Continuous Control Monitoring: HP and Google's Perspective

Segment S13

September 17, 2007

Jessica Amezquita, Hewlett-Packard Company
Erik Jonte, Google, Inc
Brad Ames, Hewlett-Packard Company

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Agenda

- Continuous Control Monitoring Premise and Framework
- HP Walkthrough
- Google Walkthrough
- Summary of our Learnings

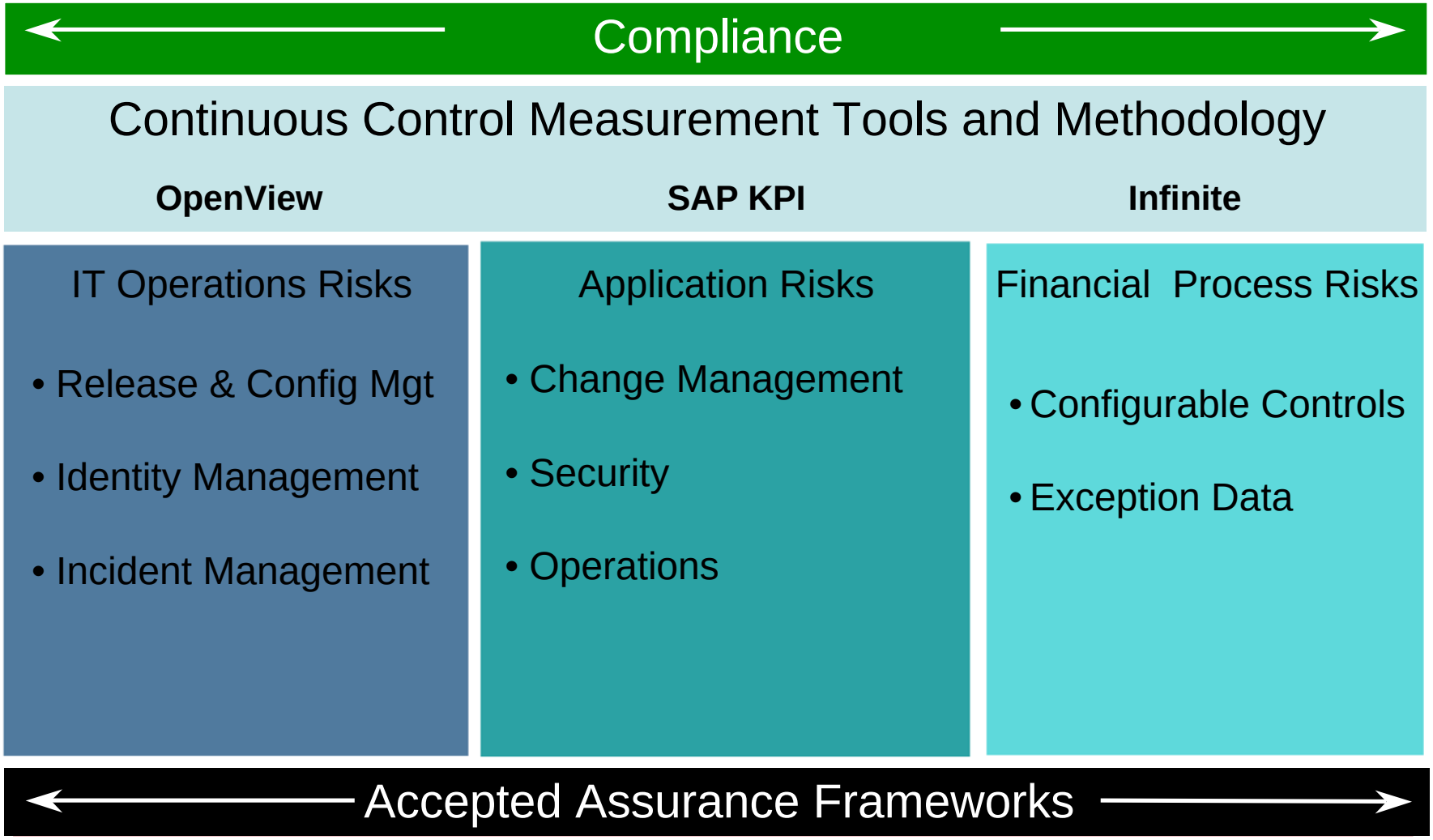
Build toward a Strategy

- Continuous Control Measurement (CCM) is a monitoring and benchmarking approach adopted by HP internal audit to see emerging risk across the enterprise
- The CCM tools and methodology enable the examiner and governance to shift from a historical view to an ongoing strategic perspective
- Since risk and response to risk can be analyzed remotely, HP is reducing time and intrusion in the field by implementing the CCM tools and methodology

Premise for Continuous Control Monitoring

- **Uncertainty** - Less comfort regarding how risk is managed results in more testing.
- **Tolerance** - Tolerance and control activities go together. Low tolerance for risk mean more control processes which reduces testing.
- **Response** - CCM provides a way for auditors to gain visibility to risk tolerance, response to risk and generates confidence.
- **Interdependence** - It all goes together. Not all of the controls in the environment need to be tested to conclude on risk. When one control is strengthened it will effect another.

