



Faro de Auditoría

Boletín Flash del Comité
Latinoamericano de
Auditoría Interna (CLAIN)

FELABAN

No. 1 - Octubre 2015

IIA CMBOK: Reflexiones regionales: América Latina

Recientemente el IIA Global publicó la versión en español de uno de los 25 reportes que forma parte de las conclusiones del CBOK 2015 del Instituto de Auditores Internos Global; el estudio más grande de la profesión de auditoría del mundo que encuestó a más de 14 mil profesionales. En la muestra Latinoamericana, respondieron 1,460 profesionales.

Este estudio ya se puede solicitar al IAI de Ecuador (adjuntamos el link para la versión libre en inglés).

¿Sabía Usted que la región tiene la mitad de auditores certificados que el promedio mundial (43%)? ¿O que nuestros auditores tienen más años de experiencia que los del promedio global?

Más importante aún, este estudio nos permite tomar en consideración recomendaciones concretas “Puntos de actividad” en los campos de:

- Gestión de riesgos
- Relevancia en la organización
- Riesgos tecnológicos

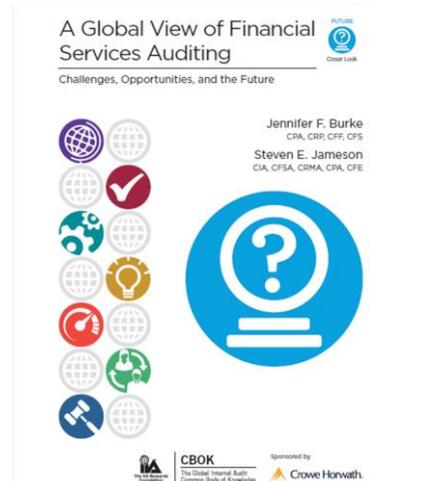
PCAOB: Sumario de inspecciones – octubre 2015

Hace 2 semanas el Public Company Accounting Oversight Board, ente creado por la Ley Sarbanes-Oxley para evaluar el trabajo y la independencia de los auditores externos, publicó su segundo sumario de observaciones encontradas durante su periodo regular de evaluación. El primero, estuvo dedicado a las empresas comisionistas de valores o *brokerage-firms*.

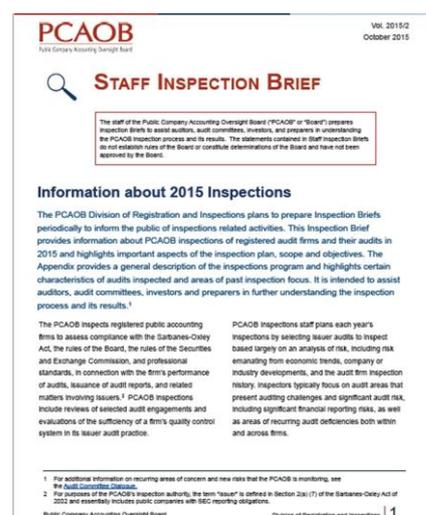
Conforme a este documento, las 3 áreas de deficiencias de auditoría recurrentes son:

- i. El control interno sobre el repoorte financiero
- ii. La evaluación y respuesta al riesgo de errores materiales
- iii. Estimaciones contables y medidas de valor razonable, sobre todo la información clave y los supuestos significativos utilizados para que la gerencia desarrolle sus estimaciones.

Asimismo el PCAOB recomienda poner énfasis en temas sensibles para su revisión como: fusiones y adquisiciones, reconocimiento de ingresos, activos no financieros, sobre todo el crédito mercantil, instrumentos financieros, entre otros. **¿Cómo nos impacta?** Sin duda los auditores externos, se voltearán hacia nosotros a solicitar pruebas de control.



[http://theiia.mkt5790.com/CBOK_Lat
in_America_Reflections/](http://theiia.mkt5790.com/CBOK_Lat_in_America_Reflections/)



[http://pcaobus.org/Inspections/Docu
ments/Inspection-Brief-2015-2-2015-
Inspections.pdf](http://pcaobus.org/Inspections/Documents/Inspection-Brief-2015-2-2015-Inspections.pdf)

IIA Financial Services Audit Center: 11 Temas de Ciberseguridad, que las instituciones financieras deben considerar hoy

Conforme al Instituto de Auditores Internos Global, la ciberseguridad es probablemente el tópico de TI más discutido entre ejecutivos, auditores internos, comités de auditoría y miembros del directorio. Por lo tanto ocupa el 1er lugar en la lista de nuestros 10 principales riesgos de tecnología (Navigating Technology's Top 10 Risk, Flora y Rai, CBOK, IIA 2015).

