



バーゼルⅡのための IT 統制目標

コンプライアンスのための
ガバナンスと
リスクの管理の
重要性

IT ガバナンス協会®

IT ガバナンス協会(ITGITM)(www.itgi.org)は、企業の情報技術の方向性とコントロールに関する国際レベルでの議論と標準化を推進するため 1998 年に設立された。効果的な IT ガバナンスは、IT によるビジネス達成目標のサポート、IT へのビジネス投資の最適化、および IT にかかわるリスクと機会の適切な管理を確実に保証する上で有用である。IT ガバナンス協会は、企業のリーダーや取締役会が IT ガバナンスにおける責務を果たす上で役立つ独自の調査内容、電子資料、および事例研究内容を提供している。

免責事項

ITGI と著者は、主として情報リスク管理担当者、IT 実務者や銀行専門家に対する教育を目的として、本書を作成した。ITGI と著者は、本書の使用に関するいかなる責任も負わない。本書は、すべての適切な手続やテストを含むものではなく、また、合理的に同じ結果を導く、本書に記載されていない手続およびテストを除外するものでもない。特定の手続およびテストの妥当性は、対象とするシステムまたは IT 環境における特定の統制の状況について十分に考慮し、専門家としての判断を下すべきである。

情報開示

© 2007 ITGI. All Rights Reserved. ITGI の書面による事前の許可無く、本書の全部または一部の使用、複写、複製、改変、配布、表示、検索システムへの組込、あらゆる形式および方法による送信(電磁的、機械的、写真複製、記録、その他の方法を問わず)を行うことを禁止する。学術、組織内および非営利の目的ならびにコンサルティング・アドバイザー業務での使用に限り、本書の全部または一部の複製が認められるが、出典を完全な形で表示しなければならない。本書に関する、その他の権利や許可は与えられない。

IT Governance Institute

3701 Algonquin Road, Suite 1010

Rolling Meadows, IL 60008 USA

Phone: +1.847.606.5700

Fax: +1.847.253.1443

E-mail: info@itgi.org

Web site: www.itgi.org

IT Control Objectives for BASELII の日本語版について

本著作物の内容

この著作物は、IT ガバナンス協会 (ITGI) の許諾の下、日本 IT ガバナンス協会 (ITGI Japan) が、IT Control Objectives for Basel II を英語から翻訳したものです。ITGI Japan は著作物の翻訳の正確さについてのみ、その責任を有します。

原著は、随所で CoBIT の内容に触れていますが、翻訳は、CoBIT4.1 日本語版の内容に整合するようにしています。また、BASEL II に関連する文章に関しては、既出の翻訳資料等が存在する中で、用語等は可能な限り整合するように翻訳作業を進めています。ただし、表現については異なる部分がございますので、その旨ご容赦下さい。

IT Control Objectives for BASELII の日本語版によせて

日本 IT ガバナンス協会は、日本語の文化圏の IT ガバナンスの向上を願って、以下の3つのミッションをもとに活動をおこなっています。

1. IT ガバナンスの世界の知識の日本語化
2. IT ガバナンスの日本化
3. 世界の IT ガバナンスへの貢献

一番目のミッションでは、COBIT をはじめとして、多くの英語の文献を、この2年間で翻訳してきました。ISACA の日本の支部の会員だけでなく、多くの企業、団体、個人の方々の寄付と貢献で、これらの活動は行なわれています。

今回も、そのひとつの追加として、KPMG ビジネスアシュアランス株式会社様の翻訳の貢献で、短時間で金融機関向けのバーゼル対応の IT のガイドラインの日本語版のリリースをご報告できることは、わが国の IT ガバナンスのプロフェッションの育成のためにうれしいことです。

2と3についても成果を、COBIT の日本化された解説本の出版などのかたちで実現を始めています。順次ご報告できるように取り組んでおりますのでご期待ください。

協会の活動に賛同される企業の方々は、ぜひ、賛助会員として ITGI JAPAN の活動をご支援ください。

ITGI JAPAN
会長 松尾 明

ISACA 東京支部では、これまで、COBIT に関する様々な調査・研究活動を続けております。COBIT の元となった“Control Objectives”の翻訳(「情報システム管理ガイド」として出版)に始まり、第2版、第3版(マネジメントガイドライン)の翻訳、公開を行ってまいりました。更に、NRI セキュアテクノロジーズ株式会社、並びに、多くの日本 IT ガバナンス協会、ISACA 会員有志により日本語化を行い、最新バージョンである COBIT 4.1 の日本語版も公開しております。

今回皆様に提供するものは、COBIT を取り巻く出版物である、IT Control Objectives for BASEL II の日本語版です。これは、金融サービス取引における、進化を続けるリスク管理のフレームワークに基づくものであり、新しい BASEL II への対応として、ISACA 国際本部の Focus Group が中心となり取りまとめたものです。ISACA 東京支部からも、当 Focus Group にメンバーを派遣し、その成果として世に送り出しています。

今回、KPMG ビジネスアシュアランス株式会社様のご協力を頂き、この出版物の日本語化が完了し、広く皆様に提供出来る事は大変嬉しい限りです。COBIT 並びに関連ドキュメントは、ISACA の活動の柱とする IT アシュアランス、情報セキュリティ、そして IT ガバナンスの分野での存在価値をますます高めています。これからも、多くの皆様に有用な情報を提供出来る様、日本 IT ガバナンス協会と協同し活動を進めて参りたいと思います。

ISACA 東京支部 2008-2009 会長
太田 均

謝辞

本著作物の作成に貢献した次の方々に深く感謝する。

主な寄稿者

Rolf von Roessing, CISA, CISM, CISSP, FBCI, KPMG Germany, Germany

Focus Group

Urs Fischer, CISA, CIA, CPA, Swiss Life, Switzerland

Christopher Fox, ACA, eDelta, USA

Jimmy Heschl, CISA, CISM, KPMG, Austria

Markus Gaulke, CISA, CISM, KPMG Germany, Germany

Marcelo Gonzalez, CISA, Banco Central Republica Argentina, Argentina

Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia

Masaki Nakamura, CIA, Sumitomo Mitsui Banking Corporation, Japan

Robert Stroud, CA Inc., USA

Robert White, CISA, ACA, ING Bank, UK

ITGI Board of Trustees

Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, PIIA, KPMG LLP, UK, International President

Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President

Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President

Howard Nicholson, CISA, City of Salisbury, Australia, Vice President

Jose Angel Pena Ibarra, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President

Robert E. Stroud, CA Inc., USA, Vice President

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP, USA, Vice President

Frank Yam, CISA, FHKCS, FHKIoD, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group,

Hong Kong, Vice President

Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President

Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, Past International President

Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee

Tony Hayes, FCPA, Queensland Government, Australia, Trustee

IT Governance Committee

Tony Hayes, FCPA, Queensland Government, Australia, Chair

Max Blecher, Virtual Alliance, South Africa

Sushil Chatterji, Edutech, Singapore

Anil Jogani, CISA, FCA, Avon Consulting Ltd., UK

John W. Lainhart IV, CISA, CISM, IBM, USA

Lucio Molina Focazzio, CISA, Colombia

Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada
Michael Schirmbrand, Ph. D., CISA, CISM, CPA, KPMG LLP, Austria
Robert E. Stroud, CA Inc., USA John Thorp, The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp, University of Antwerp Management School, and
IT Alignment and Governance Research Institute (ITAG), Belgium

Security Management Committee

Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJLPD, USA, Chair
Manuel Aceves, CISA, CISM, CISSP, Cerberian, Mexico
Kent Anderson, CISM, Network Risk Management LLC, USA
Yonosuke Harada, CISA, CISM, CAIS, ITGI-Japan, Japan
Yves Le Roux, CISM, CA Inc., France
Mark Lobel, CISA, CISM, CISSP, PricewaterhouseCoopers LLP, USA
Vernon Poole, CISM, Sapphire Technologies Ltd., UK
Jo Stewart-Rattray, CISA, CISM, Vectra Corp., Australia
Rolf von Roessing, CISA, CISM, CISSP, FBCI, KPMG Germany, Germany

ITGI 加盟企業およびスポンサー

ISACA 支部

American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
Analytix Holdings Pty. Ltd.
B Wise B.V. CA Inc.
Hewlett-Packard
IBM
ITpreneurs Nederlands B.V.
LogLogic Inc.
Phoenix Business and Systems Process Inc.

Project Rx Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions

日本語版 翻訳者

KPMG ビジネスアシュアランス株式会社
(IT Control Objectives for BASELII 翻訳プロジェクトチーム)
榎木 千昭 (リーダー)
山田 茂
関 克彦
荒川 良紀
奥村 優
橋本 純佳
亀島 大輔
高城 綾子
遠藤 真紀子
泉田 理絵
情野 里奈
瀧澤 和子

日本語版 レビュー担当者

リーダー
松原榮一 (ITGI Japan 理事、翻訳委員会委員長)
(ガートナー ジャパン)
メンバー
中村正樹 (本書の原著の著者の一人)
(株式会社三井住友銀行)
本村和也 (レビュー時: (財)金融情報システムセンター)
(現在: みずほ信託銀行株式会社)
安部靖雄 (ITGI Japan 理事)
(監査法人トーマツ)

目次

はじめに	9
1. エグゼクティブ・サマリー	10
範囲と目的	10
本書の読み方	10
2. ガバナンス、リスク管理、コンプライアンスービジネスにおける最優先事項	12
3. 規制の発展経過	14
4. バーゼルⅡにおけるリスク管理のアプローチ	16
5. オペレーショナル・リスク管理の必要性	18
リスク管理の手法	18
オペレーショナル・リスク管理のフレームワーク	19
COSO の構成要素	22
オペレーショナル・リスクの原則と IT との関係	28
6. 情報リスク管理	31
IT に関する指針	31
損失の原因と IT リスク	39
IT リスクシナリオ分析	42
7. 業務プロセスから IT リスク、IT 統制へ：COBIT フレームワークの適用	45
既存文書の利用	45
バーゼルⅡにおけるビジネスライン・アプローチ	45
IT リスクの定義	46
IT 統制の定義	50
8. 主要 IT リスク指標の使用	52
付録ⅠーバーゼルⅡの概要	54
付録ⅡーCOSO ERM とバーゼルⅡとの主な関連	63
付録ⅢーバーゼルⅡ原則1：第二の柱ー監督上の検証プロセス(2006年6月)とCOSO ERMー総合的フレームワーク(2004年9月)との主な関連	64
付録ⅣーCOSO ERM フレームワークのデータ品質への依存度	66
付録ⅤーバーゼルⅡとCOBIT	68
付録ⅥーCOBIT プロセス	74
付録ⅦーABC 銀行：実施例	82
付録Ⅷー参考文献	88

はじめに

金融機関は、バーゼル銀行監督委員会が定めた新しい自己資本比率規制、いわゆるバーゼルⅡが求める新しい課題への対応を迫られている。この規制は、金融サービス取引における、進化を続けるリスク管理のフレームワークに基づくものである。1988年に定められた第1次自己資本比率規制と異なり、情報リスクと情報技術(IT)とが、現代のビジネスを構成する重要な要素となっている。多くの金融機関は、ITインフラストラクチャ、アプリケーション、およびITに関連する内部統制において、根本的な変革を経験してきた。

本著作物の目的は、意見の一致に向けたステップを明らかにすることである。金融サービスと金融システムは、世界経済における非常に重要なインフラストラクチャであると認識されている。同様に、オペレーショナル・リスクと情報リスクの管理、ならびにITの統制は、現在では優れたコーポレート・ガバナンスに不可欠な要素であると見なされている。戦略の最上位レベルでは、経営陣による金融システムに対する監督や優れたガバナンスは、この2つを1つのモデルに統合することを必要としている。

ITGIは、高く評価されたIT Control Objectives for Sarbanes-Oxley(現在、第2版)に続き、金融機関におけるリスクにいち早く対応した、IT Control Objectives for Basel IIの第1版(本書)を発表した。本書は、オペレーショナル・リスクや情報リスクの管理者、IT実務者、およびITに職責を持つ金融専門家のためのガイダンスを提供することを意図している。主な目的は、オペレーショナル・リスクや情報リスクの管理、ならびにバーゼルⅡの要件と実施すべき対策について、明確で誤解の無いガイダンスを持つフレームワークを提供することである。

バーゼルⅡに基づいて、正式で標準化された一連のIT統制を提供することには多くの理由がある。また、金融機関に適用可能なフレームワークも数多く存在している。Control Objectives for Information and related Technology(CoBIT®)²は、ITのリスクとコントロールを管理する包括的なガバナンスのフレームワークであり、バーゼルⅡに関連するオペレーショナル・リスクおよび情報リスクの管理の制度化への要求に対応した実績を持ち、また確立された一連のITプロセスとコントロールを提供している。CoBITは、定評のあるガバナンスのフレームワークとして国際的に認知されており、幅広く、グローバルなグッドプラクティスとみなされている。CoBITは、その多用性と簡潔さ、また継続的な改訂が行われていることによって、独自に作られたソリューションや類似のフレームワークに対して、一線を画している。

本書は、様々な金融機関の上級専門家で構成された委員会において開発された。本書は、様々な仮説、見解および当然とみなされていた考え方について詳細に検討したのち、一般からの評価を受けるためのドラフトを公開するという厳密なプロセスによって、より信頼性を高めることができた。本書は、銀行家や金融専門家の観点を踏まえ、オペレーショナル・リスクと情報リスクの管理、ならびにIT統制の必要性を明らかにしている。

ITGIは、本書の継続的改善、および金融機関のニーズへの対応に資するコメントを歓迎する。コメントは info@itgi.org 宛、お送りいただければ幸いである。

Everett Johnson, CPA
Past International President
IT Governance Institute

¹ 銀行以外の組織を考慮し、本書では、銀行ではなく、金融機関という用語を可能な限り使用する。

² ITGI, CoBIT, USA, 1996-2007, www.itgi.org

1. エグゼクティブ・サマリー

範囲と目的

本書は、バーゼルⅡにおけるオペレーショナル・リスク管理、および情報リスク管理のためのフレームワークを提供している。本書は、情報リスク管理者、IT実務者ならびに金融サービス専門家という、オペレーショナル・リスクと情報リスクに関連する3つのグループを対象としている。本書で示されているフレームワークによって、金融機関は、広く認められているプロセスとコントロールをITの領域に適用することができる。本書で示すIT統制の目標と管理プロセスは、オペレーショナル・リスクに対する情報技術の役割を対象とするものである。

以下の各章で、バーゼルⅡにおけるリスクの概要、オペレーショナル・リスクとITリスクとの関連性、および情報リスク管理へのアプローチについて解説する。

本書の読み方

ガバナンス、リスク管理、コンプライアンス(GRC)は、ビジネスにおける最優先事項になっている。利害関係者からの要求の増大、より厳しい社会的な監視、業績への新たな期待が、ビジネスの新たな進化をもたらす。コーポレート・ガバナンスを強化する流れを、数々のイニシアチブにおいて見ることができる。優れたガバナンスとは、不十分な情報の流れ、不適切なコミュニケーション、行動ならびにリスクに関する不適切な理解といった、不備に対応するものである。「2. ガバナンス、リスク管理、コンプライアンスービジネスにおける最優先事項」では、GRCの考え方について解説する。

規制の強化と詳細化は、銀行や金融機関の監督当局におけるGRCの重要性を表している。この数年にわたり、GRCに関連した規制が、次々に策定されている。あらゆる種類の規制が、銀行やテクノロジーのさまざまな側面を対象とした、詳細なフレームワークへと変貌を遂げている。近年、国内外の規制は、次第に情報管理、情報技術、ならびにこの分野における専門家の規律を対象とするようになった。「3. 規制の発展経過」では、規制強化の要因について解説する。

2004年に、バーゼル銀行監督委員会は、金融機関のリスクに対する新しいアプローチである、第2次自己資本比率規制のフレームワークを発表した。バーゼルⅡの目的は、信用リスクとオペレーショナル・リスクに対して、より強力なリスク管理のための手法を導入し、リスクと所要自己資本との関連性を強めることである。この新たな規制には、金融機関がリスク管理のためのフレームワークやシステムの質を向上させれば、最低所要自己資本を削減できるというインセンティブが設けられている。これは、強力なGRCフレームワークを持つ金融機関に対して、競争上の優位性を与えるものである。各金融機関において、そのリスク・エクスポージャの総量によって、所要自己資本が決定される。GRCへの取り組みは、所要自己資本を削減する重要な要因となる。「4. バーゼルⅡにおけるリスク管理のアプローチ」では、バーゼルⅡのフレームワークで定められた、リスク管理のアプローチについて解説する。

オペレーショナル・リスクは、とりわけ重要なリスクカテゴリーとみなされている。このリスクは金融機関に内在しており、例えば金利リスクのような他のカテゴリーのリスクと異なり、多種多様である。しかし、オペレーショナル・リスクの識別と測定は、銀行や他の金融機関にとっては、明らかに非常に困難な試みである。情報技術および情報管理は、GRCを管理し、ひいては自己資本を最適化する総合的戦略の鍵である。アプリケーション、インフラストラクチャやコントロールなど、ITに関係する要素は全て、オペレーショナル・リスクの一部として定義されている。「5. オペレーショナル・リスク管理の必要性」では、オペレーショナル・リスクの概要と、情報リスクとの関連性について解説している。さらに、オペレーショナル・リスクに関するバーゼルⅡの原則と、ITリスクとの関連性について示している。

情報リスクに適切に対処するためには、ビジネス主導によるアプローチが要求される。ビジネスプロセスに基づいて、コントロールと評価指標との定義付けが進められ、ITに関連した一連のコントロールは、コンプライアンスと成熟度を評価するための一連の指標によって補完される。情報リスクがビジネスプロセスに影響を与える場合、リスクの削減と緩和のための取り組みは、組織のGRCフレームワークにおける不可欠な要素となる。「6. 情報リスク管理」では、オペレーショナル・リスクと情報リスクの管理のための10の指針を定義し、バーゼルⅡと情報リスクとを関連付けている。この指針は、バーゼルⅡで示されている、オペレーショナル・リスク管理の原則に対応している。

バーゼルⅡは、ビジネス主導のリスク管理アプローチを要求している。GRCをサポートするモデルとしてCoBITを適用するためには、IT統制はITリスクに対応していなければならない。ITリスクは、ビジネスプロセスにおけるビジネスリスクの一部である。「7. 業務プロセスからITリスク、IT統制へ：CoBITフレームワークの適用」では、ビジネスプロセスの観点に基づいて、情報リスクからIT統制に至る論理的な流れの概要をまとめている。この章では、IT実務者およびリスク管理担当者が、バーゼルⅡに関連するリスクに段階的に対応するために、CoBITとその概念を理解する方法について解説している。

リスク管理は、目標、パフォーマンスおよびリスクレベルを示す指標の利用を含んでいる。「8. 主要ITリスク指標の使用」では、主要リスク指標(KRI)の概念と、バーゼルⅡへの適用について解説している。各KRIは、オペレーショナル・リスク全体を改善するための、リスク評価とリスク管理の継続的なプロセスをサポートしている。この章では、指標の種類、リスク管理プロセス全体における重要性、および包括的なオペレーショナル・リスク管理と情報リスク管理のフレームワークに適した、KRIの定義について解説している。

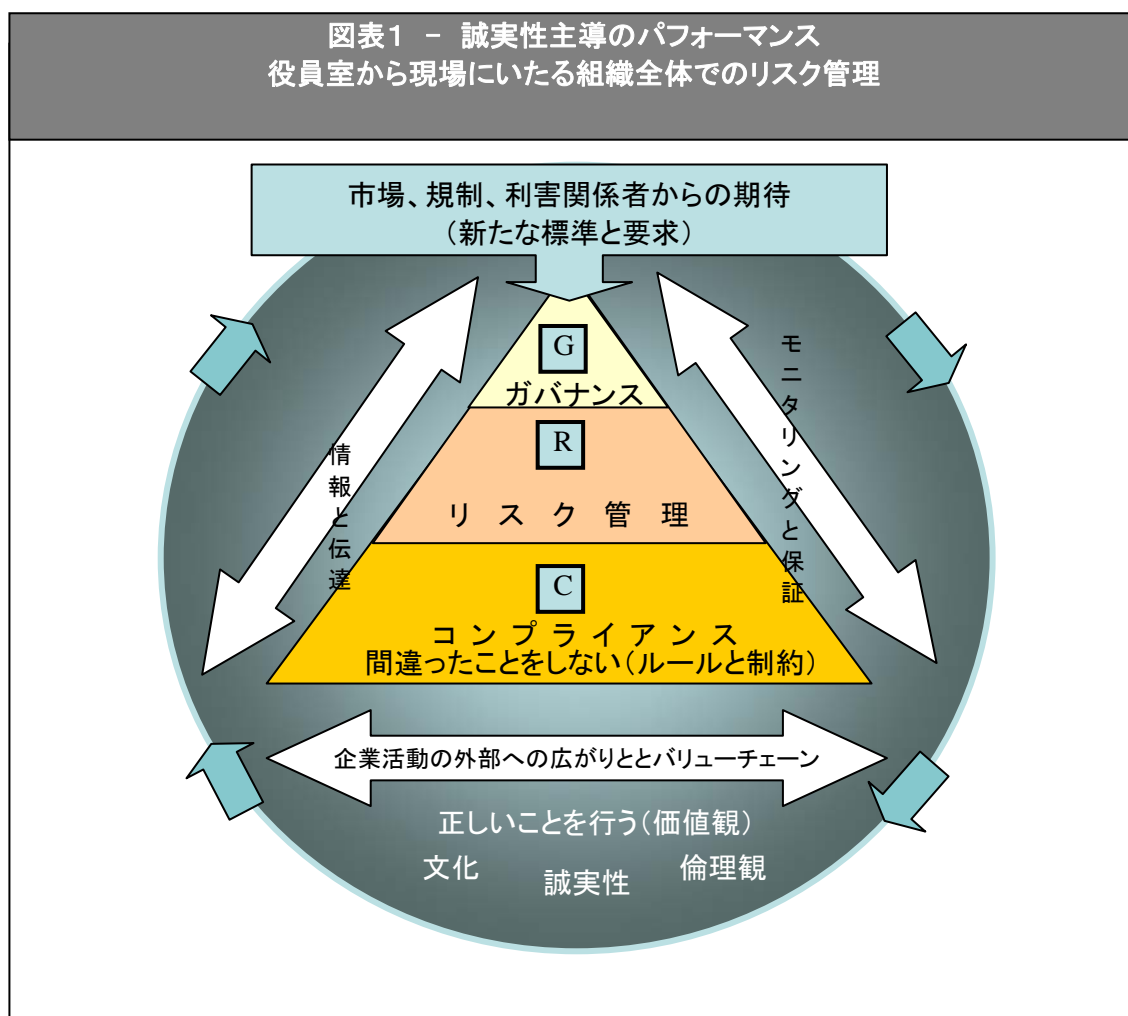
2. ガバナンス、リスク管理、コンプライアンス—ビジネスにおける最優先事項

GRCは、事業における最優先事項となった。以下に挙げるような数多くのイニシアチブにおいて、コーポレート・ガバナンスを強化しようとする傾向を見ることができる。

- 企業の評判とブランド価値の保護
- 投資家、国会議員、監督当局、顧客、従業員、アナリスト、消費者、その他の重要な利害関係者からの増大する要求と期待への対応
- ガバナンス、倫理、リスク管理、コンプライアンスによる価値の向上、ならびにパフォーマンスに対する要求の管理
- 法の施行範囲の拡大と増大する罰金、罰則、事業停止による影響からの組織、経営陣、取締役の保護、および危機と復旧の管理
- 企業の社会的な責任、ならびに受託者責任の透明かつ積極的な遂行

組織は、このようなイニシアチブによる影響に対応しなければならない。GRCに関して、成功を収めてきた組織といえども、急速に変化する環境に対して、今後も適応し続けることができる保証はない。企業に対する調査の結果では、多くの企業が、利害関係者からの要求の増大に、効果的に対応していくことは難しいと考えていることが示されている。

図表1は、組織の全ての階層を対象とする、コーポレート・ガバナンスに関する責任の全体像を示している。GRCに関する主な責任は取締役会にあるが、全ての組織単位は、経営陣が設定したGRC原則を導入し適用しなければならない。



GRCについては、その実現に向けた、統合的アプローチを採用すべきである。GRCの分野ごとに異なるアプローチを採用した組織は、大幅なコストの増加や作業の重複につながる可能性が高い。また、事後的で消極的なGRCアプローチは、効率性に悪影響を与える可能性があり、能動的でプロセス主導型のイニシアチブの実行を不可能とはいえないが、困難にする。

優れたガバナンスとは、戦略を設定し、リスクを管理し、価値を提供し、パフォーマンスの測定を行うものである。経営陣と従業員は、強固なGRCフレームワークにより、利害関係者の利益という考え方を組織全体に行き渡らせることができる。このようなフレームワークは、誠実な経営、企業資産と知的財産の最大限の活用、およびリスクの理解と管理を行うための基礎である。また、GRCのフレームワークのあらゆる部分が、優れたコーポレート・ガバナンスの重要な構成要素となる。

組織は、地政学上の不安定性、グローバル化、積極的な成長目標、競争の激化、情報の氾濫によるリスクの増大に対応しなければならない。リスク管理は、常に、金融機関のコア・コンピテンシーであり続けてきた。今日では、全社規模で統合的なリスク管理を行うことは、法的な責務となっている。企業家活動とリスクは、排他的なものではない。統合的リスク管理は、十分な情報に基づいた経営判断や、耐えられる受容可能な水準のリスクを、意識的に受け入れることを可能にする手段のひとつである。従って、企業ガバナンスの一部としてのリスク管理は、利害関係者からの信頼を強化し、企業家活動に携わる組織に確かな方向性を与えるであろう。

コンプライアンスは、チェックリストを用いた受身型のアプローチからスタートして、優れたガバナンスを支援するための、将来を考える積極的な規律へと進展した。ルールに基づいたコンプライアンスは、現在でも重要な要素ではあるが、コンプライアンスは、今や要件リストによって単純に機能するものではなくなっている。多くの場合、規制や基準で定められたコンプライアンス要件は、成熟度に基づいて、継続的な改善を目的とするものとなっている。従って、市場慣行、ベンチマーク、また新たなビジネスの発展は、グローバルビジネスの絶え間ない変化や課題を前提として、コンプライアンスの概念に盛り込まれなくてはならない。

GRCは、事業の参入や運営を開始した後で、検討を始めるものではない。GRCは、組織を守り、組織の誠実性を保持することの必要性を、社外の利害関係者やビジネスパートナー、ならびに社内の従業員やアソシエートに対して表明するものである。GRCに注力する国会議員は、国内外の有権者や支持者の利害を代弁しているといえる。様々な法令に、優れたガバナンスの必要性に関する、社会的な合意が反映されている。GRCに関する規制は、このような合意を、産業別、業種別の状況に合わせてコンセプトに置き換えるものである。業界団体や標準化団体が、GRCに関連するコンセプトの計画、導入、維持に合意している。

バーゼルⅡとそのリスク管理に関する条項は、金融業界におけるガバナンスの構造、およびフレームワークの構築に対する関心の高さを反映している。新しい自己資本比率規制は、初期のイニシアチブとそのGRC要件を超える範囲に広がっている。バーゼルⅡの各構成要素と構成単位は、情報技術、セキュリティ、事業継続への諸課題を含む、経営および技術上の側面を幅広くカバーしており、銀行や金融機関における専門家の規律に方向性を与えている。

情報そのもの、情報関連技術、および情報管理に関する様々な課題の重要性は、ますます高くなっている。また、今日の銀行や金融サービスは、取引と統制の両面において、複雑な情報技術に一層依存するようになっている。基幹業務プロセスと、そのサポートに不可欠な技術とをつなげることは、GRCの重要な責務の一部である。その結果として生み出される、情報管理に関する優れたガバナンスのフレームワークは、統制とコンプライアンスのみに限定されるものではない。GRCの優先順位は、情報技術とその可能性に関して、事業をグローバルにサポートする全ての取り組みに反映されなくてはならない。バーゼルⅡの観点では、業務上の損失と風評被害に加え、ITガバナンスモデルの整備状況あるいは運用の有効性における不備は、オペレーショナル・リスクに対する所要自己資本増加の一因となり得る。これについては、「5. オペレーショナル・リスク管理の必要性」で詳しく論じている。