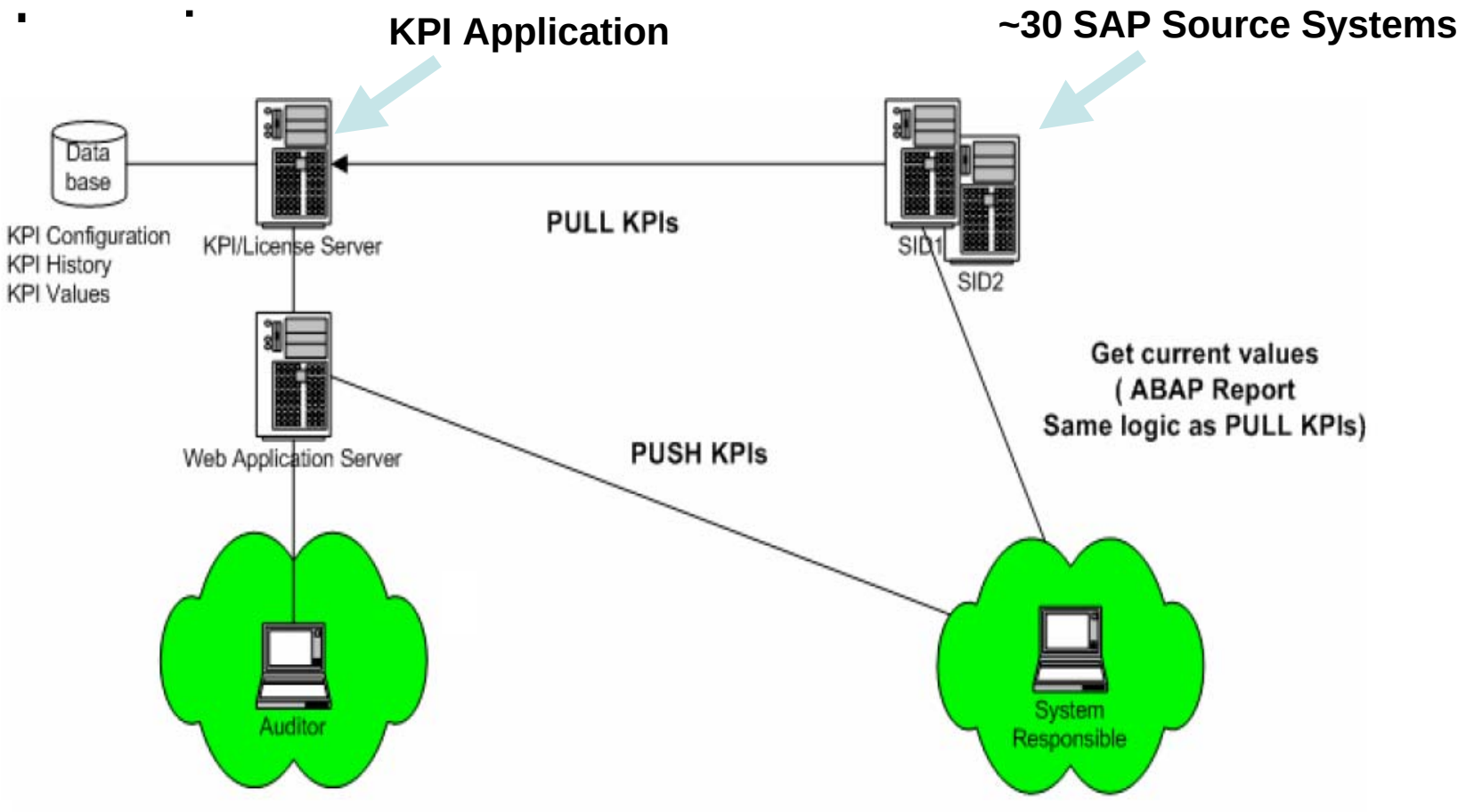
Alignment is the Key to Provide a Portfolio View of Risk



