

(仮 訳)

バーゼル銀行監督委員会

健全なオペレーショナル・リスク管理のための諸原則

2011年6月

バーゼル銀行監督委員会
SIG オペレーショナル・リスク・サブグループ

議長：足立 光年、日本銀行

Australian Prudential Regulation Authority	Michael Booth
National Bank of Belgium	Jos Meuleman
Banco Central do Brasil, Brazil	Wagner Almeida
Office of the Superintendent of Financial Institutions, Canada	James Dennison
	Aina Liepins
China Banking Regulatory Commission	Meng Luo
Banque de France	Jean-Luc Quémard
Deutsche Bundesbank, Germany	Marcus Haas
Federal Financial Supervisory Authority (BaFin), Germany	Frank Corleis
Reserve Bank of India	Rajinder Kumar
Bank of Italy	Marco Moscadelli
日本銀行	宮村 円絵
金融庁、日本	長藤 剛
Surveillance Commission for the Financial Sector, Luxembourg	Didier Bergamo
Netherlands Bank	Claudia Zapp
Polish Financial Supervision Authority	Grazyna Szwajkowska
Central Bank of the Russian Federation	Irina Yakimova
South African Reserve Bank	Jan van Zyl
Bank of Spain	María Ángeles Nieto
Finansinspektionen, Sweden	Agnieszka Arshamian
Swiss Financial Market Supervisory Authority	Paul Harpes
Financial Services Authority, United Kingdom	Andrew Sheen
	Khim Murphy
Federal Deposit Insurance Corporation, United States	Alfred Seivold
Federal Reserve Board, United States	Adrienne Townes Haden
	Kenneth G. Fulton
Federal Reserve Bank of Boston, United States	Patrick de Fontnouvelle
Federal Reserve Bank of New York, United States	Ronald Stroz
Office of the Comptroller of the Currency, United States	Carolyn DuChene
	Maurice Harris
Office of Thrift Supervision, United States	Eric Hirschhorn
Financial Stability Institute	Amarendra Mohan
Secretariat of the Basel Committee on Banking Supervision, Bank for International Settlements	Andrew Willis

目 次

	頁
はじめに	1
監督当局の役割	2
オペレーショナル・リスク管理の諸原則	3
オペレーショナル・リスク管理の基本原則	9
ガバナンス	11
取締役会	11
上級管理職	13
リスク管理環境	15
リスクの特定と評価	15
モニタリングと報告	19
統制と削減	20
業務の復旧と継続	24
ディスクロージャーの役割	25
付：参考文献	27

健全なオペレーショナル・リスク管理のための諸原則

はじめに

1. バーゼル銀行監督委員会（以下、委員会）は、2003年2月に公表した「オペレーショナル・リスクの管理と監督に関するサウンド・プラクティス」（以下、サウンド・プラクティス）において、銀行業界と監督当局が遵守すべき原則の枠組を明確化した。委員会は、その後に公表した「自己資本の測定と基準に関する国際的統一化：改訂された枠組」において、業界のサウンド・プラクティスが進化し続けるという見通しを述べた¹。以後、銀行と監督当局はオペレーショナル・リスク管理の枠組（以下、「枠組」）を如何に実施するかについて、知識と経験を蓄積してきた。損失データの収集、定量的影響度調査、ガバナンスやデータやモデリングに関するプラクティスの幅の調査といった努力も、業界や監督当局の知識を深め、業界のサウンド・プラクティスを形成するための助けとなった。
2. 委員会は、上記の変化に対応するため、2003年に公表したサウンド・プラクティス文書を改訂し、現在業界で用いられている、より強固なオペレーショナル・リスク管理のサウンド・プラクティスを反映させるべきであると判断した。「健全なオペレーショナル・リスク管理のための諸原則」は、サウンド・プラクティスの進化を織り込み、健全なオペレーショナル・リスク管理に関する11の原則について詳述している。それらの原則では、（1）ガバナンス、（2）リスク管理環境、および（3）ディスクロージャーの役割、が取り上げられている。委員会は本改訂文書において、オペレーショナル・リスク管理にかかる業界のサウンド・プラクティスに沿って具体的な原則を提示することにより、サウンド・プラクティスの既存の枠組を強化している。これらの原則は、2003年以来、監督当局と業界が継続的に行ってきた意見交換の過程で形成されたものである。今回公表された「健全なオペレーショナル・リスク管理のための諸原則」は、2003年版サウンド・プラクティス文書を置き換えるものであり、委員会が2006年6月に公表した「自己資本の測定と基準に関する国際的統一化：改訂された枠組」のパラグラフ651に言及されている文書となる。

¹ バーゼル銀行監督委員会、「自己資本の測定と基準に関する国際的統一化：改訂された枠組」、パラグラフ646。

3. 「銀行組織における内部管理体制のフレームワーク」（委員会、1998年9月）は、オペレーショナル・リスクの分野で委員会が現在行っている作業の基盤である。いずれも監督当局向けの文書である「実効的な銀行監督のためのコアとなる諸原則」（委員会、2006年10月）および「コア・プリンシプル・メソドロジー」（同）、また、「自己資本の測定と基準に関する国際的統一化：改訂された枠組」の第二の柱において委員会が提示している諸原則も、銀行がオペレーショナル・リスクに関する方針、手続、リスク管理システムを設計する際に参照すべき重要な資料である。
4. 監督当局は今後とも銀行に対し、「オペレーショナル・リスク管理のためのより高度なシステムや実務を開発するにつれ、提供されている手法の中で漸次それに見合ったものに移行する」²ことを奨励する。したがって、本文書では業界で現在形成されつつあるサウンド・プラクティスについて述べているものの、監督当局は、銀行がオペレーショナル・リスク管理の手法を不断に改善することを期待する。また、本文書では銀行の「枠組」の主要な要素を取り上げている。それらの要素は、個別に切り離してとらえられるべきではなく、企業全体に適用されるオペレーショナル・リスク管理の総合的枠組の一部となるべきである。
5. 委員会は、本文書に述べられている原則は全ての銀行に適用可能なサウンド・プラクティスであると考ええる。委員会は、銀行がこれらの原則を適用する際に、それぞれの銀行の業務の性質、規模、複雑性およびリスク・プロファイルを考慮に入れることを前提としている。

監督当局の役割

6. 監督当局は、銀行の「枠組」に対する評価の一環として、オペレーショナル・リスクに関する銀行の方針、手続およびシステムを取り上げ、第三者の立場から直接ないし間接に定期検証する。監督当局は、銀行で事態がどのように推移しているかを当局が常に把握してられるよう、適切なメカニズムが設けられていることを確保する。
7. 監督当局は、オペレーショナル・リスクを評価する際、オペレーショナル・リスク管理の原則によりカバーされている分野を全て評価の対象とする。監

² バーゼル銀行監督委員会、「自己資本の測定と基準に関する国際的統一化：改訂された枠組」、パラグラフ 646。

監督当局はまた、銀行が金融グループに属している場合、グループ全体にわたって適切かつ統合的な手法でオペレーショナル・リスクを管理するプロセスと手続が設けられていることを確保しようとしている。こうした評価を行う際は、然るべき手続にしたがって、他の監督当局と協力したり情報を交換したりすることが必要となるかもしれない³。一部の監督当局は、こうした評価のプロセスに外部監査人を用いることを選択するかもしれない⁴。

