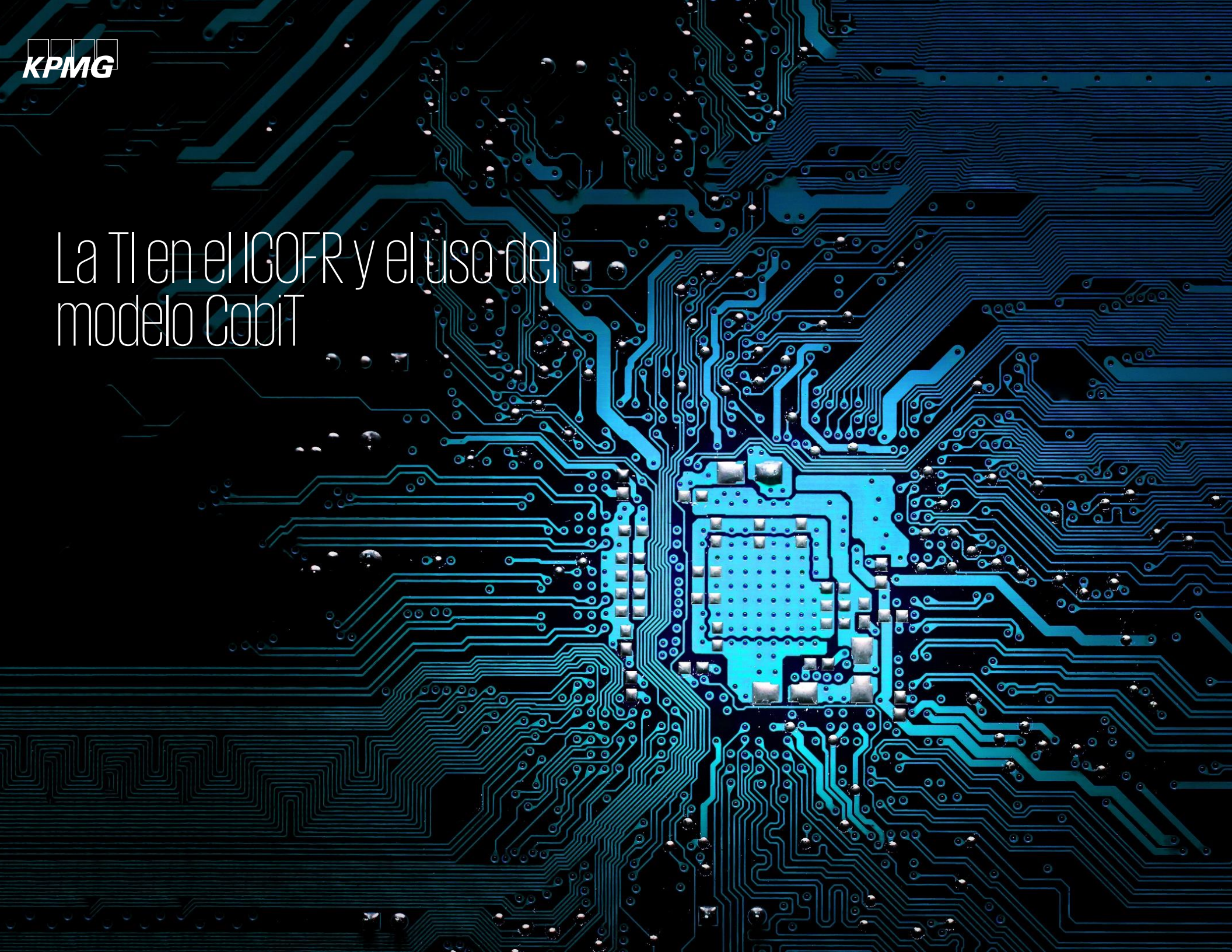
KPMG

La TI en el ICOFR y el uso del modelo CobiT



Presentadores

Fabio Alexander Rojas Roldán CISA, CRISC
Socio
Information Risk Management
KPMG en Colombia

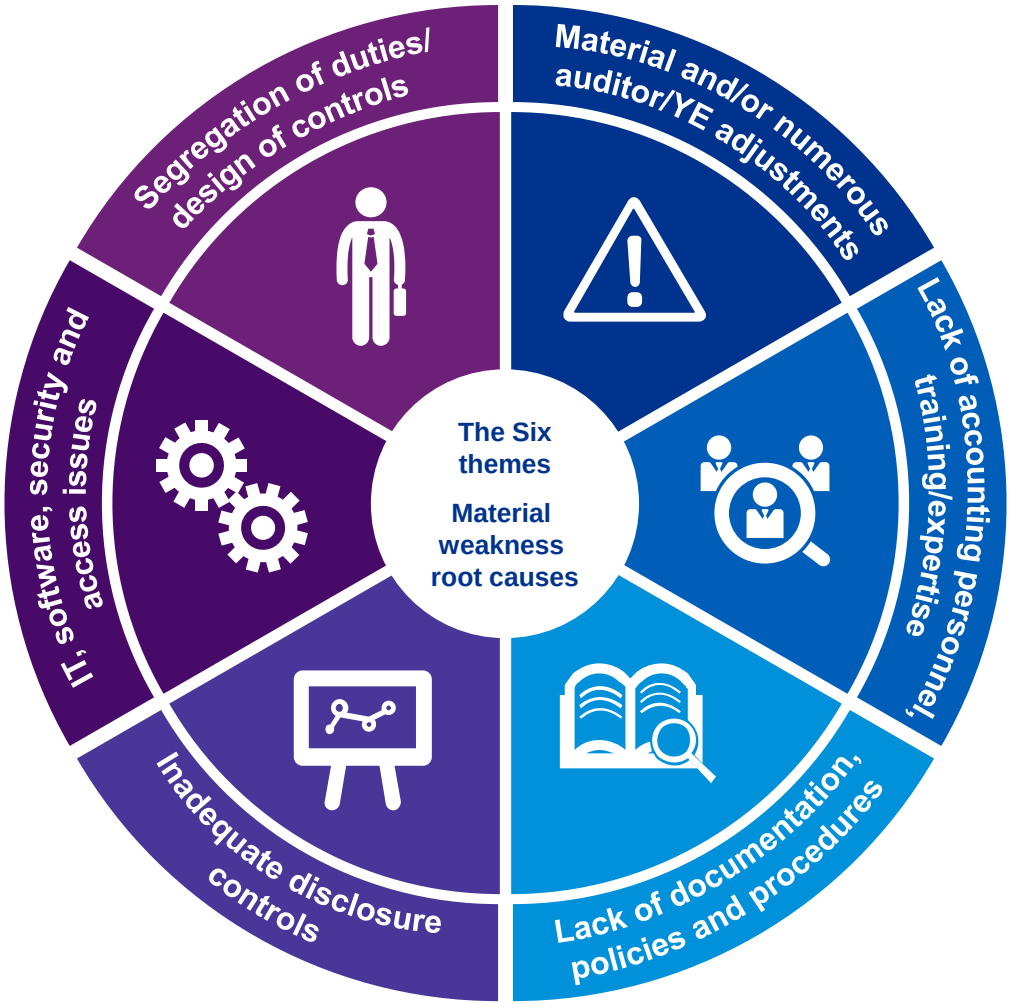
Gustavo Cubides CISA, CRISC
Senior Manager
Information Risk Management
KPMG en Colombia

Agenda

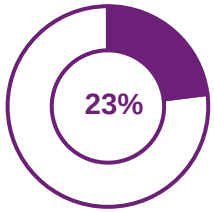
	**Antecedentes** ¿Qué esta sucediendo?
	Usando Cobit para soportar el ICOFR Controles de TI en el ICOFR Cobit vs COSO Controles de TI a nivel de la Entidad Controles Generales de TI
	**Controles de aplicación** Como identificar los controles de aplicación Clasificación de los controles de aplicación Segregación de funciones

Antecedentes

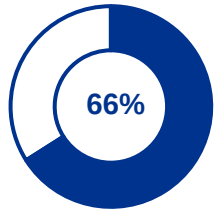
Tendencia de las debilidades materiales



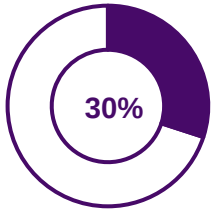
MWs by issue type



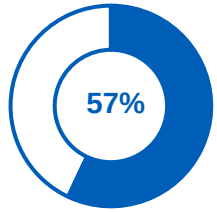
Segregation of duties/design of controls



