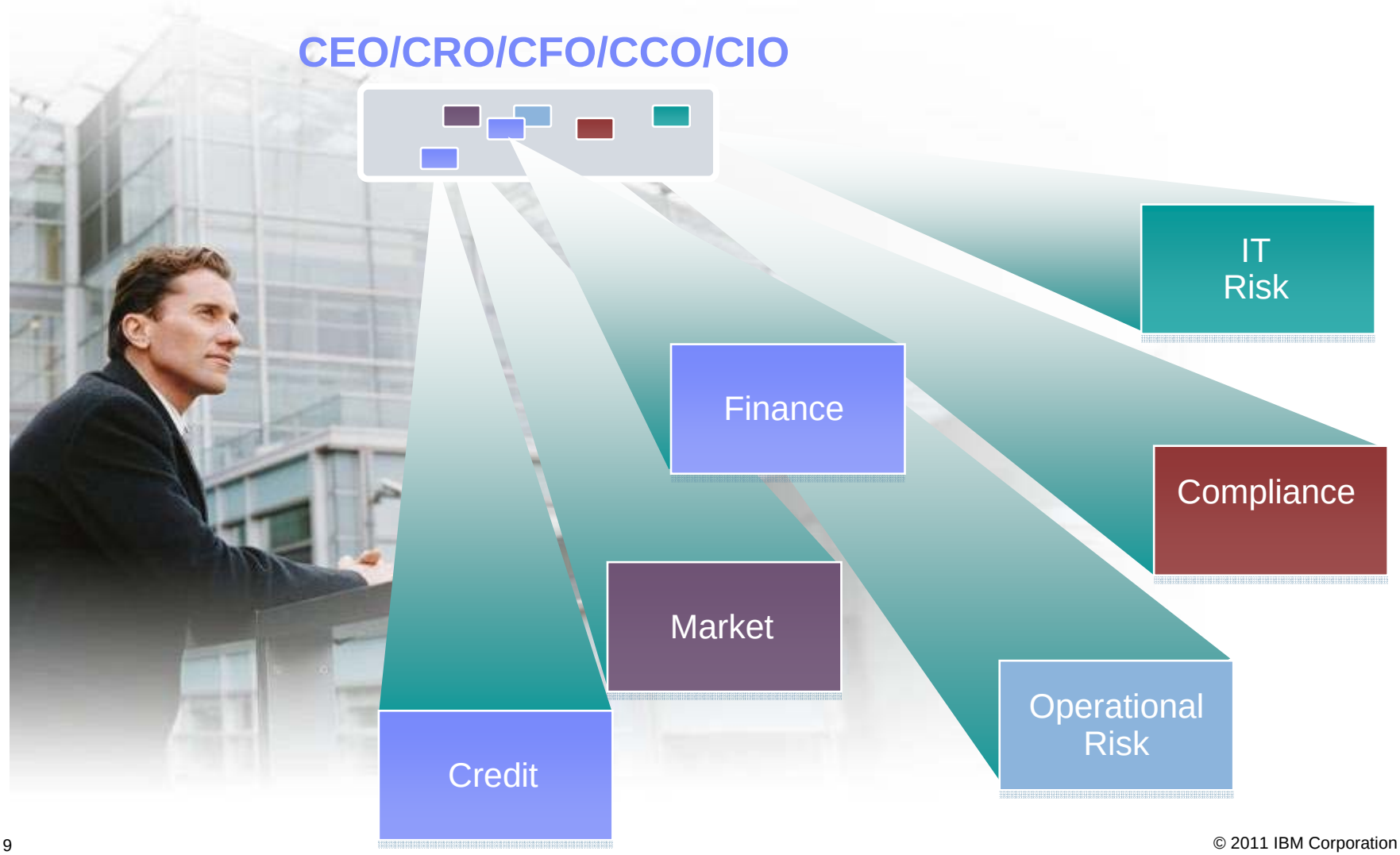


Designed to….

- Enable innovation through secured infrastructure and platforms
- Reduce number and complexity of required security controls
- Reduce redundant security expenses
- Improve organizational and operational agility and resiliency
- Deliver needed visibility, control and automation

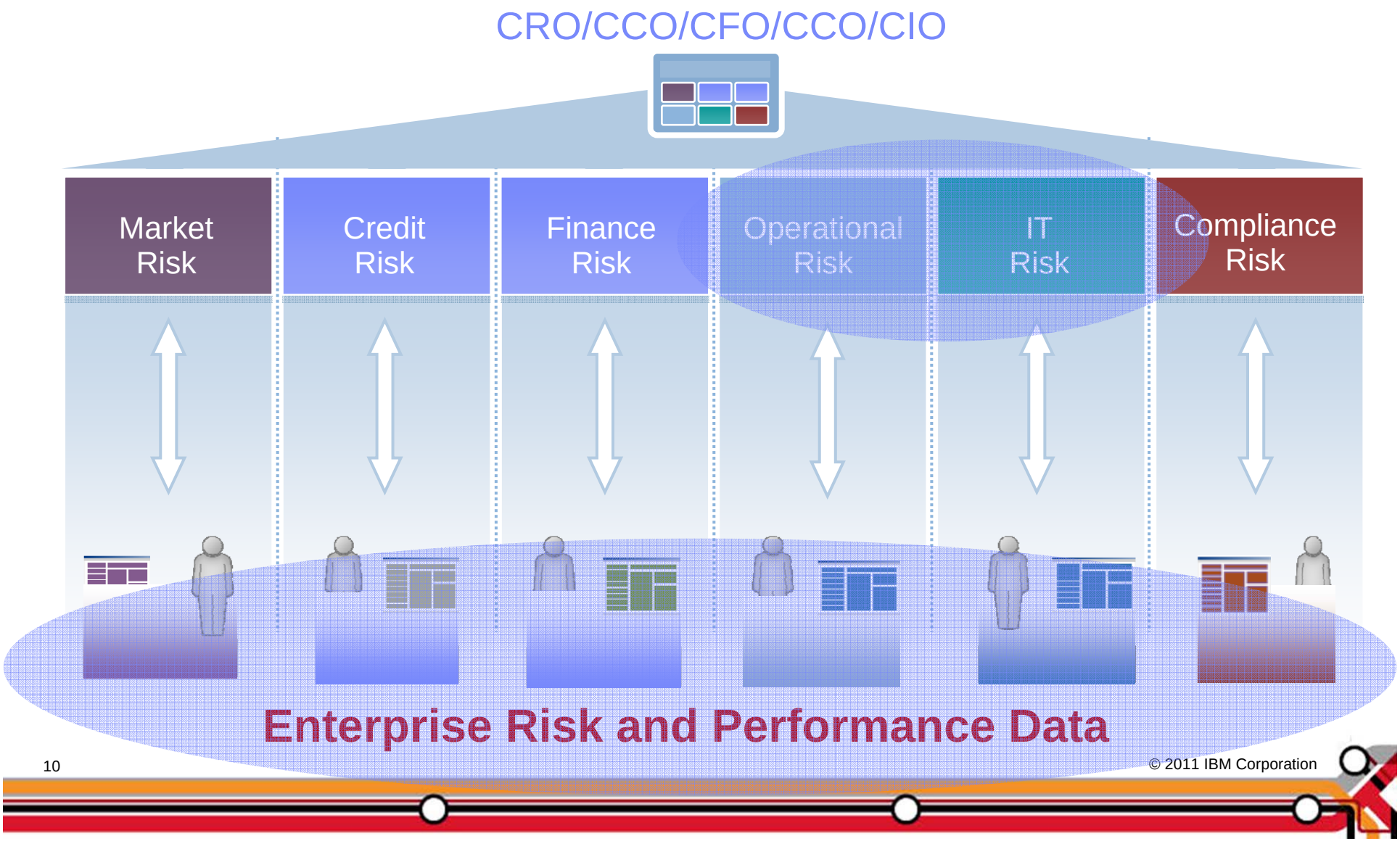
© 2011 IBM Corporation

Companies Struggle with Fragmentation of Risk and Compliance Information – *And have difficulty providing transparency*



© 2011 IBM Corporation

An Integrated Approach Facilitates Transparency



© 2011 IBM Corporation

Strategic Focus in Governance Risk and Compliance

- Integrate with enterprise risk and performance data
- Improve analytic quantification of risk exposure and trade-offs of right risk vs. reward to allocate resources appropriately
- Instrument analysis with real-time compliance, configuration and control monitoring information
- Dynamically update and distribute risk and regulatory content libraries to contribute to reducing risk and situations that could result in regulatory fines