3. 規制の発展経過

法、規制、基準および一般的に受入れられている業界の慣行は、全て、GRC の目標をサポートするという共通の目的に貢献するものである。実務者が期待する、実務への適用可能性や必要条件の詳細性において、国内および国際規制、特に銀行や金融サービスのような特定の業種を対象とする規制条項が、GRC の基礎を構成している。

規制活動の強化は、規制における要求の詳細化と合わせて、GRC が、銀行や金融サービスの監督当局が重要な関心を寄せる分野であることを証明している。この数年の間に、以下のような GRC 関連の規制が、次々に策定されている。

- バーゼル II
- 財務報告に関わる諸法令 (例: 2002 年米国サーベンス・オクスリー法)
- プルデンシャル規制

あらゆる種類の規制が、金融サービスや金融工学の様々な領域を対象とする詳細なフレームワークへと変貌を遂げている。近年、国内外の規制は、次第に、このような分野における情報管理、情報技術、および専門的な領域を対象とするようになってきている。この結果、経営陣と専門的な実務者は、組織における GRC を支援するために、現行の規制を、実務的で管理しやすいコンセプトに転換する立場にある。

規制変更の要因には、以下のようなものがある。

- 金融工学の進歩と高度化による、金融機関の活動とリスク・プロファイルの複雑化
- 銀行のグローバル化と金融業務の国境を越えた広がり
- 市場の監視、監督の必要性に基づく、地理的な管轄を越えた監督当局の連携の拡大
- マネー・ロンダリング防止の法規制のように、金融業界の他分野にも影響を与えるコンプライアンス要件の拡大
- 強化されたガバナンス、企業倫理、独立性、透明性、および市場への厳格な情報開示の重要性を強調する、企業の説明責任への一層の期待
- 役員受託者責任の遂行、責任範囲の大幅な拡大、および取締役会と委員会の潜在的責任に関する注意義務基準への一層の期待
- ガバナンスやリスク管理に対する社会的関心の高まりと、規制に関する協議へのより強い影響力を伴う民間利益団体、株主、メディアからの圧力の増大
- 様々なアプリケーションやデータベースから作成される内部および外部向けの報告
- 自国や相手国の監督当局に対応したコンプライアンス標準の多様化
- 効率的で効果的なサービスを提供するための IT インフラへの高度な依存と、法的管轄権をまたぐ資金決済の発展にともなう第三者への依存の高まり

規制は、国際的なビジネス環境が複雑化するにつれて、現在は対象となっていない領域にも規制が及び、将来はもっと詳細な規制が導入される。規制対象の変化は、過剰規制と見なされる可能性もある。しかし、監督当局には、株主、透明性、誠実な経営の保護を含め、金融機関に対する市場の信頼、金融機関の安全性および健全な実務 (サウンドプラクティス) を維持することが期待されている。

原則ベースの規制に向う傾向はあるが、規制や基準の中味は、引き続き、ルールベースのままであろう。バーゼル II の導入により、規制には、プロセスベースの条項と、結果ベースの条項が盛り込まれている。ルールベースの規制、および新たに導入されつつある原則ベースの規制において、コンプライアンスに関する責任は金融機関にある。金融機関の取締役会と経営陣は、GRC のプロセスが安定していて、拡張された規制にも準拠していることについて、監督当局を満足させなければならない。

結果的に、金融機関は、拡大する規制範囲、また今後適用される詳細な要求事項に適応していかなければ

ならない。これまでは規制されていなかった情報管理や情報技術などの分野、ならびにセキュリティ、業務継続およびプライバシーなどの関連分野を含め、積極的にGRCに取り組むための強固なビジネスプロセスを導入する必要がある。

4. バーゼルⅡにおけるリスク管理のアプローチ

ビジネスに附随するリスクは、過去数年にわたって発生した一連の事件により、より大きな社会的関心を集めるようになった。不正事件、巨額の信用破綻、情報技術の不正利用などを含む、数多くの事件がこれに含まれる。メディアの反応や社会的な関心の高さは、国際金融システムの信用を維持するうえでの、リスク管理の重要性を裏付けるものである。

銀行および金融業界においては、一般的に、管理可能な GRC の構造を構築するためにリスクを分類する必要がある。通常、リスクカテゴリーは、典型的な銀行または金融機関における主要な業務に対応している。このリスクカテゴリーには、以下のようなものがある。

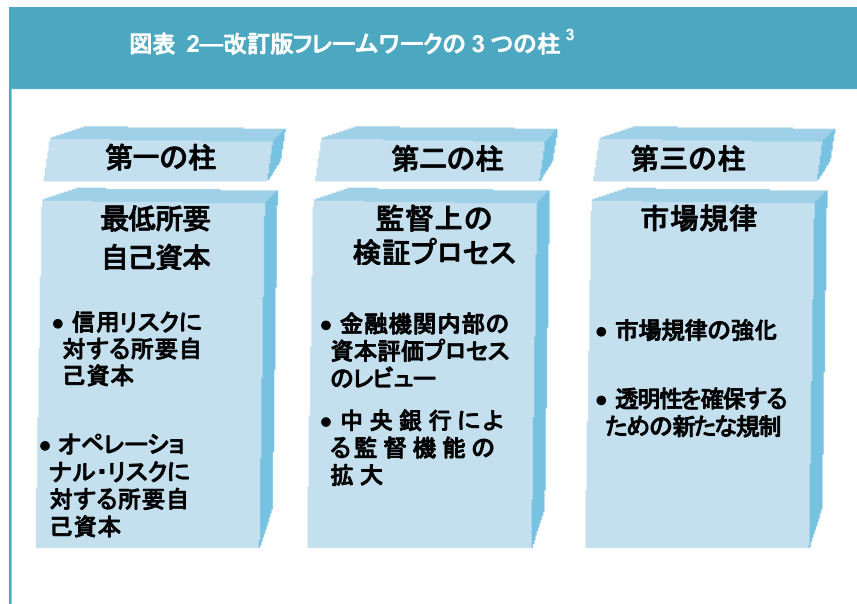
- 信用リスク
- 市場リスク
- オペレーショナル・リスク
- 流動性リスク
- 金利リスク
- 法務リスク
- 戦略リスク
- 風評リスク

バーゼル銀行監督委員会は、2004年に、金融機関のリスクに対する高度なアプローチを導入するための、新しい自己資本比率規制を公表した。バーゼルⅡの目的は、信用リスクおよびオペレーショナル・リスクに対して、より強固なリスク管理手法を導入すること、およびリスクと所要自己資本との関連性を強化することである。新しい規制には、金融機関がリスク管理のためのフレームワークやシステムの質を向上させれば、所要自己資本を削減できるというインセンティブが設けられている。これにより、強固な GRC フレームワークを構築した金融機関は競争上の優位性を得ることができる。各金融機関の自己資本賦課は、全体的なリスク・エクスポージャーによって決定されることになる。GRC に関するイニシアチブは、自己資本賦課を削減する手段となりうる。リスクと所要自己資本に関する新たな考え方が出てきたことによって、多くの金融機関では、その組織構造やプロセスを見直し、再評価しなければならないであろう。

バーゼルⅡのリスクアプローチは、情報技術と情報管理の複雑性を網羅するように考案されている。図表2は、3つの柱から構成される、高度化されたフレームワークを示している。

- **最低所要自己資本** –バーゼルⅠの信用リスクに対するアプローチの改善、およびオペレーショナル・リスクにかかわる新たな所要自己資本の導入
- **監督上の検証プロセス** –資本の管理とコントロールのための健全な方針と手続を含む、銀行の自己資本最適化プロセスに対する、監督上の検証と自己評価の導入
- **市場規律** –市場規律を強化し、市場、格付機関、および株主の認識に影響を与える新たな開示義務の導入

図表 2—改訂版フレームワークの3つの柱³



第一の柱における最低所要自己資本は、第二の柱を確実に実施することにより達成することが重要である。これに加えて、第三の柱における情報開示は、市場規律が他の2つの柱を効果的に補完するうえで、必要不可欠なものである。

金融機関は、リスクおよび所要自己資本を評価・管理するにあたって、さまざまな手法の中から自社の GRC の成熟度レベルに合ったものを選択することができる。より先進的なリスク管理手法を選択した金融機関は、自己資本賦課を低く抑えられる可能性がある。対象とするリスクカテゴリーによって手法は異なる。また、より先進的な手法へと徐々に移行することが期待されている。金融機関は、費用便益の検討や経営陣の戦略的意思決定の結果、全体的なリスクをあえて高めに想定し、その分、資本を増やすという選択もできる。ただし、信用リスクにおいて内部格付手法を導入する場合は、その前に、オペレーショナル・リスクに関する先進的手法を導入しなければならない。(訳注;なお、日本の金融庁告示では、このルールは存在しない。)

第二の柱である監督上の検証は、金融機関の GRC に関して、質的な保証を与えるものである。各国の金融サービス監督当局は、最低所要自己資本の達成状況を監視し、問題がある場合には、必要な措置を取らなければならない。「付録 I バーゼル II の概要」に、監督上の検証における4つの基本原則について、詳細に記述している。監督プロセスの原則と範囲において、金融機関と監督当局との間に、継続的な対話があることが想定される。

第三の柱である市場規律では、リスクと GRC に関する情報の開示が導入されている。これは、すべての市場参加者に対して、各金融機関の全体的なリスク、および重要な潜在的リスクを開示することを意図している。その結果として、市場規律が強化され、偏在していたリスクが市場全体の動きに反映される。

情報開示規制は、信用リスク、市場リスク、オペレーショナル・リスク、金利リスクの各リスクにおける潜在的損失、および実際の損失を算出し、公開するよう定めている。この要求により、他の市場参加者は、各金融機関のリスク・プロファイルを詳細に評価することが可能となる。リスク別の詳細な損失額算出の手法は、「付録 I バーゼル II の概要」に記載している。

³ この図表では、バーゼル II フレームワークの構成要素の詳細のうち、変更されたもののみを示している。各柱の詳細については、付録 I 「バーゼル II の概要」を参照のこと。

5. オペレーショナル・リスク管理の必要性

オペレーショナル・リスクは、最低所要自己資本を決定するための重要な要素である。オペレーショナル・リスクは、金融機関の業務全体、特に、基礎となるテクノロジーやインフラストラクチャにおける、損失の可能性に関連する全ての領域に及んでいる。情報技術の重要性は、オペレーショナル・リスクに対する自己資本賦課と、直接的な相互関係を持っていることが多い。そのため、オペレーショナル・リスクのカテゴリーは、信用、市場、金利リスクよりも、広い範囲にわたっている。オペレーショナル・リスクの複雑性と範囲を考えると、GRCのフレームワークとそのイニシアチブは、他のリスクとは直接関連しない、組織の全ての範囲を対象とする必要がある。

リスク管理の手法

オペレーショナル・リスクは、以下の3つの手法のいずれかを用いて管理される。

- 基礎的手法(BIA)
- 標準的手法(STA)
- 先進的計測手法(AMA) ※金融機関の内部損失データを用いる手法

この3つの手法からの選択に加え、金融機関は、主要なビジネスやITに関連する、最低基準を遵守しなければならない。巻末の「付録I バーゼルIIの概要」では、この基準の詳細と、上記の3つの手法について解説している。

バーゼルIIで初めて、自己資本充実度の計算に、初めてオペレーショナル・リスクが組み込まれた。この理由は、多くの金融機関で巨額の損失が発生したこと、またこの損失は、より効果的な統制と高度なビジネスプロセスがあれば避けられた可能性があることにある。

さらに、金融機関におけるITやインターネット利用の拡大、金融商品の一層の複雑化とデリバリーチャネルの多様化によって、オペレーショナル・リスクの識別と評価がますます必要となっている。

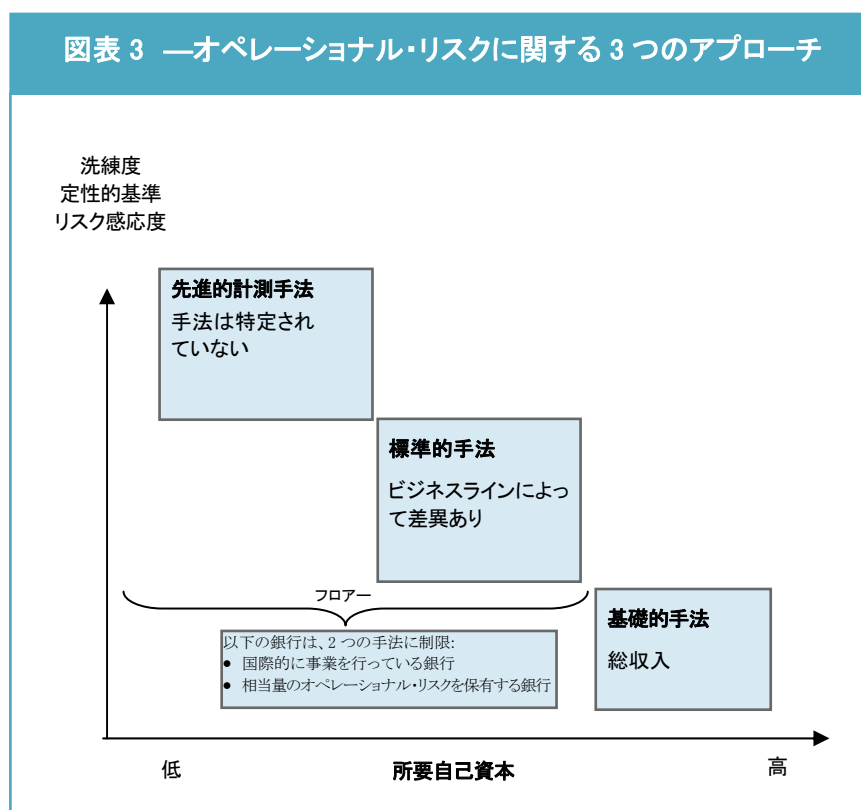
バーゼル委員会は、バーゼルIIにおいて、オペレーショナル・リスクを次のように定義している。

「オペレーショナル・リスクは、不適切な、または失敗した内部プロセス、人、システム、あるいは外部事象によって発生する損失のリスクと定義される。」

この定義には、法務リスクは含まれるが、戦略リスクと風評リスクは含まれない。現段階では、オペレーショナル・リスクは、バーゼルIIで定義された8%の最低所要自己資本に含まれている。オペレーショナル・リスクを評価するために、銀行は様々な代替的アプローチを採用することができる。

バーゼル委員会は、**図表3**に示したとおり、オペレーショナル・リスクの定量化手法として、洗練度とリスク感応度が低い方から順に、基礎的手法、標準的手法、先進的計測手法という3つの手法を提供している。

図表3 —オペレーショナル・リスクに関する3つのアプローチ



信用エクスポージャーに関する自己資本規制の考え方と同じく、この3つの手法は、順を追って複雑になっており、複雑なものほど、リスク感応度が高い。上位の手法を採用すれば、銀行は所要自己資本を低く抑えることができるが、その分、より高度な条件を満たさなければならない。

金融機関は、定性的、定量的条件は次第に厳しくなるが、オペレーショナル・リスクの計測システムや実務をさらに洗練させつつ、上位の手法に段階的に移行していくことを、奨励されている。このインセンティブとして、より高度な手法を用いることによって、自己資本の自由度を高めることが認められている。

金融機関は、特定のビジネスラインに限定して上位の手法を適用することもできる。ただし、この場合も、金融機関は、一定の条件を満たさなければならない。

全ての金融機関は、バーゼル委員会のガイダンスノートに定義された最低基準に適合しなければならない。「オペレーショナル・リスクに関する健全な実務(サウンドプラクティス)」が示す基準には、以下の事項が含まれる。

- 取締役会と経営陣は、オペレーショナル・リスク管理の監督に関して、積極的な役割を果たさなければならない。
- 銀行は、機能し、完全に導入され、統合されたリスク管理システムを持たなければならない。
- 採用する手法にあわせ、その実施に十分な要員を確保しなければならない。

オペレーショナル・リスク管理のフレームワーク

オペレーショナル・リスクは、特に重要なリスクカテゴリーと見なされている。このリスクは、金融機関の業務に内在しており、また、通常の業務運営は、金利リスクなどの比較的狭い範囲を対象とするリスクカテゴリーと比べると、多種多様である。このため、オペレーショナル・リスクを識別し計測することは、銀行や金融機関にとって非常に困難であることが明らかになっている。

監督当局や他の関係機関が指摘するように、オペレーショナル・リスクの定義においては、個別業務を、全社的リスク管理のフレームワークに統合する前に考慮すべき、さまざまな個別のリスク要因がある。オペレーショナル・リスクに分類される個別リスクの多くは、コンプライアンスやコーポレート・ガバナンスの問題に関連して

いる。その他のリスクは、主要な業務を支えるテクノロジーやインフラストラクチャに関する、深い理解を必要とする。

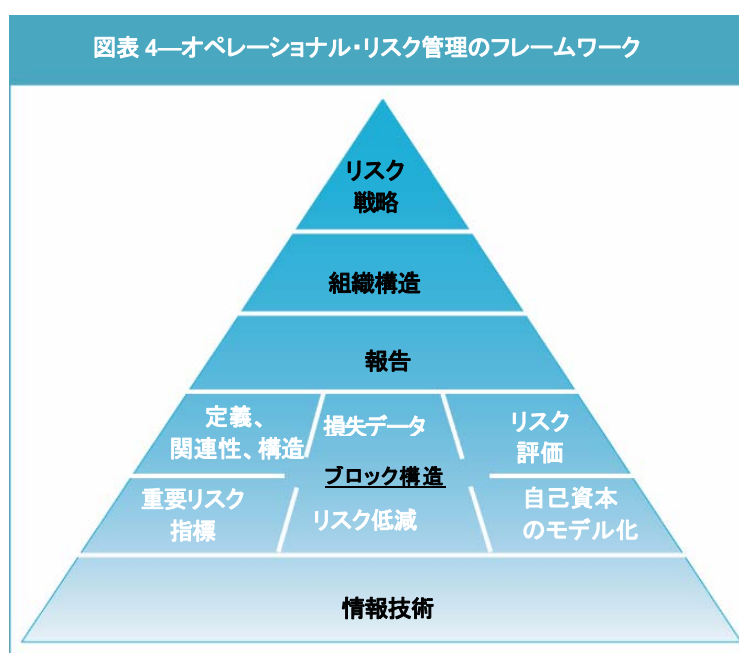
バーゼル委員会は、銀行に対して、オペレーショナル・リスク管理のフレームワークを導入することを求めている。このフレームワークの領域や範囲は明示されていないが、**図表 4** では、オペレーショナル・リスクを管理する方法の例を示している。

リスク戦略

オペレーショナル・リスク戦略は、マネジメントフレームワークにおける、その他の構成要素の実施を促すものである。包括的リスク戦略では、リスク選好や許容度、日常のリスク管理にかかわる方針およびプロセスについて、明確な指針を提供すべきである。

組織構造

組織構造は、全てのオペレーショナル・リスク管理活動を支える、組織全体の基礎である。この観点から、金融機関は、広範な部門、機能および個人に対して、集中または分散された役割と責任を定義し割り当てる必要がある。



報告

オペレーショナル・リスクは、全ての部門に関係するものであり、オペレーショナル・リスク管理に関する報告は、従来からの市場リスクや信用リスクに関する報告に比べ、広い範囲を対象とする。この報告は、次の2つの特徴的な事項に対応しなければならない。

- 経営陣とリスク管理部門に対する、定義済の担当業務に関連するオペレーショナル・リスク情報の提供
- 事業担当の経営陣、取締役会、リスク委員会に対する、リスクカテゴリー別にまとめられた情報の報告

定義、関連性、構造

金融機関には、オペレーショナル・リスクと損失事象の種類、ならびに原因と結果を表現するための共通語が必要である。また、規制上の要求事項を充たすため、必要なルールを関連付けることも必要である。定義や関連性を明確にし、構造化することによって、金融機関は、オペレーショナル・リスクに関連した情報を効果的に識別し、評価、報告することができる。

損失データ

オペレーショナル・リスクのフレームワークを適切に構成するためには、オペレーショナル・リスクによるさまざまな種類の損失事象を把握するためのデータベースが必要である。監督当局は、内部損失データベースに対して、包括的であること、およびリスク評価プロセスでの使用が正式に承認される前の数年分を含むデータを蓄積することを求めている。バーゼルⅡでは、先進的計測手法の採用にあたっては、初期導入時に最低3年分、最終的には5年分のデータを、内部損失データとして蓄積することを求めている。外部データを含む過去データに対するニーズは、多くの金融機関が、データベースを可能な限り迅速に本番稼働させようとする取り組みを推進する背景となっていた。

金融機関は、共通語の設定とあわせて、オペレーショナル・リスクの損失データを収集、評価、モニタリング、報告するためのプロセスを必要とする。このプロセスは、臨時の報告から定例のリスク報告まで、あらゆる経営上の意思決定の基礎を提供するように設計され、リスク評価とともに定量化モデルを支えるものとなるであろう。

リスク評価

リスク評価は、体系化されたシナリオ分析を、あらゆる部門において実施することによって、主要な潜在的リスクを認識する、定性的な手法である。リスク評価の手法によって、過去の損失データの不足に起因する知識の不足を補うことができる。この手法は、リスクを敏感にとらえる方法により、オペレーショナル・リスクを能動的に識別しようとするものである。

重要リスク指標(KRI)

金融機関は、測定とモニタリング活動の一部として、システム、プロセス、商品、要員、その他の環境に関する早期警報を提供するKRIに基づいて、オペレーショナル・リスクを評価すべきである。KRIは、将来の行動の予測でなく、実際のデータを使用する点において、リスク評価とは異なるものである。

リスク低減

金融機関は、リスクの特定と定量化を行うことによって、適切な方針、手続、システムおよびコントロールによる、リスク低減を目的とする戦略を導入することができる。

自己資本のモデル化

自己資本のモデル化は、規制および経済上の自己資本の計算を含むものである。これには、内部および外部損失データ、シナリオデータ、ビジネス環境、統制要因、保証パラメータなどの補助的な情報を含む入力データの定義、オペレーショナル・リスクを計測するための数学的または統計的な相関関係や仮説の設定、モデルの導入、およびモデルの妥当性の評価などが必要となる。

情報技術

適切な情報技術(IT)は、オペレーショナル・リスク管理のフレームワークの基礎であり、またこれを推進するものである。ITシステムは、広範なオペレーショナル・リスク情報に対応するとともに、さまざまな内部システムおよび外部情報と連携しなければならない。

バーゼル委員会は、「オペレーショナル・リスクの管理と監督に関する健全な実務(サウンドプラクティス)⁴」において、情報技術の高度化の進展は、金融機関の業務をより複雑にする要因であると明言している。ITは、戦略的情報システムや経営管理情報システムの運用において、重要な役割を果たしている。今日、このようなシステムは、経営陣、金融機関の監督当局、市場参加者、そして、その他の重要な利害関係者からの要求を満たすための企業活動から、切り離すことのできないものである。財務および業務管理システムにおける情報技術の利用の拡大に伴って、特に重要性の高い情報システムにおいて、統制は従来から必須のものとして認識されてきた。

バーゼル委員会は、「銀行組織における内部統制(内部管理体制)のフレームワーク⁵」において、トレッドウェイ組織委員会(COSO)による全社的リスク管理(ERM)のフレームワークで示されたガイダンスに従って構築された、内部統制システムに関する定義と基本要素を採用した。バーゼルⅡでは、このレポートを、最低基準を満たすための必須要件と見なしている。また、存在するリスクに対する監督プロセスの感度を高めるとともに、より優れたリスク管理を目指すインセンティブを、銀行に与えることを意図している。コーポレート・ガバナンス、取締役会や経営陣による直接的説明責任、全般統制、およびリスク管理プロセスの改善は、健全な自己資本管理を行

⁴“Sound Practices for the Management and Supervision of Operational Risk” 2003年2月 バーゼル銀行監督委員会

⁵“Framework for Internal Control Systems in Banking Organisations” 1998年9月 バーゼル銀行監督委員会

うための鍵となる要素と見なされている。

COSO は、ビジネス倫理、有効な内部統制およびコーポレート・ガバナンスにより財務報告の品質向上に取り組む、ボランテアの民間組織である。COSO は、トレッドウェイ委員会として知られる、独立の民間組織である不正な財務報告全米委員会をサポートするために、1985 年に組織された。組織委員会には、米国公認会計士協会 (AICPA)、アメリカ会計学会 (AAA)、財務役員国際組織 (FEI)、内部監査人協会 (IIA) および管理会計士協会 (IMA) が参加している。

COSO のモデルは、情報管理や情報技術について明確には言及していない。しかし、IT は、財務諸表リスク、規制リスク、あるいはオペレーショナル・リスクなどのリスクの種類にかかわらず、内部統制制度のあらゆる範囲に存在するものである。その結果、組織のリスク管理における重要な構成要素となっている。CobiT のフレームワークは、IT リスクを管理するための、明確で広く認められた、一連の IT 統制のプロセス、目的、活動を提供している。また COSO のフレームワークとコンセプトにも適合している。CobiT は、上位レベルの全社的なリスクの管理と個別の IT リスクに関する問題とのギャップをつなぐものである。次のセクション以降では、IT への影響を含め、COSO についてさらに詳しく検討する。

COSO の構成要素

IT 統制が、どのように COSO ERM のフレームワークに対応しているかを示すことは重要である。組織は、COSO の全ての構成要素に関連する IT 統制に対応できる、適切な能力を備えておくべきである。COSO では、以下の8つが、効果的な内部統制のための重要な構成要素として示されている。

- 内部環境
- 目的の設定
- 事象の識別
- リスクの評価
- リスクへの対応
- 統制活動
- 情報と伝達
- モニタリング

次のセクションでは、上記の各構成要素について概説する。また、各構成要素について、IT に関連する検討事項を概説する。以下のセクションでは、斜字体の部分は、COSO ERM のフレームワークからの引用であることを示す。

内部環境

内部環境は、リスク管理の理念を含む、リスクに対する考え方の基準を決定する。また、有効な内部統制の基礎を形成し、「経営者の姿勢」を確立し、コーポレート・ガバナンス構造の頂点に位置するものとなる。内部環境の構成要素において提示される問題は、組織全体に当てはまる。

しかし、IT には、ビジネスとの連携、役割と責任、方針と手続、および技術力をより強く求められるという特徴が頻繁に見られる。統制環境と IT に関する留意点として、次のようなものがある。

- IT は、独立したビジネス組織、つまり、別の統制環境であるという誤った見方をされる場合が多い。
- IT は技術的要素として複雑だけでなく、組織全体の内部統制システムに組み込まれる方法も複雑である。
- IT の導入によって、統制活動の追加や改善を必要とする、新しいリスクの発生や、既存のリスクの増大につながる可能性がある。
- IT は、十分に確保することが難しい専門スキルを必要とする。

- 重要なプロセスもしくはIT機能の一部がアウトソースされている場合には、ITの委託先への依存が高まる可能性がある。
- IT統制の主管が不明確になる可能性がある。

内部環境は、バーゼルⅡの原則1、3、6、10に関連している。

目的の設定

COSO ERMでは、4つの大きな目的が示されている。

業務目標

組織業務の有効性と効率性に関連する。また、パフォーマンスと利益に関する目標、損失に対するリソースの保護を含んでいる。業務目標は様々であり、構造とパフォーマンスに関する経営陣の選択に基づいて決定される。

金融機関は、主要な商品、業務、プロセス、およびシステムに影響する全てのITプロセスに存在するオペレーショナル・リスクを識別すべきである。例えば、ある重要なプロセスが365日24時間のサービスタイムと90%の可用性を前提としている場合、この目標達成に関連するITリスクについて評価することが必要となるであろう。