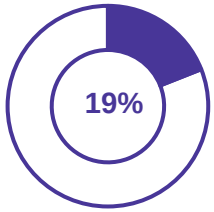
Material and/or numerous audit/year end adjustments



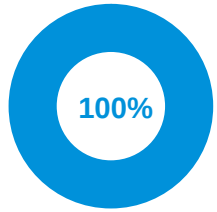
IT, software, security and access issues



Lack of accounting personnel, training/expertise



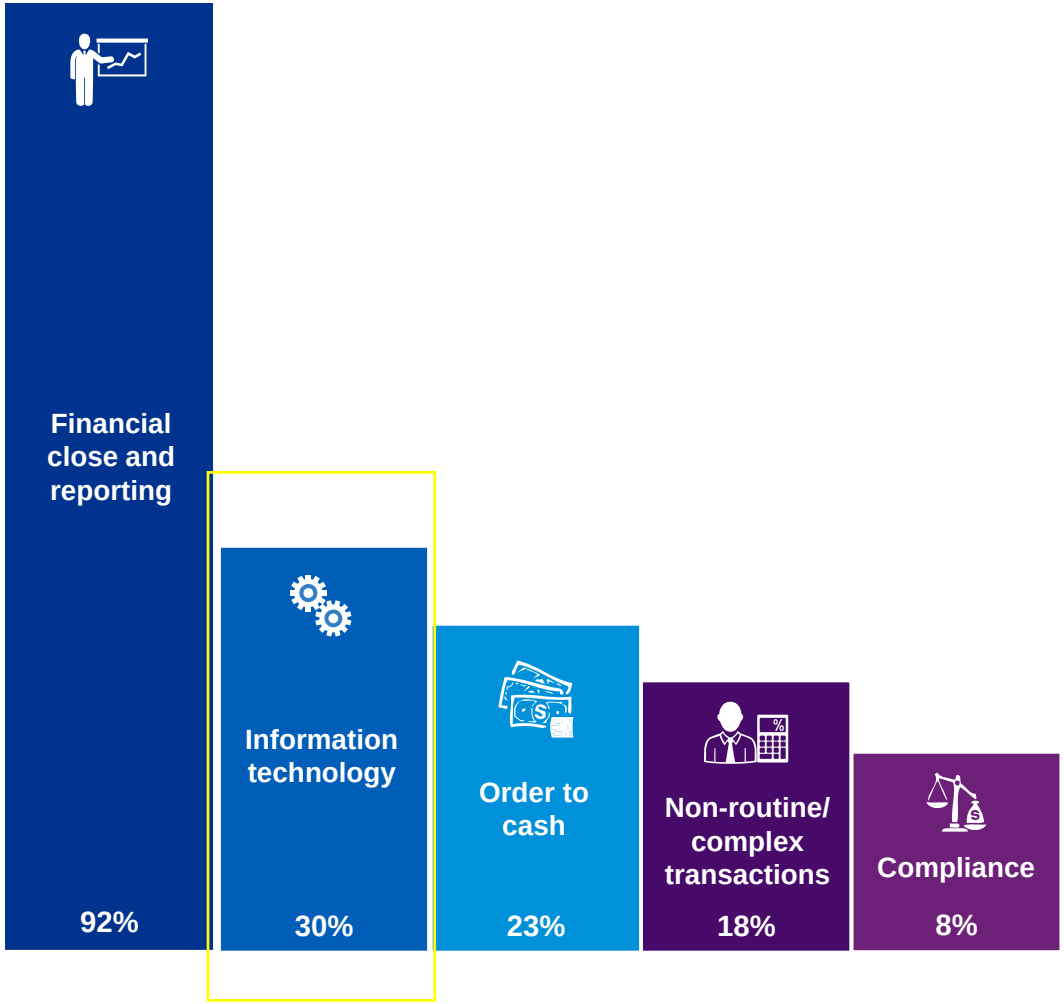
Inadequate disclosure controls



Lack of documentation, policies and procedures

Resumen de las debilidades materiales reportadas

MWs by process area



The top five process areas impacted, which represent 75% of the MW issues disclosed

75%

Ejemplo de debilidades materiales

Temas comunes

Documentación, políticas y procedimientos débiles

“…Procedimientos y políticas insuficientes para reporte financiero y contable, con respecto a la aplicación de principios y requerimientos contables.

Controles de revelación inadecuados

"... existían deficiencias con respecto a ciertos aspectos de nuestra información financiera histórica y ... hemos llegado a la conclusión de que nuestras revelaciones previas con respecto a la suficiencia de nuestros controles de divulgación, controles internos y cambios en los controles internos pueden no haber sido correctos".

Débil entrenamiento al personal de contabilidad y experiencia insuficiente

“…La Compañía no mantiene recursos técnicos suficientes para asegurar que los estados financieros estén acorde con los requerimientos contables.”

Temas de informática, software, seguridad y acceso.

"... faltaban controles con respecto al acceso a las aplicaciones y al mantenimiento de datos maestros ... controles para asegurar que los cambios en las aplicaciones financieras estén debidamente autorizados y probados y que el acceso a los sistemas de información, aplicaciones financieras y hojas de cálculo clave estén adecuadamente restringidos.”

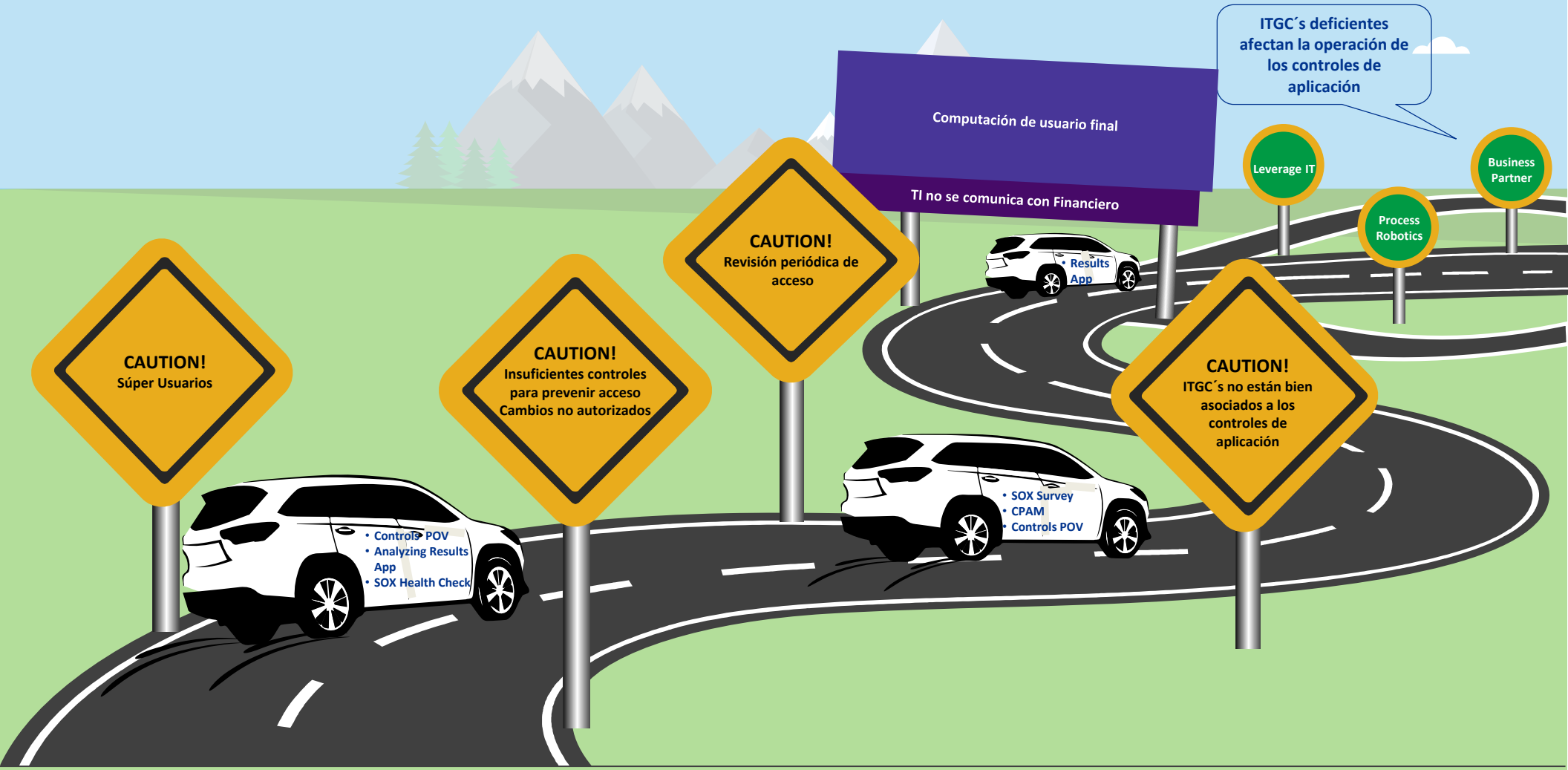
Numerosos ajustes de fin de año

“… no se diseñó y mantuvieron controles sobre modelos de revisión efectivos, asunciones y datos utilizados en el desarrollo de estimados o cambios a las asunciones y datos relacionados.

