# Continuous Monitoring:
Benchmarking Automated Controls

Vijay Venkatesh, IT Audit Lead
Carrie Gilstrap, IT Audit Manager
Brad Ames, Internal Audit Director
Hewlett-Packard Company

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Agenda

- Premise for Continuous Monitoring
- HP's Continuous Monitoring Model
- Illustrations
- Take Away Learnings
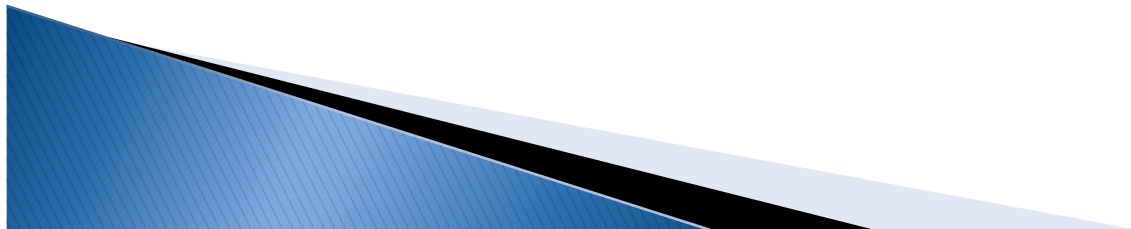
The Opportunity

Post SOX organizations are inclined to embed compliance and assessment (audit) teams to assure good internal controls and are committed to operational excellence, solid metrics for measuring the process and continuous improvement.

We believe that with some additional focus and prioritization, that these organizations can move to a _continuous monitoring_ approach and create a better control environment with much less investment and expense than today's environment..

Continuous Monitoring will allow for far fewer audits including SOX automated control benchmarking.

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
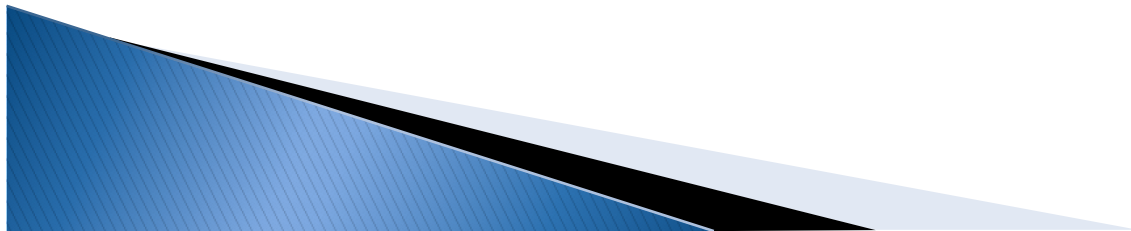
Premise for Continuous Control Measurement

- **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.

Continuous Control Measurement (CCM)

▸ Provides a way to reduce uncertainty and assess risk
▸ Gives ongoing visibility to risk and the control environment
▸ Measures key control indicators to isolate outliers
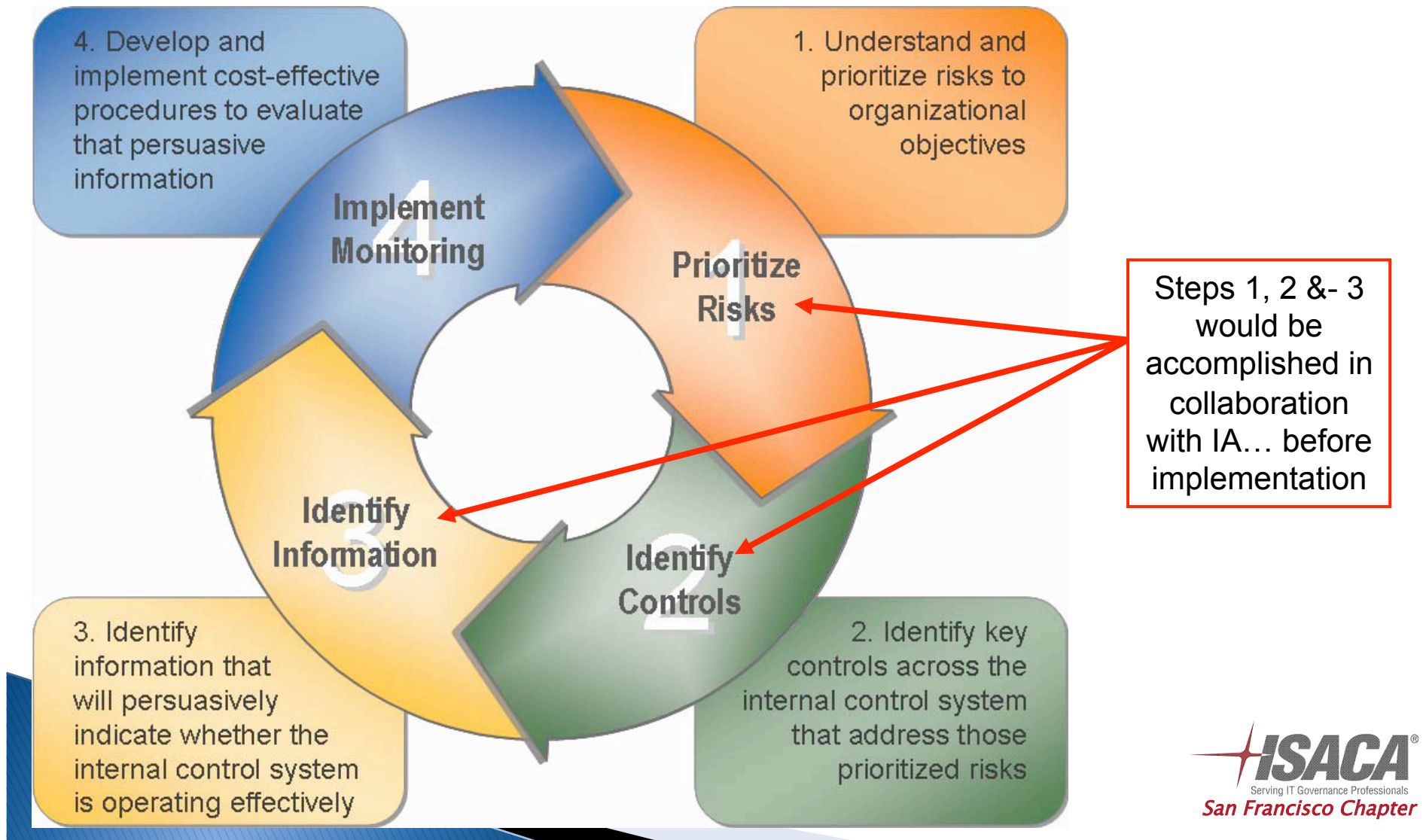▸ Allows a more timely conclusion regarding the control environment

Continuous Control Measurement
makes complex things simple to see.

From project to progress: Ongoing benefits of CCM

▸ Modeling Key Control Indicators enables us to:
  ◦ Link change to real risk and risk response
  ◦ Reduce audit uncertainty
  ◦ Simplify Sarbanes Oxley testing
  ◦ Focus prospectively
▸ Measuring Key Control Indicators provides:
  ◦ Early possession of information regarding emerging risk
  ◦ Current disclosure of changes in the control environment
  ◦ Transparent attestation: Precise auditor deployment
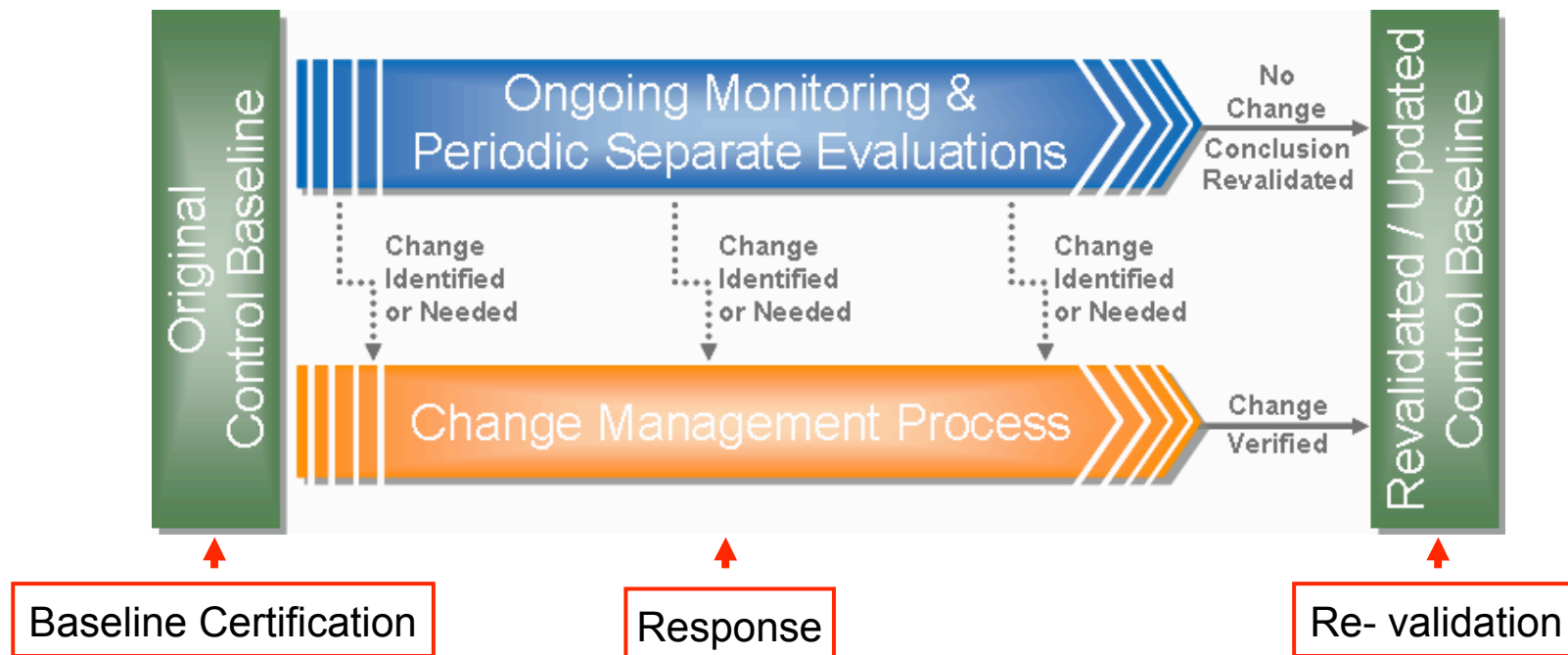
The Steps Toward Continuous Monitoring
COSO Guidance on Monitoring Internal Control Systems

4. Develop and implement cost-effective procedures to evaluate that persuasive information

Implement Monitoring 4

1. Understand and prioritize risks to organizational objectives

Prioritize Risks 1

Steps 1, 2 &- 3 would be accomplished in collaboration with IA… before implementation

Identify Information 3

3. Identify information that will persuasively indicate whether the internal control system is operating effectively

Identify Controls 2

2. Identify key controls across the internal control system that address those prioritized risks

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

How Continuous Monitoring Works
COSO Guidance on Monitoring Internal Control Systems

Trending and comparing changes to a predefined threshold will sustain and carry forward the Baseline Certification with minimal examination.
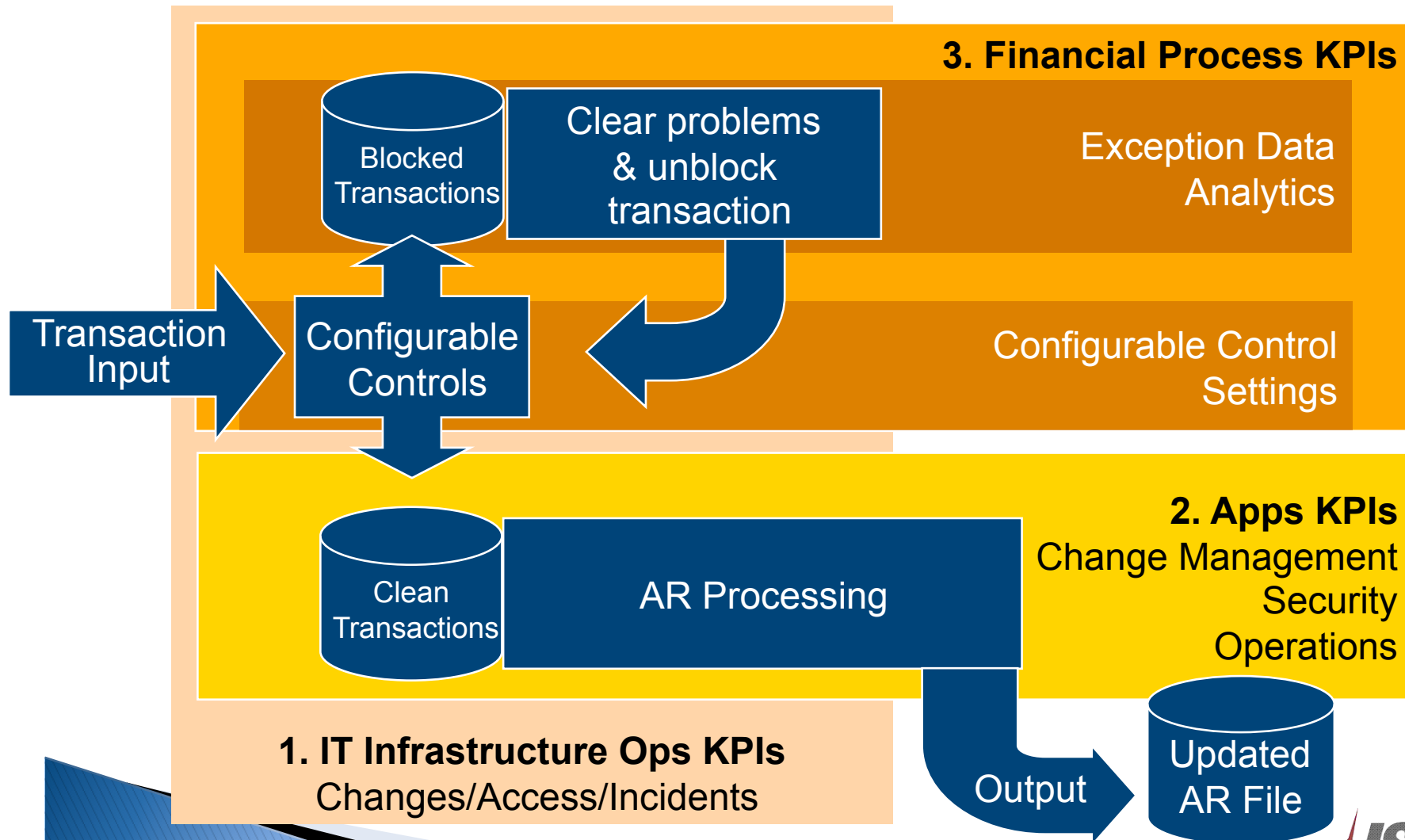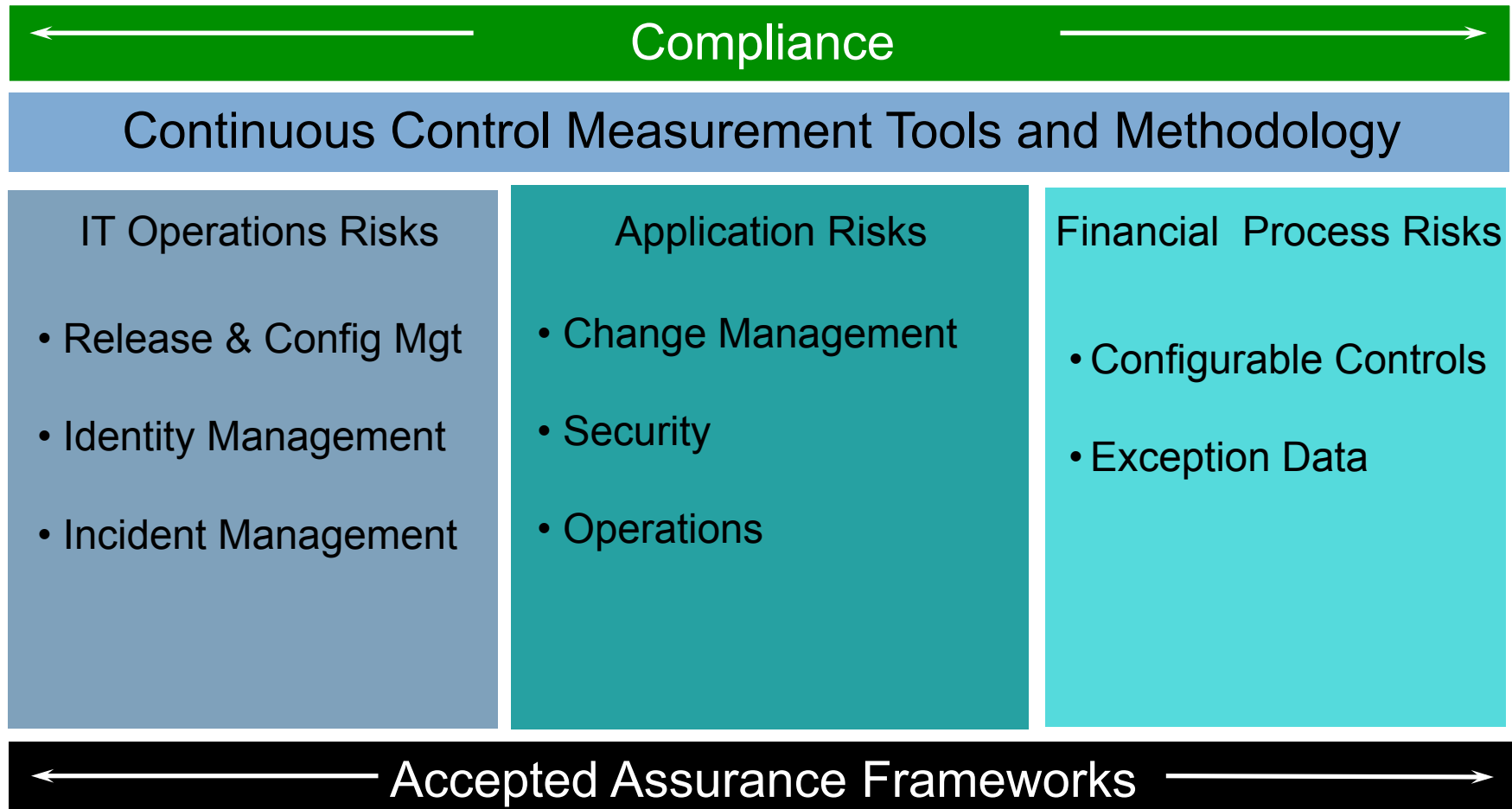
Measuring IT Risk