En el breve artículo de Centro de Servicios Financieros del IIA se ofrece un rápido checklist que los auditores podemos utilizar como guía para la evaluación de este importante, emergente y creciente riesgo: 1) Gobierno; 2) Gestión de los temas de ciberseguridad; 3) Recursos; 4) Riesgos compartidos por la infraestructura; 5) Autenticación multifactor; 6) Testeo de penetración; 7) Protección y respuesta ante la intrusión; 8) Entrenamiento; 9) Administración de proveedores externos, 10) Ciberseguridad y recuperación de desastres; y 11) Seguros de ciberseguridad.

Orientaciones sobre Principios de gobierno corporativo para bancos del Comité de Supervisión Bancaria de Basilea 2015

Durante este mes se publicó la versión en español de este documento emitido en julio del presente año.

En su introducción, Basilea considera que *“Un buen gobierno corporativo es esencial para el correcto funcionamiento del sector bancario y de la economía en su conjunto. Los bancos desempeñan un papel crucial en la economía mediante la intermediación de capital entre ahorradores y depositantes para actividades que fomentan el desarrollo empresarial y crecimiento económico. La seguridad y robustez de los bancos son clave para la estabilidad financiera, por lo que su forma de operar es fundamental para la solidez económica. Deficiencias en el gobierno de los bancos con una influencia significativa en el sistema financiero pueden provocar la transmisión de problemas al sector bancario y a la economía en su conjunto”*.

El documento presenta las orientaciones a través de 13 principios. El principio 10 se refiere a la función de auditoría interna de los bancos: *“La función de auditoría interna debe proporcionar aseguramiento independiente al Consejo y respaldar al Consejo y a la alta dirección en la promoción de un proceso de gobierno eficaz y la solidez a largo plazo del banco”*

PWC 2015 Estudio sobre el estado de la profesión de auditoría interna

Si bien este documento regularmente consultado fue emitido a mediados de año, sugerimos su revisión ; sobre todo por la casi unánime demanda del mayor uso de análisis de data en auditoría.

Figure 10: Internal audit's use of data analytics



11 CYBERSECURITY ISSUES FINANCIAL INSTITUTIONS SHOULD CONSIDER NOW

Regulatory guidance provides a useful cybersecurity checklist

1 GOVERNANCE, ORGANIZATION, AND REPORTING. Tone at the top matters on any key issue; cybersecurity is no exception. Consider these questions:

Does your board include members with sufficient understanding of cybersecurity and its interrelated technology and operational concerns to provide effective governance in this key area? Many bank boards, especially at local, community or regional banks, are composed of some members who may not have deep understanding of information technology (IT). Without that understanding, your board is not in a position to effectively evaluate or question your cybersecurity posture. This is a good time to consider the composition of your board. If you do not have a member or members with the right mix of IT and operational acumen to provide effective governance over cybersecurity, it may be time to consider the inclusion of those skills.

Of course, governance and reporting are not the province of your board alone. How integrated are IT issues, including cybersecurity, in your leadership structure?

How siloed is your leadership? Cybersecurity isn't just an IT issue. It can only be addressed effectively when it is addressed holistically. If your institution is treating cybersecurity like an IT issue, it's time to rethink your approach.

On Dec. 12, 2014, the New York State Department of Financial Services issued guidance on areas specific to cybersecurity on which it plans to focus in future examinations, stating, "The Department encourages all institutions to view cybersecurity as an integral aspect of their overall risk management strategy, rather than solely as a subset of information technology."

While these points may only be of immediate interest to New York financial institutions, federal regulators and regulators at the state level are all paying increasing attention to cybersecurity, and they are all likely to focus on a similar list of concerns; cybersecurity should be a top-of-mind strategic concern for every financial institution. The frequency and sophistication of cyberattacks continues to mushroom, and the potential ramifications to your organization of a successful attack are too serious to ignore.

The 11 areas of focus included in the New York guidance provide a useful checklist of cybersecurity concerns. So let's consider them one at a time.

<https://dl.theiia.org/FSAC/Knowledge-Brief-11-Cybersecurity-Issues.pdf>

Comité de Supervisión Bancaria de Basilea

Orientaciones

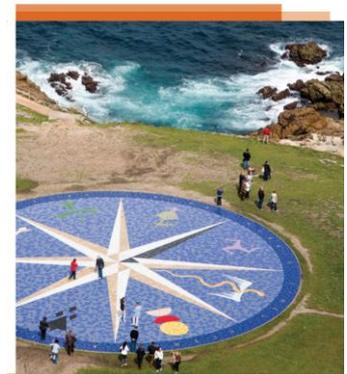
Principios de gobierno corporativo para bancos

Julio de 2015



https://www.bis.org/bcbs/publ/d328_es.pdf

2015 State of the Internal Audit Profession Study Finding True North in a period of rapid transformation



<http://www.pwc.com/gx/en/audit-services/publications/assets/pwc-2015-state-of-the-internal-audit-profession-study.pdf>