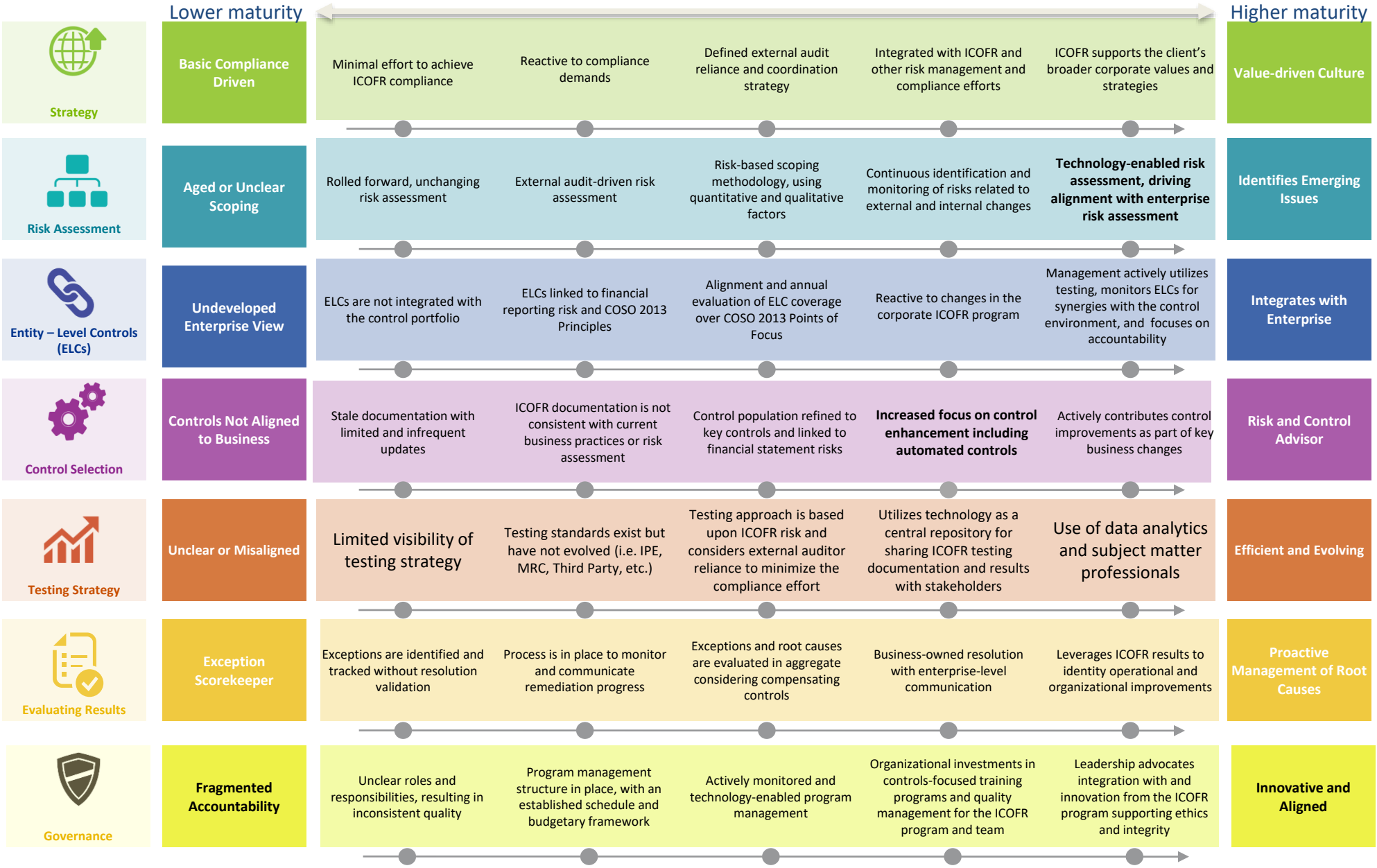
Segregación de funciones / diseño de controles.

"... determinó que el diseño de controles sobre asuntos contables no rutinarios no establecía una separación de tareas suficiente entre el análisis de asuntos contables no rutinarios y la realización de revisiones suficientemente detalladas del análisis y las conclusiones contables".

PCAOB - Deficiencias en ITGC´s



Nivel de madurez del ICOFR



KPMG 2016 Encuesta SOX

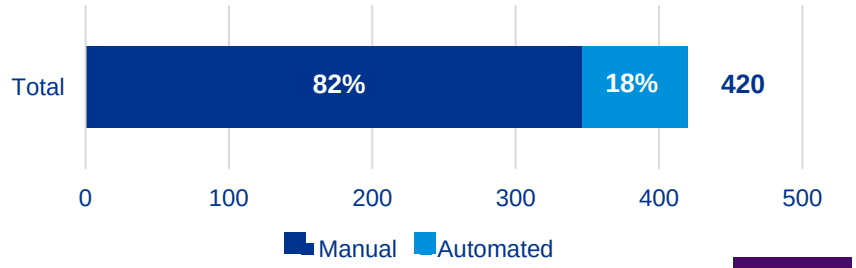
En promedio el 18% del total de controles es automático

-El 98% de las compañías estiman que el 20% de sus controles clave es automático.
-El 46% indican que incrementar los controles automáticos es una de sus áreas focales.

El futuro del negocio, incluyendo el reporte financiero, es más automatización. Las compañías invierten de forma significativa en recursos, por ejemplo implementando ERP y diseñando GITC´s.

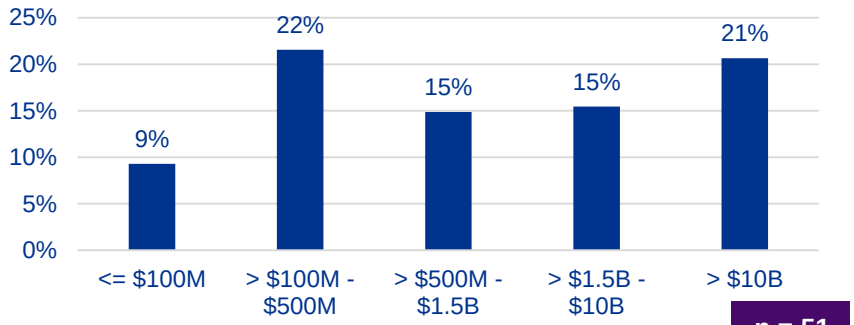
-Un programa saludable y eficiente de control interno, debería incluir tanto controles manuales como automáticos.
-Moverse hacia un mayor porcentaje de controles automáticos, contribuye a la capacidad de reducir costos tanto en operar como en evaluar esos controles.
-Cada vez existe mayor presión del regulador por validar la completitud y la exactitud de toda la información utilizada en los controles y por ello las compañías deberían migrar de hojas de calculo hacia reportes automatizados.

