Risk Analytics

IBM Internal Audit:
An Essential Component of Governance, Risk and Compliance

Dave Erickson
Risk Analytics Business Development Executive
East US

Devin Hart
IBM Risk Analytics
New York

NYSICA
New York State Internal Control Association

Agenda

1. The future of Governance Risk and Compliance
2. Internal audit and its function within Governance Risk and Compliance
3. Challenges for internal audit
4. IBM’s internal audit capabilities and best practices
5. Questions

GRC: Key concepts

Risk management

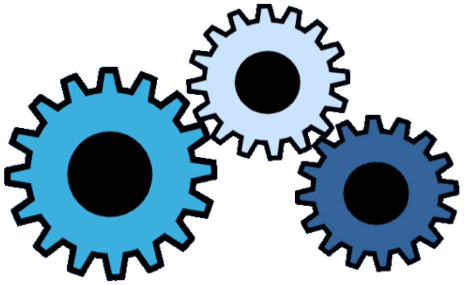
The set of activities designed to support maximum business performance through the identification, measurement, and treatment of uncertainty.

Governance

The values, culture, policies, processes, and oversight that define the structure by which the organization directs and manages itself.

Compliance

The act of adhering to, and demonstrating adherence to, regulations, standards, policies, and procedures.



GRC

The coordination of these three domains to **improve efficiency** with shared resources and **strengthen decision-making** by producing more complete and accurate information.

GRC represents the parameters within which a company drives success.

The Enterprise GRC platform will continue to extend its reach

Extension into New GRC Domains

Companies are moving a range of **risk oversight** functions onto GRC platforms, such as fraud risk, model validation, new product approval, vendor risk and business continuity

GRC Convergence

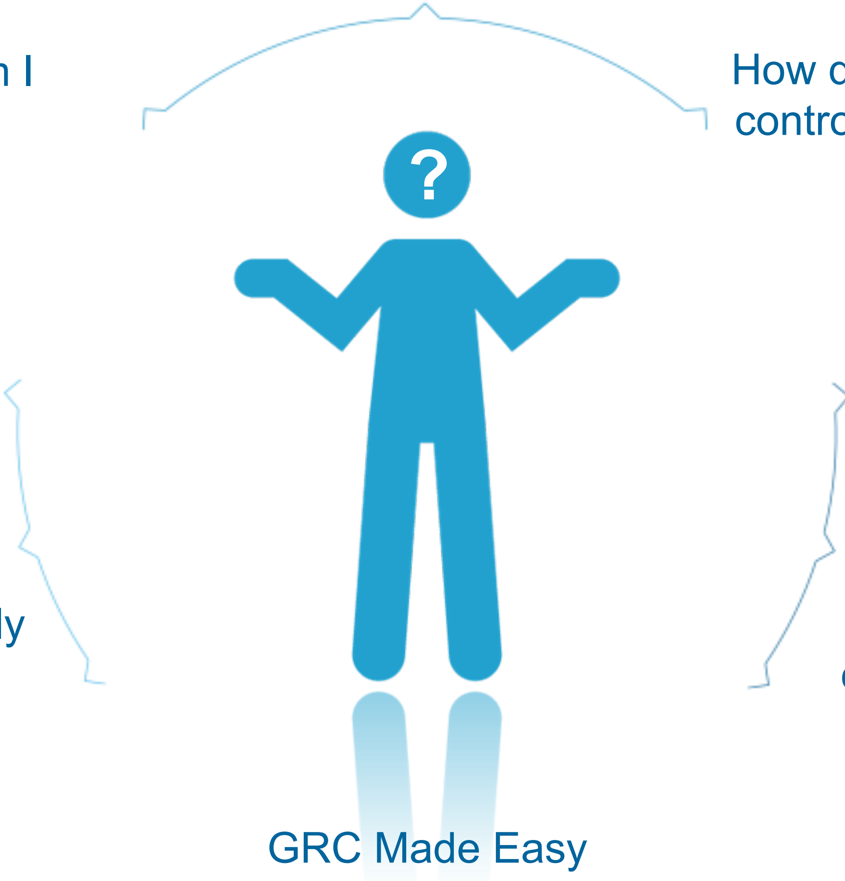
The financial crisis showed the importance of **integrated risk management** to optimize outcomes. Inability to aggregate and share risk across the business was a key deficiency. The importance of the GRC platform has increased as a buying priority

Integration with Operational Systems

As GRC practices mature, there is an increased requirement for **integration with operational systems** including IT security, fraud detection, claims systems, and portfolio management

Every member of an organization is responsible for governance, risk management and compliance

from top executives and the board to business process owners and front line staff



What GRC tasks am I responsible for?

How do I know which risks and controls have been assessed?

How do I easily find the relevant data that I need?

What is the context of the risks that I manage?

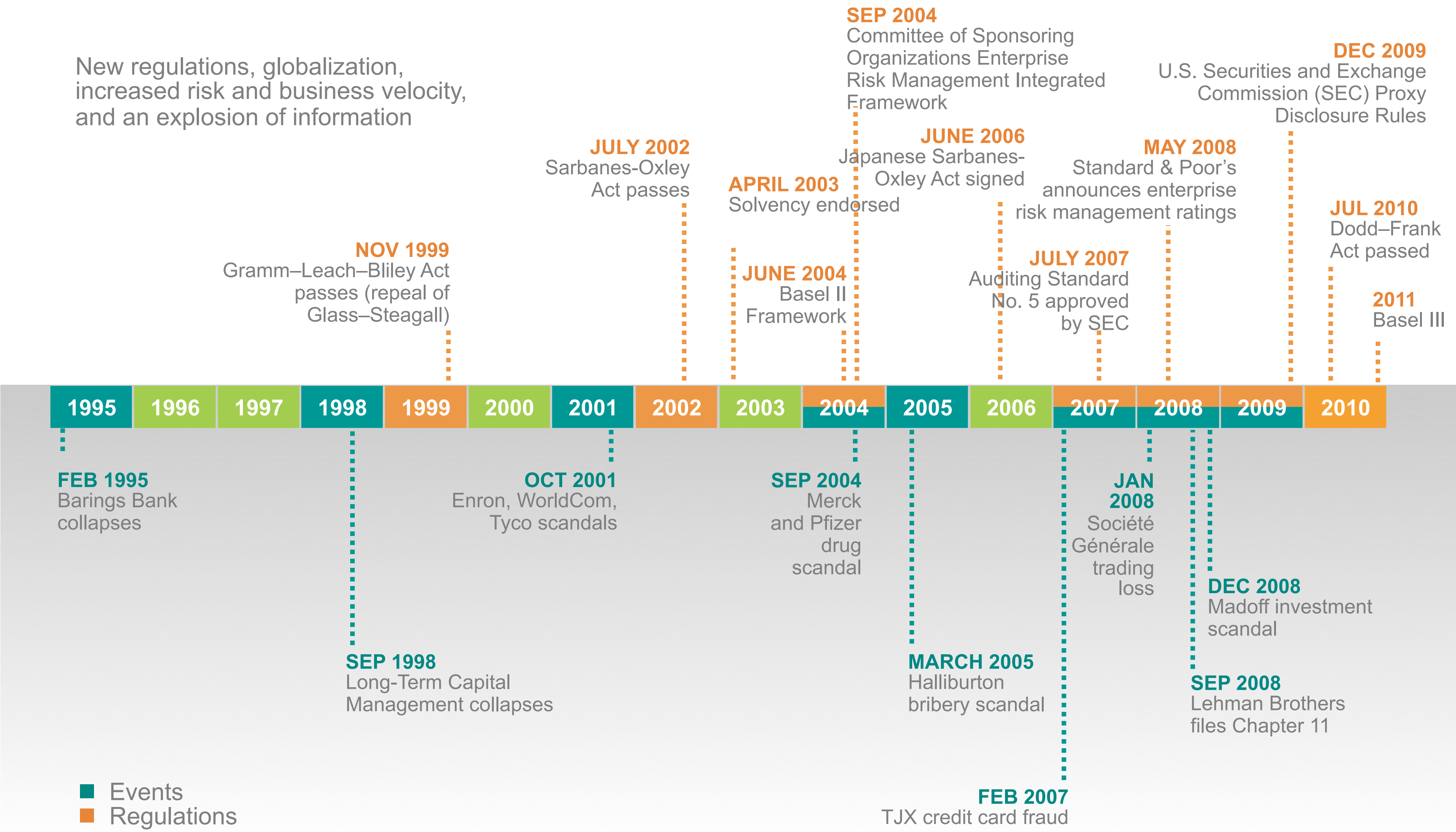
How can I more efficiently update my GRC data?

How do the risks and controls compare across the processes that I manage?

GRC Made Easy

Risk is a significant challenge in today’s business environment

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



1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010

FEB 1995
Barings Bank collapses

SEP 1998
Long-Term Capital Management collapses

NOV 1999
Gramm–Leach–Bliley Act passes (repeal of Glass–Steagall)

OCT 2001
Enron, WorldCom, Tyco scandals

JULY 2002
Sarbanes-Oxley Act passes

APRIL 2003
Solvency endorsed

JUNE 2004
Basel II Framework

SEP 2004
Committee of Sponsoring Organizations Enterprise Risk Management Integrated Framework

SEP 2004
Merck and Pfizer drug scandal

MARCH 2005
Halliburton bribery scandal

JUNE 2006
Japanese Sarbanes-Oxley Act signed

FEB 2007
TJX credit card fraud

JULY 2007
Auditing Standard No. 5 approved by SEC

JAN 2008
Société Générale trading loss

MAY 2008
Standard & Poor’s announces enterprise risk management ratings

SEP 2008
Lehman Brothers files Chapter 11

DEC 2008
Madoff investment scandal

DEC 2009
U.S. Securities and Exchange Commission (SEC) Proxy Disclosure Rules

JUL 2010
Dodd–Frank Act passed

2011
Basel III

■ Events
■ Regulations

Risk management failures can be hugely damaging in terms of direct losses as well as reputational damage

UBS reaches $50m settlement over bond

— *The Times*
August 7, 2013

Nationwide Insurance data breach affects 1.1 million people

— NBC News
December 6, 2012

Outages hit Bank of America electronic and phone banking

— *Los Angeles Times*
February 1, 2013

TD Bank to pay $52.5 million in U.S. settlements over Ponzi scheme

— *Reuters*
September 23, 2013

JP Morgan agrees to $5.1bn fine with mortgage regulator

— *The Guardian*
October 25, 2013

There is a growing need to manage risks that can affect operational performance

Insider threats, cyber crime and fraud cost billions and affect reputation

Network security

Theft of information related to SecurID tokens affected 40 million people who use the tokens to access the internal computer networks of 25,000 corporations, including defense contractors.

Data privacy

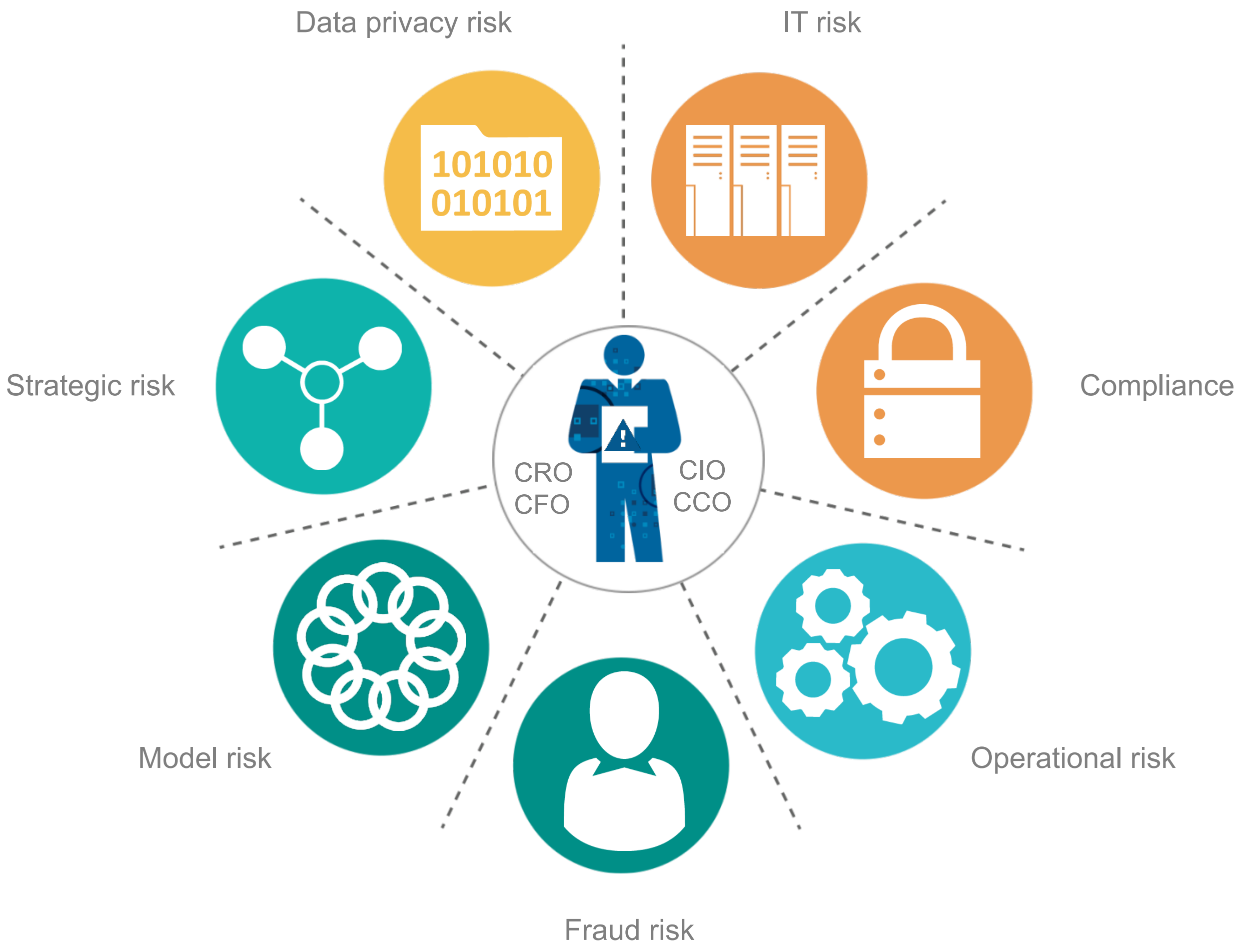
Personal information including credit and debit card numbers was stolen from more than100 million accounts of a prominent game console.

