

**Comité de Basilea
sobre Supervisión Bancaria**

**Prácticas sólidas para la administración
y supervisión del riesgo operacional**

Julio 2002

BANCO DE PAGOS INTERNACIONALES

Grupo de Administración de riesgo del Comité de Basilea sobre Supervisión Bancaria

Presidente:

Sr. Roger Cole – Federal Reserve Board, Washington, D. C.

Banque Nationale de Belgique, Bruselas	Dominique Gressens
Commission Bancaire et Financière, Bruselas	Jos Meuleman
Oficina del Superintendente de Instituciones Financieras, Ottawa	Jeff Miller
Commission Bancaire, Paris	Laurent Le Mouël
Deutsche Bundesbank, Frankfurt am Main	Magdalene Heid Karin Sagner-Kaiser
Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn	Kirsten Strauss
Banca d'Italia, Roma	Claudia Dauria
Bank of Japan, Tokyo	Eiji Harada
Financial Services Agency, Tokyo	Hirokazu Matsushima
Commission de Surveillance du Secteur Financier, Luxemburgo	Davy Reinard
De Nederlandsche Bank, Amsterdam	Klaas Knot
Banco de España, Madrid	Guillermo Rodríguez-García Juan Serrano
Finansinspektionen, Estocolmo	Jan Hedquist
Sveriges Riksbank, Estocolmo	Thomas Flodén
Eidgenössische Bankenkommission, Bern	Martin Sprenger
Financial Services Authority, Londres	Helmut Bauer Victor Dowd Jeremy Quick
Federal Deposit Insurance Corporation, Washington, D.C.	Mark Schmidt
Federal Reserve Bank of New York	Beverly Hirtle Stefan Walter
Federal Reserve Board, Washington, D.C.	Kirk Odegard
Oficina del Contralor de la Moneda, Washington, D. C.	Kevin Bailey Tanya Smith
European Central Bank, Frankfurt am Main	Panagiotis Strouzas
European Commission, Bruselas	Michel Martino Melania Savino
Secretaría del Comité de Basilea sobre Supervisión Bancaria, Banco de Pagos Internacionales	Stephen Senior

Tabla de Contenidos

Introducción	1
Marco teórico	2
Tendencias y prácticas de la industria	4
Prácticas sólidas	5
Desarrollo de un Ambiente apropiado de administración de riesgo	6
Administración de riesgo: Identificación, Evaluación, Monitoreo y Mitigación/Control	6
Rol de los Supervisores	7
Rol de la Divulgación	7

Prácticas Sólidas para la Administración y Supervisión del Riesgo Operacional

El documento consultivo de Prácticas Sólidas para la Administración y Supervisión de Riesgo Operacional, preparado por el Grupo de Administración del riesgo del Comité de Basilea sobre Supervisión Bancaria (el Comité), originalmente se publicó en diciembre del 2001. El Comité está agradecido por muchos de los comentarios recibidos de las instituciones, asociaciones de industria, autoridades de supervisión y otros, y resalta que estos comentarios han jugado un papel sustancial en la re-elaboración de este documento. Debido a un número de cambios importantes a las Prácticas Sólidas incorporados en esta versión revisada, el Comité ha decidido comunicarlo para un segundo, corto período de consulta antes de su finalización.¹ El Comité agradecería por lo tanto los comentarios sobre los principios revisados descritos en este documento. Estos comentarios deben remitirse a las autoridades nacionales relevantes de supervisión y banco centrales y pueden también ser enviados a la Secretaria del Comité de Basilea sobre Supervisión Bancaria a Bank for International Settlements, CH-4002 Basel, Switzerland para el 30 de septiembre del 2002. Los comentarios pueden también enviarse vía e-mail: BCBS.capital@bis.org² o por fax: + 41 61 280 9100. Los comentarios sobre este documento no se colocarán en el website del BIS.

Introducción

1. El siguiente documento describe un conjunto de principios que proveen un marco de referencia para la efectiva administración y supervisión del riesgo operacional, a usarse por bancos y autoridades de supervisión cuando se evalúa las políticas y prácticas de la administración del riesgo operacional.
2. El Comité reconoce que el enfoque exacto para la administración del riesgo operacional escogido por un banco individual dependerá de un rango de factores, incluyendo su tamaño y sofisticación y la naturaleza y complejidad de sus actividades. Sin embargo, a pesar de estas diferencias, unas estrategias y vigilancia claras por la junta directiva y alta dirección, una cultura sólida de control interno (incluyendo, entre otras cosas, claras líneas de responsabilidad y segregación de deberes), un reporte interno efectivo, y una planeación

¹ Por favor tomar nota de que el Comité no planea emitir una versión revisada de la segunda parte de las Prácticas Sólidas de diciembre de 2001 “*Supervisory Guidance for a Comprehensive Operational Risk Management Programme*” (Directriz de Supervisión para un Programa Comprensivo de Administración de riesgo Operacional).

² Por favor use esta dirección electrónica únicamente para enviar los comentarios y no para correspondencia.

contingente son elementos cruciales de un marco efectivo de administración de riesgo operacional para bancos de cualquier tamaño y alcance. El documento previo del Comité Un Marco para Sistemas de Control Interno en Organizaciones Bancarias (septiembre 1998) consolida su actual trabajo en el campo del riesgo operacional.

Marco Teórico

3. La desregulación y globalización de servicios financieros, junto con la creciente sofisticación de la tecnología financiera, están haciendo las actividades de los bancos (y así sus perfiles de riesgo) más diversas y complejas. El desarrollo de las prácticas bancarias sugiere que otros riesgos además del de crédito, riesgo de tasa de interés y riesgo de mercado pueden ser sustanciales. Los ejemplos de estos nuevos y crecientes riesgos que los bancos enfrentan incluyen:

- Si no es apropiadamente controlado, el uso de tecnología más altamente sofisticada tiene el potencial para transformar los riesgo de los errores de procesamiento manual a riesgos de falla de sistema, ya que se confía más en los sistemas globalmente integrados;
- El crecimiento del comercio electrónico trae consigo riesgos potenciales (por ej., temas de fraude externo y de seguridad de sistema);
- Las fusiones a gran escala, des-fusiones y consolidaciones ponen a prueba la viabilidad de los sistemas nuevos o recientemente integrados;
- La emergencia de los bancos que actúan como proveedores de servicio a gran volumen crea la necesidad de un mantenimiento continuo de controles internos y sistemas de respaldo altamente calificados;
- Los bancos pueden involucrarse en las técnicas de mitigación de riesgo (por ej., colateral, derivados de crédito, convenios de neteo y titularizaciones de activos) para optimizar su exposición al riesgo de mercado y riesgo de crédito, pero lo cual a la vez puede producir otras formas de riesgo; y
- El uso creciente de convenios de *outsourcing* y la participación en los sistemas de compensación y pago pueden mitigar algún riesgo pero también pueden presentar otros riesgos significativos a los bancos.