8. 監督検証を通じて把握した問題点に対処する方法は様々である。監督当局は、個別銀行の状況や銀行を取り巻く営業環境に最も適した手段を用いる。監督当局は、オペレーショナル・リスクに関する最新の情報を入手するため、銀行や外部監査人との間に直接的な報告メカニズムを設けることを望むかもしれない（例えば、オペレーショナル・リスクに関する銀行内部の経営報告を定例的に監督当局に提出することを求める）。
9. 監督当局は、銀行が最近成し遂げた改善や今後の整備計画をモニターおよび評価することによって、銀行自らの継続的な取り組みを促すうえで引続き積極的な役割を果たす。銀行のこうした取り組みを他の銀行と比較し、その結果をフィードバックすれば、銀行は自らの作業の相対的位置付けを知ることができる。更に、一部の取り組みが何故効果を発揮しないかが判明した場合は、整備計画の策定プロセスを支援するため、一般的な表現を用いて当該情報を伝えることができる。

オペレーショナル・リスク管理の諸原則

10. オペレーショナル・リスク⁵は銀行の全ての商品、業務、プロセスおよびシステムに付随するリスクであり、同リスクを有効に管理することはこれまでも常に銀行のリスク管理計画の重要な一要素であった。したがって、オペレーショナル・リスクが健全に管理されているということは、銀行の取締役会や上級管理職が商品、業務、プロセスおよびシステムを有効に運営してい

³ 「新 BIS 規制のクロスボーダー実施に係る基本原則」（バーゼル銀行監督委員会、2003 年 8 月）、「オペレーショナル・リスクの先進的計測手法（AMA）に関わる母国・現地における監督当局の協力及び所要自己資本配分手法のための諸原則」（バーゼル銀行監督委員会、2007 年 11 月）を参照。

⁴ 「銀行監督当局と銀行の外部監査人との関係」（バーゼル銀行監督委員会、2002 年 1 月）。

⁵ オペレーショナル・リスクは、「内部プロセス・人・システムの不適切性または外生的事象から損失を被るリスク」と定義される。本定義には法務リスクが含まれるが、戦略リスクおよび評判リスクは含まれない。

るといふことの証左にほかならぬ。委員会は、銀行システム全体にわたりオペレーショナル・リスク管理の有効性を促進・強化することを目的として、本文書を公表する。

- 1 1. 一般にリスク管理とは、銀行を脅かすリスクを特定し、(可能であれば)それらのリスクに対するエクスポージャーを測定し、実効的な自己資本計画とモニタリング・プログラムが存することを確認し、リスク・エクスポージャーとそれに対応する所要自己資本を継続的にモニターし、リスク・エクスポージャーを統制および削減するための措置をとり、リスク・エクスポージャーと自己資本ポジションを上級管理職と取締役会に報告する、というプロセス全体を包摂する概念である。一方、内部統制は通常、銀行の日々の事務に組み込まれ、業務が効率的かつ効果的に行なわれていること、信頼性の高い情報が適時かつ完全に作成されていること、関連法規が遵守されていることを可能な限り確保するように設計されている。しかし、この二つの概念は実際には密接に関連しており、両者の違いを云々することよりも、それぞれの目的を達成することの方が重要である。
- 1 2. 銀行内部の健全なガバナンスは、オペレーショナル・リスク管理の実効的な「枠組」を支える礎である。オペレーショナル・リスク管理に係る内部ガバナンスの問題は、信用リスクやマーケット・リスクの管理に際して直面する問題と似通っているが、オペレーショナル・リスク管理を巡る課題は他のリスク・カテゴリーとは異なり得る。
- 1 3. 委員会は、オペレーショナル・リスクに係る健全なガバナンスを実務に導入する銀行が増えていることを認識している。オペレーショナル・リスクに係る業界共通の健全なガバナンスの実務は、しばしば三つの防衛線から成る。すなわち、業務ラインの管理、独立した全社的なオペレーショナル・リスク管理機能、および独立した検証である⁶。これら三つの防衛線がどの程

⁶ 「オペレーショナル・リスクの先進的手法のための監督指針」(バーゼル銀行監督委員会、2011年6月)において議論されている通り、独立した検証は以下の要素を含んでいる。

「枠組」の確認(Verification)は定期的に、通常、銀行の内部および(または)外部監査によって実施されるが、その他の適切な資格を有する独立した外部団体が関与することもある。確認(Verification)活動は、取締役会で承認された施策と一致している「枠組」全体の有効性を検査するほか、検証(Validation)プロセスが確実に独立し、既定の銀行の方針と一致した方法で確実に実施されていることを検査する。

検証(Validation)は、銀行が使用している計量システムが十分な頑健性を有し、その入力、仮定、プロセスおよび出力の整合性に対する保証を確実なものとするものである。特に、独立した検証(Validation)プロセスは、リスク計量方法が、銀行のオペレーショナル・リスク・プロファイルを十分に反映したオペレーショナル・リスク所要自己資本を

度公式に適用されるかは、銀行の性質、規模、複雑性、および業務のリスク・プロファイルに応じて異なる。しかし、いずれの場合にも、オペレーショナル・リスクに係るガバナンス機能は当該銀行の総合的なリスク管理のガバナンス構造に完全に組み入れられているべきである。

14. 業界実務においては、業務ラインの管理が防衛の第一線となる。すなわち、オペレーショナル・リスクに係る健全なガバナンスにおいては、商品、業務、プロセスおよびシステムに付随するリスクを特定および管理する責任を負うのは当該商品等にそれらの義務を有する業務ラインである、ということが認識されている。
15. 防衛の第二線は通常、機能的に独立した全社的なオペレーショナル・リスク機能 (corporate operational risk function、CORF)⁷である。一般に、本機能が業務ラインのオペレーショナル・リスク管理活動を補完している。CORFがどの程度独立性を有するかは銀行によって異なる。小規模銀行では、他の機能と職責を分離し、独立した立場からプロセスや機能を検証することによって独立性を確保しているかもしれない。大規模銀行では、CORFはリスクの発生源である業務ラインとは異なる報告ラインを有し、銀行全体のオペレーショナル・リスクの枠組を設計・維持し、継続的に開発する責任を負う。CORFには、オペレーショナル・リスクの測定と報告のプロセス、リスク委員会、および取締役会への報告に係る責任が含まれ得る。CORFの重要な機能のひとつは、銀行全体のリスク管理システムおよびリスク計測・報告システムに対する業務ラインからのインプット、および同システムから業務ラインへのアウトプットを批判的に検証することである。CORFは、同機能に課されている様々な責任を有効に果たすため、オペレーショナル・リスク管理の分野に専門知識を有する人材を十分確保すべきである。
16. 防衛の第三線は、オペレーショナル・リスク管理に係る統制、プロセスおよびシステムについて、独立した検証と批判を受けることである。この検証は、所要の能力を有し、適切な訓練を受け、「枠組」の構築・実施・運用に関与していない者によって行われなければならない。こうした検証は、監

算出することに、より一層の保証を与えるべきである。内部的検証 (Validation) の定量的側面に加え、オペレーショナル・リスク・モデルのデータ入力、方法論および出力に対する検証 (Validation) も全てのプロセスに亘り重要である。

⁷ 多くの法域で、独立した全社的なオペレーショナル・リスク機能は「全社的なオペレーショナル・リスク管理機能 (corporate operational risk management function)」と呼ばれている。

