Comité Latinoamericano de Auditoría Interna y Evaluación de Riesgos
CLAIN

Conferencias@Clain:

"Implementación del COSO 2013, lo bueno, lo malo y lo feo, caso Credicorp"

10 de diciembre, 2015

Sobre el conferencista

Jose Esposito Li-Carrillo
MA, CIA, CRMA, CRISC, AMLCA
Auditor Corporativo
Credicorp Ltd

Licenciado en Economía de la Universidad del Pacífico, Perú; Master en Economía con especialización en Econometría por la Universidad de Wisconsin, EE.UU.; CIA y CRMA por el IIA, CRISC por ISACA, (AML/CA) por Florida International University.

Ocupa el cargo de Auditor Corporativo de Credicorp Ltd. desde enero de 2010.

Profesor de la Maestría en Finanzas de la Escuela de Postgrado de la Universidad del Pacífico en Perú. Vice Presidente del Comité de Auditoría Interna de la Asociación de Bancos del Perú y Presidente del Comité Latinoamericano de Auditores Internos de FELABAN.

Disclaimer

Esta presentación y los comentarios brindados durante su exposición, son de entera responsabilidad del conferencista.

Credicorp Ltd ni sus subsidiarias se hacen responsables de las opiniones aquí vertidas.

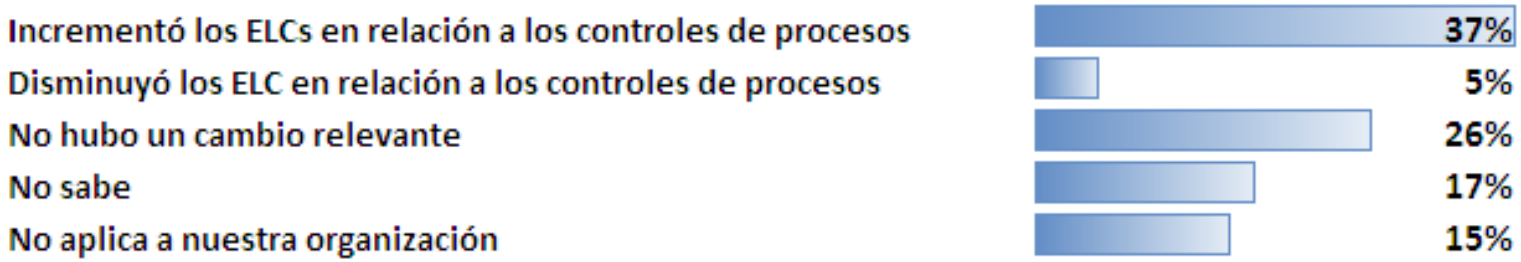
Agenda

- Primeros resultados del COSO 2013
- Credicorp y el Marco de Control Interno
- Cambios Metodológicos realizados a los procesos de evaluación de riesgos para aplicar COSO 2013
- Resultados y recomendaciones

Primeros resultados

Según Protiviti, de las casi 3,500 empresas que deben presentar información a SEC con año fiscal dic 2014; al 2 de abril 2015, solo el 18% reportó no haber adaptado el COSO 2013

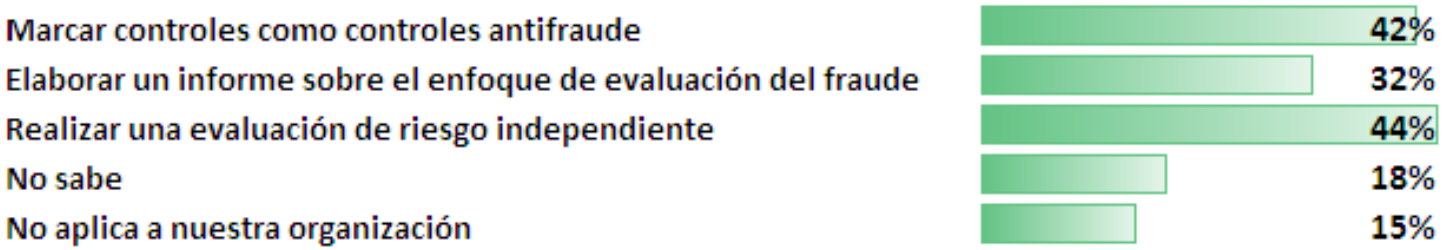
¿La implementación de COSO incrementó o disminuyó la proporción de controles a nivel entidad (ELCs) en relación cntroles a nivel proceso en su evaluación SOX?



Fuente.- Webinar Top Ten Lessons learned from Implementing COSO 2013, Protiviti, 29/4/2015

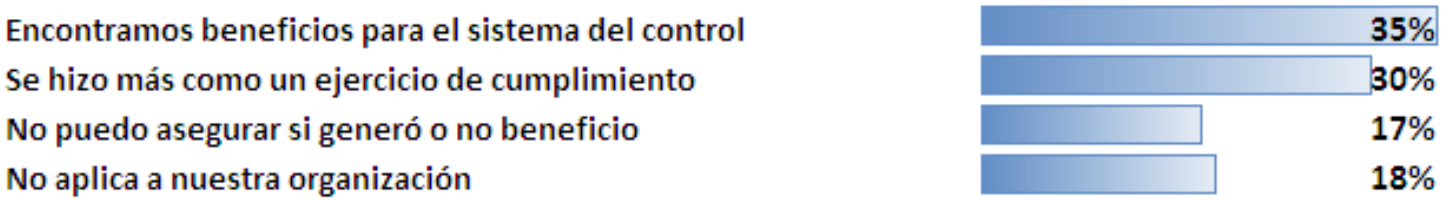
Primeros resultados

¿Qué nuevas actividades realizó en su evaluación del fraude para SOX?



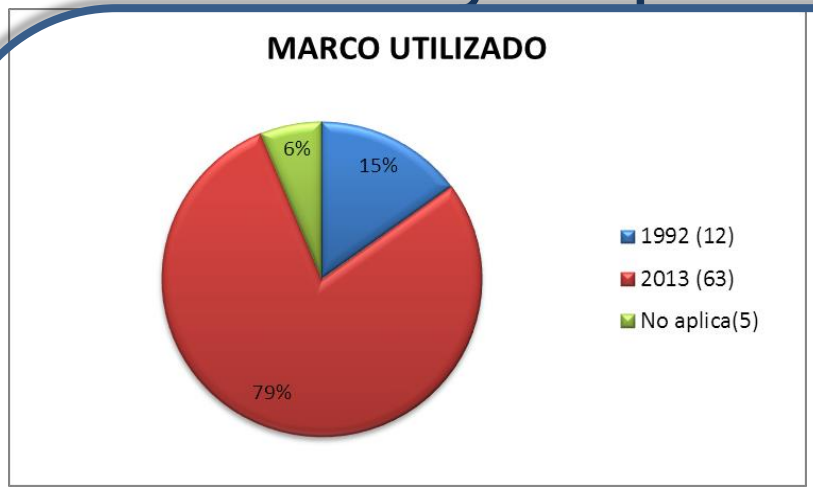
Fuente.- Webinar Top Ten Lessons learned from Implementing COSO 2013, Protiviti, 29/4/2015

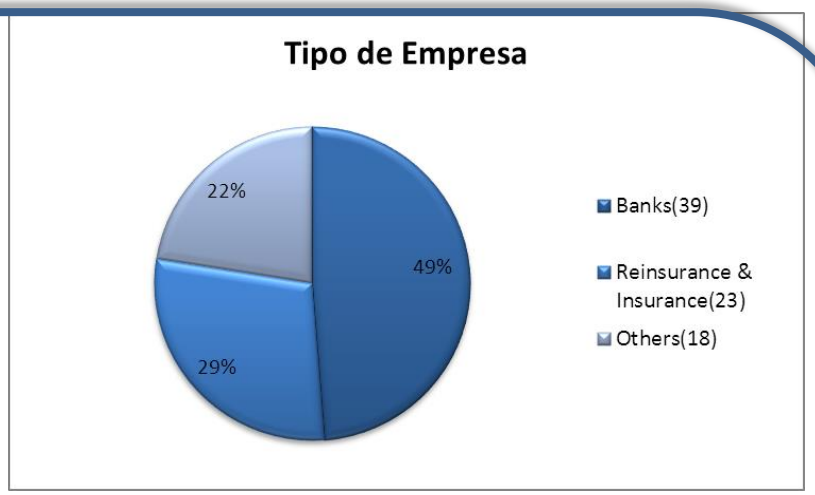
Al implementar COSO 2013 usted.....?

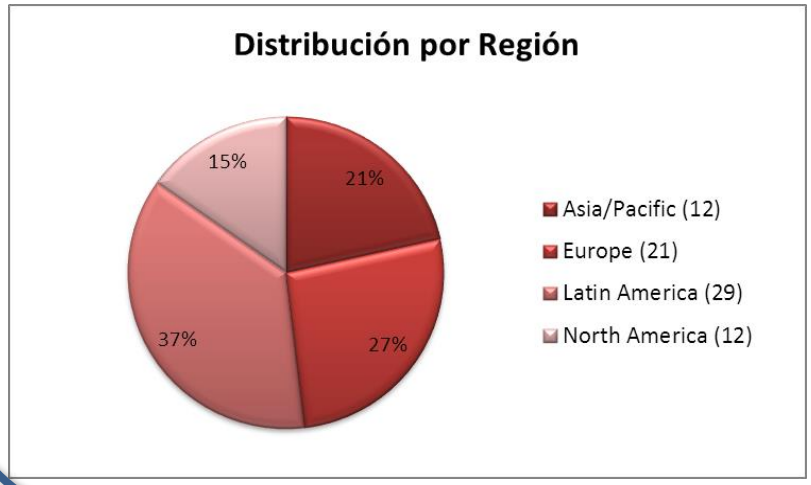


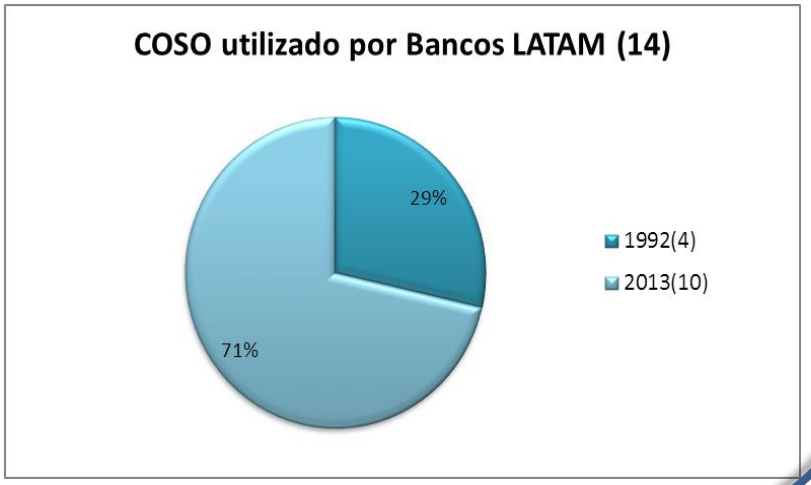
Fuente.- Webinar Highlights from Protiviti´s 2015 SOX Compliance Survey, 19/5/2015