Access control

A trader familiar with access controls from years spent in the compliance department of a multinational banking and financial services company cost that company more than USD7 billion.

Most companies have a fragmented view of risk

and have trouble leveraging risk information for better decisions



Risk managers face a range of challenges today

The top of the list includes regulation, governance and profitability

Pressure on boards to improve risk oversight

Risk governance expanding to new areas such as social, third party and model validation

Regulatory proliferation and increased rate of change

Increased regulatory scrutiny and supervision

Elevated interest in operational risk

Aligning risk and performance management

Organizations are moving beyond collection of data to risk-aware decision making

Business requires an integrated view of risk across the enterprise

Data challenges

Challenges

- Data silos
- Manual data processes
- No data controls
- No data archiving
- No data/model separation

Opportunities

- Data warehouse
- Automated data processes
- Secured/audited data
- Archived data
- Data/model separation

Accurate, secure, audited data is needed so that

Risk information can be trusted for decision-making

Reporting challenges

Challenges

- Disparate systems
- Spreadsheet models
- Inconsistent assumptions
- Lack of version control
- Lack of controls

Opportunities

- Integrate disparate models
- Limited spreadsheet use
- Consistent assumptions
- Grid enabled
- Model controls

Consistent and reliable reporting is needed so that

Risk information can be trusted for decision-making

New York State Audit Recommendations

provided
include
staff
agreements
procurement
monitor
annual
State
balance
supported
accordance
Owners
Offi
process
statements
payment
approved
Perform
audit
officials
costs
Council
individual
inmate
student
time
cials
collection
detailed
bills
contract
accruals
list
accuracy
project
maintain
agency
capital
cash
approval
report
accounts
written
appropriate
enforce
Law
verify
Require
projects
service
Department
records
payroll
inspections
annually
debt
Adopt
reports
District
bank
provide
properly
financial
rights
ce
employee
made
billing
plan
funds
including
worked
prior
Controller
determine
required
receipts
independent
documentation
within
job
policies
offi
compliance
procedures
code
County
bridge
City
Treasurer
accurate
Develop
review
tax
Town
Fiscal
maintenance
contracts
benefits
policy
complete
item
use
adequate
budget
controls
manner
retained
documented
regarding
Review
timely
fund
lead
services
management
reconciliations
Sheriff
Implement
disbursements
claims
system
develop
paid
students
forms
overtime
approve
pricing
operations
expenditures
President
information
Company
actual
hours
require
budgets
leave
pay
indicating
assign
accounting
document
duties
Foundation
work
reviews
current
checks

NYSICA

New York State Internal Control Association

Challenges for internal audit

- Audit committees to support and strengthen internal and external audit functions, internal controls, and financial management and financial reporting functions are more common in state governments (NY State is a good example)

- Changes in SOX or SOX-like financial requirements

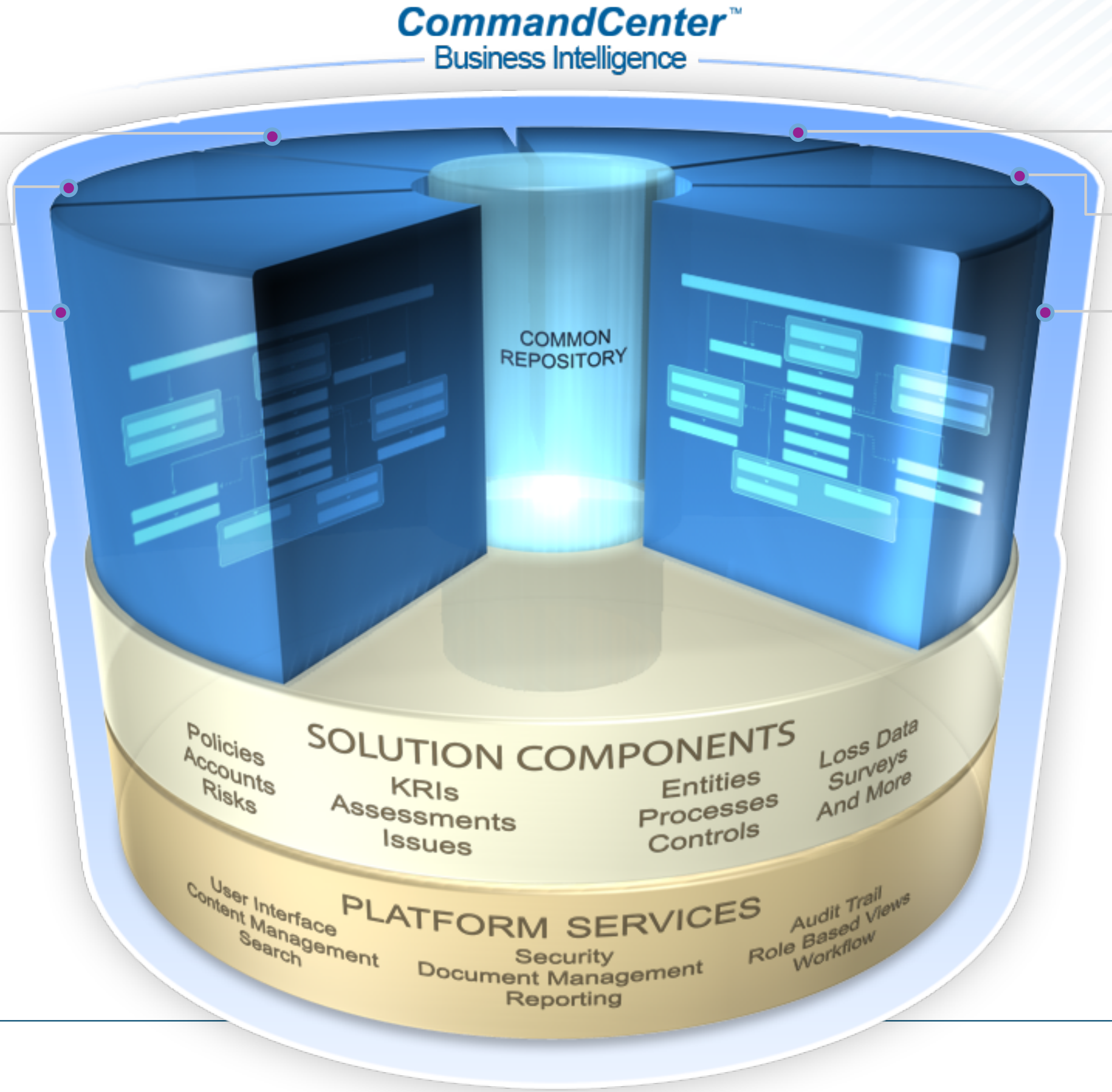
- Annual reports on activity (consolidating data)

- Performance evaluations (self-testing)

- Gathering accurate and consistent testing evidence

- Improving audit efficiency (resource planning, workflow)

IBM’s Integrated Approach to Risk Management



Internal Audit Management

Financial Controls Management

IT Risk & Compliance Management

Operational Risk Management

Policy & Compliance Management

Other Platform Extensions (New Product Approval, Business Continuity Management, Vendor Management, Model management & Enhancement request tracking, etc.)

Governance, risk and compliance solutions from IBM can help you overcome these challenges

Integrate multiple areas of risk and compliance by having a central platform for integrated reporting, workflow and policies.

Support virtually any risk management methodology via a patented, adaptable framework enabling easier configuration.

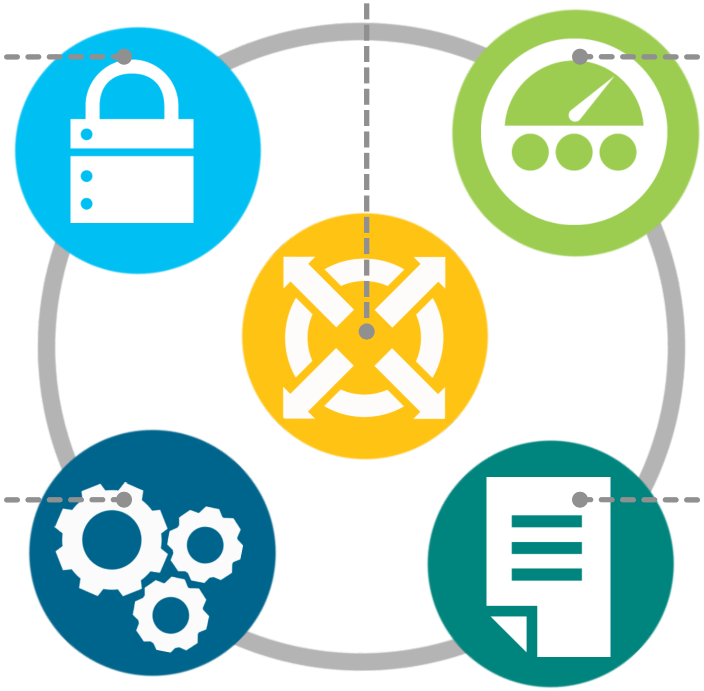
Provide visibility into the state of risk in business with interactive dashboards and ad hoc reports for decision support.

Facilitate an ecosystem of process, technology and content to provide better alignment and value to the business.

Automate the compliance and risk management activities' powerful workflow for automating business processes.

Centralize oversight, reporting, accountability, social collaboration, and visual and predictive analytics.

Supporting GRC according to your organization’s current state of readiness and maturity



Data model
Record types
Fields
Record relationships
Field dependencies

Security model
Users
Roles
Delegated administration

User interface configuration
Menu layout
Home page layout
Hierarchy views
List views
Form layout
Activity views

Business automation
Job types
Tasks
Business rules

Reporting framework
Reporting views
Reports
Ad hoc query

Supports your methodology and your process
Can lower total cost of ownership and increase user adoption

New York State Audit Recommendations

provided
Perform
include
staff
audit
agreements
procurement
monitor
annual
State
balance
supported
accordance
Owners
Offi
individual
detailed
process
statements
bills
payment
approved
contract
accruals
list
approval
enforce
report
Law
Require
payroll
inspections
annually
inmate
student
time
officials
cials
costs
Council
collection
cash
accuracy
accounts
project
verify
maintain
written
appropriate
agency
capital
records
projects
service
Department
debt
properly
financial
rights
ce
Adopt
employee
reports
made
District
bank
provide
billing
Controller
determine
required
plan
funds
including
worked
prior
compliance
procedures
City
Treasurer
receipts
code
County
independent
documentation
within
job
policies
offi
accurate
Develop
review
bridge
contracts
tax
Town
Fiscal
maintenance
policy
benefits
timely
complete
item
use
adequate
students
budget
controls
manner
retained
documented
regarding
Review
lead
fund
Sheriff
Implement
disbursements
claims
system
develop
paid
services
management
reconciliations
operations
forms
expenditures
overtime
approve
pricing
assign
actual
hours
require
budgets
President
information
Company
document
duties
Foundation
accounting
leave
pay
indicating
work
reviews
current
checks

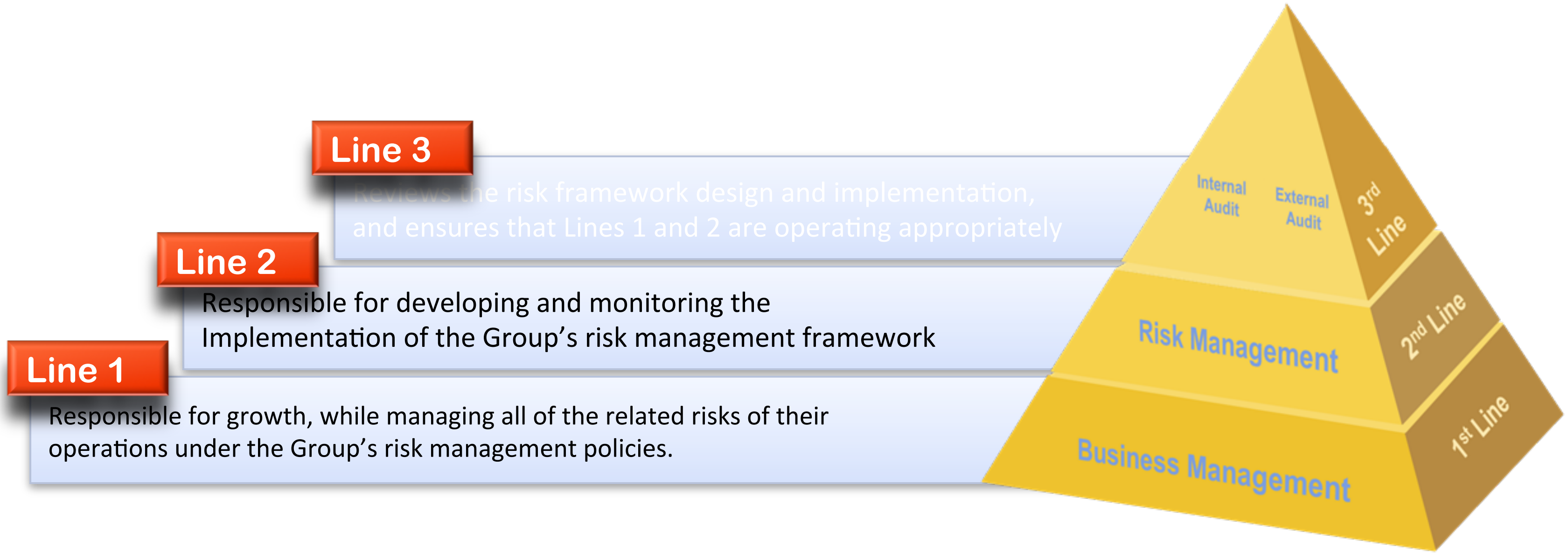
NYSICA
New York State Internal Control Association

3 Lines of Defence Model

3 Lines of Defence is a governance model to provide integrity over its risk management practices.

Operationally, the model defines three levels of risk management accountabilities and the boundaries that exist between each level, to provide a complete system of risk management.

The pyramid is an effective representation of the model as it graphically shows the breadth and depth of risk management practices that should exist at each level to complete the risk management system.