査機能もしくは検証の対象となるプロセスやシステムから独立した職員が行ってもよいが、適切な要件を満たす外部者に依頼することもできる。

17. オペレーショナル・リスク統制が上記の三つの防衛線から成るモデルを採用している場合でも、防衛三線の構造や活動内容は、各銀行の商品、業務、プロセスおよびシステムの内容、規模およびリスク管理手法によってしばしば異なる。三つの防衛線が強固なリスク文化を共有し、緊密なコミュニケーションを保っていることは、オペレーショナル・リスクに係る良好なガバナンスの重要な要件である。
18. 内部監査は、「枠組」が所期のとおり適用され、有効に機能していることを独立の立場から検証するために不足のない範囲で行なわれるべきである⁸。監査業務を外部に委託する場合は、前提となる取決めの実効性、および、外部委託した監査機能に防衛の第三線を依存することの適切性を上級管理職が検討すべきである。
19. 内部監査の責務には、銀行全体を見渡して、「枠組」とそれに関連するガバナンス・プロセスが総合的に適切かつ十分であるか否かを評価することが含まれる。内部監査は、単に取締役会の定めた方針や手続が遵守されているか否かを検証するにとどまらず、「枠組」が組織全体のニーズや監督当局の期待を満たしているか否かを評価すべきである。たとえば、具体的なリスク選好度やリスク許容度を設定することは内部監査の権限外であるとしても、如何にそうした限度が設定され、また、そうした限度が環境変化に応じて何故また如何に変更されるかのプロセスの頑健性は内部監査において検証されるべきである。
20. オペレーショナル・リスク管理は進化の途上にあり、また業務環境は絶え間なく変化するため、経営陣は、「枠組」の方針、手続およびシステムが常に十分な頑健性を維持していることを確保すべきである。オペレーショナル・リスク管理が改善されるか否かは、オペレーショナル・リスク管理者の問題意識がどの程度取り上げられ、また、同管理者の警告に対して上級管理職がどの程度迅速かつ適切に対応する用意があるかに依存する。

⁸ 内部監査および外部監査の役割については、「銀行の内部監査および監督当局と監査人との関係」（パーゼル銀行監督委員会、2001年8月）に詳しい。

オペレーショナル・リスク管理の基本原則

原則1：取締役会は、強靱なリスク管理文化を育成するため、自ら指導的な役割を果たすべきである。取締役会と上級管理職⁹は、強靱なリスク管理によって導かれる企業文化を育成すべきである。取締役会と上級管理職が育成する企業文化はまた、適切な基準とインセンティブを支持および提示することによって、職業意識と責任感に基づく行動を促すものとなるべきである。この観点から、強靱なオペレーショナル・リスク管理の文化¹⁰が組織全体に存することを確保する責任は、取締役会に存する。

原則2：銀行は、「枠組」を構築、実施および維持し、銀行の総合的なリスク管理プロセスに完全に組み入れるべきである。個別銀行が選択するオペレーショナル・リスク管理の「枠組」は、それぞれの銀行の性質、規模、複雑性、リスク・プロファイルを含む様々な要因に依存する。

ガバナンス¹¹

取締役会

原則3：取締役会は、「枠組」を設定・承認し、定期的に検証すべきである。取締役会は上級管理職を監督し、方針、プロセスおよびシステムが全ての意思決定レベルにおいて有効に実施されていることを確保すべきである。

原則4：取締役会は、オペレーショナル・リスクに係るリスク選好度ないしリスク許容度¹²を定めた趣意書（statement）を承認し、検証すべきである。本趣

⁹ 本文書では、経営陣が取締役会と上級管理職により構成されていることを前提とする。委員会は、取締役会や上級管理職の機能に係る法規の枠組が国によって大きく異なることを認識している。一部の国では、取締役会の唯一とは言わないまでも主要な機能は、執行部（上級管理職、総括マネジメント）が与えられた任務を確実に遂行するよう監督することにある。このため、取締役会は監督委員会（supervisory board）と呼ばれることがある。この場合、取締役会には執行機能がない。他の国では、取締役会がより広い権能を持ち、銀行経営の全般的な枠組を設定している。こうした相違点に鑑み、本文書においては、取締役会および上級管理職という用語を法律的な構成概念としてではなく、銀行内における二つの決定機能を表象する用語として用いる。

¹⁰ 企業内部のオペレーショナル・リスク文化とは、当該企業がオペレーショナル・リスク管理に取り組む意欲と様式を決定する、個人レベルおよび企業レベルの価値観、姿勢、能力および行動の総体を意味する。

¹¹ 「コーポレート・ガバナンスを強化するための諸原則」（バーゼル銀行監督委員会、2010年10月）も参照されたい。

¹² 「リスク選好度」とは、銀行がリスクとリターンの特性を考慮のうえ、どの程度のリスクを引き受けるかを定めるハイレベルの意思決定である。この用語は、将来的なリスク受

意書には、当該銀行として、どのような性質、タイプおよび水準のオペレーショナル・リスクを引き受ける用意があるかが明記されているべきである。

上級管理職

原則5：上級管理職は、明快、実効的かつ頑健なガバナンス構造を構築し、取締役会の承認を受けるべきである。同構造には、明確に定義され、透明性と一貫性を備えた責任系統が設けられているべきである。上級管理職は、自行の主要な商品、業務、プロセスおよびシステムに伴うオペレーショナル・リスクを管理するための方針、プロセスおよびシステムを組織全体にわたって一貫性をもって実施し、維持することについて責任を有する。上級管理職は、定められたリスク選好度ないしリスク許容度との整合性に配慮しつつ本責任を果たすべきである。

リスク管理環境

リスクの特定と評価

原則6：上級管理職は、リスクとインセンティブが十分に理解されるように、全ての主要な商品、業務、プロセスおよびシステムに付随するオペレーショナル・リスクが特定および評価されることを確保すべきである。

原則7：上級管理職は、全ての新しい商品、業務、プロセスおよびシステムが所定の承認プロセスを経て導入されること、また、同プロセスにおいてオペレーショナル・リスクも十分に評価されることを確保すべきである。

モニタリングと報告

原則8：上級管理職は、オペレーショナル・リスク・プロファイルと大規模な損失エクスポージャーを定期的にモニターするプロセスを実施すべきである。オペレーショナル・リスクの能動的管理を支えるものとして、取締役会、上級管理職および業務ラインの各レベルに適切な報告メカニズムが設けられているべきである。

容についての考え方であると解釈されることが多い。「リスク許容度」とは、業務上掲げた目標からどの程度乖離することを認めるかを定める、より具体的な意思決定である。この言葉は、銀行が受け入れる用意のあるリスク量を意味すると受け止められることが多い。本文書では、この二つの用語を同義として用いる。

統制と削減

原則 9：銀行は、方針とプロセスとシステム、適切な内部統制、適切なリスク削減および（または）リスク移転戦略から成る、強靱な統制環境を整備すべきである。

業務の復旧と継続

原則 10：銀行は、業務の復旧と継続に関する計画を策定し、業務に基だしい混乱が生じた場合にも事務を継続し、損失の拡大を防ぐ能力を確保すべきである。

ディスクロージャーの役割

原則 11：銀行のパブリック・ディスクロージャーは、当該銀行がオペレーショナル・リスク管理に如何に取り組んでいるかを利害関係者が評価できるような方法で行われるべきである。

オペレーショナル・リスク管理の基本原則

原則 1：取締役会は、強靱なリスク管理文化を育成するため、自ら指導的な役割を果たすべきである。取締役会と上級管理職は、強靱なリスク管理によって導かれる企業文化を育成すべきである。取締役会と上級管理職が育成する企業文化はまた、適切な基準とインセンティブを支持および提示することによって、職業意識と責任感に基づく行動を促すものとなるべきである。この観点から、強靱なオペレーショナル・リスク管理の文化が組織全体に存することを確保する責任は、取締役会に存する。

2.1. リスク管理と業務上の倫理について確固とした文化が確立されている
銀行は、大きなダメージにつながり得るオペレーショナル・リスク事象に見舞われる蓋然性が低く、仮にそうした事象が起こったとしても、より実効的に対応することができる。取締役会と上級管理職の行動、方針、プロセスおよびシステムは、健全なリスク管理文化の礎である。