4. El diverso conjunto de riesgos listados anteriormente pueden ser agrupados bajo el título de 'riesgo operacional', que para propósitos de supervisión el Comité ha definido como: 'el riesgo de pérdida resultante de procesos internos fallidos o

inadecuados, personas y sistemas o de eventos externos'.³ La definición incluye el riesgo legal pero excluye el riesgo estratégico, de reputación y sistémico.

5. El Comité reconoce que el riesgo operacional es un término que tiene una variedad de significados dentro de la industria, y por consiguiente para propósitos internos, los bancos pueden escoger adoptar sus propias definiciones de riesgo operacional. Cualquiera que sea la definición exacta, una comprensión clara por los bancos de lo que se entiende por riesgo operacional es crítico para la efectiva administración y control de la categoría de riesgo. Es también importante que la definición considere el rango completo de riesgos operacionales materiales que afronta el banco y abarque las causas más significativas de severas pérdidas operacionales. Los tipos de evento de riesgo operacional que el Comité – en cooperación con la industria – ha identificado que tienen el potencial de resultar en pérdidas sustanciales incluyen los siguientes:

- **Fraude interno.** Los actos de un tipo de intento de fraude, malversación de fondos o evadir regulaciones, la ley o política de la compañía, excepto los eventos de diversidad / discriminación, que implican por lo menos una parte interna. Los ejemplos incluyen la mal información intencional de posiciones, hurto del empleado, y negociación interna de valores a propia cuenta de un empleado.
- **Fraude externo.** Los actos por una tercera parte, de un tipo de intento de fraude, malversación de fondos o evadir la ley. Los ejemplos incluyen robo, falsificación, emisión de cheque sin fondos y daño provocado por pirateo computacional.
- **Prácticas de empleo y seguridad de lugar de trabajo.** Actos inconsistentes con las leyes o contratos de empleo, salud o seguridad, o que resultan en pago de reclamos de perjuicio personal, o reclamos relacionados a temas de diversidad / discriminación. Los ejemplos incluyen los reclamos de compensación de trabajadores, violación de la salud del empleado y a reglas de seguridad, actividades de labor organizada, reclamos de discriminación y responsabilidad general (por ejemplo, un cliente que se equivoca y falla en una oficina sucursal).
- **Clientes, productos y prácticas de negocios.** Una falla no intencional o negligente en cumplir una obligación profesional a clientes específicos (incluyendo requerimientos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto. Los ejemplos incluyen infracciones fiduciarias, mal

³ Esta definición se adoptó de la industria como parte del trabajo del Comité en el desarrollo de una carga mínima de capital regulatorio para el riesgo operacional. Mientras este documento no es una parte formal del marco de capital, el Comité sin embargo espera que los elementos básicos de un marco sólido de administración de riesgo operacional establecidos en este documento informen las expectativas de supervisión cuando se revise la adecuación de capital bancario.

uso de información confidencial de cliente, actividades impropias de negociación de valores sobre la cuenta del banco, lavado de dinero, y venta de productos no autorizados.

- ***Daño a activos físicos.*** Pérdida o daño a activos físicos por desastre natural u otros eventos. Los ejemplos incluyen terrorismo, vandalismo, terremotos, incendios e inundaciones.
- ***Interrupción de negocios y fallas del sistema.*** Interrupción de negocios o fallas del sistema. Los ejemplos incluyen fallas de hardware y software, problemas de telecomunicación y pérdida de utilidad.
- ***Administración de la ejecución, entrega y proceso.*** Administración fracasada de procesamiento de transacción o proceso, y relaciones con contrapartes comerciales y vendedores. Los ejemplos incluyen errores de entrada de datos, fallas de administración colateral, documentación legal incompleta, acceso no autorizado dado a cuentas de clientes, mal desempeño de contraparte no-cliente y disputas de vendedor.

Tendencias y prácticas de la industria

6. En su trabajo sobre la supervisión de los riesgos operacionales, el Comité se ha enfocado a desarrollar una mejor comprensión de las tendencias y prácticas actuales de la industria para la administración del riesgo operacional. Estos esfuerzos han implicado numerosas reuniones con organizaciones bancarias, encuestas de prácticas de la industria, y análisis de los resultados. Con base en estos esfuerzos, el Comité cree que tiene una buena comprensión del rango actual de prácticas de la industria bancaria, como también los esfuerzos de la industria por desarrollar métodos para la administración de riesgos operacionales.

7. El Comité reconoce que la administración de riesgos operacionales específicos no es una nueva práctica; ha sido siempre importante para los bancos tratar de prevenir el fraude, mantener la integridad de los controles internos, reducir errores en el procesamiento de transacciones y sucesivamente. Sin embargo, lo que relativamente es nuevo es la visión de la administración de riesgo operacional como una práctica comprensiva comparable a la administración del riesgo de crédito y de mercado en principio, si no siempre en forma. Las tendencias citadas en la introducción a este documento, combinado con un número creciente de eventos de pérdida operacional de alto perfil por todo el mundo, han conducido a los bancos y supervisores a ver cada vez más a la administración del riesgo operacional como una disciplina inclusiva, como ha sido ya el caso en muchas otras industrias.