Line 3

Reviews the risk framework design and implementation, and ensures that Lines 1 and 2 are operating appropriately

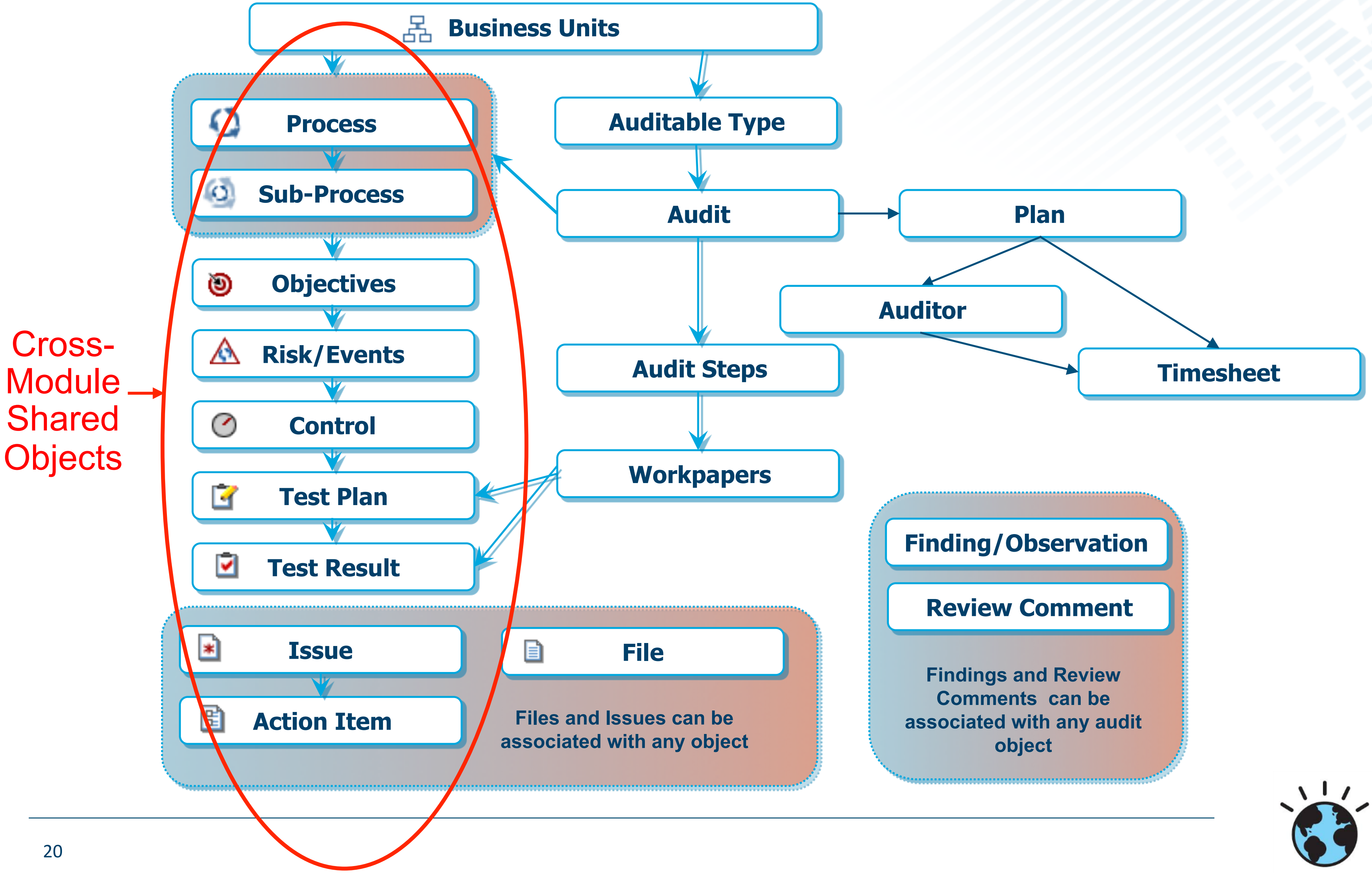
Line 2

Responsible for developing and monitoring the Implementation of the Group's risk management framework

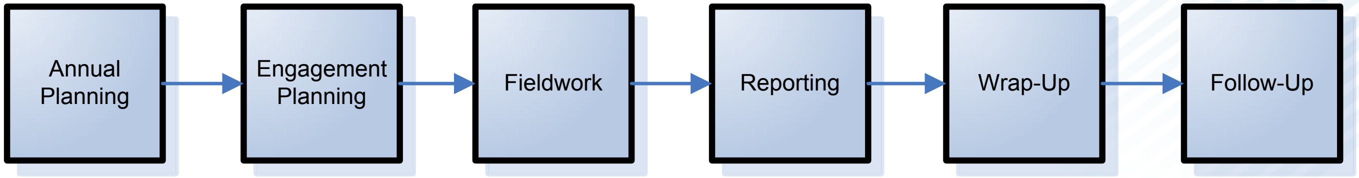
Line 1

Responsible for growth, while managing all of the related risks of their operations under the Group's risk management policies.

Audit Framework Example with Add’l Audit Data Elements



Overview of Capabilities in Internal Audit



Annual Planning

- Define audit universe
- Perform risk assessment for scoping
- Create multi-year audit schedule

Engagement Planning

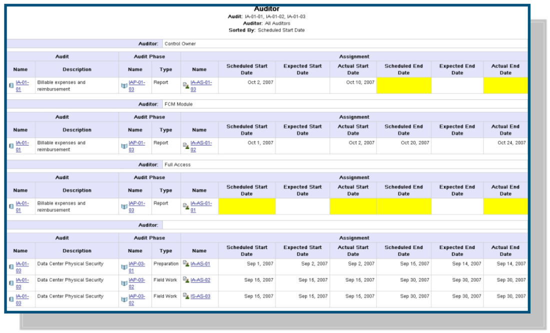
- Resource requirements
- Allocate resources
- Define scope and work programs

Fieldwork

- Perform audits
- Create and store workpapers
- Track auditor time
- Leverage management's test plans and results

Reporting, Wrap-up and Follow-up

- Generate automated audit reports
- Management Action Plans
- Prepare for future audits



Auditor

Audit: IA-01-01, IA-01-02, IA-01-03
Auditor: All Auditors
Sorted By: Scheduled Start Date

Auditor: Control Owner

Audit		Audit Phase		Assignment						
Name	Description	Name	Type	Name	Scheduled Start Date	Expected Start Date	Actual Start Date	Scheduled End Date	Expected End Date	Actual End Date
IA-01-01	Billable expenses and reimbursement	IAP-01-03	Report	IA-AS-01-03	Oct 2, 2007		Oct 10, 2007			

Auditor: FCM Module

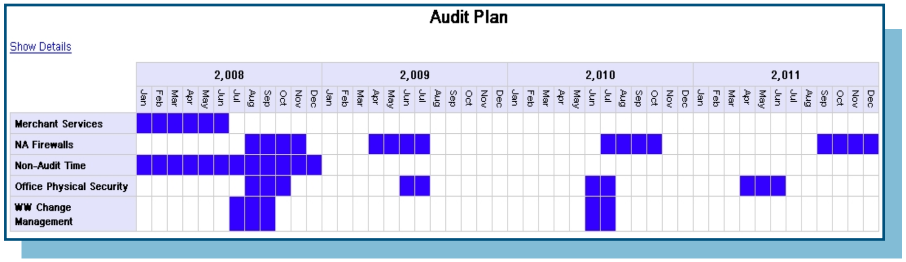
Audit		Audit Phase		Assignment						
Name	Description	Name	Type	Name	Scheduled Start Date	Expected Start Date	Actual Start Date	Scheduled End Date	Expected End Date	Actual End Date
IA-01-01	Billable expenses and reimbursement	IAP-01-03	Report	IA-AS-01-02	Oct 1, 2007		Oct 2, 2007	Oct 20, 2007		Oct 24, 2007

Auditor: Full Access

Audit		Audit Phase		Assignment						
Name	Description	Name	Type	Name	Scheduled Start Date	Expected Start Date	Actual Start Date	Scheduled End Date	Expected End Date	Actual End Date
IA-01-01	Billable expenses and reimbursement	IAP-01-03	Report	IA-AS-01-01						

Auditor:

Audit		Audit Phase		Assignment						
Name	Description	Name	Type	Name	Scheduled Start Date	Expected Start Date	Actual Start Date	Scheduled End Date	Expected End Date	Actual End Date
IA-01-03	Data Center Physical Security	IAP-03-01	Preparation	IA-AS-01	Sep 1, 2007	Sep 2, 2007	Sep 2, 2007	Sep 15, 2007	Sep 14, 2007	Sep 14, 2007
IA-01-03	Data Center Physical Security	IAP-03-02	Field Work	IA-AS-02	Sep 15, 2007	Sep 15, 2007	Sep 15, 2007	Sep 30, 2007	Sep 30, 2007	Sep 30, 2007
IA-01-03	Data Center Physical Security	IAP-03-02	Field Work	IS-AS-03	Sep 15, 2007	Sep 15, 2007	Sep 15, 2007	Sep 30, 2007	Sep 30, 2007	Sep 30, 2007



Audit Plan

Show Details

	2,008											
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Merchant Services	■	■	■	■	■	■						
NA Firewalls								■	■	■	■	
Non-Audit Time	■	■	■	■	■	■	■	■	■	■	■	■
Office Physical Security								■	■	■		
WW Change Management							■	■	■			

	2,009											
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Merchant Services												
NA Firewalls				■	■	■	■					
Non-Audit Time												
Office Physical Security						■	■					
WW Change Management												

	2,010											
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Merchant Services												
NA Firewalls							■	■	■	■		
Non-Audit Time												
Office Physical Security						■	■					
WW Change Management						■	■					

	2,011											
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Merchant Services												
NA Firewalls									■	■	■	■
Non-Audit Time												
Office Physical Security				■	■	■						
WW Change Management												

Business intelligence via IBM Cognos software

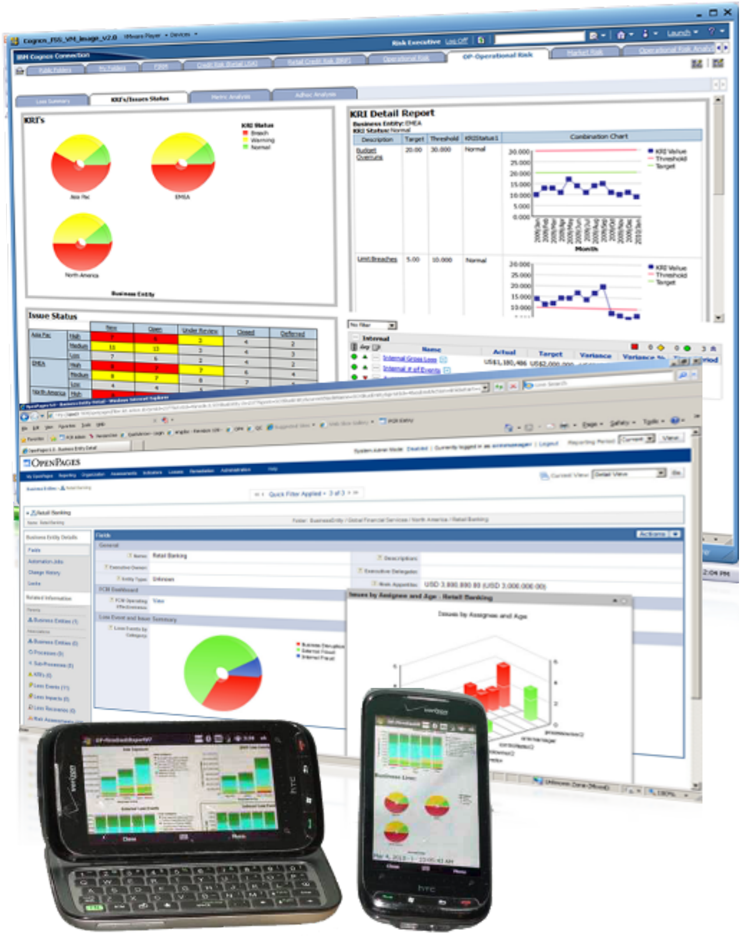
Provide rich, interactive, real-time dashboards and reports.

Enable drill-down from reports into supporting reports as well as the underlying detail data.

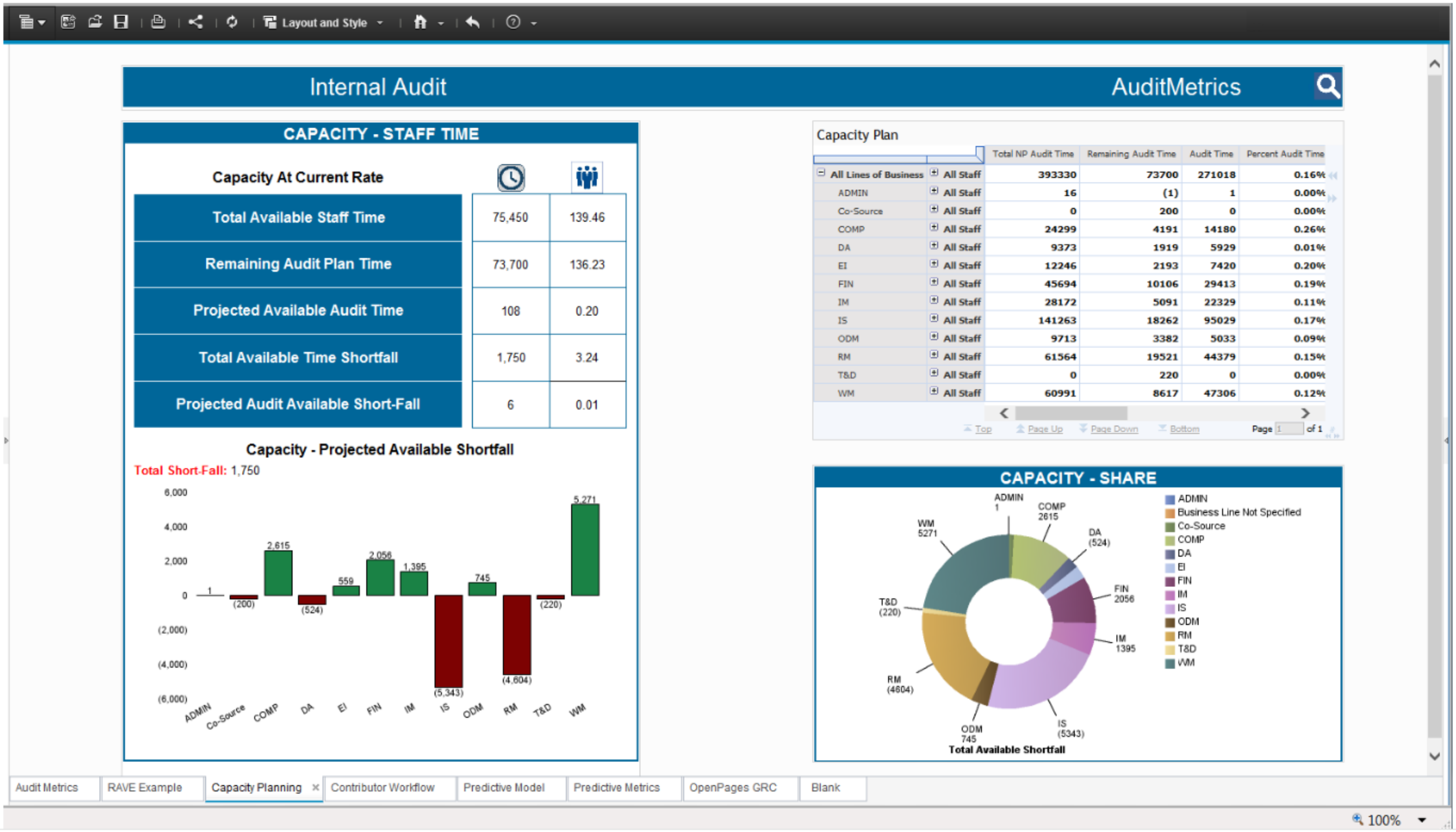
Provide comprehensive monitoring and management across the business.