Industry Specific

Finance

Customer

Human Capital

Supply Chain

Business Intelligence

Predictive and Advanced Analytics

Financial Performance & Strategy Management

Governance Risk and Compliance

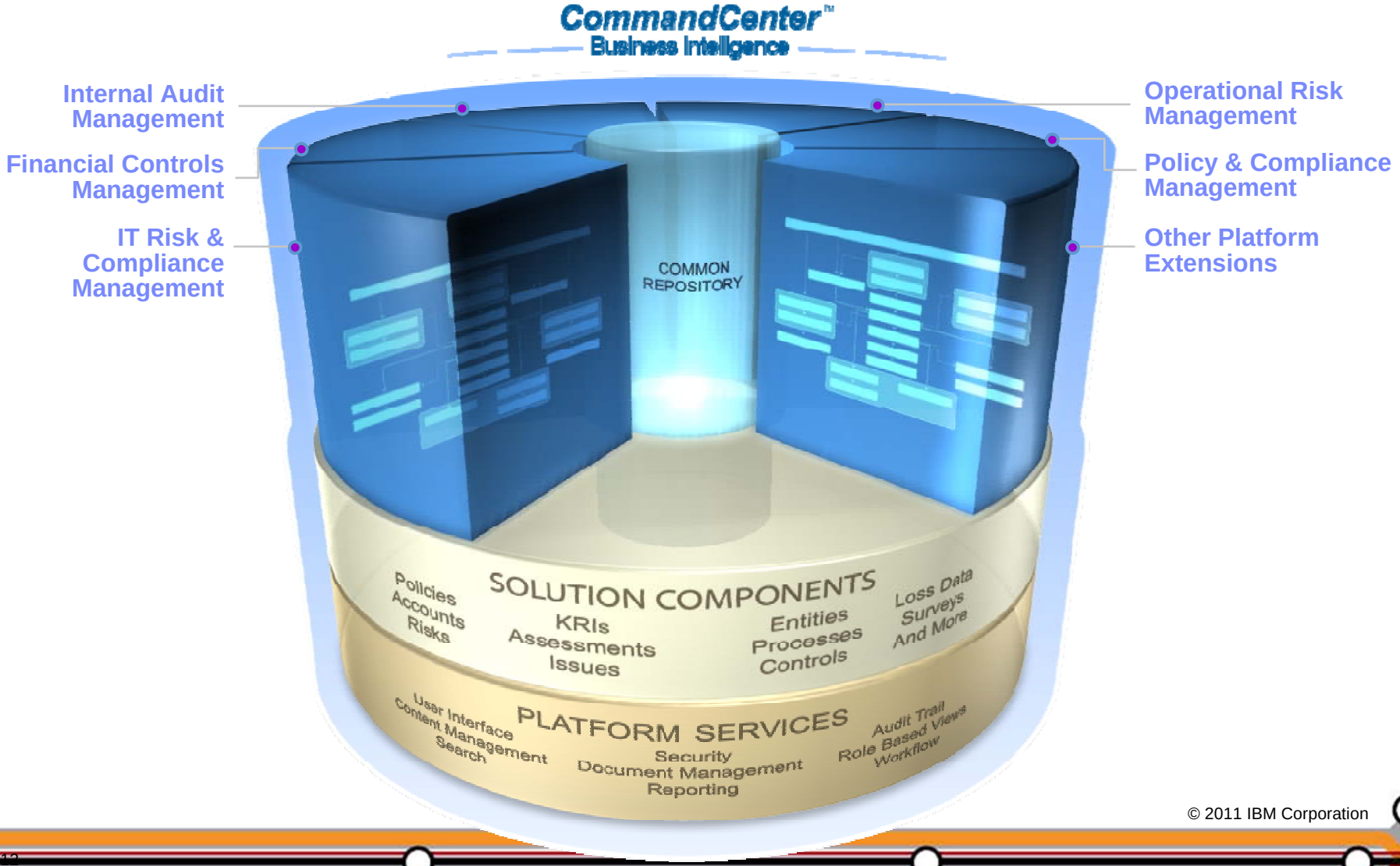
Analytic Applications

Globally Integrated, Market Leading Capabilities

BAO SIMPLIFICATION AND INTEGRATION

© 2011 IBM Corporation

OpenPages GRC Platform Provides an Integrated Approach to Risk Management



© 2011 IBM Corporation

Monitoring Enterprise Risk and Performance Data

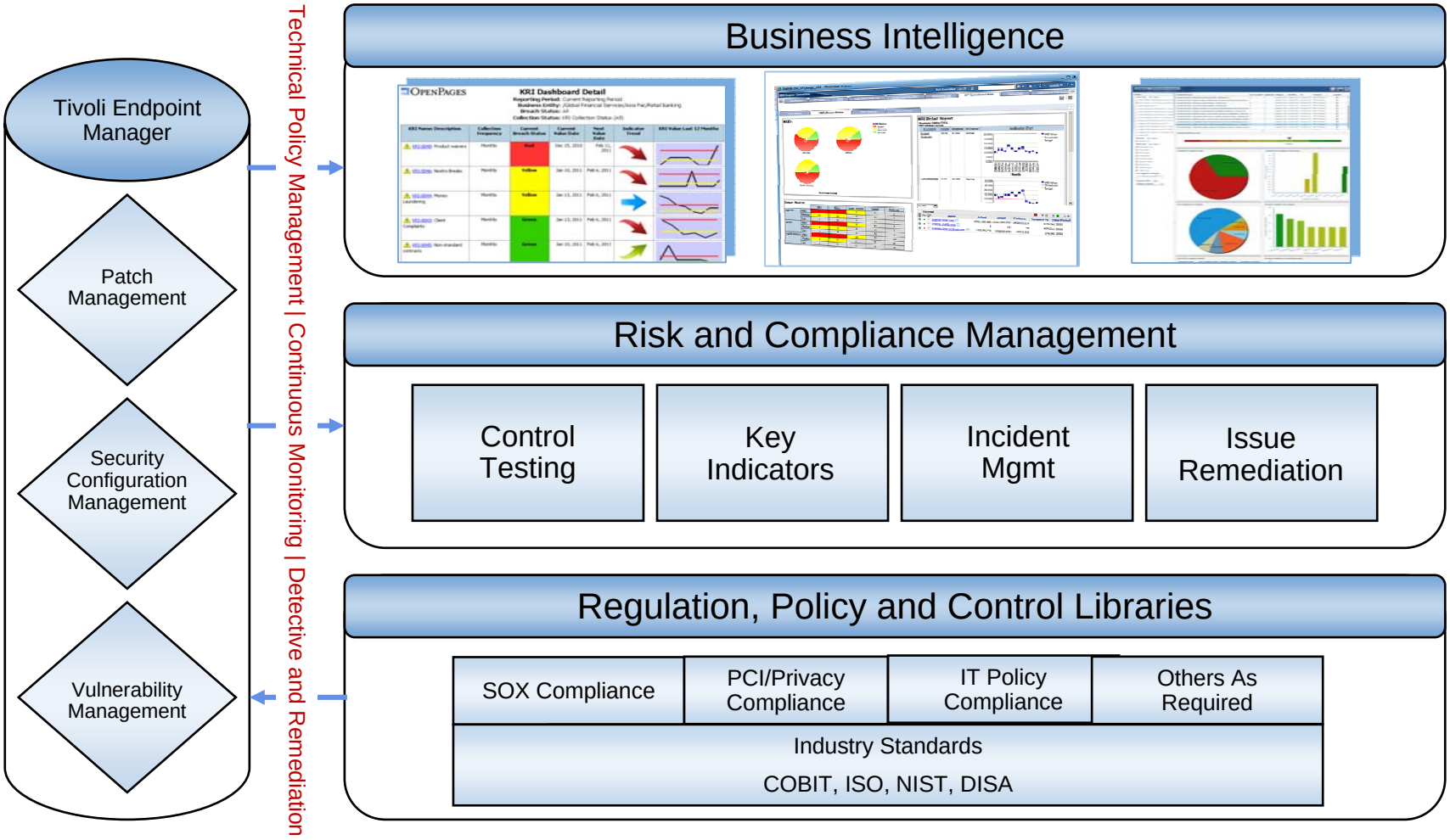
- Challenge: Much GRC data is reliant on human input, which can be error-prone, time-consuming, and lagging

Shared Risk and Compliance Framework

- Strategy:
  - Instrument analysis with near real-time compliance configuration and control monitoring information
  - IT security, compliance, configuration, & control monitoring
  - Enterprise content management, records retention, eDiscovery
  - Asset management systems
  - Verticals: Anti-Money Laundering, Liquidity Risk, etc.

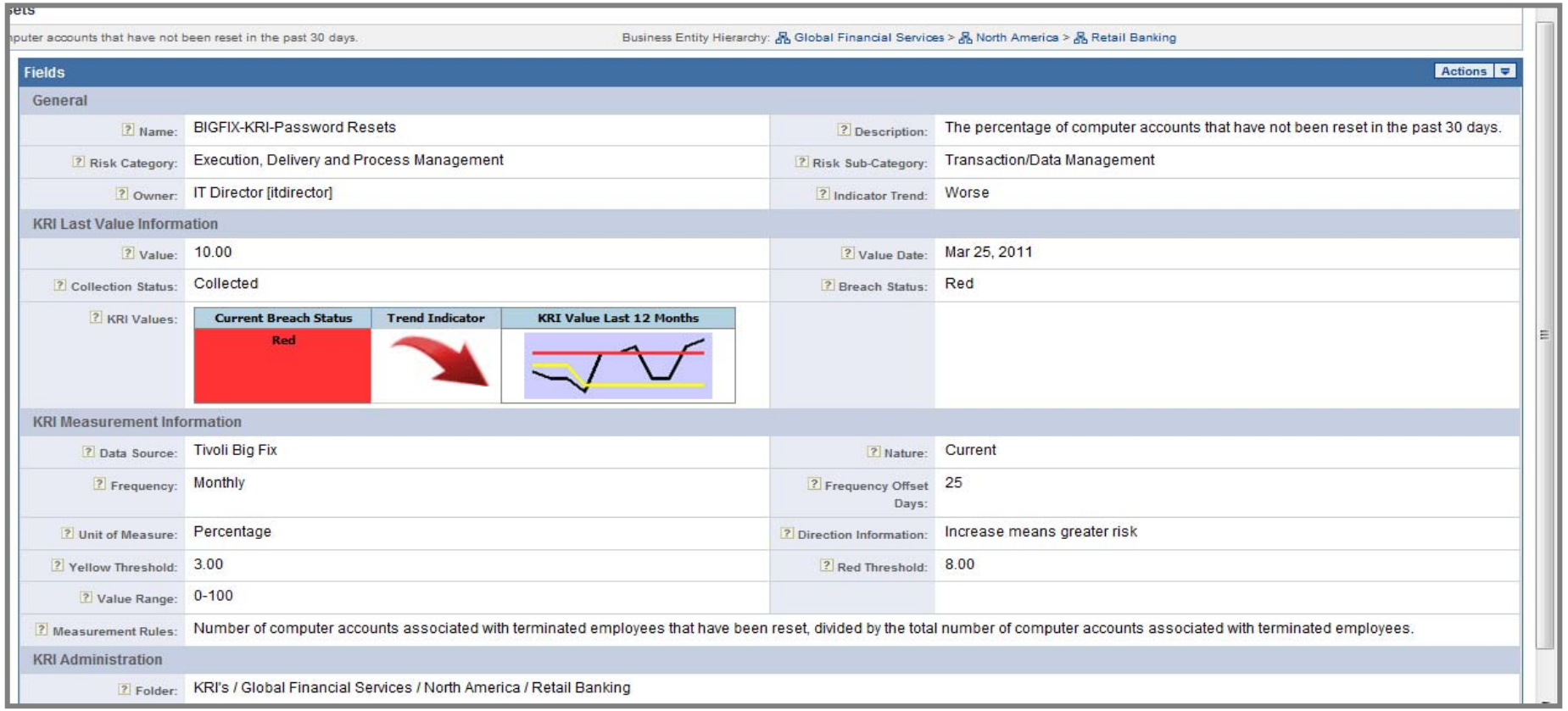
© 2011 IBM Corporation

Drive successful IT Governance using rich asset data, security compliance metrics, and endpoint configuration management from TEM as inputs into OpenPages GRC processes and reporting



© 2011 IBM Corporation

Example: Key Control Indicators



puter accounts that have not been reset in the past 30 days.

Business Entity Hierarchy: Global Financial Services > North America > Retail Banking

Fields — Actions

General

Name:	BIGFIX-KRI-Password Resets	Description:	The percentage of computer accounts that have not been reset in the past 30 days.
Risk Category:	Execution, Delivery and Process Management	Risk Sub-Category:	Transaction/Data Management
Owner:	IT Director [itdirector]	Indicator Trend:	Worse

KRI Last Value Information

Value:	10.00	Value Date:	Mar 25, 2011
Collection Status:	Collected	Breach Status:	Red

KRI Values:

Current Breach Status	Trend Indicator	KRI Value Last 12 Months
Red		

KRI Measurement Information

Data Source:	Tivoli Big Fix	Nature:	Current
Frequency:	Monthly	Frequency Offset Days:	25
Unit of Measure:	Percentage	Direction Information:	Increase means greater risk
Yellow Threshold:	3.00	Red Threshold:	8.00
Value Range:	0-100		
Measurement Rules:	Number of computer accounts associated with terminated employees that have been reset, divided by the total number of computer accounts associated with terminated employees.		

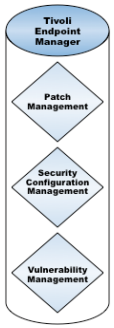
KRI Administration

Folder:	KRI's / Global Financial Services / North America / Retail Banking

Key Control Indicator mapping to Control 'Regular changes to account passwords' (terminated employee accounts not reset)

© 2011 IBM Corporation

Tivoli Endpoint Manager, built on BigFix technology: How it Works



Lightweight, Robust Infrastructure

- Use existing systems as Relays
- Built-in redundancy
- Support/secure roaming endpoints

Cloud-based Content Delivery

- Highly extensible
- Automatic, on-demand functionality

Single Server & Console

- Highly secure, highly scalable
- Aggregates data, analyzes & reports
- Pushes out pre-defined/custom policies

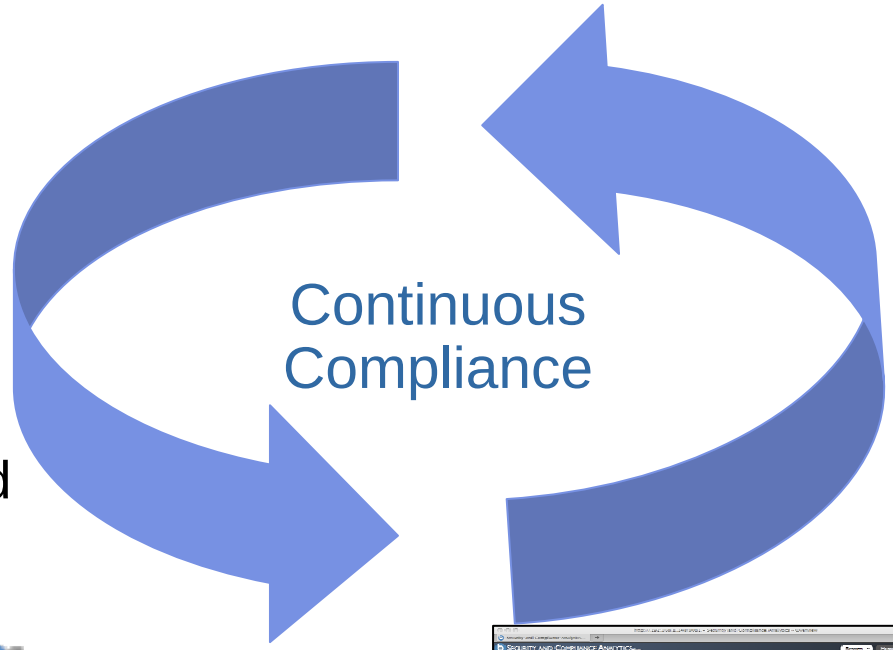
Single Intelligent Agent

- Performs multiple functions
- Continuous self-assessment & policy enforcement
- Minimal system impact (< 2% CPU)