COSO 2013 y empresas financieras no EEUU







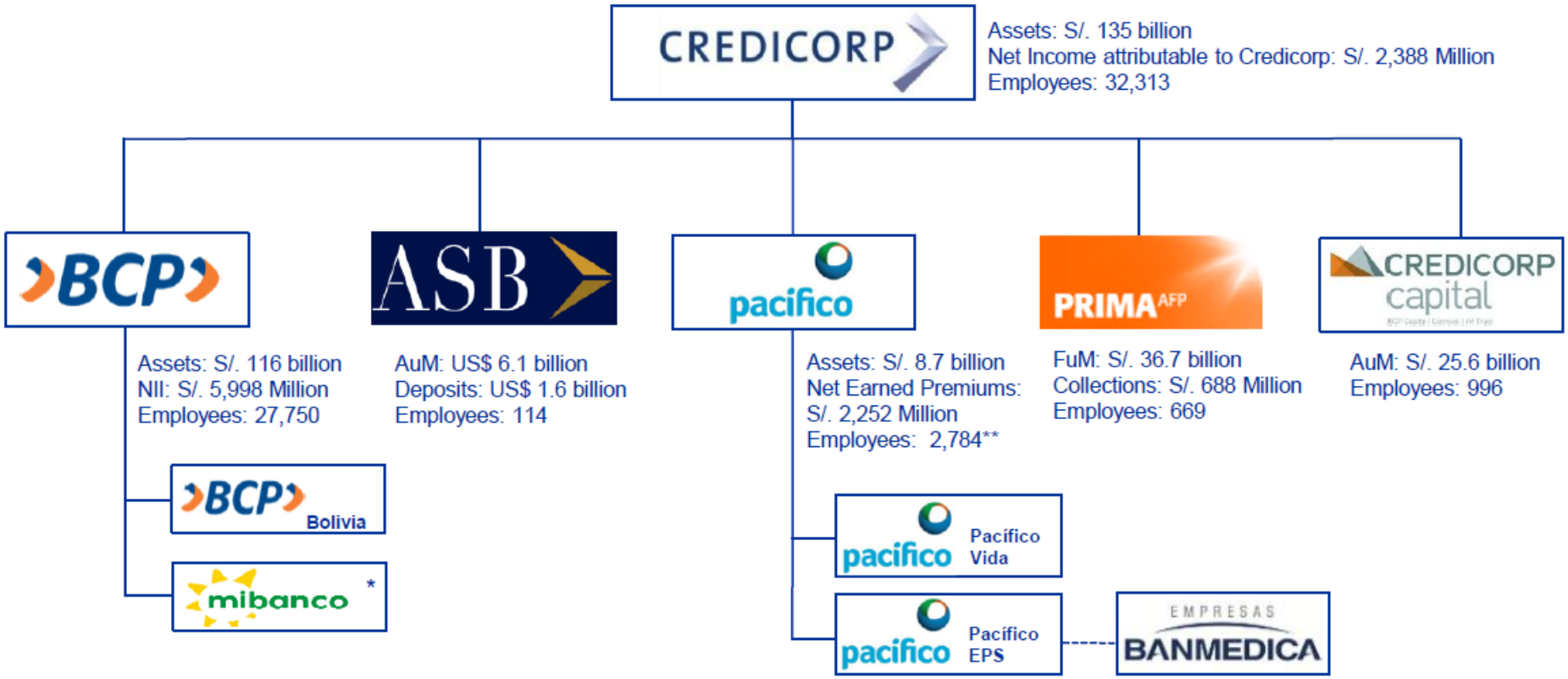


Fuente: Data del NYSE Connect 10-09-2015; elaboración propia

Agenda

- Primeros resultados del COSO 2013
- Credicorp y el Marco de Control Interno
- Cambios Metodológicos realizados a los procesos de evaluación de riesgos para aplicar COSO 2013
- Resultados y recomendaciones

Credicorp en cifras

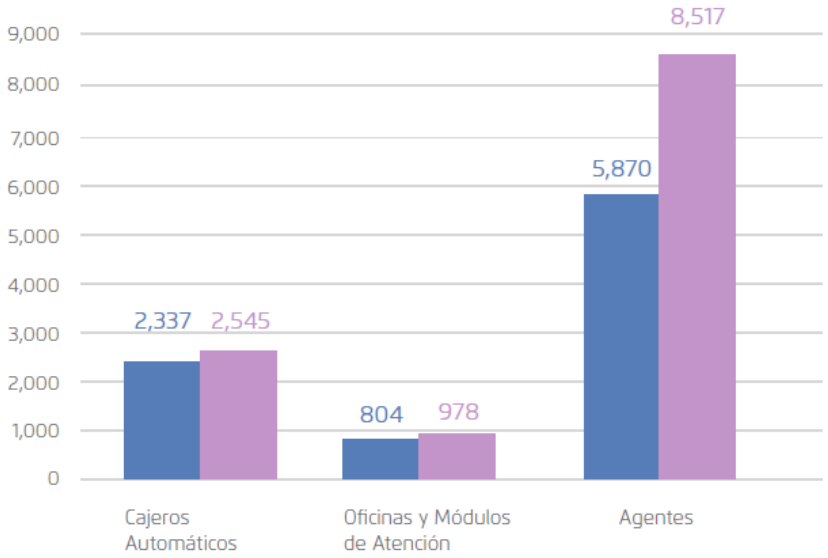


Canales de distribución

Canales de distribución de Credicorp

Puntos de contacto	2012	2013	2014
BCP consolidado	**8,358**	**8,844**	**11,873**
BCP	7,922	8,312	7,820
Edyficar	162	190	214
Mibanco	-	-	3,484
BCP Bolivia	274	342	355
Grupo Pacífico	**142**	**150**	**150**
Prima AFP	**17**	**17**	**17**
Credicorp	**8,517**	**9,011**	**12,040**

Canales de distribución de Credicorp (Unidades)



Marco de Control Interno en Credicorp

- El año 2006, Credicorp, como la mayoría de empresas que listan en NYSE decidió adoptar el COSO como marco de control interno
- Para SOX, “control interno efectivo” es: aquel sistema de control sobre el reporte financiero que ayuda a asegurar que las empresas produzcan estados financieros confiables, que puedan ser utilizados por los inversionistas al tomar decisiones (PCAOB).

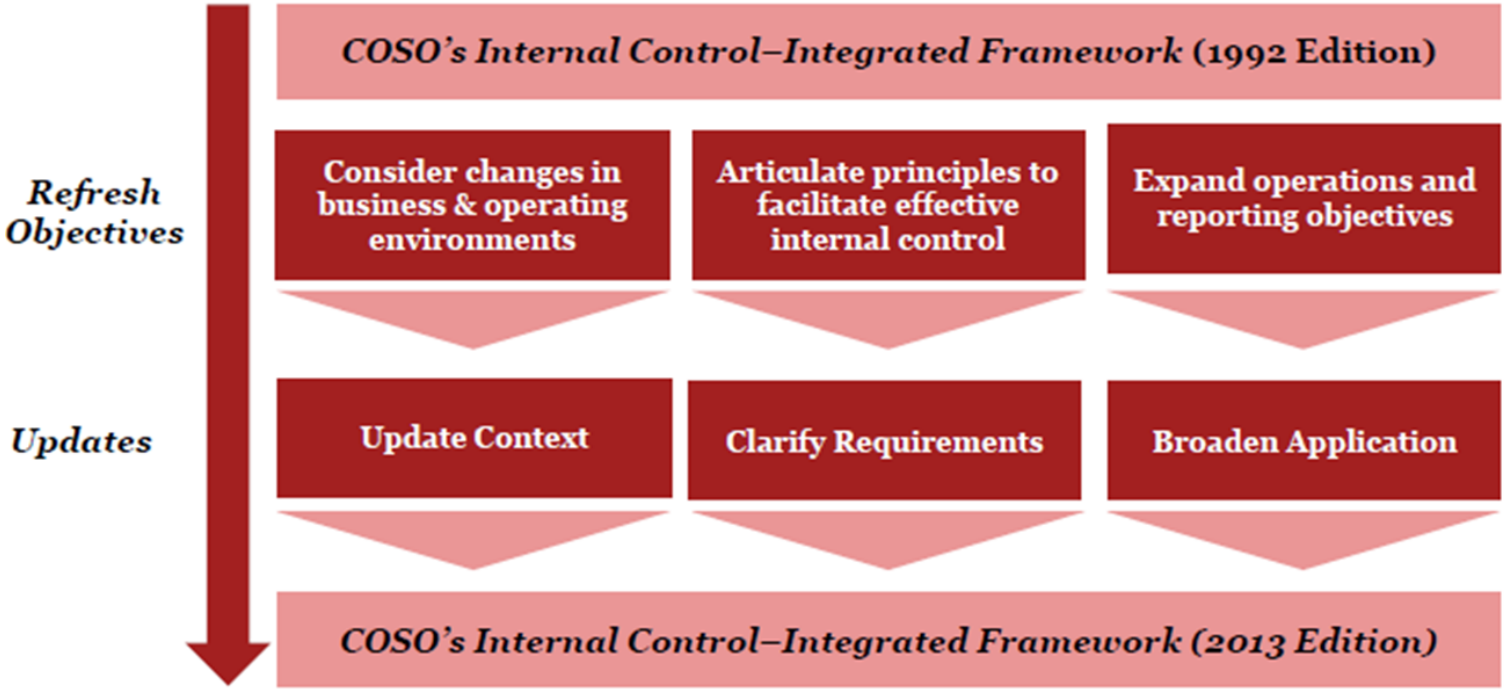
La Gerencia es responsable de mantener un sistema de control interno sobre el reporte financiero (“ICFR” por sus siglas en inglés) que provea una seguridad razonable respecto a la confiabilidad del reporte financiero y de la preparación de estados financieros para propósito externo de acuerdo a los principios de contabilidad generalmente aceptados. (SEC 17 CFR Part 241)