Average number of total controls – manual and automated



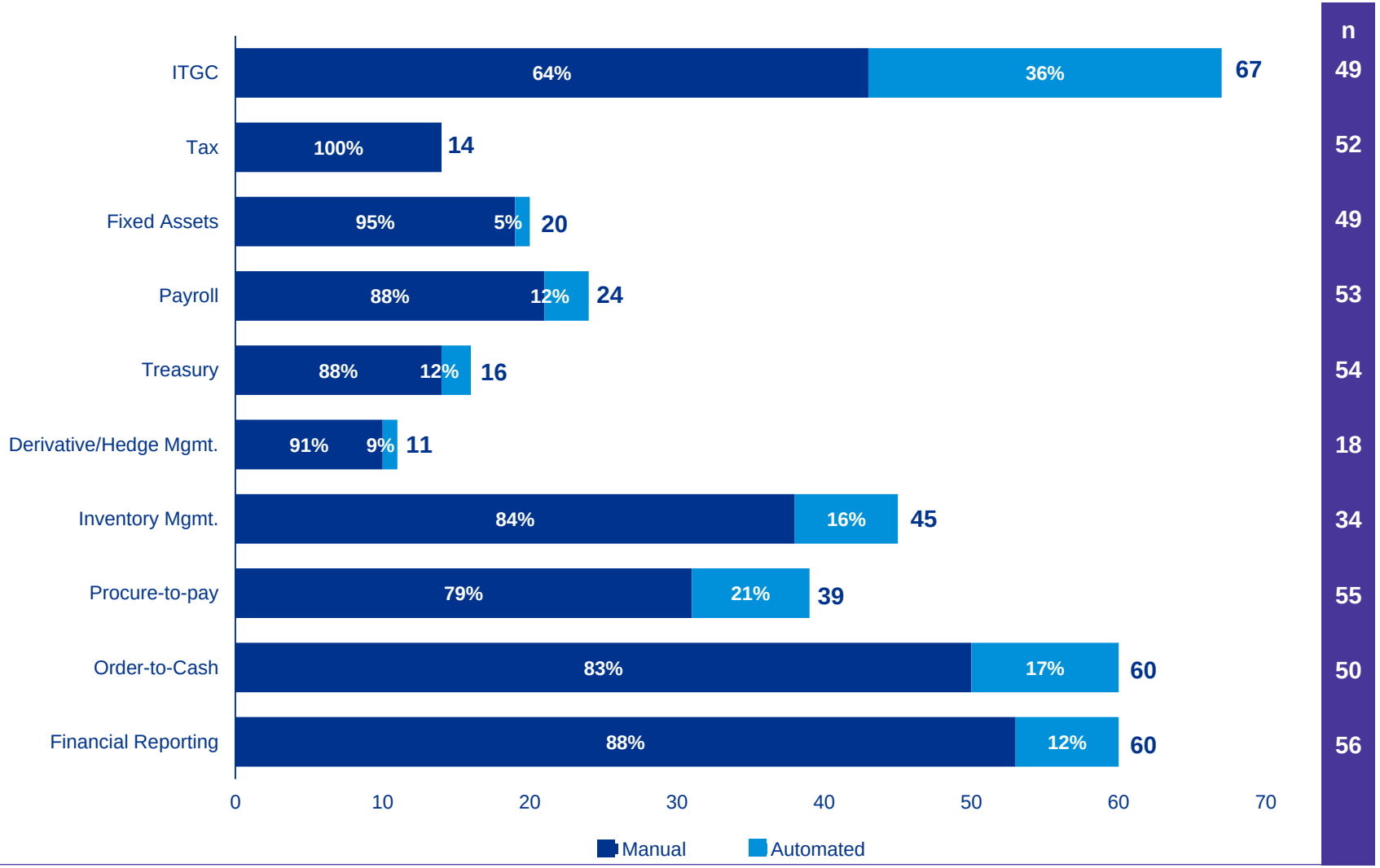
n = 51

Percent of total controls that are automated – by annual revenue



n = 51

KPMG 2016 Encuesta SOX

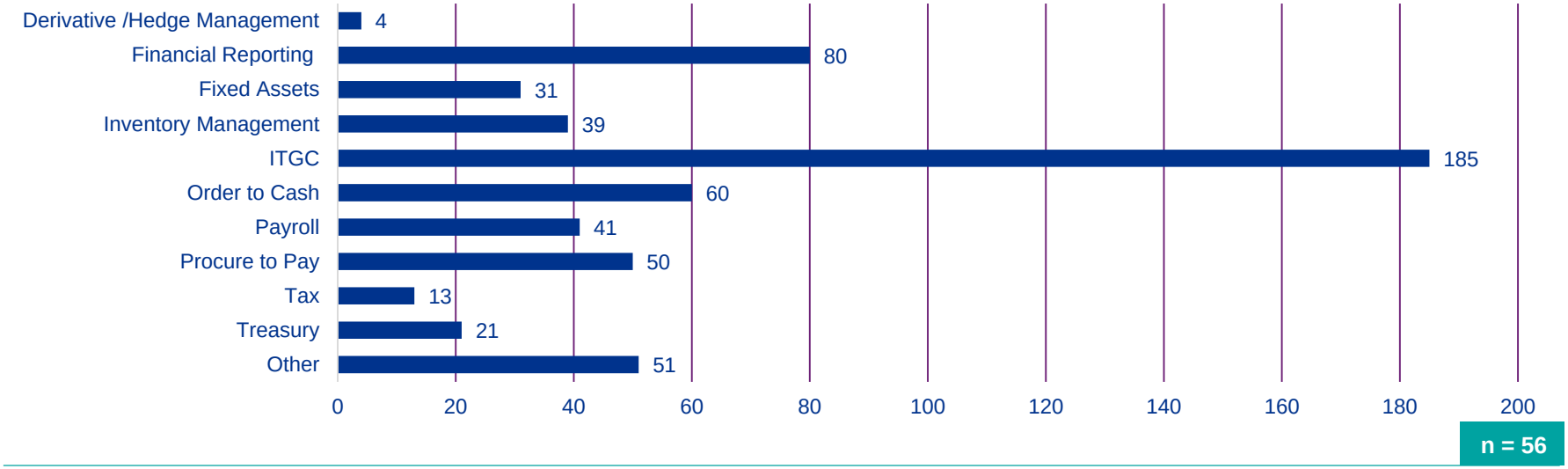


KPMG 2016 Encuesta SOX

73% de las compañías encuestadas, reportaron uno o mas deficiencias de control.

El proceso que comúnmente presenta mas deficiencias de control fue los controles generales de TI (GITC´s)

Count of control deficiencies



n = 56

10 average control deficiencies per company

KPMG

Coso Vs. CobiT

COBIT

La importancia de un buen gobierno de TI

Las empresas exitosas reconocen los beneficios de la tecnología de la información y la utilizan para impulsar el valor de sus partes interesadas. Estas empresas también comprenden y gestionan los riesgos asociados, como el aumento del cumplimiento normativo y la dependencia crítica de muchos procesos de negocios en la tecnología de la información (TI).