▸ Key Performance Indicators (KPIs) of IT Controls exist at various levels in the organization:
1. IT Infrastructure Operations
2. Applications
3. Financial Processes

▸ How does audit assess these controls by area?

Accounts Receivable (AR) Cycle: 3 areas of KPIs

3. Financial Process KPIs

Blocked Transactions

Clear problems & unblock transaction

Exception Data Analytics

Transaction Input

Configurable Controls

Configurable Control Settings

Clean Transactions

AR Processing

2. Apps KPIs
Change Management
Security
Operations

1. IT Infrastructure Ops KPIs
Changes/Access/Incidents

Output

Updated AR File

Alignment is the Key

Compliance

Continuous Control Measurement Tools and Methodology

IT Operations Risks	Application Risks	Financial Process Risks
• Release & Config Mgt	• Change Management	• Configurable Controls
• Identity Management	• Security	• Exception Data
• Incident Management	• Operations	

Accepted Assurance Frameworks

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Walkthrough Illustrations

▸ Carrie.Gilstrap@hp.com
▸ IT Audit Manager

▸ Vijay.Venkatesh@hp.com
▸ IT Audit Lead

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
  - Segregation of Duties
- Operations
  - Number of users with the ability to create/modify/delete jobs
- Configurable Application Controls

Maintenance

- Change Management: Move to Production Process Segregation
  - Controls exist to ensure that Developers cannot move changes to the Production environment
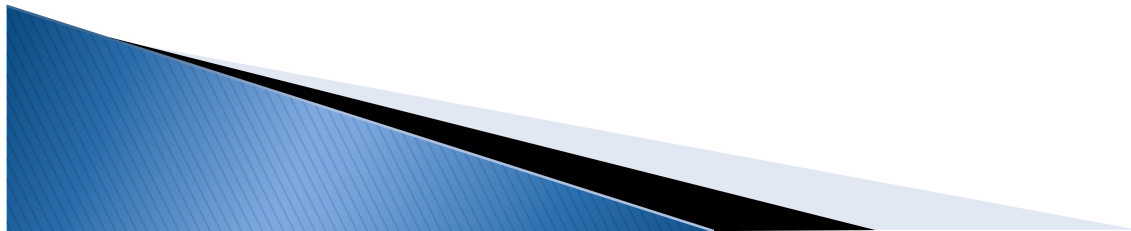
D7 Maintenance – KPI values

- Users with Dev Key on DEV instance
  - showing users from production with a developer key on DEV

- All users with Dev Key on DEV instance
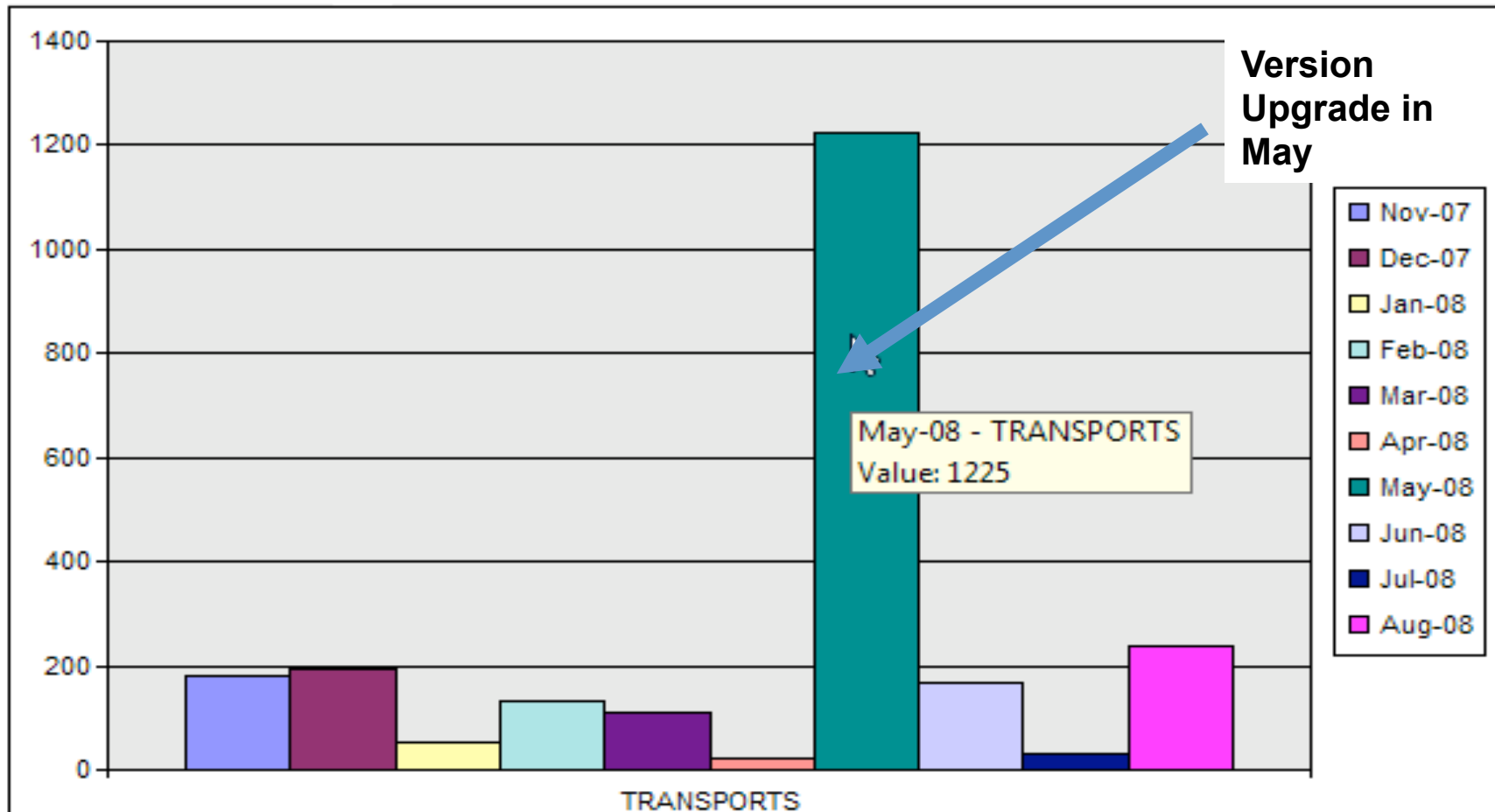 - showing all users with a developer key on DEV

				Last	Current
User		System	#	71	71
	by type	Service	#	1	1
		Reference	#	0	0
		CPIC an...	#	75	77
			#	0	0
		Total...	#	3715	3691
	by usage	Never log...	#	85	77
	special	Users with Dev Key on DEV instance	#	33	36
		All users with Dev Key on DEV instances	#	55	65
	by profile	SAP_ALL	#	1	1

Users who have been identified to have a developer account on the Dev. instance of this platform
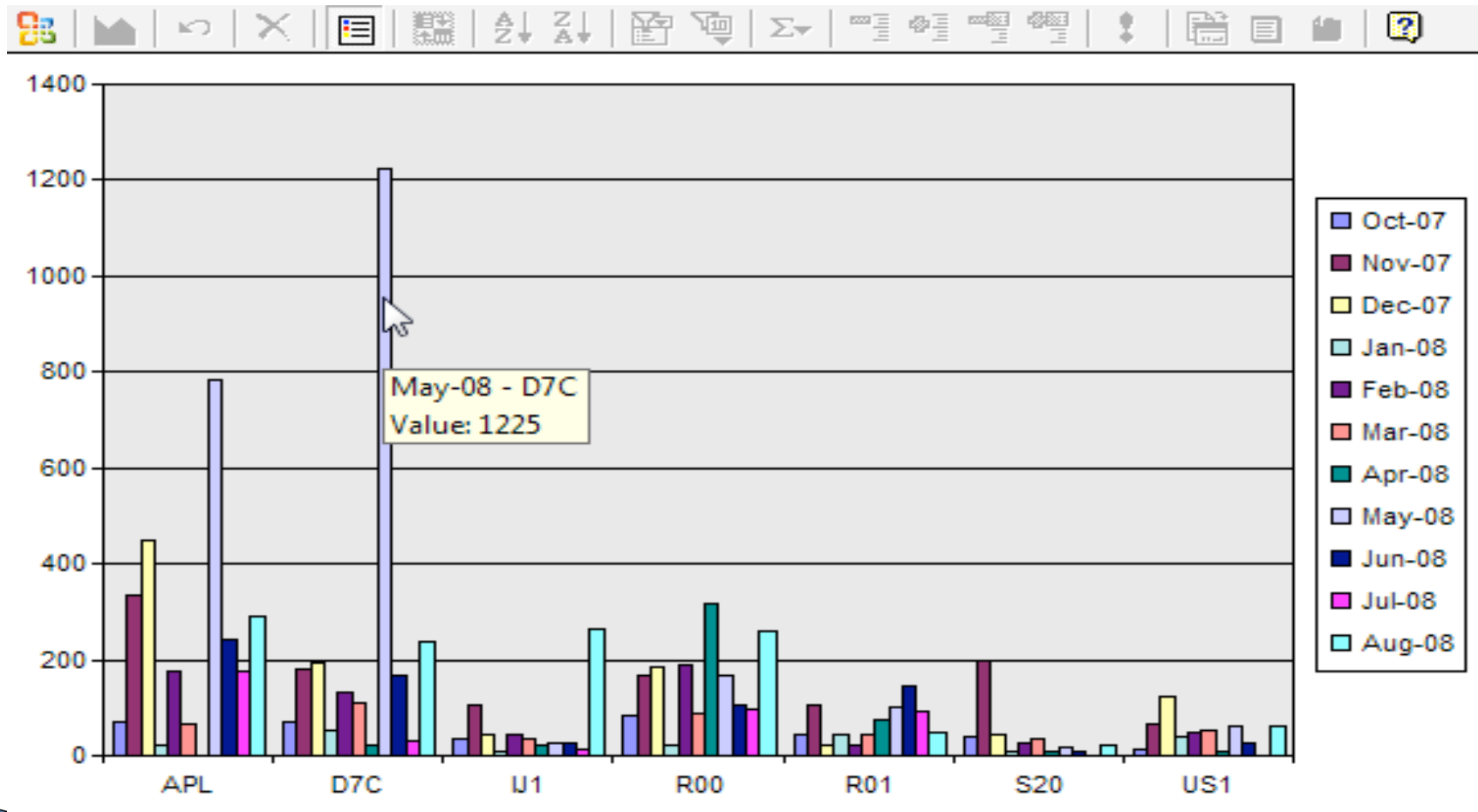
Users with DEV Key and Transport Management – Comparison Across Systems
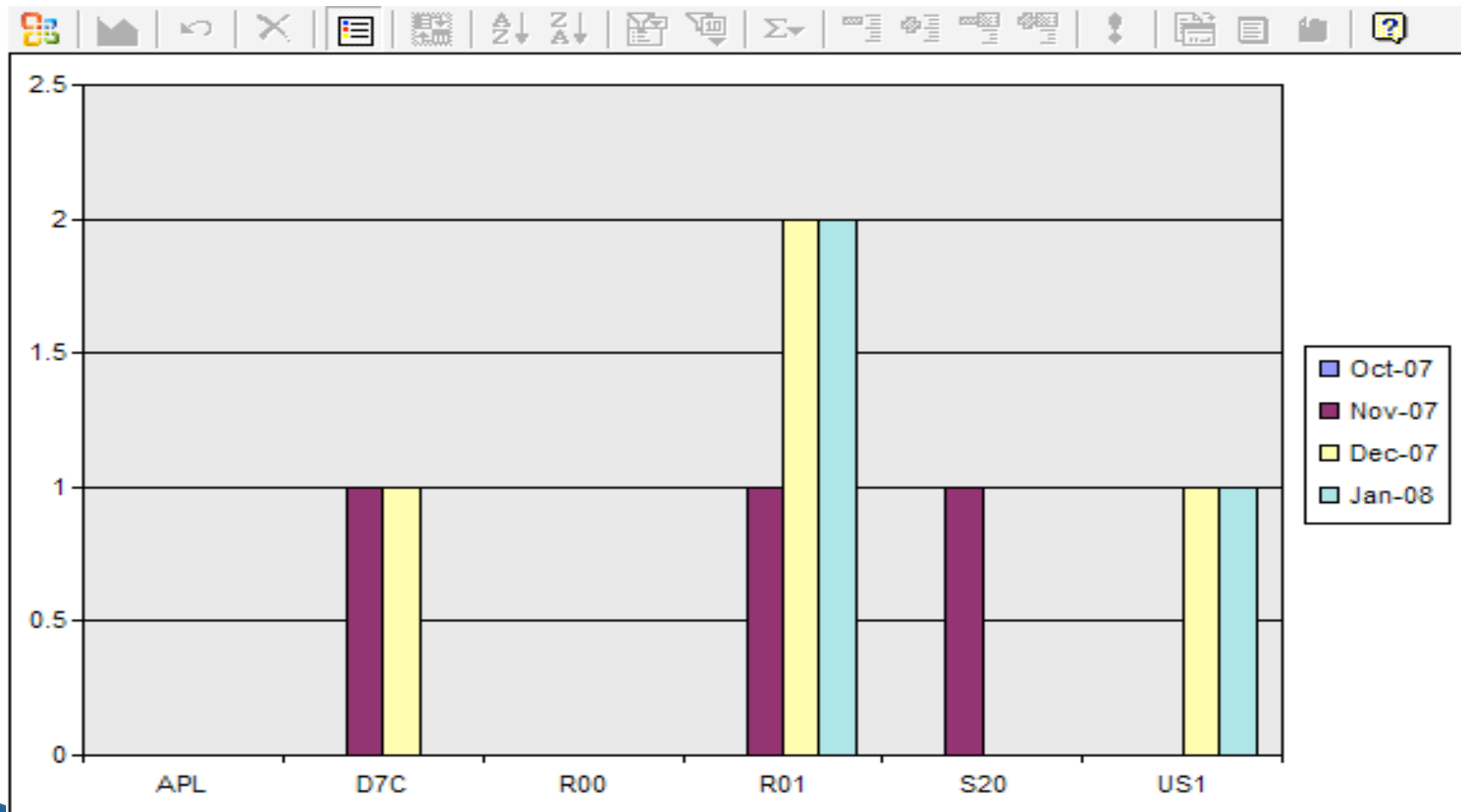
Number of Transports – D7C (November 2007 through August 2008)