© 2011 IBM Corporation

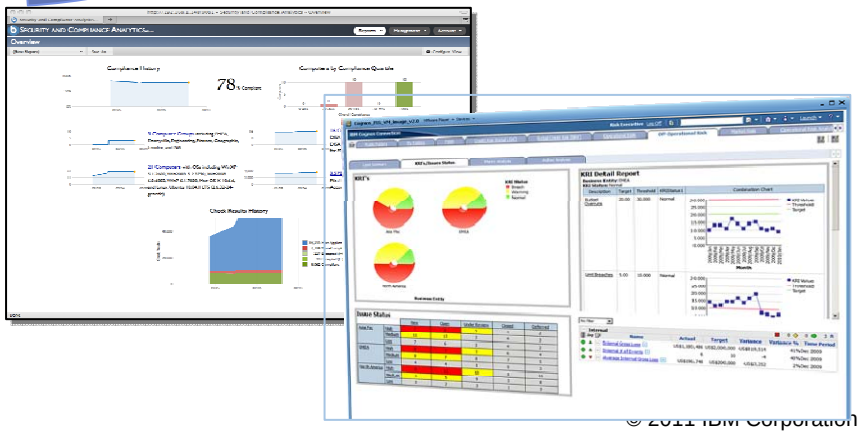
TEM for Security and Compliance

- Continuously monitor and enforce
- Provide real-time visibility
- Identify and remediate critical gaps
- Aggregate and drill-down reporting



OpenPages GRC

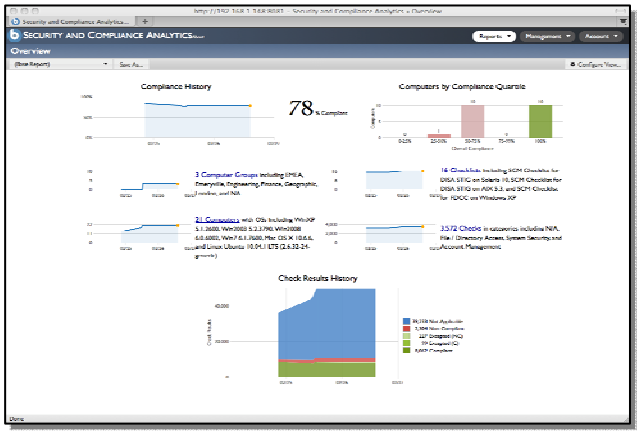
- Integrated analysis and reporting
- Manage control environment, obligations, corporate policies and processes
- Dashboards for corporate risk and compliance



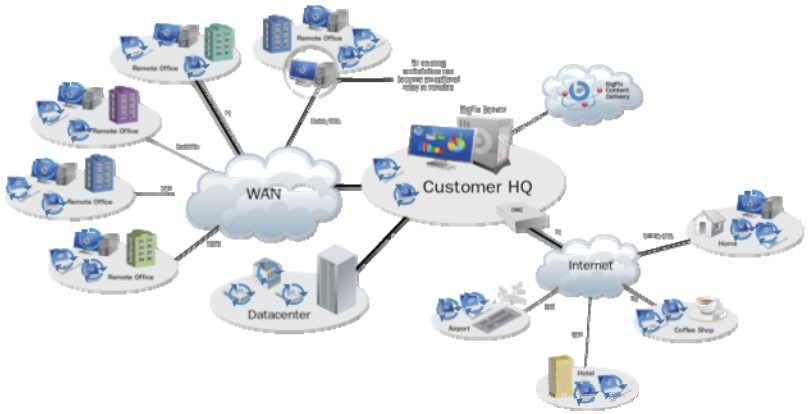
© 2011 IBM Corporation

Summary

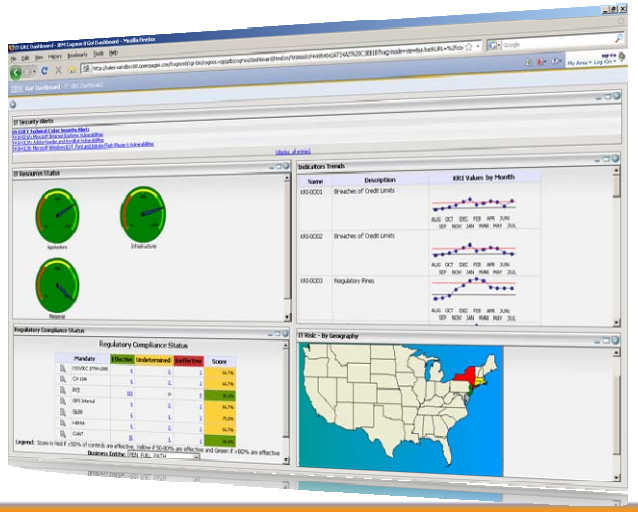
- Compliance status of IT systems is critical for effective IT risk management
- Real-time visibility and autonomous enforcement has been implemented on millions of endpoints already
- Why continue to manually scan and test IT environments? It's costly, inefficient, and error prone.
- We're bringing it together



Tivoli Endpoint Manager delivers real-time visibility and enforcement at scale.

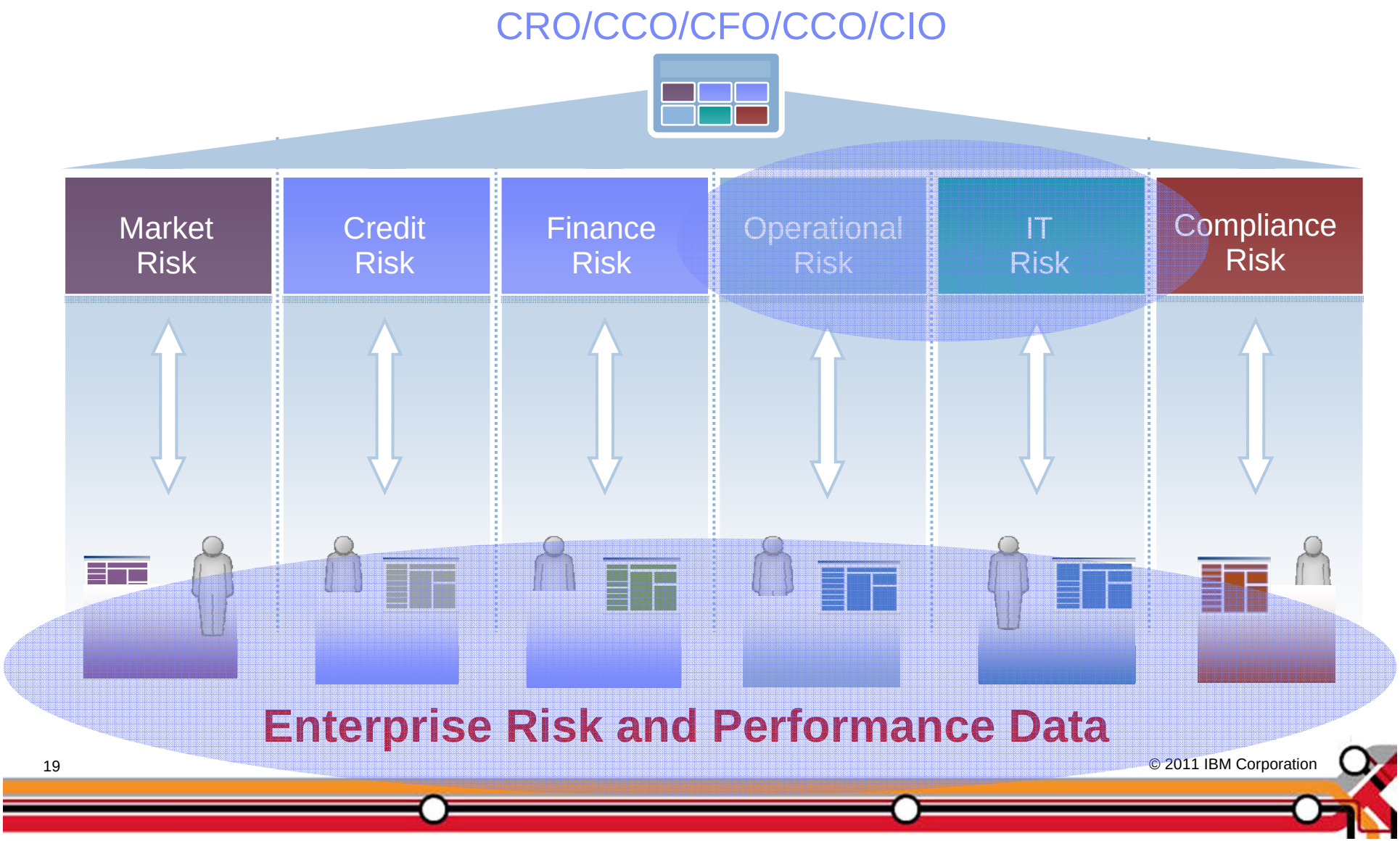


OpenPages ITG delivers policy-driven, process-centric IT risk and compliance.



© 2011 IBM Corporation

An Integrated Approach Facilitates Transparency



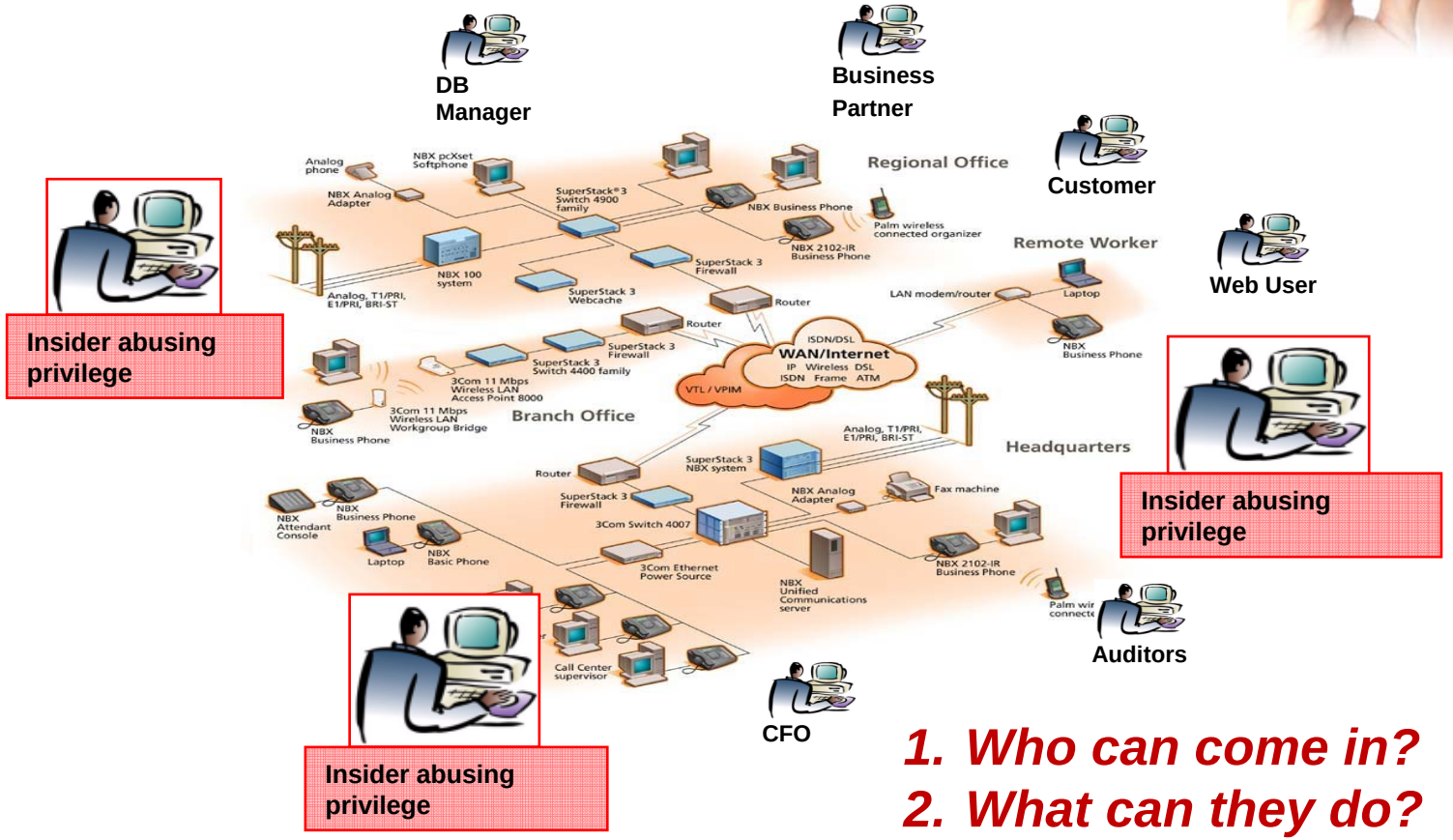
© 2011 IBM Corporation

Monitoring IT Risk: Can you answer these questions?