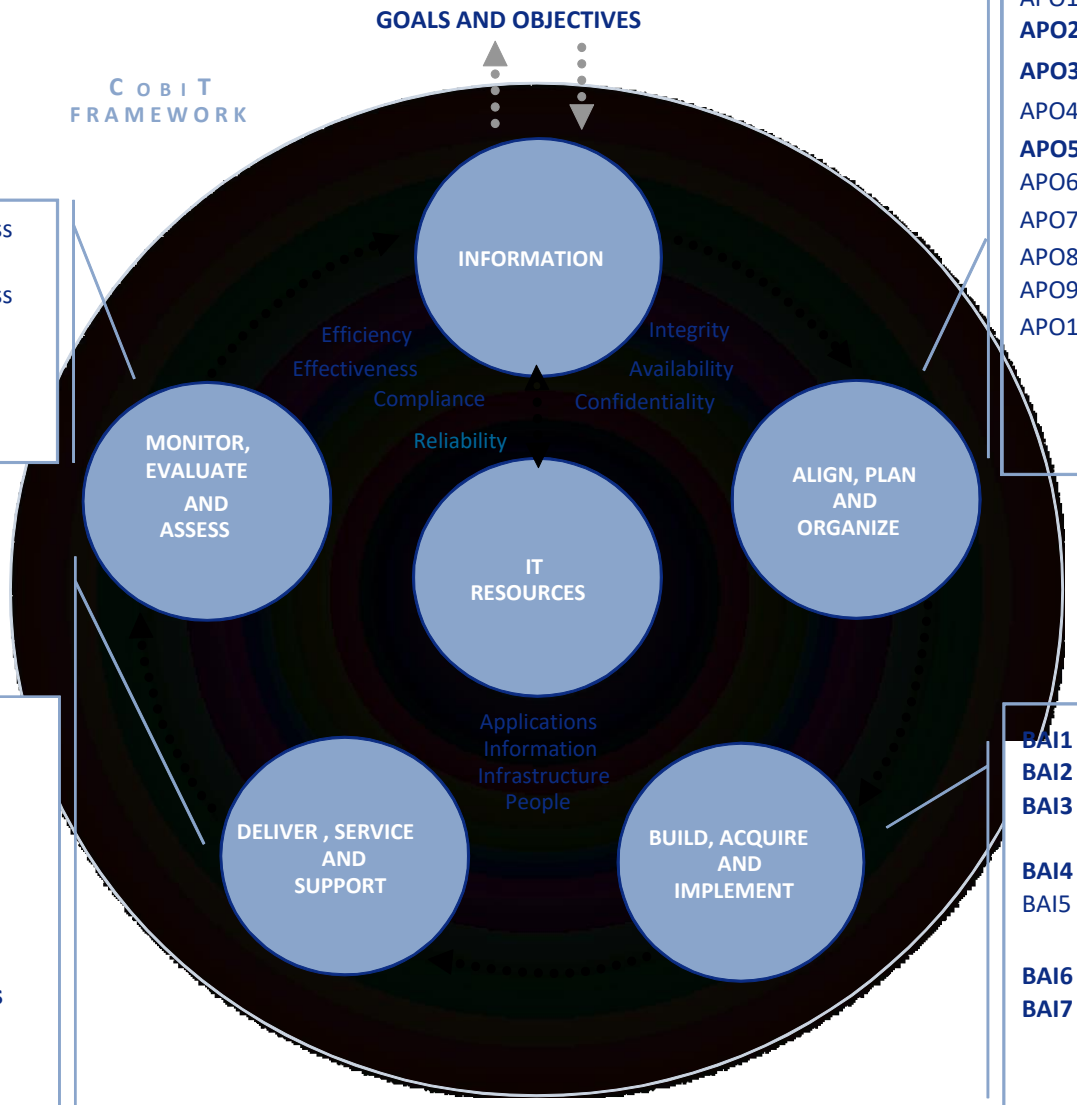
COBIT como marco de gobierno de TI

Los objetivos de control para la información y la tecnología relacionada (COBIT) proporcionan buenas prácticas en un marco de dominio y proceso y presentan actividades en una estructura lógica y manejable.

Evaluación de TI utilizando COBIT

Para que la TI tenga éxito en la entrega frente a los requisitos del negocio, la administración debe implementar un sistema o marco de control interno. La orientación comercial de COBIT consiste en vincular los objetivos comerciales con los objetivos de TI, proporcionar métricas y modelos de madurez para medir sus logros, e identificar las responsabilidades asociadas de los propietarios de procesos de TI y de negocios.

Modelo de procesos de CobiT



MEA1 Monitor, evaluate and assess performance
MEA2 Monitor, evaluate and assess Internal control
MEA3 compliance with external

APO1 Manage IT management framework
APO2 Manage strategy
APO3 Manage enterprise architecture
APO4 Manage innovation
APO5 Manage portfolio
APO6 Manage budget and costs
APO7 Manage human resources.
APO8 Manage relationships
APO9 Manage service agreements
APO10 Manage Suppliers.

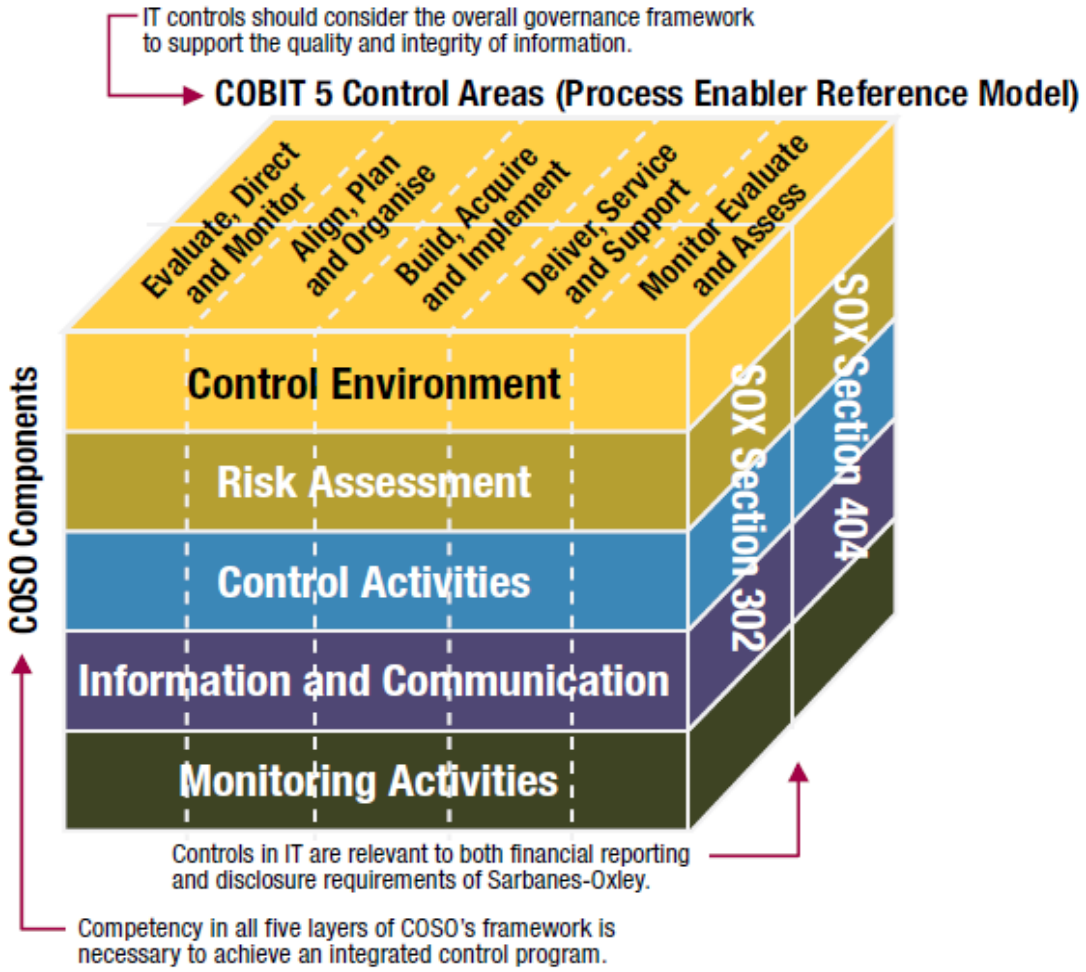
-

DSS1 Manage Operations
DSS2 Manage service requests and incidents
DSS3 Manage problems
DSS4 Ensure continuity
DSS5 Ensure security services
DSS6 Manage business process controls

BAI1 Manage programs and projects
BAI2 Manage requirements definition
BAI3 Manage solutions identification and build
BAI4 Manage availability and capacity
BAI5 Manage organizational change
BAI6 Manage changes
BAI7 Manage change acceptance and transitioning

CobiT Vs. COSO

Figure 8—Mapping COBIT to the COSO Cube



Source: Adapted from COSO, "Internal Control—Integrated Framework," Executive Summary, USA, May 2013. Used with permission.

KPMG

Usando CobiT para SOX

Marco COSO vs COBIT

Figure 9—Summary COBIT Areas/COSO Components *(cont.)*

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
Build, Acquire and Implement (BAI) (Program Development and Program Change)																				
	•	Manage Requirements Definition	BAI02						•			•	•	•		•	•			
	•	Manage Solutions Identification and Build	BAI03						•			•	•	•		•	•			
	•	Manage Availability and Capacity	BAI04									•	•	•		•	•			
	•	Manage Changes	BAI06						•		•	•	•	•		•	•			
	•	Manage Change Acceptance and Transitioning	BAI07						•	•	•	•	•	•		•	•			
	•	Manage Configuration	BAI10						•		•	•	•	•		•	•			
Deliver, Service and Support (DSS) (Operations and Access to Programs and Data)																				
	•	Manage Operations (Includes Outsourced Services)	DSS01						•	•	•	•	•	•	•	•	•			
	•	Manage Service Requests and Incidents	DSS02						•				•	•		•	•			
	•	Manage Problems	DSS03						•				•	•		•	•			
	•	Manage Backup Arrangements	DSS04.07						•				•	•		•	•			
	•	Manage Security Services	DSS05						•	•	•		•	•		•	•			
	•	Manage Business Process Controls (including App Controls)	DSS06					•	•	•	•		•	•		•	•			

Principio 8: *La organización considera el potencial de fraude en la evaluación de los riesgos para el logro de los objetivos.*

DSS05.04: *Administrar la identidad del usuario y el acceso lógico.*

DSS06.03: *Administrar roles, responsabilidades, privilegios de acceso y niveles de autoridad.*

Usando CobiT 5 para SOX

— Controles de aplicación
1. Mapeo
2. Configuración
3. Controles de Interface
4. Reportes de excepciones
5. Acceso / SOD

-Aseveraciones en EF´s
1. Integridad
2. Existencia
3. Exactitud
4. Valuación
5. Presentación

— BAI06- Manage Changes
— BAI07- Manage Change Acceptance and Transitioning

— Las solicitudes de cambios de TI deben registrarse, evaluarse para determinar su impacto, aprobarse y debe mantenerse la segregación de los roles operativos y de desarrollo

— Los cambios deben probarse para garantizar que cumplan con los requisitos del usuario y no afecten negativamente el

— Relación de la muestra de cambios de producción seleccionados para revisión que se migraron a producción sin un ticket de cambio válido.

