Basilea II: un gran incentivo a la gestión de riesgos

Introducción

En un seminario realizado en Washington entre el 1 y 3 de Junio de 2004 fue manifestado que: “Basilea II no es un complemento a la gestión de riesgos, es un marco regulatorio e incentiva la gestión de riesgos”. Suena importante. Más aún cuando quienes coincidieron en la afirmación fueron Alan Greenspan (FED) y Jaime Caruana (BIS).

Otro dato que empieza a darnos una idea de la dimensión de Basilea II es que los grandes bancos de Europa estiman presupuestos para implantarlo que van de 100 a 200 millones de euros en cada uno de ellos.

Este artículo pretende, en principio, informar a la comunidad de auditores en general (no solo bancarios) sobre el formidable impacto que tendrá Basilea II sobre la gestión de riesgos en los sistemas financieros y en las economías de los países y, por lo tanto, sobre nuestra profesión, cada vez más –correctamente - enfocada a la gestión de riesgos.

Qué es Basilea II?:

Cuando mencionamos a Basilea II nos referimos - en una suerte de simplificación – al Nuevo Acuerdo de Capital emitido por el Comité de Basilea que debe comenzar aplicarse a fines de 2006 y 2007 oficialmente y en prueba a partir de 2006 por los Bancos que indiquen los Bancos Centrales que adhieran al mismo.

Este comité tiene sede en la ciudad Suiza del mismo nombre y funciona en el edificio del BanK for International Settlements (BIS). El Comité de Basilea es también conocido como el “Banco Central de los Bancos Centrales” porque está integrado por representantes de los Bancos Centrales de más de 100 países miembros, entre ellos el Banco Central de la República Argentina. Debe aclararse que Basilea emite recomendaciones que orientan pero que no son mandatorias para los Supervisores Bancarios (léase bancos centrales) de cada país.

Ya sabemos que es Basilea, ahora por qué II?

Su antecesor, el Acuerdo de Capitales de Basilea (Basilea I), fue pronunciado en 1988 y entró en vigencia en 1992. En 15 años, el lector ya imaginará que este Comité no ha emitido sólo dos recomendaciones sino cientos. En efecto, es ésta una muestra más de la importancia que el mundo asigna al Nuevo Acuerdo al denominarlo Basilea II.

Basilea I, en su momento surgió como una exigencia de los países más industrializados para aumentar la solvencia de los sistemas financieros "nivelando para arriba". Su rotundo éxito se debió a la simplicidad de su aplicación y a que permitió uniformar criterios en una industria que internacionalmente se manejaba con criterios muy disímiles.

Entre los problemas más destacados que presenta es que su propia simpleza no permite una adecuada identificación de los verdaderos riesgos. No olvidemos que ha sido en la década de los '90 en la cual se produjeron avances notables en la medición y en la gestión de riesgos (modelos no contemplados por Basilea I).

Como resultado de esto paulatinamente se ha venido incrementando el desfasaje entre los negocios bancarios cada vez mayores y el capital regulado que permite cumplir con los objetivos de solvencia y eficiencia que persiguen justamente las regulaciones.

El reconocimiento de esta situación sumado a los nuevos modelos y tendencias internacionales en materia de riesgo y corporate governance han sido los disparadores materiales e intelectuales del Nuevo Acuerdo de Basilea.

Entre los objetivos que persigue Basilea II se destacan:

- Perfeccionar el acuerdo anterior;
- Promover la seguridad y la salud de los sistemas financieros;
- Fomentar la competencia en igualdad de condiciones;
- Definición de capitales mínimos regulados en base a criterios más sensibles al riesgo;
- Mejora en performance de los procesos bancarios: eficiencia;
- Mejorar la supervisión bancaria (a través de los Bancos Centrales);
- Transparencia en las informaciones.

Para lograr los objetivos mencionados Basilea II se basa en tres "pilares":

Los Pilares del Nuevo Acuerdo:

- **Pilar I. Requerimiento mínimo de capital:** persigue un adecuado gerenciamiento de riesgos por parte de las entidades bancarias fomentando el desarrollo de modelos de gestión de riesgos propietarios

- **Pilar II: Proceso de examen supervisor:** busca un doble objetivo de aumentar la fiscalización por parte de los Bancos Centrales a la vez de hacer más profesional la administración bancaria.

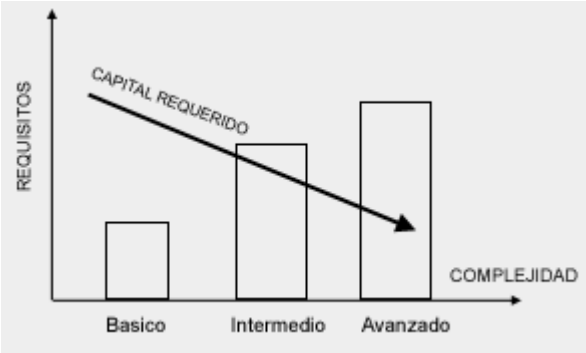
- **Pilar III: Disciplina de mercado:** se pretende uniformar la gestión de informaciones a brindar al mercado asegurando su corrección y transparencia.

Pilar I Requerimientos mínimos de Capital:

Sin entrar en cuestiones demasiado técnicas, no pretendidas en el desarrollo del presente artículo, mencionaremos que Basilea II no presenta modificaciones en cuanto a regulaciones de capital para riesgo de mercado entendiendo que está adecuadamente cubierto con el Acuerdo anterior. Sí presenta importantes modificaciones para el riesgo de crédito e incorpora la gestión de riesgos operativos.

Adelantemos que, tanto en los requerimientos de capital regulatorio para riesgo crediticio como para riesgo operativo Basilea propone tres métodos para su implementación. Dichos métodos contienen diferente nivel de complejidad y requisitos. Los más simples son menos costosos en su implementación inicial pero requieren una mayor integración de capital porque los ponderadores de riesgos son más elevados. Los más desarrollados, además de la disminución en el capital total regulado, al tener mayores requisitos para su implementación se verán beneficiados en el mediano y largo plazo al obtener mayor eficiencia operativa mediante una mejor gestión de riesgos.