Deliver executive dashboards and reports and empower the user.

Enable users to design and run reports tailored to their business needs.



Audit resource planning with immediate visualization of results



CAPACITY - STAFF TIME

Capacity At Current Rate		
Total Available Staff Time	75,450	139.46
Remaining Audit Plan Time	73,700	136.23
Projected Available Audit Time	108	0.20
Total Available Time Shortfall	1,750	3.24
Projected Audit Available Short-Fall	6	0.01

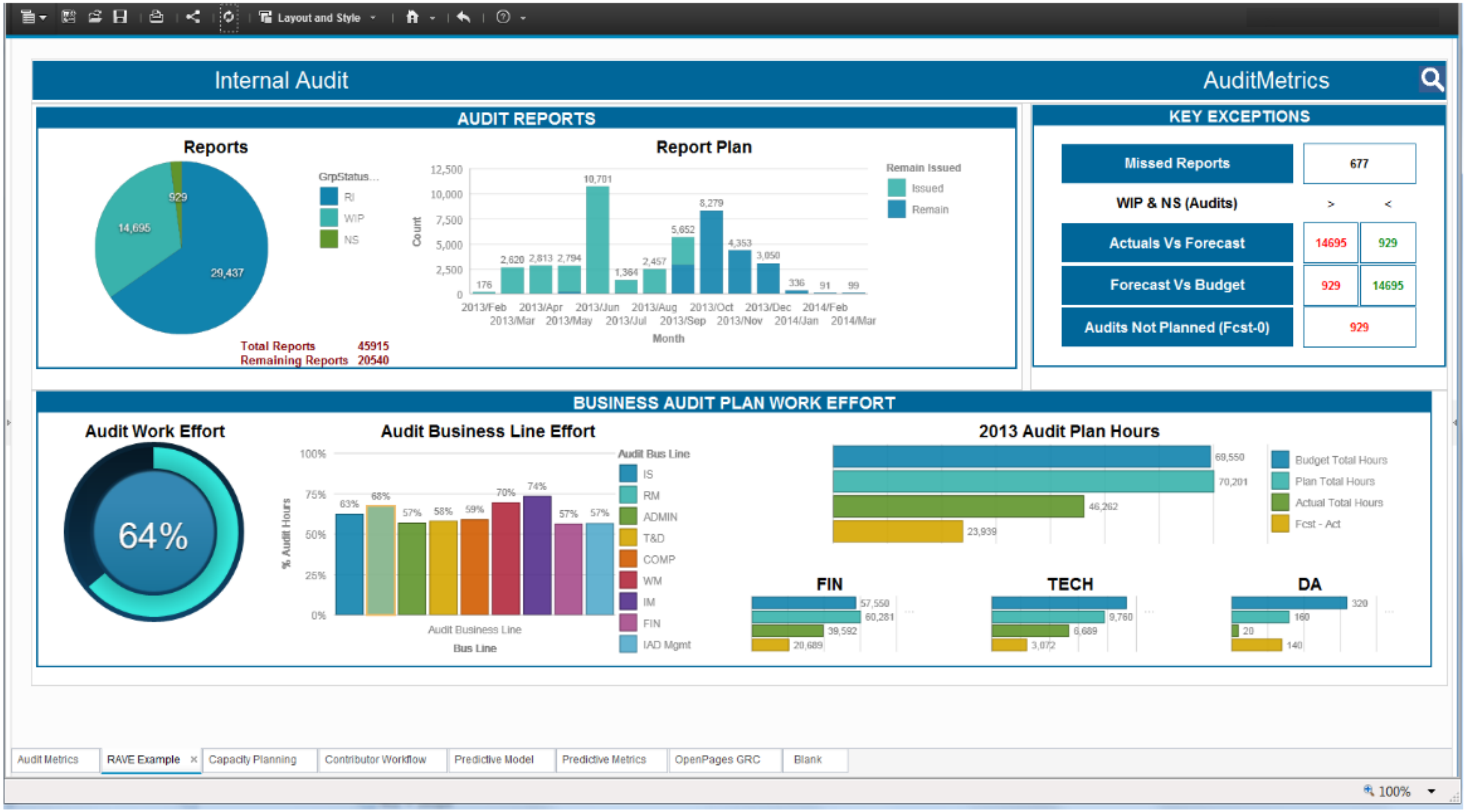
Total Short-Fall: 1,750

Capacity Plan

		Total NP Audit Time	Remaining Audit Time	Audit Time	Percent Audit Time
All Lines of Business	All Staff	393330	73700	271018	0.16%
ADMIN	All Staff	16	(1)	1	0.00%
Co-Source	All Staff	0	200	0	0.00%
COMP	All Staff	24299	4191	14180	0.26%
DA	All Staff	9373	1919	5929	0.01%
EI	All Staff	12246	2193	7420	0.20%
FIN	All Staff	45694	10106	29413	0.19%
IM	All Staff	28172	5091	22329	0.11%
IS	All Staff	141263	18262	95029	0.17%
ODM	All Staff	9713	3382	5033	0.09%
RM	All Staff	61564	19521	44379	0.15%
T&D	All Staff	0	220	0	0.00%
WM	All Staff	60991	8617	47306	0.12%

Top Page Up Page Down Bottom Page 1 of 1

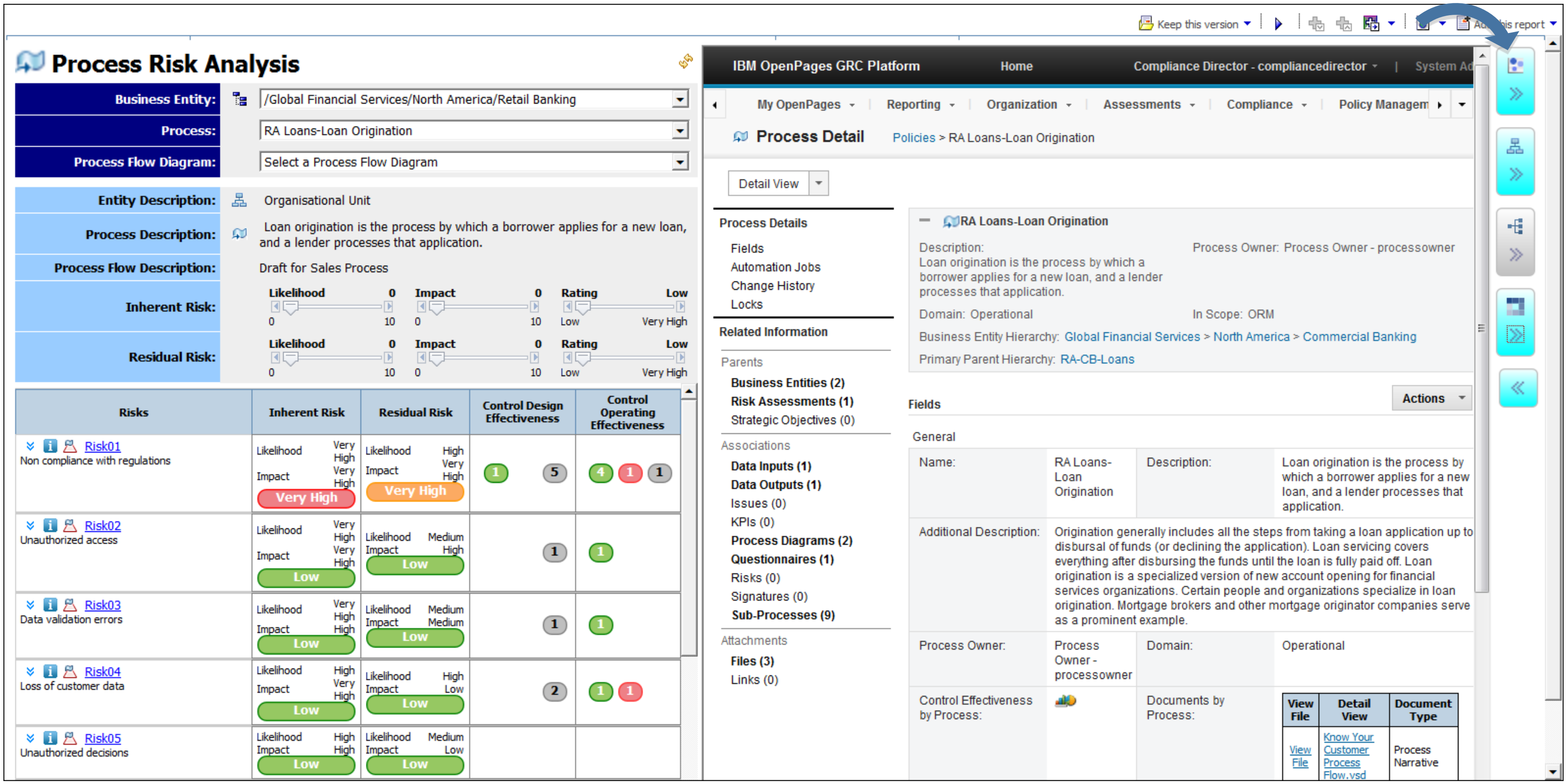
Audit Dashboards: User driven, relevant dashboard context, self-service, enterprise level, access consistent data, share reporting, dashboards,



Total Reports 45915
Remaining Reports 20540

KEY EXCEPTIONS		
Missed Reports	677	
WIP & NS (Audits)	>	<
Actuals Vs Forecast	14695	929
Forecast Vs Budget	929	14695
Audits Not Planned (Fcst-0)	929	

Interactive Reporting Visualization



Process Risk Analysis

Business Entity:	/Global Financial Services/North America/Retail Banking
Process:	RA Loans-Loan Origination
Process Flow Diagram:	Select a Process Flow Diagram
Entity Description:	Organisational Unit
Process Description:	Loan origination is the process by which a borrower applies for a new loan, and a lender processes that application.
Process Flow Description:	Draft for Sales Process
Inherent Risk:	Likelihood 0 (0–10); Impact 0 (0–10); Rating Low (Low–Very High)
Residual Risk:	Likelihood 0 (0–10); Impact 0 (0–10); Rating Low (Low–Very High)

Risks	Inherent Risk	Residual Risk	Control Design Effectiveness	Control Operating Effectiveness
Risk01 Non compliance with regulations	Likelihood Very High Impact Very High Very High	Likelihood High Impact Very High Very High	1 5	4 1 1
Risk02 Unauthorized access	Likelihood Very High Impact Very High Low	Likelihood Medium Impact High Low	1	1
Risk03 Data validation errors	Likelihood Very High Impact High Low	Likelihood Medium Impact Medium Low	1	1
Risk04 Loss of customer data	Likelihood High Impact Very High Low	Likelihood High Impact Low Low	2	1 1
Risk05 Unauthorized decisions	Likelihood High Impact High Low	Likelihood Medium Impact Low Low		

Process Detail

Policies > RA Loans-Loan Origination

Process Details

- Fields
- Automation Jobs
- Change History
- Locks

Related Information

Parents

- **Business Entities (2)**
- **Risk Assessments (1)**
- Strategic Objectives (0)

Associations

- **Data Inputs (1)**
- **Data Outputs (1)**
- Issues (0)
- KPIs (0)
- **Process Diagrams (2)**
- **Questionnaires (1)**
- Risks (0)
- Signatures (0)
- **Sub-Processes (9)**

Attachments

- **Files (3)**
- Links (0)

RA Loans-Loan Origination

Description:
Loan origination is the process by which a borrower applies for a new loan, and a lender processes that application.