報告目標

報告の信頼性に関連する。組織の内部および外部への報告を含み、財務情報と非財務情報の両方に関連する可能性がある。

バーゼルⅡの報告目標、また関連するプロセスは、サーベインス・オクスレー法の報告目標よりも、広い範囲を対象としている。財務報告に加え、リスク管理に関する報告、情報開示のための報告についても考慮する必要がある。

コンプライアンス目標

関係法令の遵守に関連する。外部要因によって決定され、全ての組織、また場合によっては、業種を超えて、類似したものとなる場合が多い。

IT組織は、コンプライアンスが必要な法的要件を認識すべきである。この要件には、コンティンジェンシープランの策定といった公式なもの、あるいは明確には定義されていない、金融機関の安全で健全な環境づくりに対する検査官の期待などが含まれている。

戦略目標

組織の達成目標を定義するために、経営陣が設定する上位目標に関連する。また、コンプライアンスに関するイニシアチブおよびリスク管理と直接結びつくべき、組織の業務手順および報告手続にも関連している。

部門における目標と報告の手続は、オペレーショナル・リスクに対する経営陣の期待に関連付けられる必要がある。ITは、基本的な金融業務の実施と管理の中核となる要素である。ITの目標は、組織の戦略目標と整合性を取る必要がある。

目的の設定は、バーゼルⅡの原則4に関連している。

事象の識別

COSO ERMの説明：

経営陣は、発生した場合には、組織に影響を及ぼす潜在的な事象を識別し、その事象が、戦略の実施および目標の達成に関する組織の能力を損なう可能性があるかどうかを判断する。組織に負の影響を与える事象はリスクであり、経営陣による評価と対応が必要となる。

COSO ERMで識別されている技術的事象のカテゴリーは、**図表5**のとおりである。

図表 5 — COSO ERM における事象カテゴリー	
外部要因	内部要因
妨害	データインテグリティ
E-Commerce	データとシステムの可用性
外部データ	システム選定
新しい技術	開発
	展開
	維持管理

COBIT のプロセスと関連付けられた事象の例は、「付録 V バーゼル II と COBIT」に記載されている。

事象の識別は、バーゼル II の原則 4 と 5 に関連する。

リスク評価

COSO ERM の説明：

リスク評価を行うことによって、組織は、どのような潜在的な事象が、どの程度、組織の目標達成に影響する可能性があるかを検討することができる。経営陣は、発生可能性と影響度という2つの視点によって事象を評価する。また、通常は、定性的手法と定量的手法とを組み合わせて評価を行う。

リスク評価は、経営陣によってあらかじめ設定された目標に関連する、リスクの識別と評価を含み、統制活動を決定する基礎となる。内部統制リスクは、組織の他の部門に比べ、IT 関連の組織において、より広い範囲に及ぶ可能性がある。リスク評価は、組織全体を対象とする全社レベル、あるいは、個別のプロセスや事業単位を対象とする活動レベルで行われる場合がある。

全社レベルのリスク評価として、以下のような対応が期待されると考えられる。

- IT 委員会の責任には、以下のような事項が含まれている。
 - IT に関する内部統制戦略計画の策定、効果的で適時の実施と導入、ならびにリスク管理計画全体への統合の監督
 - IT 管理、データセキュリティ、プログラムの変更と開発などを含む、IT リスクの評価

業務レベルでは、以下のような事項が期待されるであろう。

- システム開発手法全体に組み込まれた正式なリスク評価
- インフラストラクチャの運用と変更プロセスに組み込まれたリスク評価
- プログラム変更プロセスに組み込まれたリスク評価

リスク評価は、バーゼル II の原則 4 および 5 と関連している。

リスクへの対応

COSO ERM の説明：

リスクへの対応には、リスクの回避、低減、共有、受容が含まれる。経営陣は、リスクへの対応を考慮するにあたって、リスクの発生可能性と影響度、ならびに費用と便益に対する影響を

評価し、残余リスクを、受容可能な水準まで低減できる対策を選択する。経営陣は、起こり得るあらゆる可能性を考慮し、組織全体のリスクあるいはリスクポートフォリオの視点から、残余リスク全体が、組織のリスク選好の範囲内に収まるかどうかを判断する。

リスクへの対応は、以下のカテゴリーに区分することができる。

- 回避 リスクの原因となる活動から撤退すること。複数の「適材適所」のアーキテクチャの組み合わせから、標準的なITインフラストラクチャに移行することも、リスクの回避となる場合がある。
- 低減 リスクの発生可能性または影響度、もしくはその両方を低減する措置。典型的には、プログラム変更機能の集中化など、日常業務における様々な意思決定に関連するものである。
- 共有 移転あるいは一部を他者と共有することによって、リスクの発生可能性または影響度を低減すること。一般的な手法として、保険への加入、ヘッジ取引の実施、業務のアウトソーシングなどがある。
- 受容 リスクの発生可能性または影響度に関する措置を何も取らないこと。例えば、セキュリティポリシーでは8文字のパスワードが要求されているが、アプリケーションでは6文字しか設定できない状況で、そのリスクを受け入れると判断する場合がある。

リスクへの対応は、バーゼルⅡの原則 6 および 7 に関連している。

統制活動

統制活動は、ビジネス目標、およびリスクを低減する戦略の達成を目的として実施される方針、手続、および実務である。統制活動は、識別されたリスクを低減するために、統制目標ごとに設定される。

信頼できる情報システムと有効な IT 統制活動なくして、組織が、正確な財務報告を作成することは困難と考えられる。COSO は、この認識に基づいて、情報システムに関する統制活動として、全般統制と業務処理統制という、2つの幅広い分類を示している。

全般統制は、組織のアプリケーションシステムから生成される、財務情報の信頼性を確保することを目的として設計されており、以下のような種類の統制が含まれている。

- データセンターの運用に関する統制—ジョブの作成とスケジューリング、オペレータの作業、データのバックアップとリカバリー手順などに関する統制。
- システムソフトウェアに関する統制—システムソフトウェア、データベース管理システム、通信ソフトウェア、セキュリティソフトウェアおよびユーティリティの効果的な調達、導入、保守に関する統制。
- アクセスセキュリティに関する統制—システムの不適切な使用や、無権限者による使用を防止するための統制。
- アプリケーションシステムの開発と維持管理に関する統制—システムの設計と導入を含む、開発標準に関する統制。開発または維持管理プロジェクトをコントロールするための、開発フェーズの区分、文書化に関する要件、変更管理、承認とチェックポイントの要点が示される。

業務処理統制は、不正なトランザクションが実行されることを防止、または検知するために、プログラムに組み込まれる統制である。業務処理統制は、必要に応じて他の統制と組み合わせることによって、トランザクション処理の網羅性、正確性、承認と妥当性を裏付けるものである。業務処理統制には、以下のようなものが含まれる。

- バランス統制—手作業または自動で集計した数字を、コントロールトータルと照合し、データ入力エラーを検知する。例えば、オンライン受注入力システムで処理された取引の合計数と、請求システムで処理された件数の合計との自動的な照合がある。
- チェックデジット—計算によってデータを検証する。部品番号には、納入業者からの発注の誤りを検出し、修正するためのチェックデジットが含まれる場合がある。統一商品コード(UPC)は、商品とベンダーを識別するチェックデジットが含まれている。
- 使用可能データリスト—受付可能なデータを、あらかじめ定義されたリストとしてユーザに提供する。例えば、イントラネットのサイトには、商品のドロップダウンリストが掲載されていることがある。

- データ合理性テスト－現在もしくは経験に基づいた合理性パターンと、収集されたデータとを比較する。例えば、ホームセンターから仕入先への異常に大量な木材の注文は、調査の対象となる場合がある。
- 論理テスト－範囲制限や、入力値のテストなどがある。例えば、形式が定められたクレジットカード番号がある。

全般統制は、業務処理統制の有効性を確保するために必要なものである。また、情報処理の正確性と、組織の管理、ガバナンス、報告に使用される情報のインテグリティを確保するには、この2つの統制が必要である。手作業の統制から、自動化された業務処理統制への移行が進むにつれて、全般統制が一層重要なものとなる。

統制活動は、バーゼルⅡの原則6に対応している。

情報と伝達

COSOは、事業を経営し、組織の統制目標を達成するには、組織の全ての階層において、情報が必要であると述べている。しかし、必要となる情報の識別、管理および伝達は、IT部門にとっての永遠の課題である。統制目標の達成に必要な情報を識別すること、また各人の職務遂行を可能とする方法と時間内での情報の伝達を行うことが、COSOのその他の7つの要素の実現をサポートする。

IT組織は、財務報告に関連する、ほとんどの情報を処理している。しかし通常、その業務範囲は、より広い範囲に及んでいる。IT部門は、電子メールシステムや意思決定支援システムのように、重要な事象の識別と伝達を目的とする機能の導入を支援することもある。

COSOは、以下の事項を含む、情報の品質について言及している。

- 適切性－正しい情報か
- 適時性－必要なときに利用でき、適切な時間内に報告されるか
- 最新性－最新の情報か
- 正確性－データは正確か
- アクセス可能性－認可された個人が、必要なときにアクセスできるか

組織レベルでは、以下の対応が期待されると考えられる。

- 会社の方針の策定と伝達
- 月次／四半期／年次のマネジメント報告および情報開示報告の期限、照合、様式と内容を含む、報告要件の策定と伝達
- 財務情報の統合と伝達

業務レベルでは、以下の対応が期待されると考えられる。

- 企業方針の目的を達成するための基準の策定と伝達
- 事業目的を達成するための情報の識別と適時の伝達
- セキュリティ違反の識別と適時の報告

情報と伝達は、バーゼルⅡの原則3、5、6、10に対応している。

モニタリング

モニタリングは、継続的、また一定時点における評価プロセスを通じた、マネジメントによる内部統制の監視を含み、IT管理において、ますます重要なものとなっている。

COSOは、2006年に、有効なモニタリングを行うために実施すべき事項として以下の提案を行っている。

- 可能な範囲でのオペレーションとの統合－継続的モニタリングが、組織の業務活動に組み込まれていること。
- 客観的な評価の実施
- 専門知識を備えた評価者の活用－評価者は、評価対象、およびそれが情報の信頼性を確保するための活動とどのように関連しているのかについて理解していること。
- フィードバックの検討－経営陣、金融機関の監督当局、および市場参加者が、財務報告、リスク管理およびコンプライアンスに関する内部統制の有効性についてフィードバックを受けること。
- 範囲と頻度の調整－経営陣、および金融機関の監督当局は、統制対象のリスクの重要性、リスクを低減するコントロールの重要性、および継続的モニタリングの有効性に応じて、独立した評価の範囲と頻度を変更すること。

従来以上に、IT のパフォーマンスと有効性は、その基礎となる統制の有効性に関する評価指標を通して、継続的にモニタリングされるようになっている。

次の例について考えてみる。

- 不備の識別と管理－評価指標を確立し、評価指標に対する実績値の傾向を分析することによって、処理の失敗に関する根本的な原因を理解するための手掛かりを得ることができる。このような原因を是正することによって、システムの正確性、処理の網羅性、およびシステムの可用性を向上することができる。
- セキュリティのモニタリング－効果的なITセキュリティ・インフラストラクチャを構築することによって、不正アクセスのリスクが低減される。セキュリティの水準を強化することによって、不正な取引や不正確な報告が行われるリスクを低減することができる。さらに、アプリケーションやITインフラストラクチャに問題が起きた場合でも、主要システムが使えなくなるリスクを低減することにつながる。

IT 組織では、次に挙げるように、様々なかたちでの独立した評価が行われている。

- 内部監査
- 外部監査
- 監督当局による検査
- ネットワーク攻撃および侵入検査
- 第三者によるパフォーマンスとキャパシティ分析
- IT の有効性レビュー
- コントロールの自己評価
- 第三者によるセキュリティレビュー
- プロジェクトの事後レビュー

組織レベルでは、次のような対応が期待される。

- システムの運用状況に関する、集中した継続的モニタリングの実施
- セキュリティに関する、集中したモニタリングの実施
- IT に関する内部監査の実施（監査は活動レベルで実施されるが、監査委員会に対する監査結果の報告は、組織レベルで実施される）

業務レベルでは、次のような対応が期待される。

- 不備の識別と管理
- 各拠点におけるシステム運用やセキュリティのモニタリング
- 各拠点における IT 要員の監督

モニタリングは、バーゼルⅡの原則 2、8、9 に対応している。

オペレーショナル・リスクの原則とITとの関係

情報技術と情報管理は、GRCの管理および所要自己資本の最適化に関する、包括的な戦略の鍵となる要素である。アプリケーション、インフラストラクチャの各要素、および統制など、ITに関連する部分は、全てオペレーショナル・リスクの一部として定義されている。図表6では、オペレーショナル・リスクに関するバーゼルIIの原則、それに対応するCOSO ERMの構成要素、ならびにITへの関連性と要求事項とを示している。

この原則は、本書の利用と導入を、統合されたGRCフレームワークに沿って実現することを目的としている。

図表6 バーゼルIIの原則、COSOの構成要素、ITへの関連性と要求事項

バーゼルIIの原則 注: 斜字体箇所はバーゼルIIからの引用	COSOの構成要素	ITへの関連性と要求事項
適切なリスクの管理環境の構築		
<p>原則1:</p> <p>取締役会は、個別に管理すべきリスクカテゴリーの1つとして、銀行におけるオペレーショナル・リスクの主な状況を認識し、銀行のオペレーショナル・リスク管理フレームワークの承認、および定期的な見直しを行うべきである。このフレームワークでは、銀行全体としてのオペレーショナル・リスクを定義し、その識別、評価、モニタリング、および統制と低減に関する原則を提供すべきである。</p>	内部環境	ITは、全般的なリスク管理プロセスの一部に統合すべきである。
<p>原則2:</p> <p>取締役会は、銀行のオペレーショナル・リスク管理のフレームワークを、業務から独立し、必要な教育を受けた適切な要員による、効果的かつ包括的な内部監査の対象とすべきである。内部監査部門は、オペレーショナル・リスク管理に、直接の責任を負うべきではない。</p>	モニタリング	<p>ITを含む金融機関のオペレーショナル・リスク管理のフレームワークは、内部監査計画の対象とすべきである。</p> <p>IT内部監査部門には、適切なスキルを備えた要員を配置すべきである。この要員は、バーゼルII、リスク管理の原則、金融機関に対する規制および監督上の要求事項について理解すべきである。</p> <p>IT内部監査部門は、金融機関の監督当局によるレビューの対象とすべきである。</p> <p>適切な場合、外部の専門家を利用すべきである。</p>
<p>原則3:</p> <p>マネジメントは、取締役会に承認されたオペレーショナル・リスク管理のフレームワークの導入に関して、責任を負うべきである。フレームワークは銀行全体を対象として導入されるべきであり、また、全ての階層の従業員が、オペレーショナル・リスク管理における自身の役割について理解すべきである。マネジメントは、銀行の主要な商品、活動、プロセスおよびシステムにおけるオペレーショナル・リスクの管理方針、プロセスおよび手続の策定にも責任を負うべきである。</p>	内部環境 情報と伝達	<p>IT部門の幹部は、経営陣と同等の責任を負う。</p> <p>銀行で採用されたフレームワークは、ITに関する要求事項を満たすよう、適合させるべきである(最も一般的なGRCフレームワークは、ITについて、詳細には解説していない)。金融機関のGRCフレームワークに適合した、IT統制のフレームワークを導入することも考えられる。</p> <p>採用されたフレームワークは、金融機関の監督当局と検査官が対象とする可能性がある範囲を網羅しているべきである。例えば、ITコーポレート・ガバナンス、IT計画と組織、セキュリティ、システム開発、プログラム変更、運営とサポート、内部統制に関する責任などがある。</p>

<p>パーゼルⅡの原則</p> <p>注:斜字体箇所はパーゼルⅡからの引用</p>	<p>COSOの構成要素</p>	<p>ITへの関連性と要求事項</p>
<p>リスクの管理:識別、評価、モニタリングと低減/コントロール</p>		
<p>原則4:</p> <p>銀行は、全ての主要な商品、活動、プロセス、システムにかかわるオペレーショナル・リスクを識別し、評価すべきである。銀行は、新しい商品、活動、プロセス、システムの導入前、または実施前に、オペレーショナル・リスクについて、適切な評価を行うようにすべきである。</p>	<p>目的の設定</p> <p>事象の識別</p> <p>リスクの評価</p>	<p>リスク評価は、銀行に大きな影響を及ぼす可能性がある全てのIT活動、例えば、プログラム変更、インフラストラクチャ変更、またセキュリティモニタリングなどについて行うべきである。</p> <p>リスク評価は、システム開発とリリース管理のプロセスに統合すべきである。</p> <p>重大な影響を受ける可能性のある利害関係者は、リスク評価に関与すべきである。</p> <p>リスク評価の結果は、その他のリスク評価の結果と統合されて、GRCフレームワークに盛り込まれるべきである。</p>
<p>原則5:</p> <p>銀行は、オペレーショナル・リスクの状況と、損失につながる可能性がある重大なエクスポージャについて、定期的に監視するプロセスを導入すべきである。オペレーショナル・リスクを積極的に管理するための情報を、経営陣と取締役会に対して定期的に報告すべきである。</p>	<p>事象の識別</p> <p>リスクの評価</p> <p>情報と伝達</p>	<p>オペレーショナル・リスクの評価を、年間計画と戦略計画のサイクルに含むべきである。</p> <p>オペレーショナル・リスクは、組織内外で重要な事象が発生した場合には、再評価すべきである。例えば、災害が発生したときに、コンティンジェンシープランを見直すことなどがある。</p> <p>リスクの評価指標を識別し、監視すべきである。望ましくない兆候が発見された場合、原因調査を実施し、的確な対策をとらるべきである。</p>
<p>原則6:</p> <p>銀行は、重大なオペレーショナル・リスクの統制と低減のいずれか、または両方を行うための方針、プロセスおよび手続を策定すべきである。銀行は、リスク制限とコントロール戦略を定期的に見直し、適切な戦略を用いて、リスク選好とリスク・プロファイル全体の観点に基づいて、オペレーショナル・リスクに関する現状認識を修正すべきである。</p>	<p>リスクへの対応</p> <p>内部環境</p> <p>情報と伝達</p> <p>統制活動</p>	<p>オペレーショナル・リスクを低減するために、IT内部統制のフレームワークを構築すべきである。</p> <p>IT内部統制のフレームワークを、適切な方針、プロセス、手続によって確立すべきである。</p> <p>オペレーショナル・リスクは、組織内外で重要な事象が発生した場合には、再評価すべきである。例えば、他の銀行を買収したときに、システム統合がオペレーショナル・リスクに与える影響について検討することなどがある。</p> <p>ITに関する方針と手続を、最低年に1回、見直し、承認すべきである。</p>
<p>原則7:</p> <p>銀行は、重大な業務の中断が発生した場合にも事業を継続し、損失を最小化できるよう、コンティンジェンシープランおよび事業継続計画を策定すべきである。</p>	<p>リスクへの対応</p>	<p>IT部門は、全社事業継続計画と事故対応管理に対応した、ITに関する継続計画と管理手続を策定すべきである。</p>

<p>バーゼルⅡの原則</p> <p>注:斜字体箇所はバーゼルⅡからの引用</p>	<p>COSOの構成要素</p>	<p>ITへの関連性と要求事項</p>
<p>監督当局の役割</p>		
<p>原則 8:</p> <p>監督当局は、全ての銀行に対して、リスク管理に関する全体的な取り組みの一部として、主要なオペレーショナル・リスクの識別、評価、モニタリング、および統制/低減を行うための効果的なフレームワークを確立することを求めるべきである。</p>	<p>モニタリング</p>	<p>IT部門は、金融機関の監督当局の要求事項に対応した、ITリスク管理のフレームワークを導入すべきである。</p>
<p>原則 9:</p> <p>監督当局は、オペレーショナル・リスクに関する銀行の方針、手続および実務に対する、直接的または間接的な独立的評価を、定期的実施すべきである。監督当局は、銀行の対応状況を継続的に把握する仕組みを構築すべきである。</p>	<p>モニタリング</p>	<p>IT部門の幹部は、ITに関する監督上のコンプライアンス要件が、オペレーショナル・リスクおよび監督当局の要求事項に対応するための組織全体の方針と手続に、確実に統合されるようにすべきである。また検査官が発見した不備については、適時に対応が行われるようにすべきである。</p> <p>ITコンプライアンス担当部門は、監督当局が、ITに関する対応状況を継続的に把握できるように、金融機関のコンプライアンス部門に統合すべきである。</p>
<p>原則 10:</p> <p>銀行は、市場参加者がオペレーショナル・リスク管理に関するアプローチを評価できるように、十分な情報公開を行うべきである。</p>	<p>内部環境</p> <p>情報と伝達</p>	<p>IT部門は、主要なオペレーショナル・リスクを構成する全ての関連リスクを識別し、その内容を取締役会と経営陣に伝達すべきである。</p>

6. 情報リスク管理

情報とITの管理においては、GRCに対応するための具体的アプローチが必要である。IT環境の複雑性、ビジネスプロセスとの相互依存性、および間接的なリスクの識別とそのリスクへの対応の必要性は、ITリスクのフレームワークを定義し、展開していくうえでの重要な要因である。リスクの評価、統制および低減は、組織が、バーゼルⅡに基づいて選択したオペレーショナル・リスク全体を管理する手法に整合させ、実施すべきである。オペレーショナル・リスクの管理と監督に関する健全な実務(サウンドプラクティス)⁶で定義されているオペレーショナル・リスクの原則から、情報とITリスクの管理に必要な指針を導き出すことができる。

ITに関する指針

本書の指針を適用することは、ITの実務者、また情報技術を担当する金融専門家にとって必要である。後述するITに関する指針(ITGP)は、以下の資料に基づいて作成された。

- *International Convergence of Capital Measurement and Capital Standards (バーゼルⅡ自己資本規制またはバーゼルⅡ)*、バーゼル委員会発行(2006年6月)⁷
- *Sound Practices for the Management and Supervision of Operational Risk*で定義された諸原則、バーゼル委員会発行(2003年2月)⁸
- *Enterprise Risk Management—Integrated Framework*、COSO発行(2004年9月)⁹

ITGP1(オペレーショナル・リスクの認識)

情報管理および情報技術は、オペレーショナル・リスク管理の重要な構成要素である。実務者、内部監査人および金融業務の専門家は、情報リスクの重要性について認識すべきである。

組織は、オペレーショナル・リスクが全体のリスクポジション、ひいては自己資本賦課に影響することを認識すべきである。また組織は、ITの構成要素について定義を明確にし、理解を深めていく必要がある。この理解は、ITリスクが存在しているという、事実のみに留まるべきではない。GRCに関連する全ての目標と実務は、組織全体のGRCフレームワークとの整合性が保たれていなくてはならない。

バーゼルⅡでは、オペレーショナル・リスクを、「不適切な、または失敗した内部プロセス、人、システム、あるいは外部事象によって発生する損失のリスクと定義される。この定義には、法務リスクを含む。」と定義している。法務リスクには、監督当局による処分や企業間の示談の結果としての、罰金、ペナルティおよび懲罰的損害賠償が含まれるが、これに限定されるものではない。ただし、オペレーショナル・リスクには、「戦略リスクと風評リスクは含まない¹⁰」とされている。多くのIT関連リスクは、システムばかりでなく、要員または内部プロセスにおける課題にも関係しており、前述したオペレーショナル・リスクの定義は、情報技術と情報管理についても適用すべきである。重要なインフラストラクチャの機能を阻害するような、インシデントや災害等の外部事象は、情報技術に影響を与える可能性がある。

信用リスク、金利リスク、流動性リスクなど、金融業務における重要なリスクの管理と同様に、厳しい基準を、オペレーショナル・リスク管理にも適用すべきである。しかし、オペレーショナル・リスクの中で典型的なものは、金融業務におけるその他のリスクと異なり、損失の一方で利益が期待できるといったものではなく、通常の企業活動の中に存在し、リスク管理プロセスに影響を与える¹¹。同時に、不適切なオペレーショナル・リスク管理は、組

⁶ *Sound Practices for the Management and Supervision of Operational Risk* バーゼル銀行監督委員会(2003年2月)参照。

⁷ *International Convergence of Capital Measurement and Capital Standards*の詳細については、www.bis.org/publ/bcbs107.htm参照。

⁸ *Sound Practices for the Management and Supervision of Operational Risk*の詳細については、www.bis.org/publ/bcbs91.htm参照。

⁹ *Enterprise Risk Management—Integrated Framework*の詳細については、www.coso.org/publications.htm参照。

¹⁰ *International Convergence of Capital Measurement and Capital Standards* バーゼル銀行監督委員会(2006年6月)の段落644参照。

¹¹ バーゼル委員会は、信用リスクや市場リスクがほとんどない業務(例えば、資産管理や支払および決済など)において、オペレーショナル・リスクを許容

織のリスク・プロファイルに誤りを生じさせ、組織に大きな損失を与える可能性がある。

これは、金融機関における情報管理と IT の領域に関して、IT に存在するオペレーショナル・リスクは、信用リスクや市場リスク等その他の GRC 要素と、少なくとも同等に、詳細かつ包括的に管理されなくてはならないことを意味している。そのため、IT に関連する GRC の要素を、予算、経営資源および経営陣の注意と支援の観点から、適切に管理すべきである。

ITGP2(内部監査の要件)

IT 内部監査部門は、有効かつ包括的な必要がある。監査の有効性を保つために、適切なスキル、要員および予算を確保すべきである。

一般的に、内部監査の重要性を、内部 IT 監査、または業務や情報リスクの監査を行う組織、およびその機能に反映すべきである。金融機関の規模と複雑さに応じて、IT 内部監査部門のスキル、要員、予算を決定すべきである。内部要員だけでは十分な対応ができない場合には、外部の専門家を活用することも考えられる。IT 内部監査は、組織の監査委員会に対する最終的な責任を負い、必要に応じて取締役会への報告を行うべきである。

IT 内部監査は、組織の経営陣に対して公平であり、また独立的でなければならないことに留意すべきである。

ITGP3(マネジメントの方針、プロセス、手続)

情報管理および情報技術を、リスク管理に関する適切な方針、プロセス、手続に基づいて統治すべきである。実務者、内部監査人および金融専門家に対しては、組織の GRC フレームワークに一致したガイダンスを示すべきである。

GRC を管理するには、GRC 全体の構造と構成に合致し、明確に定義され、文書化された一連の方針、プロセスおよび手続が必要である。IT 方針は、範囲と内容について、具体的で的を絞ったものにすべきである。この指針は、リスク関連コントロール (ITGP6 参照) を除く、リスク管理プロセスの要件を対象としている。

オペレーショナル・リスクに関する規律は、オペレーショナル・リスク管理にのみ有効であり、他のリスクを所管する部門の場合、その所管するリスクとは分けて考える必要がある。これは、信用リスクまたは市場リスク管理部門がオペレーショナル・リスクに関して実施した作業は、信用リスクまたは市場リスクへの対策とはならないことを意味する。同様に、信用リスクまたは市場リスク管理部門で発生したオペレーショナル・リスクの事故は、信用リスクまたは市場リスクの事故とはならない。

この指針は、金融機関において IT を主管する部門にとって、特に重要である。多くの場合、信用リスク、市場リスクおよびその他の主要なビジネスリスクを管理し、コントロールし、報告するために IT が導入される。しかし、IT アプリケーションやインフラストラクチャなどの IT の構成要素は、特定の目的と関係なく、オペレーショナル・リスクの範囲に含まれる。例えば、信用リスクを測定するアプリケーションの不具合は、IT の障害であり、オペレーショナル・リスクとしてのシステム障害である。

ITGP4(リスク評価)

情報管理と情報技術においては、組織の GRC フレームワークに従った、承認された手法によって、個別のリスク評価を行うべきである。リスク評価では、情報技術固有の複雑性や間接的なリスク要因を考慮すべきであ