El siguiente cuadro demuestra lo antedicho:



Requerimiento de capital para Riesgo de Crédito:

En el método denominado estándar – el básico – se utilizan los ratings de las agencias calificadoras de riesgos (Basilea enuncia una serie de condiciones o requisitos que las calificadoras deben cumplir para que los Bancos Centrales las admitan como tales). Luego a cada calificación dividida por tipo de crédito (con Gobiernos soberanos, interbancario, con empresas, etc.) se le aplica un ponderador de riesgo que Basilea define. Ejemplo: por un crédito interbancario calificado desde AAA a AA- debe aplicarse un ponderador de riesgo del 20%. Simple pero muy caro.

En el método basado en ratings internos (IRB) – el intermedio - debe considerarse la probabilidad de default o incumplimiento dada básicamente por el análisis de elementos indicativos de la probabilidad que el deudor no pague totalmente su crédito y por el nivel morosidad.

Finalmente el método IRB avanzado, establece otro tipo de medición utilizando como ponderador de riesgo la tasa de recupero de los créditos del propio banco. Esto tiene un importante significado en términos de performance de la gestión crediticia incluyendo su recupero mediante la cobranza porque dicha tasa dependerá de cómo actuó el Banco a lo largo de varios años y no dependerá de situaciones o mediciones puntuales.

En este método se considera pérdida económica aquélla relacionada con las obligaciones principales e intereses no cobrados, las quitas y descuentos realizados y todos los costos directos o indirectos incurridos para el recupero del activo.

Para los distintos métodos Basilea prevé un amplio menú de mitigadores de riesgos incluyendo garantías, colaterales financieros (la norma explicita que activos pueden ser utilizados como colaterales) y, aún, se pueden compensar créditos y deudas de una misma contraparte.

Requerimiento de capital para Riesgo Operativo:

En este caso en el método básico la previsión por riesgo operativo importa simplemente calcular el 15% del Resultado bruto de la entidad. Muy caro, verdad?

Una variante tampoco demasiado feliz es la del método estándar (el intermedio del gráfico) que fija porcentajes a aplicar al resultado bruto por línea de negocio según el siguiente detalle:

Líneas de Negocio	Valor
Finanzas corporativas	18%
Negociación y ventas	18%
Banca minorista	12%
Banca comercial	15%
Liquidaciones y pagos	18%
Servicios de agencias	15%
Administración de activos	12%
Intermediación minorista	12%

Por último, aparece el **método avanzado** (AMA) con las principales innovaciones y mejoras. En este caso el capital regulatorio surge como

resultado de aplicar sistemas de gestión de riesgos propietarios suficientemente desarrollados cuyas estimaciones de pérdidas deberán considerar fallas internas y externas, madurez del ambiente de control interno, análisis de escenarios, entorno de negocios y, con un intervalo de confianza del 99.9%, calcular las estimaciones como sumatoria de las pérdidas esperadas y no esperadas por la organización. Más barato pero mucho más complejo.

Los Supervisores bancarios exigirán a las entidades para poder adoptar este método, además de la solidez del modelo a aplicar, el cumplimiento de requisitos cualitativos de admisión, tales como:

- Consejo Directivo y los principales ejecutivos involucrados en la gestión de riesgos;
- La existencia de función de gestión de riesgo operacional independiente, responsable por la implementación de la estructura de riesgo operacional de la institución;
- Integración del sistema de medición de riesgo en la rutina diaria de gerenciamiento de riesgo;
- Proceso de reporte regular a la gerencia de la unidad de negocios, ejecutivos y Consejo Directivo;
- Existencia de sistemas para documentar, monitorear y gerenciar los riesgos;
- Validación del sistema de medición de riesgo por los organismos reguladores y por la auditoría externa

Pilar II: Proceso de examen supervisor:

Mediante 4 principios se exige a los Bancos contar con un proceso permanente que permita evaluar la suficiencia de capital total y se pretende de los Supervisores Bancarios la facultad de fiscalización, de exigencia de medidas correctivas cuando fuere necesario y en su caso intervenir las entidades que no cumplan con los requerimientos de capital.

Pilar III: Disciplina de mercado:

Establece la necesidad de contar con una política formal de divulgación de las informaciones que permitirá a los usuarios evaluar aspectos básicos referidos a:

- El ámbito de aplicación;
- Las exposiciones al riesgo;
- Los procesos de evaluación del riesgo;
- La suficiencia de capital de la institución

La entidad debe contar con un proceso de evaluación permanente de dicha política.

Quién debe aplicar Basilea II:

La letra fría del acuerdo obliga a los Bancos que son internacionalmente activos. Previendo distintos niveles de consolidación de riesgos para todas las inversiones del conglomerado financiero, ya sea en Bancos locales, Sociedades de valores, otras entidades financieras controladas, compañías de seguros, y hasta participaciones en sociedades comerciales.

Entonces surge la siguiente pregunta: una organización que no pertenece al grupo anterior no debería preocuparse por Basilea II?

Europa ya ha decidido implantar el Nuevo Acuerdo en todos los Bancos independientemente que sean internacionales o no, en principio para uniformar el sistema financiero y permitir a nivel macro contar con un sistema solvente y que contribuya al desarrollo económico de los países y, a nivel micro, evitar que aquéllos Bancos que no lo implanten y permanezcan en Basilea I pierdan competitividad respecto de aquéllos que implanten Basilea II.

Este razonamiento es totalmente trasladable a América Latina que sufrirá posibles consecuencias de fragmentación de su sistema financiero. Es decir, si el Banco Central de un país no obliga a implantar Basilea II puede ocurrir que los Bancos de capitales nacionales continúen con Basilea I y que los de capitales extranjeros lo implanten o no en función de las exigencias de sus casas matrices.

Por otra parte, se entiende que las entidades que utilicen modelos de gestión de riesgos antiguo no tendrán la misma calificación crediticia que las de Basilea II con lo cual su acceso al crédito se verá dificultado y con la necesidad de pagar sobretasas compensatorias por trasladar al prestador un mayor nivel de riesgo.

Basilea II afectará sólo a los Bancos?

Es indudable la influencia que tiene el sistema financiero en la actividad económica y en las posibilidades de desarrollo de un país. En general los países importadores de capital pueden verse perjudicados en la medida que los tomadores no puedan demostrar que tienen una adecuada gestión de riesgos.

Ahora bien, si analizamos la cuestión desde un punto de vista de cada organización en particular y –de paso- respecto de la profesión de Auditor en particular, es fácil percibir que para los nuevos modelos de

gestión de riesgos (COSO-ERM por ejemplo), Basilea II presenta un incentivo muy importante y la vez una base conceptual para comenzar a gerenciar riesgos de una forma más adecuada.