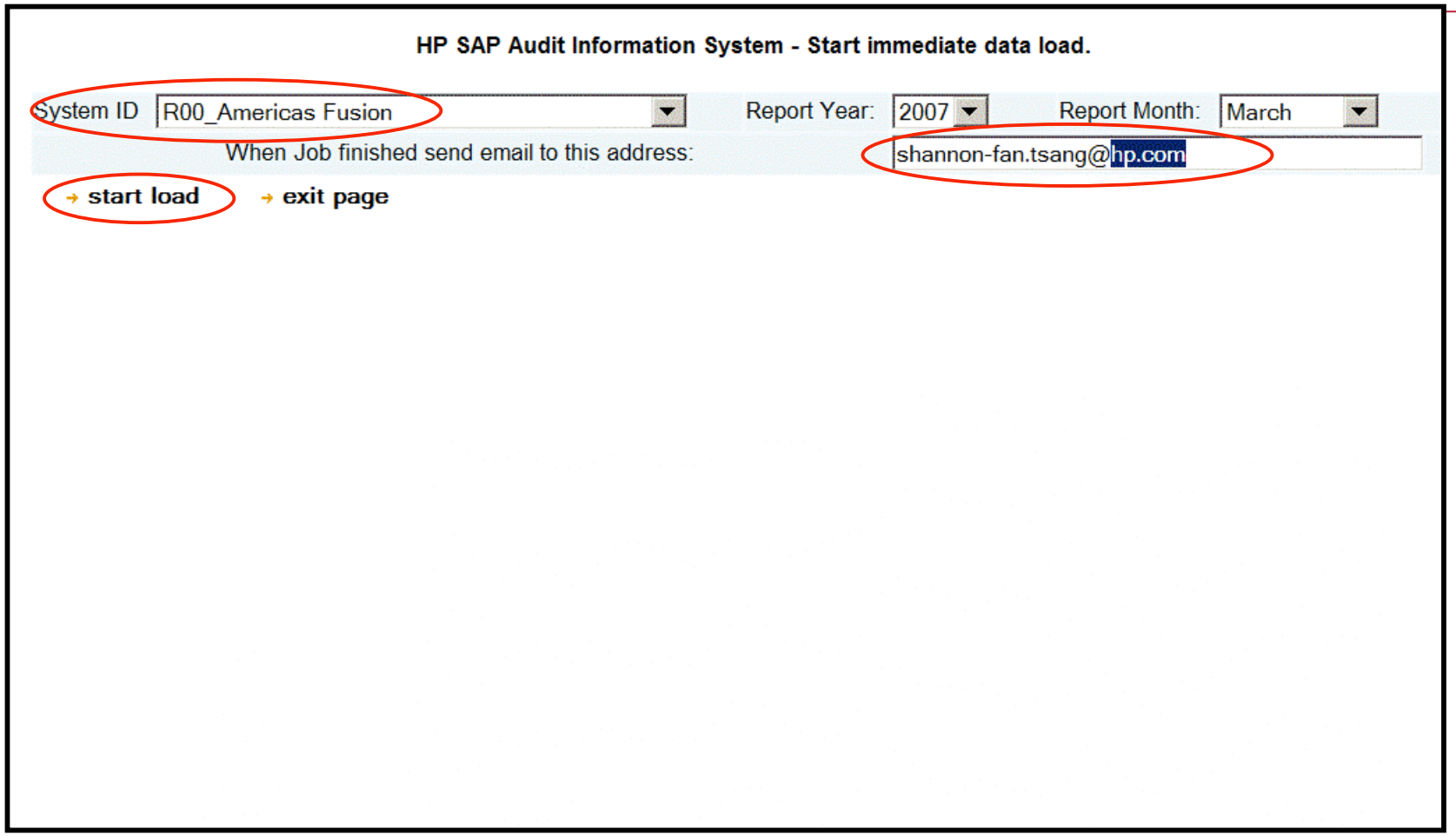
HP Walkthrough

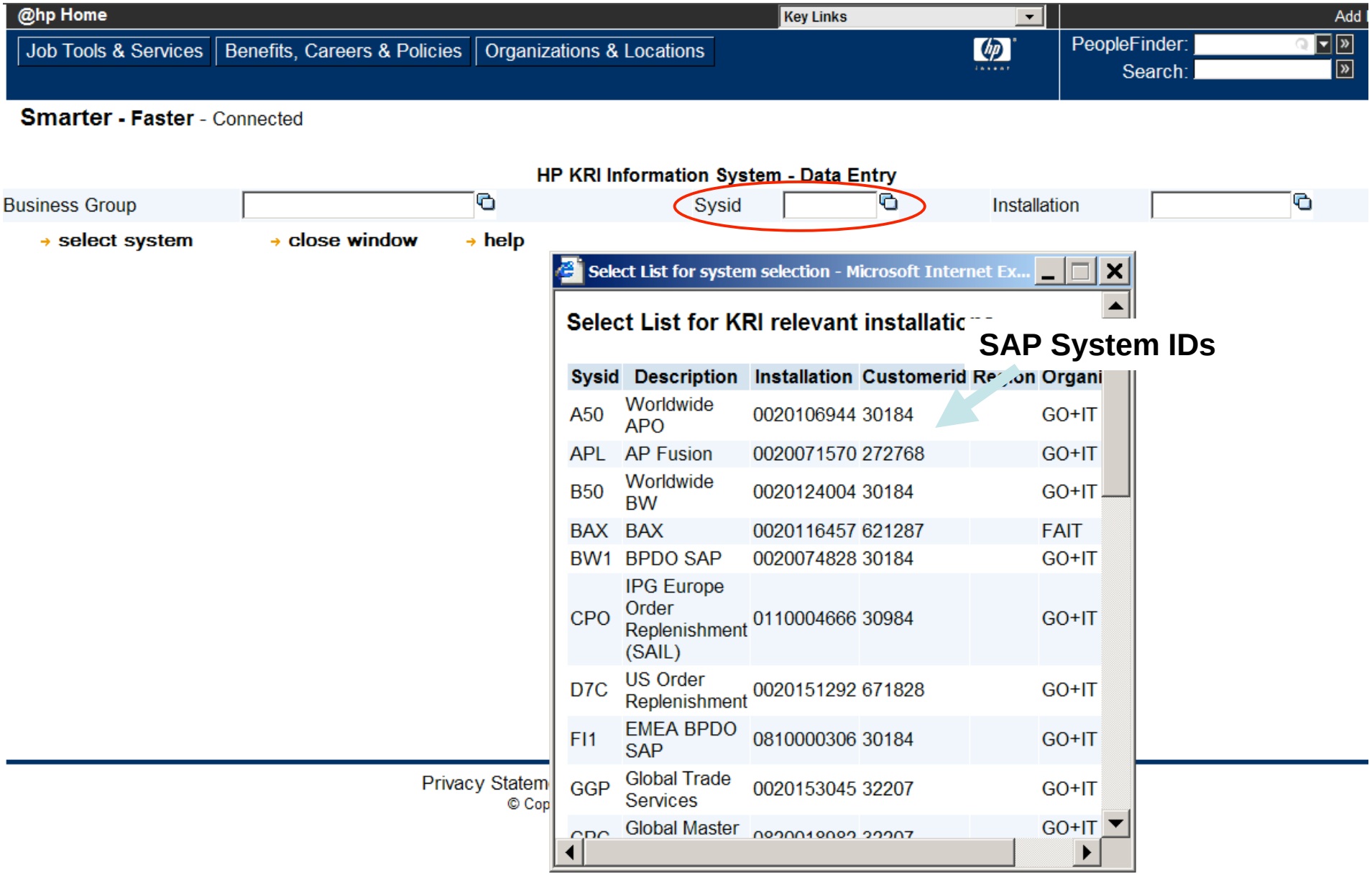
- Jessica.Amezquita
- Jessica.amezquita@hp.com
- Internal Audit Manager