Según director del PCAO, el 5.2% de la muestra 2014, presentó opinión calificada Sobre el ICRF. http://pcaobus.org/News/Speech/Pages08102015_Franzel.aspx

COSO como marco de control

- Para ello se trabajó con un Big 4 quien ayudó a implementar la metodología para evaluar el *control interno* (Norma Credicorp 4205.010.02 Evaluación del Sistema de Control Interno):
  - **A nivel entidad**: se le encargó a Auditoría que prepara para la Gerencia un “cuestionario de control interno”
  - **A nivel proceso**: ARO y Procedimientos relevan los procesos y auditoría prueba controles clave
- COSO 2013 debía ser actualizado y formalizado antes del 15 de diciembre 2014, por ello Auditoría Interna se preparó:
  - Participando en foros, seminarios, webinars y cursos a nivel internacional (Asbanc, Felaban, IIA, Protiviti, PWC, EY, Deloitte, KPMG)
  - Coordinando con auditores externos locales sobre el modelo de implantación (EY y PWC), contando con su aprobación.

Por qué se ha actualizado el COSO?



Fuente.- PWC, Aligning your GCR solution to the updated COSO framework, webinar, enero 28, 2014

Qué **no** esta cambiando...

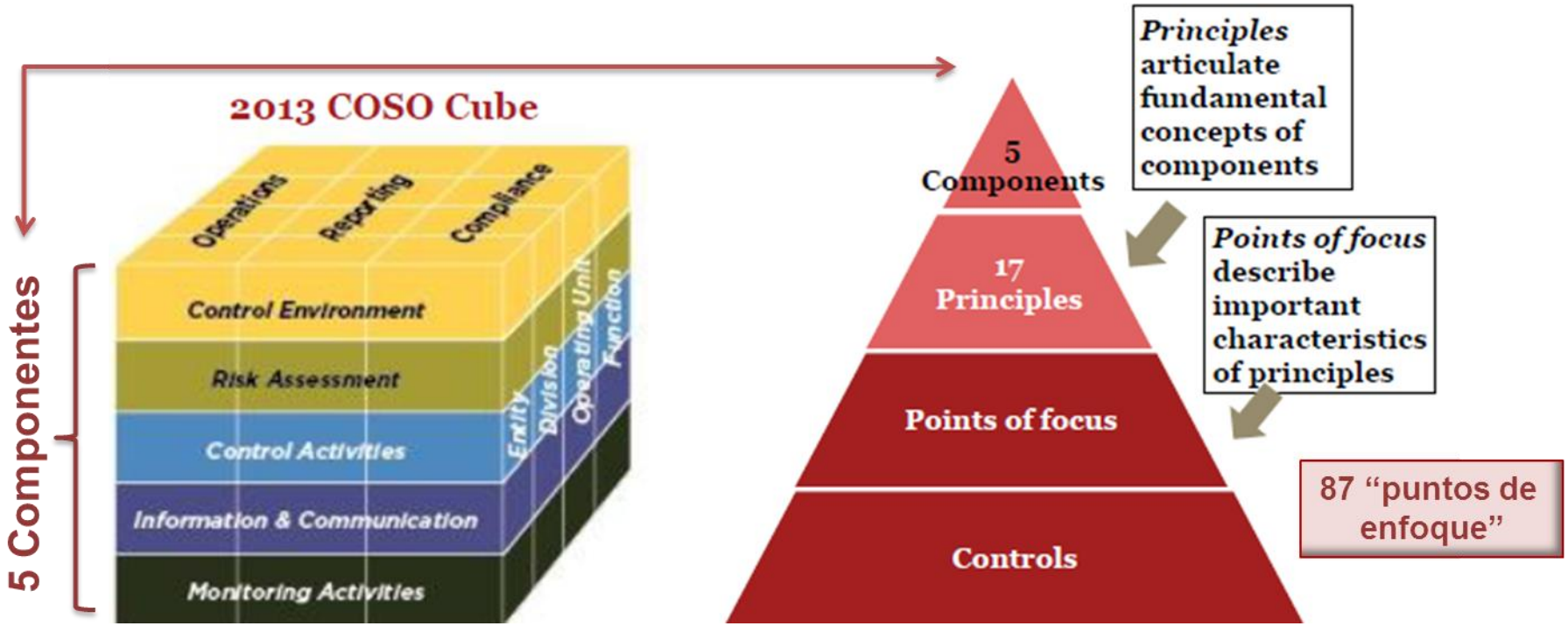
- La definición central de control interno
- Tres categorías de objetivos y 5 cinco componentes de control interno
- Cada uno de los cinco componentes de control interno son necesarios para que el control interno sea efectivo
- El rol significativo del juicio experto, en el diseño, implementación y conducción del control interno, y en la evaluación de su efectividad

Qué está cambiado...

- Se han considerado los cambios en el ambiente operativo y de negocios
- Se han expandido los objetivos de operaciones y reporte
- Los conceptos fundamentales que subyacen a los cinco componentes se articulan como “principios”
- Se han agregado ejemplos y propuestas adicionales relativos a operaciones, cumplimiento y reporte no financiero.

Fuente.- COSO, COSO & Project Overview, mayo 2013, traducción propia

Estructura del COSO 2013



Fuente.- PWC, Aligning your GCR solution to the updated COSO framework, webinar, enero 28, 2014

Ambiente de Control	1. Demuestra compromiso con la integridad y los valores éticos 2. El Directorio demuestra independencia y ejerce supervisión 3. La Gerencia establece la estructura, autoridades y responsabilidades 4. Demuestra compromiso a mantener individuos competentes 5. Mantiene individuos conscientes de su responsabilidad
Evaluación de Riesgos	6. Define sus objetivos con claridad 7. Identifica y analiza sus riesgos 8. Considera el fraude en la evaluación de riesgos 9. Identifica y evalúa los cambios significativos
Actividades de Control	10. Desarrolla actividades de control que mitigan los riesgos 11. Selecciona y desarrolla controles generales sobre los aplicativos 12. Despliega los controles a través de políticas y procedimientos
Información y Comunicación	13. Usa información relevante 14. Comunica internamente 15. Comunica externamente
Supervisión	16. Conduce evaluaciones continuas y por separado 17. Evalúa y comunica deficiencias oportunamente

Fuente.- PWC, IAI España, 2014

Efectividad del Control Interno

Un sistema efectivo de control interno requiere que:

- **Cada uno de los componentes y principios relevantes estén presentes y funcionando**
- **Los cinco componentes están operando junto de manera integrada**

Los componentes están presente y funcionando,

- Presente, los componentes y principios existen en el diseño e implementación del sistema de control interno para lograr determinados objetivos
- Funcionando, si existe evidencia que los componentes y principios continúan existiendo en el desarrollo normal del sistema de control interno
- En suma, “presente” se refiere al diseño e implementación, mientras que “funcionando” se refiere a la efectiva operación

Los componentes operan juntos cuando:

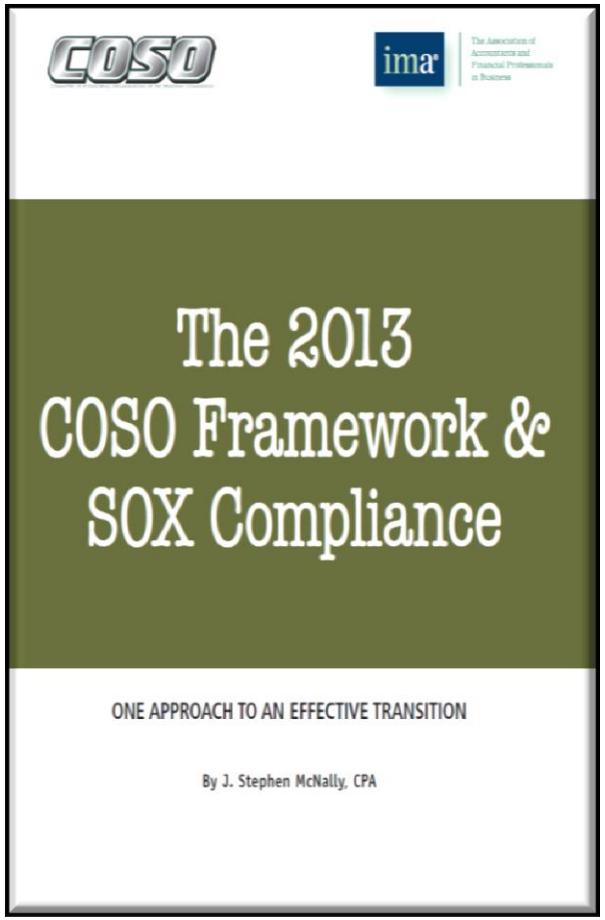
- Están presentes y funcionando
- La deficiencias de control interno agregadas entre los componentes no resultan en la existencia de una mayor deficiencia (*debilidad material*)

Agenda

- Primeros resultados del COSO 2013
- Credicorp y el Marco de Control Interno
- Cambios Metodológicos realizados a los procesos de evaluación de riesgos para aplicar COSO 2013
- Resultados y recomendaciones

5 pasos para el proceso de transición

1. Desarrollar sensibilización, *expertise* y alineamiento
2. Realizar una evaluación de impacto preliminar
3. Facilitar la sensibilización amplia (i.e. la organización), entrenamiento y evaluación integral
4. Desarrollar y ejecutar el plan de transición al COSO
5. Impulsar la mejora continua



http://www.coso.org
Protiviti: “COSO 2013-Getting started with implementation”