Number of Transports across applications (October 2007 through August 2008)

Number of Transports across applications – Detail Report

System	_Oct-07	_Nov-07	_Dec-07	_Jan-08	_Feb-08	_Mar-08	_Apr-08	_May-08	_Jun-08	_Jul-08
APL	70	334	450	20	174	66	-	782	240	176
D7C	69	179	194	55	133	110	22	1225	166	33
IJ1	36	104	44	9	45	34	23	27	28	12
R00	82	166	183	23	188	87	318	168	105	98
R01	46	104	23	45	24	46	75	100	146	94
S20	41	196	44	7	26	34	9	16	7	2
US1	13	65	123	39	47	54	11	63	26	1

History for KRI:TRANSPORTS

Sheet1

File   Edit   View   Favorites   Tools   Help

HP KRI Information System - Data Entry

Business Group	GO+IT - SCIT		Sysid	R00	Installation	
Year	2007		Month	March	Client	
Detail Level	○ Low - 1 ○ Medium - 2 ● High - 3				Last Data Pull:	

→ edit data   → reset system   → close window   → help

AREA	GROUP	ITEM	SITEM	UNIT

Last / Current Month

		Used (active)		#
		Unused (4 to 6 months)		#
		Unused (>		#
		Expired < 395 days (13 months)		#
	only dialog	Expired > 395 days (13 months)		#
		Locked		#
		Dialog		#
		System		#
		Service		#
User	by type	Reference		#
		CPIC and Communication		#
		Others		#
		Total number of Logons		#
	by usage	Never logged on		#
	special	Users with Dev Key on DEV instance		#
	by profile	SAP_ALL		#
	Profiles	Assigned to Users		#
User Roles&Profiles		Unassigned to Users		#
	Roles/Activity Groups	Assigned to Users		#
		Unassigned to Users		#
			Display	#
			Create	#

Number of Users

		Delete	#	30	30	
	Transport	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	

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Active Users (USED) vs. Privileged Users (SAP_ALL)
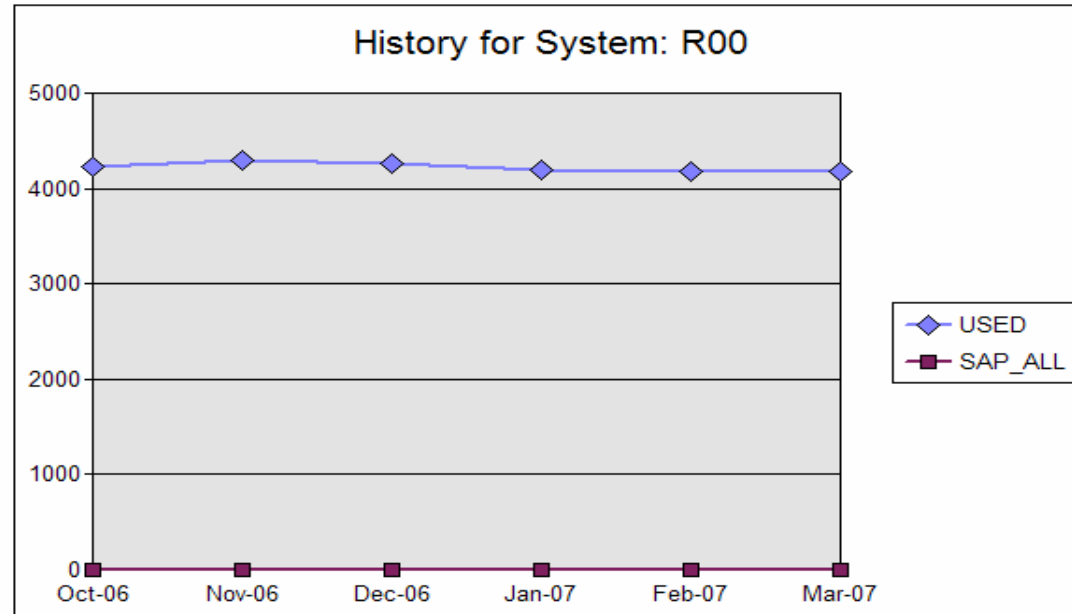
History for System: R00						
KPI:	**Oct-06**	**Nov-06**	**Dec-06**	**Jan-07**	**Feb-07**	**Mar-07**
USED	4,230	4,292	4,262	4,200	4,176	4,182
SAP_ALL	5	5	5	5	5	5

SAP_ALL Comparison Across Similar Applications (October 2006 – March 2007)

History for KRI:SAP_ALL
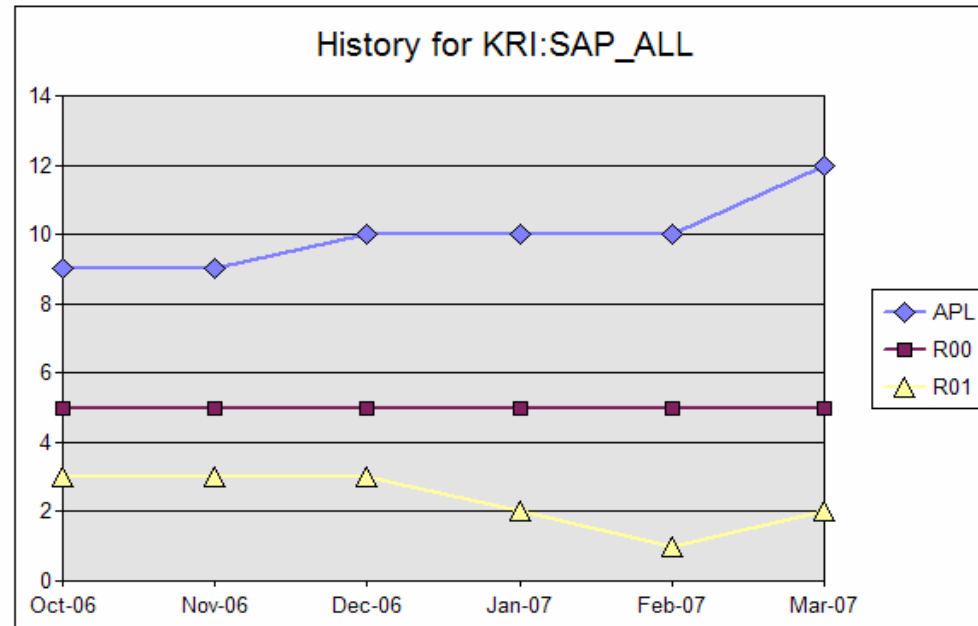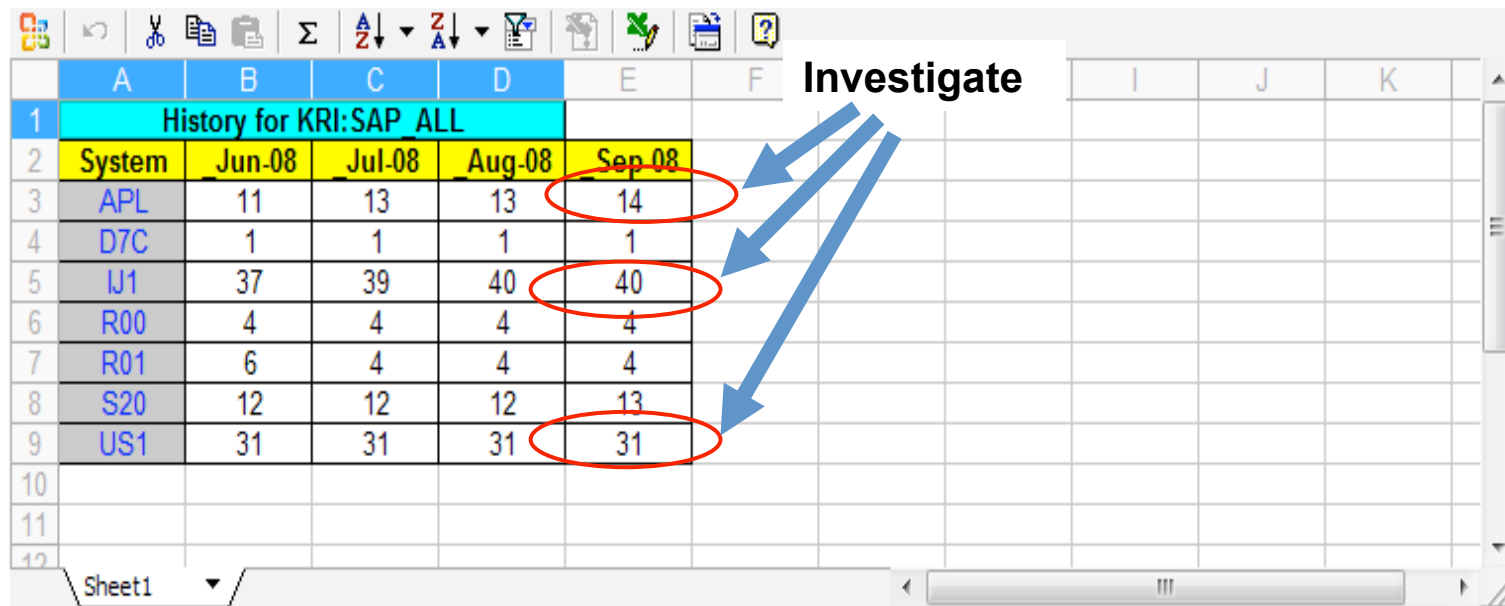
SAP_ALL Comparison Across Similar Applications (October 2006 – March 2007)

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

SAP_ALL Comparison Across Similar Applications (June 2008 – Sept 2008)

SAP_ALL Comparison Across Similar Applications (June 2008 – Sept 2008)

SAP_ALL Details for IJ1 – September 2008

| Logon name:	Client:	UserID:	Email:	Logon type:	User group:	rprise Dir. - Emp	Logon status:	Logon created:	Logon valid to:	Last logon:
20354062	100	kritika.khemani@hp.com	ika.khemani@hp.c	DIALOG	BASIS:SECRTY	20354062	USED	30.07.2008	31.12.9999	12.09.2008
20387283	100	luis-enrique.perez@hp.com	enrique.perez@hp.	DIALOG	BASIS:SECRTY	20387283	USED	07.03.2008	31.12.9999	11.09.2008
ALEREMOTE	100	basisuser@hp.com	basisuser@hp.co	CPIC/COMM	INTERFACE		USED	19.01.2005	-	03.09.2008
APOREMT_IJ1	100			SYSTEM	INTERFACE		USED	01.06.2007	31.12.9999	01.09.2008
BATCHAM	100	batchuser@hp.com	batchuser@hp.con	SYSTEM	BATCHUSER		USED	03.07.2003	-	31.08.2008
BATCHBO	100	batchuser@hp.com	batchuser@hp.con	SYSTEM	BATCHUSER		USED	05.09.2001	-	28.08.2008
BATCHCV	100	batchuser@hp.com	batchuser@hp.con	SYSTEM	BATCHUSER		USED	11.02.2002	-	01.09.2008
BATCHGL	100	batchuser@hp.com	batchuser@hp.con	SYSTEM	BATCHUSER		USED	16.02.2001	-	02.09.2008
BATCHIE	100	batchuser@hp.com	batchuser@hp.con	SYSTEM	BATCHUSER		UNUSED1	09.02.2001	-	19.08.2008
BATCHLTA	100	batch_sap@hp.com	atch_sap@hp.con	SYSTEM	BATCHUSER		USED	13.09.2002	-	24.07.2008
BATCHLTE	100	batchuser@hp.com	batchuser@hp.con	SYSTEM	BATCHUSER		UNUSED1	13.09.2002	-	26.03.2007
BATCHMRS	100	basisuser@hp.com	basisuser@hp.con	SYSTEM	BATCHUSER		UNUSED1	16.10.2003	-	26.03.2007
BATCHPR	100	batchuser@hp.com	batchuser@hp.con	SYSTEM	BATCHUSER		USED	09.02.2001	-	30.08.2008
BATCHSAP	100	batchuser@hp.com	batchuser@hp.con	SYSTEM	BATCHUSER		USED	21.08.2003	-	02.09.2008
BATCHSD	100	batchuser@hp.com	batchuser@hp.con	SYSTEM	BATCHUSER		UNUSED1	11.02.2002	-	22.09.2008
BATCHSG	100	batchuser@hp.com	batchuser@hp.con	SYSTEM	BATCHUSER		USED	24.10.2001	-	02.09.2008
CMUSER	100	basisuser@hp.com	basisuser@hp.con	SYSTEM	INTERFACE		UNUSED2	03.12.2001	-	03.12.2001
DDIC	100	basisuser@hp.com	basisuser@hp.con	CPIC/COMM	SUPER		UNUSED1	19.06.1992	-	28.03.2007
ELAINEL	100	elaine.lee@hp.com	elaine.lee@hp.con	DIALOG	IT DEVELOPER	00355340	USED	02.11.2006	31.12.9999	12.09.2008
FAXUSER	100	basisuser@hp.com	basisuser@hp.con	CPIC/COMM	INTERFACE		USED	16.11.2003	-	10.03.2008
FINCPIC	100	basisuser@hp.com	basisuser@hp.con	CPIC/COMM	INTERFACE		USED	04.10.2001	-	03.09.2008
IJ1BATCH	100	batchuser@hp.com		SYSTEM	INTERFACE			-	-	-
IXOSCPIC	100	basisuser@hp.com	basisuser@hp.con	SYSTEM	INTERFACE		UNUSED2	09.11.2004	-	25.10.2005
OSS302620	100	basisuser@hp.com	basisuser@hp.con	DIALOG	SAPNET		EXPIRED1	10.04.2008	01.05.2008	16.04.2008
PAPIDOC2IJ1	100	basisuser@hp.com	basisuser@hp.con	CPIC/COMM	INTERFACE		USED	12.09.2007	31.12.9999	-
RFCCONNECT	100	basisuser@hp.com	basisuser@hp.con	CPIC/COMM	INTERFACE		USED	07.12.2000	-	03.09.2008
RSIMA2445ALE	100	basisuser@hp.com	basisuser@hp.con	CPIC/COMM	INTERFACE		USED	09.02.2001	-	03.09.2008
SAP*	100	basisuser@hp.com	basisuser@hp.con	DIALOG	SUPER		UNUSED2	16.01.2001	31.12.9999	28.03.2007
SAP439650	100	hugh.oconnor@hp.com	gh.oconnor@hp.c	DIALOG	SAPNET	00117436	EXPIRED1	28.05.2008	20.06.2008	09.06.2008
SAPOSS1	100	basisuser@hp.com	basisuser@hp.con	DIALOG	SAPNET		EXPIRED2	07.01.2002	17.11.2006	08.11.2006
SPLOADER_IE	100	basisuser@hp.com	basisuser@hp.con	CPIC/COMM	INTERFACE		UNUSED2	02.04.2001	-	02.06.2004
SRM3RFC	100	scitsapsecurityamericas@hp.com	sc-it-basis-team@	CPIC/COMM	INTERFACE		USED	17.01.2001	-	19.08.2008
TIDAL2IJ1	100			CPIC/COMM	INTERFACE			-	-	-
TWW_TKX	100	basisuser@hp.com		SYSTEM	INTERFACE			-	-	-
TWW_TKX_IE	100	basisuser@hp.com	basisuser@hp.con	SYSTEM	INTERFACE		USED	09.02.2001	-	04.04.2008
TWW_TKX_PR	100	basisuser@hp.com	basisuser@hp.con	SYSTEM	INTERFACE		USED	09.02.2001	-	30.05.2008
TWW_TKX_SG	100	basisuser@hp.com	basisuser@hp.con	SYSTEM	INTERFACE		USED	25.10.2001	-	28.05.2008
TWW_TKX_WC	100	basisuser@hp.com	basisuser@hp.con	SYSTEM	INTERFACE		USED	19.06.2002	-	26.10.2007