- Did anyone touch or modify sensitive data inappropriately? **(acceptable use)**
- Are outsourcers managing systems and data responsibly? **(change management)**
- Were there any unauthorized changes to the operating environment? **(change management)**
- Are we alerted when rogue administrative accounts are created? **(account management)**
- Are system administrator and system operator activities logged and reviewed on a regular basis?
- Is all access to sensitive data – including root/administration and DBA access – logged and monitored?
- Are security incidents and suspicious activity analyzed, investigated and remedial actions taken?

© 2011 IBM Corporation

Monitoring IT Risk:
What are your trusted users doing on your network?



1. *Who can come in?*
2. *What can they do?*
3. *Can you easily prove it to an auditor?*

© 2011 IBM Corporation

Prevent insider threats

- ✓ **Monitor privileged user behaviour** and **report** exceptions when a policy is violated
- ✓ **Alert** on insider threats using near real time analytics
- ✓ **Analyze and investigate** suspicious activity and take remedial **actions**
- ✓ **Enforce policies** while ensuring **employee productivity**

- ✓ Integrate into **Identity Management** for **closed loop auditing**

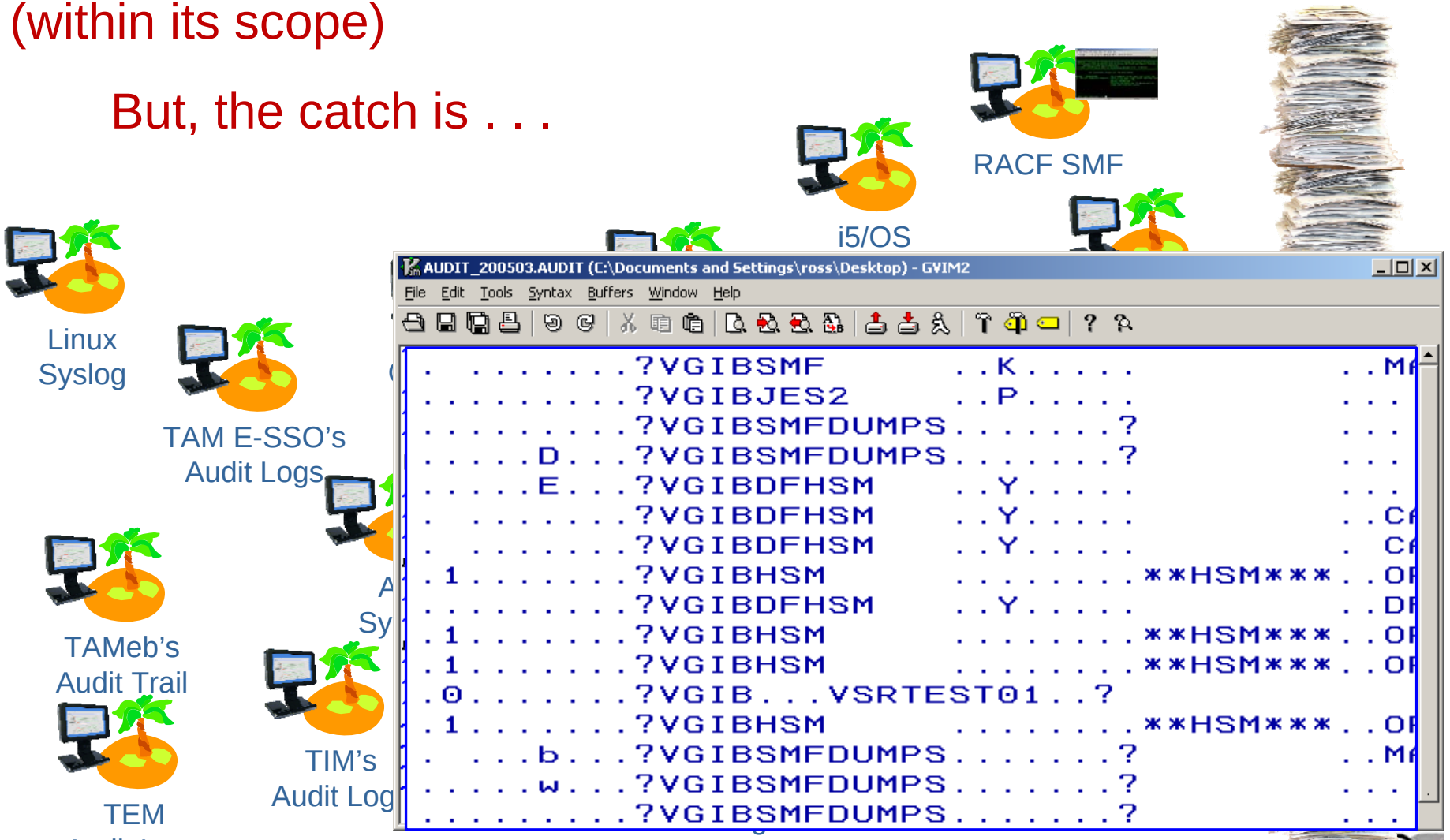
- Protect your intellectual property
- Prove to your auditors that you can monitor and audit access to sensitive information

© 2011 IBM Corporation

Every one of your solutions may address compliance . . .

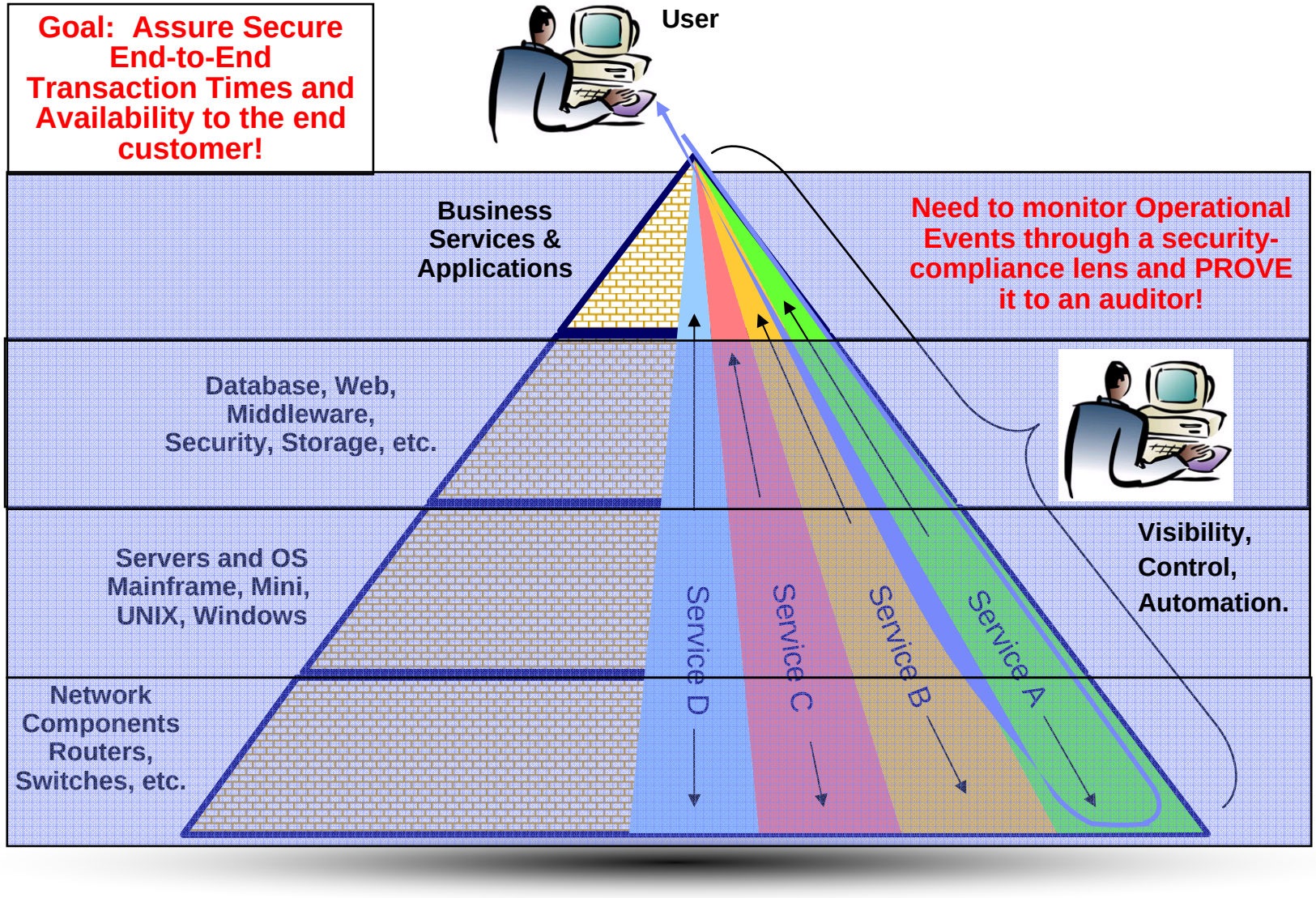
(within its scope)

But, the catch is . . .



© 2011 IBM C

Why is compliance so difficult?

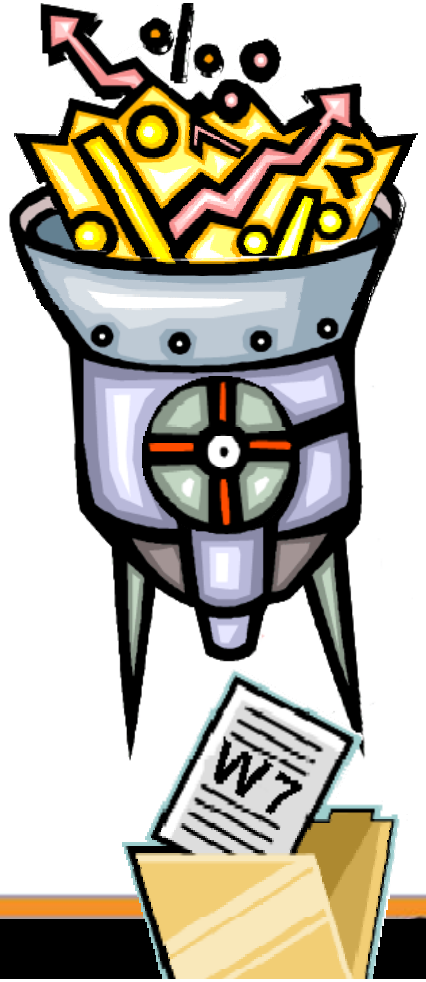


© 2011 IBM Corporation

IBM Tivoli Security Information & Event Manager

What Does It Do?

- Automated enterprise audit management and reporting
- Enables knowledge of who's accessing what
- Spans application, database, OS (distributed/mainframe) resources



Voluminous audit information from many different sources

"W7" Analysis/Processing

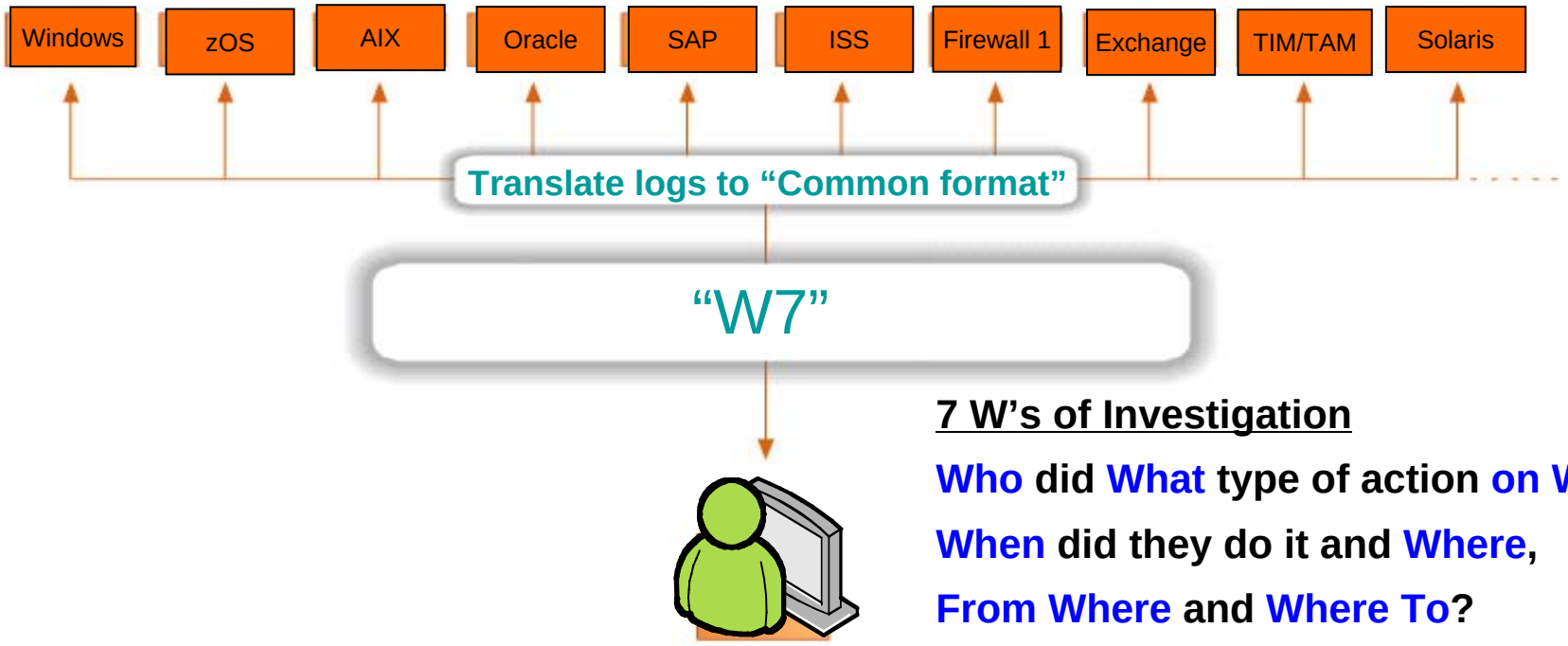
Who **took** What **type of action** on What resource**?**

When **did they do it and** Where**,** From Where **and** Where To**?**

Clear, crisp, normalized audit info

© 2011 IBM Corporation

TSIEM: All logs in your enterprise in a single language



7 W’s of Investigation

Who did What type of action on What?