Process Owner: Process Owner - processowner

Domain: Operational

In Scope: ORM

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

Primary Parent Hierarchy: RA-CB-Loans

Fields

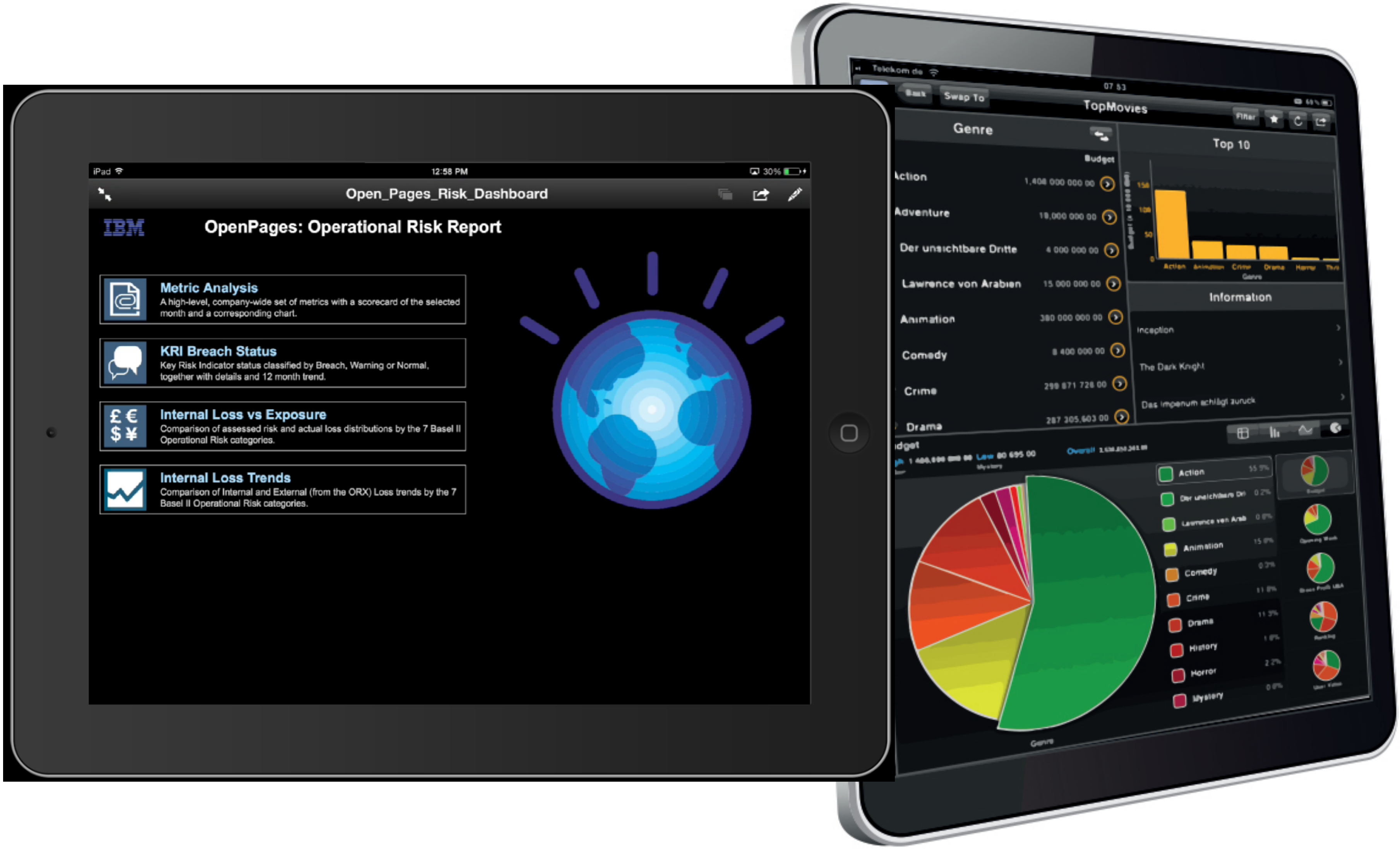
General

Name:	RA Loans-Loan Origination	Description:	Loan origination is the process by which a borrower applies for a new loan, and a lender processes that application.
Additional Description:	Origination generally includes all the steps from taking a loan application up to disbursal of funds (or declining the application). Loan servicing covers everything after disbursing the funds until the loan is fully paid off. Loan origination is a specialized version of new account opening for financial services organizations. Certain people and organizations specialize in loan origination. Mortgage brokers and other mortgage originator companies serve as a prominent example.		
Process Owner:	Process Owner - processowner	Domain:	Operational
Control Effectiveness by Process:		Documents by Process:	

View File	Detail View	Document Type
View File	Know Your Customer Process Flow.vsd	Process Narrative

NYSICA
New York State Internal Control Association

Full reporting capabilities supported on mobile devices



iPad 12:58 PM 30%

Open_Pages_Risk_Dashboard

OpenPages: Operational Risk Report

Metric Analysis
A high-level, company-wide set of metrics with a scorecard of the selected month and a corresponding chart.

KRI Breach Status
Key Risk Indicator status classified by Breach, Warning or Normal, together with details and 12 month trend.

Internal Loss vs Exposure
Comparison of assessed risk and actual loss distributions by the 7 Basel II Operational Risk categories.

Internal Loss Trends
Comparison of Internal and External (from the ORX) Loss trends by the 7 Basel II Operational Risk categories.

Summary of IBM's advantages in GRC

Comprehensive capabilities across virtually all aspects of governance, risk and compliance

Flexible data model, workflows, forms and reports to address the needs of organizations

Virtually unmatched reporting, analytics and visualization capabilities with embedded Cognos software

Powerful ecosystem of relevant risk, compliance and business process technologies to complement OpenPages software

Breadth of expertise and services capabilities covering technology and GRC

OpenPages software has a demonstrated history of successful GRC implementations and satisfied client references

Why does this matter to You?

1. Protect and preserve taxpayer funds

2. Improved audit management efficiency resulting reduced cost

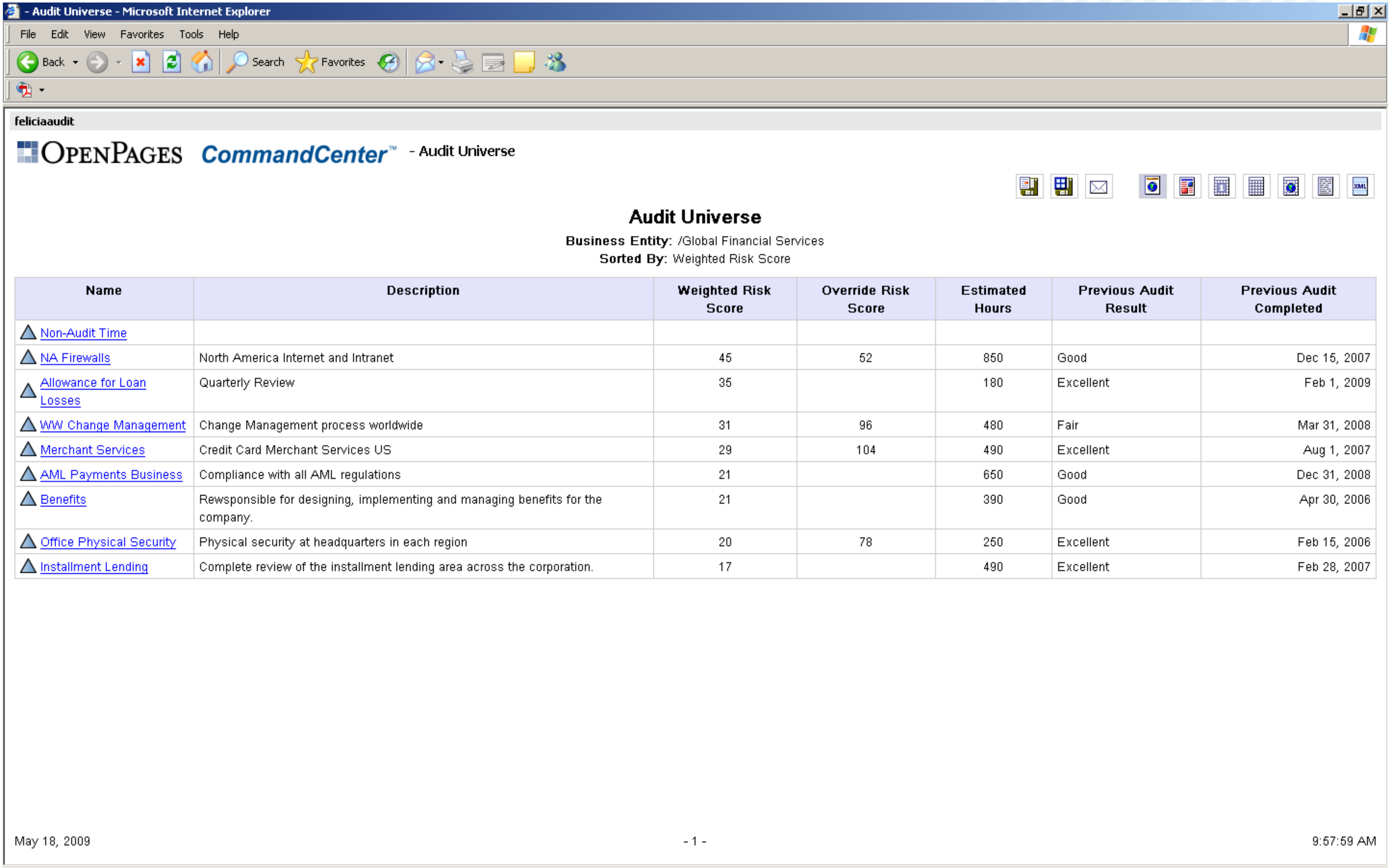
5. Protect reputation

4. Enhance transparency

5. Increase audit accuracy and overall success of audit results

Thank you.

Audit Universe Report (sorted by weighted risk score)



feliciaaudit

OpenPages CommandCenter™ - Audit Universe

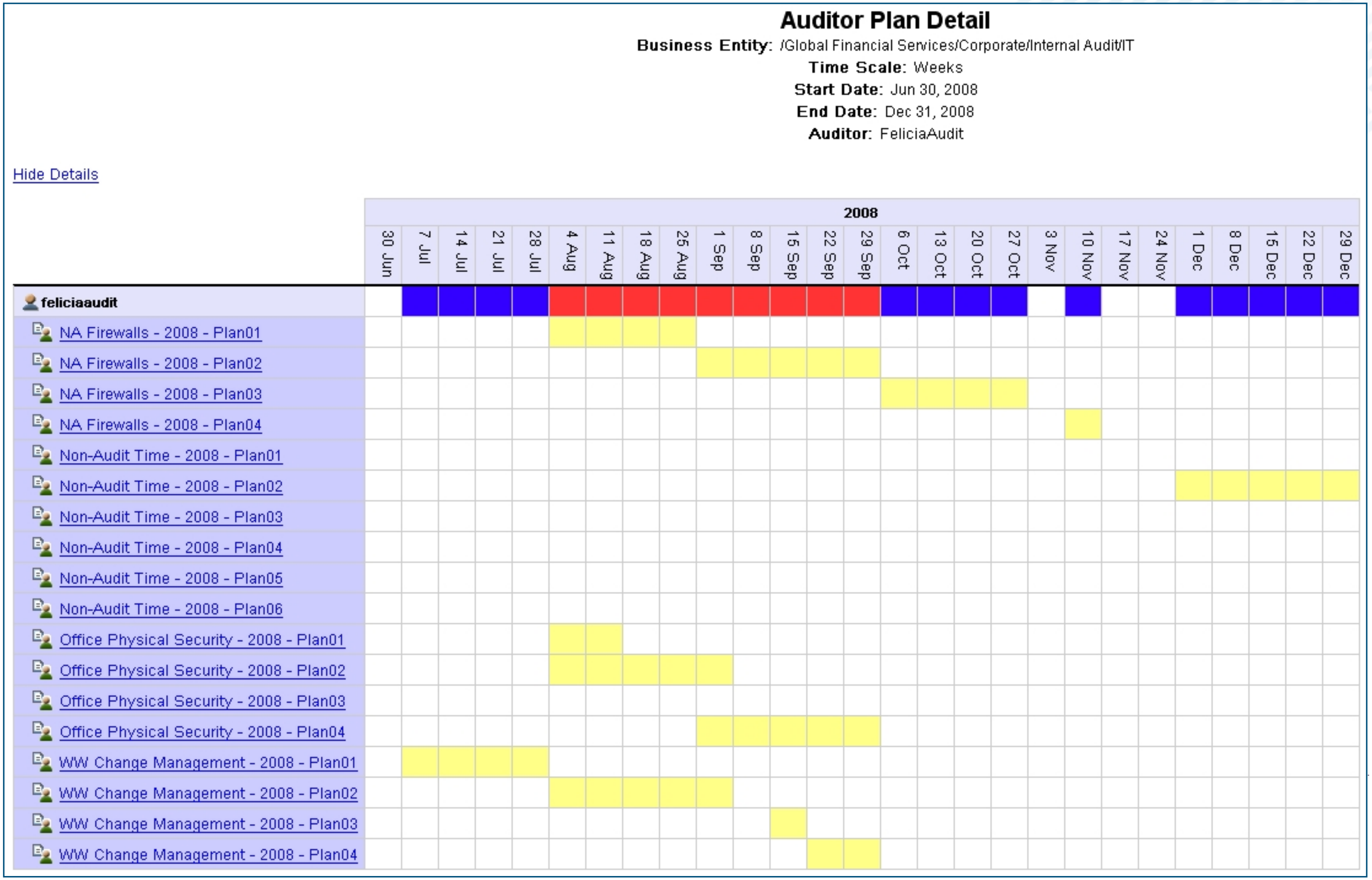
Audit Universe

Business Entity: /Global Financial Services
Sorted By: Weighted Risk Score

Name	Description	Weighted Risk Score	Override Risk Score	Estimated Hours	Previous Audit Result	Previous Audit Completed
△ Non-Audit Time						
△ NA Firewalls	North America Internet and Intranet	45	52	850	Good	Dec 15, 2007
△ Allowance for Loan Losses	Quarterly Review	35		180	Excellent	Feb 1, 2009
△ WW Change Management	Change Management process worldwide	31	96	480	Fair	Mar 31, 2008
△ Merchant Services	Credit Card Merchant Services US	29	104	490	Excellent	Aug 1, 2007
△ AML Payments Business	Compliance with all AML regulations	21		650	Good	Dec 31, 2008
△ Benefits	Rewsponsible for designing, implementing and managing benefits for the company.	21		390	Good	Apr 30, 2006
△ Office Physical Security	Physical security at headquarters in each region	20	78	250	Excellent	Feb 15, 2006
△ Installment Lending	Complete review of the installment lending area across the corporation.	17		490	Excellent	Feb 28, 2007