SAP_ALL Details for APL – September 2008

Logon name:	Client:	UserID:	Email:	Logon type:	User group:	erprise Dir. - Emp	Logon status:	Logon created:	Logon valid to:	Last logon:
									List of 14 login(s):	
00401213	016	santiago.elias@hp.com	ntiago.elias@hp.c	DIALOG	SUPER	00401213	USED	15.05.2008	31.12.9999	11.09.2008
ALEUSER	016	apladm@hp.com	apladm@hp.com	CPIC/COMM	CPIC		USED	16.12.2000	-	11.09.2008
ALICE 445	016	basisuser@hp.com	basisuser@hp.con	CPIC/COMM	CPIC		USED	02.07.2001	-	11.09.2008
APFUSNBATCH	016	apfusnbatch@sappap.sapnet.hp.com		SYSTEM	BATCH_PSDA			-	-	-
CIDJCPIC	016	basisuser@hp.com	basisuser@hp.con	CPIC/COMM	CPIC		LOCKED	21.11.2000	-	09.09.2008
DDIC	016	randy.alabado@hp.com	ndy.alabado@hp.c	DIALOG	SYSTEM	00375747	UNUSED2	14.11.2000	-	04.01.2008
FINCPIC	016	basisuser@hp.com	basisuser@hp.con	CPIC/COMM	CPIC		USED	01.03.2005	-	02.05.2008
IXOSCPIC	016	basisuser@hp.com	basisuser@hp.con	SYSTEM	CPIC		USED	05.12.2005	-	14.05.2008
SAPOSS	016	basis@hp.com	basis@hp.com	DIALOG	FRZN NOSAPAP		EXPIRED1	27.03.2008	19.06.2008	10.07.2008
SOLMAN_RFC	016	kumar-lalit.mangla@hp.com	basisuser@hp.con	CPIC/COMM	CPIC	20263191	LOCKED	20.09.2005	31.12.9999	11.09.2008
TIDAL2APL	016	sudhir.kulkarni@hp.com	dhir.kulkarni@hp.c	CPIC/COMM	8IT	20191499	USED	09.07.2007	31.12.9999	11.09.2008
USRBATCH	016	michael.rullkoetter@hp.com	ael.rullkoetter@hp	SYSTEM	SYSTEM	00116165	UNUSED2	05.03.2007	-	05.03.2007
WF-BATCH	016	batchuser@hp.com	uichun@email.cor	SYSTEM	BATCH_CIDJ		USED	02.04.2001	-	11.09.2008
WORKFLOW	016	workflow@ctss232.sgp.hp.com	w@ctss232.sgp.h	SYSTEM	BATCH_CIDJ		UNUSED2	02.04.2001	-	16.08.2001

SAP_ALL – Comparison Across Systems – July 2004 versus September 2008

System	Jul-04	Sep-08
APL	23	14
R01	8	4
R00	7	4
IJ1	33	40
D7C	1	1

Number of Users with access to SAP_ALL (July 2004 versus September 2008)


Increase over the 4 year period for IJ1
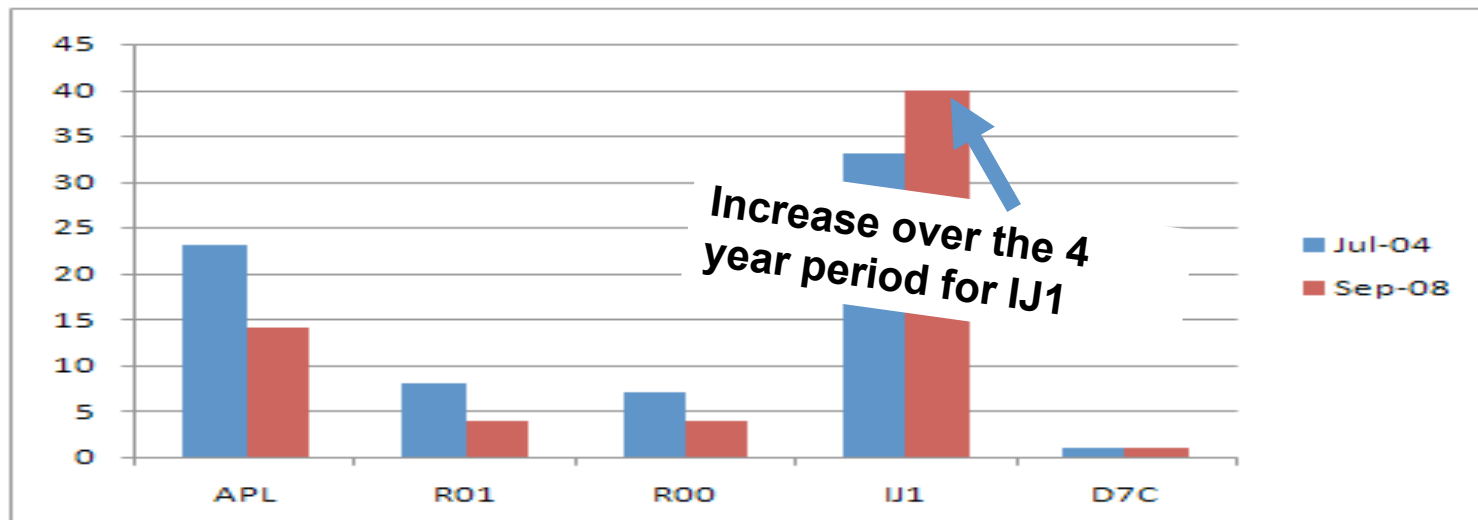
Comprehensive User Profile Reports – D7C – September 2008
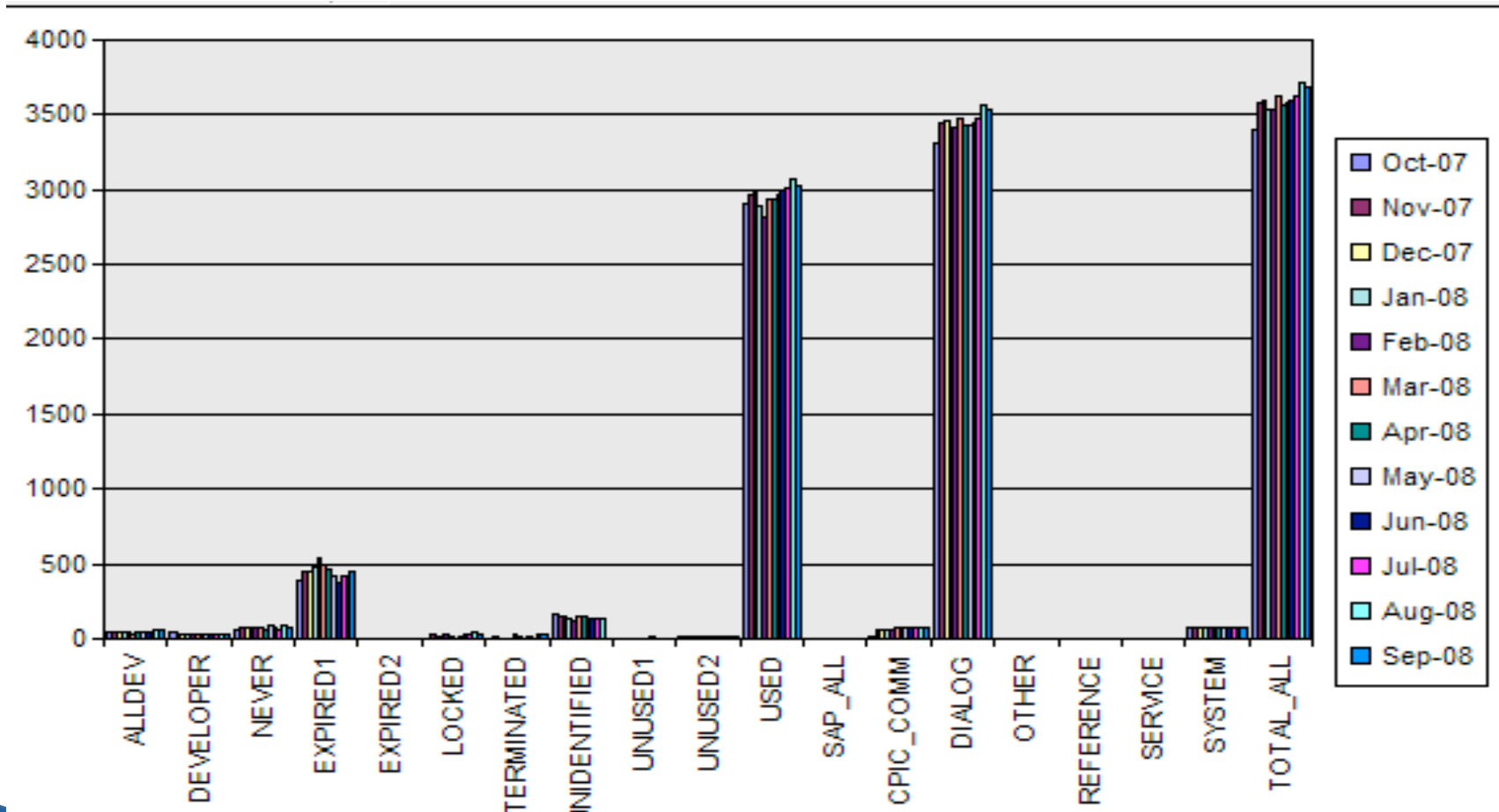
Comprehensive User Profile Report Details – D7C – September 2008