8. En el pasado, los bancos confiaban casi exclusivamente en los mecanismos de control interno dentro de las líneas de negocio, complementados por la función

de auditoría, para administrar el riesgo operacional. Mientras que éstos siguen siendo importantes, recientemente ha habido una aparición de estructuras y procesos específicos enfocados a la administración del riesgo operacional. A este respecto, un número creciente de organizaciones ha concluido que un programa de administración de riesgo operacional provee seguridad y solidez al banco, y por lo tanto están avanzando en el manejo del riesgo operacional como una clase de riesgo distinta, pero similar en su tratamiento al riesgo de crédito y de mercado. El comité cree que un intercambio activo de ideas entre los supervisores e industria es clave para el desarrollo continuo de la directriz apropiada para la administración de exposiciones relacionadas al riesgo operacional.

9. Este documento está organizado en las siguientes líneas: desarrollo de un ambiente apropiado de administración de riesgo; administración de riesgo: identificación, evaluación, monitoreo y control / mitigación; el rol de los supervisores; y el rol de la divulgación.

Prácticas sólidas

10. En el desarrollo de estas prácticas sólidas, el Comité ha diseñado bajo su trabajo existente sobre la administración de otros riesgos bancarios significativos, como el riesgo de crédito, riesgo de tasa de interés y riesgo de liquidez, y el Comité cree que debe aplicarse el rigor similar a la administración del riesgo operacional. Sin embargo, está claro que el riesgo operacional difiere de otros riesgos bancarios en que normalmente no se toma directamente en retorno por una recompensa esperada, sino existe en el curso natural de la actividad corporativa, y que esto afecta el proceso de administración de riesgo.⁴ Al mismo tiempo, la falla en administrar apropiadamente el riesgo operacional puede resultar en una aserción falsa del perfil de riesgo / retorno y expone a la institución a pérdidas significativas. Reflejando la diversa naturaleza del riesgo operacional, para los propósitos de este documento, la 'administración' del riesgo operacional toma el significado de la ' identificación, evaluación, monitoreo y control / mitigación' del riesgo. Esta definición contrasta con la utilizada por el Comité en previos documentos de administración de riesgo de la 'identificación, medición, monitoreo y control /mitigación' de riesgo. En común con su trabajo sobre otros riesgos bancarios, el Comité ha estructurado este documento de prácticas sólidas alrededor de un número de principios. Éstos son:

⁴ Sin embargo, el Comité reconoce que en algunas líneas de negocio con riesgo mínimo de crédito o de mercado (por ej., administración de activo, pago y liquidación), la decisión de incurrir en riesgo operacional, o competir con base en la habilidad para administrar y efectivamente preciar este riesgo, es una parte integral del cálculo de riesgo / recompensa del banco.

Desarrollo de un Ambiente Apropriado de Administración de Riesgo

Principio 1: La junta directiva⁵ debe estar enterada de los aspectos más importantes de los riesgos operacionales del banco como una categoría de riesgo distinta que debe ser administrada, y debe aprobar y revisar en forma periódica el marco de administración de riesgo operacional. El marco debe proveer una definición a nivel de firma del riesgo operacional y descansar en los principios de cómo el riesgo operacional es identificado, evaluado, monitoreado y controlado / mitigado.

Principio 2: La junta directiva debe asegurar que el marco de administración de riesgo está sujeto a auditoría interna efectiva y comprensiva por personal operacionalmente independiente, competente y apropiadamente capacitado. La función de auditoría interna no debe de ser directamente la responsable de la administración del riesgo operacional.

Principio 3: La alta dirección debe tener la responsabilidad de implementar el marco de administración de riesgo operacional aprobado por la junta directiva. El marco debe implementarse completamente en la toda la organización bancaria, y todos los niveles de personal deben comprender sus responsabilidades con respecto a la administración del riesgo operacional. La alta dirección debe también tener la responsabilidad de desarrollar políticas, procesos y procedimientos para la administración del riesgo operacional en todos los productos, actividades, procesos y sistemas del banco.

Administración de Riesgo: Identificación Evaluación, Monitoreo y Mitigación / Control

Principio 4: Los Bancos deben identificar y evaluar el riesgo operacional inherente en todos los productos materiales, actividades, procesos y sistemas. Los bancos deben asegurar también que antes de que los nuevos, productos, actividades, procesos y sistemas sean introducidos o emprendidos, el riesgo operacional inherente en ellos está sujeto a procedimientos adecuados de evaluación.

⁵ Este documento se refiere a una estructura de administración compuesta de un consejo de directores y alta dirección. El Comité está consciente de que existan diferencias significativas en los marcos legislativo y regulatorio a través de los países con respecto a las funciones de la junta directiva y alta dirección. En algunos países, el consejo tiene la principal, si no exclusiva, función de supervisar el cuerpo ejecutivo (alta dirección, administración general) para así asegurar que la última cumple sus tareas. Por esta razón, en algunos casos, este se conoce como el consejo de supervisión. Esto significa que el consejo no tiene funciones ejecutivas. En otros países, el consejo tiene una competencia más amplia en que descansa el marco general para la administración del banco. Debido a estas diferencias, los términos ‘consejo de directores’ y ‘alta dirección’ son usados en este documento no para identificar las construcciones legales sino para etiquetar las funciones de doble toma de decisión dentro de un banco.

Principio 5: Los bancos deben implementar un proceso para monitorear regularmente los perfiles de riesgo operacional y exposición material a las pérdidas. Debe haber un reporte regular de información pertinente a la alta dirección y la junta directiva que apoya la administración proactiva del riesgo operacional.

Principio 6: Los bancos debe tener políticas, procesos y procedimientos para controlar o mitigar los riesgos operacionales materiales. Los bancos deben evaluar la factibilidad de limitación de riesgo alternativa y estrategias de control y debe ajustar su perfil de riesgo operacional usando estrategias apropiadas, a luz de su apetito y perfil de riesgo global.

Principio 7: Los bancos deben tener establecidos planes de continuidad de contingencia y de negocios para asegurar su capacidad de operar en medio de tensiones y minimizar pérdidas en el evento de severa interrupción del negocio.

Rol de los Supervisores

Principio 8: Los supervisores bancarios deben requerir que todos los bancos, sin considerar el tamaño, tengan un marco efectivo establecido para identificar, evaluar, monitorear y controlar o mitigar los riesgos operacionales materiales como parte de un enfoque global a la administración de riesgo.