When did they do it and Where,

From Where and Where To?

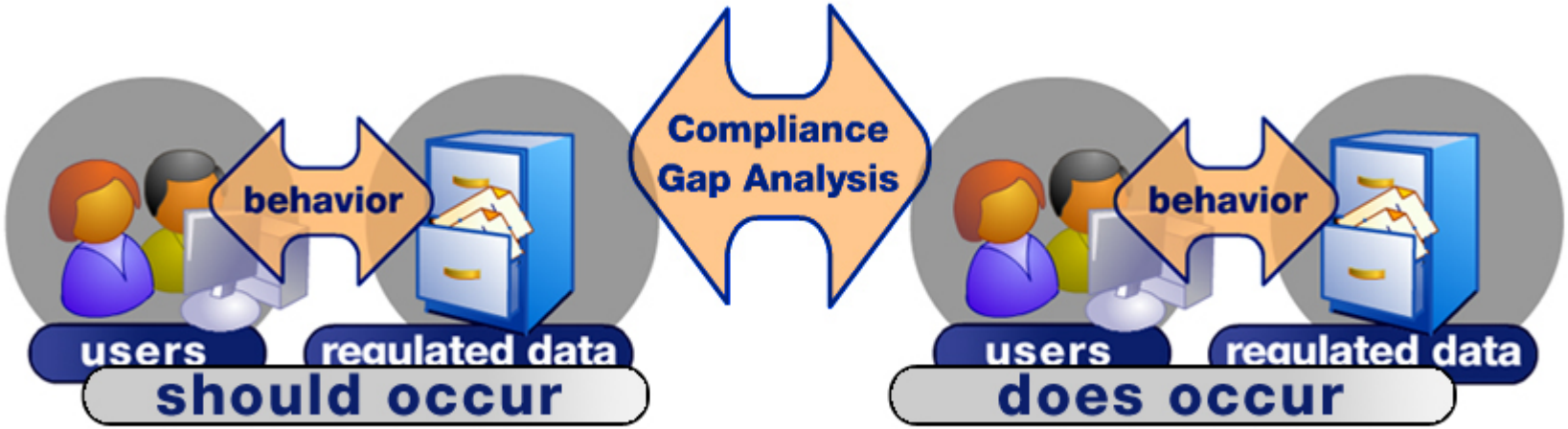
TSIEM's W7 saves your information security and compliance staff time and money.

- **reduces the need for skilled staff**
- **produces reports auditors can understand**
- **automates monitoring across the enterprise.**

© 2011 IBM Corporation

TSIEM enables Acceptable Use Monitoring

Compares desired versus actual behavior...



... like an auditor does.

© 2011 IBM Corporation

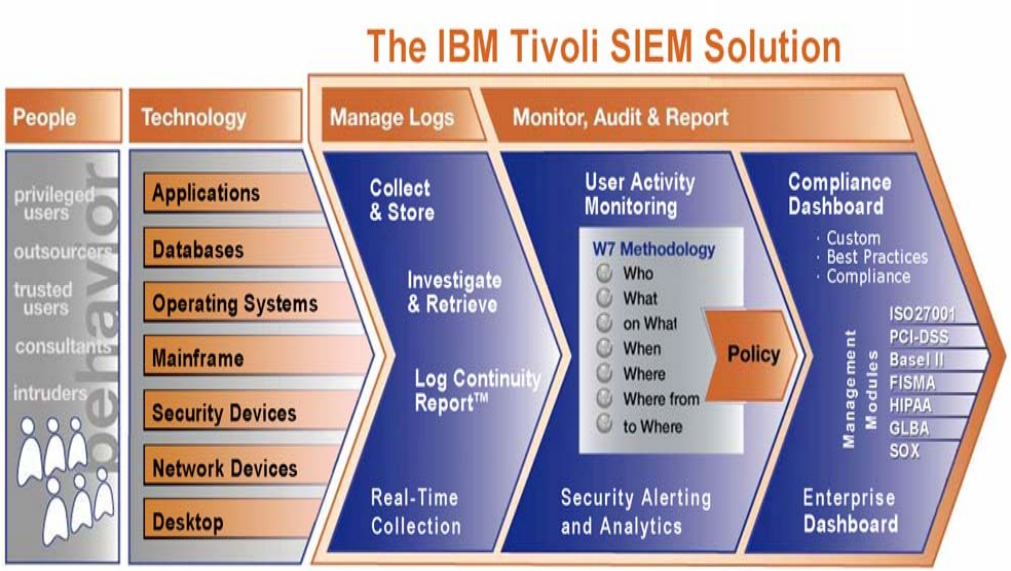
Assessing compliance: Tivoli Security Information and Event Manager

Manage logs and monitor privileged users for insider threat and compliance initiatives

Tivoli Security Information and Event Manager provides a single, integrated product for insider threat, audit and compliance

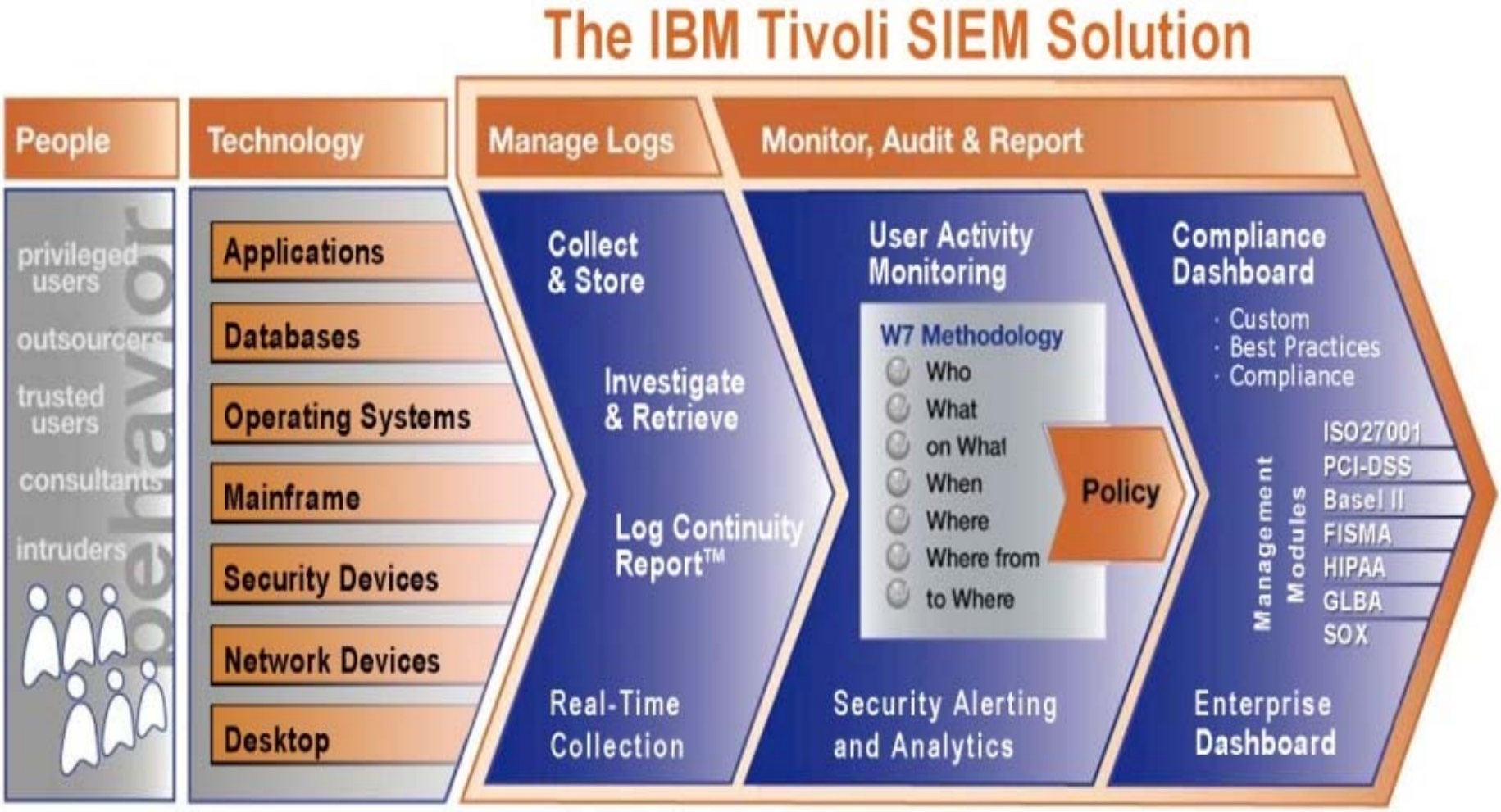
Highlights

- Single, integrated product
- Log Management Reporting
- Unique ability to monitor user behaviour
- Enterprise compliance dashboard
- Compliance management modules and regulation-specific reports
- Broadest, most complete log and audit trail capture capability
- W7 log normalisation translates your logs into business terms
- Makes it easy to compare behaviour to regulatory and company policies