	A	B	C	D	E	F	G	H	I	J	K	L
					History for System: D7C							
	KRI:	Nov-07	Dec-07	Jan-08	Feb-08	Mar-08	Apr-08	May-08	Jun-08	Jul-08	Aug-08	Sep-08
	ALLDEV	51	51	51	51	36	39	39	40	41	55	65
	DEVELOPER	35	34	31	31	30	30	29	31	29	33	36
	NEVER	81	77	59	71	69	66	93	71	67	85	77
	EXPIRED1	445	450	473	539	495	462	417	382	420	416	454
	EXPIRED2	3	3	3	3	5	5	4	4	4	5	2
	LOCKED	25	8	21	29	18	0	18	37	27	41	35
	TERMINATED	8	5	3	6	26	16	7	9	4	27	37
	UNIDENTIFIED	143	152	141	125	150	145	140	141	142	135	4
	UNUSED1	5	4	3	5	6	7	8	6	4	6	5
	UNUSED2	10	12	14	15	15	16	13	16	20	22	17
	USED	2960	2990	2895	2818	2940	2934	2972	3003	3007	3078	3029
	SAP_ALL	1	1	1	1	1	1	1	1	1	1	1
	CPIC_COMM	58	59	60	60	75	75	71	74	75	75	77
	DIALOG	3448	3467	3409	3409	3479	3424	3432	3448	3482	3568	3542
	OTHER	0	0	0	0	0	0	0	0	0	0	0
	REFERENCE	0	0	0	0	0	0	0	0	0	0	0
	SERVICE	1	1	1	1	1	1	1	1	1	1	1
	SYSTEM	69	69	69	69	71	71	71	71	71	71	71
	TOTAL_ALL	3576	3596	3539	3539	3626	3571	3575	3594	3629	3715	3691
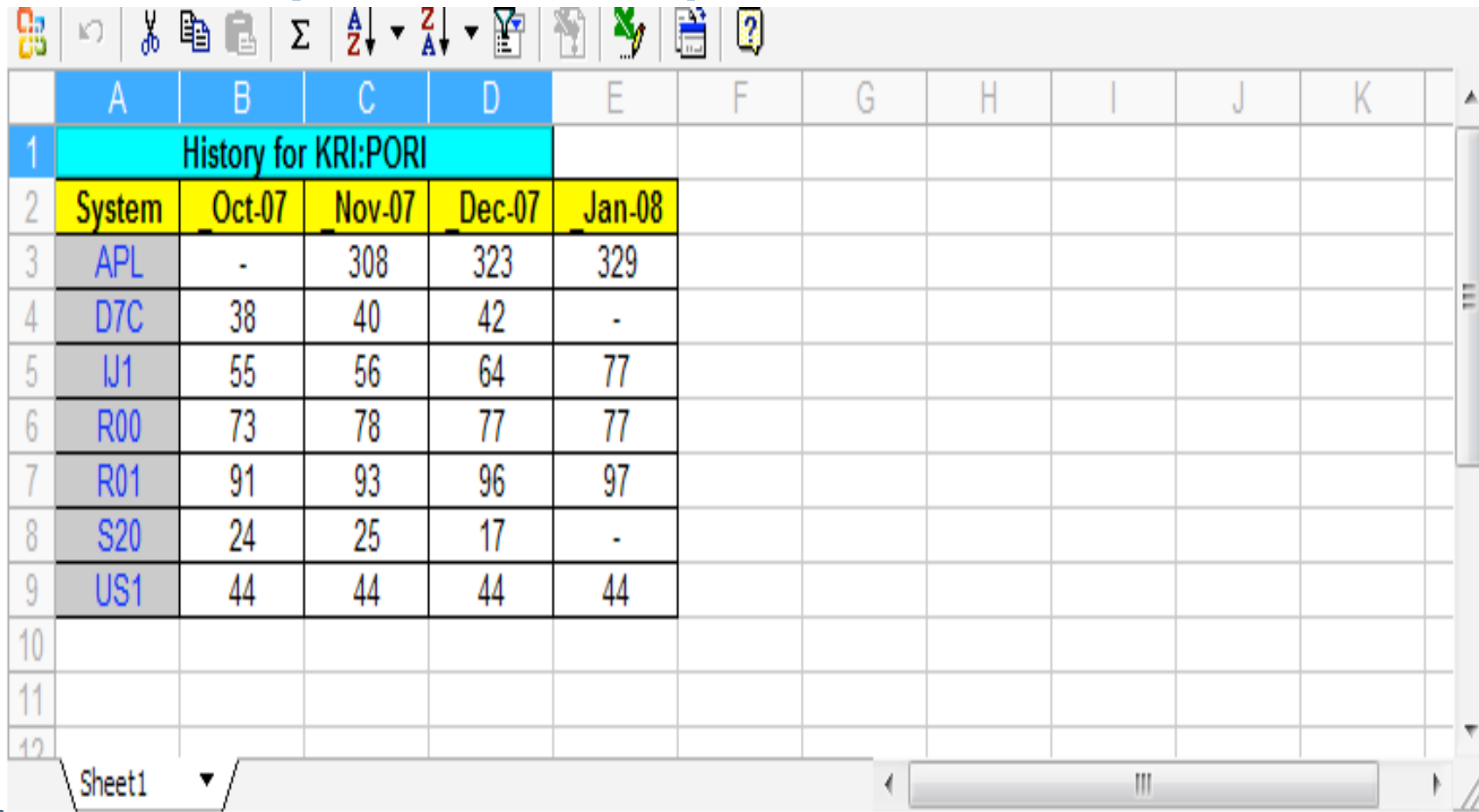
Comparison of Terminated Users Across Applications (October 2007 through September 2008)
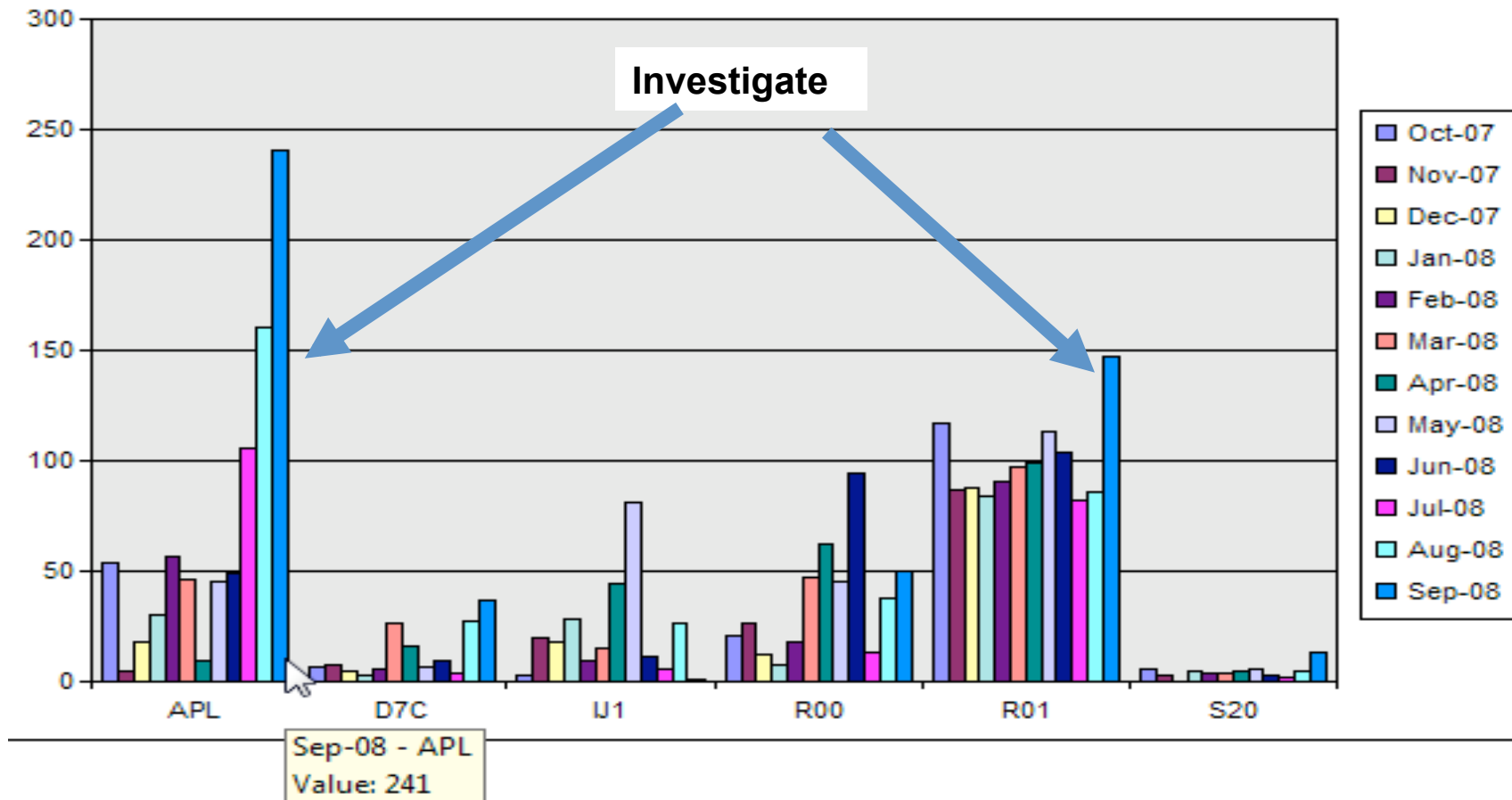
Comparison of SOD Conflicts across applications – Purchase Orders, Receipts and Inventory
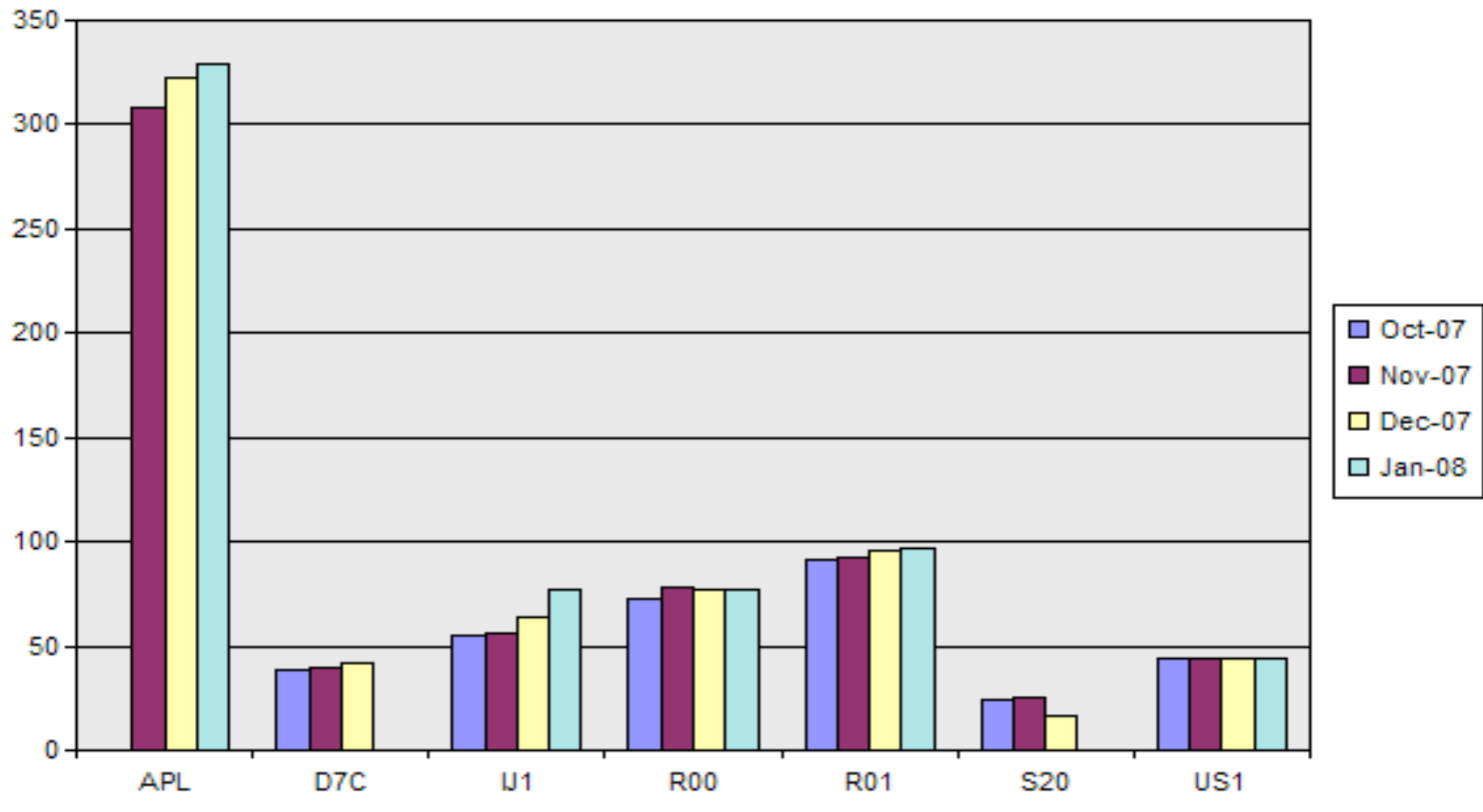
Comparison of SOD Conflicts across applications – Purchase Orders, Receipts and Inventory – Detail report

System	_Oct-07	_Nov-07	_Dec-07	_Jan-08
APL	-	308	323	329
D7C	38	40	42	-
IJ1	55	56	64	77
R00	73	78	77	77
R01	91	93	96	97
S20	24	25	17	-
US1	44	44	44	44

History for KRI:PORI

Comparison of SOD Conflicts across applications – Vendors, Invoices and Payments

Comparison of SOD Conflicts across applications – Vendors, Invoices and Payments – Detail Report

System	_Oct-07	_Nov-07	_Dec-07	_Jan-08
History for KRI:VIP				
APL	-	174	181	184
D7C	43	46	47	-
IJ1	61	62	65	78
R00	56	62	62	62
R01	156	159	165	169
S20	30	32	23	-

Unidentified Dialog Logins – Comparison Across Systems

Unidentified Dialog Logins – Comparison Across Systems – Detail report

1	History for KRI:UNIDENTIFIED											
2	System	_Oct-07	_Nov-07	_Dec-07	_Jan-08	_Feb-08	_Mar-08	_Apr-08	_May-08	_Jun-08	_Jul-08	_Aug-08	_Sep-08
3	APL	160	186	186	134	98	349	118	119	112	128	169	44
4	D7C	166	143	152	141	125	150	145	140	141	142	135	4
5	IJ1	28	480	28	30	28	28	31	35	30	27	26	1
6	R00	249	251	265	257	217	217	210	202	195	177	171	4
7	R01	159	292	169	156	134	122	157	156	147	140	133	6
8	S20	16	135	54	9	9	46	46	46	47	46	44	0
9	US1	9	11	8	8	8	8	8	8	8	8	8	12

Job Scheduling – SM37 – Comparison Across systems
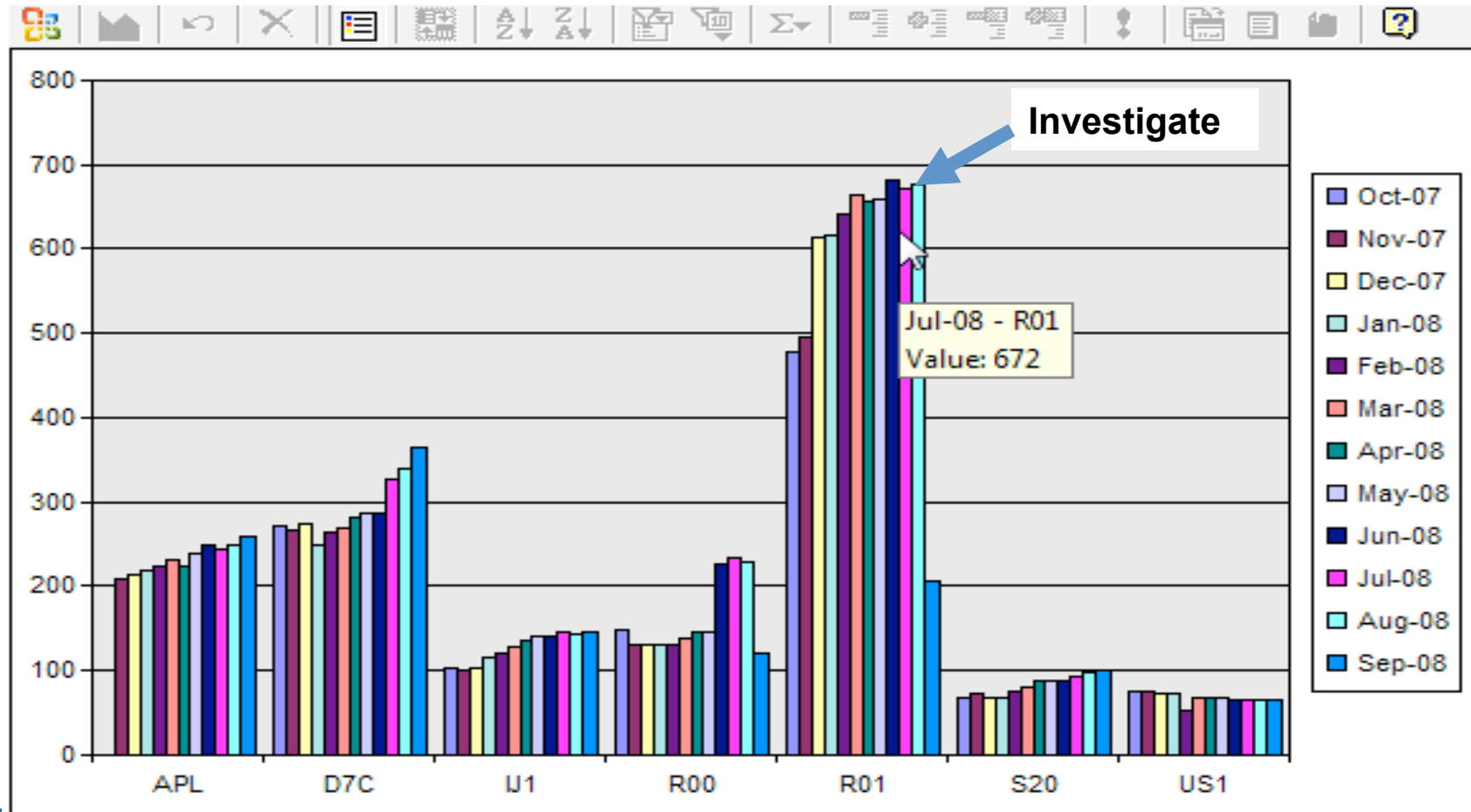
Job Scheduling – SM37 – Comparison Across systems – Detail report

	A	B	C	D	E	F	G	H	I	J	K
1	History for KRI:SM37										
2	System	_Oct-07	_Nov-07	_Dec-07	_Jan-08	_Feb-08	_Mar-08	_Apr-08	_May-08	_Jun-08	_Jul-08
3	APL	-	208	213	218	225	232	224	239	250	245
4	D7C	271	267	273	248	263	268	282	287	287	328
5	IJ1	103	100	102	115	121	129	136	141	142	147
6	R00	149	130	131	131	131	139	145	145	226	233
7	R01	478	495	614	617	642	664	656	660	682	672
8	S20	68	74	67	68	76	80	88	88	88	94
9	US1	75	75	74	73	52	67	67	67	66	65
10											
11											
12											