Es claro que los riesgos de mercado y de crédito no hacen al negocio principal de una explotación industrial o comercial sin embargo estas podrían aprovechar muchas lecciones sobre riesgo operacional. Todas ellas sufren (o pueden sufrir) fraudes internos o externos, fallas tecnológicas, productos mal diseñados, errores en la gestión de clientes, siniestros, errores de procesamiento, etc.

Por otra parte, presentar un mejor perfil de riesgo por parte de una Empresa puede ser importante a la hora de negociar condiciones con los Bancos. Explicamos que Basilea II propone calificar los riesgos de crédito en base a su tasa de recupero por lo cual los Bancos que lo apliquen van a preferir los clientes sanos en cuanto a riesgo ya que un cliente que presente problemas de pago va a afectar su tasa de recupero por años. Sin duda la mayor demanda de clientes con buen perfil de riesgos va a generar una competencia a nivel de pricing.

Cuál es la contribución que puede hacer la Auditoría:

Los auditores siempre hemos dicho que los halagos por las excelentes campañas comerciales que terminaron hoy habría que corroborarla con los resultados que producirán en los próximos meses cuando se pretenda recuperar el activo. De alguna manera Basilea II vino a darnos la razón.

El Auditor tanto Interno como Externo debe informarse y formarse para poder cumplir los requerimientos de auditar el proceso de gestión de riesgos en general y los requisitos del pilar 3 que está muy alineado a la Ley Sarbanes Oxley.

Por otra parte Basilea representa una excelente oportunidad para incentivar en cada organización un enfoque gerencial administrando riesgos. En este sentido, el Auditor Interno puede convertirse en el campeón de riesgos en las organizaciones que no cuentan con un Risk Officer y en aquéllas que ya cuentan con esa estructura será un usuario e interlocutor calificado de todo lo que esa gerencia produzca.

Cuál es la situación en Argentina:

El Banco Central de la República Argentina no ha regulado sobre la materia ni se ha pronunciado en forma oficial. La situación actual del sistema financiero argentino y los empobrecidos patrimonios de los principales bancos hacen pensar que no hay intención seria por parte del BCRA de hacerles invertir mucho dinero en estos temas. Con un sistema financiero argentino que recién está comenzando a salir de un

riesgo de tipo sistémico es entendible que no se apuren los tiempos para grandes cambios en riesgo de crédito y comenzar a medir riesgo operacional.

No obstante, en Abril de 2004 el Ministerio de Economía emitió el Decreto 476/04 que, basado en la Directiva 2002/87/CE emitida por el Parlamento Europeo en relación a la Supervisión adicional de los conglomerados financieros crea el Gabinete de Coordinación de Regulación y Supervisión Financiera.

Dentro de los considerandos, el decreto textualmente menciona que "resulta conveniente considerar las modernas recomendaciones emanadas del Foro conjunto de Conglomerados Financieros, integrado por el Comité de Basilea para la Supervisión Bancaria, la Organización Internacional de Comisiones de Valores y la Asociación Internacional de Supervisores de Seguros, sobre medidas de capital, coordinación entre supervisores e intercambio de informaciones".

Una de las funciones del Gabinete será la de "propiciar la adopción de medidas acordes a las tendencias regulatorias internacionales para los sectores regulados por los organismos representados" (entre ellos el BCRA).

Conclusiones:

El Nuevo Acuerdo de Capitales presenta notorias ventajas respecto del anterior permitiendo una mejor relación entre capital económico y regulatorio.

Esto se logrará ya que impulsa una gestión de riesgos moderna que incluye:

- La utilización de sistemas integrados de gestión de riesgos de crédito, mercado y operacional;
- La utilización de indicadores que permitan gestión de riesgos en el día a día;
- Herramientas de estimación de pérdidas futuras;
- El compromiso de la Alta Dirección con la gestión de Riesgos; y
- La figura del Risk Officer exigiendo una oficina de riesgos totalmente independiente de la gestión operativa.

Por otra parte se alinea también con los modelos más desarrollados de Corporate Governance en su tercer pilar al fomentar la uniformidad de informes financieros y su transparencia.

La mejora en la gestión de riesgos y una mayor transparencia en las informaciones es importante para la sociedad en su conjunto porque ayudan a mejorar la salud y la solvencia del sistema financiero. A la vez

el incentivo a mejorar los niveles de eficiencia en general hace a dicho sistema más competitivo y con un mejor nivel de servicio para los usuarios.

Finalmente creo que los Auditores no debemos dejar de lado la oportunidad de alinearnos con los avances en materia de gestión de riesgos ya que es una materia que siempre hemos impulsado y que obviamente traerá beneficios directos e indirectos a la profesión.

ERM como base del gobierno corporativo

Las exigencias de mercado y regulatorias - Parte II (1)

Incumbencias de Auditoría y ERM

A continuación, entramos en un tópico nuevo: las incumbencias de Auditoría y de ERM. Algunos las tenemos bastante claras, pero suelen no estar claras en general en el mercado. Roles y responsabilidades: todos en la empresa tienen responsabilidad en ERM: el Comité Ejecutivo, la Gerencia de línea, los risk officers, los auditores, el compliance officer y el personal. Todos están involucrados, de modo tal que acá el plan de training y de involucramiento y de distribución de roles tiene que ser completo. A ERM no lo hace uno solo.

Veamos el Estándar 2110.A1 del IIA: “Auditoría Interna tiene que monitorear y evaluar —no hacer— la efectividad del gerenciamiento de riesgos en la organización”. Acá está la separación entre lo que tiene que hacer Auditoría y lo que tiene que hacer la línea como gerenciamiento de riesgo. Hay una opinión similar enunciada en el Código Combinado, que acaba de revisarse en 2003, y también en el Informe Turnbull de 1999. Las normas que nosotros acabamos de recibir de Boston en el Banco también hablan de esto y hay un párrafo subrayado que dice que es la línea la que tiene que hacer todo esto, respaldada por assurance o por ERM, pero no por Auditoría. Y lo tiene así porque está escrito en las nuevas regulaciones, con lo cual se vuelve a lo básico, a que Auditoría, después de la SarbOx, debe poner más énfasis en lo contable. Todos queremos hacer más pero no podemos ser auditores, advisories, hacer gestión de riesgo, ser compliance officers, tener toda una gama de cosas que nos desvía del objetivo contable que finalmente es el que tenemos que asegurar (los auditores)

En esta diapositiva hay un párrafo que está traducido literalmente. Resulta que la filial del Reino Unido del Instituto de Auditores Internos lleva mucho la directiva en esto y, a pesar de que es un capítulo que por supuesto depende de la central mundial, se maneja en forma bastante independiente y a mí me consta a través de muchos años de seguimiento que es líder en esto y emite una serie de documentos que se llaman position statements. La opinión formal del Instituto sobre ERM: Auditoría Interna debe permanecer independiente y debe verse así en todo momento del proceso de gerenciamiento, es decir, debe ser y debe verse así. Opina que la responsabilidad primaria del gerenciamiento es de la línea y que los auditores internos no deben gerenciar riesgos y su responsabilidad es evaluar el proceso como cualquier otro proceso. Así se expidió en 2002 —hace menos de un año— el Instituto.