May 18, 2009 - 1 - 9:57:59 AM

Audit Plan Detail Report



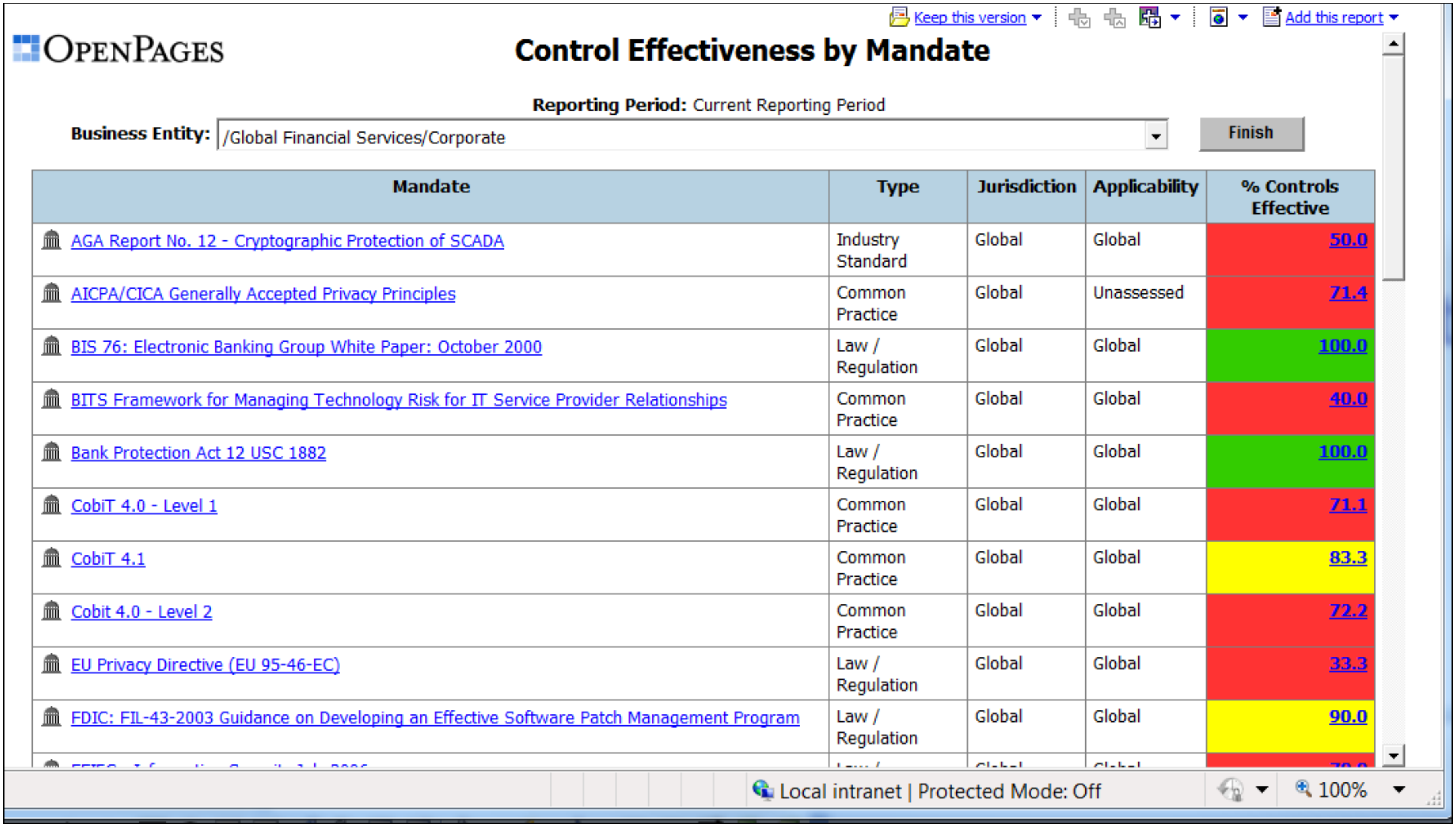
Auditor Plan Detail

Business Entity: /Global Financial Services/Corporate/Internal Audit/IT
Time Scale: Weeks
Start Date: Jun 30, 2008
End Date: Dec 31, 2008
Auditor: FeliciaAudit

Hide Details

	2008																										
	30 Jun	7 Jul	14 Jul	21 Jul	28 Jul	4 Aug	11 Aug	18 Aug	25 Aug	1 Sep	8 Sep	15 Sep	22 Sep	29 Sep	6 Oct	13 Oct	20 Oct	27 Oct	3 Nov	10 Nov	17 Nov	24 Nov	1 Dec	8 Dec	15 Dec	22 Dec	29 Dec
feliciaaudit		🟦	🟦	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟦	🟦	🟦	🟦		🟦			🟦	🟦	🟦	🟦	🟦
NA Firewalls - 2008 - Plan01						🟨	🟨	🟨	🟨																		
NA Firewalls - 2008 - Plan02										🟨	🟨	🟨	🟨	🟨													
NA Firewalls - 2008 - Plan03															🟨	🟨	🟨	🟨									
NA Firewalls - 2008 - Plan04																				🟨							
Non-Audit Time - 2008 - Plan01																											
Non-Audit Time - 2008 - Plan02																							🟨	🟨	🟨	🟨	🟨
Non-Audit Time - 2008 - Plan03																											
Non-Audit Time - 2008 - Plan04																											
Non-Audit Time - 2008 - Plan05																											
Non-Audit Time - 2008 - Plan06																											
Office Physical Security - 2008 - Plan01						🟨	🟨																				
Office Physical Security - 2008 - Plan02						🟨	🟨	🟨	🟨	🟨																	
Office Physical Security - 2008 - Plan03																											
Office Physical Security - 2008 - Plan04										🟨	🟨	🟨	🟨	🟨													
WW Change Management - 2008 - Plan01		🟨	🟨	🟨	🟨																						
WW Change Management - 2008 - Plan02						🟨	🟨	🟨	🟨	🟨																	
WW Change Management - 2008 - Plan03												🟨															
WW Change Management - 2008 - Plan04													🟨	🟨													

Control Effectiveness by Mandate - For a selected Business Entity, the report shows the % of effective controls with Processes by Mandate.



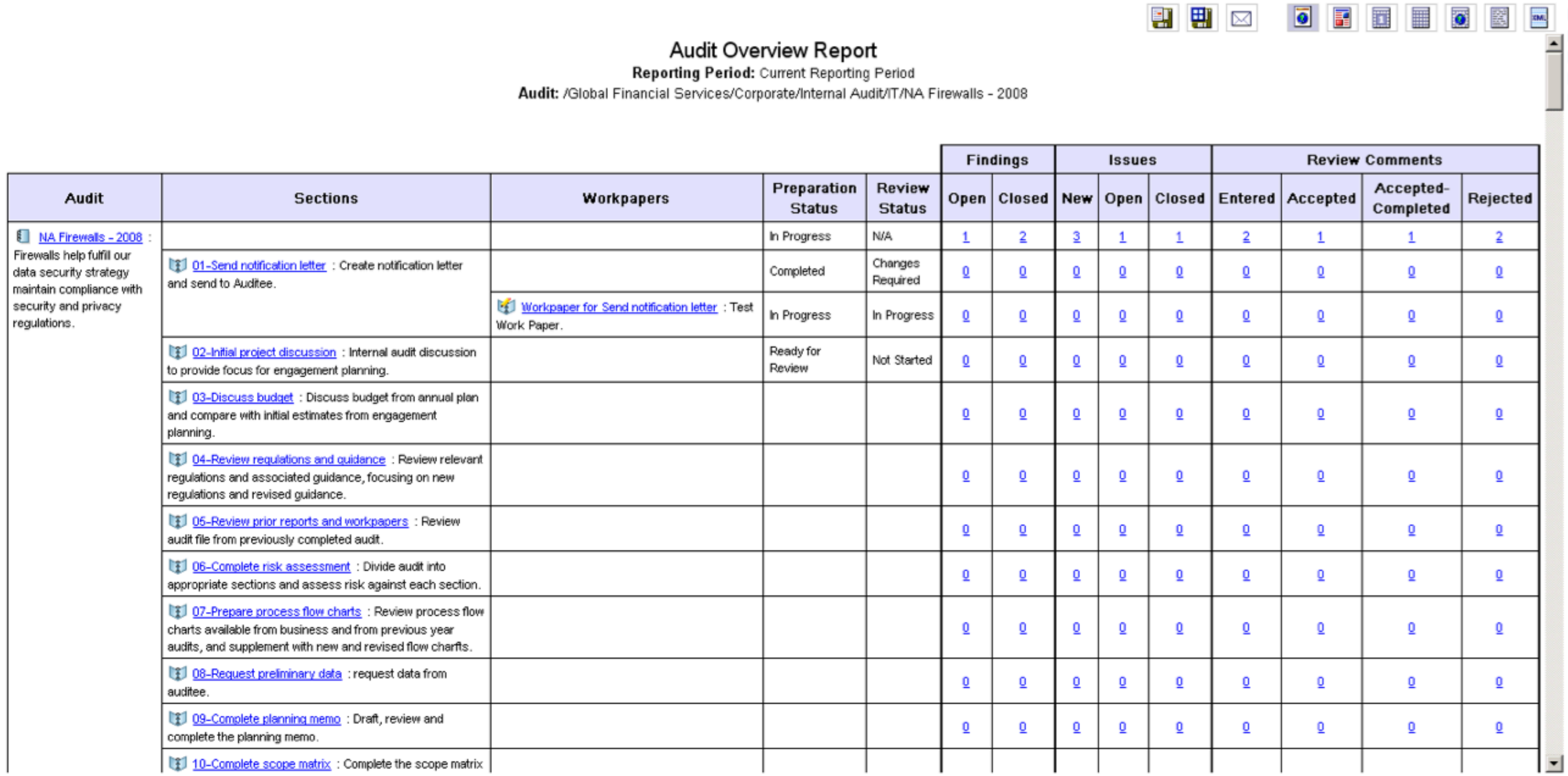
Control Effectiveness by Mandate

Reporting Period: Current Reporting Period

Business Entity: /Global Financial Services/Corporate

Mandate	Type	Jurisdiction	Applicability	% Controls Effective
AGA Report No. 12 - Cryptographic Protection of SCADA	Industry Standard	Global	Global	50.0
AICPA/CICA Generally Accepted Privacy Principles	Common Practice	Global	Unassessed	71.4
BIS 76: Electronic Banking Group White Paper: October 2000	Law / Regulation	Global	Global	100.0
BITS Framework for Managing Technology Risk for IT Service Provider Relationships	Common Practice	Global	Global	40.0
Bank Protection Act 12 USC 1882	Law / Regulation	Global	Global	100.0
CobiT 4.0 - Level 1	Common Practice	Global	Global	71.1
CobiT 4.1	Common Practice	Global	Global	83.3
Cobit 4.0 - Level 2	Common Practice	Global	Global	72.2
EU Privacy Directive (EU 95-46-EC)	Law / Regulation	Global	Global	33.3
FDIC: FIL-43-2003 Guidance on Developing an Effective Software Patch Management Program	Law / Regulation	Global	Global	90.0
FFIEC - Information Security July 2006	Law /	Global	Global	70.0

Audit Overview Report



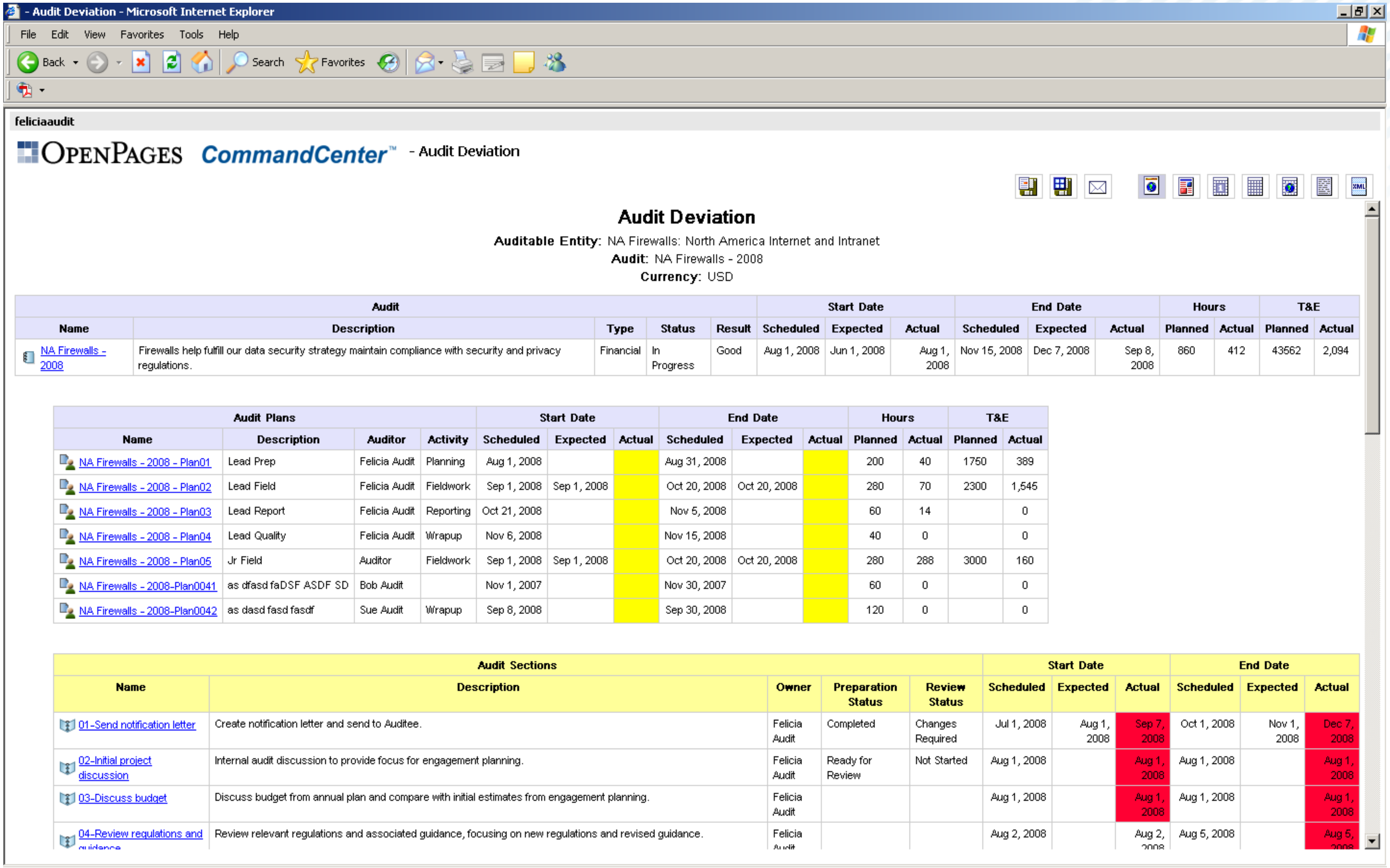
Audit Overview Report

Reporting Period: Current Reporting Period

Audit: /Global Financial Services/Corporate/Internal Audit/IT/NA Firewalls - 2008