Sheet1

P2P Process Flow | Application Controls | KPI – Benchmarking
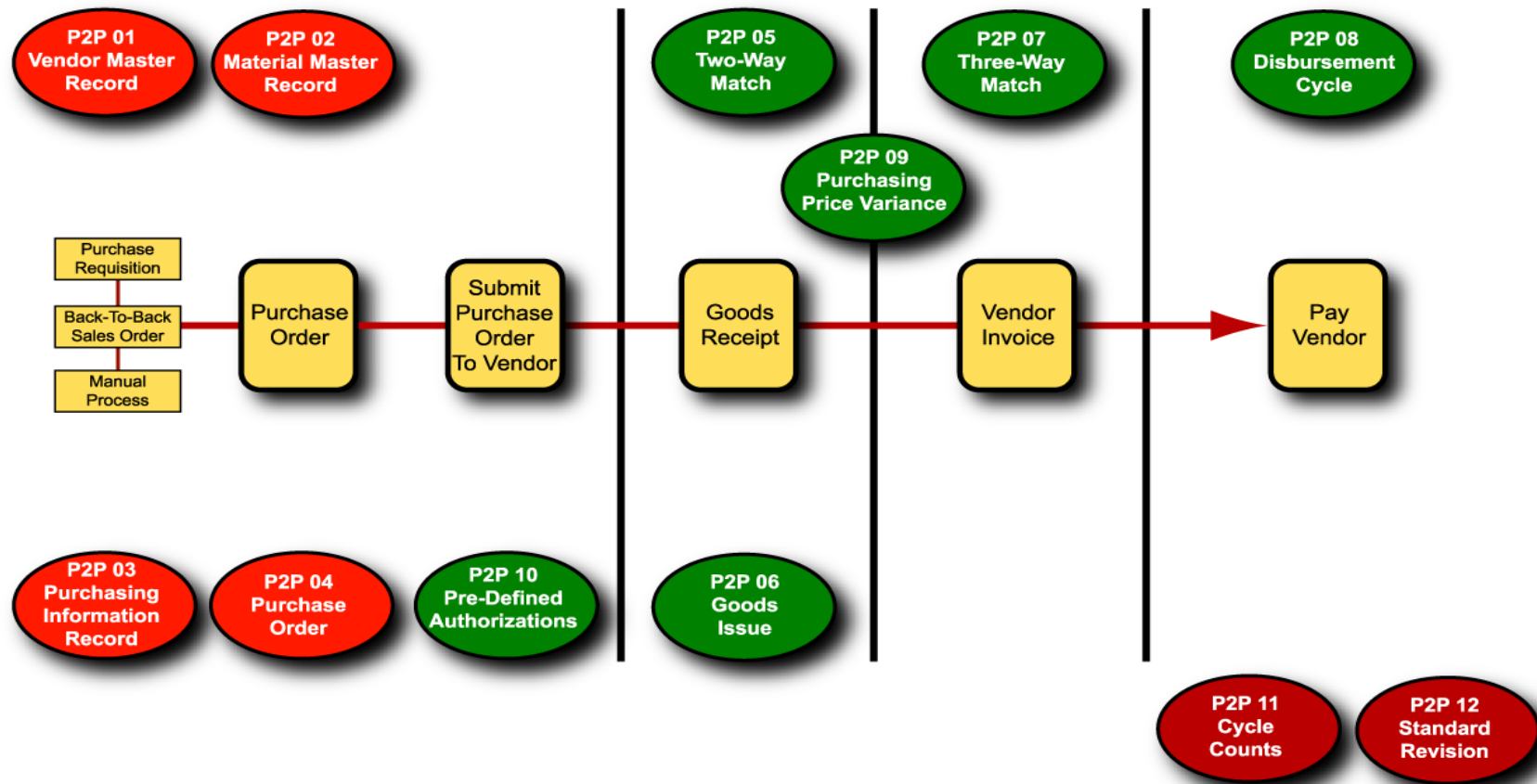
Standard Configuration	Chart of Accounts (T004)	#	27
	GL Account Groups (T077S)	#	235
P2P_01: Vendor Account Group	Vendor Account Groups (T077K)	#	34
	VAG Field Settings (T077V)	#	5848
P2P_02: Material Master Record Configuration	Material Types (T134)	#	41
	Valuation Classes (T025V)	#	34
	Material Groups (T023)	#	1123
	Qty./Val. Update (T134M)	#	5670
	MM Field Attributes (T130F)	#	1048
	MM Field Settings (T130V2)	#	10560
	Product Division (TSPA)	#	193
	Plant_Business Area Assignment (T134G)	#	7339
P2P_03: Field Selections (PIR)	Field Setting Groups for PIR (T162Y)	#	20
	Field Settings for PIR (T162V)	#	1225
	Field Sel. for Purch. Info Record (T162)	#	119
P2P_04: Back-to-Back Processing	PO Document Types (T161)	#	62
P2P_05/07: Standard GL Accounts(Two/Three-Way-Match)	GL accounts for Inventory Posting (BSX) (T030)	#	267
	GL accounts for Gain/loss from revaluation (UMB)	#	227
	GL accounts for Offsetting entry for inventory posting (GBB)	#	3425
	GL accounts for Cost (price) differences (PRD) (T030)	#	366
	GL accounts for GR/IR clearing account (WRX) (T030)	#	149
	GL accounts for Over-/Underpayment (ZDI) (T030)	#	55

P2P_08 Paying Company Codes (Disbursement Cycle)	Paying Company Codes (T042B)	#	48
P2P_08 Bank Determination (Disbursement Cycle)	Ranking Order (T042A)	#	252
	Bank Accounts (T042I)	#	239
	Available Amounts (T042D)	#	133
	Value Dates (T042V)	#	105
	Expenses_Charges (T042S)	#	60
P2P_10: PO Release Procedures	Release Indicators (T16FB)	#	3
	Release Codes (T16FC)	#	9
	Release Groups (T16FG)	#	4
	Release Strategies (T16FS)	#	20
	Role to Release Code (T16FW)	#	0
P2P_11: Cycle Count	Counting Cycles (T159C)	#	80
	Inventory Default Values (T335)	#	271
	Inventory Types per Storage Type (T331)	#	920
	Inventory Control Warehouse Number (T340D)	#	35
P2P_12: Cost Component Structure (Standard Revision)	Cost Component Structure (TCKH4)	#	3
P2P_12: Costing Types (Standard Revision)	Costing Types (TCK01)	#	29
P2P_12: Valuation Variants (Standard Revision)	Valuation Variants (TCK05)	#	18
P2P_12: Date Control (Standard Revision)	Date Control (TCK16)	#	8

P2P Application Controls | KPI – Benchmark Report

HP SAP Audit Information System (KPI)

HP Audit Information System - Application Controls - Benchmark Report

Documentation	
Data Entry	
Monthly KPI	
Start Load	
Reports	
SYSTEM HISTORY	
>Top5 basis trend	
>Users trend	
KRI HISTORY	
>Availability	
>Transports	
>Used Logins	
RATIO REPORTS	
>Rate of Change	
>Ratio Users:Profiles	
COMPLETE HISTORY	
User Roles	
PROFILE CHANGES	
USER CHANGES	
TRANSPORTS	
EMPLOYEE ACCOUNTS	
SOD CONFLICTS	
Application Controls	
Benchmark Report	
KPI Report	
Table Change Logs	
▪ **Login requests**	
▪ **HPSC SST incident requests**	
▪ **Email to tool support**	

Base Audit: SOX - P2P App Controls - Velocity - 2008 (2008068)

Base month and Base year are determined by date of last audit.

Base month:	12	Base year:	2007
Compare month:	September	Compare year:	2008

→ details   → exit page

Please select controls:

Procure-to-Pay Controls

- ☑ All controls
- ☐ Standard Configuration (00)
- ☐ Vendor Master (01)
- ☐ Material Master (02)
- ☐ Purchase Information Record (03)
- ☐ Lockbox Payments (04)
- ☐ 2-way match (05)

Benchmark Report – Base Month

unchanged
changed entries
new entries
unchanged
new entries
new entries

Changed/Unchanged/New Entries for Procure to Pay Controls

ISACA
Serving IT Governance Professionals
San Francisco Chapter

P2P Application Controls | KPI – Benchmark Report Details

	A1	▼	f_x	Benchmark report for Standard Configuration							

	A	B	C	D	E	F	G	H	I	J	K	L
86	**Comparison of Account Assignment Categories**											
87	**Mode**	**AcctAssCat**	Old Descript.	New Descript.	Old Consumpt.	New Consumpt.	Old Acct.chng.	New Acct.chng.	Old IR change.	New IR change.	Old GR	New GR
88					No Changes in Account Assignment Categories							
89	**Benchmark report for 3-way match**											
90	**Comparison of Standard Accounts**											
91	**Mode**	**Chrt/Accts**	**Trans.**	**Val.gp.cde**	**Acct modif**	**Val. Class**	Old G/L acct	New G/L acct	Old G/L acct	New G/L acct		
92	New	WFTP	WRX	US00		3700	-	2390019999	-	2390019999		
93	**Comparison of Delivery Complete Flag**											
94	**Mode**	**Plant**	Old Del. compl	New Del. compl								
95	New	6450	-	X								
96	**Comparison of Tolerance Limits**											
97	**Mode**	**CoCode**	**Tol. Key**	Old Val.	New Val.	Old Check	New Check	Old No check	New No check	Old Val.	New Val.	Old Check
98	New	US98	DQ	-	0.00	-	-	-	X	-	200.00	-
99	New	US98	LD	-	45.00	-	X	-	-	-	45.00	-
100	New	US98	PP	-	10000.00	-	X	-	-	-	10000.00	-
101	**Comparison of Duplicate Invoice Check**											
102	**Mode**	**CoCode**	Old PO text	New PO text	Old Auto. MAIL	New Auto. MAIL	Old Stoch.blk	New Stoch.blk	Old Check amnt	New Check amnt	Old Threshold	New Threshold
103	New	US98	-	-	-	-	-	X	-	X	-	0.00
104	**Comparison of Tax Codes**											
105	**Mode**	**CoCode**	Old Credit	New Credit	Old Debit	New Debit	Old Credit	New Credit	Old Debit	New Debit	Old Credit	New Credit
106	New	US98	-	-	-	-	-	-	-	-	-	-
107	**Comparison of Payment Blocks**											
108	**Mode**	**Pymt block**	Old TEXTL	New TEXTL	Old CHAR1	New CHAR1	Old Pmnts blck	New Pmnts blck	Old Not chgble	New Not chgble		
109					No Changes in Payment Blocks							
110	**Benchmark report for Disbursement Cycle**											
111	**Comparison of Standard Accounts**											
112	**Mode**	**Chrt/Accts**	**Trans.**	**Val.gp.cde**	**Acct modif**	**Val. Class**	Old G/L acct	New G/L acct	Old G/L acct	New G/L acct		
113					No Changes in Standard Accounts							
114	**Comparison of Payment Methods**											
115	**Mode**	**CoCode**	Old CoCd	New CoCd	Old ULSK1	New ULSK1	Old ULSK2	New ULSK2	Old ULSD1	New ULSD1	Old ULSD2	New ULSD2
116					No Changes in Payment Methods							
117	**Comparison of Ranking Order for automatic Payments**											

Sheet1 / Sheet2 / Sheet3

Three Way Match – Monitoring Account Configuration Changes
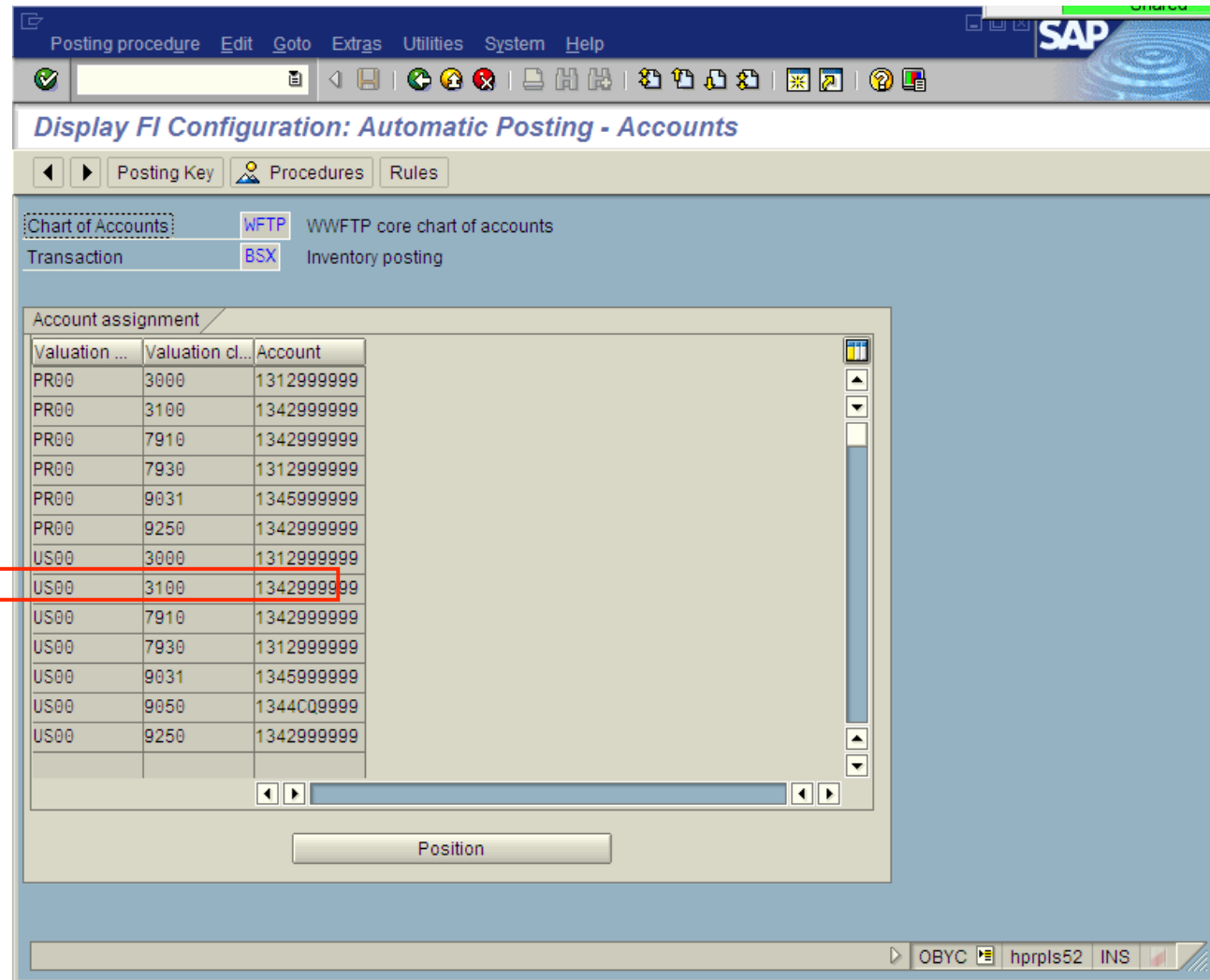
- Correctness and Accuracy of GL Account Postings –
  - Inventory Account
  - Accounts Payable Accrual Account
  - Cost (Price) Differences Account

- Examples of SAP configuration
  - Inventory Postings 'BSX' (Example: For company code US00, for transaction BSX used for inventory postings, valuation class 9031 , the old GL account 1345 changes to some other account)
  - Cost (price) differences 'PRD' (Example: For company code US00, for transaction PRD used for PPV postings, valuation class 3100 and no valuation modifier, the old GL account 3352 changes to some other account)
  - Accounts Payable Accrual 'WRX' (Example: For company code US00, for transaction WRX used for GRIR postings, valuation class 3100 , the old GL account 2390 changes to some other account)

- Impact of the Change
  These are standard accounts configured in SAP that are mapped to the General ledger. These changes will affect GL postings

- Change Category
  Critical

- Likelihood of the Change
  Infrequent

- Additional Procedures Need to assess the magnitude of the change, inquire about the reason for the change, and perform a business walkthrough –

Example: SAP Configuration – Inventory Postings Configuration for Chart of Accounts WFTP, Transaction Key BSX

KPI Monitoring Metrics Report – Inventory Postings Configuration for Chart of Accounts WFTP, Transaction Key BSX

Sys id:	Client:	Chart of Accounts:	Transaction Key:	Valuation group	Valuation Class:	G/L account number Debit:	G/L account number Credit:
D7C	300	WFTP	BSX	US00	3000	1312999999	1312999999
D7C	300	WFTP	BSX	US00	3100	1342999999	1342999999
D7C	300	WFTP	BSX	US00	7910	1342999999	1342999999
D7C	300	WFTP	BSX	US00	7930	1312999999	1312999999
D7C	300	WFTP	BSX	US00	9031	1345999999	1345999999
D7C	300	WFTP	BSX	US00	9050	1344CQ9999	1344CQ9999
D7C	300	WFTP	BSX	US00	9250	1342999999	1342999999