1. Desarrollar sensibilización, *expertise* y alineamiento

- Familiarizarse con el COSO 2013
- Reunirse con la Gerencia y discutirlo
- Proveer entrenamiento a todos los involucrados en el sistema de control
  - Quién entrena?
  - A quién?
  - Cómo?
  - Cuándo?
- Establecer un Plan para la transición:
  - Desarrollar un cronograma de transición
  - Designar roles y responsabilidades
  - Comunicar el Plan
- Reunirse con auditores externos para conocer sus expectativas
- Codificar (entender) los 17 principios
- Identificar los puntos de enfoque de cada principio

Actividades desarrolladas

Sensibilización 1

- Comprar el COSO (se agotó!) y traducirlo
- UAI: 0rganización de talleres de lectura y discusión (obligatorio)
- Intercambio de opiniones con Gerencias: CFO, CRO, Riesgo Operativo, Cumplimiento, Prevención de Fraudes, GdH
- Participación en todo foro sobre la materia
- Presentaciones al Consejo de Gerencia Credicorp (febrero) , Comité de Auditoría CA (febrero) y Directorio (marzo)
- Constante comunicación con el Presidente del CA
- Capacitación a segunda línea de defensa

Capacitación UAI

Sensibilización 1

Fecha	Lugar	Organizador	Tema
mayo 2013	Web	Deloitte	COSO 2013 Framework
julio 2013	Orlando	IIA	IIA International Conference
enero 2014	Web	PWC	SAP GRC Webcast: Solutions to COSO 2013
enero 2014	Web	PROTIVITI	Regulatory Hot Topics for the Financial Services Industry in 2014
Abril 2014	Web	PROTIVITI	COSO 2013: mapping controls to principles
mayo 2014	Buenos Aires	FELABAN	18th CLAIN
mayo 2014	Web	PROTIVITI	Highlights from Protiviti's 2014 SOX Compliance Survey
mayo 2014	Web	PROTIVITI	Keeping Pace with SOX Compliance
mayo 2014	Web	PROTIVITI - IMA	Improving Organizational Performance and Governance with COSO
mayo 2014	Web	PROTIVITI - IMA	COSO:What's New, What's Changed, Why Does it Matter and Other Frequently Asked Questions
junio 2014	Web	PROTIVITI	COSO 2013: Managing the Project for Success and IPO Readiness
junio 2014	Web	PROTIVITI-FEI	COSO 2013: The implications of IT Control
junio 2014	Web	Mc Gladrey	Simplify the complexity of third party management
junio 2014	Web	PROTIVITI-FEI	COSO 2013: Assessing Fraud Risk in ICEFR & Overall Implementation
julio 2014	London	IIA	IIA International Conference
agosto 2014	Web	IIA AEC	COSO 2013 Implementation – Are You Ready?
octubre 2015	Panama	ISACA	Latin CACS
octubre 2014	Web	IIA	Integrated Reporting: Understanding Today's Environment
noviembre 2014	Web	Deloitte	Implementing COSO: Insights to Help You Reach the Finish Line

Fichero de POFs

Sensibilización

1

Evaluación de Principios – Ambiente de Control
Principio 1: Compromiso con la Integridad y los Valores Éticos
Puntos de Enfoque
• **Establecimiento del "Tone at the Top" en la organización?**– ¿Cómo la Gerencia y el Directorio demuestran la importancia de la integridad y de los valores éticos a la hora de apoyar el funcionamiento del Sistema de Control Interno? - **Revisar códigos de ética, instrucciones, acciones y comportamiento pasados que evidencien el comportamiento de la Alta Dirección. (por ejemplo mensajes por intranet, envío de afiches, diagramas, etc.).**
• **Definición de estándares de conducta** – ¿Se encuentran adecuadamente plasmadas las expectativas del Directorio y la Gerencia en la relación con la integridad y los valores éticos dentro de las normas de conducta de la entidad?, ¿Cómo se asegura que las normas de conducta sean adecuadamente comunicadas a todos los niveles de la organización, así como a proveedores, socios comerciales y otros stakeholders? - **Verificar mediante la revisión de papeles de trabajo de la organización como se aseguró que se incluyan las expectativas del Directorio y la Gerencia en relación con integridad y valores éticos - Revisar mediante que canales se da a conocer las normas de conducta a través de la entidad y a otros stakeholders - Verificar cómo se asegura que el personal y otros stakeholders revise las normas de conducta. (por ejemplo firmando cartas o cargos de compromiso, fichas, etc.).**
• **Evaluación de la adeherencia a los estándares de conducta** – ¿Qué procesos se han establecido para evaluar si el personal actúa en base a las normas de conducta establecidas? - **Indagar con las Áreas encargadas cuales son los procedimientos que se han establecido para evaluar si el personal da cumplimiento a las normas de conducta - Verificar que la Gerencia de Desarrollo Humano (u otra Gerencia encargada) haya establecido mecanismos que permitan reflejar los incumplimientos a las normas de conducta dentro de las decisiones de compensación variable**
• **Gestión de las desviaciones oportunamente** – ¿Qué procedimientos se han establecido para identificar comportamientos que se consideren desviaciones a las normas de conducta? - **Solicitar las Actas del Comité de Ética Credicorp e identificar si los procedimientos establecidos para ese fin se realizan de forma oportuna y sistemática - Identificar y evaluar si se está gestionando adecuadamente el Sistema de Denuncia Credicorp a través del proveedor y las gerencias involucradas en su administración. Evaluar los reportes al Comité de Auditoría**
Ejemplo de Control relacionado con el Principio

Perdón, es confidencial !!!!!

CREDICORP

2. Realizar una evaluación de impacto preliminar

- La principal conclusión de esta etapa seguramente será su percepción de qué tan bien aplicó COSO 1992!!!!!
- Realizar la evaluación preliminar: mapear los controles a los principios y obtener conclusión preliminar sobre:
  - ✓ Si el diseño de los controles documentados es efectivo
  - ✓ Si se he determinado que los controles operan de manera efectiva, ello permitiría a la Gerencia a concluir que los principios están “presentes y funcionando”
  - ✓ Diagnosticar brechas y documentarlas
  - ✓ Sobre ellas, **planificar acciones** para el 2014
- Reunirse nuevamente con auditores externos para revisar resultados

Actividades desarrolladas

Evaluación Preliminar 2

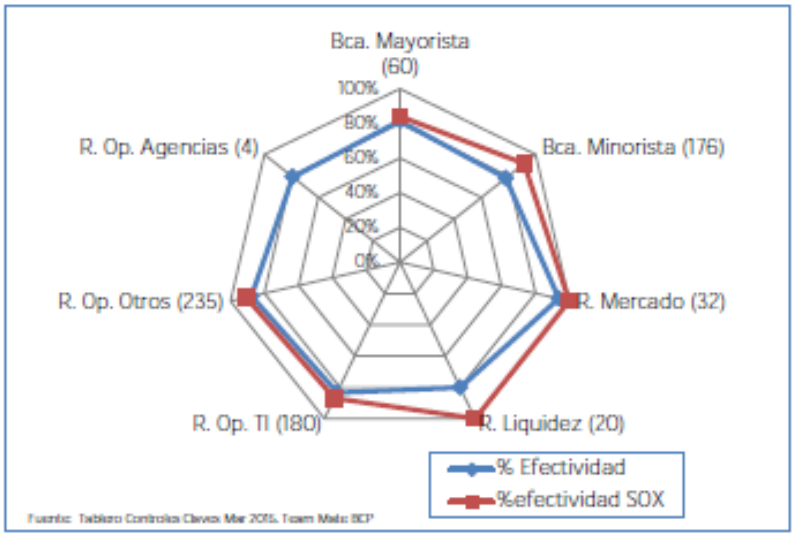
- Se estableció equipo de trabajo, patrocinado por CFO, liderado por AI:
  - Expertos de Riesgos
  - Cumplimiento
  - Prevención de Fraude
  - Contabilidad
- Se estableció un plan de trabajo para evaluar brechas de manera inmediata y se comunicó a la Alta Gerencia
  - En paralelo, las subsidiarias hacían lo mismo
- Por un tema de coyuntura el DEA patrocinó el proceso
- Se coordinó enfoque con los 2 auditores externos

Actividades desarrolladas

Evaluación Preliminar 2

- Enfoque utilizado: controles clave SOX a principios (Protiviti- 5 pasos)
- Se formaron 5 equipos especializados, incluyendo especialistas para componentes adhoc (ej. fraude)
- Los resultados fueron re-evaluados “peer review”
- No se encontraron brechas significativas pero sí oportunidades de mejora
  - Relevar mejor
  - Nuevos controles (de 196 a 233)
- Nuevas reuniones con auditores externos

I. Análisis Efectividad por Tipo de Riesgo



Conforme a la metodología propuesta por COSO (Illustrative Tools for Assesing Efectiveness of a System of Internal Control, COSO 2013) y Protiviti (“COSO 2013-Getting started with implementation” (2013, Protiviti): 5 PASOS

1. Se revisó y amplió la matriz de riesgos y controles de los procesos del banco (Anexo 12 del Manual de Auditoría) incorporando los siguientes conceptos:
   - Objetivo operativo del proceso
   - Principios que afectan a los controles
   - Observaciones relacionadas a los principios afectados



	SISTEMA DE CONTROL INTERNO											
	Evaluación de Riesgos				Actividades de Control			Información y Comunicación			Seguimiento y Monitoreo	
Descripción del Control	6. Define sus objetivos con claridad	7. Identifica y analiza sus riesgos	8. Considera el fraude en la evaluación de riesgos	9. Identifica y evalúa los cambios significativos	10. Desarrolla actividades de control que mitigan los riesgos	11. Selecciona y desarrolla controles generales sobre los aplicativos	12. Despliega los controles a través de políticas y procedi-mientos	13. Usa información relevante	14. Comunica internamente	15. Comunica externamente	16.Conduce evaluacio-nes continuas y por separado	17.Evalúa y comunica deficiencias oportuna-mente
Cumple con el Principio("X")	0	3	23	4	180	85	178	175	69	24	62	49
No Cumple con el Principio ("N")	0	1	0	0	7	3	7	5	1	0	0	1

2. Se analizaron los 196 Controles Claves SOX y sus 35 procesos relacionados probados el 2013 para identificar cómo los controles afectan a los principios y encontrar posibles brechas (principios que no son evaluados por controles).