2.2. 取締役会は、行動規範ないし倫理規定を設け、公正性（integrity）や倫理感について最も高い期待水準を明確に掲げるべきである。行動規範や倫理規定においては、容認される業務行動・禁止される業務行動を特定すべきである。期待と説明責任が明確にされていることにより、銀行職員はリスク

に関する自らの役割と責任、および行動を起こす権限を理解することができる。上級管理職がリスク管理と行動倫理を一貫して支援することは、行動規範と倫理、報酬戦略および研修プログラムを説得力をもって推進することにつながる。報酬政策は、定められたリスク選好度ないしリスク許容度、長期的戦略の方向性、財務上の目標、および総合的な安全性と健全性に沿ったものとするべきである。また、報酬政策はリスクと報償¹³を適切にバランスさせたものとするべきである。

- 2 3. 上級管理職は、組織内のあらゆるレベルにおいて、オペレーショナル・リスクに関する適切な水準の研修が提供されることを確保すべきである。研修の内容は、対象となる職員の職位、役割および責任に応じて異なるべきである。

原則 2：銀行は、「枠組」を構築、実施および維持し、銀行の総合的なリスク管理プロセスに完全に組み入れるべきである。個別銀行が選択するオペレーショナル・リスク管理の「枠組」は、それぞれの銀行の性質、規模、複雑性、リスク・プロファイルを含む様々な要因に依存する。

- 2 4. 健全なリスク管理の基本的な前提条件は、取締役会と管理職が自行の商品、サービスおよび業務に付随するリスクの性質と複雑性を全体として理解していることである。このことはオペレーショナル・リスクにおいて特に重要である。なぜなら、オペレーショナル・リスクは全ての商品、業務、プロセスおよびシステムに内在するからである。

- 2 5. オペレーショナル・リスクの性質と複雑性を理解するために必要不可欠な手段は、「枠組」の構成要素を自行の総合的なリスク管理プロセスの中に完全に組み入れることである。「枠組」は、グループ・レベルや業務ライン・レベルなど、組織のあらゆるレベルにおいてリスク管理プロセスに適切に組み入れられるべきである。新規に採用する業務、商品、システム、プロセスも例外ではない。また、オペレーショナル・リスクの評価結果は、総合的な業務戦略の策定プロセスに織り込まれるべきである。

- 2 6. 「枠組」は、取締役会により承認された方針として包括的かつ適切に文書化されているべきである。また、「枠組」ではオペレーショナル・リスク

¹³ 「報酬実務におけるリスクと業績の調整手法」（バーゼル銀行監督委員会、2011年5月）、「健全な報酬慣行に関する原則」（金融安定化フォーラム、2009年4月）、『健全な報酬慣行に関する原則』実施基準」（金融安定理事会、2009年9月）も参照されたい。

やオペレーション上の損失が定義されているべきである。オペレーショナル・リスクや同リスクに係る損失エクスポージャーが適切に定義され、分類されていない場合、「枠組」の有効性は大幅に低下する惧れがある。

27. 「枠組」を記した文書においては、以下のことが明確に述べられているべきである。

- (a) 報告ラインや説明責任を含め、オペレーショナル・リスク管理のために用いられるガバナンス構造を特定する
- (b) リスク評価の手段、および、それらの手段がどのように用いられるかを説明する
- (c) 容認されるオペレーショナル・リスク選好度ないしは許容額、固有リスクと残余リスクの閾値ないし限度額、承認されているリスク削減戦略およびリスク削減手段について説明する
- (d) 固有リスクおよび残存リスクに対するエクスポージャーの閾値ないし限度額を設定およびモニターする方法について説明する
- (e) リスクを報告するプロセスおよび経営情報システム（MIS）を設ける
- (f) オペレーショナル・リスクの用語に共通の定義を与え、リスクの特定、エクスポージャーの評価、リスク管理目標の設定が一貫性を持って行なわれることを確保する¹⁴
- (g) オペレーショナル・リスクについて独立した立場から適切な検証および評価が行なわれるプロセスを設ける
- (h) オペレーショナル・リスク・プロファイルが大きく変化した場合は必ず方針の検証を行い、必要な改訂を行うことを義務付ける

ガバナンス

取締役会

原則3：取締役会は、「枠組」を設定・承認し、定期的に検証すべきである。取

¹⁴ オペレーショナル・リスクの用語に一貫性のある定義が与えられていない場合、リスクを特定・分類することや、リスクの評価・モニタリング・統制・削減に係る責任を割り当てることができなくなる惧れが大きい。

取締役会は上級管理職を監督し、方針、プロセスおよびシステムが全ての意思決定レベルにおいて有効に実施されていることを確保すべきである。

28. 取締役会は以下のことを行なうべきである。

- (a) オペレーショナル・リスクを管理する文化、そして、そのプロセスをサポートするプロセスを確立する。それにより、自行の戦略や業務に付随するオペレーショナル・リスクの性質や範囲に関する理解を深め、組織内の全リスクを管理するための総合的な枠組に統合、もしくは、調和するような動的な監視および統制環境を整備する
- (b) 上級管理職に対し、「枠組」の基盤となる諸原則について明瞭なガイダンスと指示を与え、上級管理職が同原則に則って策定した方針を承認する
- (c) 「枠組」を定期的に検証し、市場の変化やその他の外部環境要因から生じたオペレーショナル・リスクや、新たな商品、業務、プロセス、システム（業務量の変化など、リスク態様や優先順位の変化を含む）に係るオペレーショナル・リスクが特定・管理されていることを確保する
- (d) 自行の「枠組」が、監査人ないしその他の適切に訓練された者によって、独立の立場から有効に検証されることを確保する
- (e) 経営陣が業界のベスト・プラクティスの進化¹⁵に伴い、その利用を図ることを確保する

29. 強固な内部統制はオペレーショナル・リスク管理の決定的に重要な側面である。取締役会は、強固な統制環境の実現に関し、経営陣の責任および説明責任の系統を明確にすべきである。統制環境が強固であるためには、オペレーショナル・リスクを管理する機能、業務ライン、およびサポート機能が互いに適切に独立している、もしくは分離されているべきである。

原則4：取締役会は、オペレーショナル・リスクに係るリスク選好度ないしリスク許容度を定めた趣意書（statement）を承認し、見直すべきである。本趣意書には、当該銀行として、どのような性質、タイプおよび水準のオペレーショナル・リスクを引き受ける用意があるかが明記されているべきである。

¹⁵ バーゼル銀行監督委員会、「自己資本の測定と基準に関する国際的統一化：改訂された枠組」、パラグラフ 718(xci)。

30. 取締役会は、リスク選好度ないしリスク許容度にかかる趣意書を承認および検証するにあたり、関連する全てのリスク、自行のリスク回避度、現在の財務状況、および戦略の方向性を勘案すべきである。同趣意書は、銀行内の様々なオペレーショナル・リスク選好度を包摂し、それらのリスク選好度が整合的であることを確保すべきである。取締役会は、具体的なオペレーショナル・リスクに設定された適切な閾値あるいは限度額（thresholds or limits）、および、総合的なオペレーショナル・リスク選好度ないし許容額を承認すべきである。
31. 取締役会は、限度額や、総合的なオペレーショナル・リスク選好度ないし許容額に係る趣意書の適切性を定期的に検証すべきである。本検証に際しては、外部環境の変化、業務量や活動量の大幅な増大、統制環境の質、リスク管理やリスク削減に係る戦略の有効性、損失実績、および限度額超過の頻度・程度・性質を考慮に入れるべきである。取締役会は、経営陣がリスク選好度ないしリスク許容度に係る趣意書を遵守しているか否かをモニターし、違反が早期に把握され、是正措置が講じられるよう図るべきである。