Baseline Sample   New Entries   Changed Entries
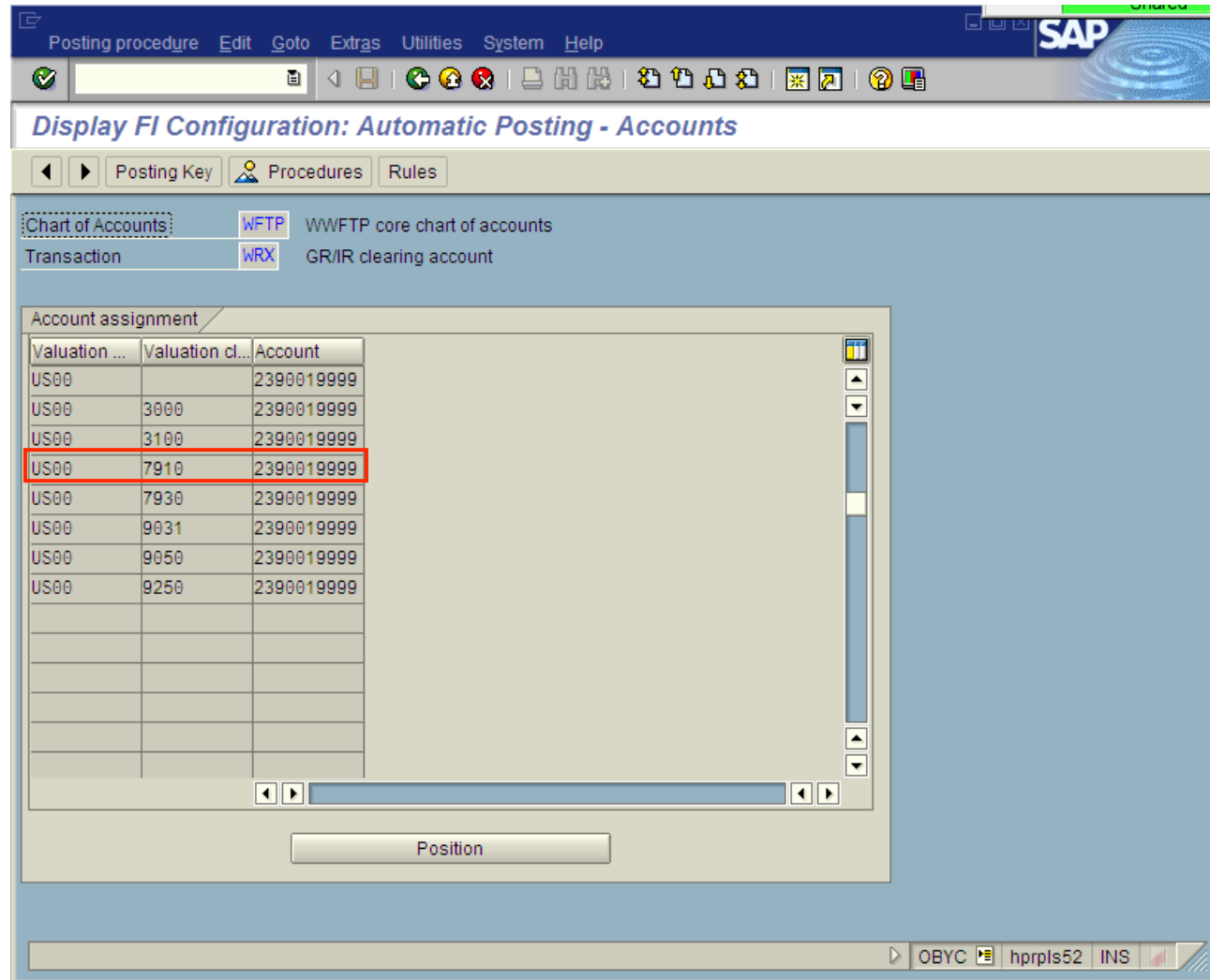
Example: SAP Configuration –Accounts Payable Accrual Postings Configuration for Chart of Accounts WFTP, Transaction Key WRX

SAP Configuration – GR/IR Postings Configuration for Chart of Accounts WFTP, Transaction Key WRX

Sys ID:	Client	Chart of Accounts :	Transaction Key:	Valuation group	Valuation Class:	G/L account number Debit:	G/L account number Credit:
D7C	300	WFTP	WRX	US00		2390019999	2390019999
D7C	300	WFTP	WRX	US00	3000	2390019999	2390019999
D7C	300	WFTP	WRX	US00	3100	2390019999	2390019999
D7C	300	WFTP	WRX	US00	3700	2390019999	2390019999
D7C	300	WFTP	WRX	US00	7910	2390019999	2390019999
D7C	300	WFTP	WRX	US00	7930	2470019999	2470019999
D7C	300	WFTP	WRX	US00	9031	2390019999	2390019999
D7C	300	WFTP	WRX	US00	9050	2390019999	2390019999
D7C	300	WFTP	WRX	US00	9250	2390019999	2390019999

Baseline Sample   New Entries   Changed Entries
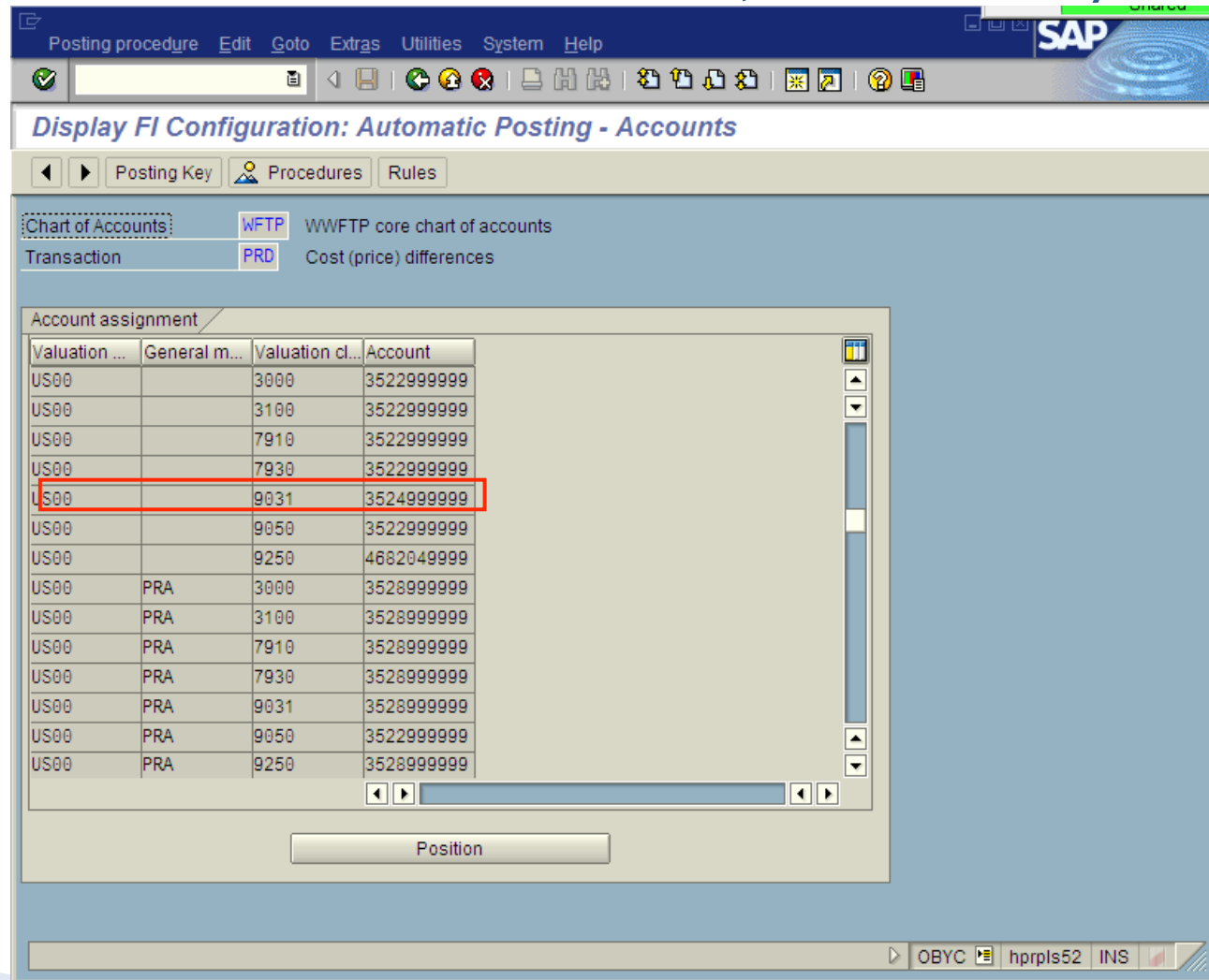
Example: SAP Configuration –Cost (Price) Variance Postings Configuration for Chart of Accounts WFTP, Transaction Key PRD

KPI Monitoring Metrics Report – Cost (Price) Variance Postings Configuration for Chart of Accounts WFTP, Transaction Key PRD

D7C	300	WFTP	PRD	US00		3000	3522999999	3522999999
D7C	300	WFTP	PRD	US00		3100	3522999999	3522999999
D7C	300	WFTP	PRD	US00		7910	3522999999	3522999999
D7C	300	WFTP	PRD	US00		7930	3522999999	3522999999
D7C	300	WFTP	PRD	US00		9031	3524999999	3524999999
D7C	300	WFTP	PRD	US00		9050	3522999999	3522999999
D7C	300	WFTP	PRD	US00		9250	4682049999	4682049999
D7C	300	WFTP	PRD	US00	PRA	3000	3522999999	3522999999
D7C	300	WFTP	PRD	US00	PRA	3100	3528999999	3528999999
D7C	300	WFTP	PRD	US00	PRA	7910	3528999999	3528999999
D7C	300	WFTP	PRD	US00	PRA	7930	3528999999	3528999999
D7C	300	WFTP	PRD	US00	PRA	9031	3528999999	3528999999
D7C	300	WFTP	PRD	US00	PRA	9050	3522999999	3522999999
D7C	300	WFTP	PRD	US00	PRA	9250	3528999999	3528999999

Baseline Sample   [yellow]   New Entries   [orange]   Changed Entries   [red]

Comparison with Baseline – Tolerance Limits

KPI SNAPSHOT VIEWER - VELOCITY P2P APPLICATION CONTROLS
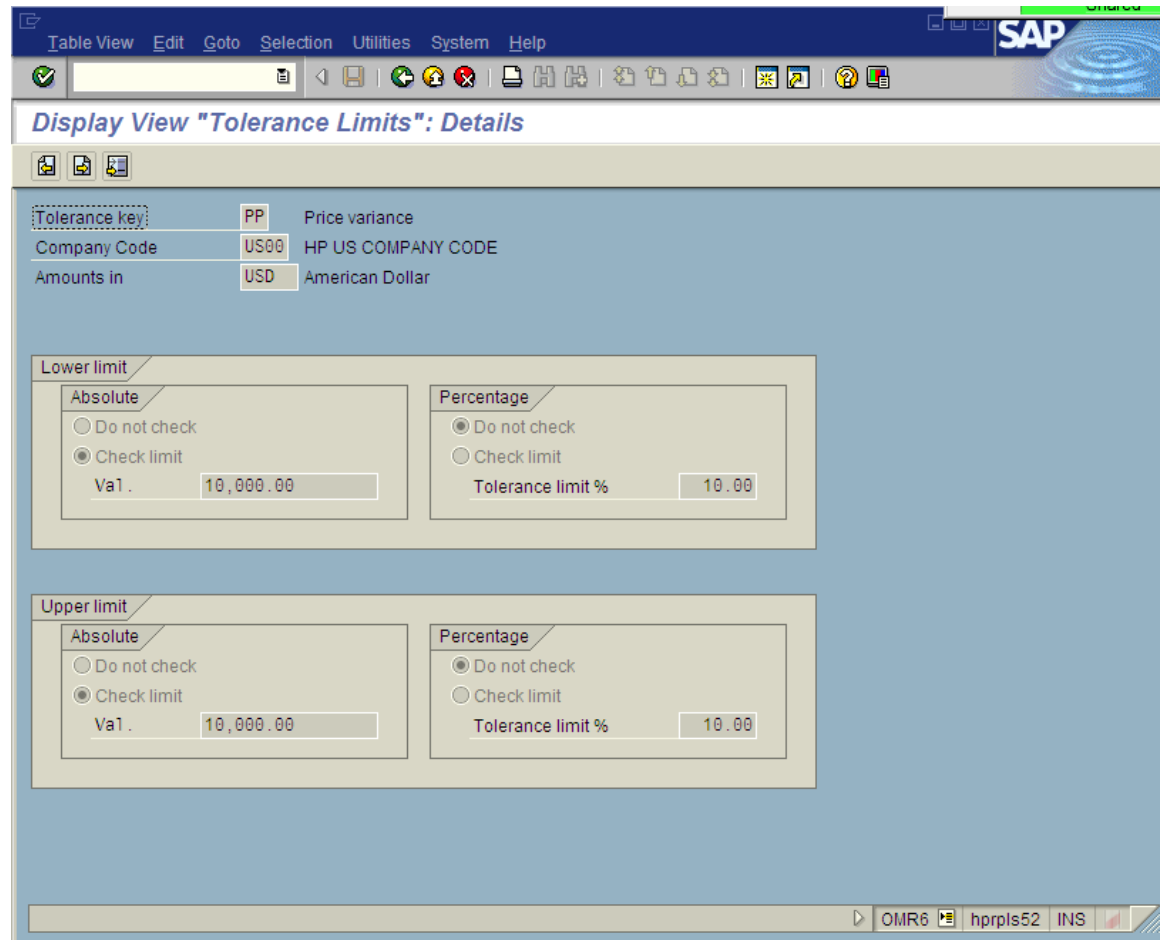
LOG ON TO KPI

Click on a process name for viewing the process flow and documentation for that process. Please note that the bullets below are collapsible. Under each area, you will find links for accessing configuration screenshots from the Dec 2007 audit and a link to the September 2008 KPI detail reports for comparison

- **Three Way Match - Account Configuration**
- **Disbursements to Vendors**
- **Three Way Match - Tolerance Settings**
  - ○ **Quantity Variance - DQ**
  - ○ **Price Variance - PP**
    - ■ Baseline - December 2007 Velocity Application Controls Audit - PP Tolerance Setting
    - ■ KPI Report - September 2008 - PP Tolerance Setting

      For company code US00, the upper and lower limit value for tolerance setting PP is 10000
  - ○ **Blanket PO Time Limit Exceeded - LD**
- **Standard Revision**
- **Goods Issue**
- **Material Master Data**
- **Vendor Master Data**
- **Chart of Accounts and related Configuration changes due to Version Upgrades**