Principio 9: Los supervisores deben conducir, directa o indirectamente, la evaluación independiente regular de las políticas, procedimientos y practicas de un banco relacionadas a los riesgos operacionales. Los supervisores deben asegurar que existan mecanismos apropiados de reporte establecidos que les permitan permanecer informados de los desarrollos en los bancos.

Rol de la Divulgación

Principio 10: Los bancos deben hacer divulgación pública suficiente para permitir a los participantes del mercado evaluar su enfoque a la administración del riesgo operacional.

Desarrollo de un Ambiente apropiado de Administración de Riesgo

11. La falta de comprender y administrar el riesgo operacional, que está presente virtualmente en todas las transacciones y actividades del banco, puede grandemente incrementar la probabilidad de que algunos riesgos no serán

reconocidos y estarán incontrolados. El consejo y la alta dirección son responsables de crear una cultura organizacional que establezca una alta prioridad en la administración efectiva del riesgo operacional y adherencia a sólidos controles operativos. La administración del riesgo operacional es más efectiva cuando la cultura de un banco se enfatiza en altos estándares de conducta ética en todos los niveles del banco. El consejo y alta dirección deben promover una cultura organizacional que establezca mediante acciones y palabras las expectativas de integridad para todos los empleados en la conducción del negocio del banco.

Principio 1: La junta directiva⁵ debe estar enterada de los aspectos más importantes de los riesgos operacionales del banco como una categoría de riesgo distinta que debe ser administrada, y debe aprobar y revisar en forma periódica el marco de administración de riesgo operacional. El marco debe proveer una definición a nivel de firma del riesgo operacional y descansar en los principios de cómo el riesgo operacional es identificado, evaluado, monitoreado y controlado / mitigado.

12. La junta directiva debe aprobar la implementación de un marco a nivel de firma para administrar explícitamente el riesgo operacional como un riesgo distinto al de seguridad y solidez del banco. El consejo debe proveer a la alta dirección con clara directriz y dirección con respecto a los principios que fundamentan el marco y aprueban las políticas correspondientes desarrolladas por la alta dirección.

13. En este documento, un marco de riesgo operacional se entiende incluye una definición apropiada de riesgo operacional que claramente articula lo que constituye el riesgo operacional en ese banco. El marco debe cubrir el apetito y tolerancia del banco para el riesgo operacional, como se especifica mediante las políticas para la administración de este riesgo, incluyendo el alcance, y manera en la cual el riesgo operacional se transfiere fuera del banco. Esto debe también incluir políticas que describan el enfoque del banco para identificar, evaluar, monitorear y controlar / mitigar el riesgo. La formalidad y sofisticación del marco de administración de riesgo operacional del banco debe ser proporcionado con el riesgo incurrido por el banco.

14. El consejo es responsable de establecer una estructura de administración capaz de implementar el marco de administración de riesgo operacional de la firma. Ya que un aspecto importante de la administración del riesgo operacional se relaciona al establecimiento de fuertes controles internos, es particularmente importante que el consejo establezca líneas claras de responsabilidad y reporte administrativos. Además, deben existir responsabilidades segregadas y líneas de reporte entre las funciones de control y el ingreso que generan las líneas de negocio. El marco debe también articular los procesos claves que la firma necesita establecer para administrar el riesgo operacional.

15. El consejo debe revisar el marco en forma regular para asegurar que el banco esté administrando los riesgos operacionales que surgen de cambios externos en el mercado y otros factores ambientales, como los riesgos operacionales asociados con nuevos productos, actividades o sistemas. Este proceso de revisión debe también enfocarse a incorporar innovaciones de industria en la apropiada administración del riesgo operacional para las actividades, sistemas y procesos del banco. Si es necesario, el consejo debe asegurar que el marco de administración de riesgo operacional sea revisado a luz de este análisis, para que los riesgos operacionales materiales sean capturados dentro del marco.

Principio 2: La junta directiva debe asegurar que el marco de administración de riesgo está sujeto a auditoría interna efectiva y comprensiva por personal operacionalmente independiente, competente y apropiadamente capacitado. La función de auditoría interna no debe de ser directamente la responsable de la administración del riesgo operacional.

16. Los bancos deben establecer una cobertura adecuada de auditoría interna para verificar que las políticas y procedimientos operativos son efectivamente implementados.⁶ El consejo (ya sea directa o indirectamente a través de su comité de auditoría) debe asegurar que el alcance y frecuencia del programa de auditoría es apropiado a los riesgos implicados. La auditoría debe periódicamente validar que el marco de administración de riesgo operacional de la firma está siendo implementado en forma efectiva a través de la firma.

17. Al alcance en que la función de auditoría está involucrada en la vigilancia del marco de administración de riesgo operacional, el consejo debe asegurar que la independencia de la función de auditoría se mantenga. Esta independencia puede comprometerse si la función de auditoría está directamente involucrada en el proceso de administración de riesgo operacional. La función de auditoría puede proveer datos a aquellos responsables de la administración del riesgo operacional, pero no debe tener por sí misma responsabilidades directas. En la práctica, el Comité reconoce que la función de auditoría en algunos bancos (particularmente bancos pequeños) pueden tener responsabilidad inicial por el desarrollo de un programa de administración de riesgo operacional. Cuando este sea el caso, los bancos deben comprender que la responsabilidad de la administración de riesgo operacional día a día es transferida a otra parte en una forma oportuna.

Principio 3: La alta dirección debe tener la responsabilidad de implementar el marco de administración de riesgo operacional aprobado por la junta directiva. El marco debe implementarse completamente en la toda la organización bancaria, y todos los niveles de personal deben comprender sus responsabilidades con respecto a la administración del riesgo

⁶ El documento del Comité, *Internal Audit in Banks and the Supervisor's Relationship with Auditors* (Auditoría Interna en los Bancos y La Relación del Supervisor con los Auditores) -agosto de 2001- describe el papel de la auditoría interna y externa.

operacional. La alta dirección debe también tener la responsabilidad de desarrollar políticas, procesos y procedimientos para la administración del riesgo operacional en todos los productos, actividades, procesos y sistemas del banco.