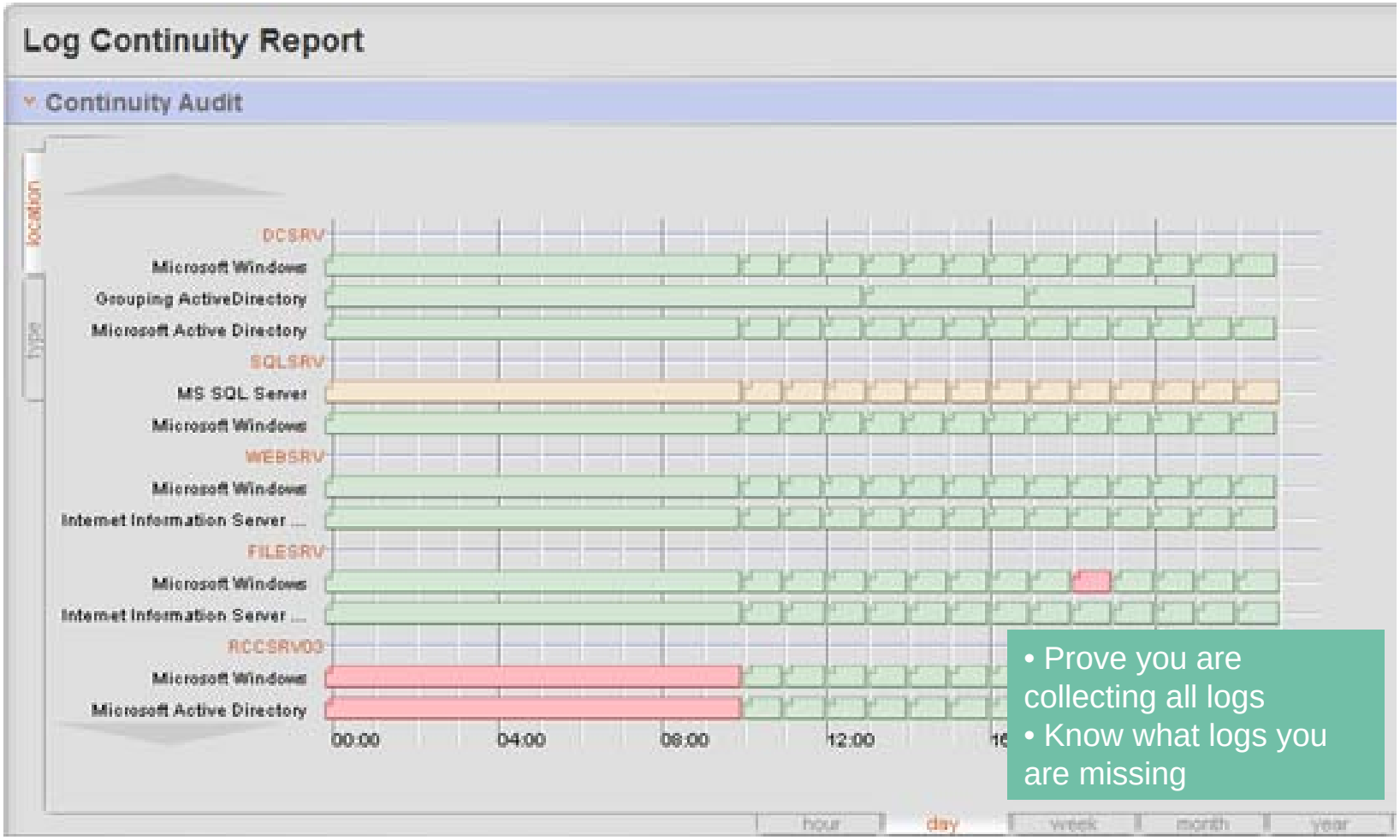
© 2011 IBM Corporation

Tivoli Security Information & Event Manager



© 2011 IBM Corporation

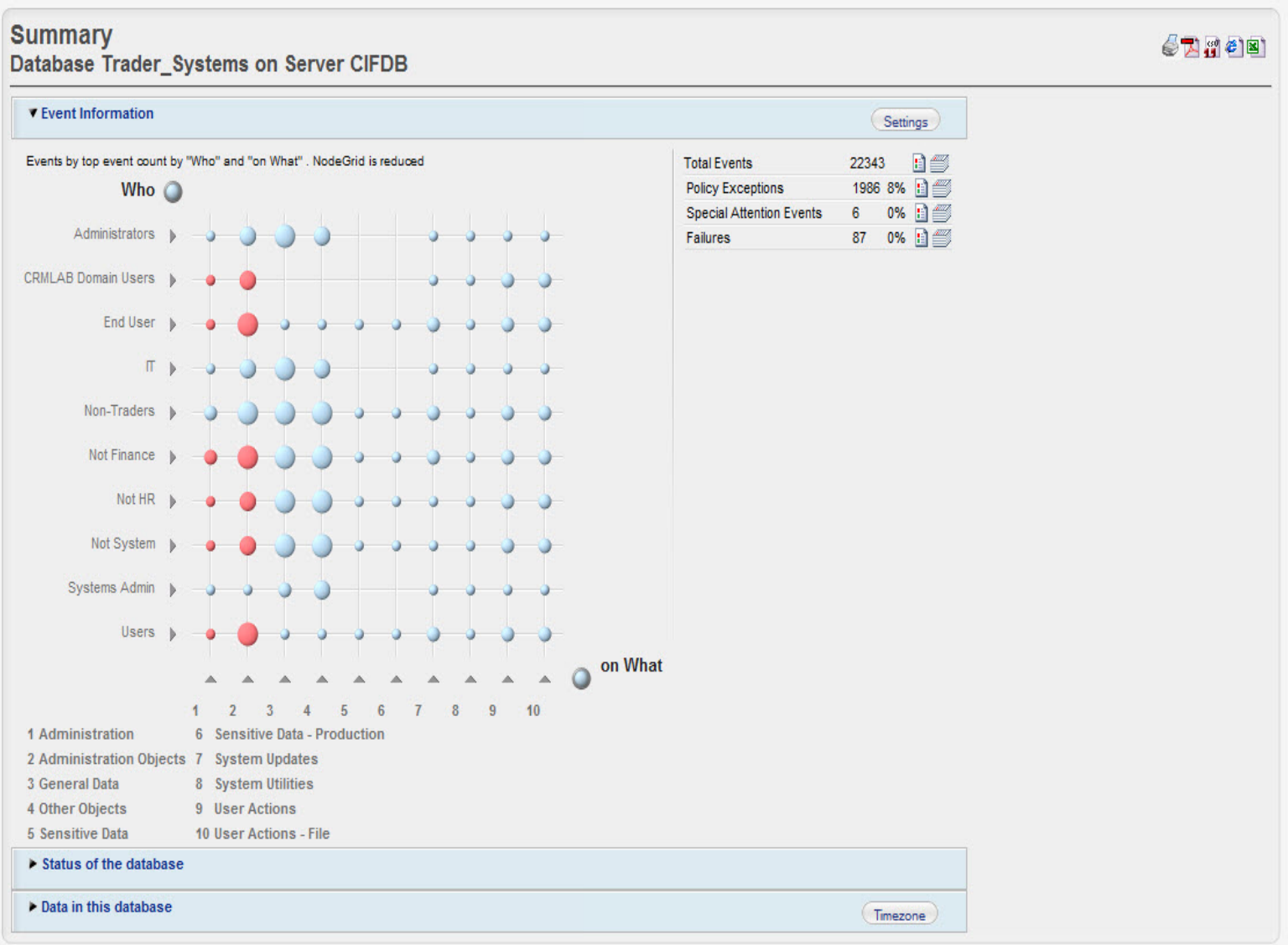
Log Management: Continuity Report



- Color codes are used to show the quality of the log archive
- Notifications can be sent to alert when gaps are found

© 2011 IBM Corporation

Security Dashboard: Compliance at a Glance



- Quick Drill-down
- Policy Exceptions
- Special Attentions
- Failures
- Trends
- Reporting DBs
- Aggregation DBs
- Enterprise Overview
- Reports Distribution
- Self-audit

© 2011 IBM Corporation

Example: Privileged User Monitoring with TSIEM

Event Detail

Event information

	Field	Group	
Severity	2 (1x)	-	
When	Fri Oct 31, 2006 08:05:01 GMT +02:00	Office Hours (10)	10
What	Grant : Privilege / Success	Security Changes Administration	50 40
Where	SRV_DC_034 (Windows)	Finance Server	50
Who	Jim Hofferman	Administrators Database Admin Finance Admin	30 30 20
From Where	XPWKST03 (Windows)	Workstation	10
On What	USER : Chin055 / Chin055	Authorization Objects	30 20
Where To	SRV_DC_034 (Windows)	Finance Server	50

Incident Tracking

Additional information

Investigate

Time: Fri Oct 31, 2006 08:05:01 GMT +02:00 (+/-) 1 minute

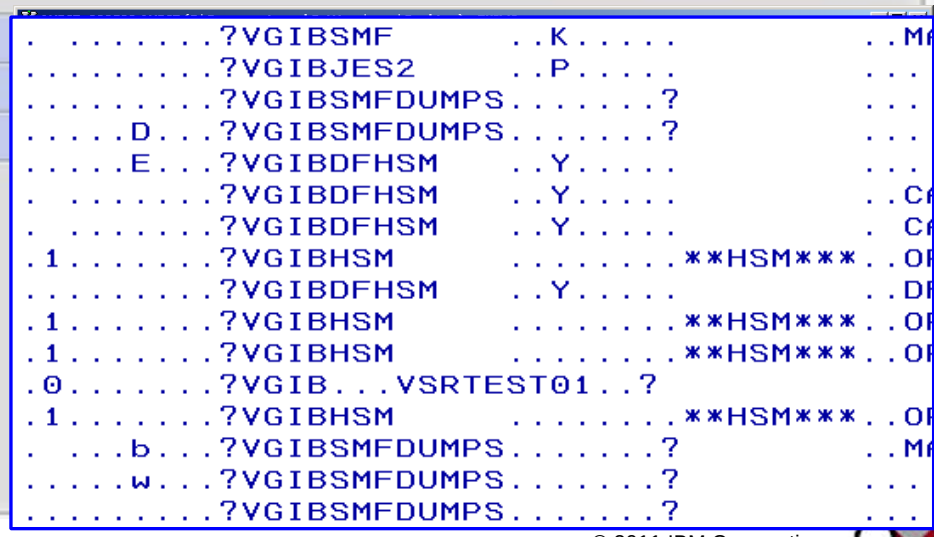
Selected time zone: GMT+01:00 Rome, San_Marino, Sarajevo

Filter by Platform: SRV_DC_034 (Windows)

Filter by User: Jim Hofferman

Investigate

Logrecords...



© 2011 IBM Corporation

TSIEM 2.0 Log Management server features

- Reliable and scalable log collection and archiving
- Flexible integration, able to collect any type of log located on any type of machine in a tcp/ip network.
- Out-of-the-box log management reports
- Out-of-the-box best practice log analysis reports.
- Customizable search tool for advanced log analysis.
- Includes TDI: **The ultimate information transformation swiss army knife!**

© 2011 IBM Corporation

TDI 7.0

The ultimate information transformation swiss army knife.

Axis Easy Web Service Server Connector
Axis Easy Web Service Invoke
Axis Java-to-Soap
Invoke Soap Web Service
Axis Soap-to-Java

LDAP Connector
LDAP Server Connector
Tivoli Access Manager Connector
TSIEM Connector
Windows Users and Groups Connector

Active Directory Changelog Connector v2
IBM Directory Server Changelog Connector
Netscape/iPlanet Changelog Connector
zOS LDAP Changelog Connector

JDBC Connector
Properties Connector
SystemStore Connector
RDBMS Changelog Connector

AssemblyLine Connector
Server Notifications Connector
AssemblyLine Function Component

Domino Change Detection Connector
Domino Users Connector
Lotus Notes Connector

Exchange Changelog Connector
Mailbox Connector
SendEMail Function Component

TIM DSMLv2 Connector
DSMLv2 SOAP Connector
DSML v2 SOAP Server Connector
Generic JNDI Connector
ITIM Agent Connector

EMF SDOToXML Function Component
EMF XMLToSDO Function Component

Timer Connector

As of June 26,2010

AssembyLines

Add new TSIEM event sources easily.

Generic Log Adapter Connector
RAC Connector
CBE (Common Base Event) components

JMX Connector
SNMP Connector
SNMP Server Connector
TCP Connector
TCP Server Connector

Remedy/Peregrine /CCMDB tickets
Maximo MEA / IF
Many custom Components on
OPAL, tdi-users.org or on request

PeopleSoft Connector
Siebel Connector
SAP ALE IDoc Connector
SAP R/3 Business Object Repository
SAP R/3 User Registry
SAP R/3 RFC Component

Script Connector
Generic Java Method
Parser FC

Remote secure command Line
z/OS TSO/E Command Line
Command Line Connector
MemQueue Connector

Memory Stream Connector

HTTP/REST Connector
File System Connector
FTP Client Connector
URL Connector
HTTP Client
HTTP Server Connector

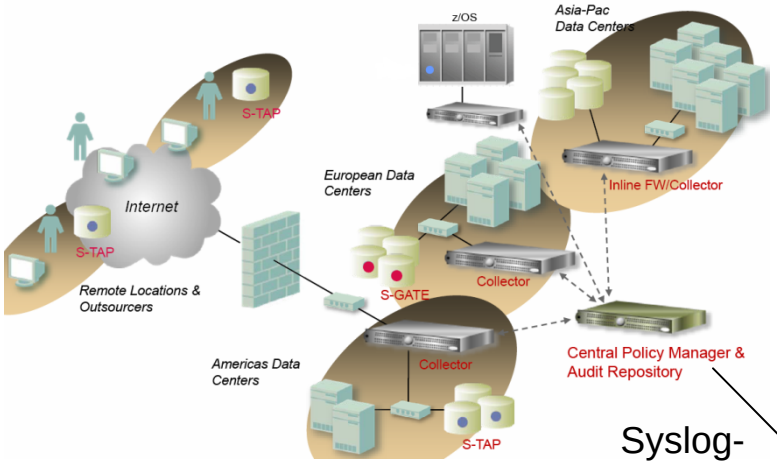
IBM MQ Series Connector
JMS Pub/Sub Connector
MQe Password Store Connector

CCMDB
Netcool
RSS

Parsers
CSV
DSML v1 & v2
Fixed Record
HTTP
LDIF
Line reader/writer
SOAP
Script
XML
XML Sax
XSL