するの、それともオペレーショナル・リスクを管理し効率的に評価する能力を身につけて対処するのか、その判断の結果が、銀行におけるリスクとそれに見合った報酬の計算に不可欠であると考えている。

る。

ITリスクと関連するリスク要因を理解するには、直接的および間接的リスクについて深く理解することが可能なリスク評価手法を選択すべきである。リスク評価には、IT固有リスクとITの利用に起因するリスクの両方を含むべきである。

効果的かつ効率的なリスク管理を行うには、主要なリスクを含む、組織のリスク・プロファイルが必要である。リスク・プロファイルは、組織における主要リスクの一覧を提供するとともに、ビジネスライン、リスク管理者、セキュリティ実務者、事業継続計画の担当者および内部監査部門に対して、それぞれの責任範囲において、どのようにリスク管理の責任を果たすべきかを明確に伝えるべきである。また、IT組織では、適切な職務分離を行うべきである。

ITGP5(リスクと損失のモニタリング)

情報管理および情報技術にかかわる損失を、測定し、文書化すべきである。特定のリスク・プロファイルを、監視すべきである。

情報技術に関連した損失を、組織が実施する、損失に関する総合的なモニタリングに従って監視すべきである。リスク・プロファイルには、情報技術の複雑性と、金融機関における情報技術の利用状況を、適切に反映すべきである。

組織は、自らのリスク選好、すなわち受容可能なリスクの大きさについて、明確に定義する必要がある。定義したリスク選好の範囲外にあるリスクや事象を、即座に改善措置を取ることができるよう識別すべきである。インシデントに対する責任は、組織のインシデント管理および上位者、上位組織への報告に関する方針に従って割当てる必要がある。また、この方針には、最高経営責任者(CEO)、最高リスク管理責任者(CRO)、最高情報セキュリティ責任者(CISO)、内部監査部門およびリスク監査委員会に、重大なインシデントと関連するリスクを報告するためのプロセスを定義すべきである。

進化しつつある規制制度に対するコンプライアンスは、正確な報告に重点を置いている。バーゼルⅡにおけるデータ品質は、それ自体が目的ではなく、目的を達成するための手段であるが、リスクに基づく資本の配置を行うには、高品質かつ最新のデータを必要とする。確実な情報は、リスク管理強化の鍵である。財務報告書の正確性と内部統制の有効性を証明するにあたって、不適切なデータ品質は、経営者の意思決定に誤りをもたらす可能性がある。

「先進的計測手法(AMA)の主な論点につきみられたプラクティスの幅」¹²では、データ品質に関する課題を、次のように示している。

先進的計測手法(AMA)を採用した銀行が収集する、オペレーショナル・リスクデータの性質と品質は、その銀行の定量化プロセスの結果ばかりではなく、オペレーショナル・リスク管理における意思決定にも影響を与える。そのため、バーゼルⅡでは、銀行がAMAを採用する条件として、オペレーショナル・リスクデータが満たすべき基準を定めている。この基準は、主に、どのようにデータを収集し利用するかという、データの性質に関連するものである。この基準の目的は、AMAの効果的な導入に欠かせない、データのインテグリティと包括性に対する、監督当局の最低限の要求について見解を示すことにある。

AMAにおけるオペレーショナル・リスクデータには、リスク定量化、リスク管理、会計やその他の形式の報告を含む、複数の用途がある。2つ以上の用途に適したデータもあれば、1つの用途のみに適しているデータもある。

データ品質を確保するためには、情報を管理し、そのインテグリティ、正確性、網羅性および適時性を確保するためのプロセス、手順および規律を構築することが必要である。データ品質を確保するための基本的な属性には、以下の事項を含むべきである。

¹² “Observed Range of Practice in Key Elements of Advanced Measurement Approaches (AMA)” the Accord Implementation Group’s Operational Risk Subgroup (AIGOR) (2006年10月)。本論文は、特に先進的計測手法に関するバーゼルⅡの要件について、それを満たすためのオペレーショナル・リスク管理フレームワークの開発、導入、維持に関連する実務上の諸課題に焦点をあてている。

- 正確性
- インテグリティ
- 一貫性
- 網羅性
- 妥当性
- 適時性
- アクセス可能性
- 有用性
- 可監査性

様々なアプリケーションによって提供されるデータの品質は、その情報が作成される元となったデータの品質とインテグリティによって決まる。データを、組織の資産として取り扱っている組織は、積極的なデータ管理の取り組みを進める上で有利である。データ品質を自己の問題と考えない組織は、常に「ゴミからはゴミしか生まれない」という状況に陥る。

データ品質に関するコミットメントは、会社全体に行き渡る明確な説明責任の体制と合わせて、経営トップによって推進される必要がある。最終的には、取締役会、CEO、CFO、CRO および CISO が、コンプライアンスのためのデータのインテグリティと適合性に関する説明責任を負う。

ITGP6(統制とリスク削減に関する方針、プロセス、手続)

情報管理と情報技術を、リスクの統制および削減に関する適切な方針、プロセス、手続に基づいて統治すべきである。実務者、内部監査人および金融専門家に対して、組織の GRC フレームワークに一致したガイダンスを示すべきである。

リスクの統制および低減に関する方針、プロセスおよび手続を、経営方針を補完するものとして導入すべきである。これには、コントロールと測定に関するプロセス、個別のリスクを低減するための手続、および情報管理および情報技術にかかわるリスクを幅広く対象とするその他のガイダンスが含まれる。リスクの統制および低減を、総合的なリスク管理プロセス(ITGP3 参照)とは別のものとして考えるべきである。

規制のもとにある金融機関であっても、市場では、たった一人の人間によって評判が損なわれる可能性があるため、組織のあらゆる部門や個人が、コンプライアンスに関連するリスクを認識し、責任を負うべきである。また、その組織の中で最も脆弱で非倫理的な従業員が、組織としての脆弱性や倫理性の水準となるため、不十分な統制環境に対する責任を、組織全体で負っていく必要がある。取締役会や経営者は、有効な統制環境を認識し、それを維持する企業文化を構築するための経営者の姿勢を示す必要がある。その一方で、組織内のすべての個人は、内部統制について、理解すべきである。コンプライアンスがないところでは、ルールは無意味である。

ITGP7(事業継続管理)

情報管理と情報技術を、包括的な事業継続の管理プロセスによって、保護すべきである。IT の継続に関する管理プロセスを、組織全体の事業継続管理のフレームワークと整合性が保つべきである。

IT の継続性、インシデント管理および復旧は、全て、包括的な IT 継続の管理プロセスの要素である。困難な状況においても、IT と主要なビジネスプロセスを継続させることができるよう、IT の継続を、事業継続と整合することが重要である。

金融機関の事業継続に関する上位原則は、バーゼル委員会¹³によって文書化されている。この原則では、実施とモニタリングに関する経営陣の責任のもとで、組織は、事業継続管理(BCM)プロセスを整備、導入すべきであることが明記されている。この上位原則には、その他の基準および出版物¹⁴において述べられている、事業継続管理における継続的なライフサイクルの要素が含まれている。情報管理および情報技術に関するIT継続計画を、情報リスクに関する計画と同様に、適用されている方法やフレームワークにかかわらず、企業全体の事業継続管理に従って、実施すべきである。また、さまざまな文献¹⁵で示されているように、IT継続の計画、実施、モニタリングを適切に行うべきである。ITは、より広い概念である事業継続管理に関して組織が持つ能力の一部である。十分に練り上げられたIT継続は、ビジネスからの強い支援と、ビジネスプロセスオーナーとの協働が不可欠である。これは、ITは、単独では存在することができず、また他と切り離された継続計画の対象とはならないためである。

ITGP8(リスク統制とリスク低減のフレームワーク)

情報管理と情報技術を、組織のGRCフレームワークにおける不可欠な要素とすべきである。情報に関連したリスクの統制と低減を、GRCフレームワークにおいて定義し、認識すべきである。

ITに関連したリスクに関する統制と低減の計画、および活動を、GRCフレームワークに従って、計画、実行、モニタリングすべきである。いかなる技術的な手段も、GRCフレームワークにおいては、それぞれ異なる種類のリスクとして認識すべきである。これには、組織マネジメント、個別の統制、コンプライアンスのガイダンスなどが含まれるであろう。

ITに関連したリスクの統制と低減は、しばしば、ERMフレームワークの一部として定義され、また、組織的なGRCの一部でもある。ERMは、人によって違った意味を持つ可能性がある、極めて幅広い内容を持つ用語である。COSOでは、ERMに関して、次のように述べている。

- ERMは、プロセスである。目的を達成するための手段であり、それ自体が目的ではない。
- 人から影響を受ける。単なる方針、サーベイ、形式ではなく、組織内のあらゆる要員と関係している。
- 戦略の設定に適用される。
- 全ての階層および部門を含む組織全体に適用され、リスクに関して、組織全体のポートフォリオの視点を取ることを含む。
- 組織に影響を与える可能性のある事象を識別し、リスク選好の範囲内にリスクが入るよう管理するために設計されている。
- 組織の経営者および取締役会に対して、絶対的ではないが、合理的な保証を与える。
- 目的達成のために組み立てられる。その目的は、1つのカテゴリーに含まれる場合もあれば、複数のカテゴリーに含まれる場合もある。また、カテゴリーが重複している場合もある。

ERMの基本的な前提は、すべての組織は、利害関係者に対して、なんらかの価値を提供するために存在するということである。どのような組織であろうと、不確実性に直面するのであって、経営者の課題は、利害関係者のために価値の向上を目指すにあたって、組織が受容できる不確実性の程度を決定することである。不確実性は、組織の価値を喪失させる可能性と高める可能性の両方を持つために、リスクでもあり事業機会でもある。ERMによって、経営者は、不確実性とそれに付随するリスクや事業機会に有効に対応でき、価値を創造するた

¹³ ジョイントフォーラム“事業継続に関する原則の概要”(2006)参照。

¹⁴ 英国規格(BS25999-1)および事業継続協会発行 *Good Practice Guidelines for Business Continuity Management, 3rd Edition* (2007年)参照。

¹⁵ ITIL(ITサービス継続性管理)、ISO27001、およびBS PAS 77参照。

めの組織の能力を向上させることができる。

経営者が、成長および収益の目標と、関連するリスクとの間で最適なバランスを保つように戦略や目的を設定し、その目的を達成するために、資源を効率的かつ有効に配分した場合に、組織の価値が最大化される。

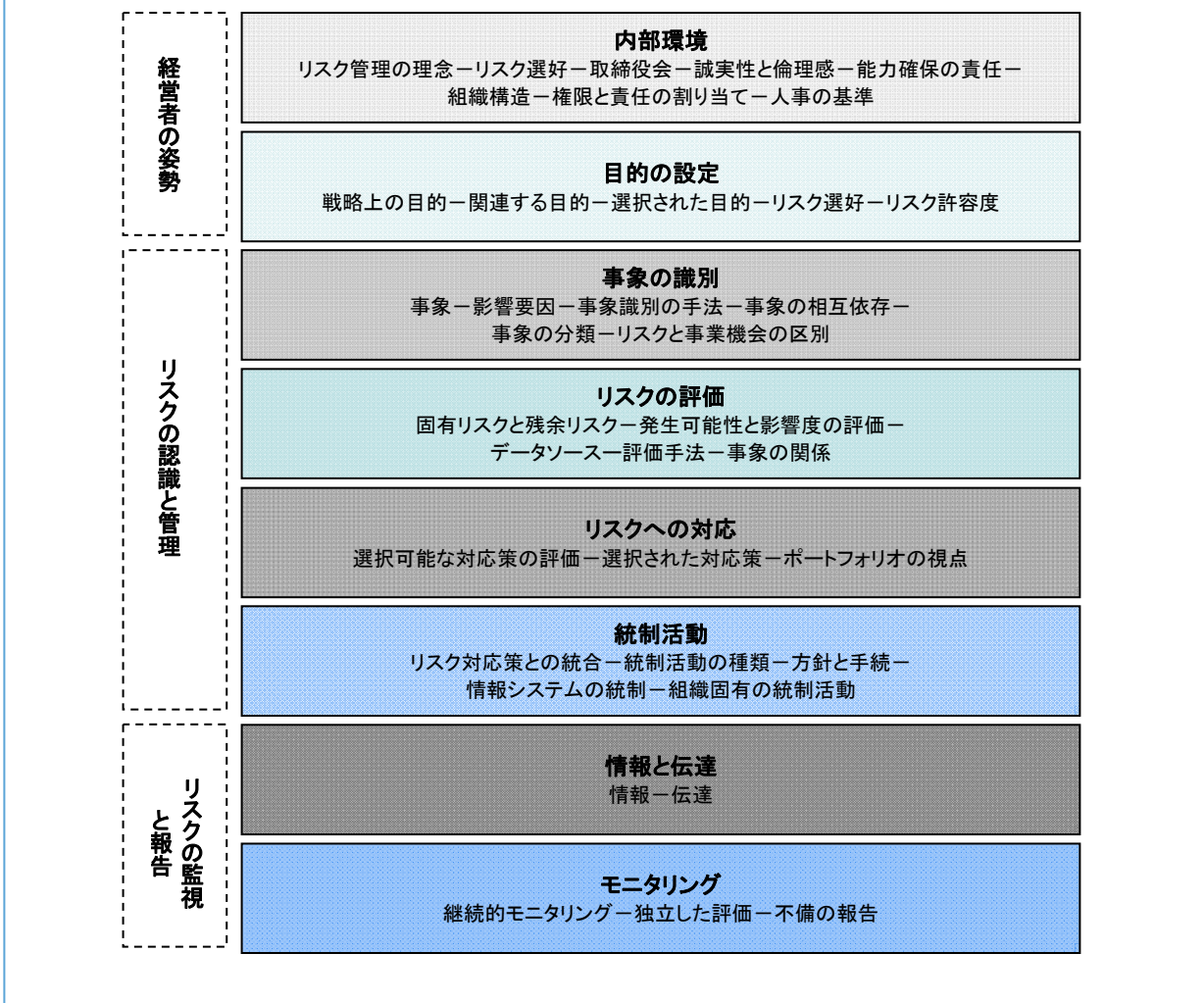
ERMには、以下の内容が含まれる。

- リスク選好と戦略との調整－経営者は、戦略に関する代替案の評価、選択した戦略に関連する企業目的の設定およびリスク管理の仕組みの構築において、組織のリスク選好を考慮する。
- リスクへの対応に関する意思決定の質の向上－ERMは、リスクの回避、低減、共有、受容といったリスク対応の代替策の中から、対応策を識別し選択するための明確な方向性を示す。
- 業務上の予期できない事象と損失の低減－組織は、潜在的な事象を識別する能力を高めることによって、予期できない事象の発生、および関連する費用と損失を低減するための対策を確立する。
- 複数あるいは企業全体にわたるリスクの識別と管理－すべての企業は、組織の異なる部門に影響を及ぼす、広範囲で多様なリスクに直面している。ERMは、相互に関連する影響への効果的な対応、および複数のリスクへの一体化した対応を促進させる。
- 事業機会の認識－経営陣は、すべての領域における潜在的な事象を考慮することによって、事業機会を識別し、積極的に理解することができる。
- 資本配分の改善－経営陣は、リスクに関する確かな情報を得ることによって、全体的な資本の必要額を効果的に評価し、資本の配分を改善することができる。

図表7に示されているとおり、COSO ERMフレームワークは、経営者の姿勢、リスクの認識と管理、リスクの監視と報告という3つの異なるドメインの下に、内部環境からモニタリングまで、相互に関連する8つの構成要素によって構成されている。¹⁶

¹⁶ 各構成要素については、COSOの文献で詳しく説明されており、www.coso.org/publications.htmから、少額でダウンロード可能である。

図表7-COSO ERM フレームワーク



ERM では、企業全体のリスク管理に関して、全体論的アプローチを採用している。ERM は、マイナス面あるいはリスクの回避のみを対象とするのではなく、むしろ、十分な情報に基づくバランスのとれたアプローチによって、リスクを受け入れるものである点に留意することが重要である。統制の8つの構成要素は、組織全体に存在し機能していなければならない。これには、企業目標に影響を与える主要なリスクの識別が含まれる。このリスクは、まず、統制が全く存在しない場合のリスクの理解を含む、固有リスクとして評価される。次に、固有リスクに対して、存在している統制を考慮して、残余リスクが評価される。残余リスクが、リスク選好の範囲を超えている場合、これをリスク選好の範囲内に収めることができるように、追加的な統制が導入される。

企業目標の達成は、統合された ERM フレームワークの成果とみなされる。企業目標は、次のように分類される。

- 戦略－組織のミッションと一致しそれをサポートする上位目標
- 業務－様々な経営資源の効果的かつ効率的な利用
- 報告－信頼性
- コンプライアンス－適用法令

情報管理および情報技術に関するリスク管理のイニシアチブとプログラムは、GRC アプローチ全体に統合すべきである。この指針を適用する実務者は、ISACA/ITGI の刊行物である CoBiT を利用して、COSO に基づく ERM と IT との関係について理解すべきである。

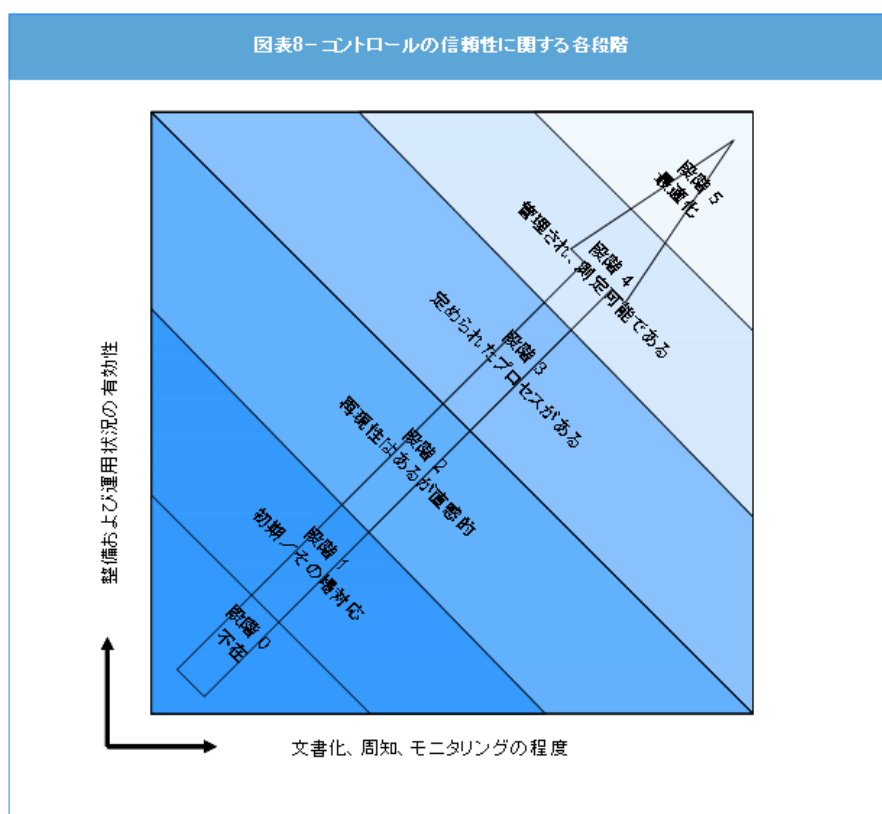
ITGP9(独立した評価)

情報管理および情報技術にかかわるリスクを、監督上の検証プロセスに対応できるよう適切に文書化すべきである。独立した監査部門は、オペレーショナル・リスクと情報リスクのプロファイルに従って、ITに関連するオペレーショナル・リスクの管理について、検証しなければならない。

監督のための検証プロセスの実行を可能にし、サポートするための要件に従って、情報関連リスクを、文書化することが求められる。文書は、定期的な外部レビューを含め、公正かつ独立したレビューの対象とすべきである。IT リスクにかかわる文書の監査および独立したレビューは、組織が定義したリスク・プロファイルと整合性が保たれるべきである。

組織は、ERM の全体的な能力について、成熟度評価を採用すべきである。「能力」とは、規律やプロセスがどの程度機能しているかを表し、「成熟度」は、その能力がどの程度発達しているかを示す指標である。成熟度モデルで分析の対象となるプロセスは、少なくとも、管理され測定可能であることが求められる、ステージ4の段階にあるべきである。

ERM フレームワークの各要素は、図表 8 に示す、コントロールの信頼性に関する6つの段階で評価される。



- 0 不在—識別可能なプロセスが完全に欠落している。企業は、対応すべき問題が存在することすら認識していない。
- 1 初期/その場対応—企業は、対応が必要な問題の存在について認識している。ただし、標準化された

プロセスは存在せず、対応は、個人的に、または場合に応じて場当たりので行われている。総合的な管理方法は体系化されていない。

- **2 再現性はあるが直感的**—同じ仕事に携わる複数の要員において同等の手続が行われる段階にまで、プロセスが進歩している。標準的な手続に関する正式な研修や周知は行われておらず、実行責任は、個人に委ねられている。個人の知識への依存度が高く、そのため誤りが発生しやすい。
- **3 定められたプロセスがある**—手続は、標準化および文書化されており、研修により周知されている。ただし、このプロセスに従うかどうかの判断は個人に委ねられているため、プロセスからの逸脱はほとんど発見される見込みがない。手続自体は、既存の実施基準を正式化しただけのものであり最適化されていない。
- **4 管理され、測定が可能である**—手続のコンプライアンス状況をモニタリングおよび測定でき、プロセスが効果的に機能していないと判断された場合に対処が可能である。プロセスは常に改善され、優れた実践方法(手法)が提供される。自動化やツールの活用は、限定的または断片的に行われている。
- **5 最適化**—継続的改善、および他社との比較による成熟度モデル化の結果、プロセスがベストプラクティスのレベルにまで最適化されている。ITは、統合され、ワークフローが自動化されている。これにより、品質と有効性を向上させるツールが提供され、企業の迅速な環境適応に貢献している。

組織の ERM 能力に関する成熟度のフレームワークは、ボトムアップおよびトップダウンの両面から、評価され、管理されなければならない。また、ERM は、統合されたフレームワークでなくてはならない。従って、能力成熟度評価は、モニタリングにおけるデータの品質、役割の明確さ、ツール、要員のスキル等に関して、ERM フレームワーク全体を弱体化する可能性がある問題点を発見できるものでなければならない。詳細は、「付録 IV COSO ERM フレームワークのデータ品質への依存度」を参照のこと。

ITGP10(ディスクロージャー)

実務者、内部監査人および金融専門家は、開示対象となる全ての情報に関するリスクを識別すべきである。このリスクは、組織の GRC フレームワークの定義に従って、利害関係者に対して伝達すべきである。また、必要に応じて、是正処置を講じるべきである。

組織において識別されたリスク、不備、その他の課題は、その影響度と重要性について評価し判断すべきである。個別のリスクまたは複数のリスクの組み合わせによって、開示を要する業務上の損失につながる可能性がある場合には、適切に、利害関係者に情報を伝達しなくてはならない。この報告の方法を、GRC の全体的フレームワークにおいて、明確に定義すべきである。

損失の原因と IT リスク

オペレーショナル・リスクは容易に認識できるものであるが、包括的に定義することは難しい。リスク要因は、金融機関業務のあらゆる部分で見出すことができる。損失の可能性は、通常プロフィットセンターあるいは価値貢献部署とは考えられていない部署の業務停止が原因となる場合もある。バーゼル委員会は、オペレーショナル・リスクを、「不適切な、または失敗した内部プロセス、人、システム、あるいは外部事象によって発生する損失のリスク¹⁷」と定義している。この定義には、法務リスクは含まれるが、戦略リスクと風評リスクは含まれていない。特に

¹⁷ Basel Committee on Banking Supervision, “Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework—Comprehensive Version,” June 2006

強調されている点は、リスクは相互依存的でありうるという事実である。これを踏まえ、「システムミック・リスク」、つまり、領域を超えて、あるいは組織を超えて作用するリスクについて考慮すべきである。システムミック・リスクが発生する要因の一つとして、金融機関は、通常、情報技術と情報管理に依存していることに加え、基幹業務のプロセスをサポートするために、複雑なインフラストラクチャを必要としているという事実がある。

IT は、オペレーショナル・リスクの重要な構成要素であり、したがって、オペレーショナル・リスクに対応する所要自己資本の一部を構成する。

オペレーショナル・リスクは、一般的には、その発生原因によって定義されることが多い。これは、原因が事象の分類に関する有効な仕組みとなっているためである。原因には、以下の事項が含まれている。

- プロセッサー企業の業務遂行に起因する損失事象
- 要員－従業員による過失や不正行為に起因する損失事象
- システムサービスの停止や技術的失敗に起因する損失事象
- 外部事象－企業の業務継続能力を脅かす、自然現象あるいは自然現象以外の事象に起因する損失事象

バーゼルⅡの文脈では、定義に関して、厳密な因果関係を示すことが重要である。オペレーショナル・リスク以外の主要なリスクカテゴリーである信用リスクと市場リスクにおいても、明確に識別可能な原因が定義されている。信用リスクに関しては供与された信用であり、市場リスクに関しては参入時の市場におけるポジションである。

銀行が、オペレーショナル・リスクに関する独自の定義を採用する場合でも、その定義は、銀行における重大なオペレーショナル・リスクの全てを考慮したものであり、かつ、業務における重大な損失の可能性に関する、最も重要な原因を含むものでなくてはならない。

原因の種類ごとの分類は、オペレーショナル・リスク管理の出発点、特に、リスクを低減するか、移転するか、または受容するかという検討に利用できる。IT リスクの管理において有用な、より高度な透明性と区分を提供するためには、原因の 4 つの種類について、さらに 3 つのレベルの原因カテゴリーに分類すべきである。これが特に重要なのは、実際のリスクは、しばしば複数の原因によって発生するが、分類は 1 つに決めなくてはならないためである。

この考え方を明確にするための例を、以下に示す。

例1

内部者が、内部 Web アプリケーションのプログラムの誤りを悪用した場合には、その原因を「システム」に分類すべきである。一方、外部からの侵入者がハッキングツールやフィッシング、マルウェアを用いて銀行のコンピュータにアクセスした場合は、「外部事象」に分類すべきである。

例2

データセンターで発生した火災によって、IT システムが損害を受け、ビジネス活動において IT が利用できなくなる場合について考える。バーゼルⅡの原因と損失事象の区分を用いると、原因は「外部事象」に分類され、損失事象は「物理的資産への損害／災害」に分類される。

因果関係を詳しく見ると、このリスク事象の原因は以下のようになる。

外部事象(火災)－災害(データセンター内の火災)－物理的資産への損害(IT システムの破壊)－ビジネス停

止(ビジネスプロセスが実行不可能)

この比較的単純なリスク事象においても、すでに、「物理的資産の損害」、および「ビジネス停止とシステム障害」という2種類のバーゼルⅡの損失事象に関連していることがわかる。この事象が発生した場合、ビジネスの停止そのものは、「システム」に起因するものである。また、もしこの火災が、電気工事者が2つの電源ケーブルを接続し間違えたことが原因で発生したものであった場合、3つ目の原因として、「要員」が追加されるであろう。

あるいは、IT担当者が十分なテストをせずに、また、データをバックアップすることなく、本番環境に新リリースを適用した場合には、一般的には「変更管理」と呼ばれる、システムの本番環境へのリリースの「プロセス」が、4つ目の原因として追加される。

この例は、リスクの連鎖や、その結果として発生した損失の原因となった事象を、種類によって分類し、重み付けを行うことの難しさを浮き彫りにしている。この例によって、発生原因に基づくオペレーショナル・リスクの定義は、情報関連のリスクにも適用すべきことが、さらに明らかとなる。リスクの識別と分類に関する手法を導入している金融機関は、COBITが提供する情報とプロセスを使用して、レベルⅡのリスク分類についても識別すべきである。また、その後で、個々の定性的、定量的なリスク評価を行うことによって、レベルⅢのリスクを識別し、優先順位をつけるべきである。