SAP KPI Tool Design



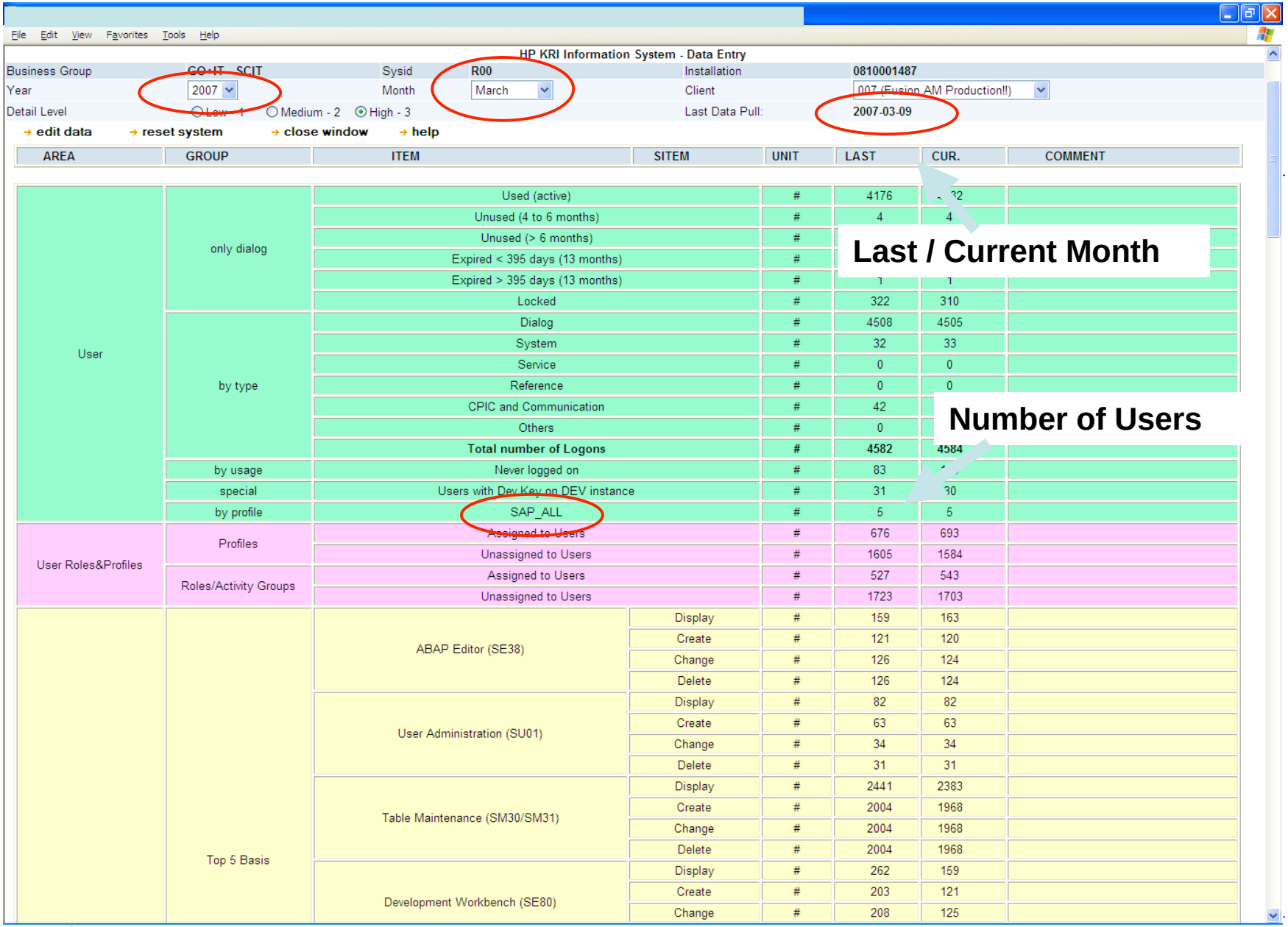
Manual Data Trigger Request




@hp Home
Key Links
Job Tools & Services
Benefits, Careers & Policies
Organizations & Locations
PeopleFinder:
Search:
Smarter - Faster - Connected
HP KRI Information System - Data Entry
Business Group
Sysid
Installation
select system
close window
help
Select List for system selection - Microsoft Internet Ex...
Select List for KRI relevant installatic
SAP System IDs
Sysid
Description
Installation
Customerid
Organi
A50 Worldwide APO 0020106944 30184 GO+IT
APL AP Fusion 0020071570 272768 GO+IT
B50 Worldwide BW 0020124004 30184 GO+IT
BAX BAX 0020116457 621287 FAIT
BW1 BPDO SAP 0020074828 30184 GO+IT
CPO IPG Europe Order Replenishment (SAIL) 0110004666 30984 GO+IT
D7C US Order Replenishment 0020151292 671828 GO+IT
FI1 EMEA BPDO SAP 0810000306 30184 GO+IT
GGP Global Trade Services 0020153045 32207 GO+IT
Global Master
Privacy Statem
© Cop

What is HP Currently Monitoring?

- Change Management
  - Number of transports
  - Users with the ability to develop and migrate changes to production
- Security
  - Number of users (active, locked, expired)
  - Password parameters
  - Privileged access (SAP_ALL, users with ability to maintain customer credit terms)
  - Terminated employee check
- Operations
  - Number of users with the ability to create/modify/delete jobs



File Edit View Favorites Tools Help

HP KRI Information System - Data Entry

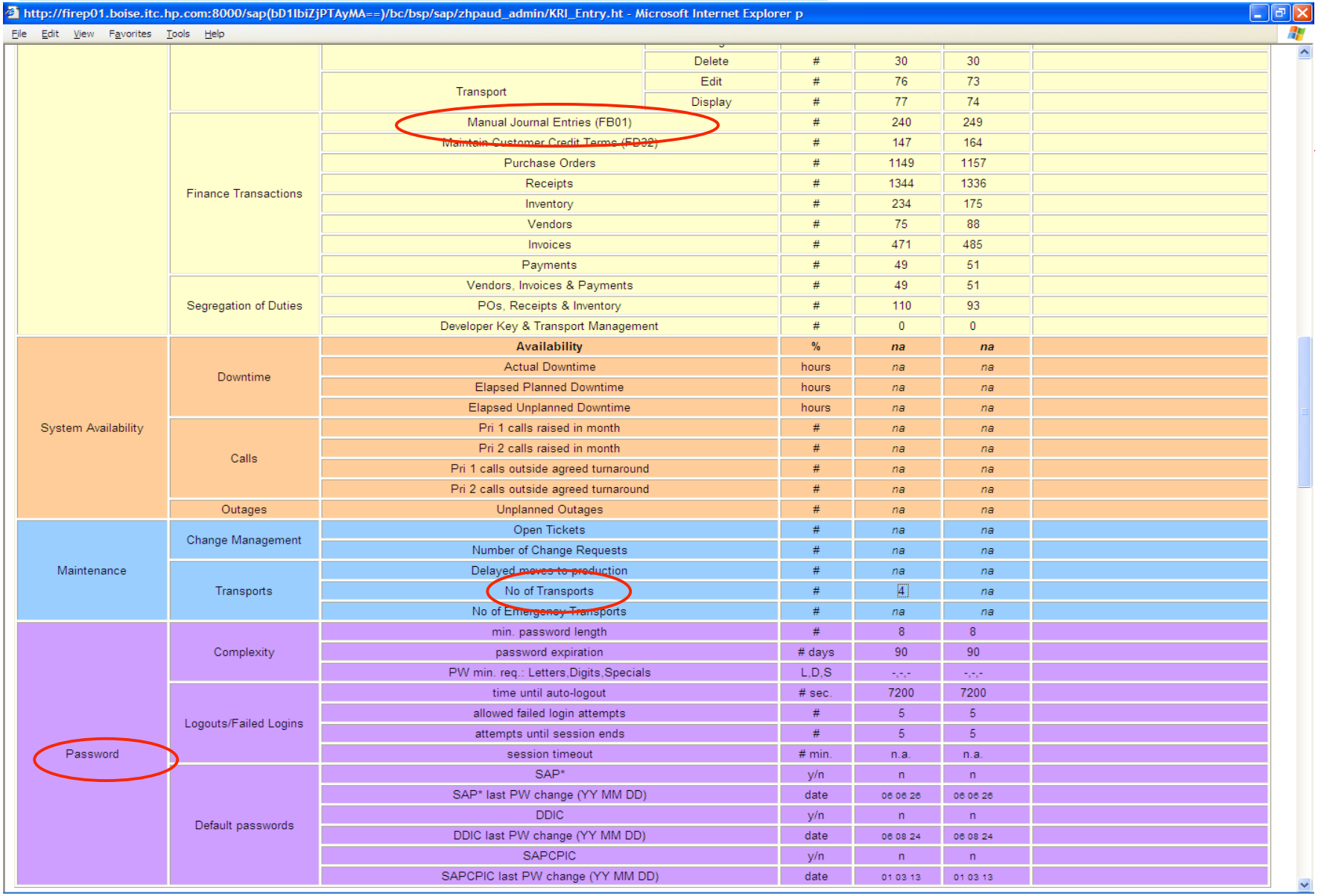
Business Group	GO-IT_SCIT	Sysid	R00	Installation	0810001487
Year	2007	Month	March	Client	007 (Fusion AM Production!!)
Detail Level	Low - 1	Medium - 2	High - 3	Last Data Pull:	2007-03-09