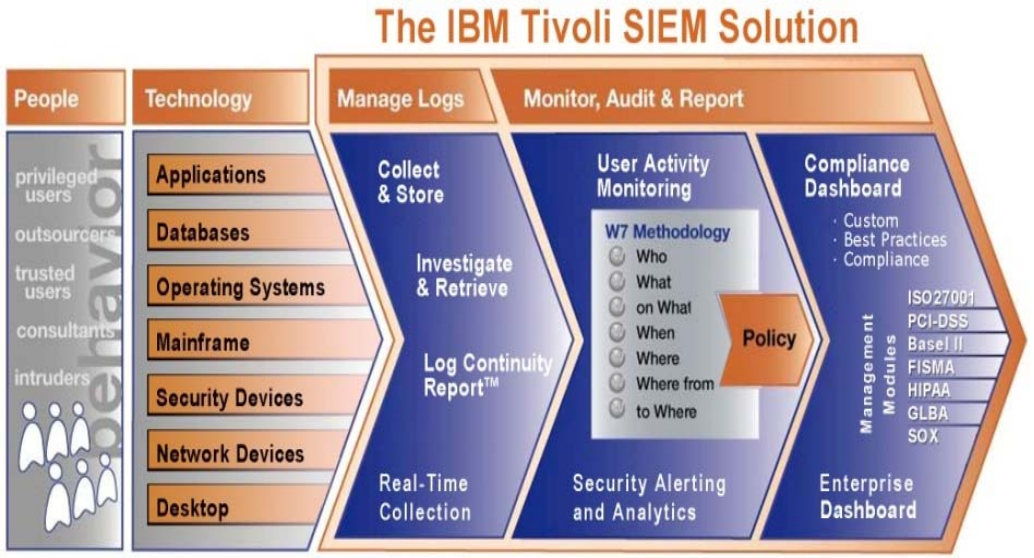
© 2011 IBM Corporation

TSIEM with Guardium: Database monitoring
Low overhead with no reliance on native logging



- Granular database monitoring and protection
- Low overhead; no reliance on native logging
- Database location and classification
- Database assessment and hardening
- Automated compliance reporting and workflow
- Export alerts and key data to TSIEM

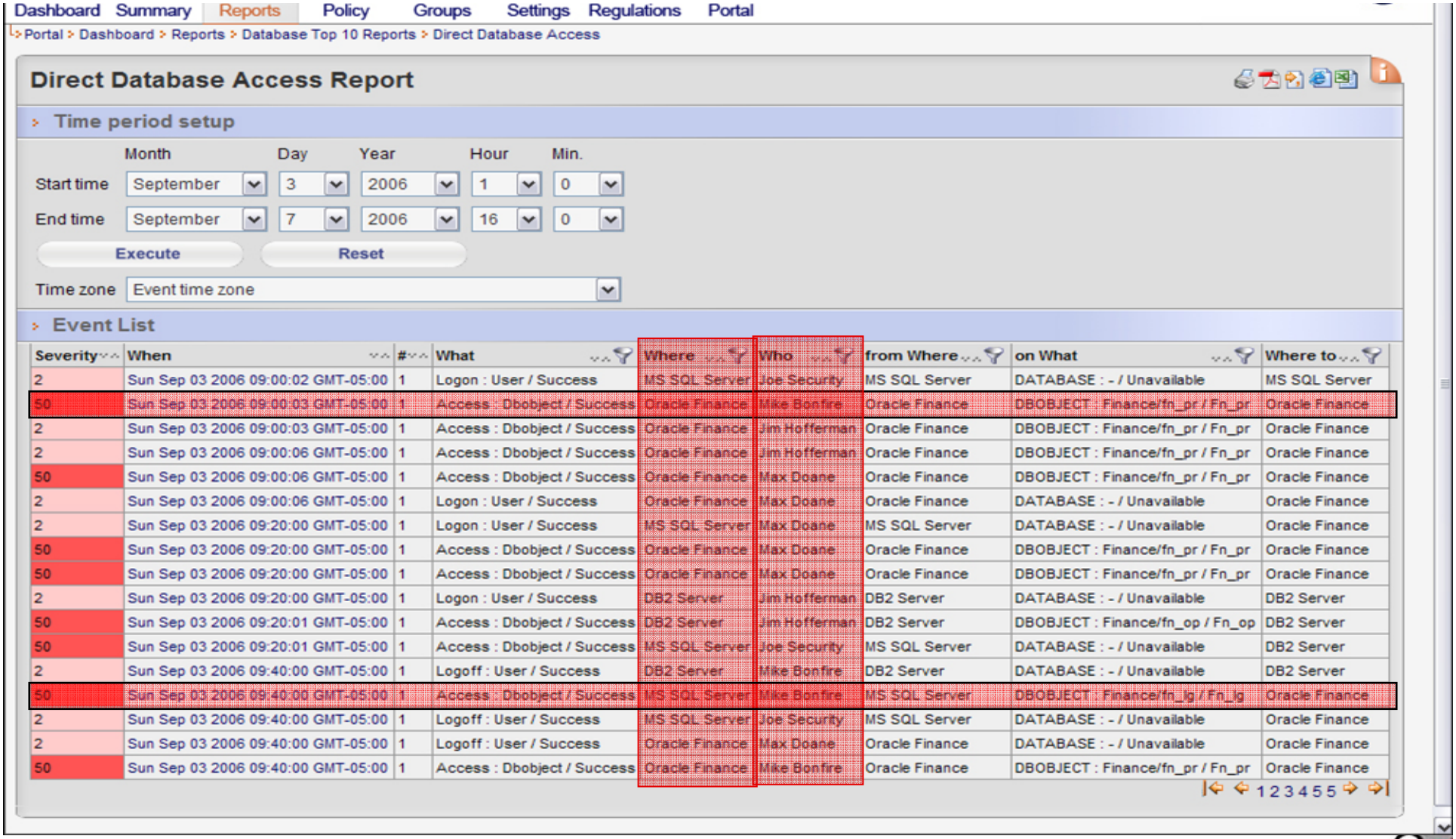
Syslog-CEF Feed



- Integrate Guardium alerts and data
- Enterprise compliance and audit
- Forensics
- Log management
- Compliance management modules for ISO27001, GLBA, SOX, HIPAA, etc.

© 2011 IBM Corporation

Example: Database Activity Monitoring with TSIEM



Dashboard Summary Reports Policy Groups Settings Regulations Portal

Portal > Dashboard > Reports > Database Top 10 Reports > Direct Database Access

Direct Database Access Report

Time period setup

	Month	Day	Year	Hour	Min.
Start time	September	3	2006	1	0
End time	September	7	2006	16	0

Execute Reset

Time zone: Event time zone

Event List

Severity	When	#	What	Where	Who	from Where	on What	Where to
2	Sun Sep 03 2006 09:00:02 GMT-05:00	1	Logon : User / Success	MS SQL Server	Joe Security	MS SQL Server	DATABASE : - / Unavailable	MS SQL Server
50	Sun Sep 03 2006 09:00:03 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Mike Bonfire	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:03 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Jim Hofferman	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Jim Hofferman	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
50	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Max Doane	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Logon : User / Success	Oracle Finance	Max Doane	Oracle Finance	DATABASE : - / Unavailable	Oracle Finance
2	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Logon : User / Success	MS SQL Server	Max Doane	MS SQL Server	DATABASE : - / Unavailable	Oracle Finance
50	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Max Doane	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
50	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Max Doane	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Logon : User / Success	DB2 Server	Jim Hofferman	DB2 Server	DATABASE : - / Unavailable	DB2 Server
50	Sun Sep 03 2006 09:20:01 GMT-05:00	1	Access : Dbobject / Success	DB2 Server	Jim Hofferman	DB2 Server	DBOBJECT : Finance/fn_op / Fn_op	DB2 Server
50	Sun Sep 03 2006 09:20:01 GMT-05:00	1	Access : Dbobject / Success	MS SQL Server	Joe Security	MS SQL Server	DATABASE : - / Unavailable	DB2 Server
2	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	DB2 Server	Mike Bonfire	DB2 Server	DATABASE : - / Unavailable	DB2 Server
50	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Access : Dbobject / Success	MS SQL Server	Mike Bonfire	MS SQL Server	DBOBJECT : Finance/fn_lg / Fn_lg	Oracle Finance
2	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	MS SQL Server	Joe Security	MS SQL Server	DATABASE : - / Unavailable	Oracle Finance
2	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	Oracle Finance	Max Doane	Oracle Finance	DATABASE : - / Unavailable	Oracle Finance
50	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Mike Bonfire	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance

1 2 3 4 5 5

© 2011 IBM Corporation

ISO 27001/2 Reporting

Regulations Resource Center

- ▸ HIPAA
- ▸ NERC CIP
- ▸ GLBA
- ▸ FISMA
- ▸ COBIT
- ▸ PCI-DSS v1.2
- ▾ ISO 27001
  - Classification Template
  - Policy Template
  - Reports
  - Documentation
- ▾ BASEL II
  - Classification Template
  - Policy Template
  - Reports
  - Documentation
- ▸ Sarbanes Oxley

The resource center provides pre-defined classification and policy templates, reports, and a reference material.

Classification Template

download

- ▸ Who (group)
- ▸ What (group)
- ▸ On What (group)
- ▸ When (group)
- ▾ Where (group)

Group name	Description
Customer	Customer systems
Customer Information Systems	Customer Information Systems are systems that process customer data such as invoice processing , credit history etc.
Finance	All workstations and servers owned by Finance
HR	All workstations and servers owned by Human Resources
Local Workstation	A workstation installed and used within the organisation
Mail	Devices and systems handling e-mail
Management Workstation	Management Workstations used to gather and display systems management data and events

Policy Template

download

▾ Policy Rules

Who (group)	What (group)	When (group)	Where (group)	On What (group)	Where From (group)	Where To (group)	Description
HR Management		Out of Office Hours		HR Data			
Managers		Office Hours					
HR Staff		Office Hours		HR Data	Local Workstation		
Marketing		Office Hours		Customer Data			
IT							
Finance Staff		Office Hours		Financial Data			
Sales Management							
Sales Staff							
		System					
		System					
Administrators							
		Logon					
Users							

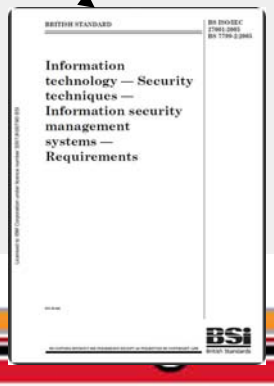
▸ Attention Rules

ISO 27001-Regulation Reports

Import custom reports | Add custom reports

ISO 27001

Title	Description	Action
ISO 27001 (5.1) Information security policy	Current, active security policy	
ISO 27001 (7.1.1) Classification	Assets defined to the system	
ISO 27001 (7.1.2) Accountability for assets	Asset classification and ownership	
ISO 27001 (10.1.2,12.5) Operational change control	Changes to the operating environment such as system updates, DBA activity etc.	
ISO 27001 (10.2.2) External contractors	Exceptions and failures caused by External Contractors	
ISO 27001 (10.4) Covert channels and trojan code	Exceptions found from anti-virus software	
ISO 27001 (10.6) Network management	Actions and events caused by users on Network Services.	
ISO 27001 (10.8.4) Mail server	Exceptions and failures for the Mail Server assets	
ISO 27001 (10.9.3) Publicly available systems	Actions and exceptions on Publicly Published Data	
ISO 27001 (10.10.1) Log archive	Log archive dates and locations	
ISO 27001 (10.10.1) Log collection	Log collection schedule and platforms	
ISO 27001 (10.10.1) Log storage	Log storage report for all platforms	
ISO 27001 (10.10.3) Logging and reviewing events	Exceptions and failures recorded by the Tivoli Security Information and Event Manager system	
ISO 27001 (10.10.4) Operator log	Actions performed by the IT Admin staff	
ISO 27001 (11.2) Review of user access rights	Actions performed by administrators on users	
ISO 27001 (11.2.4) Supervision and review - access control	Successes and failures against key assets	
ISO 27001 (11.3.1) User responsibilities and password use	Logon failures and successes either locally or remotely	
ISO 27001 (11.4) Malicious attacks	Exceptions and failures due to malicious attacks on the network	
ISO 27001 (11.4.3) Node authentication	Authentication of connections to remote computer systems	
ISO 27001 (11.4.4) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers	



ISO 27001/2 Reporting

ISO 27001-Regulation Reports

Import custom reports | Add custom reports

Reports Overview, showing first screen of many available report selections mapped to the ISO27001 control objectives and controls in Annex A.