バーゼル委員会が特定した、重要な損失につながる可能性のある業務上の事象の種類は、以下のとおりである。

- 内部不正
- 外部不正
- 従業員の行動と職場の安全
- 顧客、製品、商慣習
- 物理的資産への損害
- ビジネスの停止およびシステム障害
- 実行、導入、プロセス管理

また、バーゼル委員会は、下位区分および活動例と合わせ、それぞれの損失事象の定義を示している。

原因と損失事象を考慮すると、多くのオペレーショナル・リスクが、火災によるデータセンターの焼失など、ITに直接的に関連する問題、あるいは、アプリケーションプログラムのエラーによる、ビジネスプロセス・コントロール(フォー・アイズ・プリンシプル¹⁸)の停止といった、ITに間接的に関連する問題のいずれかのかたちで、ITに関連していることが分かる。

ITリスクの管理においては、バーゼルⅡの原因と損失事象の種類について、さらに定義を行わなければならない。

オペレーショナル・リスク管理における、オペレーショナル・リスクの識別、測定、モニタリング/コントロールにおいて、バーゼルⅡの定める原因および損失事象では、その範囲が十分でない可能性がある。複数の原因と、その結果として引き起こされる事象は、相互依存的な関係を形成しており、その関係の全てを記述することはできない。その結果、因果関係とその影響を示すために、リスクシナリオを使うことが考えられる。このようなシナリオは、最も一般的なITリスクの種類と組織への影響を示すうえで、利用価値の高いツールである。

¹⁸ フォー・アイズ・プリンシプルとは、すべてのビジネス上の決定や取引には、CEO および CFO の承認が必要であることを意味する。

IT リスクシナリオ分析

バーゼルⅡでは、先進的計測手法(AMA)を採用する金融機関に対しては、非常に重大、かつ不定期に発生する事象に対するエクスポージャを評価する際に、外部データと合わせて、シナリオ分析、および専門家の意見を利用することを求めている。シナリオ分析の手法を用いることによって、経験のあるビジネス管理者とリスク管理の専門家が、協調して、重大な損失の可能性に関する合理的な評価を行うことができる。

オペレーショナル・リスク管理や情報リスク管理の手法において、内部監査やITコンプライアンスを担当する、経験豊富なIT実務者、情報セキュリティ専門家、ビジネス管理者、リスク管理専門家、内部監査やITコンプライアンス部門のIT専門家は、ITシナリオに関して、発生の可能性と、その重大な損失をもたらす合理的な可能性について、互いに議論すべきである。

図表9のITシナリオは、その例と考えることができるものであり、重要性の観点からAとBとに分類されている。この分類は、特定のITシナリオに関する、金融業界における相対的な重要性を示している。

シナリオ分析を実施するにあたっては、リスク要因の発生頻度と重要度を考慮すべきである。これは、この分析が、詳細な統計的損失分布に関して、専門家による、十分な根拠に基づいた分析を行うことを目的としているためである。専門家の評価において、業務上の損失データが利用できない場合には、過去の経験や市場の慣習に基づく推定や予想によって代替することもできる。

図表9-ITシナリオ		
ITシナリオの例	シナリオの内容	カテゴリー
承認されたユーザによる、未承認の行為	アクセス権のあるユーザが、修正機能、ソフトウェアやシステムの不正操作、アプリケーションデータの変更、アクセス権限管理の回避、または入力データの不正操作などの機能を不適切に使用する。	A
サービスの中断	ハードウェア/ソフトウェアの障害、重要なサービスや基盤システムの停止、重要なデータの損失、サービス拒否(DOS)、キャパシティ計画の誤りが発生する。	A
不完全なトランザクション処理	エラーや不完全なトランザクションの処理が検知されず、誤った処理が行われる。	A
機密性を有する資産の悪用	承認されたアクセス権を持つ者が、アクセス権を悪用する。	A
プロジェクトの失敗	プロジェクトが、合意された期間内に、予算内で、適切な品質をもって完了されない。	A
製品の失敗	セキュリティに関する要件定義の失敗、あるいは製品選択、導入時のセキュリティ設計の不備。	B
外部委託リスク	外部委託業者のサービスを利用することに関するリスクの定義が不十分、あるいは管理が不適切。	B
機密性を有する資産、あるいは重要な	ハードウェア/ソフトウェア、デバイス、システム出力、データファイル、ノートPC、モバイル機器等が	B

資産の盗難	盗まれる。	
悪意のある活動	ハッキング、フィッシング、ソーシャルエンジニアリング、またはサイバー恐喝の被害にあう。	B
プロセスの失敗	機密性を有するビジネスプロセスにおいて、十分なセキュリティが確保されない。	B

図表 10 では、カテゴリーA に分類された IT シナリオに関する、リスク要因を例示している。

シナリオ分析では、複数のシナリオの相互関係について、考慮することが求められる。これは、1 つ以上のリスクに起因し、複数かつ同時に発生する業務上の損失事象によって発生する損失の可能性を特定し、評価するうえで不可欠だからである。シナリオでは、情報に関連するリスクの相対的重要性を評価するために、内部の損失データについて検討すべきである。また、利用可能な場合、市場データやその他の過去データに対するシナリオの妥当性を確認するために、外部の損失データについて検討すべきである。

専門家の意見に基づくシナリオ分析とリスク評価を行う場合は、長期にわたって使用可能な実損失データと比較することによって、頻繁にその正当性を確認し再評価すべきである。これは、リスク管理に適用する定性的手法の妥当性を確保するうえで、必要な措置である。

図表 10—カテゴリーA の IT シナリオに関するリスク要因の例

IT シナリオ	発生頻度に関するリスク要因	影響度に関するリスク要因
承認されたユーザによる、未承認の活動	<ul style="list-style-type: none"> 機密性を有するアプリケーション機能へのアクセス権を持つユーザ 管理者による統制の不足 アクセス許可の不適切な定義 管理者権限の濫用 ソフトウェアやシステムへの不適切なアクセス 	<ul style="list-style-type: none"> システムから出力される例外レポートの不適切なモニタリング マネジメントによる統制の不足 監査によるレビューの不足 不適切なセキュリティポリシー セキュリティ意識向上のための適切な教育の欠如 説明責任の不足 不適切なアクセス管理
サービスの中断	<ul style="list-style-type: none"> サービス中断の原因になり得る、損害を与える可能性のあるインシデントの数 損害に対するハードウェアとソフトウェアの脆弱性 システムとアプリケーションとの相互依存関係の特定の失敗 	<ul style="list-style-type: none"> サービス中断につながる可能性がある状況とその影響を正確に特定する能力の不足 サービス中断につながる可能性がある事象に対するモニタリングの失敗 インシデントの検知および報告に関する手順の策定と導入の失敗
不完全なトランザクション処理	<ul style="list-style-type: none"> 処理エラーが検知されない可能性 	<ul style="list-style-type: none"> 不完全な処理によって、深刻な損害が生じる可能性
機密性を有する資産の	<ul style="list-style-type: none"> 共有IDまたはグループアカウントの数 機密情報を扱うアプリケーション、またはアプリ 	<ul style="list-style-type: none"> モニタリングツールの不足、または一貫性のないツールの使用

悪用	<ul style="list-style-type: none"> リケーション機能へのアクセス権を持つユーザの数 ・ 包括的なセキュリティポリシー、手順、標準の不足 ・ セキュリティ意識向上のための教育の失敗 ・ 管理者によるモニタリングと是正の不足 ・ ビジネス手順とプロセスを定義する際のセキュリティの考慮の不足 	<ul style="list-style-type: none"> ・ セキュリティ事故への対応能力の不足
プロジェクトの失敗	<ul style="list-style-type: none"> ・ プロジェクトの数 ・ プログラム/プロジェクトに関して定義されている管理手順の品質 	<ul style="list-style-type: none"> ・ プロジェクト予算 ・ 重要なプロジェクトの数

7. 業務プロセスから IT リスク、IT 統制へ: COBIT フレームワークの適用

バーゼル委員会は、オペレーショナル・リスクの測定と管理に関して、ビジネスラインを考慮した手法を推奨している。標準的手法では、ビジネスラインごとの総収益が、ビジネスオペレーションの規模を計る一般的な指標であり、また、ビジネスラインごとのオペレーショナル・リスクのエクスポージャーを示す尺度と考えられている。

既存文書の利用

ほとんどの金融機関には、業務プロセスを記述した、次のような文書が存在している。

- 方針と手続(特に監督当局から要請され、コンプライアンス部門により更新されている場合)
- 業務プロセスの見直しに関する文書
- 財務報告に関するコンプライアンス文書(例えば、サーベンス・オクスリー法)

このような文書は、オペレーショナル・リスク分析を開始する際に、その基礎として利用できることが多い。例えば、財務報告にかかわるキー・コントロールの特定を目的としているが、サーベンス・オクスリー法やその他の財務報告のためのコンプライアンス文書が作成されている場合がある。トレーディングのプロセスでは、一般的には、バックオフィスにおけるマッチングおよび照合プロセスがキー・コントロールである。フロント・システムのコントロールが、この対象となることは通常考えにくい。しかし、オペレーショナル・リスク管理の観点では、フロント・システムが重要である。例えば、顧客ごとの取引制限、トレーディング戦略(特に、トレーディング戦略を決定する際のリスク選好の評価)、セキュリティおよびプログラム変更管理は全て、オペレーショナル・リスクの評価において重要である。

バーゼルⅡにおけるビジネスライン・アプローチ

金融機関は、ビジネスラインの観点に加え、システム部門など、2つ以上のビジネスラインをまたいで活動する集中化された部門(IT部門など)におけるリスクを管理しなくてはならない。最終的に、バーゼル委員会は、銀行における全ての活動を、以下の8つのビジネスラインのいずれかに関連付けることを求めている。

- コーポレート・ファイナンス
- トレーディングとセールス業務
- リテール銀行業務
- 商業銀行業務
- 支払・決済業務
- エージェンシー・サービス
- アセットマネジメント業務
- リテール仲介業務

ほとんどのビジネスラインは、IT なしでは業務を遂行することができない。もちろん、IT を必要とする程度は、業務によって異なっている。リテール顧客に対して、電子バンキング機能を提供するリテール仲介業務では、常時利用可能でなければならない複雑な IT システムが必要であることは明らかである。一方、コーポレート・ファイナンス業務においては、新商品開発や、個別取引のためのモデルやソフトウェアベースのシナリオを迅速に開発する能力といった、全く異なる能力が必要とされる。

オペレーショナル・リスクのエクスポージャーは、重要な全ての商品、活動、プロセス、およびシステムにおける固有のオペレーショナル・リスクを認識し、評価することによって明らかにすべきである。銀行は、大きな問題となる可能性があるリスクの識別に加えて、リスクに対する脆弱性を評価する必要がある。この評価は、各ビジネスラインにおけるプロセスの体系的、かつ詳細な分析に基づいて行われる。商品やサービスを外部の顧客へ提供するプロセスは収入と収益の源であるので、この評価は商品に関連するプロセスから開始するのが通常適している。

金融機関は、リテール仲介業務では、リテール顧客に対して、取引所での株式の購入などのサービスを提供する。このサービスを利用するためには、顧客は、インターネットを利用したアプリケーションに注文を入力しなければならない。注文が承認された後に、銀行が注文を処理し、取引所で取引が実行され、顧客に決済内容が送信される。同時に顧客のポートフォリオに、購入した株式が追加され、顧客の口座から代金が引き落とされる。処理が行なわれる前に、顧客の本人確認が行われ、その顧客が、指示した取引を実行する権限を持っているかどうか、顧客情報でチェックされる。この一連のプロセスは、中核となるアプリケーションだけでなく、価格情報や取引所における決済を提供する、金融機関内外の複数の IT システムによって提供されている。

このようなプロセスにおいて、固有リスクのエクスポージャーを評価する方法の1つとして、リスクシナリオを適用できる。リテール仲介業務における認証情報の盗難などのシナリオは、プロセスの要点を詳細に知ることによって、かなり正確に評価することが可能である。ただし、金融機関全体に関連するシナリオは、一定の確度をもって評価することは難しい。

オペレーショナル・リスクの様々なシナリオにおける典型的なリスク要因は、業務プロセスで実施されている統制によって、発生頻度や、影響の拡大が抑止されている。想定されるシナリオの影響度を評価する際には、内部あるいは外部の損失データなどに加え、リスクを低減する統制についても考慮する必要がある。

IT リスクの定義

COBIT は、リスク評価で使用するシナリオを設計、構築する際に、検討中のシナリオにおける標準的な統制環境を定義するための参考となる、適用可能な統制プロセスを提供している。

図表11はカテゴリーA の IT シナリオと、統制目標との対応例を示している。

図表 11－COBIT のプロセスに対する IT シナリオの関係の例	
IT シナリオ	COBIT プロセス
承認されたユーザによる、未承認の行為	DS5 システムセキュリティの保証
サービスの中断	DS4 継続的なサービスの保証
不完全なトランザクション処理	AC4 処理のインテグリティと正当性
機密性を有する資産の悪用	DS5 システムセキュリティの保証
プロジェクトの失敗	PO10 プロジェクト管理

上位のリスク評価では、組織が全社レベルおよびプロセスレベルの統制で構成された、十分な統制環境を導入しているかどうか検討すべきである。全社レベルの統制には、通常、次の COSO の構成要素が組み込まれている。

- 統制環境
- リスク評価

- 情報と伝達
- モニタリング(一部)

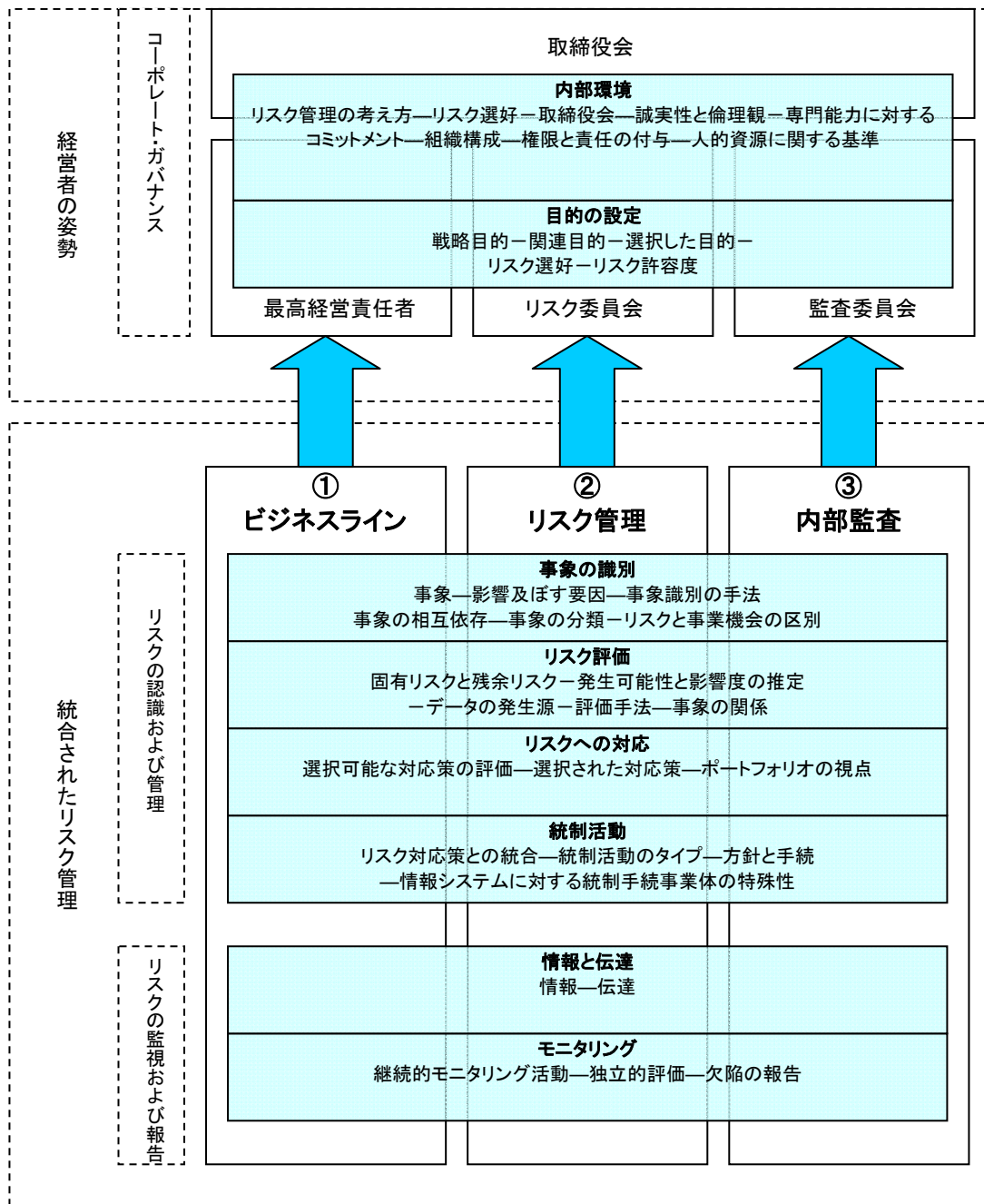
全社レベルの統制の一部には、複数の防御階層と各階層における責任という考え方を含む場合がある。多くの会社では、リスク管理者を任命しているが、その経験、勤続年数、および役職に大きな違いがある。ある組織では、リスク管理者は上位の役職として位置づけられており、決定に異議を唱えることや、契約条項の確認などに関する、詳細な評価を行う権限が与えられている。その一方、リスク管理部門の本質的な要件である、決定に異議を唱える権限は与えられず、基本的なリスク評価を行う役割に限定されている組織もある。

コンプライアンス、内部監査、リスク管理の各機能を体系化するために、3段階ラインによる企業防衛モデル(図表 12 参照)に沿って体制を構築した組織もある¹⁹。この防衛モデルでは、リスク管理は第2段階の防衛ラインとして独立したチェックを行う。また、監査は、第1、第2段階の防衛ラインが意図したとおりに機能していることについての保証を提供する。

リスクベースおよび原則に基づく監督の進展の中で、規制へのコンプライアンスは、組織の統合的 ERM フレームワークの成果として明らかになってきた。信用リスク、金利リスク、流動性リスク、およびオペレーショナル・リスクを含む、全てのリスク管理の規律に関する効果的なガバナンスは、図表 12 で示した COSO ERM のフレームワークに基づいた、3段階ラインの企業防衛モデルの能力成熟度に強く依存するものとなる。

¹⁹ 3段階ラインによる企業防衛モデルは多くの金融サービス業者で既に採用されている。(National Australia Bank の 2006 Annual Financial Report (ページ 15: Risk Management :Introduction) にあるモデルを参照)

図表 12 —企業防衛モデル： ERM フレームワーク



統制は、図表 13 で示されているように、統合的な ERM において重要な機能を持つ、明確に定義され、独立した防衛ライン(ビジネスライン、リスク管理、内部監査)によって実施されなければならない。3 段階ラインによる防衛モデルは、リスクに責任を負い管理する機能、リスクを監視する機能、および独立した保証を提供する機能に区分される。

- 取締役会は、組織のリスク選好を設定し、リスク管理の戦略を承認し、組織の内部統制システムに関する最終的な責任を負う。²⁰経営陣の支援を受けた CEO は、組織のリスク管理に関する全般的な責任を負う。各業務を遂行する管理者や要員は、管理対象のリスクに対する第一義的な責任を負う。管理者や要員には、自らの業務において生じる全社的なリスクの認識、評価、管理、モニタリング、そして報告に関する責任を負う

²⁰ 取締役会は、次の事項に関する責任を負うべきである。銀行の全般的なビジネス戦略および重要なポリシーの承認と定期的なレビューに関する責任。銀行における主要なリスクについて理解し、リスクの許容水準を定義し、経営陣が、リスクの識別、測定、監視、およびコントロールするのに必要な対応を行うことを確実にすること。組織の構成を承認すること。経営陣が、内部統制システムの有効性を確実に監視するようにすること。なお、取締役会は、最終的には十分で有効性の高い内部統制システムの構築と維持に関する責任を負うべきである。

出展「Basel Committee on Banking Supervision, Principle 1, Framework for Internal Control Systems in Banking Organisations」

ことが要求される。

- リスク主管部門によって支援される最高リスク管理責任者は、第2段階の防衛ラインに責任を負う。また、リスク委員会、および最終的には取締役会に対する説明責任を負う。日常のリスク管理の責任は、最高リスク管理責任者ではなく、第1段階の防衛ラインにある。リスク管理部門は、通常、次の業務を行う。

一経営陣に、リスク管理方針の承認を求める。客観的な監督を行う。他の専門家やリスク関連の主管部署と協力して、ERM活動を調整する。

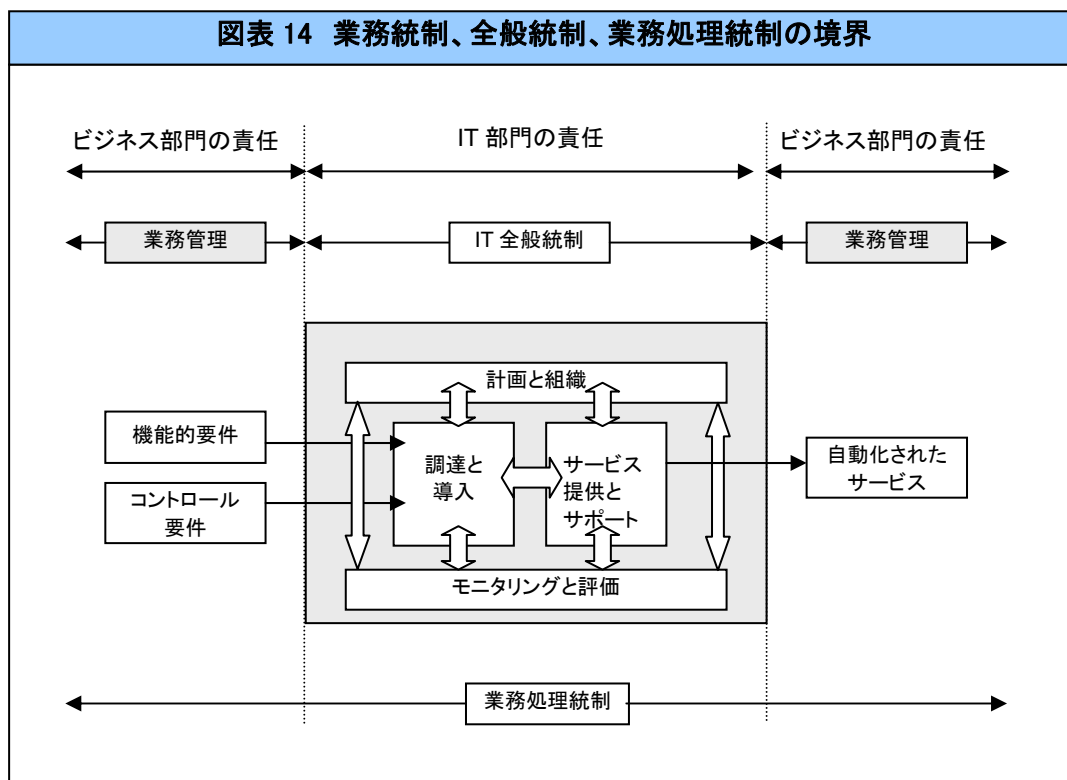
図表 13 3段階ラインの概念	
第1ライン	業務目標、方針、規則、および社内基準に合致した、リスク管理活動
第2ライン	業務目標、方針、規則、および社内基準を支援、あるいは異議を唱えるための、客観的なリスク分析と報告
第3ライン	第1、第2ラインにおいて、業務目標、方針、規則、および社内基準に合致して業務が行われていることの確信

一業務部門のマネジメントに対して、リスクの認識、評価、管理、モニタリング、および報告に関する、全般的かつ専門的な支援や助言を行なう。

- 第3段階の防衛ラインである内部監査は、組織全体にわたる全社的リスク管理の有効性に関して、独立した保証を提供する。内部監査部門は、監査委員会、そして最終的には取締役会に対する説明責任を負う。

IT 統制の定義

リスクは、組織全体の視点から、定義され評価される必要があり、さらに詳細に、プロセスレベルでの検討が行われる。統制の導入は、全社的な視点を経て全般的な統制へ、さらに個別で詳細なプロセス統制へと展開する。図表 14 は、この関係を、業務と IT の両方に関連する、全般的な業務プロセスの観点から図示したものである。



全社レベルの統制

COBIT は、金融機関に対して、全社レベルの統制に関する、戦略的な視点を持った、総合的な一連の統制目標を提供している。この統制目標は、組織が置かれた環境に応じて検討するべきであり、その事業優先度によって、GRC に関する戦略的観点が決定される。経営陣は、良好なコーポレート・ガバナンスを確立するためのさまざまなモデルを選択することができるが、COBIT のフレームワークを適切に適用すべきである。事例についての質問は、全社レベルの統制に関する、全般的で高いレベルでの理解を得るのに有用であろう。その一方で、全社レベルの統制に関する合理的な保証を得るために、必要となる統制の目標について、対象と範囲を決定するのは、管理者、オペレーショナル・リスクおよび情報リスクの専門家の責任である。

IT 全般統制

バーゼル II のリスク事象の種類に関連する統制目標は、「付録 V バーゼル II と COBIT」に記載されている。IT 全般統制は、一般的に、プロセスレベルとアプリケーションレベルの統制を実現するために整理された統制目標である。COBIT では、IT 全般統制について、アプリケーションに特有のものから、組織全体に適用可能なものまで、200 以上の統制目標を定義している。例えば、アプリケーションに対するアクセスコントロールのフレームワークなど、IT 全般統制の個別の項目では、業務のワークフローにおける、より詳細な統制について説明している。ワークフローにおけるキー・コントロールは、IT 全般統制によって定められた原則や範囲に従わなければならない。したがって、業務トランザクションにおけるデータの生成や変更に関する個別のアクセス制限は、アクセスコントロールのフレームワークに基づく方針に従わなければならない。

全般統制として実施されたキー・コントロールは、全般統制そのものの有効性を支えるものである。アクセスコントロールのシナリオでは、キー・コントロールがワークフローに組み込まれているという事実によって、アクセスコントロールのフレームワーク(全般統制)がそのワークフローに対して、一貫して適用されていることが裏付けられる。逆に、アクセスコントロールのフレームワークが完全には導入されていない場合、ワークフローレベルのアクセスコントロールには、ギャップが存在することになる。

プロセスレベル統制

プロセスレベル統制は、多くの場合、業務処理統制に相当する。銀行の業務プロセスは、ITアプリケーションに強く結び付けられており、業務プロセスにおける統制は、その業務プロセスで利用されるITアプリケーションによって実施されている。例えば、リテール証券業務において、誤った売りを行ってしまうリスクは、ITアプリケーションに入力されたデータの妥当性をチェックする機能を提供する、IT業務処理統制によって低減される。

ITアプリケーションは、IT全般統制によって管理されており、ITアプリケーションが業務仕様書に基づき開発、運用されていることや、ユーザに対して、業務に応じて定められているアクセスのみが許可されていることを保証する。

さらに、金融機関は、CobiTの統制目標を、必要不可欠な全般統制と業務処理統制の定義、および導入された統制の成熟度評価に利用することもできる。またCobiTは、6つの業務処理統制目標を推奨している。この業務処理統制目標は、業務処理統制番号(AC)で区分されている。