上級管理職

原則5：上級管理職は、明快、実効的かつ頑健なガバナンス構造を構築し、取締役会の承認を受けらるべきである。同構造には、明確に定義され、透明性と一貫性を備えた責任系統が設けられているべきである。上級管理職は、自行の主要な商品、業務、プロセスおよびシステムに伴うオペレーショナル・リスクを管理するための方針、プロセスおよびシステムを組織全体にわたって一貫性をもって実施し、維持することについて責任を有する。上級管理職は、定められたリスク選好度ないしリスク許容度との整合性に配意しつつ本責任を果たすべきである。

32. 上級管理職は、批判的な意見を述べる事が可能な確固としたメカニズムや、問題を解決するための有効なプロセスを設定・維持することに責任を有する。こうしたメカニズムやプロセスには報告や事後検証のシステムが含まれ、また、必要な場合には問題解決のために案件を上層部の適切なレベルに上げてゆくプロセスも含まれる。銀行は、三つの防衛線から成るアプローチが十分に機能していることを証明し、このアプローチが適切かつ満足すべき手法で実施され、機能することを確保するため、取締役会と上級管理職がどのような対策を講じているかを説明することができるべきである。

33. 上級管理職は、取締役会が設定したオペレーショナル・リスク管理の「枠組」に基づいて、具体的な方針や手続を策定すべきである。それらの方針や手続は、様々な業務単位において実施され、検証を受ける。上級管理職は、権限と責任と報告関係を明確に付与することにより、説明責任を促進・維持すべきである。上級管理職はまた、リスク選好度ないしリスク許容度に係る趣意書に沿ってオペレーショナル・リスクを管理することが可能となるよう、所要の経営資源を確保すべきである。更に上級管理職は、それぞれの業務単位で行なわれている活動に付随するリスクに照らし、経営陣による監督プロセスが適切であることを確保すべきである。
34. 上級管理職は、オペレーショナル・リスクの管理に責任を有する職員が、信用リスク、マーケット・リスク、その他のリスクの管理に責任を有する職員、および、保険によるリスクの移転やアウトソーシングの取極めなど外部サービスの調達に責任を有する職員との間で、実効的な調整や意思疎通を図ることを確保すべきである。これが行なわれていない場合、総合的なリスク管理プログラムに重大な間隙や重複が生じる惧れがある。
35. CORF（オペレーショナル・リスク機能）のマネージャーは、職責を有効に果たすため、銀行内で十分に高い地位を与えられているべきである。オペレーショナル・リスク機能のマネージャーは、信用リスク、マーケット・リスク、流動性リスクなど、他のリスク管理機能のマネージャーと同等の（commensurate）地位を与えられているべきであり、職位によってそれが明確であることが望ましい。
36. 上級管理職は、所要の経験、技能、および経営資源へのアクセスを有する職員によって業務が遂行されることを確保すべきである。リスク方針の遵守をモニターおよび執行する立場にある職員は、モニターの対象となる業務単位から独立した権限を有するべきである。
37. 銀行のガバナンス構造は、業務の性質、規模、複雑性、およびリスク・プロファイルに即しているべきである。オペレーショナル・リスクに係るガバナンス構造を設計する際、銀行は以下のことを考慮すべきである。
- (a) 委員会の構造 — 本部機能（central group function）と、同機能から独立した業務単位から成る大規模で複雑な銀行の場合、取締役会によって企業レベル（enterprise level）に設けられたリスク委員会が全リスクを監視し、この委員会に経営執行レベル（management level）のオペレーショナル・リスク委員会が報告を行なう、という構造が業界

のサウンド・プラクティスである。企業レベルのリスク委員会は、当該銀行の性質や規模や複雑性に応じて、国別、業務別ないし機能別に設けられたオペレーショナル・リスク委員会から情報提供を受ける。小規模で複雑性の低い銀行は、取締役会のリスク管理委員会が直接オペレーショナル・リスクを監視するという、より平坦な組織構造を用いてもよい。

- (b) 委員会の構成 — オペレーショナル・リスク委員会（小規模銀行の場合はリスク委員会）には、銀行実務、財務管理ないし独立した立場でリスク管理を担当するメンバーが参加することが業界のサウンド・プラクティスとなっている。また、いくつかの法域では既に要件となっているように、委員会には独立した非執行取締役メンバーが加わることもある。
- (c) 委員会の活動 — 委員会は、生産的な議論と意思決定を行なうことができるよう、十分な時間と経営資源を与えられ、適切な頻度で会合すべきである。委員会の実効性を検証・評価することが可能であるよう、委員会の活動は適切に記録されるべきである。

リスク管理環境

リスクの特定と評価

原則 6： 上級管理職は、全ての主要な商品、業務、プロセスおよびシステムに付随するオペレーショナル・リスクが特定および評価され、それらのリスクとインセンティブが十分に理解されることを確保すべきである。

38. リスクの特定と評価は有効なオペレーショナル・リスク管理システムの基本である。リスクを有効に特定するためには、内部要因¹⁶と外部要因¹⁷の双方を考慮する必要がある。銀行は、リスクを正しく評価することによって、自らのリスク・プロファイルをより正確に把握し、リスク管理の資源と戦略を最も効果的に振り向けることができるようになる。

39. オペレーショナル・リスクを特定および評価するために用い得る手段には以下が含まれる。

¹⁶ たとえば、銀行の構造、業務の性質、人的資源の質、組織の改変、職員の定着状況など。

¹⁷ たとえば、全般的環境や業界の変化、テクノロジーの進歩など。

- (a) 内部監査の発見事項：監査の発見事項は主として統制の弱点や脆弱性に焦点が当てられるが内部あるいは外部の要因に起因する固有リスクに係る示唆が得られることもある。
- (b) 内部的な損失データの収集と分析：オペレーショナル損失にかかる内部データは、オペレーショナル・リスクに対する自行のエクスポージャーや内部統制の有効性を評価するための有意義な情報である。損失事象を分析すれば、大規模損失の原因について示唆を得ることができるほか、統制上の問題が局所的なものなのかシステム全体に共通するものなのかについての情報も得られる¹⁸。銀行は、オペレーショナル・リスクに対するエクスポージャーの全貌をより完全に把握するため、信用リスクやマーケット・リスクに係る損失にオペレーショナル・リスクがどの程度寄与しているかを把握およびモニターすることが有益であると考えられるかもしれない。
- (c) 外部データの収集と分析：外部データとは、自行以外の組織に生じたオペレーション上の損失事象に係る、グロス損失額、日付、回収額、原因情報などである。外部損失データは、内部損失データと比較することができるほか、自行の統制環境の問題点を検証したり、これまで特定していなかったリスク・エクスポージャーに注意を向けたりするために用いることもできる。
- (d) リスクの評価：リスクの評価は、しばしば「リスクの自己評価(Risk Self Assessment、RSA)」と呼ばれる。銀行は RSA において、種々の潜在的脅威や脆弱性を勘案のうえ、自行の事務遂行プロセスを評価し、それらの脅威や脆弱性からどのような影響を受け得るかを検討する。「リスク・統制の自己評価 (Risk Control Self Assessments、RCSA)」も類似した手法である。RCSA では通常、固有リスク（統制が行なわれる以前のリスク）、統制環境の有効性、および残余リスク（統制が行なわれた後も残存するリスク）を評価する。RCSA を用いてスコアカード方式の採点を行なうこともある。すなわち、残余リスクにウェイト付けすることによって RCSA の評価結果を数値に変換し、統制環境における残余リスクを相対的に格付することができる。
- (e) 業務プロセスのマッピング：業務プロセスのマッピングは、業務プロ