ISO 27001

Title	Description	Action
ISO 27001 (5.1) Information security policy	Current, active security policy	
ISO 27001 (7.1.1) Classification	Assets defined to the system	
ISO 27001 (7.1.2) Accountability for assets	Asset classification and ownership	
ISO 27001 (10.1.2,12.5) Operational change control	Changes to the operating environment such as system updates, DBA activity etc.	
ISO 27001 (10.2.2) External contractors	Exceptions and failures caused by External Contractors.	
ISO 27001 (10.4) Covert channels and trojan code	Exceptions found from anti-virus software	
ISO 27001 (10.6) Network management	Actions and events caused by users on Network Services.	
ISO 27001 (10.8.4) Mail server	Exceptions and failures for the Mail Server assets	
ISO 27001 (10.9.3) Publicly available systems	Actions and exceptions on Publicly Published Data	
ISO 27001 (10.10.1) Log archive	Log archive dates and locations	
ISO 27001 (10.10.1) Log collection	Log collection schedule and platforms	
ISO 27001 (10.10.1) Log storage	Log storage report for all platforms	
ISO 27001 (10.10.3) Logging and reviewing events	Exceptions and failures recorded by the Tivoli Security Information and Event Manager system	
ISO 27001 (10.10.4) Operator log	Actions performed by the IT Admin staff	
ISO 27001 (11.2) Review of user access rights	Actions performed by administrators on users	
ISO 27001 (11.2.4) Supervision and review - access control	Successes and failures against key assets	
ISO 27001 (11.3.1) User responsibilities and password use	Logon failures and successes either locally or remotely	
ISO 27001 (11.4) Malicious attacks	Exceptions and failures due to malicious attacks on the network	

© 2011 IBM Corporation

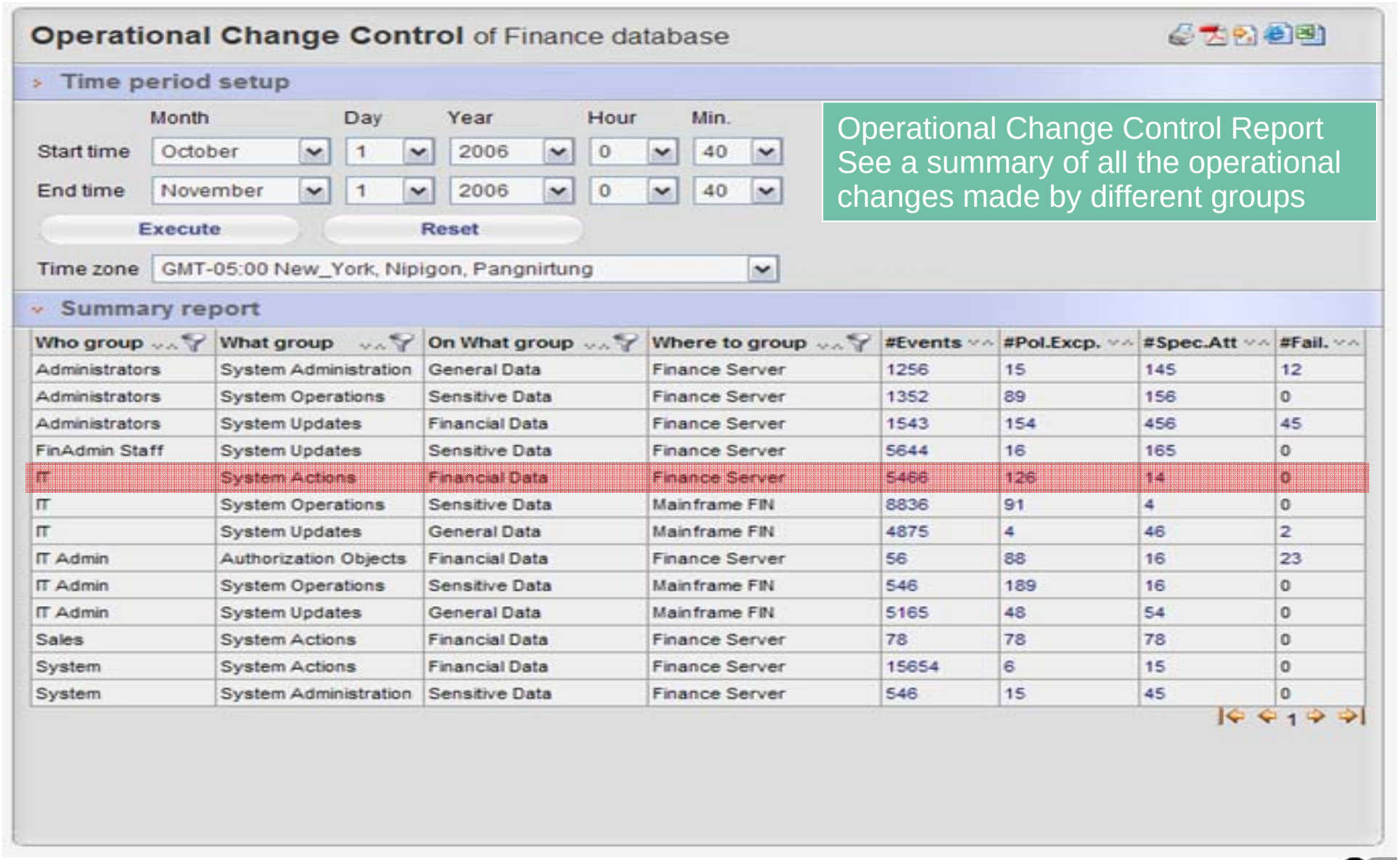
PCI-DSS Regulation Reports

Add custom report | Import custom reports

PCI-DSS

Title	Description
PCI-DSS (1.2) Network intrusions	Unauthorized network access events
PCI-DSS (1.3) Network exposures	Exposures resulting from network misconfiguration
PCI-DSS (1.4) Network access violations	Exceptions and failures on network access
PCI-DSS (2.1,2.2) Configuration exposures	Exposures resulting from systems misconfiguration
PCI-DSS (2.3) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers.
PCI-DSS (5.1,5.2) Anti-virus configuration exposures	Exposures resulting from misconfiguration of anti-virus software
PCI-DSS (5.1,5.2) Covert channels and trojan code	Exceptions found from anti-virus software
PCI-DSS (6.1) Security patches	Exceptions and failures caused by insufficient security patch levels
PCI-DSS (6.3.3,6.3.4) Source code access	Exceptions and failures caused by accessing source code.
PCI-DSS (6.3.3,6.3.4) System test data	Controlled access to System test data.
PCI-DSS (7.1) Information access restrictions	Who accessed sensitive or private data successfully or unsuccessfully.
PCI-DSS (7.1) Sensitive system isolation	Exceptions and failures against sensitive systems data in asset groups Cardholder data, User, HR Data, Source Code, and Financial Data
PCI-DSS (8.5) Access Enforcement	Logon successes and failures, both locally and remotely
PCI-DSS (8.5) Account Management	System account management activity
PCI-DSS (8.5) System account policies	Exceptions and failures caused by systems account policy violations
PCI-DSS (10.2.1) Cardholder data access	Successful and failed cardholder data access
PCI-DSS (10.2.2) Operational change control	Changes to the operating environment such as system updates, DBA activity etc.

© 2011 IBM Corporation



Operational Change Control of Finance database

Time period setup

	Month	Day	Year	Hour	Min.
Start time	October	1	2006	0	40
End time	November	1	2006	0	40

Execute Reset

Time zone: GMT-05:00 New_York, Nipigon, Pangnirtung

Operational Change Control Report
See a summary of all the operational changes made by different groups

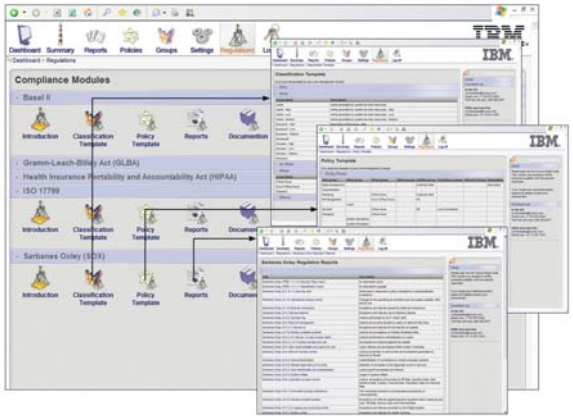
Summary report

Who group	What group	On What group	Where to group	#Events	#Pol.Excp.	#Spec.Att	#Fail.
Administrators	System Administration	General Data	Finance Server	1256	15	145	12
Administrators	System Operations	Sensitive Data	Finance Server	1352	89	156	0
Administrators	System Updates	Financial Data	Finance Server	1543	154	456	45
FinAdmin Staff	System Updates	Sensitive Data	Finance Server	5644	16	165	0
IT	System Actions	Financial Data	Finance Server	5466	126	14	0
IT	System Operations	Sensitive Data	Mainframe FIN	8836	91	4	0
IT	System Updates	General Data	Mainframe FIN	4875	4	46	2
IT Admin	Authorization Objects	Financial Data	Finance Server	56	88	16	23
IT Admin	System Operations	Sensitive Data	Mainframe FIN	546	189	16	0
IT Admin	System Updates	General Data	Mainframe FIN	5165	48	54	0
Sales	System Actions	Financial Data	Finance Server	78	78	78	0
System	System Actions	Financial Data	Finance Server	15654	6	15	0
System	System Administration	Sensitive Data	Finance Server	546	15	45	0

1

© 2011 IBM Corporation

Demonstrate effective controls



- Regulation specific Compliance Management Modules
  Jump start compliance reporting
- Easy to use enterprise compliance management dashboa
  Quickly gain overview of your compliance posture
- Generate highly relevant reports to view your level of compliance
  Streamline compliance management to respond to auditor's request
- Monitor most crucial events that need to be in compliance
  Prioritize so that you can mitigate threats
- Establish stringent policies, compare user behavior with that policy
  Prepare for audits and ensure compliance
- **Leverage Business Analytics to enrich Risk Management decision-making**
  Integrate with GRC and external applications

© 2011 IBM Corporation

Harley-Davidson is at the forefront of Compliance Management Implementations

Value

- Realized a return on their investment, from first day on
  - Detected malicious email and addressed affected machines in real time
- Closed the loop on user access provisioning
- Improved operational efficiency and reduced costs

Business Challenge

Compliance with GLBA, PCI and SOX

- Mgmt of insider threats and reduction of risk from privileged users
- Monitoring of external perimeter threats
- Monitoring the effectiveness of the identity and access management process

Solution

Tivoli Security Information and Event Management:

- Monitors privileged user activity,
- Provides forensic evidence
- Consolidates data for compliance
- Provides SOX, GLBA, and PCI reports

© 2011 IBM Corporation

APG uses Tivoli Security Information and Event Management to efficiently facilitate compliance efforts

Value

- ***Faster access to information***
- ***Accelerated root cause analysis***
- ***Attractive pricing model***
- ***Allows staff to efficiently prepare and respond to audit requests—such as Statement on Auditing Standards (SAS) No. 70 reporting requirements***

Business Challenge

Protect access across the enterprise including 12 different types of systems

- Prove that only people who should access client information can access client information
- Better insight and more in-depth reporting

Solution

Tivoli Security Information and Event Management helps them:

- Centralize log management, across hundreds of systems.
- Unobtrusively monitor and report on privileged user activities
- Demonstrate to auditors and management that effective controls are in place.

"With IBM Tivoli Security Information and Event Manager, we can prove what has happened inside of our systems instead of guessing."
— Riet Spigkirboer, Information Security Administrator, APG

© 2011 IBM Corporation

OpenPages - Proven by the World's Leading Companies

Financial Services

BARCLAYS
Lloyds TSB
ABSA
Bank of America
ING
FIRSTRAND
BMO Financial Group
MasterCard
ORX ASSOCIATION
UnionBank
ICAP
NATIONAL BANK OF GREECE

Insurance

AVIVA
AIG
GEICO
Swiss Re
Allianz

Energy and Power

Duke Energy
bp
BAKER HUGHES
Williams
PG&E
ALLETE

Health Services / Pharmaceuticals

CardinalHealth
HCA Hospital Corporation of America

Manufacturing

DRS TECHNOLOGIES
WORTHINGTON INDUSTRIES
WOLSELEY

Retail/Consumer

Del Monte
Constellation
mc

Telecommunications

vodafone
meteor

© 2011 IBM Corporation

44

Questions

© 2011 IBM Corporation

Thank You

© Copyright IBM Corporation 2011. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, Rational, the Rational logo, Telelogic, the Telelogic logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.