Three Way Match – Tolerance Limits – Price Variance

Three Way Match – Tolerance Limits – Price Variance

Three Way Match – Tolerance Limits – Price Variance

Number of Company Codes Monitored for Invoice Price Variance
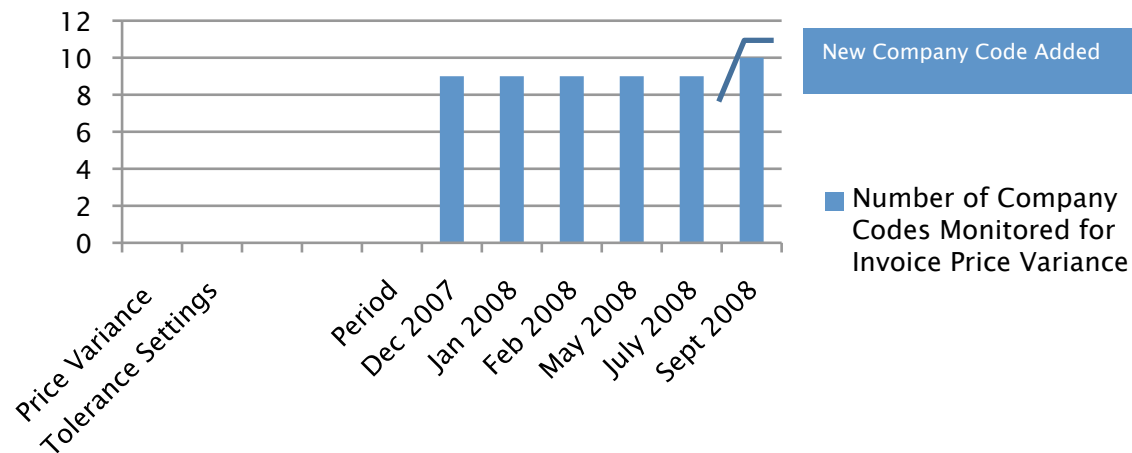
Mode	CoCode	Tol. Key	Old Val.	New Val.	Old Check	New Check
New	US98	DQ	-	200.00	-	X
New	US98	LD	-	45.00	-	X
New	US98	PP	-	10000.00	-	X

Comparison with Baseline – Disbursement Bank Accounts

KPI SNAPSHOT VIEWER - VELOCITY P2P APPLICATION CONTROLS

LOG ON TO KPI

Click on a process name for viewing the process flow and documentation for that process. Please note that the bullets below are collapsible. Under each area, you will find links for accessing configuration screenshots from the Dec 2007 audit and a link to the September 2008 KPI detail reports for comparison

- Three Way Match - Account Configuration
- Disbursements to Vendors
    - Bank Account / Sub Account Configuration
        - Baseline - December 2007 Velocity Application Controls Audit - Citibank SubAccount Configuration
        - KPI Report - September 2008 - Citibank SubAccount Configuration
    - Available Amounts for Disbursements Processing
    - Value Dates
    - Addition of New Bank Accounts
    - Addition of New Paying Company Codes
- Three Way Match - Tolerance Settings
- Standard Revision
- Goods Issue
- Material Master Data
- Vendor Master Data

For Paying Company Code US00, for ACH payments, payment method A, for Citibank CITDD account, the sub account is 1009009999

Disbursement Bank Account Configuration

Disbursement Bank Account Configuration

Benchmark Detail Report

	A139	▼	ƒx	Comparison of Standard Accounts							

	A	B	C	D	E	F	G	H	I	J	K	L
104	**Comparison of Payment Blocks**											
105	**Mode**	**Pymt block**	Old TEXTL	New TEXTL	Old CHAR1	New CHAR1	Old Pmnts blck	New Pmnts blck	Old Not chgble	New Not chgble		
106					No Changes in Payment Blocks							
107	**Benchmark report for Disbursement Cycle**											
108	**Comparison of Standard Accounts**											
109	**Mode**	**Chrt/Accts**	**Trans.**	**Val.gp.cde**	**Acct modif**	**Val. Class**	Old G/L acct	New G/L acct	Old G/L acct	New G/L acct		
110					No Changes in Standard Accounts							
111	**Comparison of Payment Methods**											
112	**Mode**	**CoCode**	Old CoCd	New CoCd	Old ULSK1	New ULSK1	Old ULSK2	New ULSK2	Old ULSD1	New ULSD1	Old ULSD2	New ULSD2
113					No Changes in Payment Methods							
114	**Comparison of Ranking Order for automatic Payments**											
115	**Mode**	**CoCd**	**Pmt method**	**Currency**		Old House bank	New House bank	Old House bank	New House bank	Old HKTIW	New HKTIW	
116					No Changes in Ranking Order for automatic Payments							
117	**Comparison of Paying Company Codes**											
118	**Mode**	**CoCd**	Old MINDS	New MINDS	Old MINDH	New MINDH	Old Pmt Advice	New Pmt Advice	Old ExRt diff.	New ExRt diff.	Old EFORN	New EFORN
119					No Changes in Paying Company Codes							
120	**Comparison of Available amounts for automatic Payments**											
121	**Mode**	**CoCode**	**House bank**	**Acct ID**	**Days**	**Currency**	Old BETRA	New BETRA	Old BETRE	New BETRE		
122					No Changes in Available amounts for automatic Payments							
123	**Comparison of Bank accounts for automatic Payments**											
124	**Mode**	**CoCd**	**House bank**	**Pmt method**	**Currency**		Old Acct ID	New Acct ID	Old UKONT	New UKONT	Old Clear.acct	New Clear.acct	Old Charge ind
125					No Changes in Bank accounts for automatic Payments							
126	**Comparison of Expenses_Charges for automatic Payments**											
127	**Mode**	**CoCd**	**Charge ind**		Old Currency	New Currency	Old SPES1	New SPES1	Old SPES2	New SPES2	Old BETRG_R	New BETRG_R
128					No Changes in Expenses_Charges for automatic Payments							
129	**Comparison of Value dates for automatic Payments**											
130	**Mode**	**CoCode**	**Pmt method**	**House bank**	**Acct ID**		Old Currency	New Currency	Old ANZTG	New ANZTG	Old BETRG_R	New BETRG_R
131					No Changes in Value dates for automatic Payments							
132	**Comparison of Payment Terms**											
133	**Mode**	**Pmnt terms**	**Day limit**		Old Explanatn	New Explanatn	Old ZFAEL	New ZFAEL	Old ZMONA	New ZMONA	Old ZTAG1	New ZTAG1	Old ZPRZ1
134					No Changes in Payment Terms							
135	**Comparison of Payment Blocks**											

In Summary

▸ Challenges
▸ Considerations for Implementation
▸ Opportunities
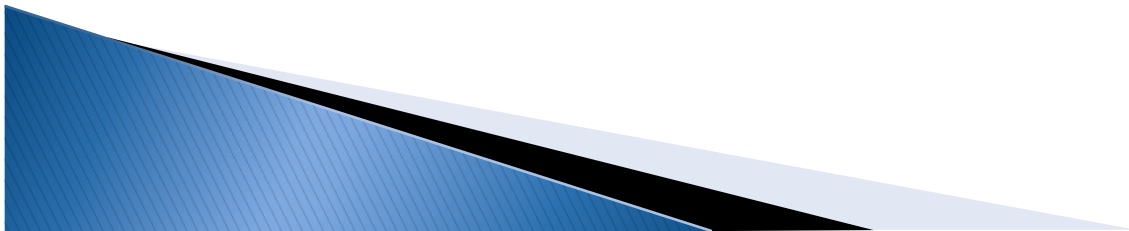
Challenges

▸ 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
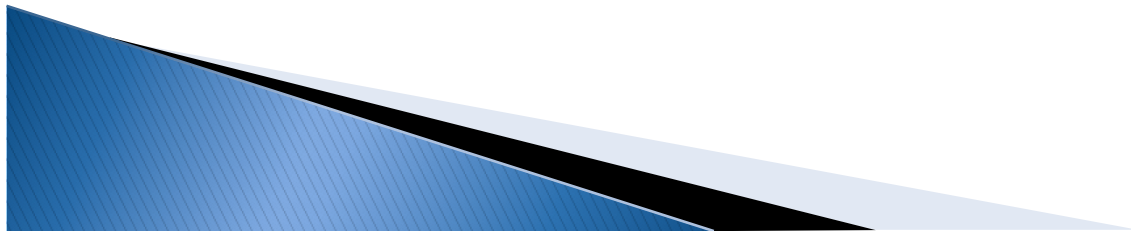
Opportunities

▸ 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.
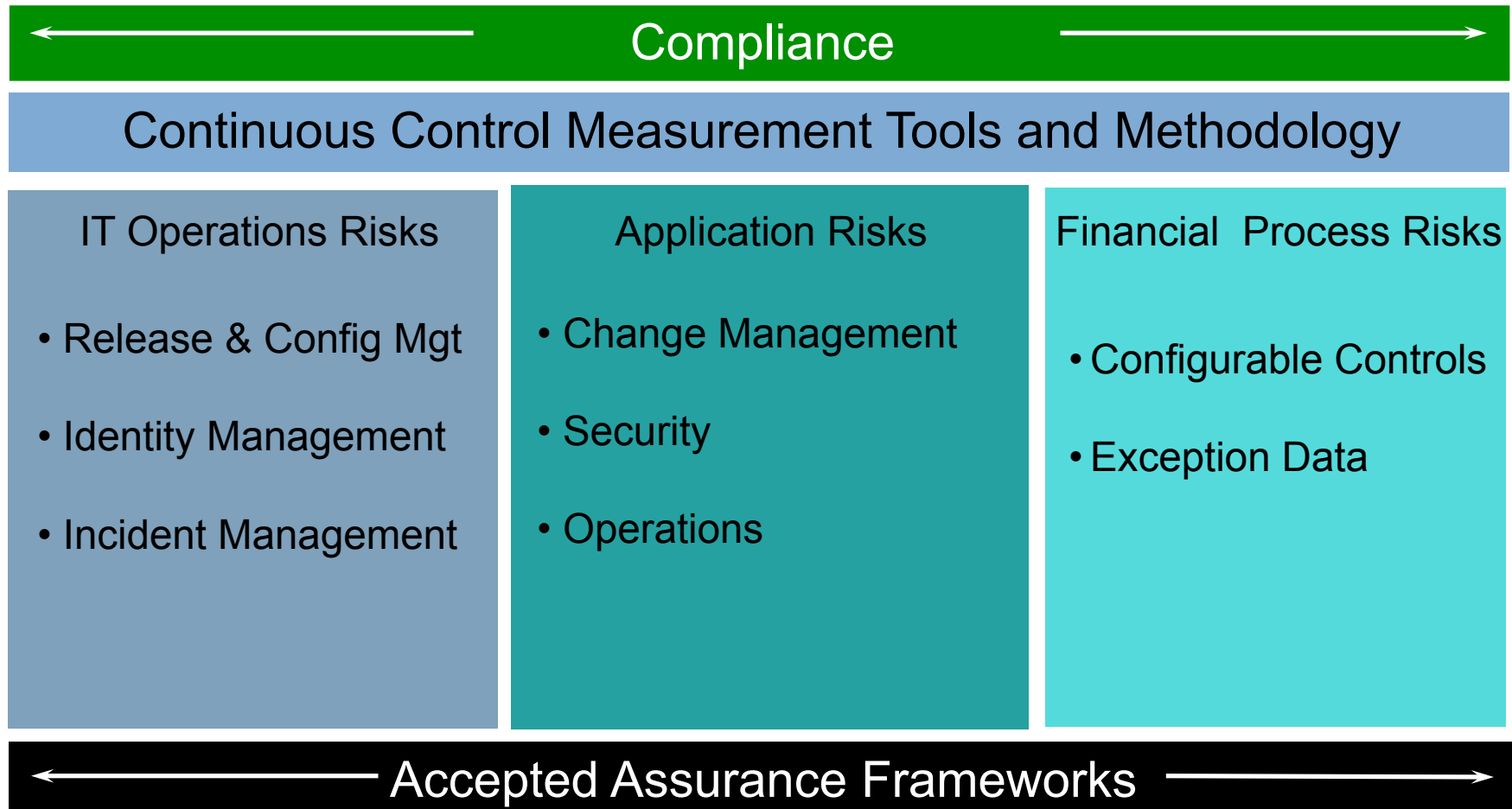
Questions and Collaboration

Vijay Venkatesh
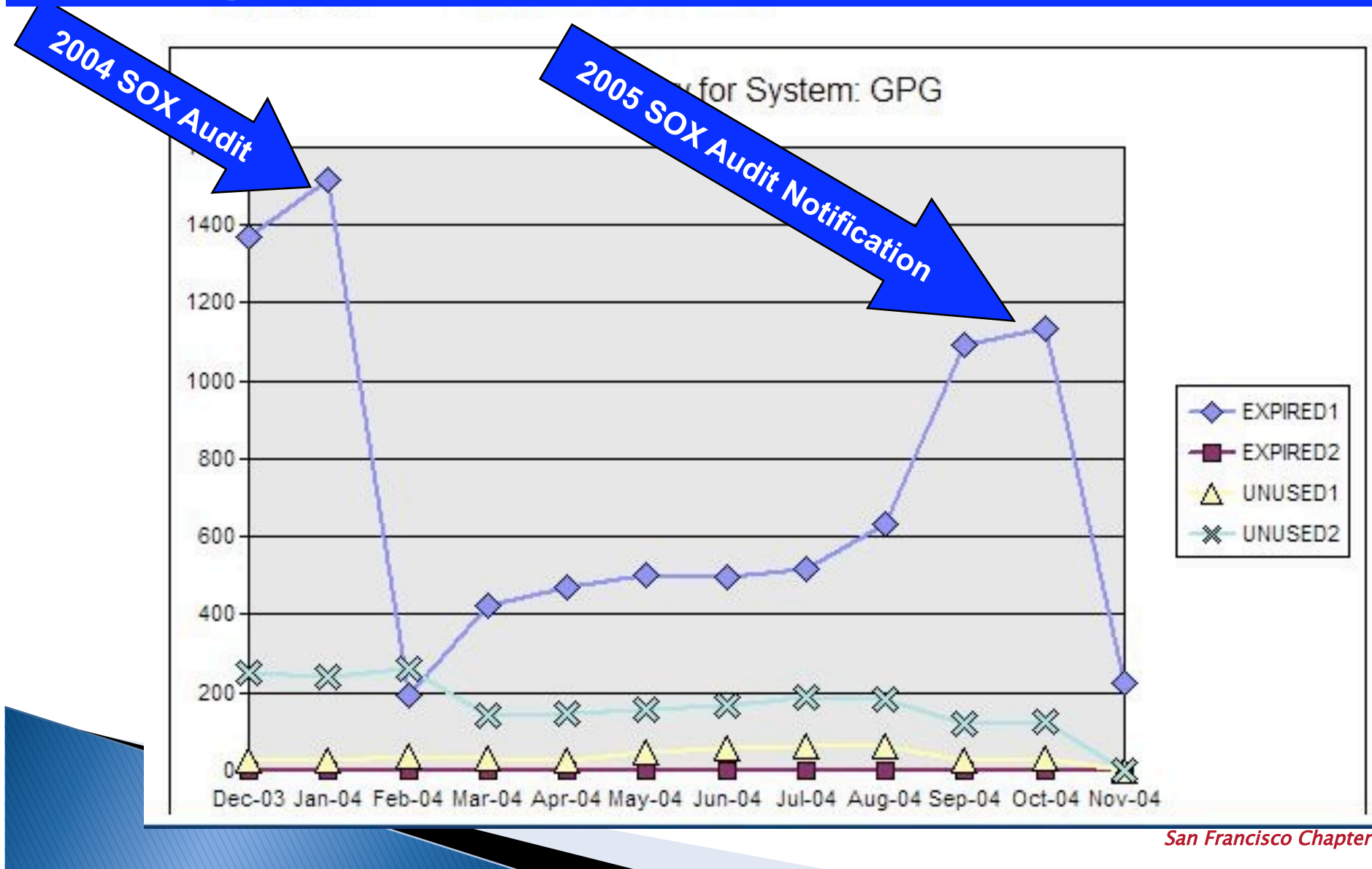Hewlett-Packard, IT Audit Lead
Vijay.Venkatesh@hp.com

Carrie Gilstrap
Hewlett-Packard, IT Audit Manager
Carrie.Gilstrap@hp.com

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

Alignment is the Key

Compliance

Continuous Control Measurement Tools and Methodology

IT Operations Risks	Application Risks	Financial Process Risks
• Release & Config Mgt	• Change Management	• Configurable Controls
• Identity Management	• Security	• Exception Data
• Incident Management	• Operations	

Accepted Assurance Frameworks

Measuring Inactive Users as a Leading Indicator of Security Effectiveness

San Francisco Chapter

Changes in IT Controls Affect Sustained Changes in Behavior

Trends in Revoking Access