- AC1 ソースデータの準備と許可—原始帳票が、定められた手続に従い、該当文書の作成と承認に関する職務分離を十分に考慮した上で、許可を受けた資格のある要員によって準備されていることを確認する。入力ミスや入力漏れは、効果的な入力フォームを作成することで最小限に抑えることができる。入力ミスや不正データを検出して、報告、訂正できるようにする。
- AC2 ソースデータの収集と入力—データ入力は、許可を受けた資格のある要員によってタイムリーに実施されるように定める。誤入力されたデータの訂正と再送信は、元のトランザクションの許可レベルを損なうことのないように実施する。元の原始文書は、復元時に必要となる場合に備えて、一定期間にわたって保存しておくようにする。
- AC3 正確性、網羅性、および真正性のチェック—トランザクションの正確性、網羅性、および妥当性を検証する。入力したデータを確認し、可能な限り原本に近づけて編集する、または修正を求めるようにする。
- AC4 処理のインテグリティと妥当性—処理サイクルを通じて、データのインテグリティと妥当性を維持する。誤りのあるトランザクションが検出されても、有効なトランザクションの処理が中断されないようにする。
- AC5 出力のレビュー、調整、およびエラー処理—出力は、許可された方法によって扱われ、適切な受領者に送付され、送信中に保護されるように、手続とこれに伴う責任を定める。出力の正確性について検証、検出、修正を行い、また、出力から得られる情報を利用できるように、手続とこれに伴う責任を定める。
- AC6 トランザクションの認証とインテグリティ—内部アプリケーションとビジネス機能/運用上の機能(企業の内外を問わず)の間でトランザクションデータをやり取りする前に、宛名が正しいかどうか、送信元の真正性、および内容のインテグリティをチェックする。送信または移送の間の真正性とインテグリティを維持する。

8. 主要 IT リスク指標の使用

リスク指標は、オペレーショナル・リスクのエクスポージャー、およびリスク・プロファイルの変動を把握するためのパラメータである。したがって、リスク指標は、オペレーショナル・リスクのリスク・プロファイルに関する早期警告システムのひとつである。リスク指標は、将来に関する見通しを提供することによって、経営陣が、リスクの傾向について文書化し分析することを可能とし、また、リスクによる損失が実現する前に、対応の必要があることを警告する。さらに、リスク指標は、リスクの許容範囲を定義することによって、リスク選好の定義を容易にする。したがって、主要リスク指標 (KRIs) は、経営陣の介入が必要な部分を単に示すというよりも、リスクの測定およびモニタリングプロセスの一部となるべきである。

主要リスク指標は、リスクの把握に特に適した指標、あるいは特に重要なリスクを把握するための指標のことである。主要リスク指標は、オペレーショナル・リスクの管理に使用され、報告の段階で重要な役割を果たす。

主要リスク指標を使用することによって、IT の欠陥や脆弱性が原因となる、業務上の損失の可能性を明らかにすることができる場合がある。業務上の損失可能性の中には、自己資本賦課の変更を必要とする可能性があるものや、最悪の場合、組織が、より高度なアプローチを採用することを妨げるものを含む可能性がある。

銀行業界では、主要リスク指標のライブラリーの開発を、Risk Management Association (RMA)²¹が進めてきた。このライブラリーは、リスク指標を定義するプロセスで利用することができる。

リスク指標を特定するための別の情報源として、CoBIT が提供する評価指標がある。CoBIT の評価指標は、パフォーマンスの要因と結果の測定に重点を置いたものであるが、プロセスを測定するための広く認められた手法であり、リスク指標を識別する基礎として活用することができる。

CoBIT のプロセス DS4、「継続的なサービスの保証」に基づく、主要リスク指標の例を図表 15 に示す。このプロセスは、IT の達成目標、IT プロセス、およびアクティビティへの寄与という、3 つのレベルで測定される。

この評価基準は、リスク指標として利用でき、CoBIT が推奨する評価基準の構造を保つ優れた方法である。さらに、成熟度の水準は、リスク低減の水準と相互に関係することから、重要な IT プロセスに関する成熟度は、リスク指標としても利用できる。

図表 15 DS4 評価指標	
評価対象	評価指標
IT 達成目標	<ul style="list-style-type: none"> ・ 予定外の機能停止に起因する、1 ユーザあたりの損失時間数(1 カ月)
IT プロセス DS4	<ul style="list-style-type: none"> ・ サービスレベルアグリーメント(SLA)に定められた要件を満たす可用性の割合 ・ IT 継続計画でカバーされていない IT に依存している重要な業務プロセスの数 ・ 復旧目標を達成したテストの割合 ・ 重要なシステムのサービス中断発生頻度
アクティビティ	<ul style="list-style-type: none"> ・ IT 継続計画の特定要素のテスト間隔

²¹ www.kriex.org

	<ul style="list-style-type: none">・ IT 部門の当該従業員 1 人あたりの、IT 継続計画に関する年間の訓練時間・ 自動化された可用性モニタリングを行っている重要インフラストラクチャの割合・ IT 継続計画のレビュー実施頻度
--	--

付録 I – バーゼル II の概要

1930年に設立された国際決済銀行(BIS)は、バーゼル銀行監督委員会を通じて、金融機関の管理体制に関する国際的な健全性基準を設けた。この基準は、各国において、法令²²、および監督当局の規則に反映されている。

バーゼル II の新しい自己資本比率規制(改訂フレームワーク)は、金融業界の過去数十年間の歴史の中で、最も重要な規制改訂の1つである。第一次見直し案による検討が1998年に開始され、2004年6月のバーゼル委員会で最終的にフレームワークとしてまとめられた。新しい規制は、金融監督の重要な第一歩であり、また、国際業務を行う銀行にとって、大きな変化のきっかけとなるであろう。各国の銀行監督当局は、2006年以降、段階的なアプローチを経て、バーゼル II の要件を実現させることを予定している。また、いくつかの国では、バーゼル II の要件が完全に実施される2015年まで、取り組みが続けられるであろう。この取り組みを主導しているヨーロッパの監督当局および銀行は、2008年までに適合を完了するだろうと多くの人が予想している。

1988年の自己資本規制のフレームワークは、現代のリスク管理手法に適合しておらず、またオペレーショナル・リスクに対応していないが、バーゼル II は、これを置き換えるものである。バーゼル II の目的は、信用リスクとオペレーショナル・リスクに関して、より強力なリスク管理手法の採用を促し、銀行の金融リスクと所要自己資本との関連性を強化することにある。新しい規制では、高度なリスク管理システムの採用に関して、所要自己資本の緩和措置など、銀行が規制対応への取り組みを進めるインセンティブを提供している。結果的に、慎重なリスク管理は、市場における競争優位性を与えるものである。さらに、自己資本比率規制は、市場の発展とリスク管理の向上の進展に、歩調を合わせるべきものである。

委員会によれば、バーゼル II の規制は、以下の事項を意図するものである。

- 国際銀行システムの健全性と安定性の強化、および現状水準での資本の維持
- 全てのリスクに対するより包括的な対応
- 銀行が保有するポジションと、その他の取引がもたらすリスクに対応した適切な資本の維持
- 複雑性とリスク選好の違いにかかわらず、全ての銀行に対して適用可能

最も重要な変更として、次の事項が挙げられる。

- 規制は、銀行単体ではなく、連結グループ全体に適用されること
- 銀行の内部格付手法に基づく自己資本比率の計算が可能であること
- 担保とのネットティングによって、信用リスクの削減の可能性が増すこと
- 自己資本比率の決定において、オペレーショナルリスクの水準が認識されること

さらに、銀行のリスク評価システムに対する監督当局による検証の基準が示され、その中で銀行との広範囲にわたる定期的なコンタクトが求められている。また、市場規律の強化を目的として、情報開示の要件が拡大されている。

²² ヨーロッパでは、基準は当初、EU 指令として EU レベルで適用されている。

この規制は、最低所要自己資本を主な目的としており、これは、商業銀行に対して、最も強い影響を与えるものである。また、新しい規制は、これまでの規制と比較して、より複雑である。しかし、この規制は、金融機関におけるさまざまなビジネスの発展と信用リスク管理の進歩と関連している。

金融機関は、信用、市場およびオペレーショナル・リスクに対する所要自己資本を監視するために、自社の業務にもっとも適した手法を選択することが認められている。この選択においては、金融機関ごとに異なるリスク・コントロールとリスク管理の状況を考慮すべきである。一般的に、リスク評価とそれに基づく所要自己資本は、より複雑になり、リスクの影響を受けやすいものとなっている。また、適用の条件として、より厳しい定性的、定量的な基準を満たす必要がある。所要自己資本に関する要件の緩和は、より先進的な手法を導入し、金融機関のリスク管理システムを発展、改善するためのインセンティブとして提供されている。

新しいフレームワークは、1988年の自己資本比率規制の主な内容を踏襲している。これには、銀行に対する一般的要件である、リスクアセットに対する最低8%の自己資本の保有、市場リスクの取り扱いに関する1996年の「市場リスクに関する改定」の基本構造、ならびに適格とされる自己資本の定義などが含まれる。

新しいフレームワークの3つの柱²³

リスクアセットに対する資本の適正化だけでは、金融市場を安定させるのに十分ではない。金融機関は、リスクによる損失を、継続的に、特定、管理、吸収することができなければならない。このために、先進的なリスク管理システムを導入し、継続的なプロセスとしてさらに発展させることが必要となる。充実した内部リスク管理システムを導入している金融機関は、その健全性と正確性に関する監督当局による承認を前提として、所要自己資本を削減することができる。この考え方に基づいて、監督当局は、金融機関の監督について、定量的な手法から定性的モデルへと移行しつつある。監督上の検証は新しいフレームワークの第二の柱と考えられている。

市場規律が他の2つの柱を効果的に補完することを確実にするうえで、開示要件の拡大は不可欠である。

第一の柱：最低所要自己資本

バーゼルⅡでは、最低所要自己資本はリスクアセットに対して最低8%と決められており、この割合自体はこれまでの規制から変更されていない。総リスクアセットは、市場リスクおよびオペレーショナル・リスクに対する所要自己資本を12.5倍したものに、信用リスクに関するリスクアセットの合計を加算したものである。

主に、信用リスクとオペレーショナル・リスクの評価方法が変更されているが、監督を目的とする総自己資本の定義、および総市場リスクの計算方法は変更されていない。

信用リスク

バーゼル委員会は、図表16に示すとおり、所要自己資本について、リスクウェイトに基づく手法を採用している。対象となる金融機関は、信用リスクに対する所要自己資本の計算において、標準的手法(通常、より多くの所要自己資本につながる)、もしくは内部モデル(通常、より少ない所要自己資本につながる)のいずれかを選択できる。内部モデルの使用は、監督当局が定める基準を満たしている場合に、監督当局が承認する。

標準的手法²⁴

²³ 以下の文章は、2004年6月にバーゼル銀行監督委員会が公表した、バーゼルⅡフレームワークに基づいている。

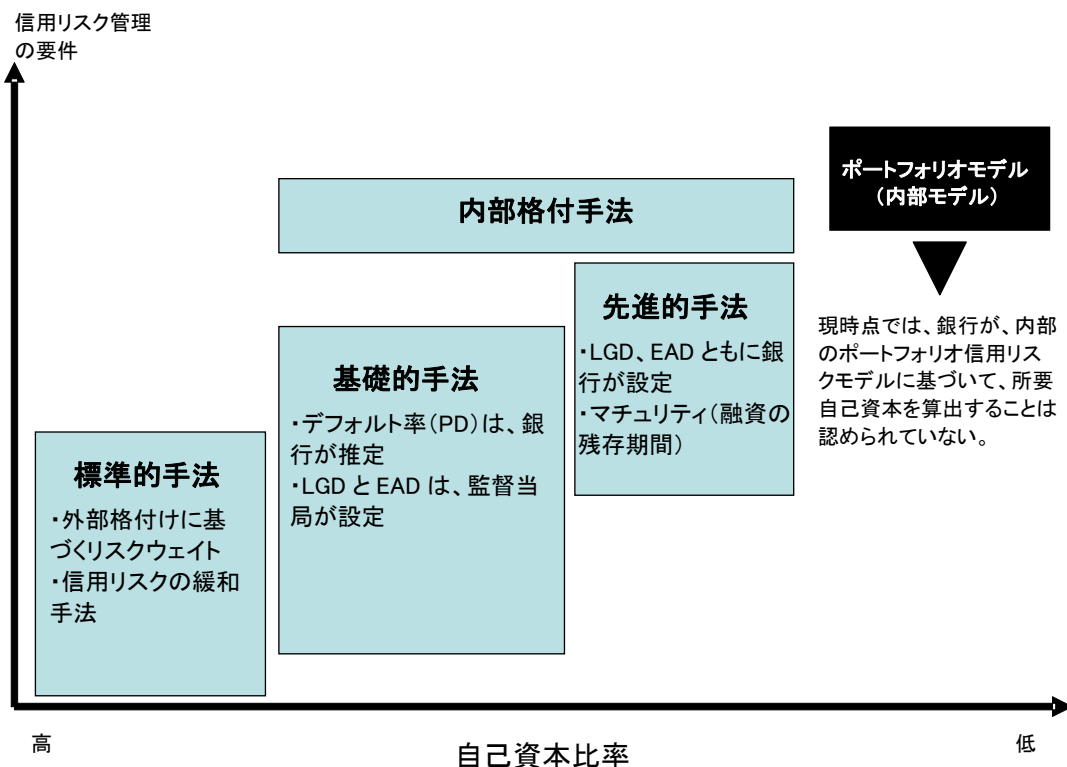
バーゼルⅡでは、信用リスクに関して、リスクウェイトを引き続き使用する。しかし、リスクウェイトは、Standard & Poor'sやMoody'sなどの外部信用評価機関(ECAI)の格付けに基づいて調整すべきである。リスクウェイトの決定にあたって使用する、政府、金融機関、企業に対する貸付及び貸付債権の証券化商品の格付けは、各国の監督当局が選定、承認しているECAIが付与したものでなくてはならない。

今回初めて、資産担保証券(ABS)の取り扱いが、一般規則に追加された。金融機関が、証券化を間接的に支援する(銀行が、投資家として行動する)場合、金融機関は、ECAIの格付けに見合った自己資本を保持している必要がある。原資産の所有者としての金融機関は、証券化に含まれる直接または間接の信用リスクの大きさに応じて、所要自己資本を減少することができる。

例えば、担保、ワラント債、クレジットデリバティブおよびネットィング契約等の信用リスクを最小化する方法は、リスク水準の決定において、さらに重要なものとなってきた。担保として認められている範囲は、拡大している。新しい規制では、将来起こる可能性がある市場価格の変動に応じた、担保の調整が要求されている。

²⁴ IT リスクは、標準的手法を採用した場合は、所要自己資本には影響しない。

図表 16 信用リスク計測の3つの手法



内部格付手法 (IRB)

標準的手法と比較して、内部格付手法は、銀行が抱える個別のリスクの状況をより適切に考慮するものであり、リスクウェイトに基づく所要自己資本という目的に、さらに近づくものである。監督当局が設定する最低基準を満たすことを条件として、金融機関は、所与のエクスポージャーに対する所要自己資本を決定する際に、各行独自の内部格付モデルとリスク構成要素の推計値を使用することができる。

金融機関は、銀行勘定に関連するエクスポージャーを、その元となるリスクの性質の違いによって、11の区分に分類しなければならない。その中で、資産については、企業、政府、銀行、リテールおよびエクイティに区分されている。これらの区分において、リスク構成要素は、それぞれ格付けに基づく個別のリスクパラメータに関連付けられている。

内部格付手法のフレームワークにおける、それぞれの資産区分に対して、リスクウェイトごとに異なる規制が定められている。基本的には、金融機関は、次のいずれかの手法を選択することができる。

- 簡便な、基礎的手法
- より広範囲に組織の内部格付モデルを受け入れ、リスク構成要素を推計する先進的手法

内部格付手法には、以下のリスク構成要素が織り込まれている。

- デフォルト率 (PD) – 銀行は、内部格付に基づいて、債務者を定められたリスク区分のいずれかに分類する。また、リスク区分ごとに、一年以内にデフォルトが発生する可能性を推計しなければならない。
- デフォルト時与信額 (EAD) – 与信枠が設定されている場合、特定日における枠の利用について決定する必要はない。EADとは、デフォルト時の貸付残高の推計値を指す。
- デフォルト時損失率 (LGD) – デフォルトが発生した場合、金融機関の損失は、担保および債務者資産の売却からの回収額によって決まる。LGDは、信用デフォルト発生時の純損失額全体の推計値を表す。
- 実効マチュリティ (M) – 実効マチュリティは、取引相手による義務履行までの最長の残存期間であり、内部格付手法においてリスク要因とみなされる。与信期間が長いほど、債務不履行リスクが高いと評価される。

できるだけ多くの金融機関が内部格付モデルを採用できるよう、次のいずれかの内部格付手法を選択することができる。

- 簡便な基礎的手法は、格付け区分別の損失の推計 (PD) のみに基づいている。その他のリスク構成要素 (EAD、LGDおよびM) は、監督当局が決定する。担保、保証、クレジットデリバティブおよびネットティング契約は、標準的手法と同様に取り扱われる。
- 先進的手法においては、金融機関は実効マチュリティを算出し、各リスク構成要素を独自に推計しなければならない。先進的手法を採用する金融機関は、広範囲に及ぶ履歴データを保持していること、および先進的手法に関する最低基準を満たすことが求められる。オフバランスのエクスポージャーを除き、信用担保や保証に関しては、制限が適用されない。

これらの推計は、信用ポートフォリオモデルにおける信用に関する指標に一致する、数学的関数に基づくも

のである。

内部格付手法の採用について監督当局の承認を得るためには、金融機関は、質の高い格付システム、第三の柱で示された広範囲の情報開示の実施などの最低基準を満たさなければならない。この基準を満たすことによって、組織内部のリスク評価システムのインテグリティを確保することが意図されている。

それぞれの顧客に割り当てられる格付区分と、これに基づいて算出される定量的情報は、リスク評価システム、リスク管理、価値設定ならびにリスク規定において不可欠の部分である。もちろん、この情報は、自己資本の適切性を評価するために利用される。前述の要件に加え、金融機関は、内部格付モデルに基づくストレステストを実施しなければならない。このテストでは、緩やかな景気後退のシナリオについて考慮すべきである。

市場リスク

市場リスクは、金利、株価もしくは外国為替など、市場価値の変化によって生じる損失のリスクである。市場リスクの測定方法や考え方は、基本的にバーゼルⅡでも変わっておらず、新しい規制において、従来以上の議論は行われていない。

オペレーショナル・リスク²⁵

前述のとおり、バーゼル委員会は、オペレーショナル・リスクについて、「オペレーショナル・リスクは、不適切な、または失敗した内部プロセス、人、システム、あるいは外部事象によって発生する損失のリスクと定義される。」と定義している。

この定義は、法務リスクを含んでいるが、戦略リスクおよび風評リスクは含まれていない。現在、オペレーショナル・リスクに対しては、8%の所要自己資本の対象となっている。オペレーショナル・リスクの量を評価するために、金融機関は、いくつかの手法の中から選んで採用することができる。

基礎的手法(BIA)

基礎的手法を採用する銀行は、過去3年のプラスの年間粗利益の平均に対する一定割合(α)を、オペレーショナル・リスクに対する資本として保持しなければならない。年間粗利益の合計は、エクスポージャ指標(EI)として使用される。EIは、想定されるオペレーショナル・リスクの指標として使用され、金利差益、手数料差益、取引差益、金融資産差益、およびその他の収益の合計から計算される。この大まかな手法は、主に、オペレーショナル・リスク管理システムを持たない、小規模な金融機関で使用されると考えられる。バーゼル委員会は、国際業務を行う金融機関は、少なくとも標準的手法を使用するものと予想している。

標準的手法(STA)

標準的手法は、基礎的手法と似た考え方に基づいているが、バーゼル委員会によって定義されたビジネスライン別に、リスク感応度を考慮しなければならない。オペレーショナル・リスクに関するエクスポージャの規模は、リテールバンキングなど、ビジネスライン別に定義される。ビジネスライン別の所要自己資本は、ビジネスライン毎に設定されたリスク指標(例えば、プラスの年間粗利益)に、そのビジネスラインに割り当てられた割合(β)を乗じて計算される。複数の割合(β)が存在することは想定されていない。

標準的手法を採用する金融機関は、より高度な基準に準拠しなければならない。この基準には、継続的なリ

²⁵ オペレーショナル・リスクの管理と監督のための健全な実務(サウンドプラクティス)(バーゼル銀行監督委員会 2003.2)

リスク削減と個々のモニタリングについて包括的プロセスが存在することが含まれる。取締役会および独立したリスク管理部門は、リスクの管理と報告に積極的に関与し、内部監査部門は、実施されている手続の健全性を検査しなければならない。さらに、オペレーショナル・リスクのデータは、実際の取引に基づく統計データによって裏づけられなければならない。また、経営陣に対する適切な報告システムが存在しているべきである。

先進的計測手法(AMA)

先進的計測手法を採用する銀行は、金融機関固有の実データと、規制上の所要自己資本を決定するための分配メカニズムを使用することができる。規制では、監督当局が設定した個別のリスク指標を持つビジネスラインを代替するものとして、オペレーショナル・リスクの種類を示す、7つの標準的損失事象(例:訴訟費用)を、合わせて提示している。

金融機関が様々な手法の開発と導入を進めている現状を考慮し、監督当局には、当手法の健全性と適切性を判断する権限が与えられている。手法の承認は、監督当局が、内部モデルに適切に組み込まれていることを期待する、さまざまな要素の実態を判断して行われる。

金融機関が採用する手法は、内部損失データに基づいていることが重要である。さらに、金融機関は、経営戦略の計画に、実際のリスク・エクスポージャを完全に取り入れなければならない。また、業務活動において生じた実際の損失を収集するシステムを導入しなければならない。このシステムは、信頼できる通年の損失履歴データが、グループ全体から確実に収集されるようにするものである。また、外部リソースからの情報を使用して、内部データを補強、検証、向上することができる適切な方法を採用すべきである。さらに、金融機関は、ストレステストとポートフォリオ分析を定期的実施し、その結果を確認すべきである。

バーゼル委員会は、規制上の所要自己資本の達成を目的とする、オペレーショナル・リスク計測に関する手法は示していない。金融機関は、どの手法を採用しても、オペレーショナル・リスクの計測が、例えば、1年間の保有期間と99.9%の信頼区間での比較など、信用リスクにおける内部格付手法と同様に、健全な基準を満たしていることを証明しなければならない。

先進的計測手法においては、一定の基準を満たしていれば、オペレーショナル・リスクの計測において、保険によるリスク軽減を考慮することが認められる。ただし、保険によるリスク軽減には、限度が設定されている。

第二の柱: 監督上の検証プロセス

第一の柱は、主として、金融機関に対する定量的要件について取り扱っている。これに対して第二の柱は、金融機関に対する監督の質的側面を対象としている。各国の監督当局は、金融機関のリスク管理システムの質的な保証について、責任を有しており、以下の責務を負っている。

- 開示要件を含む、最低基準への遵守状況を監視すること
- 先進的なリスク管理手法の開発と使用を促進すること
- 銀行が算出したリスク推計値の適切性、および所要自己資本の適切性についての意見を形成すること
- 自己資本の要件が満たされない場合、改善措置をとること

しかし、これは、適切なリスク管理システムを構築し評価する責任が監督当局に移転されるという意味ではない。監督当局の責任は、金融機関の手法と手続を検査することにある。バーゼル委員会は、監督当局の検証に関する4つの原則を示している。

- 銀行は、自己資本全体の妥当性を評価するプロセスを持つべきである。
- 監督当局は、銀行における自己資本の妥当性評価の方法と戦略について、検証と評価を行うべきである。
- 銀行は、最低所要自己資本比率を超える自己資本をもって経営すべきである。
- 監督当局は、早期警告を行うべきである。

銀行内部のリスク管理手法の活用範囲の拡大は、銀行と監督当局との間の積極的な対話を促進することを意図している。

第三の柱：市場規律

バーゼル委員会の目的は、国際金融システムの健全性と安定性を強化することにある。第三の柱で提示された開示要件は、その他の2つの柱を補完して、市場規律を有効に機能させるうえで必要不可欠なものと認識されている。銀行の内部リスクデータの公開は、他の市場参加者に対して、その銀行全体のリスクの状況に関する具体的な情報を提供する。このフレームワークは、すべての銀行が従うべき一般的な開示原則を示している。

銀行は、取締役会によって承認された、正式な情報開示の方針を持つべきである。この方針では、銀行の戦略と目標について、財務状況と収益性に関する情報開示の考え方を含めて示すべきである。さらに、銀行は、開示の適切性について評価するプロセスを導入すべきである。²⁶

この目標は、十分な情報を与えられた市場参加者は、想定されるリスクの水準およびリスク管理の水準を考慮して、投資に関する判断を行うことができるという前提に基づいている。

バーゼル委員会は、開示する情報の量と質について、柔軟な考え方を示している。基本的に、この提案は、推奨として位置付けられている。しかし、このフレームワークでは、金融機関が、内部格付など、所要自己資本を削減するための先進的なモデルを採用した場合に、従わなければならないルールが示されている。

ビジネスプロセスの複雑性や、金融機関のリスク・プロファイルによって、情報開示の頻度や量(重要情報および補足情報)は変化する。開示要件は、次の4つの領域で構成されている。

- 適用範囲 - フレームワークを適用する、企業グループの代表企業名を開示すべきである。
- 資本構造 - 資本のすべての要素について、主な特徴となる諸条件を網羅した情報の要約を開示すべきである。この情報は、払込済み株式資本/普通株式、引当金、および革新的な資本調達手段の種類と特徴を含む。これは、市場参加者に対して、銀行の金融リスクへの耐久力に関する意見を形成するうえで、必要な情報を市場参加者に提供することを目的としている。
- 現実のリスクとその構造 - この領域は、第三の柱の核となる部分である。4つの主要なリスクが定義され、

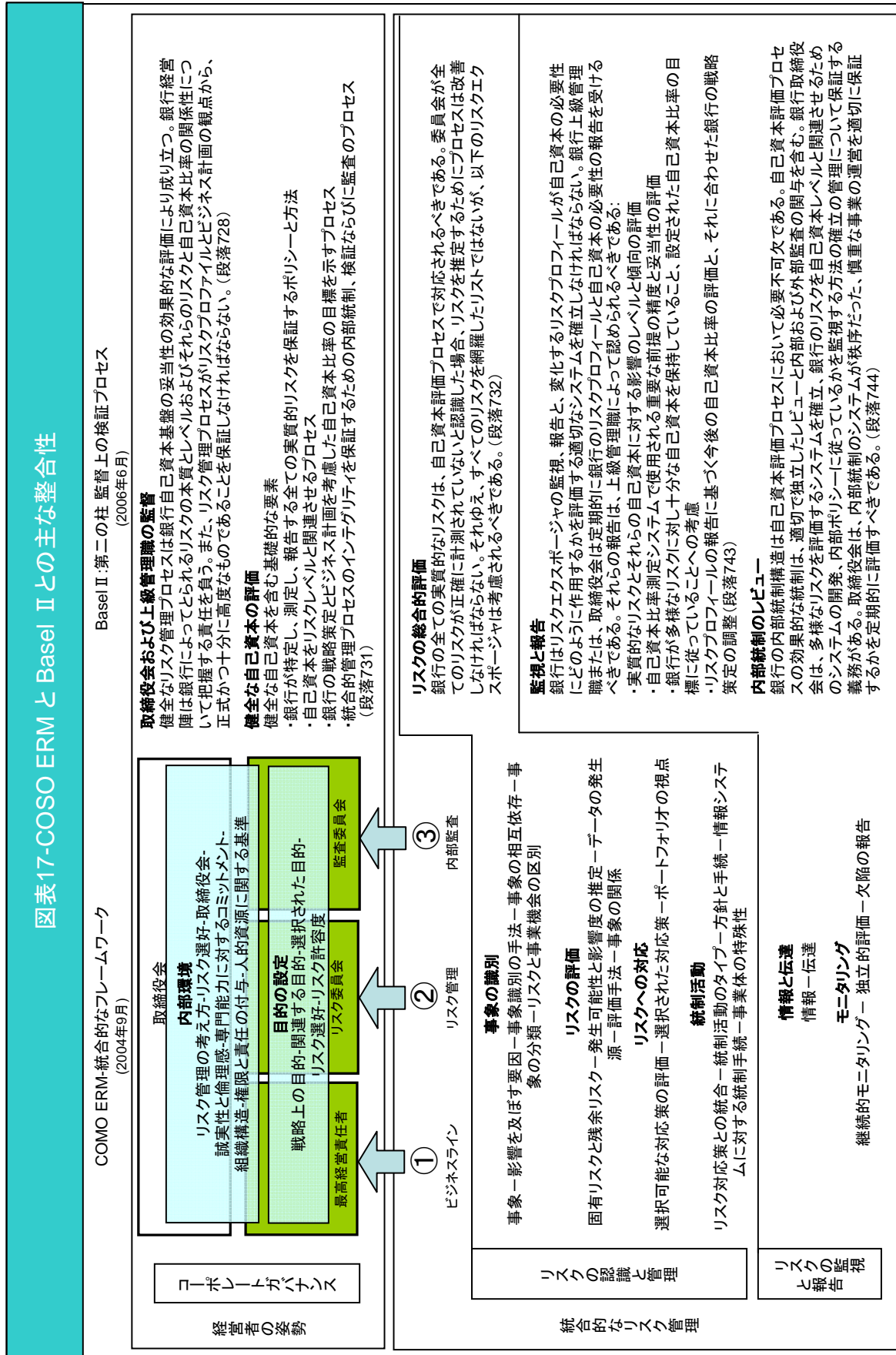
²⁶ ”バーゼルII：自己資本の測定と基準に関する国際的統一化：改訂されたフレームワーク包括版”(バーゼル銀行監督委員会 2006,6)