					Findings		Issues			Review Comments			
Audit	Sections	Workpapers	Preparation Status	Review Status	Open	Closed	New	Open	Closed	Entered	Accepted	Accepted-Completed	Rejected
NA Firewalls - 2008 : Firewalls help fulfill our data security strategy maintain compliance with security and privacy regulations.			In Progress	N/A	1	2	3	1	1	2	1	1	2
	01-Send notification letter : Create notification letter and send to Auditee.		Completed	Changes Required	0	0	0	0	0	0	0	0	0
		Workpaper for Send notification letter : Test Work Paper.	In Progress	In Progress	0	0	0	0	0	0	0	0	0
	02-Initial project discussion : Internal audit discussion to provide focus for engagement planning.		Ready for Review	Not Started	0	0	0	0	0	0	0	0	0
	03-Discuss budget : Discuss budget from annual plan and compare with initial estimates from engagement planning.				0	0	0	0	0	0	0	0	0
	04-Review regulations and guidance : Review relevant regulations and associated guidance, focusing on new regulations and revised guidance.				0	0	0	0	0	0	0	0	0
	05-Review prior reports and workpapers : Review audit file from previously completed audit.				0	0	0	0	0	0	0	0	0
	06-Complete risk assessment : Divide audit into appropriate sections and assess risk against each section.				0	0	0	0	0	0	0	0	0
	07-Prepare process flow charts : Review process flow charts available from business and from previous year audits, and supplement with new and revised flow charfts.				0	0	0	0	0	0	0	0	0
	08-Request preliminary data : request data from auditee.				0	0	0	0	0	0	0	0	0
	09-Complete planning memo : Draft, review and complete the planning memo.				0	0	0	0	0	0	0	0	0
	10-Complete scope matrix : Complete the scope matrix												

Audit Deviation Report


- Audit Deviation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
feliciaaudit
OpenPages CommandCenter™ - Audit Deviation

Audit Deviation

Auditable Entity: NA Firewalls: North America Internet and Intranet
Audit: NA Firewalls - 2008
Currency: USD

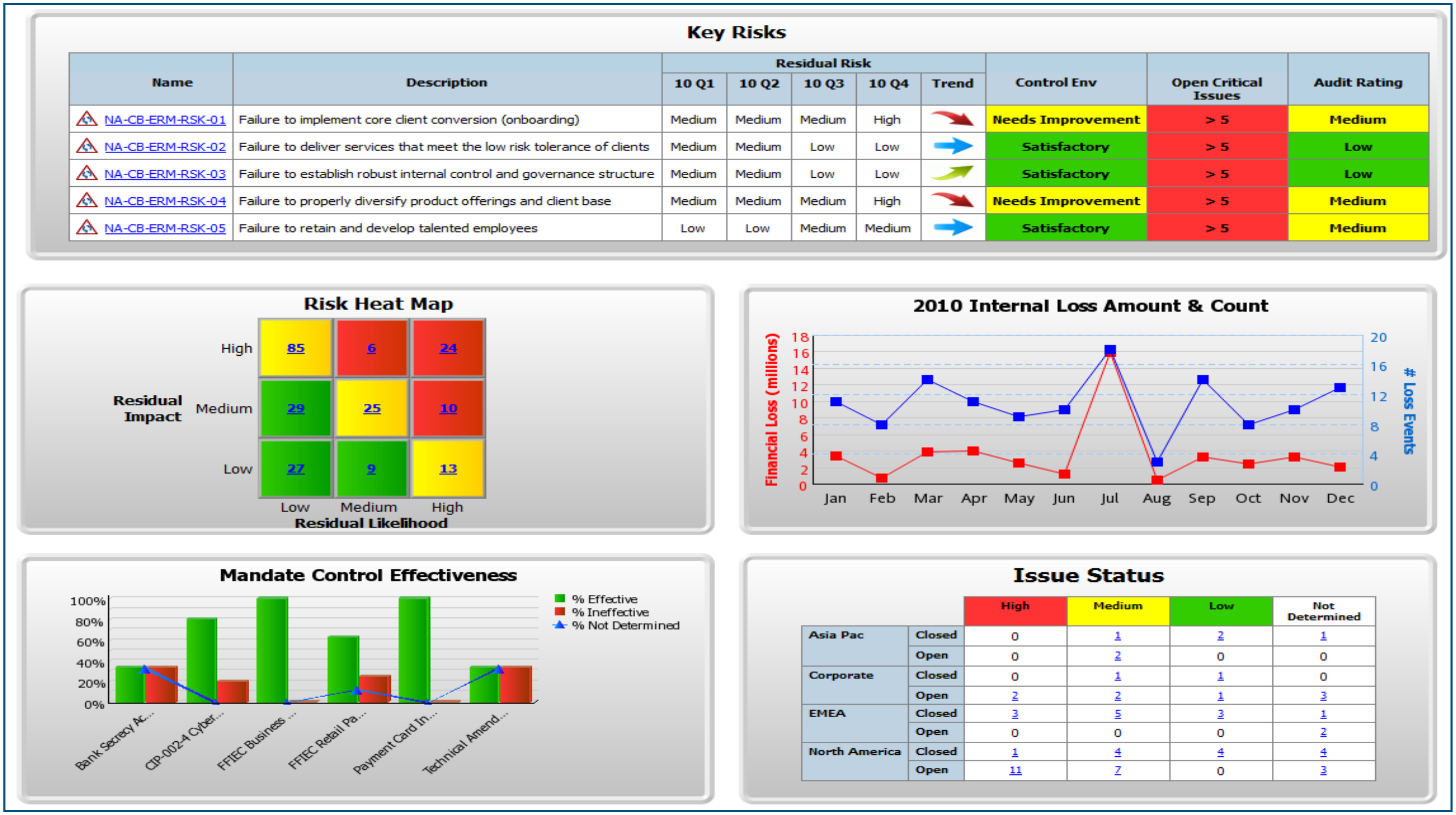
Audit					Start Date			End Date			Hours		T&E	
Name	**Description**	**Type**	**Status**	**Result**	**Scheduled**	**Expected**	**Actual**	**Scheduled**	**Expected**	**Actual**	**Planned**	**Actual**	**Planned**	**Actual**
NA Firewalls - 2008	Firewalls help fulfill our data security strategy maintain compliance with security and privacy regulations.	Financial	In Progress	Good	Aug 1, 2008	Jun 1, 2008	Aug 1, 2008	Nov 15, 2008	Dec 7, 2008	Sep 8, 2008	860	412	43562	2,094

Audit Plans				Start Date			End Date			Hours		T&E	
Name	**Description**	**Auditor**	**Activity**	**Scheduled**	**Expected**	**Actual**	**Scheduled**	**Expected**	**Actual**	**Planned**	**Actual**	**Planned**	**Actual**
NA Firewalls - 2008 - Plan01	Lead Prep	Felicia Audit	Planning	Aug 1, 2008			Aug 31, 2008			200	40	1750	389
NA Firewalls - 2008 - Plan02	Lead Field	Felicia Audit	Fieldwork	Sep 1, 2008	Sep 1, 2008		Oct 20, 2008	Oct 20, 2008		280	70	2300	1,545
NA Firewalls - 2008 - Plan03	Lead Report	Felicia Audit	Reporting	Oct 21, 2008			Nov 5, 2008			60	14		0
NA Firewalls - 2008 - Plan04	Lead Quality	Felicia Audit	Wrapup	Nov 6, 2008			Nov 15, 2008			40	0		0
NA Firewalls - 2008 - Plan05	Jr Field	Auditor	Fieldwork	Sep 1, 2008	Sep 1, 2008		Oct 20, 2008	Oct 20, 2008		280	288	3000	160
NA Firewalls - 2008-Plan0041	as dfasd faDSF ASDF SD	Bob Audit		Nov 1, 2007			Nov 30, 2007			60	0		0
NA Firewalls - 2008-Plan0042	as dasd fasd fasdf	Sue Audit	Wrapup	Sep 8, 2008			Sep 30, 2008			120	0		0

Audit Sections					Start Date			End Date		
Name	**Description**	**Owner**	**Preparation Status**	**Review Status**	**Scheduled**	**Expected**	**Actual**	**Scheduled**	**Expected**	**Actual**
01-Send notification letter	Create notification letter and send to Auditee.	Felicia Audit	Completed	Changes Required	Jul 1, 2008	Aug 1, 2008	Sep 7, 2008	Oct 1, 2008	Nov 1, 2008	Dec 7, 2008
02-Initial project discussion	Internal audit discussion to provide focus for engagement planning.	Felicia Audit	Ready for Review	Not Started	Aug 1, 2008		Aug 1, 2008	Aug 1, 2008		Aug 1, 2008
03-Discuss budget	Discuss budget from annual plan and compare with initial estimates from engagement planning.	Felicia Audit			Aug 1, 2008		Aug 1, 2008	Aug 1, 2008		Aug 1, 2008
04-Review regulations and guidance	Review relevant regulations and associated guidance, focusing on new regulations and revised guidance.	Felicia Audit			Aug 2, 2008		Aug 2, 2008	Aug 5, 2008		Aug 5, 2008

IBM®

ERM dashboard by group, with drill down capability to view additional information



Key Risks

Name	Description	Residual Risk					Control Env	Open Critical Issues	Audit Rating
		10 Q1	10 Q2	10 Q3	10 Q4	Trend			
NA-CB-ERM-RSK-01	Failure to implement core client conversion (onboarding)	Medium	Medium	Medium	High	↘	Needs Improvement	> 5	Medium
NA-CB-ERM-RSK-02	Failure to deliver services that meet the low risk tolerance of clients	Medium	Medium	Low	Low	→	Satisfactory	> 5	Low
NA-CB-ERM-RSK-03	Failure to establish robust internal control and governance structure	Medium	Medium	Low	Low	↗	Satisfactory	> 5	Low
NA-CB-ERM-RSK-04	Failure to properly diversify product offerings and client base	Medium	Medium	Medium	High	↘	Needs Improvement	> 5	Medium
NA-CB-ERM-RSK-05	Failure to retain and develop talented employees	Low	Low	Medium	Medium	→	Satisfactory	> 5	Medium

Risk Heat Map

Residual Impact				
	High	85	6	24
	Medium	29	25	10
	Low	27	9	13
		Low	Medium	High

Residual Likelihood

2010 Internal Loss Amount & Count

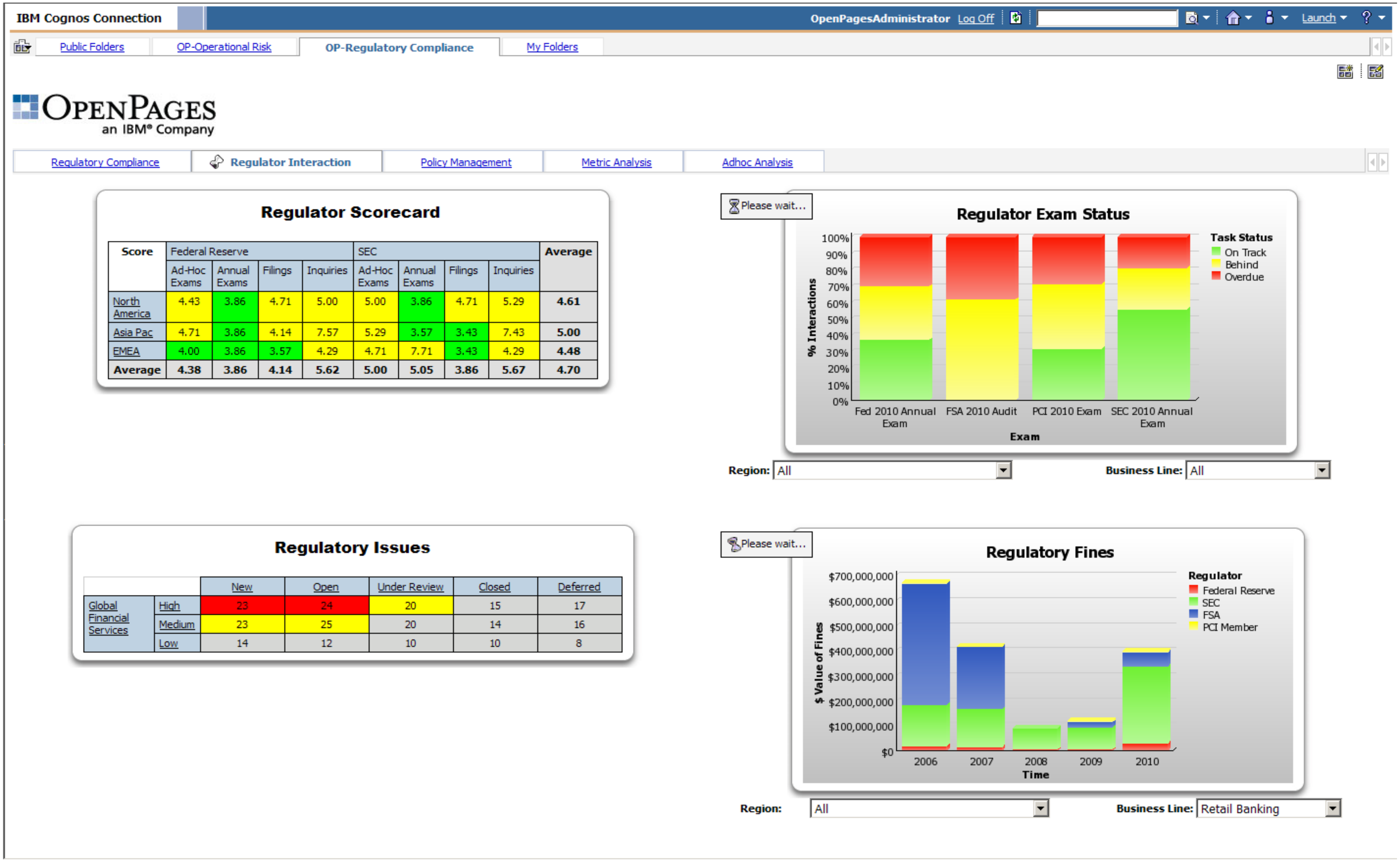
Mandate Control Effectiveness

Issue Status

		High	Medium	Low	Not Determined
Asia Pac	Closed	0	1	2	1
	Open	0	2	0	0
Corporate	Closed	0	1	1	0
	Open	2	2	1	3
EMEA	Closed	3	5	3	1
	Open	0	0	0	2
North America	Closed	1	4	4	4
	Open	11	7	0	3