→ edit data → reset system → close window → help

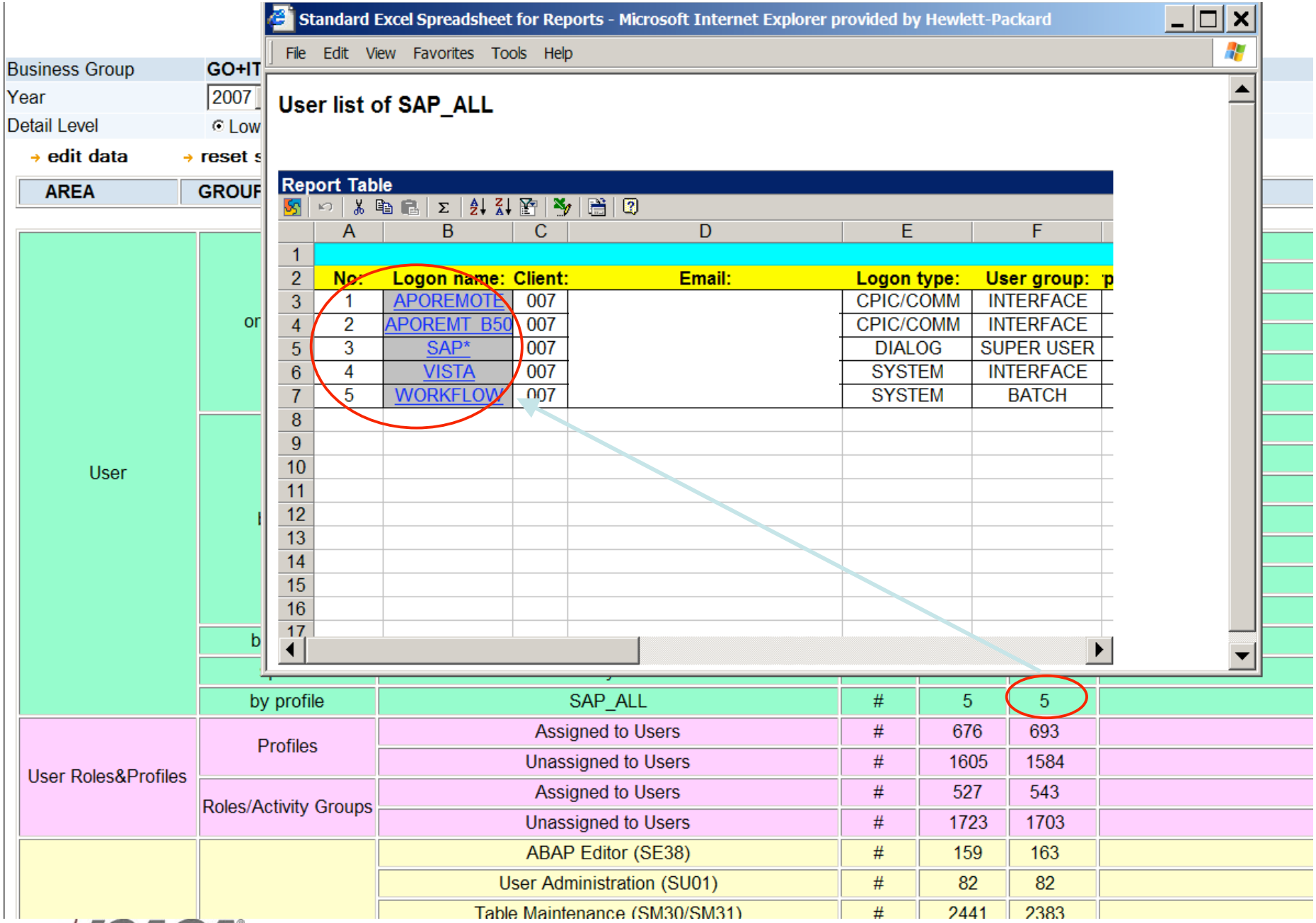
AREA	GROUP	ITEM	SITEM	UNIT	LAST	CUR.	COMMENT
User	only dialog	Used (active)		#	4176	[illegible]32	
		Unused (4 to 6 months)		#	4	4	
		Unused (> 6 months)		#			
		Expired < 395 days (13 months)		#			
		Expired > 395 days (13 months)		#	1	1	
		Locked		#	322	310	
	by type	Dialog		#	4508	4505	
		System		#	32	33	
		Service		#	0	0	
		Reference		#	0	0	
		CPIC and Communication		#	42		
		Others		#	0		
		Total number of Logons		#	4582	4584	
	by usage	Never logged on		#	83	[illegible]	
	special	Users with Dev Key on DEV instance		#	31	30	
	by profile	SAP_ALL		#	5	5	
User Roles&Profiles	Profiles	Assigned to Users		#	676	693	
		Unassigned to Users		#	1605	1584	
	Roles/Activity Groups	Assigned to Users		#	527	543	
		Unassigned to Users		#	1723	1703	
	Top 5 Basis	ABAP Editor (SE38)	Display	#	159	163	
			Create	#	121	120	
			Change	#	126	124	
			Delete	#	126	124	
		User Administration (SU01)	Display	#	82	82	
			Create	#	63	63	
			Change	#	34	34	
			Delete	#	31	31	
		Table Maintenance (SM30/SM31)	Display	#	2441	2383	
			Create	#	2004	1968	
			Change	#	2004	1968	
			Delete	#	2004	1968	
		Development Workbench (SE80)	Display	#	262	159	
			Create	#	203	121	
			Change	#	208	125	

Last / Current Month

Number of Users



		Transport	Delete	#	30	30	
			Edit	#	76	73	
			Display	#	77	74	
	Finance Transactions	Manual Journal Entries (FB01)		#	240	249	
		Maintain Customer Credit Terms (FD32)		#	147	164	
		Purchase Orders		#	1149	1157	
		Receipts		#	1344	1336	
		Inventory		#	234	175	
		Vendors		#	75	88	
		Invoices		#	471	485	
		Payments		#	49	51	
	Segregation of Duties	Vendors, Invoices & Payments		#	49	51	
		POs, Receipts & Inventory		#	110	93	
		Developer Key & Transport Management		#	0	0	
System Availability	Downtime	**Availability**		%	*na*	*na*	
		Actual Downtime		hours	*na*	*na*	
		Elapsed Planned Downtime		hours	*na*	*na*	
		Elapsed Unplanned Downtime		hours	*na*	*na*	
	Calls	Pri 1 calls raised in month		#	*na*	*na*	
		Pri 2 calls raised in month		#	*na*	*na*	
		Pri 1 calls outside agreed turnaround		#	*na*	*na*	
		Pri 2 calls outside agreed turnaround		#	*na*	*na*	
	Outages	Unplanned Outages		#	*na*	*na*	
Maintenance	Change Management	Open Tickets		#	*na*	*na*	
		Number of Change Requests		#	*na*	*na*	
	Transports	Delayed moves to production		#	*na*	*na*	
		No of Transports		#	4	*na*	
		No of Emergency Transports		#	*na*	*na*	
Password	Complexity	min. password length		#	8	8	
		password expiration		# days	90	90	
		PW min. req.: Letters,Digits,Specials		L,D,S	-,-,-	-,-,-	
	Logouts/Failed Logins	time until auto-logout		# sec.	7200	7200	
		allowed failed login attempts		#	5	5	
		attempts until session ends		#	5	5	
		session timeout		# min.	n.a.	n.a.	
	Default passwords	SAP*		y/n	n	n	
		SAP* last PW change (YY MM DD)		date	06 06 26	06 06 26	
		DDIC		y/n	n	n	
		DDIC last PW change (YY MM DD)		date	06 08 24	06 08 24	
		SAPCPIC		y/n	n	n	
		SAPCPIC last PW change (YY MM DD)		date	01 03 13	01 03 13	


Standard Excel Spreadsheet for Reports - Microsoft Internet Explorer provided by Hewlett-Packard
File Edit View Favorites Tools Help
User list of SAP_ALL
Report Table
No: Logon name: Client: Email: Logon type: User group:
1 APOREMOTE 007 CPIC/COMM INTERFACE
2 APOREMT_B50 007 CPIC/COMM INTERFACE
3 SAP* 007 DIALOG SUPER USER
4 VISTA 007 SYSTEM INTERFACE
5 WORKFLOW 007 SYSTEM BATCH
Business Group GO+IT
Year 2007
Detail Level Low
edit data
reset
AREA
GROUP
User
by profile
SAP_ALL # 5 5
User Roles&Profiles
Profiles
Assigned to Users # 676 693
Unassigned to Users # 1605 1584
Roles/Activity Groups
Assigned to Users # 527 543
Unassigned to Users # 1723 1703
ABAP Editor (SE38) # 159 163
User Administration (SU01) # 82 82
Table Maintenance (SM30/SM31) # 2441 2383

Compare Multiple KPIs Across One SAP System

HP Audit Information System - KRI History Reports for one system.