18. La administración debe trasladar el marco de administración de riesgo operacional establecido por la junta directiva a políticas, procesos y procedimientos más específicos que pueden ser implementados y verificados con diferentes unidades de negocio. Mientras cada nivel de administración es responsable de la propiedad y efectividad de las políticas, procesos, procedimientos y controles con su competencia, la alta dirección debe claramente asignar relaciones de autoridad, responsabilidad y reporte para fomentar su responsabilidad. Esta responsabilidad incluye asegurar que los recursos necesarios están disponibles para administrar el riesgo operacional efectivamente. Por otra parte, la alta dirección debe evaluar la propiedad del proceso de vigilancia de la administración a luz de los riesgos inherentes en la política de la unidad de negocios y asegurarse de que el personal está informado de sus responsabilidades.

19. La alta dirección debe asegurar que las actividades del banco se realizan por personal calificado con la experiencia necesaria y capacidades técnicas y que el personal responsable del monitoreo y aplicación de la política de riesgo de la institución tenga autoridad independiente de las unidades de riesgo que inspecciona. La administración debe asegurar que la política de administración de riesgo operacional del banco ha sido claramente comunicada al personal a todos los niveles en las unidades de negocio que incurren en riesgos operacionales materiales.

20. La alta dirección debe asegurar que el personal con responsabilidad del riesgo operacional se comunique efectivamente con el personal responsable de los riesgos de crédito, de mercado y otros riesgos, como también con aquellos en la firma que es responsable por de la obtención de servicios externos como compras de seguros y convenios de outsourcing. La falla en hacerlo así puede resultar en vacíos o traslapes en el programa de administración de riesgo global en un banco.

21. La alta dirección debe también asegurar que las políticas de remuneración del banco son consistentes con su apetito de riesgo. Las políticas de remuneración que compensan al personal que se desvían de las políticas (por ej., excediendo los límites establecidos) debilitan los procesos de administración de riesgo del banco.

22. Los objetivos integrados entre los niveles gerenciales son particularmente cruciales para los bancos que usan, o se encuentran en el proceso de implementación de tecnologías avanzadas para apoyar grandes volúmenes de transacciones. Se debe prestar particular atención a la calidad de los controles de documentación y prácticas de manejo de transacciones. Las políticas, procesos y

procedimientos relacionados a dichas tecnologías deben estar bien documentadas y diseminadas a todo el personal relevante.

Administración de Riesgo: Identificación, Evaluación, Monitoreo y Mitigación/Control

Principio 4: Los bancos deben identificar y evaluar el riesgo operacional inherente en todos los productos materiales, actividades, procesos y sistemas. Los bancos deben asegurar también que antes de que los nuevos, productos, actividades, procesos y sistemas sean introducidos o emprendidos, el riesgo operacional inherente en ellos está sujeto a procedimientos adecuados de evaluación.

23. La identificación del riesgo es de máxima importancia para el subsiguiente desarrollo del monitoreo y control operacional viables. La identificación efectiva del riesgo considera factores internos (como la complejidad de la estructura del banco, la naturaleza de las actividades del banco, la calidad de personal, los cambios organizacionales y la producción del empleado) y factores externos (como los cambios en la industria y avances tecnológicos) que podrían afectar en forma adversa el logro de los objetivos del banco.

24. Además de identificar la mayoría de los riesgos potencialmente adversos, los bancos deben evaluar su vulnerabilidad a los mismos. Una evaluación efectiva del riesgo permite al banco comprender mejor su perfil de riesgo y enfocar más efectivamente los recursos de administración de riesgo.

25. Existen varios procesos normalmente usados por los bancos para ayudarlos a identificar y evaluar el riesgo operacional:

- Auto-evaluación o evaluación del riesgo: un banco evalúa sus operaciones y actividades contra un menú de vulnerabilidades potenciales de riesgo operacional. Este proceso está dirigido internamente y a menudo incorpora listas de chequeo y/o talleres para identificar las fortalezas y debilidades del entorno del riesgo operacional.
- Mapeo del riesgo: en este proceso, varias unidades de negocio, funciones organizacionales o flujos de proceso se mapean por tipo de riesgo. Este ejercicio puede revelar áreas de debilidad y ayuda a priorizar la acción gerencial subsiguiente.
- Indicadores claves de riesgo: los indicadores de riesgo son estadísticas y/o métricas, a menudo financieras, que pueden proporcionar algunas ideas sobre la posición de riesgo de un banco. Estos indicadores tienen a ser revisados en una base periódica (mensual o trimestralmente) para alertar a los bancos sobre los cambios que pueden ser indicativos de preocupaciones de riesgo. Dichos indicadores pueden incluir el número de transacciones, tasas de producción de personal fallidas y la frecuencia y/o severidad de los errores y omisiones.

- Tarjetas de punteo: éstas proporcionan los medios para trasladar las evaluaciones cualitativas a métricas cuantitativas que dan un punteo relativo de los diferentes tipos de exposiciones de riesgo operacional. Algunos punteos pueden relacionarse a riesgos únicos en una línea de negocios específica mientras que otros pueden puntuar riesgos que atraviesan las líneas de negocios. Los punteos pueden abarcar factores de riesgos inherentes al igual que los controles para mitigarlos. Además, las tarjetas de punteo pueden usarse para asignar capital económico a líneas de negocio en relación al desempeño en la administración y control de varios aspectos de riesgo operacional.
- Límites inferiores / restricciones: ligados normalmente a indicadores de riesgo, niveles de límite inferior (o cambios) en indicadores clave de riesgo, que cuando se exceden, alertan a la administración sobre áreas de problemas potenciales.
- Medición: algunas firmas han iniciado a cuantificar su exposición al riesgo operacional usando una variedad de enfoques. Por ejemplo, los datos de la experiencia de pérdida histórica de un banco podrían proporcionar información significativa para evaluar la exposición del banco al riesgo operacional y desarrollar una política para mitigar/controlar el riesgo. Una forma efectiva de hacer buen uso de esta información es establecer un marco para rastrear y registrar en forma sistémica la frecuencia, severidad y otra información relevante sobre los eventos individuales de pérdida. Algunas firmas también han combinado datos internos de pérdida con datos externos de pérdida, análisis de escenarios y factores cualitativos de evaluación.