NYSICA
New York State Internal Control Association

Regulator Interaction



Regulator Scorecard

Score	Federal Reserve				SEC				Average
	Ad-Hoc Exams	Annual Exams	Filings	Inquiries	Ad-Hoc Exams	Annual Exams	Filings	Inquiries	
North America	4.43	3.86	4.71	5.00	5.00	3.86	4.71	5.29	**4.61**
Asia Pac	4.71	3.86	4.14	7.57	5.29	3.57	3.43	7.43	**5.00**
EMEA	4.00	3.86	3.57	4.29	4.71	7.71	3.43	4.29	**4.48**
Average	**4.38**	**3.86**	**4.14**	**5.62**	**5.00**	**5.05**	**3.86**	**5.67**	**4.70**

Region: All ▾ **Business Line:** All ▾

Regulatory Issues

		New	Open	Under Review	Closed	Deferred
Global Financial Services	High	23	24	20	15	17
	Medium	23	25	20	14	16
	Low	14	12	10	10	8

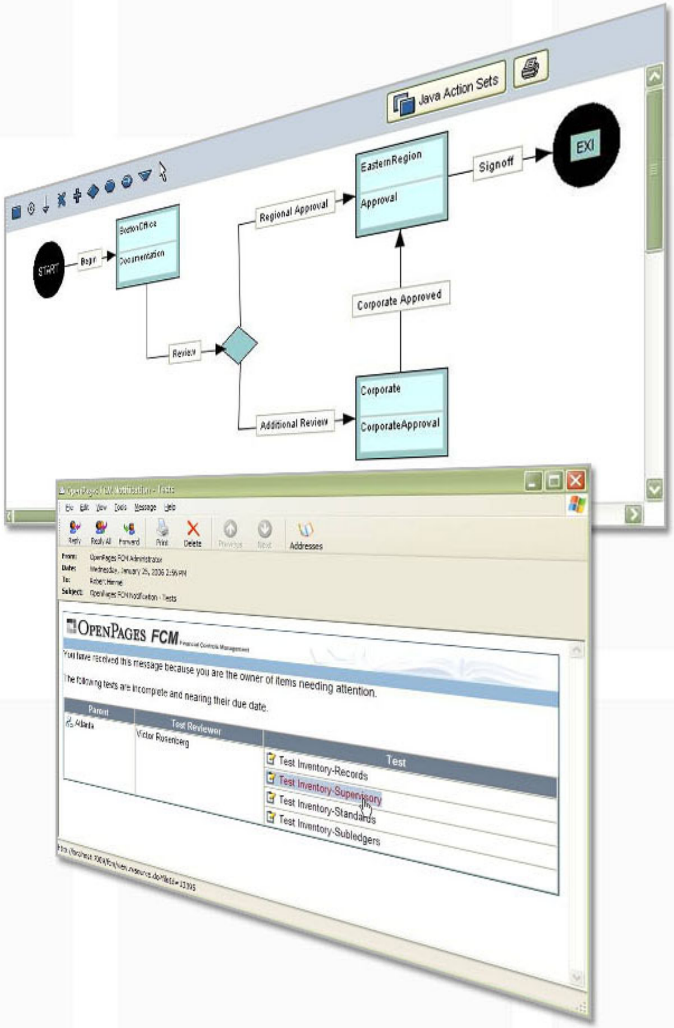
Region: All ▾ **Business Line:** Retail Banking ▾

Report mining delivers insight

Automate task assignment, notifications and reminders, data routing and tracking, and more

Robust workflow establishes and automates consistent best practice processes for:

- Assessing risk
  - Incident evaluation and enrichment
  - KRI management—threshold breach awareness
- Materiality and quantitative assessments
  - Process design reviews
  - Control testing
  - Issue remediation
  - Sign-offs and certifications
  - Practically unlimited flexibility to automate processes
- Use-case examples
  - Alerting testers and reviewers when the testing needs to be performed and reviewed
  - Alerting risk managers of KRI threshold breaches
  - Alerting business owners of regulatory requirement reviews and certifications
  - Alerting process and entity—regional and corporate owners and controllers to sign off on the internal control documentation
  - Alert issue owners (gaps identified by control reviewers) in mitigating the issues by exception



From: OpenPages FCM Administrator
Date: Wednesday, January 25, 2006 2:56 PM
To: Robert Herne
Subject: OpenPages FCM Notification - Tests

OpenPages FCM Financial Controls Management

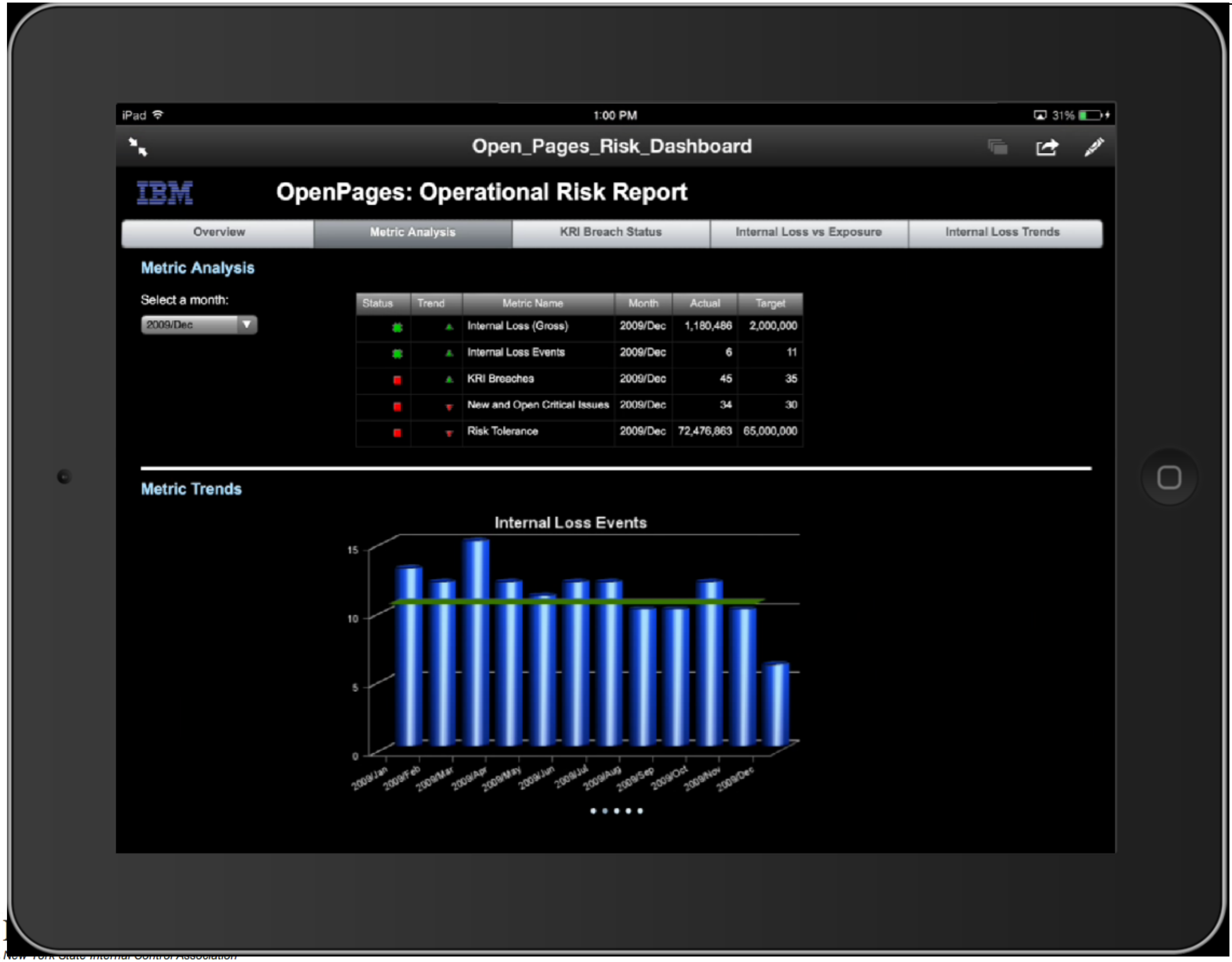
You have received this message because you are the owner of items needing attention.

The following tests are incomplete and nearing their due date.

Parent	Test Reviewer	Test
Atlanta	Victor Rosenberg	Test Inventory-Records
		Test Inventory-Supervisory
		Test Inventory-Standards
		Test Inventory-Subledgers

http://localhost:7009/fcm/view.resource.do?fileId=13395

Risk Analytics



iPad 1:00 PM 31%

Open_Pages_Risk_Dashboard

IBM **OpenPages: Operational Risk Report**

Overview | Metric Analysis | KRI Breach Status | Internal Loss vs Exposure | Internal Loss Trends

Metric Analysis

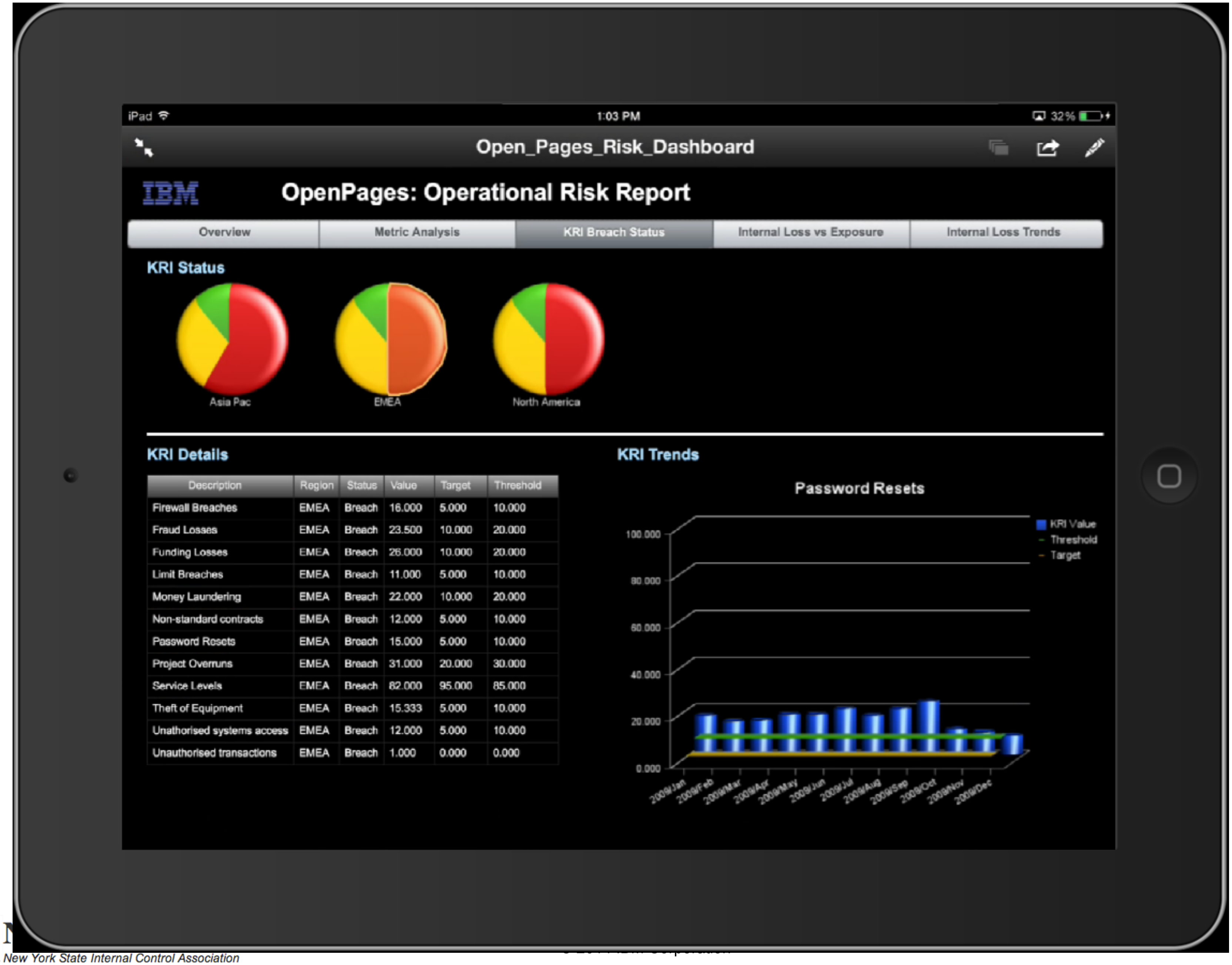
Select a month: 2009/Dec

Status	Trend	Metric Name	Month	Actual	Target
🟩	▲	Internal Loss (Gross)	2009/Dec	1,180,486	2,000,000
🟩	▲	Internal Loss Events	2009/Dec	6	11
🟥	▲	KRI Breaches	2009/Dec	45	35
🟥	▼	New and Open Critical Issues	2009/Dec	34	30
🟥	▼	Risk Tolerance	2009/Dec	72,476,863	65,000,000

Metric Trends

Internal Loss Events

Risk Analytics



Open_Pages_Risk_Dashboard

OpenPages: Operational Risk Report

KRI Status

KRI Details

Description	Region	Status	Value	Target	Threshold
Firewall Breaches	EMEA	Breach	16.000	5.000	10.000
Fraud Losses	EMEA	Breach	23.500	10.000	20.000
Funding Losses	EMEA	Breach	26.000	10.000	20.000
Limit Breaches	EMEA	Breach	11.000	5.000	10.000
Money Laundering	EMEA	Breach	22.000	10.000	20.000
Non-standard contracts	EMEA	Breach	12.000	5.000	10.000
Password Resets	EMEA	Breach	15.000	5.000	10.000
Project Overruns	EMEA	Breach	31.000	20.000	30.000
Service Levels	EMEA	Breach	82.000	95.000	85.000
Theft of Equipment	EMEA	Breach	15.333	5.000	10.000
Unathorised systems access	EMEA	Breach	12.000	5.000	10.000
Unauthorised transactions	EMEA	Breach	1.000	0.000	0.000

KRI Trends

Password Resets