Organigramas -Gran Corporación

En este esquema vemos cómo algunas corporaciones tienen embebido el tema de gerenciamiento del riesgo: acá está el directorio; el CEO; acá está el Comité de Riesgos con funciones que vamos a detallar en un momento; aquí se encuentra el risk officer, y acá están las líneas de negocios. Como ven, Auditoría tiene incumbencia de control y de evaluación en todo excepto en el Directorio. El resto está bajo el control de Auditoría, con lo cual los risk officers somos evaluados por ella. Éste es el esquema claro de compañías estadounidenses e inglesas.

Ahora bien, como ERM trae algunas resistencias y es muy nuevo, se han hecho montones de consultas y también el mismo Instituto, en su filial del Reino Unido, dentro del mismo position paper ofrece este otro esquema en forma transitoria hasta que se arranque con el esquema y el RO camine solo, digamos. Acá están el Directorio, el CEO y demás, y por otro lado está el Comité de Auditoría, con el número uno de Auditoría (CAE) que tiene Auditoría propiamente dicha y Risk Management. Son dos unidades separadas pero que reportan a un mismo director ejecutivo. Esto está aceptado como transición, pero exige alguien totalmente posicionado en la empresa, independiente, ético y con todas las cualidades habidas y por haber. Además, es transitorio hasta que esta parte pase a la línea. ¿Por qué está puesto así? Porque, como hablábamos al comienzo, toda esta parte de la empresa, de gobierno corporativo, no conoce qué es ERM, no leyó el informe, a veces ni siquiera leyó el COSO de 1992, por lo que ésta es una manera de que esto comience a ser aceptado. Así como el COSO llevó un tiempo en madurar, esto también va a llevar un tiempo de maduración, pero va a ser mucho más breve por lo que vamos a ver ahora.

El Reporte COSO ERM 2004

Pasemos al Informe COSO 2004. Hasta el 15 de octubre estuvo en borrador, en exposure draft, para poder opinar. Se piensa poner en práctica a comienzos de 2004. Es similar al COSO de 1992, aunque no será obligatorio para todos, pero seguramente se seguirá el criterio inglés del Código Combinado en el sentido de que algo debería cumplirse pero, si no se cumple, hay que explicar por qué. O sea, el Código dice: “Las empresas deberían cumplir con esto. Si no lo cumplen, expliquen por qué”. De hecho, el COSO es “obligatorio” para los que coticen en la Bolsa de Londres, pues explicar “porqué no” no es aceptado en los mercados. Presten atención a este dato que es de KPMG, también del Reino Unido: el 80% de los administradores de capitales pagan más por acciones de empresas con demostración efectiva de manejo de riesgos en un promedio del 11% de plus. Uno de los expositores anteriormente también mencionó algo parecido, sólo

que de McKinsey. Al oírlo, recordé esto que dice KPMG en un documento llamado “Asset Managers Pay More for Well Governed Companies”. En otras palabras, esto va a ser de aplicación mucho más acelerada que el Código y que el COSO de 1992 porque atrás hay muchas normas que lo están pidiendo.

Relación entre ERM y las regulaciones post-Enron

El COSO 2004 deberá aplicarse inmediatamente y será la base de sustentación de la Ley Sarbanes-Oxley. En casi todo lo que nos llega de nuestras casas matrices, vemos que dicen: “Te envío todo esto del proyecto SarbOx. Básalo en el COSO”. Lo evaluará la SEC cuando venga, sin dudas. También se exige para los que coticen en el London Stock Exchange. Será el apoyo del CEO y del CFO para certificar. Será materia prima de Auditoría Interna en las evaluaciones; Auditoría vendrá y preguntará: “¿Cómo está evaluando, documentando, etcétera, este riesgo?”. Servirá para asistir al Board en el cumplimiento del corporate governance. Y fíjense en el último bullet de la diapositiva: el Decreto 677/01 dice expresamente en el artículo 15-C que el Comité de Auditoría debe supervisar la aplicación de las políticas sobre la gestión de riesgos de la sociedad. Esto está literalmente tomado del 15-C, y puede que después del 28 de mayo y durante 2004 alguien tome conciencia de este artículo y quizás empiece a mirar hacia atrás para ver qué tiene que hacer en Argentina.

El Risk Champion

Llegamos a la definición del COSO, de ERM, de qué es el risk officer: es alguien que trabaja con otros gerentes para establecer y mantener un efectivo gerenciamiento de riesgos en sus áreas de responsabilidad. Tiene responsabilidad de monitoreo, asiste, releva información, es miembro del Comité de Riesgos, pero básicamente trabaja con la demás gente, porque dijimos que los involucrados en esto son todas las personas de la compañía, desde el primero al último, y es el nexo clave entre la línea —la línea es la que está en el día a día— y los evaluadores. Ya dijimos quiénes son los evaluadores: la SEC, el Banco Central, la OCC, el evaluador de riesgos, el evaluador de mercado. Esta persona, el risk officer, es el nexo clave. Fíjense que desde el punto de vista de Auditoría, ésta es la persona que tiene que garantizar el verde de los reportes. Si esta estructura no está, Auditoría va directamente a la línea en un esquema duro. Pero aquí tenemos una figura intermedia que tiene que ir de la mano con la línea y garantizar que los reportes salgan lo más verdes posible. Y es así porque, tarde o temprano, esto llega al accionista.