Estos 196 controles se distribuyen por tipo de riesgo y por procesos:

Por Proceso

Por Tipo de Riesgo

Tipo de Riesgo	N° Procesos	%	N° de Controles	%
Riesgo Operacional - Otros	10	29%	85	43%
Riesgo Operacional TI	10	29%	55	28%
Riesgo de Mercado	4	11%	20	10%
Riesgo de Crédito Bca. Mayorista	4	11%	18	9%
Riesgo de Crédito Bca. Minorista	6	17%	17	9%
Riesgo Operacional - Agencias	1	3%	1	1%
Total:	35	100%	196	100%

Tipo de Riesgo	Proyecto	N° de Controles
Riesgo de Crédito Bca. Mayorista	Arrendamiento Financiero	8
Riesgo de Crédito Bca. Mayorista	COMEX	6
Riesgo de Crédito Bca. Mayorista	Créditos Comerciales	1
Riesgo de Crédito Bca. Mayorista	Sistema de Evaluación de la Clasificación del Deudor yCálculo de Provisiones	3
Riesgo de Crédito Bca. Minorista	Cálculo de Intereses de Tarjeta de Crédito	4
Riesgo de Crédito Bca. Minorista	Créditos de Consumo	2
Riesgo de Crédito Bca. Minorista	Créditos Hipotecarios	4
Riesgo de Crédito Bca. Minorista	Ejecución del Presupuesto de Gastos de Marketing	2
Riesgo de Crédito Bca. Minorista	Gestión de Efectivo	1
Riesgo de Crédito Bca. Minorista	Tarjeta de Crédito	4
Riesgo de Mercado	Emisión de Valores Credicorp locales yel Extranjero	4
Riesgo de Mercado	Evaluación a la Gestión de Instrumentos Financieros Derivados	8
Riesgo de Mercado	Gestión de Inversiones - Administración de Cartera Propia	6
Riesgo de Mercado	Gestión de Tesorería: Adeudados, Cambios yRiesgo Cambiario (inc. Negocios Internacionales)	2
Riesgo Operacional - Agencias	Oficina Panamá	1
Riesgo Operacional - Otros	Activo Fijo	1
Riesgo Operacional - Otros	Administración del Riesgo Operativo	1
Riesgo Operacional - Otros	Cierre Contable - BCP	59
Riesgo Operacional - Otros	Depósitos	8
Riesgo Operacional - Otros	Evaluación del Sistema de Control Interno de los Bienes Adjudicados	1
Riesgo Operacional - Otros	Evaluación del Sistema de Control Interno en el Proceso de Conciliaciones de Cuentas con Banqueros Nacionales ydel Exterior	1
Riesgo Operacional - Otros	Gestión del Riesgo Cambiario Crediticio	1
Riesgo Operacional - Otros	Inversión en Software	5
Riesgo Operacional - Otros	Proceso de aprobación de Nuevos Productos, procesos ycanales	1
Riesgo Operacional - Otros	Transferencias delal Exterior yRemesas Migratorias	7
Riesgo Operacional TI	Cálculo de Intereses de Depósitos	5
Riesgo Operacional TI	Canal Agente BCP	2
Riesgo Operacional TI	Contratación de Servicios	1
Riesgo Operacional TI	Control de Accesos	1
Riesgo Operacional TI	Evaluación de Seguridad de la Red	9
Riesgo Operacional TI	Mantenimiento de la Infraestructura de Tecnología de Información	3
Riesgo Operacional TI	Proceso de Atención de Requerimientos	9
Riesgo Operacional TI	Proceso de Tecnología de Control de Accesos.	16
Riesgo Operacional TI	Proceso de Tecnología de Información de Continuidad de Servicios	6
Riesgo Operacional TI	Validación del Calculo de Intereses de Créditos Comerciales Vencidos	9
	Total:	196

3. Preliminarmente se determinaron qué principios se cumplían a través de controles en procesos y cuáles a través de controles a nivel entidad.

Componente COSO	Principios	N° controles relacionados con el Principio	Principio presente y funcionando
Ambiente de Control	1. Demuestra compromiso con la integridad y los valores éticos	0	🟡
	2. El Directorio demuestra independencia y ejerce supervisión	0	🟡
	3. La Gerencia establece la estructura, autoridades y responsabilidades	0	🟡
	4. Demuestra compromiso a mantener individuos competentes	0	🟡
	5. Mantiene individuos concientes de su responsabilidad	0	🟡
Evaluación de Riesgos	6. Define sus objetivos con claridad	0	🟡
	7. Identifica y analiza sus riesgos	3	🟢
	8. Considera el fraude en la evaluación de riesgos	23	🟢
	9. Identifica y evalúa los cambios significativos	4	🟢
Actividades de Control	10. Desarrolla actividades de control que mitigan los riesgos	180	🟢
	11. Selecciona y desarrolla controles generales sobre los aplicativos	85	🟢
	12. Despliega los controles a través de políticas y procedimientos	178	🟢
Información y Comunicación	13. Usa información relevante	175	🟢
	14. Comunica internamente	69	🟢
	15. Comunica externamente	24	🟢
Seguimiento y Monitoreo	16. Conduce evaluaciones continuas y por separado	62	🟢
	17. Evalúa y comunica deficiencias oportunamente	49	🟢

Leyenda:

- 🟢 El principio se encuentra presente y funcionando en a nivel proceso
- 🟡 El principio no se encuentra a nivel proceso pero se presume pueda existir y estar funcionando a nivel entidad
- 🔴 El principio no se encuentra a nivel proceso ni a nivel entidad

4. Posteriormente se revisaron los controles a nivel entidad para cubrir los principios faltantes, **evaluar su materialidad** y se recopilaron aspectos de mejora en los controles existentes.

Principalmente mayor documentación relacionada con los principios de los componentes de Evaluación de Riesgos, Actividades de Control, Monitoreo y Información y Comunicación

		Evaluación de Riesgos	Actividades de Control			Información y Comunicación		Monitoreo y Seguimiento
Descripción del Proceso	**Riesgo**	**Principio 7**	**Principio 10**	**Principio 11**	**Principio 12**	**Principio 13**	**Principio 14**	**Principio 17**
Proceso 1	**R1**		**N**	**N**	**N**	**N**		
Proceso 2	**R2**		**N**	**Y**	**Y**	**Y**		
Proceso 2	**R3**		**N**	**Y**	**Y**	**Y**		
Proceso 3	**R4**		**N**		**N**	**N**		
Proceso 3	**R5**	**N**	**N**		**N**	**N**		
Proceso 4	**R6**		**N**	**N**	**N**	**N**		
Proceso 5	**R7**		**N**	**N**	**N**	**N**	**N**	**N**
Proceso 5	**R8**		**Y**	**Y**	**N**	**Y**		
Proceso 6	**R9**		**Y**		**N**	**Y**	**Y**	
		✗	✗	✗	✗	✗	✗	✗

Leyenda:

Y El principio se encuentra presente y funcionando a nivel proceso

N El principio se presume que no se encuentra a nivel proceso revisado

¿Son significativos individual y conjuntamente?

5. Luego del trabajo realizado, concluimos preliminarmente, en relación al Control Interno sobre el Reporte Financiero (ICFR) que:

- Cada uno de los cinco componentes y 17 principios del COSO 2013 estarían presentes y funcionando (para opinar respecto al 2014, debemos realizar nuevamente las pruebas de control durante este año)
- Los cinco componentes estarían operando juntos de manera integrada
- En consecuencia, tenemos evidencia de la EFECTIVIDAD del Control Interno SOX

Componente COSO	Principios	Aplicación	
Ambiente de Control	1. Demuestra compromiso con la integridad y los valores éticos	✓	
	2. El Directorio demuestra independencia y ejerce supervisión	✓	
	3. La Gerencia establece la estructura, autoridades y responsabilidades	✓	
	4. Demuestra compromiso a mantener individuos competentes	✓	
	5. Mantiene individuos consientes de su responsabilidad	✓	
Evaluación de Riesgos	6. Define sus objetivos con claridad	✓	
	7. Identifica y analiza sus riesgos	✓	●
	8. Considera el fraude en la evaluación de riesgos	✓	●
	9. Identifica y evalúa los cambios significativos	✓	●
Actividades de Control	10. Desarrolla actividades de control que mitigan los riesgos	●	
	11. Selecciona y desarrolla controles generales sobre los aplicativos	●	
	12. Despliega los controles a través de políticas y procedimientos	●	
Información y Comunicación	13. Usa información relevante	●	
	14. Comunica internamente	✓	●
	15. Comunica externamente	✓	●
Seguimiento y Monitoreo	16. Conduce evaluaciones continuas y por separado	✓	●
	17. Evalúa y comunica deficiencias oportunamente	✓	●

Leyenda:

✓ El principio se encuentra presente y funcionando a nivel entidad

● El principio se encuentra presente y funcionando a nivel proceso

3. Facilitar la sensibilización amplia (i.e. la organización), entrenamiento y evaluación integral

- Hasta ahora, el trabajo debe ser fácil porque se ha interactuado con expertos o involucrados en la gestión de riesgos y su supervisión
- En esta etapa el reto es incluir a toda la organización para construir “Conciencia” y presión, si la evaluación preliminar resultó complicada
- Clave: que los dueños de procesos “compren” el concepto y que implanten controles

Actividades desarrolladas

Sensibilización amplia 3

- Reuniones periódicas con la segunda línea de defensa ara aclarar conceptos
  - ✓Riesgo Operativo
  - ✓Prevención de fraudes
  - ✓Sistemas y TI
  - ✓Cumplimiento
- Plan de capacitación a todo el personal por Intranet

Capacitación a todo el personal

Sensibilización amplia

3

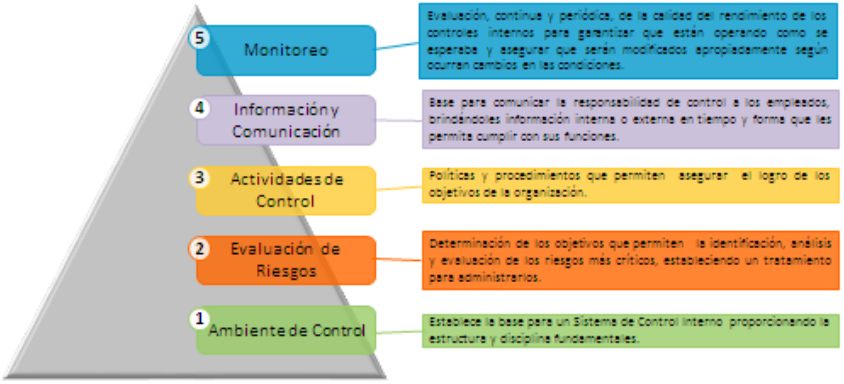
Aprobaron 12,833 colaboradores en BCP (98.6%)

Recordemos qué Estándar de Control Interno utiliza Credicorp:

- Credicorp, como la mayoría de empresas que listan en la Bolsa de Nueva York, decidió adoptar el estándar internacional de Control Interno COSO.*
  - COSO es un comité que publicó el marco de referencia de control interno para evaluar y reportar sobre el diseño y efectividad de los controles internos. En 1992, COSO publicó su primer Marco de referencia y en el 2013 emitió su última actualización.
  - El Marco COSO 2013 establece 17 principios que representan los conceptos fundamentales asociados a cada Componente.
  - Una entidad puede alcanzar un Control Interno efectivo mediante la adecuada aplicación de todos los Principios.