¹⁸ 特に大規模銀行の場合は、「自己資本の測定と基準に関する国際的統一化：改訂された枠組」（バーゼル銀行監督委員会、2006年6月）の付属文書8および9に定義されている「レベル1の業務ライン」および「損失事象のタイプ」に内部損失データをマッピングすれば、外部損失データとの比較を容易に行なうことができる。

セス、業務活動および組織機能の要所を特定する作業である。総合的な業務プロセスの何処に重大なリスクが存するかも特定される。プロセス・マップは、個別のリスク、リスクの相互依存関係、および統制やリスク管理が弱い部分を明らかにする。また、経営陣が今後とるべき対応に優先順位をつけるうえでも有用である。

- (f) リスクとパフォーマンスの指標：リスクとパフォーマンスの指標とは、銀行のリスク・エクスポージャーを示唆する数値および（または）統計である。リスク指標は、しばしば「主要リスク指標（Key Risk Indicators、KRI）」と呼ばれる。KRIは、主要リスクに対するエクスポージャーの主なドライバーをモニターするために用いられる。パフォーマンス指標は、しばしば「主要パフォーマンス指標（Key Performance Indicators、KPI）」と呼ばれ、業務プロセスがどのような状態にあるかを示唆する。この情報により、オペレーショナル・リスク管理上の脆弱性、欠陥、および損失発生の可能性について示唆が得られる可能性がある。リスクとパフォーマンスの指標は、しばしば、重要問題を上層部の適切なレベルに上げてゆくプロセスのトリガーと組み合わせで用いられる。リスクの水準が閾値あるいは限度額を超え、早急な削減計画が必要な場合は、トリガーが警告を発する。
- (g) シナリオ分析：シナリオ分析は、業務ラインやリスク管理者からエキスパートとしての意見を聴取し、どのようなオペレーショナル・リスク事象が起こり得るか、また、それによってどのような結果が生じ得るかを特定するプロセスである。シナリオ分析は、大規模なオペレーショナル・リスクが何処から生じ得るか、また、リスク管理上の追加的な統制や削減措置が必要か否かを検討するための有効な手段である。シナリオ分析のプロセスは主観性が高いため、堅固なガバナンスの枠組を設けてプロセスの公正性や一貫性を確保することが不可欠である。
- (h) 測定：大規模銀行は、リスク評価手段から得られた結果をオペレーショナル・リスク・エクスポージャー推計モデルへの入力情報とすることにより、オペレーショナル・リスクに対するエクスポージャーを定量化することが有益であると考えられるかもしれない。モデルから算出された結果は、経済資本プロセスに用いたり、業務ラインに配分してリスクとリターンを結び付けるために用いたりすることができる。
- (i) 比較分析：比較分析とは、自行のオペレーショナル・リスク・プロファイルをより包括的に把握するため、様々な評価手段から得られた結果を比較することである。たとえば、損失事象の頻度や規模に係る内

部データを RCSA と比較すれば、自己評価プロセスが有効に機能しているか否かを見極めることができる。シナリオ分析から得られたデータを内部データや外部データと比較すれば、潜在的リスク事象に対するエクスポージャーの大きさをより正確に把握することができる。

40. 銀行は内部的な価格付け、パフォーマンスの測定に当たってオペレーショナル・リスクが適切に考慮されることを確保すべきである。さもなければ、リスク・テイキングへのインセンティブと、リスク選考度およびリスク許容度が適切に調和しない可能性がある。

原則7：上級管理職は、全ての新しい商品、業務、プロセスおよびシステムが所定の承認プロセスを経て導入されること、また、同プロセスにおいてオペレーショナル・リスクも十分に評価されることを確保すべきである。

41. 一般に、銀行が新しい業務に取り組んだり新商品を開発したりする時、不慣れた市場に参入する時、新しい業務プロセスやテクノロジー・システムを導入する時、および（または）本部から地理的に離れた場所で営業する時は、オペレーショナル・リスク・エクスポージャーが拡大する。また、新しい商品、業務、プロセスおよびシステムが導入期のレベルから重要な収入源ないし業務運営上枢要な事務のレベルに移行する時には、リスクのレベルが上昇する。銀行は、リスク管理に係る統制の枠組が導入時点において適切であること、また、同枠組が新しい商品、業務、プロセスおよびシステムの拡大率ないし変化に即応していることを確保すべきである。

42. 銀行は、新しい商品、業務、プロセスおよびシステムを検証し、承認するプロセスについて、方針と手続を設けるべきである。検証と承認のプロセスにおいて検討されるべき事柄は

- (a) 新しい商品、サービス、業務に付随するリスク
- (b) それらの商品等の導入に伴って銀行のオペレーショナル・リスク・プロファイルや同リスクに対する選好度ないし許容度に生じる変化（既存の商品や業務に伴うオペレーショナル・リスクを含む）
- (c) 所要の統制やリスク管理プロセスやリスク削減戦略
- (d) 残余リスク
- (e) 関連するリスク閾値の変化、及び

(f) 新しい商品や業務のリスクを測定・モニター・管理するための手続と指標

である。承認プロセスには、新商品を導入する前に人的資源やテクノロジー基盤に適切な投資が行なわれることを確保する手順も含まれる。予期したオペレーショナル・リスク・プロファイルと大きく異なる点を把握したり、予想外のリスクを管理したりするため、新しい商品、業務、プロセスおよびシステムの導入状況はモニターすべきである。

モニタリングと報告

原則 8：上級管理職は、オペレーショナル・リスク・プロファイルと大規模な損失エクスポージャーを定期的にモニターするプロセスを実施すべきである。オペレーショナル・リスクの能動的管理を支えるものとして、取締役会、上級管理職および業務ラインの各レベルに適切な報告メカニズムが設けられているべきである。

4 3. 銀行は、オペレーショナル・リスクに関する報告の質を不断に改善することが望まれる。銀行は、報告が包括的かつ正確で、業務ラインや商品を横断して整合的かつ実施可能であることを確保すべきである。報告は適切な範囲と分量により行なわれるべきである。データが量的に過剰であったり過少であったりすると、有効な意思決定が阻害される。

4 4. 報告は適切なタイミングで行なわれるべきであり、銀行は正常な市場環境においてもストレス下の市場環境においても報告を作成する能力を有するべきである。報告の頻度は、関連するリスクや、事務環境に生じる変化の速度と性質に応じて決められるべきである。モニタリング活動の結果と、内部監査および（または）リスク管理機能による「枠組」の評価は、経営上層部や取締役会に定期的に提出する報告に織り込まれるべきである。監督当局が作成した報告（およびくまたは）監督当局のために作成した報告）は適切な場合においては銀行の上級管理職あるいは取締役会に供覧されるべきである。

4 5. オペレーショナル・リスクに関する報告には、内部的な財務、事務およびコンプライアンス関連の指標や、当該銀行の意思決定に影響を及ぼす事象や状況といった、外部的な市場・環境情報が含まれているかもしれない。オペレーショナル・リスクに関する報告には、下記のような内容が述べられているべきである。

- (a) リスク選好度ないしリスク許容度を定めた趣意書や閾値ないしは限度額に対する違反
- (b) 銀行内部に最近発生した大規模なオペレーショナル・リスク事象や損失に関する詳細情報
- (c) 関連する外部事象およびそれらの外部事象が当該銀行やオペレーショナル・リスクに配賦する資本にどのような影響を及ぼし得るか