Las responsabilidades del risk officer son: 1) Establecer las políticas de ERM; tiene que haber política, tiene que haber roles, tiene que implementarse ERM. 2) Constituir la autoridad para RM. 3) Promocionar

la competencia en ERM a través de toda la organización. 4) Integrar ERM con el resto del planeamiento de la empresa; la empresa tiene plan estratégico, tiene todo un plan que va desde los planes en palabras hasta los presupuestos en números y esto tiene que estar integrado; es decir, yo no puedo pretender ver un riesgo que no esté integrado con mi presupuesto de ganancias, de gastos y demás. 5) Establecer un lenguaje común de ERM, el cual incluye mediciones; estas mediciones tienen que ser claras y la línea tiene que saber cómo se los va a medir. 6) Tiene que desarrollar planes de acción para corregir lo que sea corregible. 7) Tiene que hacer reportes de riesgo. 8) Debe reportar al Comité de Riesgos. Uno de los mayores headhunters de esta especialidad está en el Reino Unido, que siempre es el líder en esto: Barclay Simpson, cuya dirección es www.barclaysimpson.co.uk. Yo he estado mirando el sitio y hay muchísimas búsquedas de Risk Managers.

Modelando, midiendo y cubriendo el riesgo

Seguimos con el COSO ERM: debemos modelar, medir y cubrir el riesgo. Primero hay que mirar el entorno interno de la compañía: cuál es la filosofía del gerenciamiento, si se le da importancia o no, qué cultura de riesgos tiene, qué dice el Comité Ejecutivo, qué integridad y qué valores éticos hay, qué compromiso existe con la competencia, cuál es la filosofía de la Gerencia y el estilo operativo —hay un estilo operativo en cada país, en cada empresa—, qué apetito de riesgos tiene, cuál es la estructura organizacional, cómo es la asignación de autoridad y responsabilidad, cuáles son las políticas y prácticas de recursos humanos. De manera que primero hay que ver todo el entorno interno antes de establecer la política.

Luego está el establecimiento de objetivos. Primero, los objetivos estratégicos, los riesgos relacionados con la estrategia. Los objetivos relacionados, es decir, no hay ningún riesgo ni intención de control que estén aislados en la compañía; todo es una sinergia de cosas y una cadena. No hay que perder esta relación porque, si lo hacemos, corremos el riesgo de que nos digan: “Este objetivo está priorizado por encima del otro”. Por eso tenemos que seleccionar qué ver a través del apetito y la tolerancia de riesgos: evitar, reducir, transferir, asumir.

Tenemos que identificar los eventos. Cuáles son los eventos. Cuáles son los factores que influyen sobre la estrategia: los económicos, los naturales, los políticos. Acá debemos tener mucha información. No podemos estar dentro de una oficina y hacer esto en un laboratorio; hace falta comunicación con todo el mundo. Cuáles son las metodologías y técnicas. Cómo es la interdependencia de los eventos, sobre lo que hablábamos recién. Cuáles son las categorías de eventos; priorización. Cuáles son los riesgos y las oportunidades.

Esta diapositiva se refiere a la evaluación de riesgos. Quizá la palabra self-assessment les suene de auditoría, pero aquí no se está hablado desde el punto de vista de auditoría y de las matrices. Se trata del riesgo más profundo y no de revisarlo una o dos veces al año o cuatrimestralmente, sino la evaluación de riesgo continua. Los riesgos inherentes y residuales. La probabilidad de que ocurran o no, la apariencia —pueden estar disfrazados o no— y otra vez el tema de la visibilidad, que es el riesgo oculto.

En cuanto a la respuesta al riesgo, hay que identificarlas, evaluar las diferentes respuestas posibles, seleccionar las respuestas y visión de portafolio. Seguramente hay muchas respuestas de riesgo y hay que consensuarlas, verlas, aceptarlas y, después, monitorearlas de acuerdo con lo que se haya consensuado en la respuesta. Yo no puedo ponerle a mi matriz cualquier cosa porque después el director de la línea pregunta porqué.

Actividades de control: integración con la respuesta, de acuerdo con lo que hayamos definido; tipos de actividades de control y temas que son ya sabidos.

Seguidamente, tenemos la etapa de información o comunicación. Mucha información, porque es relevante para el proceso de la toma de decisiones y es brindar un mensaje. Y la comunicación, que es para confirmar objetivos, orientar esfuerzos y generar sinergias, y es para cambiar un comportamiento. Es decir, si yo les comunico algo, es porque pretendo y espero que actúen de la forma comunicada. Y, otra vez, la estrategia y la integración.

Monitoreo: evaluaciones separadas; evaluaciones dinámicas; quién evalúa, y este último bullet que es el más importante: ERM es un proceso de evaluación en sí mismo, es decir, todo el proceso, que es continuo y que tiene los pasos que nombramos y que se amplían cada día.

Mediciones

Pasemos a analizar algunas herramientas de evaluación. El VAR (Value at Risk): en realidad esto está puesto para activos, tasas, retornos, pero puede ser para cualquier tipo de cosa financiera. No necesariamente para un banco. Puede ser la parte financiera de cualquier empresa que mueve valores. Es la peor pérdida esperada en un intervalo de tiempo bajo condiciones de mercado normales. Es decir, es el valor —$100— afectado por el riesgo: quizás el valor sea $98 si el riesgo es poco, quizá sea $50 si está muy expuesto al riesgo. Pero debemos saber que nuestros activos pueden reducirse en su valor con respecto al riesgo.

El RAC o capital ajustado por riesgo: también acá vamos a ver muchos conceptos de Basilea, Basilea es un Comité para Bancos que dicta

normas de gerenciamiento de riesgo, entre otras, fundamentalmente riesgo de crédito y riesgo operacional, y donde básicamente tenemos que mostrar capitales de acuerdo con exigencias de exposición al riesgo.

Los stress tests: es llevar a valores extremos algunas medidas para ver qué riesgo máximo puedo tener. Puede que llevándolo al extremo no tenga nada que hacer porque el valor extremo es pequeño.

Sensibilidad: es decir, ¿varió algo? ¿Varía lo demás? ¿O se queda estable?

Pérdidas en diversos casos supuestos y reales. Lo que hay que hacer aquí es cargar una base de pérdidas y de las causas de las pérdidas. Yo puedo presuponer cosas y ver qué pérdida tendría “en caso de”. Esto también se pide mucho para Bancos: las pérdidas y el porqué.

Medidas de concentración: si el riesgo está concentrado, está disperso, dónde está.

Medidas de correlación: aquí se ponen en juego fórmulas matemáticas, que tal vez no son tan importantes como el sentido común.