Sistema de Control Interno Credicorp COSO

Sistema de Control Interno Credicorp COSO



Curso: Administración del Riesgo de Operación

CREDICORP

Narrador: Recordemos también que el Sistema de Control Interno esta conformado por 5 Componentes y que nosotros como Colaboradores podemos contribuir con un Sistema de Control Interno efectivo y eficiente.

Curso: Administración del Riesgo de Operación

CREDICORP

Narrador: Recordemos qué estándar de control Interno utiliza Credicorp....

Por favor relacionada las imágenes con los componentes que consideres forma parte del mismo.....

5 La actividad de _____ forma parte del componente de Monitoreo

4 Son parte de los medios utilizados en el componente de Información y Comunicación

3 Las _____ son parte del componente de Actividades de Control

2 El establecimiento de _____ son parte del componente de Evaluación de Riesgos

1 El _____ forma parte del Ambiente de Control.

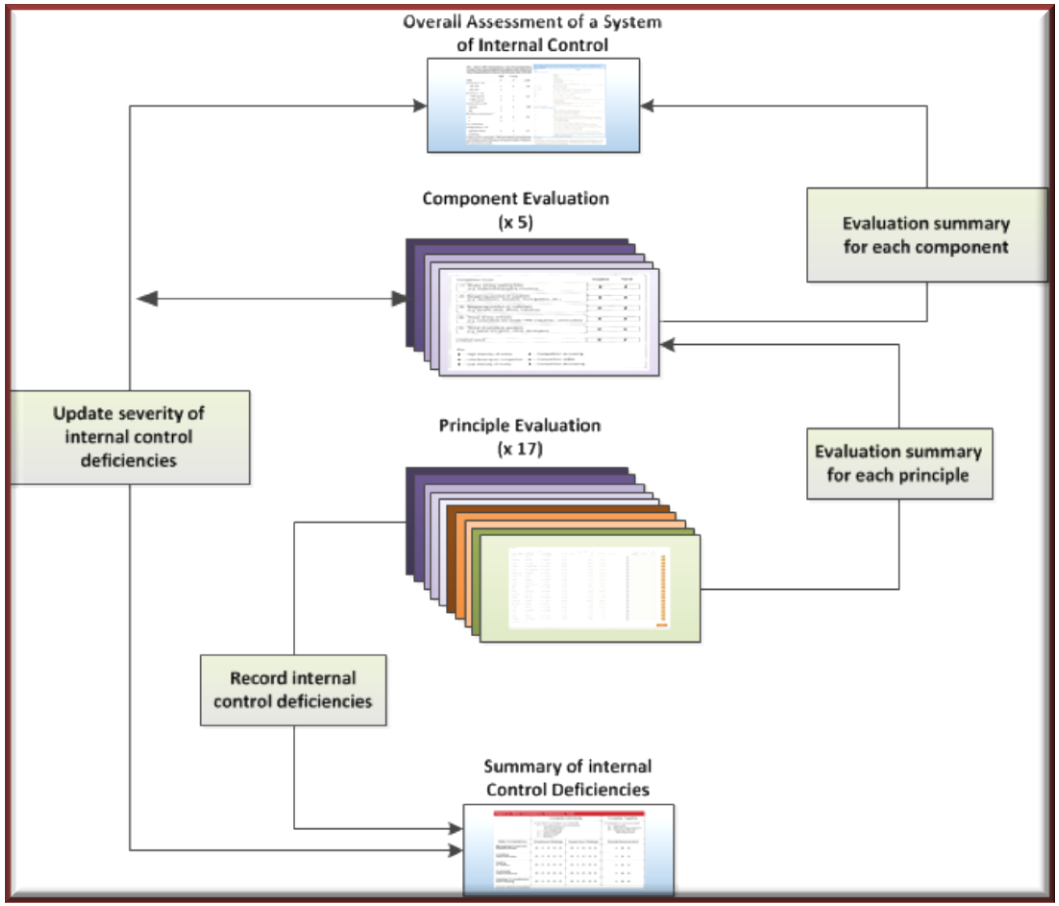
4. Desarrollar y ejecutar el plan de transición

- Esta es la etapa crítica
- Ejecutar el plan para cubrir las brechas encontradas y monitorearlo
  - ✓ Definir el gobierno del equipo de trabajo
  - ✓ Realizar los cambios metodológicos necesarios al Manual de Auditoría
  - ✓ Definir cronograma de hitos claros y accionables
- Se sugieren 3 fases:
  a) Documentación, que sustente la conclusión de control interno
  b) Pruebas de controles y retesteo en caso de deficiencias
  c) Revisión con auditores externos
- Conclusiones de la evaluación

Actividades desarrolladas

- Se actualizó:
  - ✓ Norma Corporativa de Control Interno
  - ✓ Manual Metodológico de Auditoría Interna (MMAI)
  - ✓ Manual y Normativa de Autoevaluación de Riesgos
- Se siguió casi al pie de la letra: “Illustrative tools for Assessing Effectiveness of a System of Internal Control”
- Al no encontrarse brecha relevantes nos enfocamos en las siguientes actividades
  - Mejorar soporte del Principio 8
  - Mejorar redacción de controles y documentación de pruebas en función del Staff Audit Practice Alert No. 11 “Considerations for Audits of Internal Control Over Financial Reporting” (Octubre 2013)
  - Continuar con el proceso de “adoctrinamiento”

Illustrative tools for Assessing Effectiveness of a System of Internal Control



Plantillas del COSO (www.cpa2biz.com/COSOEvalTools)

1. Overall Assessment of a System of Internal Control				
Overall Assessment of a System of Internal Control				
Entity or part of organization structure subject to the assessment (entity, division, operating unit, function)				
Objective(s) being considered for the scope of internal control being assessed		Considerations regarding management's acceptable level of risk		
Operations				
Reporting				
Compliance				
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
Control Environment				
Risk Assessment				
Control Activities				
Information and Communication				
Monitoring Activities				
Are all components operating together in an integrated manner? Evaluate if a combination of internal control deficiencies, when aggregated across components, represent a major deficiency* <Update Summary of Deficiencies Template as needed>				
Is the overall system of internal control effective? <Y/N>*				
Basis for conclusion				
* If it is determined that there is a major deficiency, management must conclude that the system of internal control is not effective.				

Reglas prácticas encontradas

Ejecución del Plan

4

1. Cuando el control no está formalizado el Principio 12 se presume no existe.
2. Cuando el control está relacionado con tecnología de información implicaría la existencia del Principio 11 y 12.
3. Cuando se realiza un control sobre un control de aplicación se podría considerar que existe el Principio 16.
4. Prohibir el uso del término Gerencia en Responsable del Control dentro del anexo 12 del Manual Metodológico, se debe especificar quién y que puesto realiza el control.
5. No existe Monitoreo sin control, por lo que si se marca la existencia del Principio 16 se debería marcar también el Principio 10
6. Si existe el Principio 14 o Principio 15 y se comunica para tomar acciones correctivas implicaría la existencia del Principio 17
7. **Sin duda, el esfurezo para establecer claramente los objetivos operativos, de reporte y de cumplimiento en cada trabajo/proceso ha generado un claro valor a la Organización**

Principio 8: Consulta

1. La gran mayoría: es inherente y sobre-entendido en cada proceso; por tanto se evalúa a nivel proceso auditable
   - En nuestra opinión, “podría no cumplir por sí solo el principio”
2. Evaluación de fraude a nivel entidad / organización patrocinada por CAE o por CRO para obtener una matriz centralizada de controles de fraude
3. Se contrató a un Big-4 para la evaluación comprehensiva, quien lo presentó al CA y se incorporó en el plan anual de AI
4. Se hizo una encuesta dirigida (con escenarios pre-establecidos de fraude), para identificar controles. Luego se consulta probabilidad e impacto para incorporarlo al Plan de Auditoría
5. Credicorp: 2 + mapeo/marca del 1

Identificación de ELCs

- En junio participamos de webinares “COSO 2013 Mapping Controls to Principles” y “COSO 2013: The Implications to IT Controls” de Financial Executives International y Protiviti
- SOX: Controles a Nivel Entidad (ELCs) son aquéllos que describen los aspectos del Control Interno que tienen un efecto generalizado en el Sistema de Control Interno de una organización. Ayudan a asegurar que las directivas relativas a la gestión de toda la Entidad se lleven a cabo. Sarbanex Oxley Section 404 – A guide for Management by Internal Control Practitioners, 2008, (p.39), publicado por el Instituto de Auditores Internos (www.theiia.org)
- Decidimos realizar
  - Mapeo de ELCs con los líderes de los 5 grupos