— Porcentaje de cambios de TI que tuvieron que ser eliminados debido a pruebas inadecuadas.

— ITGC´s relevantes
  — Acceso a programas
  — Administración de cambios
  — Desarrollo de programas
  — Operaciones por computador

— Se realicen cambios no autorizados en el entorno de TI y las aplicaciones que pueden tener un impacto negativo en el negocio.

— Los cambios del sistema no se han probado adecuadamente para garantizar que cumplen con los requisitos del usuario y no afectan negativamente a las soluciones y servicios

— Existen procedimientos para garantizar que las solicitudes de cambio se registran para los cambios en el sistema, la aplicación y la base de datos.

— Existen procedimientos para garantizar una autorización adecuada antes de la implementación en el entorno de producción / en vivo.

— Procedimiento para administrar los cambios

— Evidencia de las pruebas de aceptación del sistema y del usuario y aprobación antes de la implementación.

KPMG

Controles de aplicación ITAC's

AS2110

“.B4 The auditor should obtain an understanding of specific risks to a company's internal control over financial reporting resulting from IT. Examples of such risks include:

Confianza en los sistemas o programas que procesan datos de manera incorrecta, procesan datos inexactos o ambos.

El acceso no autorizado a datos que podría resultar en la destrucción de datos o cambios impropios en los datos, incluyendo el registro de transacciones no autorizadas o inexistentes o el registro incorrecto de transacciones (pueden surgir riesgos particulares cuando múltiples usuarios acceden a una base de datos común)

La posibilidad de que el personal de TI obtenga privilegios de acceso más allá de los necesarios para realizar sus tareas asignadas, rompiendo así la segregación de tareas

Cambios no autorizados a datos en archivos maestros

Cambios no autorizados a sistemas o programas

No hacer los cambios necesarios a los sistemas o programas

Intervención manual inadecuada

Posible pérdida de datos o incapacidad para acceder a los datos según sea necesario”

Anexo B

“.B1 While obtaining an understanding of the company's information system related to financial reporting, the auditor should obtain an understanding of how the company uses information technology ("IT") and how IT affects the financial statements.1 The auditor also should obtain an understanding of the extent of manual controls and automated controls used by the company, including the IT general controls that are important to the effective operations of the automated controls. That information should be taken into account in assessing the risks of material misstatement.2I ”

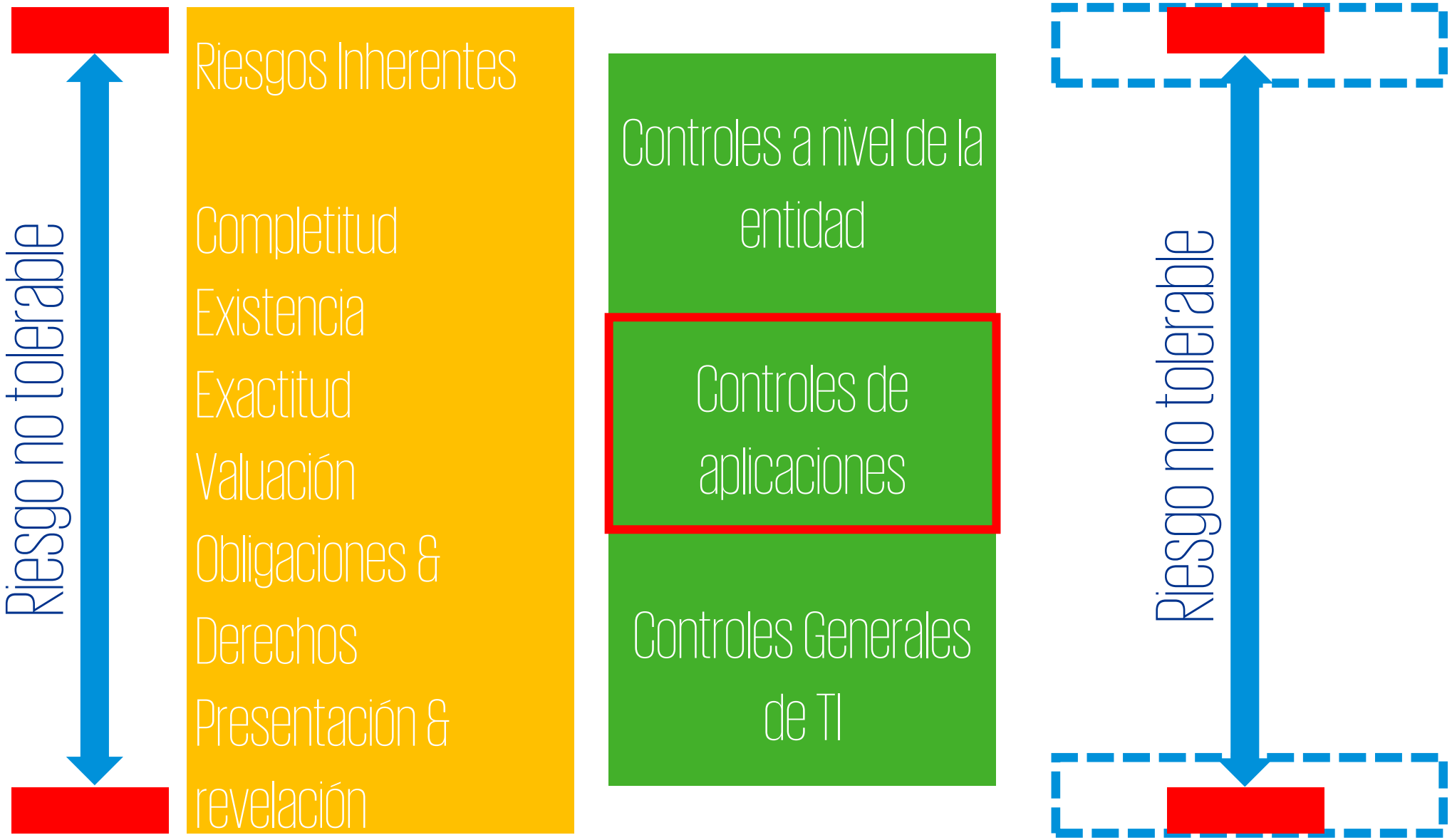
“.B3 Alternatively, a company might use automated procedures to initiate, record, process, and report transactions, in which case records in electronic format would replace paper documents. When IT is used to initiate, record, process, and report transactions, the IT systems and programs may include controls related to the relevant assertions of significant accounts and disclosures or may be critical to the effective functioning of manual controls that depend on IT. ”

TI en el reporte de estados financieros

Controles a nivel de las aplicaciones

Controles Generales de TI

Definición de riesgo ICOFR



Áreas de enfoque PCAOB

Ciclo de inspecciones 2014

Auditorías de ICOFR

- Comprender el flujo de transacciones en la compañía
- Prueba de controles relevantes de gestión
- Prueba de datos e informes usados en controles

Evaluar y responder al riesgo, particularmente cuando se trata de un riesgo significativo (incluido el riesgo de fraude).