Revisiones de procesos y walkthrough, que es “caminar a través de”. Acá hay que revisar un proceso desde que nace hasta que muere y ver dónde están los riesgos.

Más mediciones: Las famosas matrices de riesgo que ya conocemos. Los perfiles de riesgo o scorecards, es decir, tratar de hacer cuantitativo algo que en el origen fue cualitativo y dibujar un planito de cosas para que nada quede aislado. Los famosos indicadores clave de performance, de riesgo, u otros.
Los límites; por ejemplo, le doy al cliente hasta tal límite de dinero, pongo mis sistemas hasta tal pago por caja, pongo en el ATM hasta $1000 por día, no considero lavado de dinero hasta tal monto; es decir, todo tipo de límites. Todos los Sistemas de Información Gerencial (MIS), que son una herramienta para RM si están bien hechos, lógicamente. Las bases de pérdidas centrales sobre las que ya hablé. Los informes de eventos de riesgo; acá nosotros tenemos este tipo de informes y en realidad hay que declarar cuando ocurre un evento de riesgo, ya sea que termine en pérdida o no, para ver cuál es la debilidad y qué hacemos en consecuencia, y eso es bueno.
Las bases de open issues o de problemas abiertos: seguramente va a haber que tener esto disponible para las exigencias de la SarbOx, más allá del disclosure o no y de que sea interno o no, o que sea para la Alta Gerencia, pero debemos tener una base donde queden claros todos los problemas de la empresa; podemos tenerlos en Auditoría o en ERM, es lo mismo, pero los problemas tienen que estar ahí; no puede haber cosas ocultas porque el espíritu de todas estas nuevas leyes es justamente la transparencia. Un proceso de assurance continuo; esto se

ve periódicamente, cuando cada tanto viene Auditoría, salvo que Auditoría tenga un monitoreo continuo a través de CSA, de indicadores y de otras cosas. Planes de acción correctivos que consten. Los estándares de calidad también nos sirven; todo esto es input que, si se consigue, me ayuda a gestionar el riesgo en la empresa.

Hacia dónde va el riesgo: sube, baja, qué me indican el mercado, la empresa, el proceso de fabricación; para eso hago un reporte de tendencia. ¿La calidad de esto es cada vez mejor? Entonces puedo monitorearlo de otra forma. La frecuencia, la severidad, las probabilidades. Cotejar los riesgos con el mercado ("mark to market") o cotejarlos con un modelo ("mark to model"); tengo dos formas de hacerlo, que pueden ser mixtas: tengo un modelo y quiero que mi riesgo se ajuste al modelo y lo que esté fuera del modelo es el desvío; otra forma es contra el mercado: consigo datos del mercado, puede que no sea lo óptimo pero el mercado lo tolera y bueno, estoy en el mercado. Un sistema detector de operaciones inusuales; nosotros, estamos implementando uno para el fraude con cheques; se trata de sistemas que detectan —en función de una inteligencia que el mismo sistema hace— cuáles son operaciones inusuales; i.e.: si tenemos una persona que es empleado y recibe su remuneración en el día 30 de cada mes; si la persona mueve dinero todos los días intermedios del mes y por una cifra mucho más grande, eso es inusual y tenemos que ver por qué. La calidad de datos: tiene que haber un quality assurance de sistemas; lo que sale de sistemas tiene que estar revisado, no puede salir así no más. Los gaps de control interno: planeamos esto pero hicimos otra cosa; Medidas de motivación de RRHH y grado de pertenencia a la empresa, Qué tanto motiva la empresa a su gente? Temas financieros: las famosas coberturas con otras monedas, derivados y swaps, pero esto ya es muy financiero. Los seguros y las garantías. El sentido común, que no debe olvidarse porque es lo más importante.

Basilea II

Aquí tenemos una diapositiva sobre Basilea II que, como les contaba, es para Bancos. Sin embargo, fíjense que el segundo bullet —"asegurar que la estructura de gerenciamiento de riesgos esté sujeta a auditoría interna operacionalmente independiente"— coincide con lo que dice el Instituto en cuanto a las incumbencias entre ERM y Auditoría. También hay que revisar la estrategia, aprobar la estructura, desarrollar las políticas, los procesos y los procedimientos; identificar el grado de exposición a las pérdidas. Basilea II, asimismo, propone cargos de capital de acuerdo con países, exposiciones al riesgo y demás.

Básicamente, en virtud de Basilea II se monitorean el riesgo de crédito y el riesgo operativo; lo que ocurre es que el operativo ya incluye a otros tantos. Esto ya es muy específico pero hay que medir probabilidad de incumplimiento, pérdida en caso de incumplimiento, exposición al riesgo, vencimiento... Con lo cual hay indicadores; por ejemplo, si

alguien no me paga ni siquiera la primera cuota del crédito, eso ya constituye un indicador de fraude. Acá hay ratios y, finalmente, esto deriva en provisiones y en esquemas contables.

Los métodos son: Para riesgo de créditos (métodos standard, de IRB Básico e IRB avanzado), y para riesgo operativo (método de indicador básico, método standard, y métodos de medición avanzada –AMA-).

Sin política de riesgos, y sin ERM…

Veamos qué sucede sin política de riesgos y sin ERM. Si no tenemos nada al respecto, entonces no es posible hacer una auditoría basada en riesgos objetivamente. Es decir, tengo mis matrices, me muevo a través de la empresa, pero no sé si tengo todo el soporte y la forma de consenso que mencioné antes como para decir: “Voy a medir el riesgo que realmente la empresa quiere”. No es posible hacer una auditoría completa; es decir, yo hago lo que creo que mi plan me dice que es completo pero tal vez me olvido de cosas que no están medidas ni evaluadas. No hay cobertura de riesgos independiente día a día; es decir, Auditoría lo hace periódicamente y no en el día a día, porque el día a día lo hace la línea. No es posible maximizar el retorno de control self-assessment o la cobertura de assurance porque no sé adónde dirigir mis cuestionarios, no sé a quién pedirle documentación, no sé a quién preguntarle el sí/no. Pueden no detectarse necesidades de reingeniería. Puede haber riesgos no visibles, ya que se actúa por inercia. Se incrementa el riesgo de malas sorpresas. También se incrementa la dependencia de los “gerentes estrella” sobre los que ya hablamos: “No, el gerente conoce esto mejor que nadie”, pero ocupan en el fraude de cuello blanco las primeras estadísticas. Y, obviamente, sin ERM se dificulta notablemente el gerenciamiento de fraude (FRM).