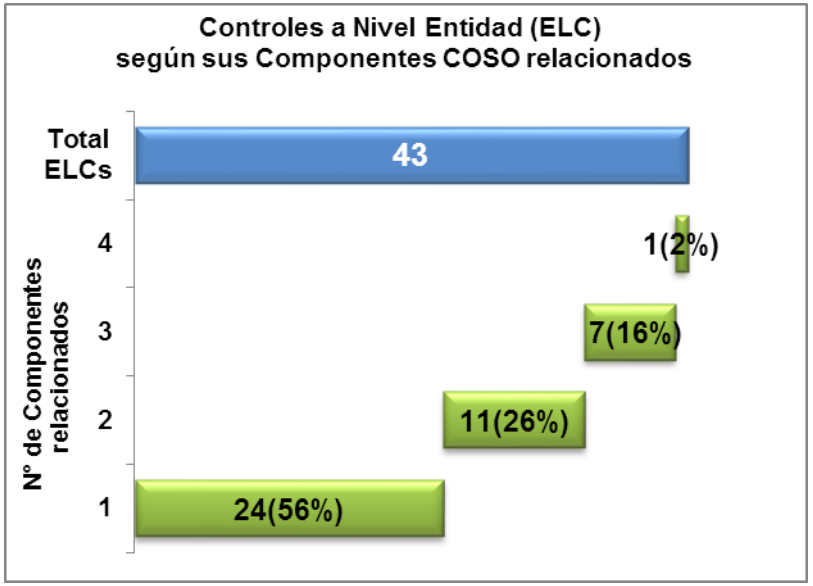
Mapeo de ELCs

		Ambiente de Control					Evaluación de Riesgos				Act. Control			Información y Comunicación			Supervisión	
		Compromiso con la integridad y la ética	Responsabilidad de Supervisión	Estructura, autoridad y responsabilidad	Compromiso con la Competencia profesional	Individuos responsables del Control Interno	Especifica objetivos adecuados	Identifica y analiza riesgos	Evalúa el riesgo de fraude	Identifica y analiza cambios significativos	Selecciona y desarrolla actividades de control	Selecciona y desarrolla Controles Generales de TI	Despliega políticas y procedimientos	Utiliza información relevante	Comunica internamente	Comunica externamente	Conduce evaluaciones continuas y/ó independientes	Evalúa y comunica deficiencias
Nº	**Descripción breve ELC**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
1	Monitoreo por parte de la Gerencia de Gestión de Cumplimiento de la firma y adherencia al Código de Ética.	X					X											
2	Aprobación por parte del Directorio del Plan Estratégico	X					X					X						
3	Aprobación por parte del Comité de Ética de las medidas de remediación a los Lineamientos de Conducta Corporativos.	X							X									
4	Reglamento del Directorio		X															
5	Autoevaluación del Directorio		X															
6	Supervisión por parte del Comité de Auditoría que la Gerencia haya implementado un adecuado Sistema de Control Interno.		X						X						X			
7	Aprobación anual por parte del Directorio del Manual de Organización y Funciones			X							X		X		X			
8	Desempeño corporativo				X	X			X								X	
9	Comité de Talento				X					X								
10	Revisión por el Comité de riesgo operativo de la evaluación de los Proveedores Críticos				X													
11	Revisión del plan de capacitación (3 programas: Riesgos, Créditos y Comercial)				X													

Mapeo de ELCs

- En el ejercicio, encontramos 43 controles a nivel entidad

Componente COSO	Principios	N° Controles a Nivel Entidad relacionados con el Principio
Ambiente de Control	1. La Organización demuestra compromiso con la integridad y los valores éticos.	3
	2. El Directorio demuestra independencia y ejerce la supervisión del desempeño del sistema de control interno.	4
	3. La Alta Dirección, con supervisión del Directorio, establece estructura, líneas de reporte, niveles de autoridad y responsabilidad.	2
	4. La Organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes, en alineación con los objetivos de la Organización.	7
	5. La Organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos.	5
Evaluación de Riesgos	6. La Organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados.	8
	7. La Organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la entidad y los analiza como base sobre la cual determinar cómo se deben gestionar.	3
	8. La Organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos.	9
	9. La Organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno.	5
Actividades de Control	10. La Organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos.	4
	11. La Organización define y desarrolla actividades de control a nivel entidad sobre la tecnología para apoyar la consecución de los objetivos.	8
	12. La Organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos que llevan dichas políticas a la práctica.	3
Información y Comunicación	13. La Organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.	4
	14. La Organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno.	5
	15. La Organización se comunica con los grupos de interés externos sobre los aspectos clave que afectan al funcionamiento del control interno.	3
Supervisión	16. La Organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes de sistema de control interno están presentes y en funcionamiento.	6
	17. La organización evalúa y comunica las deficiencias de control interno, de manera oportuna, a las partes responsables de aplicar medidas correctivas, incluyendo la Alta Dirección y el Directorio, según corresponda.	4



5. Impulsar la mejora continua

- El paso entre un sistema de control interno adecuado y el mejor sistema!
- COSO recomienda:
  - Promover la clara comunicación de la integridad y valores éticos y la importancia de mantener un sistema de control interno "*tone at the top*"
  - Inculcar la responsabilidad del control en la organización. Un buen ejemplo es la Autoevaluación del Control
  - Mejorar los sistema de reporte y monitoreo
  - Intensificar la GIR

Evaluación de Controles IT y COBIT 5

- Decidimos analizar los Controles IT, no bajo GAIT sino COBIT con el equipo de Auditoría IT
- Según el análisis del Marco COBIT 5, se identificaron 17 Controles a Nivel Entidad existentes, vinculados y alineados con 14 de los 37 procesos del Marco COBIT 5, los cuales se detallan a continuación:

Procesos de Gobierno:

1) Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.
2) Asegurar la Entrega de Beneficios.
3) Asegurar la Optimización del Riesgo.
4) Asegurar la Optimización de Recursos.
5) Asegurar la Transparencia hacia las Partes Interesadas.

Procesos de Gestión:

6. Gestionar el Marco de Gestión de TI.
7. Gestionar la Estrategia.
8. Gestionar los Recursos Humanos.
9. Gestionar el Riesgo.
10. Gestionar la Seguridad.
11. Gestión de Programas y Proyectos.
12. Gestionar la Disponibilidad y la Capacidad.
13. Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad.
14. Supervisar, Evaluar y Valorar el Sistema de Control Interno.

Evaluación de Controles IT y COBIT 5

- Ejemplo con Proceso EDM01: “Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno”

Área	Dominio	Código	Proceso	Descripcion del Proceso	Declaración del Propósito del Proceso	Cód. Práctic	Nombre de la Práctica	Principios COSO	Punto de Enfoque	Control
Gobierno	Evaluar, Orientar y Supervisar	EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.	Proporcionar un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa. Para garantizar que las decisiones relativas a TI se han adoptado en línea con las estrategias y objetivos de la empresa, garantizando la supervisión de los procesos de manera efectiva y transparentemente, el cumplimiento con los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del Consejo de Administración.	EDM01.01	Evaluar el sistema de gobierno	1,6	P1-2 P6-3	ELC2
						EDM01.02	Orientar el sistema de gobierno.	3,10,12,14	P3-1,2,3 P10-6 P12-1,2,5,6 P14-1	ELC7
						EDM01.03	Supervisar el sistema de gobierno.	11	2	ELC26

Evaluación de Controles IT y COBIT 5

Posteriormente ISACA publicó “IT Control Objectives for Sarbanes Oxley 3ra Edición”, que incluye una metodología de mapeo de controles ITGC a nivel entidad y a nivel actividad, relacionándolos con COSO 2013

Figure 9—Summary COBIT Areas/COSO Components

Entity Level	Activity Level	Detailed Activity/Objective Level	COBIT 5 Reference	COSO Component																
				Control Environment					Risk Assessment				Control Activities			Information and Communication			Monitoring Activities	
				Principles					Principles				Principles			Principles			Principles	
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Evaluate Direct and Monitor (EDM) (IT Environment)																				
•		Ensure Governance Framework Setting and Maintenance	EDM01	•	•	•		•								•	•		•	•
•		Ensure Risk Optimisation	EDM03		•			•	•	•						•	•			
•		Ensure Stakeholder Transparency	EDM05		•			•								•	•	•		•
Align, Plan and Organise (APO) (IT Environment)																				
•		Manage the IT Management Framework	APO01	•		•	•	•			•				•	•	•	•		
•		Manage Strategy	APO02					•	•							•	•			
•		Manage Human Resources	APO07	•			•				•					•	•			
	•	Manage Service Agreements	APO09					•	•				•	•		•	•			
	•	Manage Suppliers	APO10					•	•	•	•	•	•	•		•	•			
•		Manage Quality	APO11					•	•						•	•	•			
•		Manage Risk	APO12						•	•	•	•				•	•			
•	•	Manage Security	APO13					•	•	•	•	•		•		•	•			

Agregación de observaciones y evaluación final

Banco de Crédito del Perú

Evaluación de Observaciones por Principio Afectado y Criticidad

(Año 2014, Total 42 observaciones relacionados a controles SOX)

N° Principio		Criticidad BCP					Total
		Crítico	Alto	Relevante	Moderado	Bajo	
Principio 1		-	-	-	-	-	-
Principio 2		-	-	-	-	-	-
Principio 3		-	-	-	-	-	-
Principio 4		-	-	-	-	-	-
Principio 5		-	-	-	-	-	-
Principio 6		-	-	-	-	-	-
Principio 7		-	-	-	-	-	-
Principio 8		-	1	1	3	-	**5**
Principio 9		-	-	-	-	-	**-**
Principio 10		-	1	11	1	5	**30**
Principio 11		-	-		3	1	**6**
Principio 12		-	1	1	1	1	**5**
Principio 13		-	-	2	1	-	**3**
Principio 14		-	-	-	-	-	**-**
Principio 15		-	-	-	2	3	**5**
Principio 16		-	1	-	-	-	**1**
Principio 17		-	-	-	-	-	**-**
Totales		**0**	**4**	**15**	**11**	**10**	**55**

(a) Las observaciones emitidas por Auditoría Interna y pueden afectar a uno o más de los principios de COSO.