→ show report → exit page

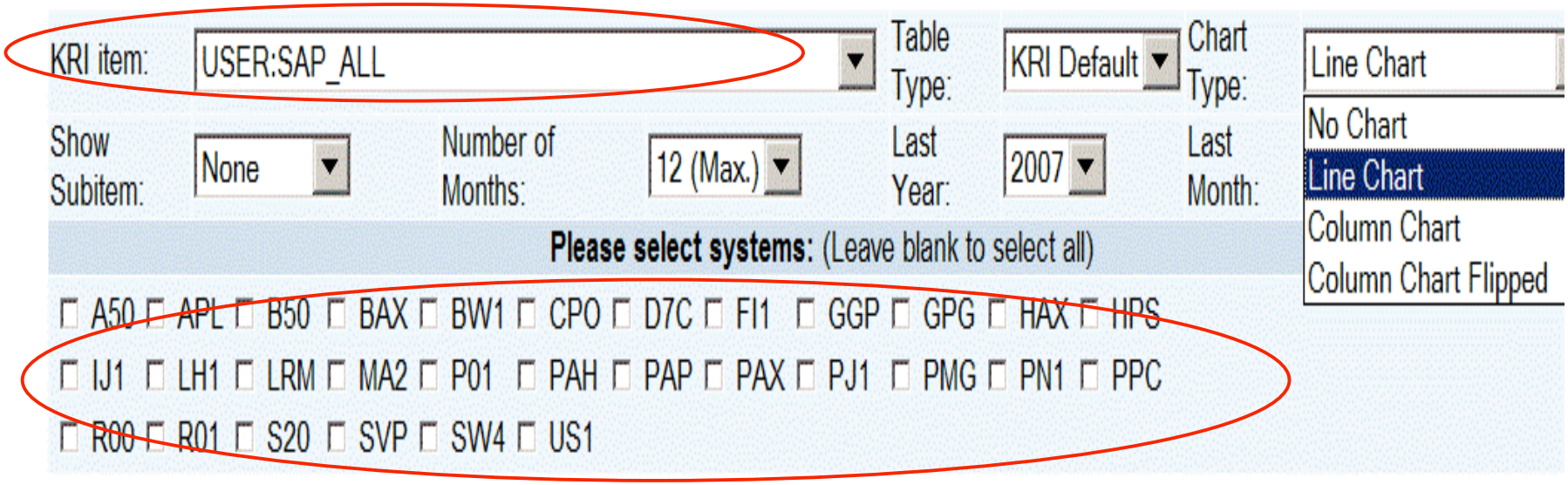
System: A50 | Show Subitems: None | Chart Type: Column Chart (No Chart / Line Chart / Column Chart / Column Chart Flipped)

Number of Months: 12 (Max.) | Last Year: 2007 | Last Month:

Please select KRIs (Leave unchecked to select all)

User	User Roles&Profiles	Transactions	System Availability	Maintenan	
☐ Used (active)	☐ Assigned to Users	☐ ABAP Editor (SE38)	☐ Availability	☐ Open Tickets	☐ min. password length
☐ Unused (4 to 6 months)	☐ Unassigned to Users	☐ User Administration (SU01)	☐ Actual Downtime	☐ Number of Change Requests	☐ password expiration
☐ Unused (> 6 months)	☐ Assigned to Users	☐ Table Maintenance (SM30/SM31)	☐ Elapsed Planned Downtime	☐ Delayed moves to production	☐ PW min. req.: Letters,Digits,Specials
☐ Expired < 395 days (13 months)	☐ Unassigned to Users	☐ Development Workbench (SE80)	☐ Elapsed Unplanned Downtime	☐ No of Transports	☐ time until auto-logout
☐ Expired > 395 days (13 months)		☐ Transport Organizer (SE01)	☐ Pri 1 calls raised in month	☐ No of Emergency Transports	☐ allowed failed login attempts
☐ Locked		☐ All Top 5	☐ Pri 2 calls raised in month		☐ attempts until session ends
☐ Dialog		☐ User Overview (SM04)	☐ Pri 1 calls outside agreed turnaround		☐ session timeout
☐ System		☐ Update Records (SM13)	☐ Pri 2 calls outside agreed turnaround		☐ SAP*
☐ Service		☐ Modify Profiles (RZ10)	☐ Unplanned Outages		☐ SAP* last PW change (YY MM DD)
☐ Reference		☐ Import Transport (STMS)			☐ DDIC

Compare One KPI Across Multiple SAP Systems



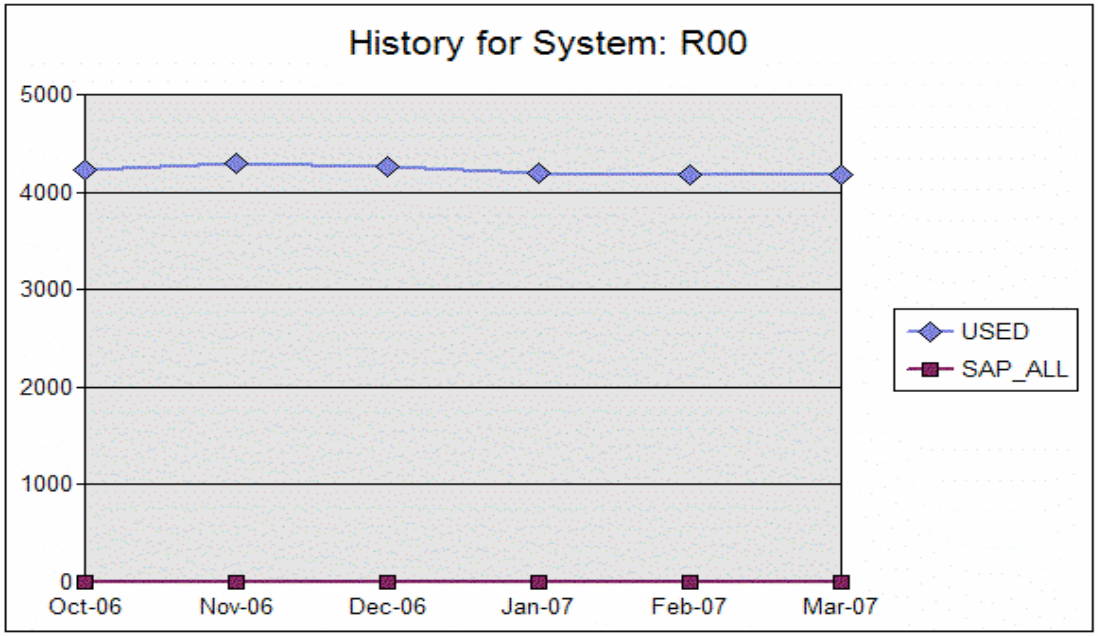
Types of Reports Available

- Current and last month detail
- Compare multiple KPIs across one SAP system
- Compare one KPI across multiple SAP systems
- Complete history report