El Comité de Riesgos.

El Comité de Riesgos estaba puesto en el organigrama que les mostré y es justamente un comité similar al de Auditoría pero que aprueba los productos, aprueba los procesos, aprueba los sistemas, aprueba los riesgos; por ejemplo, si sale algo nuevo en la empresa, el Comité tiene que aprobarlo o tiene que validar lo que existe. Provee liderazgo para las prácticas de gerenciamiento. Aprueba las políticas de riesgo. Promociona la comunicación. Evalúa la efectividad y asiste a toda esta gente: directores, Auditoría, compliance... ¿Por qué asiste a todo esto? Porque es necesario que la empresa tenga claro que ERM, como dijimos, parte de la Alta Dirección, es parte del corporate governance. Por lo tanto, tiene que haber un Comité de Riesgos. En el Banco lo tenemos; todos los bancos estadounidenses lo tienen y funciona al máximo nivel. Y puede haber subcomités: ALCO, que es Assets and

Liabilities Committee para negocios de tesorería, de créditos, operacional, etc.

El desafío de persuadir al Comité Ejecutivo de implementar ERM

¿Cómo hacemos para persuadirlo de que implemente esto? Todos sabemos que se viene la obligatoriedad. Pero podemos decirle que servirá para evitar ser la futura Enron, para permanecer en el tiempo, para competir, para atraer inversiones; ya vieron el comentario del Instituto en el Reino Unido: aquel que cotice recibe mejor paga por sus acciones. Para reducir riesgos, para dar respuesta a la SarbOx, para cotizar en el mercado de valores, para resistir la exposición pública de los medios y para seguir los estándares pioneros. Razones hay, el problema es que hay que convencer al Comité con esta lista de motivos, que podrían ser más.

Como embeber ERM en la Organización

Ahora, también hay que embeber ERM en la organización. Por eso esto tuvo una evolución, desde el risk management que no tenía la “E” adelante, hasta ahora que el COSO se la agregó y lo especificó. No debe ser una función standalone; esto es un recordatorio. Acá trabaja toda la empresa. El risk officer debe ser el facilitador, es decir, quien está en medio de ERM. Es necesario que haya training. El proceso puede requerir dos años o más, de acuerdo con el tamaño y los recursos. Cuanto antes se comience, mejor porque, lógicamente, los dos años se cuentan desde el momento en que se empieza. Resulta importante definir basics: un idioma, una moneda, una política, una metodología; no podemos hablar de cincuenta cosas a la vez. Y también se requiere un avance gradual, como mostraba una de las diapositivas.

Estructura: Gasto o Inversión?

Ahora bien, ¿cuánto cuesta cotizar en las bolsas y estructurar ERM? No es gratis. El costo está de acuerdo con el tamaño de la empresa, con el riesgo, con la distribución. Piensen que la norma está hecha en los Estados Unidos con una filosofía de gasto que no es la nuestra y que, después, se copió en nuestro país, donde existe una gran resistencia a implementarlo, sobre todo por los gastos. Es, en realidad, una inversión. ¿Por qué? Habría que preguntárselo a quienes quizás hubiesen podido prevenir quiebras, no sólo con ERM sino con todo el esquema del gobierno corporativo. Pero hablamos de prevenir riesgos e imaginémonos el que se nos ocurra: las pérdidas, los fraudes, las incobrabilidades. Para una empresa que tiene toda una visión de futuro, ERM obviamente es una inversión.

Ése es el resumen. Nos estamos anticipando, puesto que faltan algunos meses para que esto se publique, pero ya hay muchísimas empresas que lo usan. Justamente el COSO surge en cierta medida de la experiencia de los que ya lo usan y por eso está puesto para comentarios en Internet, para que los que ya lo usan puedan opinar acerca de qué les parece bien y qué no. Pero, sin duda, va a ser el soporte para todas estas regulaciones y le cubrirá las espaldas a Auditoría en cuanto a obtener más verdes en sus calificaciones.

Eso es todo lo que tengo para decirles. El material es extenso y tuve que comprimirlo mucho. La idea es que cada uno pueda desmenuzar cada línea y buscar un poco más, porque hay mucho para hablar sobre cada tema.

Uso de la Evaluación de Riesgos en la Planificación de Auditorías de TI

Selección de una Metodología de Evaluación de Riesgos

Existen numerosas metodologías de evaluación de riesgos –informatizadas y no informatizadas– disponibles para el área de Auditoría Interna. Éstas varían desde las simples clasificaciones de riesgo alto, medio y bajo basadas en el juicio del Auditor, hasta los cálculos complejos y aparentemente científicos que suministran una clasificación numérica de riesgo. El Auditor Interno debe tener en cuenta el grado de complejidad y detalle apropiados para la organización auditada.

Todas las metodologías de evaluación de riesgos dependen de juicios subjetivos en algún momento del proceso (por ej., para asignar ponderaciones a los diversos parámetros). El área de Auditoría Interna debe identificar las decisiones subjetivas requeridas a fin de utilizar una metodología específica y considerar si estos juicios pueden emitirse y validarse con un grado de exactitud apropiado.

Al decidir cuál es la metodología de evaluación de riesgos más apropiada, el área de Auditoría Interna debe tener en cuenta:

- El tipo de información que debe recopilarse (algunos sistemas utilizan el efecto financiero como única medida – esto no siempre resulta adecuado para las auditorías de TI).
- El costo del software u otras licencias requeridas para utilizar la metodología.
- El grado de disponibilidad de la información requerida.
- La cantidad de información adicional que debe recopilarse antes de poder obtener una salida confiable, y el costo de recopilar dicha información (incluyendo el tiempo que debe dedicarse a esa tarea).
- Las opiniones de otros usuarios de la metodología y sus puntos de vista sobre su eficacia en la tarea de mejorar la eficiencia y/o efectividad de sus auditorías.
- La buena disposición de la gerencia para aceptar la metodología como medio para determinar el tipo y nivel de trabajo de auditoría a realizar.

No puede esperarse que una metodología de evaluación de riesgos determinada resulte apropiada en todas las situaciones. Las condiciones que inciden en el desarrollo de las auditorías pueden modificarse con el tiempo. Periódicamente, el área de Auditoría Interna debe realizar una nueva evaluación de la idoneidad de las metodologías de evaluación de riesgos seleccionadas.