このそれぞれについて個別のデータを開示すべきである。この4つのリスクとは、銀行の勘定における信用リスク、市場リスク、オペレーショナル・リスク、および金利リスクである。基本的に、金融機関は、それぞれのリスクについて発生する可能性がある損失を推計し、実際の損失と比較すべきである。また、この比較結果を、開示すべきである。この情報に基づいて、市場参加者は、銀行のリスク管理システムの適切性と有効性を評価することが可能となるはずである。

- 自己資本充実度 - 推計されたリスクに対する所要自己資本、および全体の自己資本比率を開示すべきである。さらに、所要自己資本全体および経済資本の配分に影響する要因に関する分析についても、開示すべきである。

付録Ⅱ－COSO ERMとバーゼルⅡとの主な関連

図表17 COSO ERMとバーゼルⅡとの主な関連



付録Ⅲ—バーゼルⅡ原則1:第二の柱—監督上の検証プロセス (2006年6月)とCOSO ERM—総合的フレームワーク(2004年9月)との主な関連

図表 18 バーゼルⅡ第二の柱と、COSO ERM フレームワークとの主な関係

図表 18—バーゼルⅡ 第二の柱と COSO ERM フレームワークとの主な関係	
バーゼルⅡ 第二の柱	COSO ERM フレームワーク
<p>1. 取締役と経営陣による監督</p> <p>銀行経営者には、銀行が負うリスクの性質と水準、およびリスクと適切な自己資本の水準との関係を理解し、さらに、リスク・プロファイルと事業計画の観点から、リスク管理プロセスが、形式面、手続面および精度面で適切な状態にあることを保障する責任がある。一方、取締役会は、銀行のリスク許容度を設定するとともに、経営陣に対して、様々なリスクを評価するフレームワークの確立、リスクと銀行の自己資本の水準とを関連付けるシステムの構築、社内の方針に対する準拠状況をモニタリングする手法を確立させる責任がある。</p> <p>2. 健全な自己資本の評価</p> <p>健全な自己資本の評価のための基礎的な要素には、自己資本をリスク水準と関連付けるプロセスなど、銀行が、全ての重要なリスクを特定し、測定し、報告するために設計された方針と手順とが含まれる。また、マネジメントプロセス全体のインテグリティを確保するための内部統制、レビューおよび監査のプロセスが含まれる。</p> <p>3. リスクの包括的管理</p> <p>銀行が抱える全ての重要なリスクは、自己資本の評価プロセスの対象とすべきである。バーゼルⅡは、全てのリスクを正確に測定することはできないことを認識しているが、リスクを推計するためのプロセスは、整備すべきである。</p> <p>4. 内部統制のレビュー</p> <p>銀行の経営者が様々なリスクを評価するシステムを確立し、自己資本の水準にリスクを関連付けるシステムを構築し、内部の方針に対する準拠状況をモニタリングする手法を確立することに対し、取締役会は責任</p>	<p>1. 内部環境</p> <p>内部環境は、組織メンバーのリスク意識に影響する「組織の気風」を含むとともに、規律と構造を提供することによって、ERMにおける他のすべての構成要素の基礎となる。内部環境の要素には、リスクマネジメントに対する組織の考え方、リスク選好とリスクに関する文化、取締役会による監督、組織を構成する人々の誠実性、道徳的価値観および能力、経営陣の哲学および業務遂行のスタイル、ならびに、組織メンバーに対する権限と責任の割り当て、その組織化と育成に関する経営陣の方法が含まれている。</p> <p>2. 目的の設定</p> <p>あらゆる組織は、組織の外部および内部に原因を持つさまざまなリスクにさらされている。そのために、異なる階層とのつながりを持ち、内部的には一貫性のある目的を構築するために、事象の特定、リスク評価、リスク対応を効果的に行う必要がある。目的は、まず戦略的なレベルで設定され、これによって、業務、報告およびコンプライアンスに関する目的の基礎が確立される。目的は、組織活動におけるリスク許容度の水準を決める、組織のリスク選好と関連している。</p> <p>3. 事象の識別</p> <p>経営陣は、適切な戦略の実行と目的達成に必要な、組織の能力に影響する可能性がある事象を識別する。マイナスの影響を及ぼす可能性を持つ事象は、経営者による評価と対応を必要とするリスクである。プラスの影響を与える可能性がある事象は、マイナスの影響を相殺するものか、事業機会を表している。経営陣は、事業機会を、戦略策定と目的設定のプロセスで再検討する。組織内外のさまざまな要因によって、事象が引き起こされる。潜在的な事象の識別において、経営陣は、組織全体を考慮する。また、組織が置かれている状況と、組織のリスク許容度について考慮する。</p> <p>4. リスクの評価</p> <p>リスクの評価を行うことによって、組織は、組織目標の達成に影響を及ぼす可能性がある事象とその程度について、検討することができる。経営陣は、発生可能性と</p>

を負っている。また、内部統制システムが、秩序ある慎重な事業運営を確保するうえで、適切かどうかについて、取締役会は定期的に評価すべきである。銀行は、インテグリティ、正確性、妥当性を確保するために、リスク管理プロセスを、定期的にレビューすべきである。

5. モニタリングと報告

銀行は、リスク・エクスポージャーのモニタリングと報告、ならびにリスク・プロファイルの変更による自己資本の所要額への影響の評価を行うための、適切なシステムを構築すべきである。銀行の経営陣または取締役会は、自行のリスク・プロファイルと自己資本の所要額について、定期的に報告を受けべきである。この報告は、現在および将来の所要自己資本の推計とその感応度、ならびに、自己資本評価システムにおける主な前提に関して、経営陣による評価を可能とするものであるべきである。また、銀行が、さまざまなリスクに対して、十分な自己資本を保持しているかどうかを、設定された自己資本充実度の目標に照らして、判断することを可能とするものであるべきである。

影響度という、二つの観点から事象を評価すべきであり、また、通常、定性的手法および定量的手法を組み合わせ使用される。発生する可能性がある事象のプラスおよびマイナスの影響度は、組織全体にわたって、個別またはカテゴリごとに検証すべきである。マイナスの影響を持つ可能性がある事象については、固有リスクと残余リスクの両面から、評価すべきである。

5. リスクへの対応

経営陣は、関連するリスクを評価し、リスクへの対応方法を決定する。リスクへの対応方法には、回避、低減、共有および受容がある。経営陣は、リスクへの対応を検討する際には、費用対効果を考慮し、想定される発生可能性および影響度を、目標とするリスク許容度の範囲内に収められるように、対応を選択する。

6. 統制活動

統制活動は、経営陣が選択したリスクへの対応が、確実に実行されるようにするための方針と手続である。統制活動は、すべての階層、すべての部門を含む、組織全体にわたって実施される。統制活動には、承認、権限付与、検証、照合、業務のパフォーマンスレビュー、資産の保全および職務分離など、さまざまな活動が含まれる。

7. 情報と伝達

適切な情報が、組織の構成メンバーの職務遂行に必要な形式と時間内で、識別、収集、伝達される。情報システムは、外部事象、活動および条件に関して、組織内部で生成されたデータと情報を利用して、全社的なリスクの管理、また、目標に関して、十分な情報に基づく判断を行うために必要な情報を提供する。効果的なコミュニケーションが、組織のあらゆる方向で行われる。組織の全メンバーに対して、ERMに関する責任の重要性について、経営陣からの明確なメッセージが伝えられる。組織の全メンバーは、ERMにおける各自の責任と、各自の活動と他のメンバーの業務との関連について理解している。また、組織の全メンバーは、重要な情報を上位者に対して報告する手段を持っている。組織外部の関係者との間で、効果的なコミュニケーションが行われている。

8. モニタリング

ERMは、その構成要素の存在と機能について評価するプロセスによって、長期に渡ってモニタリングされる。これは、継続的なモニタリング活動、独立的評価、およびこの両者の組み合わせによって達成される。継続的モニタリングは、通常のマネジメント活動の中で実施される。独立した評価の範囲と頻度は、主に、リスクの評価と継続的モニタリングの方法の有効性に依拠して決まる。ERMに関する不備は、組織上層部に報告される。また、特に重要な問題は、経営陣と取締役会に報告される。

付録Ⅳ－COSO ERM フレームワークのデータ品質への依存度²⁷

COSO の構成要素	データ品質に関する考慮点
経営者の姿勢	
内部環境 内部環境は、「組織の気風」を含み、リスク管理の哲学とリスク選好、誠実性と道徳的価値観、業務の運営環境を含む、リスクの捉え方と対処方法に関する基礎を形成する。	<ul style="list-style-type: none"> データ品質は、統制環境全体を支えるものであること。 データは、組織の資産として捉えるべきこと。 データ品質のガバナンスとコントロールは、組織の明確な優先事項であること。
目的の設定 経営陣は、目的の達成に影響する事象を特定する前に、目的の設定を完了していなければならない。全社的リスク管理によって、マネジメントによる目的設定のプロセスが導入されていること、選定された目的が、組織のミッションに整合し、目的をサポートするものであること、また、組織のリスク選好に一致することが確保される。	<ul style="list-style-type: none"> 取締役会、CEO、CFO、CRO が、データの品質の確保に関する最終的な責任を負うこと。 データ管理と情報の品質に関する明確な規律と責任が存在すること。 厳格なデータ管理をサポートする方針と手順が存在すること。
リスクの識別および管理	
事象の識別 組織の目的達成に影響を及ぼす、内部および外部の事象が特定され、リスクと事業機会に区別されなければならない。事業機会は、経営陣による戦略策定または目的設定のプロセスにフィードバックされる。	データ品質が不十分な場合、以下の問題につながる可能性がある。 <ul style="list-style-type: none"> 組織の目的達成に悪影響を及ぼす、不十分な情報に基づく意思決定。 組織が、オペレーショナル・リスク、市場リスク、与信リスクを含む識別されていないリスクにさらされ、その結果、風評リスク、財務リスク、規制や法務リスク、伝染リスクなど、より大きなリスクを負う可能性。
リスクの評価	

²⁷ 「Data Quality: The Hidden Assumption behind COSO」(George Marinos, Partner, PricewaterhouseCoopers)に基づいている。

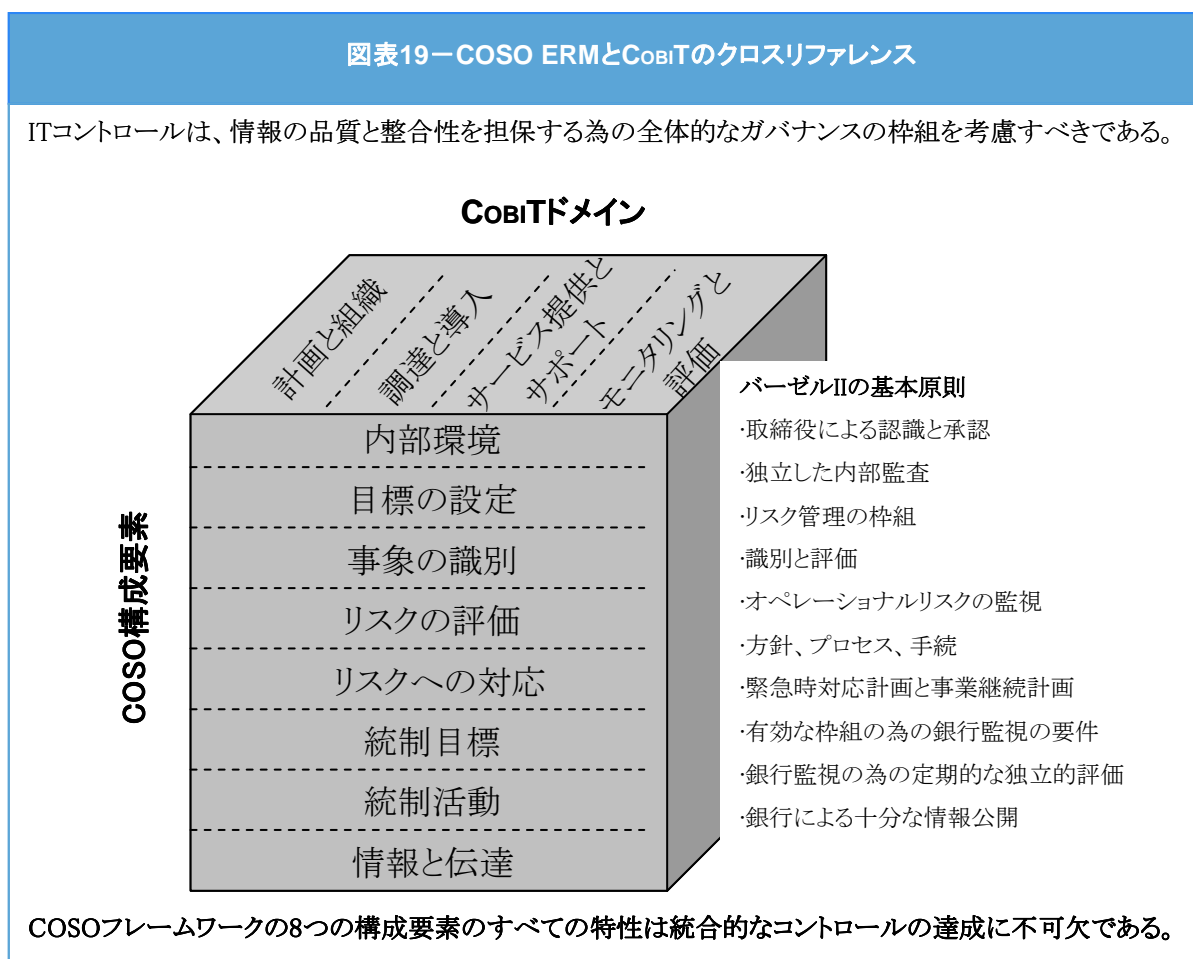
リスクの識別および管理	
<p>リスクは、発生可能性と影響度を考慮して分析され、その結果はリスクの管理方法を決定するための土台となる。リスクは、固有リスクと残余リスクの二つの側面について評価される。</p>	
<p>リスクへの対応</p> <p>経営陣は、リスクへの対応方法(リスクの回避、受容、低減、共有)を選択し、組織のリスク許容度とリスク選好に則した対策を立案する。</p>	<ul style="list-style-type: none"> 測定ができなければ、管理もできないこと。 データは、統制手段の精度を表すこと。 データ管理と情報の品質に関する明確な規律と責任が存在すること。 厳格なデータ管理をサポートする方針と手順が存在すること。
<p>統制活動</p> <p>リスクへの対応を効果的に実施するための方針と手順を策定し、導入する。</p>	

リスクの監視および報告	
<p>情報と伝達</p> <p>関連する情報を識別、収集し、組織メンバーの職務遂行に必要な形式と時間内で伝達する。より広い意味で、効果的なコミュニケーションが、組織のあらゆる方向で行われる。</p>	<ul style="list-style-type: none"> 不十分なデータ品質は、報告と対応に深刻な問題を及ぼすこと。 統制に関する機能と責務に必要な情報は、担当役員の職務遂行をサポートするために、適切な内容で適時に伝達しなければならない。
<p>モニタリング</p> <p>ERMの全体がモニタリングされ、必要に応じて修正される。モニタリングは、継続的な管理活動、独立的評価、およびその両者によって達成される。</p>	<ul style="list-style-type: none"> 有効性の高いモニタリングを行うためには、データ品質をサポートする基本的要素である正確性、網羅性、アクセス可能性、インテグリティ、妥当性、有用性、一貫性、適時性、可監査性が必要であること。

付録V—バーゼルIIとCOBIT

前述の通り、バーゼルIIには10の基本原則、COSO ERMには8つの構成要素に区分された内部統制、また、COBITには4つのドメインがある。図表19は、バーゼルIIにおけるオペレーショナル・リスクの目的を達成するためには、このすべてが実施され、統合される必要があることを示している。COBITは、ITに関して同様の詳細な指針を提供している。統制環境の識別から始まり、内部統制のモニタリングに至るCOSO ERMの8つの構成要素は、立方体の水平階層に該当し、COBITの「計画と組織」から「モニタリングと評価」までの目的ドメインに対して、個別に、また全体として適用される。

図表19は、バーゼルIIの基本原則、およびCOSOの構成要素および、COBITのドメインとの関係を示している。この図で明らかのように、COBITの多くのITプロセスは、2つ以上のバーゼルIIおよびCOSOの構成要素と関連している。これは、アプリケーション統制の基盤を成すIT全般統制の性質からして、当然のことと言える。このような複合的関係を持つ性質は、IT統制が、他の統制の基盤であること、また信頼性のある内部統制プログラムにおいて必要不可欠なものであることを裏付けるものである。



COBITは、ITのリスクとコントロールのガバナンスに関するマネジメントのための統合的フレームワークである。COBITは、4つのドメイン、34のITプロセス、200を超える統制目標によって構成されている。COBITは、ITガバナンスに関連するすべての局面を対象とするコントロールを網羅しているが、本資料の作成にあたっては、バーゼルIIのリスク管理の目的において重要なもののみを採用した。バーゼルIIでは、容易に入手可能で、広く受け入れられるフレームワークを適用することが求められているが、COBITは、その考え方に適合した、自由に利用できるフレームワークである。COBITは、組織レベルと活動レベルの両方の目的を、関連するコントロールと合わせて提

供しており、COSO やその他のガバナンスのフレームワークに対して、IT に関する構成要素を補完するものとして、世界中の組織で広く利用されている。

関連する IT プロセスとコントロールを選択するにあたっては、以下の 2 つのアプローチがある。

- リスク主導型アプローチ — 関連するリスク要因を選定し、影響度によるリスク要因の分類（最重要、重要、一定の影響、関連無し）、ならびに統制目標および関連するプロセスの識別を行う。ITGIの*CobiT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*は、リスク要因の選定を進める際に、その参考として利用できる。
- 目標主導型アプローチ — バーゼル II に関連するITの目標を識別し、CobiT の主な項目、およびITGIの刊行物である、*IT Governance Implementation Guide: Using CobiT and Val IT, 2nd Edition*が提供するガイダンスを利用する。

リスク主導型アプローチ

監督当局やその他の団体が指摘するとおり、オペレーショナル・リスクの定義には、広い範囲に及ぶ個別のリスク要因が含まれ、それらは業務的な要素を、より範囲の広い ERM のフレームワークに統合する前から考慮することができる。

一般的には、以下のリスク主導型戦略が採用されている。

- 最重要リスク、および関連する統制目標とプロセスを識別する。リスク管理の文化が導入され、ITリスクの管理を支援するITリスク管理のフレームワークが利用される。このアプローチの結果は、ERMのフレームワークに統合される。このアプローチには、リスク管理が、ITに関連する文化の一部となり、新たなリスクが認識されると、直ちに対応が取られるようになるという利点がある。
- 数多くの潜在的なリスク事象の種類を識別し、コントロールとリスク低減要因を評価した後、可能な範囲について是正措置を講じる。このアプローチは、識別されたリスクに重点を置き過ぎることによって、予期せぬリスクに対して、柔軟な対応が難しくなる不利が生じる可能性がある。また、多くのリスク要因が識別された場合、最重要リスクに重点を置いた対応が難しくなるリスクが増大する。

図表 20 は、バーゼル II のリスク事象の種類に対応した、IT 事象の種類、およびこの IT 事象の種類に対応した CobiT プロセスを例示したものである。

図表 20—バーゼル II のリスク事象の種類、IT 事象の種類、および CobiT プロセス		
バーゼル II のリスク事象の種類	IT 事象の種類	CobiT プロセス
内部不正	<ul style="list-style-type: none"> ● プログラムの不正操作 ● 修正機能の不正使用 ● システムインストラクションの不正操作 ● ハードウェアの不正操作 ● システムおよびアプリケーションデータの不正変更 ● ライセンスを受けていない、または未承認のソフトウェアの使用やコピー ● アクセス権の不正使用 	PO6 DS5 DS9 DS12

図表 20—バーゼルⅡのリスク事象の種類、IT 事象の種類、および CoBIT プロセス

バーゼルⅡの リスク事象の種類	IT 事象の種類	CoBIT プロセス
外部不正	<ul style="list-style-type: none"> ●ハッキングによる、システムおよびアプリケーションデータの不正な変更 ●部外者による物理的または電子的な機密文書の閲覧 ●アクセス権の不正使用 ●通信回線の盗聴および傍受 ●パスワードの漏洩 ●ウィルス 	DS5
従業員の行動と職 場の安全	<ul style="list-style-type: none"> ●IT資源の不正利用 ●セキュリティに関する不十分な反応 	PO6 DS5
顧客、製品、商習慣	<ul style="list-style-type: none"> ●従業員による外部への機密情報の開示 ●委託先の管理 	PO6 DS2
物理的資産への損 害	<ul style="list-style-type: none"> ●故意または過失による IT インフラストラクチャの物理的な損害 	DS12
事業停止とシステム 障害	<ul style="list-style-type: none"> ●ハードウェアまたはソフトウェアの誤作動 ●通信障害 ●従業員による妨害 ●主要ITメンバーの離職 ●ソフトウェア/データファイルの破壊 ●ソフトウェアまたは機密情報の盗難 ●コンピュータウィルス ●バックアップの失敗 ●サービス不能(DOS)攻撃 ●構成管理の誤り 	AI7 DS3 DS4 DS5 DS9 DS10
実行、導入、プロセ ス管理	<ul style="list-style-type: none"> ●電子媒体の不適切な取り扱い ●端末の放置 ●変更管理における誤り ●トランザクションの不完全な入力 ●データの入出力における誤り ●プログラミングやテストの誤り ●復旧手順のミスなど、オペレーションの誤り 	AI3 AI6 AI7 DS5 DS10

目標主導型アプローチ

目標主導型アプローチには、事業目標に対する IT 活動の整合性を高めるという利点がある。

図表 21 は、CoBIT が提供する IT 目標を示している。右側の列は、IT 目標とバーゼルⅡの関連性の有無を示している。関連性が示されていない IT 目標は、バーゼルⅡの目的とは関係がないものと見なされる。

図表 21 CoBIT IT 達成目標

達成目標	関連性
------	-----

図表 21 CobiT IT 達成目標

図表 21 CobiT IT 達成目標		
1	事業戦略と合致するビジネス要件への対応	
2	取締役会の指示に従ったガバナンス要件への対応	●
3	提供サービスとサービスレベルに対するエンドユーザの満足の確保	
4	情報利用の最適化	
5	機敏な IT 能力の創出	
6	ビジネスの機能的要件およびコントロール要件を効果的かつ効率的なコンピュータ化対応策に変換する方法の定義	
7	統合および標準化されたアプリケーションシステムの調達と保守	
8	統合および標準化された IT インフラストラクチャの調達と保守	●
9	IT 戦略に対応する IT スキルの獲得と維持	●
10	サードパーティとのリレーションシップについての相互満足の達成	●
11	アプリケーションのビジネスプロセスへのスムーズな統合	
12	IT 費用、便益、戦略、ポリシー、およびサービスレベルに関する透明性の確保と理解の実現	●
13	アプリケーションおよび技術的対応策の適切な利用と成果達成の保証	●
14	すべての IT 資産の責任の所在の明確化と適切な保護	●
15	IT インフラストラクチャ、資源、および能力の最適化	●
16	対応策とサービスの提供における不備と補正作業の必要性の削減	●
17	IT 目標の達成の保証	
18	リスクが IT 目標および資源に与える、ビジネス上の影響の明確化	●
19	重要かつ機密の情報が、当該情報へのアクセスを許可されていないユーザに開示されないことの保証	●
20	自動化された業務取引および情報交換の信頼性の確保	●
21	エラー、意図的な攻撃、または災害で生じた障害に対する、IT サービスおよびインフラストラクチャの抵抗カ・回復力の確保	●
22	IT サービスの中断または変更が及ぼすビジネスへの影響の極小化	●
23	要求に応じて IT サービスが使用可能であることの保証	●
24	IT の費用効率および事業収益性への IT の貢献度の向上	
25	品質標準を満たすプロジェクトの、期間内、かつ予算内での遂行	
26	情報および情報処理インフラストラクチャのインテグリティ維持	●
27	IT の法令へのコンプライアンスの確保	●
28	IT 活用による費用効率の高いサービス品質、継続的な改善、および将来の変更に対する対応力実現の実証	

図表 22 に示す IT プロセスは、導入プログラムの基礎として利用可能である。

図表 22 導入プログラムのための IT プロセスのサンプル
CobiT IT プロセス全体

図表 22 導入プログラムのための IT プロセスのサンプル CobiT IT プロセス全体		全体
IT プロセス		
P01	IT 戦略計画の策定	●
P02	情報アーキテクチャの定義	
P03	技術指針の決定	
P04	IT プロセスと組織及びそのかわりの定義	
P05	IT 投資の管理	
P06	マネジメントの意図と指針の周知	●
P07	IT 人材の管理	
P08	品質管理	
P09	IT リスクの評価と管理	
P010	プロジェクト管理	

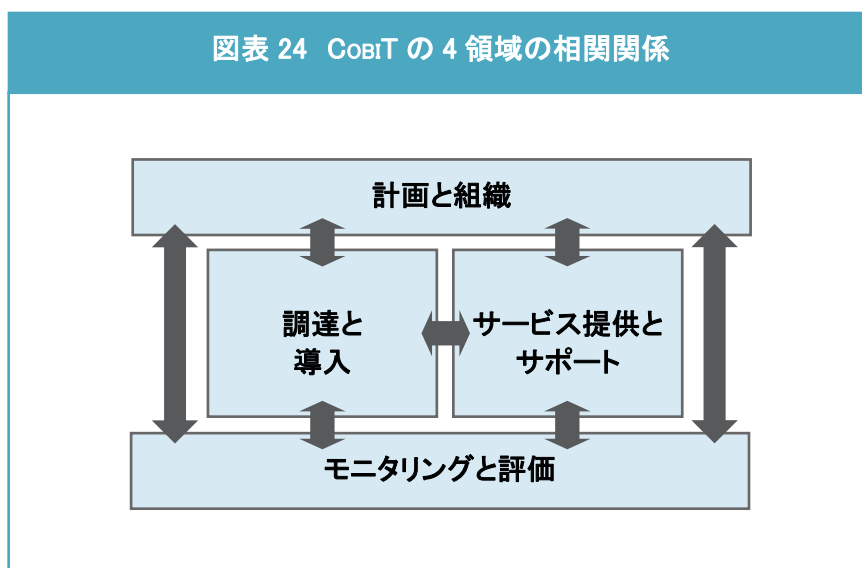
図表 22 導入プログラムのための IT プロセスのサンプル
CobiT IT プロセス全体