(b) Estas 50 observaciones corresponden al 1.02% del total de pruebas ejecutadas

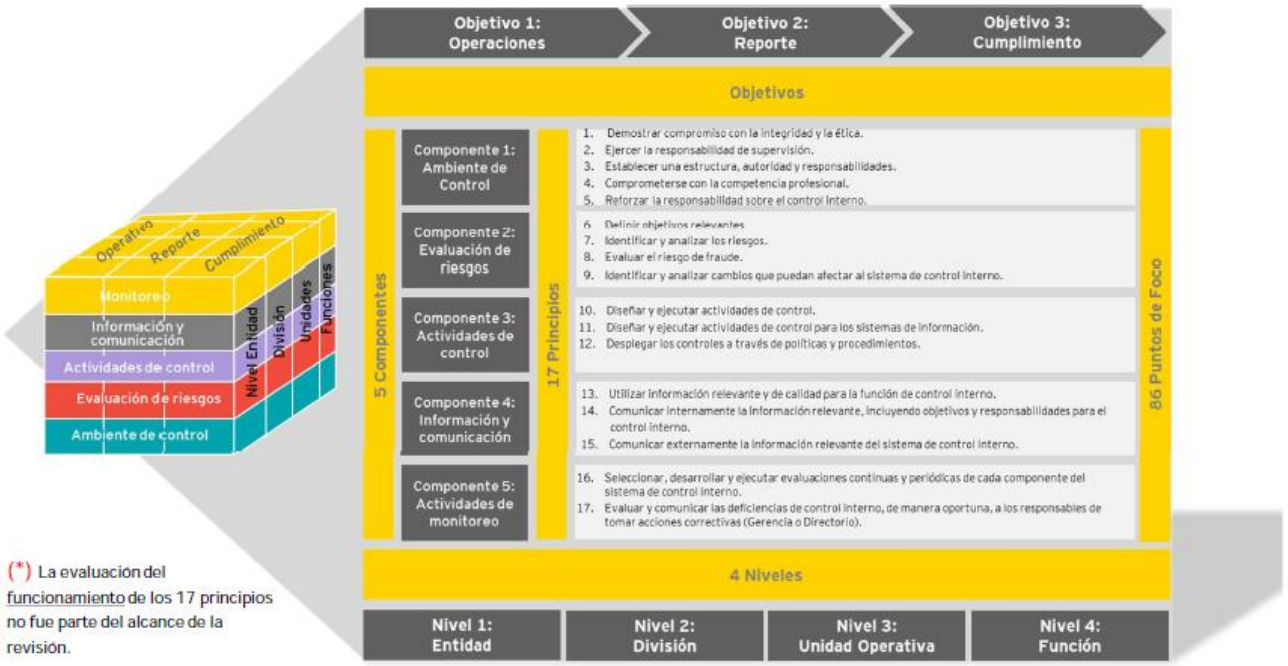
Agenda

- Primeros resultados del COSO 2013
- Credicorp y el Marco de Control Interno
- Cambios Metodológicos realizados a los procesos de evaluación de riesgos para aplicar COSO 2013
- Resultados y recomendaciones

Auditoría independiente QA

1. Objetivo y alcance

Como parte de la auditoría financiera de Credicorp, realizamos un diagnóstico sobre la existencia (*) de los 17 principios del nuevo marco COSO 2013, a través de la revisión de la documentación de soporte disponible y sostenimiento de reuniones con el personal clave.



(*) La evaluación del funcionamiento de los 17 principios no fue parte del alcance de la revisión.

Auditoría independiente OA

2. Resultados

Existencia de los 17 principios de Marco Coso 2013

Principios	Resultado
Principio 1	Sí cumple
Principio 2	Sí cumple
Principio 3	Sí cumple
Principio 4	Sí cumple
Principio 5	Sí cumple
Principio 6	Sí cumple
Principio 7	Sí cumple
Principio 8	Sí cumple
Principio 9	Sí cumple
Principio 10	Sí cumple
Principio 11	Sí cumple
Principio 12	Sí cumple
Principio 13	Sí cumple
Principio 14	Sí cumple
Principio 15	Sí cumple
Principio 16	Sí cumple
Principio 17	Sí cumple

Oportunidad de mejora

Oportunidad de mejora

Reporte del Auditor

Extracto del 20F Credicorp
pags. 231-232
www.credicorpnet.com

15. C Attestation Report of the Registered Public Accounting Firm

To the Shareholders and Board of Directors of Credicorp Ltd.

We have audited Credicorp Ltd. and Subsidiaries (hereinafter "Credicorp") internal control over financial reporting as of December 31, 2014, based on criteria established in Internal Control Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 Framework) (the COSO criteria). Credicorp's management is responsible for maintaining effective internal control over financial reporting, and for its assessment of the effectiveness of internal control over financial reporting included in the accompanying Management's Report on Internal Control over Financial Reporting. Our responsibility is to express an opinion on Credicorp's internal control over financial reporting based on our audit.

In our opinion, Credicorp maintained, in all material respects, effective internal control over financial reporting as of December 31, 2014, based on the COSO criteria.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States of America), the consolidated statements of financial position of Credicorp as of December 31, 2014 and 2013, the opening consolidated statement of financial position as of January 1, 2013 and the related consolidated statements of income, comprehensive income, shareholders' equity and cash flows, for each year ended December 31, 2014, 2013 and 2012, and our report dated April 28, 2015, expressed an unqualified opinion thereon.

Lima, Perú,

April 28, 2015

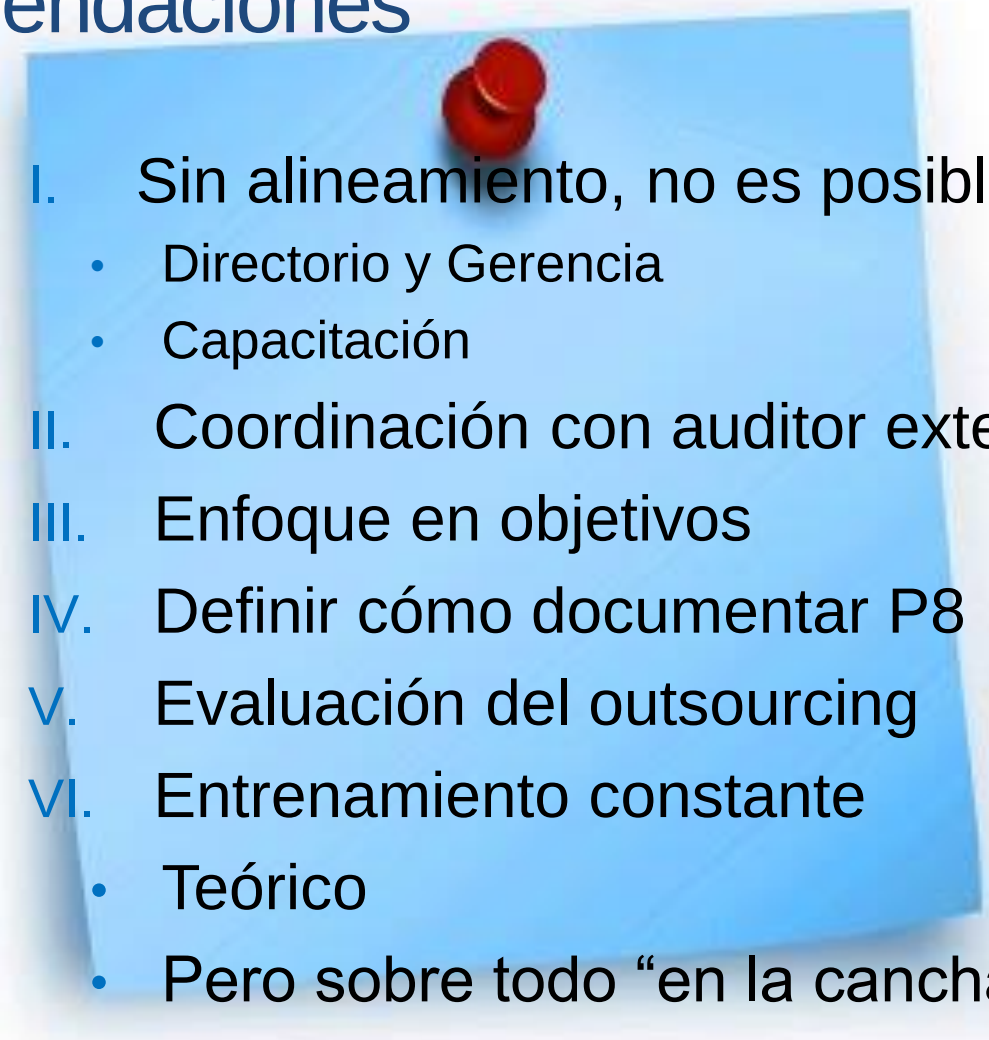
/S/ Paredes, Zaldívar, Burga & Asociados S.C.R.L

Countersigned by:
/S/ JUAN PAREDES
Juan Paredes C.P.C.C. Register N°22220

15. D Changes in Internal Control over Financial Reporting

During the period covered by this Annual Report, no changes were made to our internal control over financial reporting that have materially affected, or are likely to materially affect, internal control over financial reporting. Nevertheless, it is important to note, as stated in Item 15. Controls and procedures - 15. B Management's Annual Report on Internal Control over Financial Reporting, Credicorp aligned its policies, procedures and assessment of the internal control over financial reporting to the COSO 2013 framework.

Recomendaciones



I. Sin alineamiento, no es posible
   - Directorio y Gerencia
   - Capacitación
II. Coordinación con auditor externo
III. Enfoque en objetivos
IV. Definir cómo documentar P8
V. Evaluación del outsourcing
VI. Entrenamiento constante
   - Teórico
   - Pero sobre todo “en la cancha”

Recomendaciones

VII. Mapeo preciso de controles indirectos o ELCs

VIII. Definir y relevar exhaustivamente los controles de revisión de la gerencia: precisión

IX. Método simple para agrupar deficiencias por principio

X. Pensar y planificar desde el inicio el uso del marco de manera comprehensiva

- Lo “bueno”
  - Mayor objetividad al evaluar y concluir sobre control interno
- Lo “malo”
  - Mayor documentación de sustento y trabajo relacionado
- Lo “feo”
  - 
    Habrá que esperar para ver las “mejores prácticas”