Uso de la Evaluación de Riesgos

El Auditor Interno debe utilizar las técnicas de evaluación de riesgos seleccionadas al desarrollar el plan global de auditoría y al planificar las auditorías específicas. La evaluación de riesgos, en combinación con otras técnicas de auditoría, debe tenerse en cuenta al tomar decisiones de planificación relacionadas con:

- La naturaleza, el alcance y la oportunidad de los procedimientos de auditoría.
- Las áreas o funciones de negocio a auditar.
- El tiempo y los recursos a asignar a cada una de las auditorías.

El Auditor de SI debe tener en cuenta los siguientes tipos de riesgo, a fin de determinar su nivel global:

- Riesgo inherente
- Riesgo de control
- Riesgo de detección

Riesgo inherente

El riesgo inherente es la tendencia de un área de Tecnología de Información a cometer un error que podría ser material, en forma individual o en combinación con otros, suponiendo la inexistencia de controles internos relacionados. Por ejemplo, el riesgo inherente asociado a la seguridad del sistema operativo es normalmente alto dado que los cambios en los datos o programas, o aun su divulgación, a través de las deficiencias en la seguridad del sistema operativo podrían tener como resultado una desventaja competitiva o información de gestión falsa. Por otro lado, el riesgo inherente asociado a la seguridad de una PC independiente es normalmente bajo, cuando un análisis adecuado demuestra que no se utiliza con propósitos críticos de negocio.

El riesgo inherente para la mayoría de las áreas de auditoría de TI es normalmente alto dado que, por lo general, el posible efecto de los errores se extiende a varios sistemas de negocios y a un gran número de usuarios.

Al evaluar el riesgo inherente, el Auditor de TI debe tener en cuenta tanto los controles generales de TI como los detallados. Ello no se aplica en los casos en que la tarea del Auditor Interno esté relacionada exclusivamente con controles generales.

En lo que respecta a los controles generales de TI, el Auditor Interno debe tener en cuenta lo siguiente, al nivel apropiado para el área de auditoría en cuestión:

- La integridad, experiencia y conocimiento de la Gerencia de TI.
- Los cambios en la Gerencia de TI.
- La presión ejercida sobre la Gerencia de TI, que puede predisponerla a ocultar o distorsionar información (por ej., pérdida de datos en grandes proyectos críticos de negocios, actividades de hackers, etc.).
- La naturaleza del negocio y de los sistemas de la organización (por ej., la posibilidad de ejercer el comercio electrónico, la complejidad de los sistemas, la falta de sistemas integrados, etc.).
- Los factores que afectan el rendimiento de la organización en general (por ej., cambios tecnológicos, disponibilidad del personal de TI, etc.).
- El grado de influencia de terceros en el control de los sistemas auditados (por ej., debido a la integración de la cadena de suministro, la tercerización de los procesos de TI, las alianzas estratégicas de negocio y el acceso directo de los clientes).

Al nivel de los controles detallados de TI, el Auditor Interno debe tener en cuenta, en el nivel apropiado para el área de auditoría en cuestión:

- Los hallazgos y fecha de auditorías anteriores en el área.
- La complejidad de los sistemas involucrados.
- El nivel de intervención manual requerida.
- La propensión a la pérdida o apropiación indebida de los bienes controlados por el sistema (por ej., inventario, nómina, etc.).
- La probabilidad de que se produzcan picos de actividad en ciertos momentos del período de auditoría.
- Las actividades que no estén comprendidas en la rutina de procesamiento de SI (por ej., el uso de los utilitarios del sistema operativo para corregir datos, etc.).
- La integridad, experiencia y habilidades de la gerencia y el personal que participan en la aplicación de los controles de TI.

Riesgo de Control

Es el riesgo por el que un error, que podría cometerse en un área de auditoría -y que podría ser material, individualmente o en combinación con otros-, no pueda ser evitado o detectado y corregido oportunamente por el sistema de control interno. Por ejemplo, el riesgo de control asociado a las revisiones manuales de registros computadorizados es normalmente alto debido a que las actividades que requieren investigación a menudo se pierden con facilidad por el volumen de información registrada. El riesgo de control asociado a los procedimientos computarizados de validación de datos es normalmente bajo puesto que los procesos se aplican con regularidad.

El Auditor Interno debe evaluar el riesgo de control como un riesgo alto a menos que los controles internos pertinentes:

- Se identifiquen
- Se consideren eficaces
- Se prueben y confirmen como adecuadamente operativos (pruebas de cumplimiento)

Riesgo de Detección

Es el riesgo que se produce cuando los procedimientos sustantivos del Auditor Interno no detectan un error que podría ser material, individualmente o en combinación con otros. Por ejemplo, el riesgo de detección asociado a la identificación de violaciones de la seguridad en un sistema de aplicación es normalmente alto, debido a que en el transcurso de la auditoría, los registros de todo su período no se encuentran disponibles. El riesgo de detección asociado con la identificación de la falta de planes de recuperación ante desastres es normalmente bajo, dado que su existencia puede verificarse con facilidad.

Al determinar el nivel de pruebas sustantivas requeridas, el Auditor Interno debe tener en cuenta:

- La evaluación del riesgo inherente.
- La conclusión sobre riesgos de control a la que se llega luego de las pruebas de cumplimiento.

Cuanto más exhaustiva es la evaluación del riesgo inherente y de control, mayor es la evidencia de auditoría que debería obtener el Auditor Interno mediante la ejecución de los procedimientos sustantivos de auditoría.

Documentación

El área de Auditoría Interna deberá documentar la técnica o metodología de evaluación de riesgos utilizada en una auditoría. Normalmente, la documentación deberá incluir:

- Una descripción de la metodología de evaluación de riesgos utilizada.
- La identificación de exposiciones significativas y los riesgos correspondientes.
- Los riesgos y exposiciones que la auditoría se propone abordar.
- La evidencia de auditoría utilizada para respaldar la evaluación de riesgos del Auditor Interno.

En resumen, el nivel de trabajo de auditoría requerido para lograr un objetivo de auditoría específico resulta de una decisión subjetiva del

Auditor Interno. Uno de los aspectos de esta decisión es el riesgo de llegar a una conclusión incorrecta basada en los hallazgos de auditoría (riesgo de auditoría). El otro es el riesgo de cometer errores en el área auditada (riesgo de error). El Auditor Interno debe tener en cuenta las normas profesionales al determinar cómo implementar la evaluación de riesgos mencionada, así como también, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto de ellas.