Auditoría de estimaciones contables

Ciclo de inspecciones 2015

Más ICOFR

Riesgos ambientales

- Actividad de fusiones y adquisiciones
- Impuesto sobre la renta
- Retorno de inversión
- Precios del Crudo
- Estado de flujos de efectivo

Big data y pruebas a población completas

Riesgos de seguridad cibernética

Estándares de agente de bolsa

Ciclo de inspecciones 2016

Más ICOFR

Precisión de controles (SAPA 11)

Controles sobre informes y datos generados por el sistema

Procesos Vs controles

GITC

SAPA 11

Estimados

Ingresos

Continuidad del negocio

Agentes de bolsa

Ciclo de inspecciones 2017

ICOFR, ICOFR y más ICOFR!

- SAPA 11

Evaluar y responder a los riesgos de error del material

Estimaciones contables, incluidas las mediciones de valor razonable

Combinaciones de negocios determinación de activos reservas

Partes relacionadas

Independencia de auditor

Activos financieros

Nuevos estándares de contabilidad

Arrendamientos

Continuidad del negocio

Elementos COSO

Actividades de control

10/ La organización elige y desarrolla **actividades de control que contribuyen a la mitigación de riesgos** para el logro de objetivos a niveles aceptables. **(6)**

11/ La organización elige y desarrolla **actividades de control generales sobre la tecnología** para apoyar el cumplimiento de los objetivos. **(4)**

12/ La organización **despliega actividades de control a través de políticas** que establecen lo que se espera **y procedimientos** que ponen dichas políticas en acción. **(6)**

COBIT

DSS 06

DSS06.1/ Alinear las actividades de control embebidas en los procesos de negocio con los objetivos de negocio

DSS06.2/ Control del procesamiento de información

DSS06.3/ Administrar los roles, responsabilidades y niveles de autoridad

DSS06.4/ Administrar los errores y excepciones

DSS06.5/ Asegurar la trazabilidad de los eventos de la información y responsables

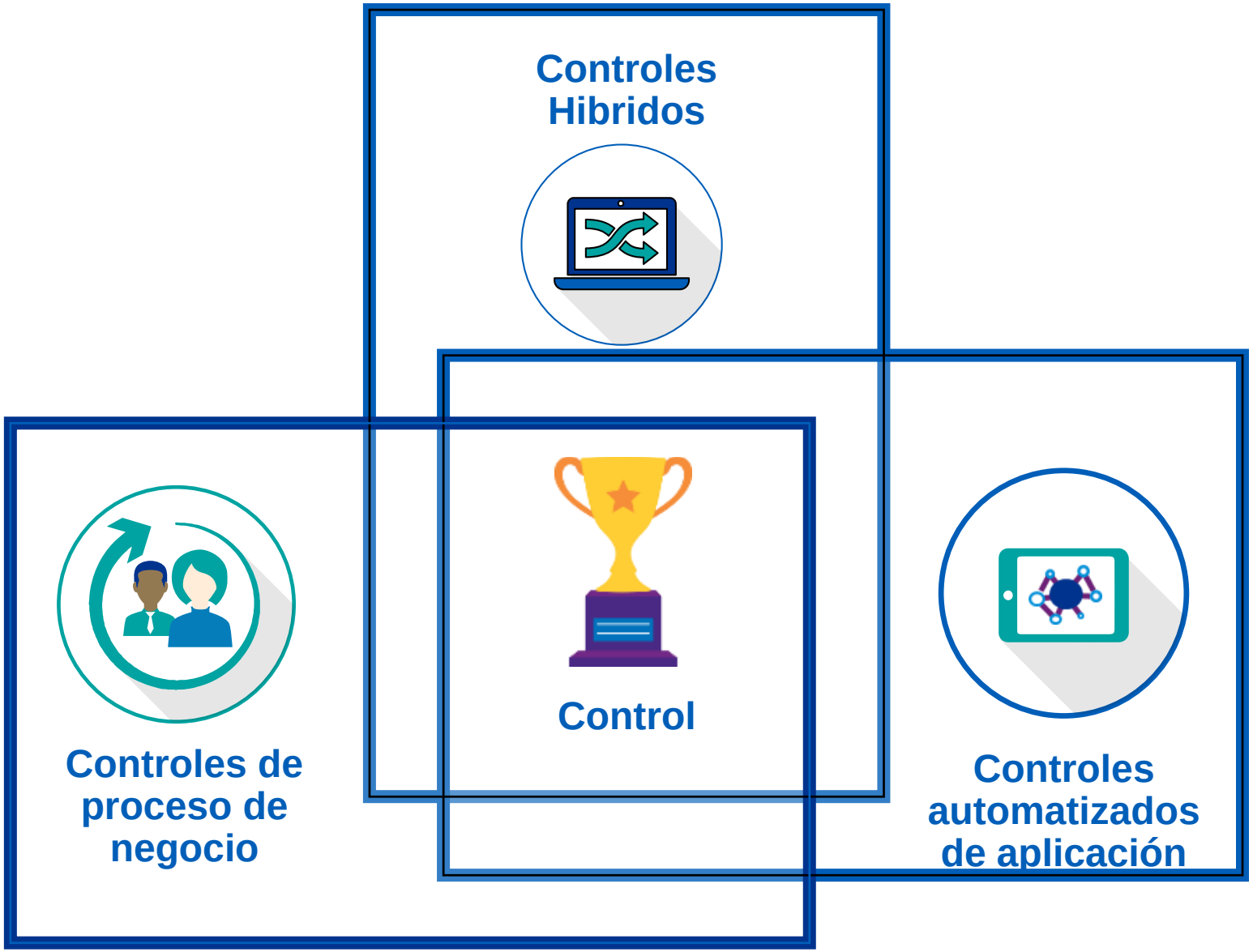
DSS06.6/ Asegurar los activos de información

Ejemplos de controles de aplicación

Ejemplo de controles de aplicación

Acceso que obliga segregación de funciones

Tipos de control



Prueba de diseño e implementación

Evaluar el **diseño** de un control involucra considerar si el control, individual o en combinación con otro, es capaz de prevenir o detector o detectar y corregir efectivamente errores materiales

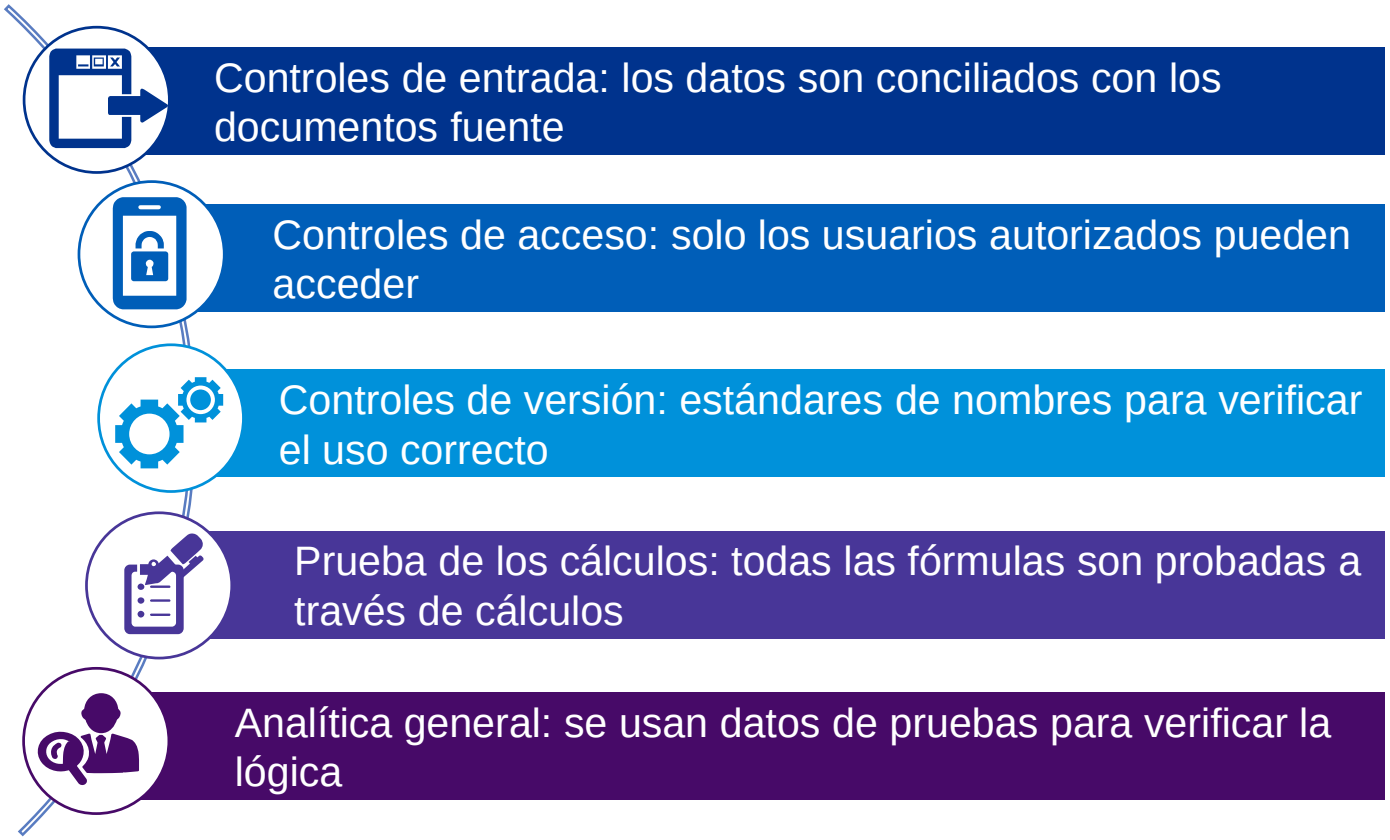
La **implementación** de un control significa que el control existe y que la entidad lo esta usando