SAP_ALL (Privileged Access)

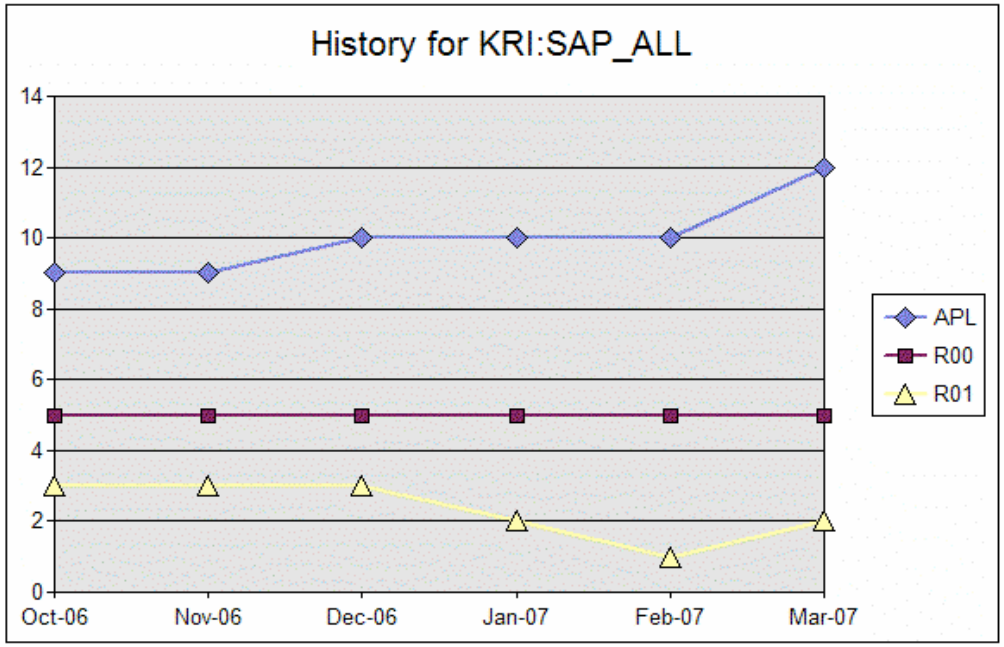
- What does this KPI tell you about the application environment?
- How does HP use this KPI?
- Limitations/Considerations

Active Users (USED) vs. Privileged Users (SAP_ALL)



History for System: R00						
KPI:	**Oct-06**	**Nov-06**	**Dec-06**	**Jan-07**	**Feb-07**	**Mar-07**
USED	4,230	4,292	4,262	4,200	4,176	4,182
SAP_ALL	5	5	5	5	5	5

SAP_ALL Comparison Across Similar Applications



History for KPI:SAP_ALL						
System	**Oct-06**	**Nov-06**	**Dec-06**	**Jan-07**	**Feb-07**	**Mar-07**
APL (Asia Pacific)	9	9	10	10	10	12
R00 (North America)	5	5	5	5	5	5
R01 (Europe)	3	3	3	2	1	2

Challenges

- Identifying KPIs
- Determining how to pull relevant data in a timely manner
- Setting up the automatic pull
- Audit traditionalist may be reluctant to change
- Without a defined methodology auditors may not know how to use CCM tools and apply approach

Considerations for Implementation

- Accuracy and completeness of data
- Let auditors develop/identify KPIs as they audit
- Involvement of external audit
- Training

Google Walkthrough

- Erik Jonte
- ejonte@google.com
- Google, Inc. IT Risk Manager

Background

- Minimal control testing automation
- Resource growth enabled investment in automation
- Desire to reduce manual testing effort

Getting Started

- Large teams not necessary
- Focus on open source or free software
- Hire / cultivate individuals with knowledge / desire to develop
- Identify low hanging fruit to build morale

The Problem

- Code Review and SOD Key Controls
- Very large population of changes
- Complex data structure
- Manual testing approach (sampling)
- Unclear success criteria for testing

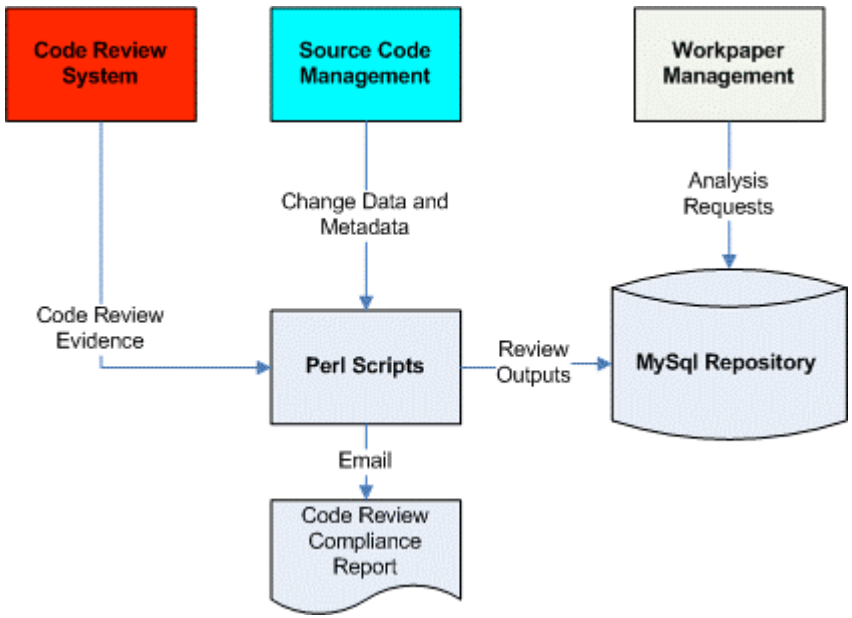
Solution Requirements

- Speed – must exceed manual testing approach
- Accuracy – must be able to detect all error conditions
- Easy Interface – cumbersome solutions are not used
- Acceptable to External Auditors