46. リスク管理のパフォーマンスを不断に強化するとともに、リスク管理に係る方針・手続・実務を向上させるため、データ捕捉とリスク報告のプロセスは定期的に分析されるべきである。

統制と削減

原則9：銀行は、方針とプロセスとシステム、適切な内部統制、適切なリスク削減および（または）リスク移転戦略から成る、強靱な統制環境を整備すべきである。

47. 内部統制は、銀行が効率的かつ実効的に事務を遂行すること、資産を保全すること、信頼性の高い財務報告を作成すること、および適用される法規を遵守することについて、妥当な水準の保証が得られるように設計されているべきである。健全な内部統制・プログラムは、リスク管理プロセスに組み込まれた五つの要素から成る。すなわち、統制環境、リスク評価、統制活動、情報とコミュニケーション、およびモニタリング活動である¹⁹。

48. 統制のプロセスと手続には、定められた方針の遵守を確保するシステムが組み入れられているべきである。方針の遵守状況を評価する際の主要素には、たとえば以下のようなことが含まれる。

- (a) 定められた目標の達成状況をトップレベルで検証する
- (b) 経営陣の監督下で業務が遂行されていることを確認する
- (c) 違犯事例の取扱いと解決を検証する
- (d) 承認や許可に係る所定のプロセスを評価し、経営陣の適切なレベルに対する説明責任が全うされていることを確保する

¹⁹ 内部統制については、「銀行組織における内部管理体制のフレームワーク」（バーゼル銀行監督委員会、1998年9月）に詳しい。

- (e) 限度値超過の例外的承認、経営陣の裁量による適用除外、その他のかたちで方針が守られなかった事例に関する報告を追跡する

49. 実効的な統制環境を確保するためには、職責を適切に分離することも必要である。相反する職責を個人やチームに与え、しかも二重の統制体制を敷くなどの予防措置を講じなければ、損失、過失、その他の不適切な行動の隠蔽を許す結果となり得る。したがって、利益相反が潜在する領域は特定され、最小限にとどめられ、独立した立場から注意深くモニターおよび検証されるべきである。

50. 銀行は、オペレーショナル・リスクに対処するため、職責の分離と二重の統制に加え、その他の伝統的な内部統制が適宜設けられていることを確保すべきである。以下は、そうした伝統的な内部統制の例である。

- (a) 承認の権限および（または）プロセスを明確に定める
- (b) 設定されたリスク限度値の遵守状況を緊密にモニターする
- (c) 銀行の資産や記録を守るため、アクセスと利用に制限を設ける
- (d) 専門能力を維持するため、適切な職員数と研修体制を確保する
- (e) 収益が妥当な期待から乖離していると考えられる業務ラインや商品を特定する継続的なプロセスを設ける²⁰
- (f) 取引や勘定を定期的に検証および照合する
- (g) 休暇制度により、役職者や職員が職責を離れている期間を連続二週間以上設ける

51. 統制環境は、テクノロジーを効果的に使い、健全に運用することによって向上する可能性がある。たとえば、自動化されたプロセスは手作業に比べて過誤が生じにくい。しかし、自動化されたプロセスにもリスクが伴うため、テクノロジーの健全なガバナンスと、テクノロジー基盤に係るリスク管理プログラムによって対処しなければならない。

52. テクノロジーが絡んだ商品、サービス、業務、プロセスおよびデリバリー・チャンネルを用いる場合、銀行は戦略リスク、オペレーショナル・リスク

²⁰ たとえば、リスクが低くマージンが小さいと思われるトレーディング業務から高収益が生み出されている場合は、内部統制上の違犯によってそうした収益が達成された可能性が疑われる。

およびレピュテーション・リスクに晒され、大規模な財務上の損失を被る可能性がある。したがって、銀行はテクノロジー・リスクを特定、測定、モニターおよび管理するための総合的なアプローチを備えているべきである²¹。健全なテクノロジー・リスク管理の要件はオペレーショナル・リスク管理の要件と同様であり、以下のことを含む。

- (a) ガバナンスと監督による統制を通じ、アウトソーシングの取極めを含めてテクノロジーが銀行の業務目的に合致し、同目的を支援するものであることを確保する
- (b) リスクの特定と評価を支援するための方針と手続を設定する
- (c) リスク選好度ないしリスク許容度に係る趣意書とパフォーマンス期待値を設定することにより、リスクの統制と管理を支援する
- (d) 実効的な統制環境を整備するとともに、リスク移転戦略を用いてリスクを削減する
- (e) 方針に定められた限度値または限度額が遵守されているか否かを検証するモニタリング・プロセスを設ける

5.3. 経営陣は、銀行に健全なテクノロジー基盤²²が整っていることを確保すべきである。健全なテクノロジー基盤は、平常時の業務量と、市場ストレス下でピークに達した業務量の双方に対応し得る能力を有し、データやシステムの完全性 (integrity)、安全性および可用性 (availability) を保証し、総合的かつ包括的なリスク管理を支える。こうして、健全なテクノロジー基盤は業務遂行上の現在の需要と長期的な需要の双方に応える。合併や買収に伴ってテクノロジー基盤が断片化したり分断されたりした場合や、コスト削減策が採られた場合、あるいは投資が不十分な場合、銀行は、異なるリスク領域間や連結ベースで情報を総合・分析したり、業務ラインや法人別にリスクを管理・報告したり、急成長期にリスクを監視・管理したりする能力を損なわれかねない。経営陣は、適切な資本を投下するなどして堅固なテクノロジー基盤を常時確保すべきであり、特に、合併前や大幅な拡大戦略を開始する前、あるいは新商品を導入する前はこの点に配意する必要がある。

²¹ 「コンピューターおよび遠隔通信システムにおけるリスク」(バーゼル銀行監督委員会、1989年7月)および「電子バンキングにおけるリスク管理の原則」(同、2001年5月)も参照されたい。

²² テクノロジー基盤 (technological infrastructure) とは、情報技術や通信システムの物理的および理論的設計、それらを構成する個々のハードウェアとソフトウェア、データ、および稼動環境を意味する。

5 4. アウトソーシング²³とは、第三者（グループ内の系列会社もしくはは系列関係のない外部企業）に銀行の業務を代行させることを意味する。アウトソーシングの対象となり得るのは、取引処理ないし事務手続である。アウトソーシングは、コストを削減し、専門能力を導入し、提供商品を拡大し、サービスを向上させるための一助となり得るが、一方でリスクも伴うため、経営陣は当該リスクに対処すべきである。取締役会と上級管理職は、アウトソーシングの取極めに伴うオペレーショナル・リスクを理解し、アウトソーシング業務に存するリスクを管理するための有効な方針と実務が設けられていることを確保する責任を有する。アウトソーシングに関する方針とリスク管理活動には以下のことが含まれているべきである。

- (a) 業務をアウトソーシングすべきか、また如何にアウトソーシングするかを決定する手続
- (b) サービス提供者を選定する際のデュー・ディリジェンスのプロセス
- (c) アウトソーシングの取極めの健全な組成（データの帰属や守秘義務、契約打切りの権利を含む）
- (d) アウトソーシングの取極めに伴うリスクを管理およびモニターするためのプログラム（サービス提供者の財務状況を含む）
- (e) 銀行およびサービス提供者における有効な統制環境の整備
- (f) 実用に耐えるコンティンジェンシー・プランの策定
- (g) 包括的な契約および（または）サービス・レベル・アグリーメント（SLA）において、サービス提供者と銀行の責任分担を明確化すること