Principio 5: Los bancos deben implementar un proceso para monitorear regularmente los perfiles de riesgo operacional y exposición material a las pérdidas. Debe haber un reporte regular de información pertinente a la alta dirección y la junta directiva que apoya la administración proactiva del riesgo operacional.

26. Un proceso efectivo de monitoreo es esencial para adecuadamente administrar el riesgo operacional. Las actividades regulares de monitoreo pueden ofrecer la ventaja de una pronta detección y corrección de deficiencias en políticas, procesos y procedimientos para la administración del riesgo operacional. La pronta detección y dirección de estas deficiencias pueden sustancialmente reducir la frecuencia y/o severidad potencial de un evento de pérdida.

27. Además de monitorear los eventos de pérdida operacional, los bancos deben identificar indicadores que puedan ser predecibles de riesgo de pérdidas futuras. Dichos indicadores (a menudo conocidos como indicadores claves de riesgo o indicadores de alerta temprana) deben ser previsores y podrían reflejar fuentes potenciales de riesgo operacional tales como crecimiento rápido, introducción de productos nuevos, volumen de ventas del empleado, interrupción de transacción, tiempo fuera de servicio del sistema, etc. Cuando los límites inferiores están directamente ligados a estos indicadores, un proceso de

supervisión eficaz puede ayudar a identificar riesgos materiales claves de una manera transparente y permitir al banco actuar sobre estos riesgos apropiadamente.

28. La frecuencia del monitoreo debe reflejar los riesgos implicados y la frecuencia y naturaleza de los cambios en el ambiente operativo. El monitoreo es más efectivo cuando el sistema de control interno está integrado a las operaciones del banco y produce reportes regulares. Los resultados de estas actividades de monitoreo deben incluirse en los reportes a la administración y junta, al igual que las revisiones de cumplimiento realizadas por la auditoría interna y/o funciones de administración de riesgo. Los reportes generados por las autoridades de supervisión pueden también informar sobre este monitoreo y deben asimismo ser reportados internamente a la alta dirección y la junta, cuando sea apropiado.

29. La alta dirección debe recibir reportes regulares de unidades de negocio y la función de auditoría interna. Los reportes deben contener datos financieros internos, operacionales y de cumplimiento, como también información de mercado externo sobre eventos y condiciones que sean relevantes para la toma de decisión. Los reportes deben ser distribuidos a niveles apropiados de administración y a áreas del banco en las que pueden tener impacto. Los reportes deben reflejar completamente cualesquiera áreas de problema y debe motivar oportunamente una acción correctiva sobre los temas pendientes. Para asegurar la utilidad y confiabilidad de estos reportes de riesgo y de auditoría, la administración debe en forma regular verificar la oportunidad, precisión y relevancia de los sistemas de reporte y controles internos en general. La administración puede también usar reportes preparados por fuentes externas (auditores, supervisores) para evaluar la utilidad y confiabilidad de los reportes internos. Los reportes deben ser analizados con vistas a mejorar el desempeño de la administración del riesgo existente como también al desarrollo de nuevas políticas, procedimientos y prácticas de administración de riesgo.

30. En general, la junta directiva debe recibir suficiente información de alto nivel para permitirles comprender el perfil de riesgo global del banco y enfocarse en las implicaciones estratégicas y materiales de riesgo operacional para el negocio.

Principio 6: Los bancos debe tener políticas, procesos y procedimientos para controlar o mitigar los riesgos operacionales materiales. Los bancos deben evaluar la factibilidad de limitación de riesgo alternativa y estrategias de control y debe ajustar su perfil de riesgo operacional usando estrategias apropiadas, a luz de su apetito y perfil de riesgo global.

31. Las actividades de control se diseñan para dirigir los riesgos que un banco ha identificado.⁷ Para aquellos riesgos que no pueden ser controlados, el banco

⁷ Para mayor detalle, ver el documento Framework for Internal Control Systems in Banking Organizations, (Marco de Sistemas de Control Interno en Organizaciones Bancarias), Comité de Basilea en Supervisión Bancaria, septiembre de 1998.

debe decidir si acepta este riesgo o se retira o reduce el nivel de actividad de negocio implicada. Los procesos y procedimientos de control deben estar establecidos y los bancos deben tener un sistema para asegurar el cumplimiento con un conjunto documentado de políticas internas concernientes al sistema de administración de riesgo. Los elementos principales de este pueden incluir:

- Revisiones de alto nivel del progreso del banco hacia los objetivos establecidos;
- Chequeo del cumplimiento con los controles de la administración;
- Políticas, procesos y procedimientos con respecto a la revisión, tratamiento y resolución de temas de no cumplimiento; y
- Un sistema de aprobaciones y autorizaciones documentado para asegurar la responsabilidad en un nivel apropiado de la administración.

32. Aunque un marco de políticas y procedimientos escritos, formales es crítico, necesita ser reforzado mediante una cultura sólida de control que promueva prácticas sólidas de administración de riesgo. Para ser efectivas, las actividades de control debe ser una parte integral de las actividades regulares de un banco. Los controles que son una parte integral de las actividades regulares permiten respuestas rápidas a las condiciones cambiantes y evitan costos innecesarios.

33. Un sistema efectivo de control interno también requiere que exista segregación apropiada de responsabilidades y que al personal no se le asignen responsabilidades que podrían crear un conflicto de interés. La asignación de dichas responsabilidades conflictivas a individuos, o un equipo, podría permitirles ocultar pérdidas, errores o acciones inapropiadas. Por lo tanto, las áreas de conflictos de interés potenciales deben ser identificadas, minimizadas y estar sujetas a un cuidadoso monitoreo y revisión independientes.

34. Además de la segregación de responsabilidades, los bancos deben asegurar que un número de otras prácticas internas están establecidas para controlar el riesgo operacional. Entre estas están el monitoreo cercano de la adherencia a límites inferiores o restricciones de riesgo asignadas, el mantenimiento de salvaguardas de acceso y uso de activos y registros, la seguridad de que el personal tiene la experiencia y entrenamiento apropiados, identificando líneas o productos de negocios donde los retornos parecen estar significativamente fuera de línea con expectativas razonables, y verificación y conciliación regular de transacciones y cuentas. La falla en implementar dichas prácticas ha resultado en pérdidas operacionales significativas para algunos bancos en años recientes.