Integration Challenges

- Getting Data Access
- Normalizing multiple data sources
- Database Storage

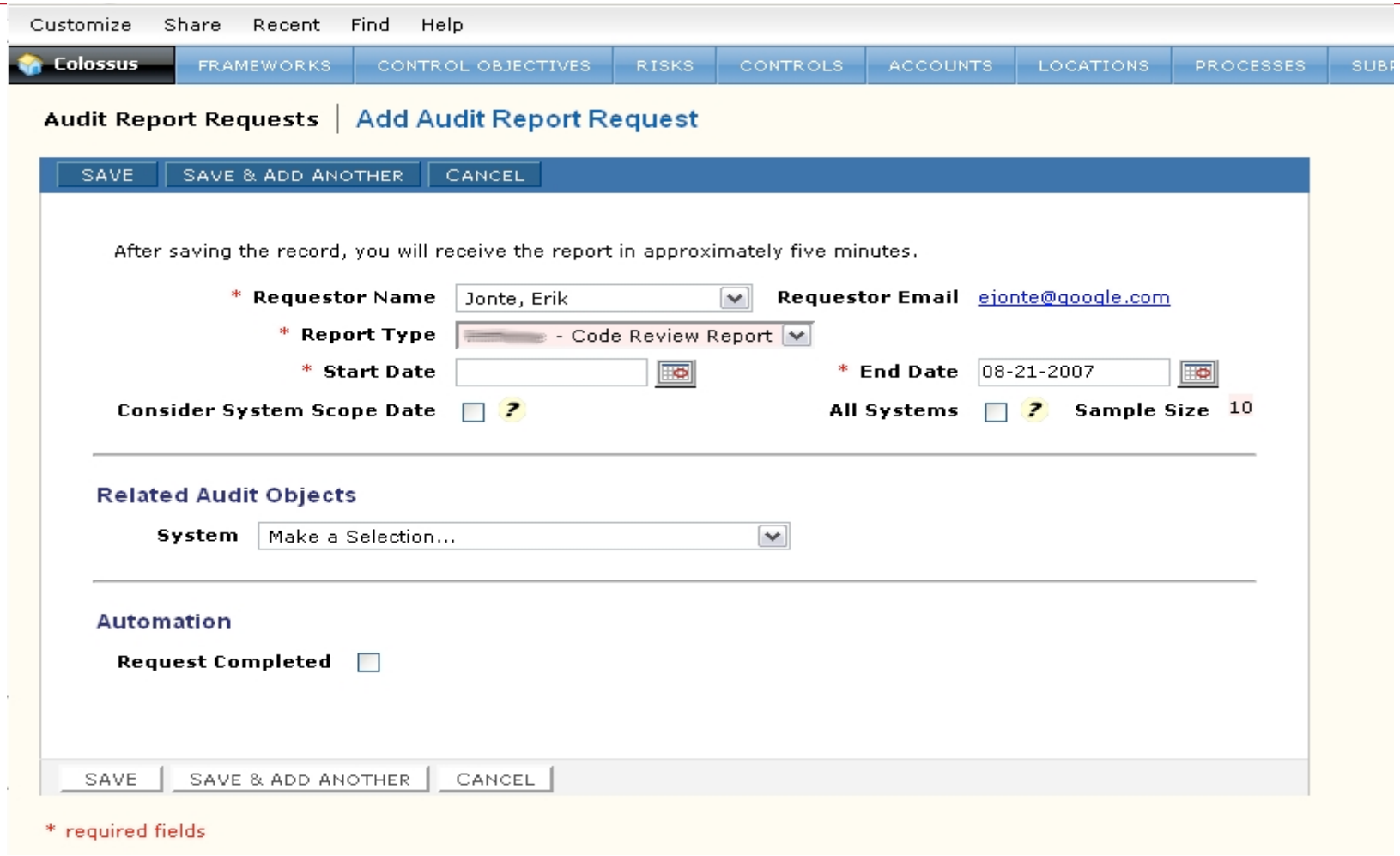
Architecture



Technology Choices

- Perl
  - Tons of text processing speed
  - Many community-available modules
  - Shallow learning curve
- MySQL
  - Free
  - Fast
  - Easy

Request Interface



Sample Report

---------- Forwarded message ----------
From: @google.com <_____ @google.com>
Date: Fri, 22 Jun 2007 00:08:59 UT
Subject: Code Review Report -
To: @google.com, @google.com

------ System: -------

---WARN: No branches configured for this system---
---Directory:
Date Range 2007/01/01 through 2007/05/28
---Directory:
Date Range 2007/01/01 through 2007/05/28
---Directory:
Date Range 2007/01/01 through 2007/05/28
---Directory:
Date Range 2007/01/01 through 2007/05/28
There were:
- 49 exemptions
- 182 exceptions; 0 migrated to a branch prior to being code reviewed
- 401 approved
-- Exception Percentage = 31.22%
---- Exception Subpercentage (Migrated to Branch) = 0.00%

---

2 attachments — Download all attachments

-Configuration.txt
1K View Download

-Results.xls
98K View as HTML

Solution Results

- Delivery to end-users
- Integration with WP management
- Audit of 100% of change population in minutes
- Audit of metadata with 100% accuracy
- Ability to conclude with certainty

Sampling Vs Automation

- Can choose sampling or 100% sample – applicability in different arenas
- Self-documenting
- Certainty over error rates
- Consistent conclusions across team members
- “Automation Dividend”

Complication

- External auditors wanted comfort over exceptions
- Segmentation of exceptions
- Defining criteria was entry into production
- Refine the notion of a true exception
- Used statistical approach to define reasonable assurance

Future Benefits

- Trending Across Time
- Integration into “Audit Data Warehouse”
- Periodic or Continuous Review

Take Aways

- Identify data sources early on
- Strive for normalization of data
- Keep the end-user in mind
- Document requirements and design
- Have a strategy for integration with external audit

In Summary

- Challenges
- Considerations for Implementation
- Opportunities

Challenges

- Deciding the measurements
- Determining how to pull relevant data in a timely manner
- Setting up the automatic pull
- Dealing with the Audit traditionalist (who may be reluctant to change)
- Following a different way – without a corresponding methodology, auditors may not fully benefit from the CCM tools.

Considerations for Implementation

- Expect auditors to identify KPIs as they audit
- Establish practices to ensure accuracy and completeness of data
- Involve external audit
- Scale appropriately for success
- Develop audit methodology to accompany the tool

Opportunities

- Benchmarking focuses the examiner to consider risk and changes to key controls in order to reduce or eliminate inspection testing
- Benchmarking provides an opportunity to shift the SOX effort from a checklist-adherence approach to an ongoing risk-based view of risk benefiting governance

By being able to constantly ‘watch’ systematic controls, examiners can more easily and confidently measure the operating effectiveness of internal controls.

Questions and Collaboration

Jessica Amezquita
Hewlett-Packard, Internal Audit Manager
Jessica.amezquita@hp.com

Eric Jonte
Google, IT Risk Manager
ejonte@google.com

Brad Ames
Hewlett-Packard, Internal Audit Director
brad.ames@hp.com

ISACA®
Serving IT Governance Professionals
San Francisco Chapter