5 5. 内部統制によってリスクに適切に対処することができず、かつ、当該リスクから手を引くことが妥当な選択ではない場合、経営陣は保険などを通じて当該リスクを他者に移転することを検討することにより統制を補完してもよい。取締役会は、自行が引き受ける用意のある、また引き受ける財務能力のある損失エクスポージャーの上限を定め、自行のリスクと保険管理プログラムを年次で検証すべきである。具体的な保険やリスク移転の必要性については個々に判断されるべきであるが、多くの法域では考慮しなければならない規制上の要件が定められている²⁴。

²³ 「金融サービスのアウトソーシング」（ジョイント・フォーラム、2005年2月）も参照されたい。

²⁴ 「オペレーショナル・リスクのモデル化における保険のリスク緩和効果の認識」（バーゼ

56. リスク移転によって健全な統制やリスク管理のプログラムを完全に代替することはできない。したがって、リスク移転は、銀行内部でオペレーショナル・リスクを遺漏なく統制することに代わるものではなく、それを補足するものとして捉えられるべきである。明らかなオペレーショナル・リスク上の過失を早急に特定し、認識し、是正するメカニズムが整っていれば、エクスポージャーは大幅に削減される。保険などのリスク削減手段が実際にどの程度リスクを削減しているか、リスクを行内の他の業務部門や領域にどの程度移転しているか、あるいはどの程度新たなリスク（たとえばカウンターパーティー・リスク）をもたらしているか、についても注意深く検討する必要がある。

業務の復旧と継続

原則10：銀行は、業務の復旧と継続に関する計画を策定し、業務に甚だしい混乱が生じた場合にも事務を継続し、損失の拡大を防ぐ能力を確保すべきである²⁵。

57. 銀行は、何らかの突発的な事象の発生により業務が混乱するリスクに晒されている。事象の程度が極めて甚だしく、業務上の義務を履行することが部分的ないし全面的に不可能になる場合もあり得る。銀行の施設、通信システム、情報技術の基盤が破壊されたりアクセス不能になったりした場合や、伝染病の蔓延によって人的資源に損害を受けたりした場合、銀行が大規模な財務損失を蒙るばかりか、金融システム全体が機能不全に陥る惧れもある。銀行は、こうしたリスクに対する回復力を身に付けるため、業務の性質、規模や複雑性に応じた業務継続計画を策定すべきである。業務継続計画の策定に際しては、自行の脆弱な部分に生じ得る現実的な（likely）、ないし想定可能な（plausible）複数のシナリオを考慮に入れるべきである。

58. 業務継続性の管理には、業務に及ぶ影響の分析、回復戦略、テスト・訓練・認知度向上のためのプログラム、および、情報伝達と危機管理のプログラムが含まれているべきである。銀行は、決定的に重要な事務処理機能²⁶、

ル銀行監督委員会、2010年10月）も参照されたい。

²⁵ 健全な業務継続計画の諸原則については、「業務継続のためのハイレベルの諸原則」（バーゼル銀行監督委員会、2006年8月）に詳しい。

²⁶ 銀行の事務処理機能には、商品・サービスを送達したり中核業務を遂行したりするための施設・人・プロセス、および、テクノロジー・システムとデータが含まれる。

主な内部および外部依存性²⁷、および適切な回復レベルを特定すべきである。また、想定可能な業務混乱シナリオを分析のうえ、財務上、事務上およびレピュテーション上の影響を評価すべきであり、そのリスク評価は、回復戦略の策定に際して優先度や目標を設定するための材料とすべきである。業務継続計画には、コンティンジェンシー戦略、業務の回復と再開の手順、また、経営陣、職員、監督当局、顧客、業者および（そうすることが適切であれば）行政当局に情報を提供するためのコミュニケーション計画が含まれているべきである。

59. 銀行は、業務継続計画を定期的に検証し、コンティンジェンシー戦略が現時点における事務、リスクや脅威、求められる回復力、および回復の優先順位と整合的であることを確保すべきである。銀行はまた、職員が業務継続計画を効果的に実行できるよう、訓練や認知度向上のためのプログラムを実施すべきである。業務継続計画は定期的にテストし、回復や再開の目標が所定の時間的枠組の中で達成され得ることを確認すべきである。可能であれば、銀行は主要なサービス提供者と共に災害回復や業務継続のテストに参加すべきである。正式なテストの結果は、経営陣や取締役会に報告すべきである。

ディスクロージャーの役割

原則 11：銀行のパブリック・ディスクロージャーは、当該銀行がオペレーショナル・リスク管理に如何に取り組んでいるかを利害関係者が評価できるような方法で行われるべきである。

60. 銀行がオペレーショナル・リスク管理に係る適切な情報を一般に開示することは、透明性に資するとともに、市場規律を通じて業界実務を向上させる。開示情報の量とタイプは、各々の銀行の業務の規模、リスク・プロファイルおよび複雑性、ならびに業界実務の変化に則して決められるべきである。
61. 銀行は、自行が実効的にオペレーショナル・リスクを特定・評価・モニターおよび統制（削減）しているかどうかを利害関係者が判断できるような方法で、オペレーショナル・リスク管理の枠組を開示すべきである。
62. 銀行の情報開示は、上級管理職ならびに取締役会が自行のオペレーシ

²⁷ 外部依存の対象には、公共事業（utilities）、ベンダー、および系列外のサービス提供者が含まれる。

ナル・リスクを評価し、管理する方法と整合的であるべきである²⁸。

63. 銀行は、取締役会によって承認された公式の開示方針を持つべきである。開示方針は、自行のオペレーショナル・リスクに関する開示内容とそのプロセスについての内部統制を定めているべきである。加えて、銀行は開示の適切性（開示の検証や開示の頻度の適切性も含む）を評価するためのプロセスを実施すべきである²⁹。

²⁸ バーゼル銀行監督委員会、「自己資本の測定と基準に関する国際的統一化：改訂された枠組」、パラグラフ 646, 810。

²⁹ バーゼル銀行監督委員会、「自己資本の測定と基準に関する国際的統一化：改訂された枠組」、パラグラフ 646, 821。

参 考 文 献

「銀行組織における内部管理体制のフレームワーク」(バーゼル銀行監督委員会、1998年9月)

「銀行の内部監査および監督当局と監査人との関係」(バーゼル銀行監督委員会、2001年8月)

「銀行監督当局と銀行の外部監査人との関係」(バーゼル銀行監督委員会、2002年1月)

「実効的な銀行監督のためのコアとなる諸原則」(バーゼル銀行監督委員会、2006年10月)

「コア・プリンシプル・メソドロジー」(バーゼル銀行監督委員会、2006年10月)

「業務継続のためのハイレベルの諸原則」(バーゼル銀行監督委員会、2006年8月)

「金融サービスにおけるアウトソーシング」(ジョイント・フォーラム、2005年2月)

「電子バンキングにおけるリスク管理の原則」(バーゼル銀行監督委員会、2001年5月)

「コンピューターおよび遠隔通信システムにおけるリスク」(バーゼル銀行監督委員会、1989年7月)

「コーポレート・ガバナンスを強化するための諸原則」(バーゼル銀行監督委員会、2010年10月)

「オペレーショナル・リスクのモデル化における保険のリスク緩和効果の認識」(バーゼル銀行監督委員会、2010年10月)

「新 BIS 規制のクロスボーダー実施に係る基本原則」(バーゼル銀行監督委員会、2003年8月)

「オペレーショナル・リスクの先進的計測手法(AMA)に関わる母国・現地における監督当局の協力及び所要自己資本配分手法のための諸原則」(バーゼル銀行監督委員会、2007年11月)