35. El Comité ha observado que el riesgo operacional parece prevalecer donde los bancos se han involucrado en nuevas actividades o desarrollado nuevos productos (particularmente donde estas actividades o productos no son consistentes con las estrategias básicas del negocio), entrado en mercados no familiares, e involucrado en negocios que están geográficamente distantes de la oficina principal. Adicionalmente, en muchas instancias, la firma no asegura que la infraestructura de control de administración de riesgo guarde la marcha con el

crecimiento de la nueva actividad del negocio. Un número de pérdidas de tamaño más regular y pérdidas del más alto perfil que han ocurrido en años recientes ha tomado lugar donde uno o una combinación de estas condiciones existió. Por consiguiente, se apoya en los bancos para asegurar que se presta especial atención a las actividades de control interno donde existen dichas condiciones.

36. Algunos riesgos operacionales significantes tienen pocas probabilidades pero potencialmente muy grande impacto financiero. Además, no todos los eventos de riesgo pueden ser controlados (por ej., desastres naturales). Las herramientas y programas de mitigación del riesgo pueden ser usados para reducir la exposición, o frecuencia y/o severidad de dichos eventos. Por ejemplo, las pólizas de seguro, particularmente aquellas con prontas y ciertas características de liquidación, pueden ser usadas para externalizar el riesgo de pérdidas de “baja frecuencia, alta severidad” que pueden ocurrir como resultado de eventos como reclamos de terceras partes resultantes de errores y omisiones, pérdida física de valores, fraude de empleados o terceras partes, y desastres naturales.

37. Sin embargo, los bancos deben ver las herramientas de mitigación del riesgo como complementarias a, más bien que un reemplazo para, el control operacional interno del riesgo minucioso. Tener mecanismos establecidos para reconocer y rectificar rápidamente errores legítimos de riesgo operacional que puedan reducir grandemente exposiciones. También se necesita una consideración cuidadosa a darse a la extensión a la cual las herramientas de mitigación de riesgo tales como seguro que verdaderamente reducen el riesgo, o transferir el riesgo a otro sector o área del negocio, o aún crear un nuevo riesgo.

38. Las inversiones en tecnología de procesamiento y seguridad de tecnología informática también son importantes para la mitigación del riesgo. Sin embargo, los bancos debe estar alertas de que la incrementada automatización podría transformar las pérdidas de alta frecuencia y baja severidad a pérdidas de baja frecuencia y alta severidad. Lo último puede asociarse con pérdida o interrupción extendida de servicios causados por factores internos o por factores que van más allá del control inmediato del banco (por ej., eventos externos). Dichos problemas pueden causar serias dificultades para los bancos y pueden amenazar la habilidad de una institución para realizar sus actividades clave de negocios. Como se discute a continuación en el Principio 7, los bancos deben establecer planes de reasunción de negocios y de contingencia que abarquen este riesgo.

39. Los bancos deben también establecer políticas sólidas para la administración de los riesgos asociados con actividades outsourcing. El outsourcing de actividades puede reducir el perfil de riesgo de la institución por la transferencia de actividades a otros con mayor experiencia y escala para administrar estos riesgos asociados con actividades de negocio especializadas. Sin embargo, el uso por un banco de terceras partes no disminuye la responsabilidad de la junta directiva y administración de asegurar que la actividad de la tercera parte sea realizada en una forma sana y sólida y en cumplimiento con leyes aplicables. Las actividades de outsourcing deben estar basadas en convenios legales rigurosos que aseguren

una clara asignación de responsabilidades entre los proveedores de servicio externo y el banco outsourcing. Adicionalmente, los bancos necesitan administrar cualesquiera riesgos residuales asociados con convenios outsourcing, incluyendo interrupción de servicios o riesgos de reputación.

40. Dependiendo de la importancia y críticamente de la actividad, los bancos deben comprender el impacto potencial sobre sus operaciones y sus clientes de cualesquiera deficiencias potenciales en servicios provistos por vendedores y otras terceras partes o proveedores de servicio intra-grupo, incluyendo averías y la falla potencial de negocio o incumplimiento de las partes externas. La junta y la administración deben asegurar que las expectativas y obligaciones de cada parte estén claramente definidas, comprendidas y aplicables. El alcance del pasivo de la parte externa y la habilidad financiera para compensar al banco por errores, negligencia, y otras fallas operacionales debe ser explícitamente considerada como parte de la evaluación de riesgo. Los bancos deben realizar pruebas de debida diligencia y monitorear las actividades de proveedores terceras partes especialmente aquellos con falta de experiencia del ambiente regulado de la industria bancaria. Para las actividades críticas, el banco puede necesitar considerar planes de contingencia, incluyendo la disponibilidad de partes alternativas externas y los costos y recursos requeridos para cambiar partes externas, potencialmente con un mínimo aviso.

41. En algunas instancias, los bancos pueden decidir ya sea retener un cierto nivel de riesgo operacional o auto-seguridad contra ese riesgo. Cuando este es el caso y el riesgo sea material, la decisión de retener o auto-asegurar el riesgo debe ser transparente dentro de la organización y debe ser consistente con la estrategia de negocios global del banco y su apetito de riesgo.

Principio 7: Los bancos deben tener establecidos planes de continuidad de contingencia y de negocios para asegurar su capacidad de operar en medio de tensiones y minimizar pérdidas en el evento de severa interrupción del negocio.

42. Por razones que pueden ir más allá del control de un banco, un evento severo puede resultar en la inhabilidad del banco en cumplir algunos o todas sus obligaciones de negocios, particularmente donde las estructuras físicas, de telecomunicación, o de tecnología de información han sido dañadas o inaccesibles. Esto puede, a la vez, resultar en pérdidas financieras significativas para el banco, como también interrupciones más amplias en el sistema financiero mediante canales como el sistema de pagos. Este potencial requiere que los bancos establezcan la reasunción de negocios y los planes de contingencia que toman en cuenta diferentes tipos de escenarios estimables a los cuales el banco puede ser vulnerable, proporcionado al tamaño y complejidad de las operaciones del banco.