Una **deficiencia de control** existe cuando el diseño o la implementación del control relevante es inefectiva. En este caso, nosotros no desarrollamos pruebas de eficacia operativa de dichos controles.

Computación de usuario final

EUC y otros documentos preparados por la Administración proveen un desafío único al grupo de controles. Por su naturaleza, la computación de usuario final Brinda el desarrollo y procesamiento de sistemas de información cercano a los usuarios. Este ambiente puede no ser sujeto al mismo nivel de control que las aplicaciones que procesan información. No obstante las salidas de la EUC pueden ser usadas por la administración en el reporte financiero y están sujetas a verificación de acuerdo con lo establecido por COSO.

Las EUC son a menudo más prevalentes en ambientes menos sofisticados de TI o en compañías pequeñas.
La importancia de las EUC han sido resaltadas e inspeccionadas por la SEC y su documentación ha estado entre los hot topics reportados por la PCACOB



Prueba de eficacia operativa

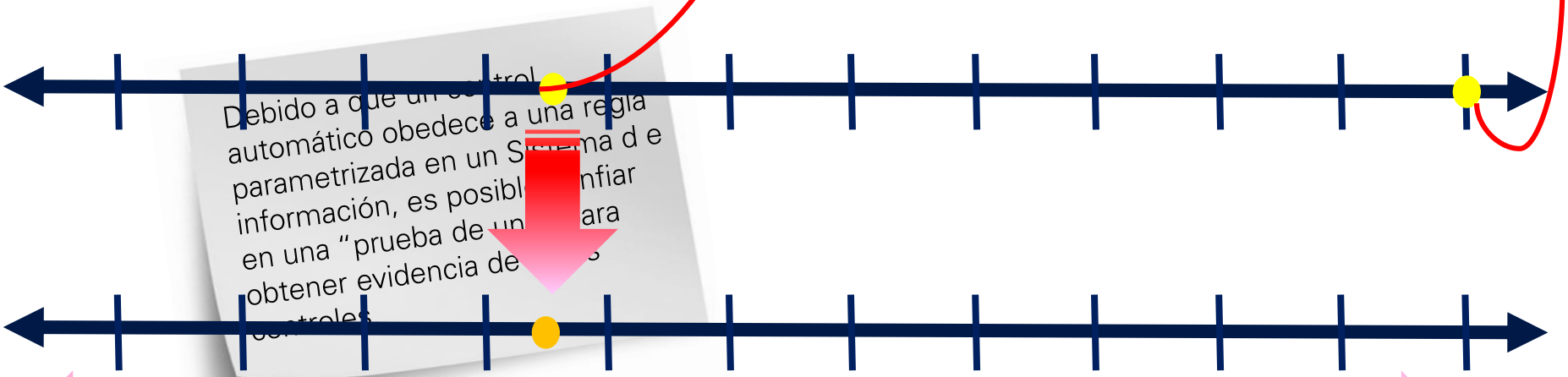
Evaluar la **eficacia operativa** de un control significa que el control opera de la forma en que esta diseñada e implementada por el período que se pretende cubrir.

“Prueba de uno” de un control automático ó parte automática de un control hibrido”

“…Regla parametrizada en un momento específico del período cubierto.

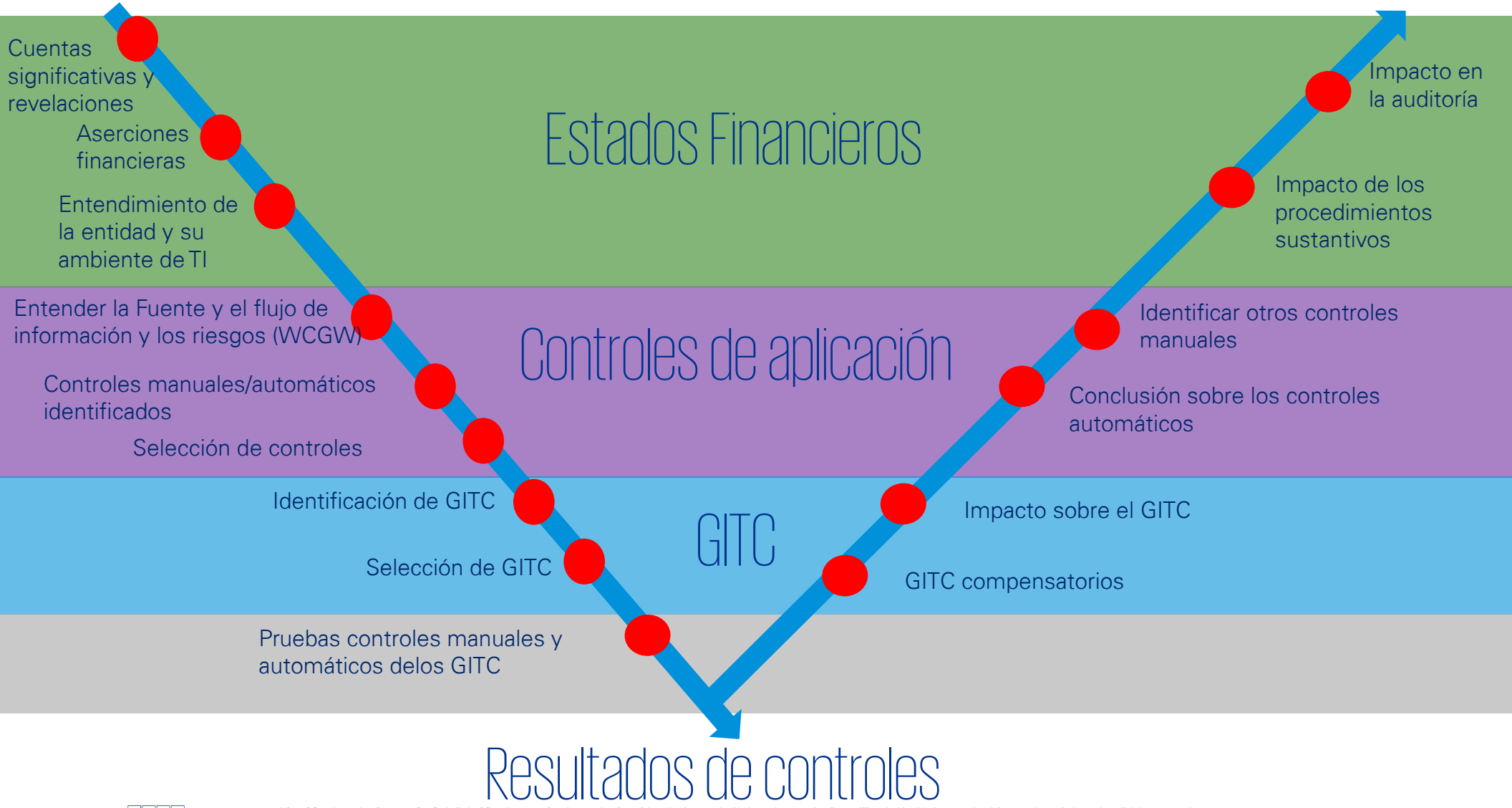
Procedimientos de Rollforward

Al final del período hay que verificar que el control continua funcionando.



Controles Generales de TI

Integrando TI en la auditoría



KPMG

Preguntas