43. Los bancos deben identificar procesos críticos de negocio, incluyendo aquellos donde exista dependencia sobre los vendedores externos u otras

terceras partes, para lo cual una reasunción rápida de servicio sería muy esencial. Para estos procesos, los bancos deben identificar mecanismos alternos para reasumir el servicio en caso de un paro. Se debe prestar particular atención a la habilidad para restablecer los registros electrónicos o físicos que son necesarios para la reasunción del negocio. Cuando dichos registros son resguardados en una instalación de gabinete, o donde las operaciones de un banco deben ser reubicadas a un nuevo lugar, debe cuidarse que estos lugares estén a una distancia adecuada de las operaciones impactadas para minimizar el riesgo que los registros primarios y resguardados y las ubicaciones estarán simultáneamente no disponibles.

44. Los bancos deben periódicamente revisar su planes de reasunción de negocios y de contingencia para que sean consistentes con las operaciones y estrategias de negocio actuales del banco. Además, estos planes deben ser probados en forma periódica para asegurar que el banco será capaz de ejecutar los planes en un evento incierto de una severa interrupción de negocios.

Rol de los Supervisores

Principio 8: Los supervisores bancarios deben requerir que todos los bancos, sin considerar el tamaño, tengan un marco efectivo establecido para identificar, evaluar, monitorear y controlar o mitigar los riesgos operacionales materiales como parte de un enfoque global a la administración de riesgo.

45. A la extensión en que los riesgos operacionales amenacen la seguridad y solidez de los bancos, los supervisores tienen la responsabilidad de animar a los bancos a desarrollar y usar mejores técnicas en la administración de estos riesgos. Consiguientemente, los supervisores deben requerir a los bancos desarrollar marcos de administración de riesgo operacional consistente con la directriz en este documento y proporcionada con su tamaño, complejidad y perfiles de riesgo.

Principio 9: Los supervisores deben conducir, directa o indirectamente, la evaluación independiente regular de las políticas, procedimientos y practicas de un banco relacionadas a los riesgos operacionales. Los supervisores deben asegurar que existan mecanismos apropiados de reporte establecidos que les permitan permanecer informados de los desarrollos en los bancos.

46. La evaluación independiente del riesgo operacional por parte de los supervisores debe incorporar una revisión de lo siguiente:

- El proceso del banco para evaluar la adecuación de capital global para el riesgo operacional en relación a su perfil de riesgo y, si es apropiado, sus objetivos de capital;

- La efectividad del proceso de administración y el entorno de control global del banco con respecto al riesgo operacional;
- Los sistemas del banco para monitorear y reportar su perfil de riesgo operacional, incluyendo datos sobre pérdidas operacionales y otros indicadores de riesgo operacional potencial;
- Los procedimientos del banco para la resolución oportuna y efectiva de los eventos y vulnerabilidades de riesgo operacional;
- El proceso de controles, revisiones y auditoría del banco para asegurar la integridad del proceso global de administración de riesgo operacional;
- La efectividad de los esfuerzos de mitigación del riesgo operacional del banco; y
- La calidad y comprensión de los planes de reasunción de negocios y de contingencia del banco.

47. Los supervisores deben también buscar asegurar que, donde los bancos sean parte de un grupo financiero, existan procedimientos establecidos para garantizar que el riesgo operacional sea administrado en una forma apropiada e integrada a través del grupo. En el desarrollo de esta evaluación, sería necesaria la cooperación e intercambio de información con otros supervisores, de acuerdo con los procedimientos establecidos. Algunos supervisores pueden escoger usar a los auditores externos en estos procesos de evaluación.

48. Las deficiencias identificadas durante la revisión del supervisor pueden ser dirigidas a través de un rango de acciones. Los supervisores deben usar las herramientas más adecuadas a las circunstancias particulares del banco y su ambiente operativo. Para que los supervisores reciban información actual sobre el riesgo operacional, pueden desear establecer mecanismos de reporte, directamente con bancos y auditores externos.

49. Dado al reconocimiento general de que los procesos comprensivos de administración de riesgo operacional aún están en desarrollo en muchos bancos, los supervisores deben tomar un papel activo en fomentar esfuerzos recurrentes de desarrollo interno para monitorear y evaluar las recientes mejoras y los planes para desarrollos futuros de un banco. Estos esfuerzos pueden entonces compararse con aquellos de otros bancos para proporcionar al banco con retroalimentación útil sobre la situación de su propio trabajo. Adicionalmente, a la extensión que existan razones identificadas de por qué ciertos esfuerzos de desarrollo han evidenciado ser inefectivos, dicha información podría ser provista en términos generales para ayudar en el proceso de planeación. Además, los supervisores deben enfocarse sobre la extensión a la cual un banco ha integrado el proceso de administración de riesgo operacional a través de toda su organización para asegurar la administración efectiva de la línea de negocio del riesgo operacional, para proporcionar claras líneas de comunicación y responsabilidad, y fomentar una activa auto-evaluación de las prácticas existentes y la consideración de posibles mejoras a la mitigación del riesgo.

Rol de la Divulgación

Principio 10: Los bancos deben hacer divulgación pública suficiente para permitir a los participantes del mercado evaluar su enfoque a la administración del riesgo operacional.

50. El Comité cree que la divulgación pública oportuna y frecuente de información relevante por parte de los bancos puede llevar a una disciplina de mercado mejorada y, por consiguiente, una más efectiva administración del riesgo. La cantidad de divulgación debe estar proporcionada con el tamaño y complejidad de las operaciones de un banco, como también a la demanda del mercado de tal información.

51. El área de divulgación de riesgo operacional aún no está bien establecida, principalmente debido a que los bancos aún están en el proceso de desarrollar las técnicas de evaluación de riesgo operacional. Sin embargo, el Comité cree que un banco debe divulgar su marco de administración de riesgo operacional en una forma que permitirá a los inversionistas y contrapartes determinar si un banco efectivamente identifica, evalúa, monitorea y controla el riesgo operacional.

Traducción de la Superintendencia de Bancos de Guatemala.