AI1	コンピュータ化対応策の明確化	
AI2	アプリケーションソフトウェアの調達と保守	
AI3	技術インフラストラクチャの調達と保守	
AI4	運用と利用の促進	●
AI5	IT 資源の調達	
AI6	変更管理	●
AI7	ソリューションおよびその変更の導入と認定	●
DS1	サービスレベルの定義と管理	
DS2	サードパーティのサービスの管理	
DS3	性能とキャパシティの管理	
DS4	継続的なサービスの保証	●
DS5	システムセキュリティの保証	●
DS6	費用の捕捉と配賦	
DS7	利用者の教育と研修	●
DS8	サービスデスクとインシデントの管理	
DS9	構成管理	●
DS10	問題管理	
DS11	データ管理	●
DS12	物理的環境の管理	●
DS13	オペレーション管理	
ME1	IT 成果のモニタリングと評価	
ME2	内部統制のモニタリングと評価	●
ME3	外部要件に対するコンプライアンスの保証	
ME4	IT ガバナンスの提供	●

付録VI—COBIT プロセス

本書の重要な目的の一つは、バーゼルⅡに準拠するために考慮すべき、特定のプロセスに関する指針を、IT 専門家に対して提示することにある。IT 組織は、常に業務の性質と範囲を考慮して、内部統制プログラムに含めるべきコントロール目標、実施するコントロール、およびテスト方法の事例を決定すべきである。

バーゼルⅡは、これらのコントロール目標や関連する統制活動に対する要求事項を指示していない。これは、引き続き、各組織が判断する事項である。したがって、組織は、オペレーショナル・リスクの管理に必要な IT 統制の性質と範囲を、状況に応じて評価すべきである。²⁸COBIT の 4 つの領域における相互関係を、**図表 24** に示す。



次のコントロールプロセスが、バーゼルⅡに関連する IT の達成目標もしくはバーゼルⅡのプロセスにマッピングされた。

計画と組織

PO2 情報アーキテクチャの定義

情報システム部門は、ビジネス情報モデルの構築のみならず、これを定期的に更新し、ビジネス情報を最大限に利用できるシステムを定義する。

このビジネス情報モデルには、組織のデータ構文規則に従った企業データディクショナリ、データ分類体系、およびセキュリティレベルが含まれる。

このプロセスは、安全で信頼性の高い情報を提供することを確実にすることにより、マネジメント層の意思決定の質を高める。また、情報システム資源をビジネス戦略に適切に合わせた合理的なものとする。

この IT プロセスにおいては、データのインテグリティおよびセキュリティに関する説明責任能力の強化のほか、アプリケーションおよび組織全体にわたる情報共有の有効性とコントロールの強化が必要である。

PO4 IT プロセスと組織およびそのかわりの定義

²⁸ ITGI が公表した *COBIT* コントロールプラクティスは、COBIT プロセスの根拠となるコントロール目標をサポートする価値要因やリスク要因、コントロールの実践に関する事例が示されている。

IT 組織は、人材、スキル、機能、説明責任、権限、役割、実行責任、および監督に関する要件を考慮して定義する。

透明性とコントロールを確保し、マネジメント層とビジネス管理部門の関与を確実にするために、IT プロセスフレームワークに、IT 組織が組み込まなければならない。

企業の戦略委員会は、取締役会を通して IT 部門の監督を徹底させなければならない。さらにビジネス部門と IT 部門が参加する 1 つ以上の推進委員会が、ビジネス上の必要性に応じて、IT 資源の優先順位を決定する。

プロセス、管理ポリシー、および手続は、組織内のすべての機能のために、整備、運用される必要がある。その際には、コントロール、品質保証、リスク管理、情報セキュリティ、データとシステムのオーナーシップ、および職務の分離に、特に留意すること。

ビジネス要件にタイムリーに対応するため、関連する意思決定プロセスには IT 部門も参加する。

PO6 マネジメントの意図と指針の周知

マネジメント層は、企業の IT コントロールフレームワークを策定し、ポリシーを定義、周知する。

継続的な周知プログラムを導入し、マネジメント層が承認および推進する使命、サービス目標、ポリシー、手続などを明確に表明する。

情報を周知することで、IT 目標の達成が促進され、さらにビジネスリスクおよび IT リスクのほか、目標や指針についての認識と理解を得ることができる。

このプロセスにより、関連法規へのコンプライアンスが確立される。

PO8 品質管理

実績のある開発プロセス、調達プロセス、および標準が組み込まれた品質管理システム(QMS)が作成、維持されている。これは、明確な品質要件、手続、およびポリシーを提示し、QMS を計画、導入、維持することで実現できる。

品質要件は、数値化された達成可能な指標として表し、周知する。

モニタリング、分析、逸脱への対応、および利害関係者への結果報告を常時行うことにより、継続的な改善を実現する。

品質管理は、IT によるビジネスへの価値提供と継続的な改善および利害関係者に対する透明性を確実に確保する上で不可欠である。

PO9 IT リスクの評価と管理

リスク管理フレームワークが構築され、維持されている。

フレームワークでは、合意された一般的な IT リスクレベル、リスク軽減戦略、および未解決のリスクについて文書化する。

すべての計画外のイベントが組織の達成目標に与える潜在的な影響を特定、分析、評価する。

未解決のリスクを許容レベルまで軽減するために、リスク軽減戦略が導入されている。

利害関係者が理解可能なように評価結果をとりまとめると同時に、財務的な観点でもとりまとめる。これにより、利害関係者から見ても、リスクが許容範囲に収まるようにする。

調達と導入

AI3 技術インフラストラクチャの調達と保守

組織は、技術インフラストラクチャの調達、導入、およびアップグレードに関するプロセスを策定する必要がある。

これを実現するには、合意された技術戦略に基づいてインフラストラクチャを調達、保守、および保護するためのアプローチを計画し、開発環境とテスト環境を用意する必要がある。

この結果、ビジネスアプリケーションに対する継続的な技術的サポートが確保される。

AI4 運用と利用の促進

新たなシステムに関する知識を利用可能にする必要がある。

このプロセスでは、ユーザおよび IT 部門のための文書や資料を作成し、アプリケーションとインフラストラクチャの適切な使用と運用を確保するための研修を実施する。

AI6 変更管理

インフラストラクチャおよびアプリケーションに関連する緊急保守やパッチ適用を含む、本番環境におけるすべての変更は、コントロールされた方法で、正式に管理されている。

変更(手続、プロセス、システムパラメーター、およびサービスパラメーターを含む)は、変更の実施前に記録、評価、および承認され、変更の実施後には計画された成果に照らしてレビューされる。

これにより、本番環境の安定性やインテグリティに悪影響を及ぼすリスクを低減できる。

AI7 ソリューションおよびその変更の導入と認定

新規システムの開発完了後、そのシステムを実際に運用可能な状態にする必要がある。

これには、適切なテストデータを使用した専用環境における公式的なテストの実施、展開と移行の指示書の策定、リリース計画策定と実際の本番環境への移行、および導入後のレビューが必要である。

これにより、運用システムが合意された計画と成果に合致していることを保証する。

サービス提供とサポート

DS1 サービスレベルの定義と管理

IT 管理部門とビジネス部門の顧客間で、求められるサービスについて効果的なコミュニケーションを行うためには、IT サービスおよびサービスレベルの定義と合意内容を文書化する必要がある。

本プロセスには、サービスレベルの達成状況についてモニタリングし、利害関係者にタイムリーな報告をすることも含まれる。

このプロセスにより、IT サービスと関連するビジネス要件との間の整合を図ることができる。

DS2 サードパーティのサービスの管理

サードパーティ(サプライヤ、ベンダー、パートナー)が提供するサービスがビジネス要件を確実に満たすようにするには、効果的なサードパーティの管理プロセスが必要である。このプロセスでは、サードパーティとの合意のもと、役割、実行責任、および要求事項を明確に定義し、このような合意事項の有効性とコンプライアンスをレビュー

一しモニタリングする。

サードパーティが提供するサービスを効果的に管理することで、不適格なサービスプロバイダに起因するビジネスリスクを最低限に抑えることができる。

DS3 性能とキャパシティの管理

IT資源の性能とキャパシティを管理するには、IT資源の性能とキャパシティを定期的にレビューするプロセスが必要である。

このプロセスには、作業負荷、ストレージ、および緊急時の要件に基づいて今後のニーズを予測することが含まれる。

このプロセスにより、ビジネス要件を支援する情報資源の継続的可用性が保証される。

DS4 継続的なサービスの保証

継続的なITサービスを提供するには、IT継続計画の作成、保守、およびテスト、遠隔地のバックアップ保管施設の確保および定期的な継続計画に関するトレーニングの実施が必要である。

効果的なサービス継続プロセスにより、主要なITサービスの中断の可能性と、このような中断が主要なビジネスの機能とプロセスに及ぼす影響を最小限に抑えることができる。

DS5 システムセキュリティの保証

情報のインテグリティを維持し、IT資産を保護するためには、セキュリティ管理のプロセスが必要である。

このプロセスには、ITセキュリティに関する役割と責務、ポリシー、標準、および手続を定め、それらを運用、改善することが含まれる。

また、セキュリティ管理には、セキュリティのモニタリングと定期的なテストの実施、および識別されたセキュリティの弱点やインシデントに対する是正措置の導入も含まれる。

セキュリティ管理を効果的に実行することで、すべてのIT資産を保護し、セキュリティの脆弱性やインシデントがビジネスに与える影響を最小限に抑えることができる。

DS9 構成管理

ハードウェアとソフトウェアの構成のインテグリティを確保するには、正確かつ網羅された構成管理用リポジトリの作成と保守が必要である。

このプロセスには、初期構成情報の収集、ベースラインの設定、構成情報の検証と監査、および必要に応じた構成管理用リポジトリの更新が含まれる。

効果的な構成管理により、システムの可用性が向上し、本番システムでの課題が最小限に抑えられ、課題を速やかに解決できるようになる。

DS10 問題管理

効果的な問題管理を実施するには、問題を特定および分類し、根本原因を分析し、問題を解決する必要がある。

問題管理プロセスには、改善のための提案事項の策定、問題の記録保持、および是正措置の状況のレビューも含まれる。

効果的な問題管理プロセスにより、システムの可用性が最大限に確保されるほか、サービスレベルの向上、費

用削減、および顧客の利便性と満足度の向上を実現できる。

DS12 物理的環境の管理

コンピュータ機器と要員を保護するには、適切に設計および管理されている物理的施設が必要である。

物理的環境を管理するプロセスには、物理的なサイト要件の定義、適切な施設の選定、および環境要因をモニタリングし物理的アクセスを管理するための効果的なプロセスの設計が含まれる。

物理的環境を効果的に管理することで、コンピュータ機器と要員にかかわる障害に起因するビジネスの中断が減少する。

モニタリングと評価

ME1 IT 成果のモニタリングと評価

IT 成果を効果的に管理するには、モニタリングプロセスが必要である。

このプロセスには、妥当な成果達成指標の定義、体系的かつタイムリーな成果報告、および成果目標から逸脱した場合の迅速な対応が含まれる。

指針やポリシーに沿って正しい運用が行われていることを確認するため、モニタリングが必要である。

ME2 内部統制のモニタリングと評価

IT のための有効な内部統制プログラムを確立するには、明確なモニタリングプロセスが必要である。

このモニタリングプロセスには、セルフ評価やサードパーティによるレビューの結果、発見されたコントロールの例外事項が含まれる。

内部統制のモニタリングの主要な利点には、効果的かつ効率的な業務運営の実現と法規制へのコンプライアンスの確保がある。

ME3 外部要件に対するコンプライアンスの保証

コンプライアンス要件への監督を効果的に行うには、法律、規制、および契約に対するコンプライアンスを確保するための、独立したレビュープロセスを確立する必要がある。

このプロセスには、コンプライアンス要求の識別やその対応の最適化と評価、準拠してきた要件に対する保証の入手、そして最後に、IT 部門のコンプライアンスに関する報告とそのほかのビジネス部門からの報告との統合が含まれる。

ME4 IT ガバナンスの提供

効果的なガバナンスフレームワークの確立には、組織構造、プロセス、リーダーシップ、役割、および責務を定義し、企業の戦略と目標に沿った企業の IT 投資を確実に実現することが含まれる。

CoBIT で定義されているそのほかのコントロールプロセスは、バーゼル II に関連した IT 達成目標あるいは IT 全般統制を構築する際に考慮すべきバーゼル II プロセスのいずれにも含まれていない。

計画と組織

PO1 IT 戦略計画の策定

ビジネス戦略およびビジネス上の優先順位に従って IT 資源の管理および割り当てを行うには、IT 戦略計画の策定が必要である。

IT 部門およびビジネス部門の利害関係者は、プロジェクトおよびサービスのポートフォリオ(全体構成)から生み出される価値の最適化を実現する責任を有する。

戦略計画を策定することにより、IT の利用機会および限界に対する主要な利害関係者の理解が深まり、現在の成果が評価され、能力と人材に関する要件が特定され、必要な投資レベルが明確となる。

ビジネス戦略やビジネス上の優先順位は IT 戦略計画のポートフォリオに反映され、IT 実行計画を通じて具現化されることになる。実行計画は、ビジネス部門と IT 部門の双方から理解が得られ、承認を受けた簡潔な目標、対応計画、および作業を規定したものである。

PO3 技術指針の決定

情報サービス部門は、ビジネス部門を支援するために技術指針を定める必要がある。そのためには、技術インフラストラクチャ計画を策定する必要がある。

また、製品、サービス、および提供手段に関して、技術が、どのような貢献ができるかについて、明確かつ現実的な見込みを立て、これを管理するアーキテクチャ委員会を設置しなければならない。

技術インフラストラクチャ計画は定期的に更新され、システムアーキテクチャ、技術指針、調達計画、標準、移行戦略、および緊急時対応などの観点を含む。

これにより、プラットフォームとアプリケーションとの間の相互運用性の改善、競争的な環境における変化へのタイムリーな対応、および情報システム要員の確保と投資におけるスケールメリットを実現できる。

PO5 IT 投資の管理

コスト、便益、予算内での優先順位、正式な予算編成プロセス、および予算に照らした管理が組み込まれたフレームワークを構築および維持し、IT 関連の投資プログラムを管理する。

利害関係者と協力し、IT 戦略計画および実行計画の枠内で総コストと便益を特定およびコントロールし、必要に応じて是正措置を講じる。

このプロセスにより、IT とビジネスの利害関係者間の協力関係が促進され、IT 資源の効果的かつ効率的な使用が可能になる。さらに、総所有コスト(TCO)についての透明性と説明責任が確保され、ビジネス上の便益および IT 関連の投資からの収益の獲得が可能になる。

PO7 IT 人材の管理

ビジネス部門に対する IT サービスの作成と提供のために、有能な人材を獲得し、維持する。

これは、採用、研修、業績評価、昇進、および解雇を支援するために、文書化され合意された行動基準を遵守することで達成される。

要員は重要な資産であり、ガバナンスおよび内部統制環境は要員の意欲と能力に大きく依拠するため、このプロセスは非常に重要である。

PO10 プロジェクト管理

すべての IT プロジェクトの管理を目的とするプログラムおよびプロジェクト管理フレームワークが確立されている。

このフレームワークでは、すべてのプロジェクトを適正に優先順位付けし、プロジェクト間の調整を行う。

プロジェクトのリスク管理およびビジネスへの価値の提供を実現するため、フレームワークには、基本計画、資

源の割り当て、成果物の定義、ユーザによる承認、サービスの提供に対する段階的なアプローチ、品質保証、正式なテスト計画、テストの実施と導入後レビューの実施が含まれる。

このアプローチにより、予想外のコストやプロジェクトの中止によって生じるリスクが軽減され、ビジネス部門およびエンドユーザへの情報伝達および両者の関与が促進される。さらに、プロジェクト成果物の価値と品質が保証され、IT 関連の投資プログラムに対するそれらの貢献度を最大化できる。

調達と導入

AI1 コンピュータ化対応策の明確化

新しいアプリケーションや機能を必要とする場合は、実際の調達または構築の前に、それらがビジネス要件を効果的かつ効率的なアプローチで確実に満たすものであるか分析する必要がある。

この分析のプロセスには、ニーズの定義、代替となる調達元の検討、技術的および経済的実現性の見直し、リスク分析およびコスト/便益分析、アプリケーションを「開発」するか「購入」するかの最終決定が含まれる。

これらすべての手続を踏むことにより、ソリューションの実施および導入コストが最小限に抑えられ、ビジネス目標の達成を確実に支援できるようになる。

AI2 アプリケーションソフトウェアの調達と保守

アプリケーションは、ビジネス要件に沿った形で利用可能になる。

このプロセスには、アプリケーションの設計、業務処理統制とセキュリティ要件の適切な組み込み、および各種標準に準拠した設計と構成が含まれる。

このプロセスにより、組織は自動化された適切なアプリケーションを利用して、ビジネス運営を的確に支援できる。

AI5 IT 資源の調達

要員、ハードウェア、ソフトウェア、サービスを含む IT 資源を調整する必要がある。

そのためには、調達手続の策定と実施、ベンダーの選定、契約等の整備、および実際の調達が必要である。

これらを行うことにより、組織はタイムリーかつコスト効率よく、必要な IT 資源をすべて確保可能になる。

サービス提供とサポート

DS6 費用の捕捉と配賦

IT 費用をビジネス部門に適性かつ公平に配賦するための体系を実現するには、IT 費用を正確に測定し、適正な配賦についてビジネス部門の同意を得る必要がある。

このプロセスには、IT 費用を捕捉し、サービスを受けるユーザへ配賦および報告するためのシステムの構築と運用が含まれる。

適正な配賦システムを導入することで、IT サービスの利用に関して、ビジネス部門が十分な情報を得た上での決定が可能になる。

DS7 利用者の教育と研修

IT 部門内を含む IT システムの全ユーザに対して効果的な教育を実施するには、ユーザグループごとの研修の

ニーズを特定する必要がある。

このプロセスには、ニーズの特定の他に、効果的な研修のための戦略の策定と実施、および結果の測定が含まれる。

効果的な研修プログラムにより、ユーザによるエラーの減少、生産性の向上、および主要コントロール(ユーザセキュリティ対策など)へのコンプライアンスの強化を実現でき、技術を一層効果的に利用できるようになる。

DS8 サービスデスクとインシデントの管理

IT ユーザの問い合わせや発生した問題に対してタイムリーかつ効果的に対応するには、適切に構成、運用されているサービスデスクとインシデント管理プロセスが必要である。

このプロセスには、インシデント登録、インシデントエスカレーション、傾向と根本原因の分析、および問題解決の機能を持つサービスデスクの設置が含まれる。

ビジネス上の便益には、ユーザからの問い合わせに対する迅速な対応による、生産性の向上が含まれる。

さらに、効果的な報告を通して、ビジネス部門はユーザ研修の不足といった根本原因の追究に取り組むことができる。

DS11 データ管理

効果的なデータ管理を実施するには、データ要件を特定する必要がある。

データ管理プロセスには、メディアライブラリ、データのバックアップと復元、およびメディアの適切な廃棄に関する管理手続の確立も含まれる。

効果的なデータ管理は、ビジネスデータの質、適時性、および可用性の保証に有用である。

DS13 オペレーション管理

データを完全かつ正確に処理するには、データ処理手続の効果的な管理と、ハードウェアの綿密な保守が必要になる。

このプロセスには、計画された処理の効果的な管理、機密性を有する出力の保護、インフラストラクチャ性能のモニタリング、およびハードウェアの予防的保守に適用する運用上のポリシーと手続を定義する。

効果的なオペレーション管理により、データのインテグリティが維持され、業務の遅延および IT 運用費用が削減される。

付録Ⅶ—ABC 銀行: 実施例

この事例は、リスクの評価と測定を行う際の検討プロセスの例を示すことを目的としている。この事例では、対象を IT 組織と1つのリスクに限定している。実際には、リスク評価の管理プロセスは、組織横断的に実施され、他のリスクの管理や既存のプログラムと統合的に実施されるであろう。

ABC 銀行は、内部不正に関連するリスクを管理しようとしている。これまでの検討において、内部不正に対する組織のリスク許容度は、低いと判断されている。重要な不正が発生する可能性は低いと考えられているが、銀行の評判に対する潜在的な影響度や、規制に関連する潜在的な費用は、高いと考えられている。関連するプロセスは、コントロール失敗の影響を拡大する可能性がある外部不正、ビジネスの中断、およびシステム障害に関連したリスクにも対応している。

内部不正に関連する IT 事象の種類は、**図表 25** のとおりである。

図表 25 - 内部不正に関連する IT 事象の種類		
バーゼル II の事象	IT 事象の種類	CoBIT プロセス
内部不正	<ul style="list-style-type: none"> ・ プログラムの不正操作 ・ 修正機能の不正使用 ・ システムインストラクションの不正操作 ・ ハードウェアの不正操作 ・ ハッキングによる、システムおよびアプリケーションデータの不正変更(訳注: 外部不正) ・ ライセンスを受けていない、または承認されていないソフトウェアの使用やコピー ・ アクセス権の不正使用 	<ul style="list-style-type: none"> ・ PO6 ・ DS5 ・ DS9 ・ DS12

ABC 銀行は、設定された目標に基づいて、内部不正に関連する CoBIT の項目を参照し、実施可能な対策について検討した。その結果、パフォーマンスの指標を、以下のように設定した。

PO6 マネジメントの意図と指針の周知

ABC 銀行は、PO6 について検討した。PO6 の内容は、以下のとおりである。

マネジメント層は、企業の IT コントロールフレームワークを策定し、ポリシーを定義、周知する。継続的な周知プログラムを導入し、マネジメント層が承認および推進する使命、サービス目標、ポリシー、手続などを明確に表明する。情報を周知することで、IT 目標の達成が促進され、さらにビジネスリスクおよび IT リスクのほか、目標や指針についての認識と理解を得ることができる。このプロセスにより、関連法規へのコンプライアンスが確立される。

さらに、ABC 銀行は、ITGP6 のコントロールおよび軽減の方針、プロセス、手続について検討した。ITGP6 の内容は、以下の通りである。

情報管理と情報技術を、リスクの統制および削減に関する適切な方針、プロセス、手続に基づいて統治すべきである。実務者、内部監査人および金融専門家に対して、組織のGRCフレームワークに一致したガイダンスを示すべきである。

達成目標の設定にあたっては、CobiTの成熟度レベルを参照した。関連性があるとみなされた成熟度レベルとその内容は、次の通りである。

- 成熟度 3—定められたプロセスがある
 - － マネジメント層は、ポリシー、計画、および手続のフレームワークを含む完全な情報コントロールと品質管理の環境を作成し、文書化および周知している。
 - － ポリシーの作成プロセスは体系化され、維持されており、スタッフに周知されている。既存のポリシー、計画および手続もある程度信頼できるものであり、重要事項も網羅されている。
 - － マネジメント層は、ITセキュリティ意識の浸透の重要性を認識しており、セキュリティ意識向上プログラムを導入している。
 - － セキュリティ意識向上のための技法が、標準化および正式化されている。
- 成熟度 4—管理され、測定が可能である
 - － マネジメント層は、内部統制のポリシーの周知に関する実行責任を負っており、重大な変更に合わせて環境の整備に必要な資源の割り当て、および実行責任の委譲を行っている。
 - － 品質およびITセキュリティに関する意識向上を確実にする、建設的かつ事前対応的な情報統制環境が確立されている。
 - － 社内の優れた実践方法(手法)を組み合わせて完成された一連のポリシー、計画、および手続が作成、維持、周知されている。
 - － それらを展開し、その後のコンプライアンス状況を確認するフレームワークが確立されている。
- 成熟度 5—最適化
 - － 情報統制環境は、戦略管理フレームワークおよび構想との整合性が確保されており、頻繁に見直しおよび更新が行われ、継続的に改善されている。
 - － モニタリング、セルフ評価、およびコンプライアンスチェックは、組織内に浸透している。
 - － ポリシーおよび知識ベースを保守し、情報周知を最大限に図るために、OAツールとCBTツール(コンピュータを利用した研修ツール)など、関連技術が駆使されている。

周知方法の改善策として、以下の事項が検討された。

- 実現不可能なベストプラクティスではなく、既存の優れた実務や将来の望ましい実務を対象とするものであること。
- 全社的な周知方法に統合されること。
- 手間や時間を極端に必要としないこと。
- 例えば、ポリシーが読まれ、理解されているなど、コンプライアンスの状況を明示できるものであること。
- コンプライアンスの状況が測定可能であること。

以下のような対策が考えられる。

- 従来の方針や手続の範囲と妥当性を見直し。ギャップが特定された場合、方針や手続は、更新されるか、新たに作成される。
- 年に1度の方針や手続の見直しや、その承認をするという方針が実行される。
- すべての方針と手続が、イントラネットに掲載される。
- 全従業員が、方針や手続の変更について、イントラネットを利用した更新研修を受けるよう求められる。この研修では、ポリシーと手続の変更点や要点についての自動化されたテストが行われる。テストには、合格の最低点が設定される。

次の測定指標が用いられる可能性がある。

- 年に1度の承認期限から、1ヶ月以上、見直しもしくは承認が遅れている方針や手続の数。
- 期限から2週間以内に、イントラネットを利用した更新研修を修了していない従業員の数や割合。
- 不正解だった質問数の割合分布で示されたテスト結果。

DS5 システムセキュリティの保証

この項目は、全体的なセキュリティ計画に統合されると考えられる。この事例の目的は、統合されたセキュリティ計画の実施方法を示すことではない。思考プロセスの特徴を示すことである。

DS5の内容は、以下のとおり。

情報のインテグリティを維持し、IT資産を保護するためには、セキュリティ管理のプロセスが必要である。このプロセスには、ITセキュリティに関する役割と責務、ポリシー、標準、および手続を定め、それらを運用、改善することが含まれる。また、セキュリティ管理には、セキュリティのモニタリングと定期的なテストの実施、および識別されたセキュリティの弱点やインシデントに対する是正措置の導入も含まれる。セキュリティ管理を効果的に実行することで、すべてのIT資産を保護し、セキュリティの脆弱性やインシデントがビジネスに与える影響を最小限に抑えることができる。

達成目標の設定にあたっては、CobiTの成熟度レベルが参照された。関連性があるとみなされた成熟度レベルとその内容は、次の通りである。

- 成熟度 4—管理され、測定が可能である：
 - ITセキュリティの責任が明確に割り当てられ、管理、実行されている。
 - ITセキュリティのリスクと影響に関する分析が、一貫して行われている。
 - セキュリティポリシーと手続が、具体的なセキュリティ基準に従って実施されている。
 - セキュリティ意識の向上に向けた取り組みには、全員の参加が義務付けられている。
 - ユーザの識別や、認証、認可が標準化されている。
 - セキュリティテストは、正式な標準プロセスに従って実施され、それがセキュリティレベルの向上につながっている。
 - ITセキュリティプロセスと組織全体のセキュリティ機能との調整が図られている。
 - ITセキュリティに関する報告と、ビジネス目標との関連付けが行われている。
 - ITセキュリティに関する研修が、ビジネス部門とIT部門の双方において行われている。

- ITセキュリティに関する研修が、義務上の要請や文書化されたセキュリティリスク分析結果に対応する形で、計画、管理されている。
- 成熟度 5—最適化:
 - ITセキュリティは、ビジネス部門とIT管理部門の共同責任であり、企業のセキュリティに関するビジネス目標に組み込まれている。
 - ITセキュリティ要件が、明確に定義および最適化されており、承認されたセキュリティ計画に盛り込まれている。
 - ユーザと顧客は、セキュリティ要件の定義に対してますます大きな説明責任を負い、設計段階からセキュリティ機能がアプリケーションに組み込まれている。
 - セキュリティインシデントへの対応は、自動化ツールを利用した正式なインシデント対応手順に基づいて、迅速に行われている。
 - 定期的なセキュリティ評価が行われ、導入したセキュリティ計画の有効性が評価されている。
 - 脅威および脆弱性に関する情報が、体系的に収集・分析されている。
 - リスクを軽減するための適切なコントロールが、直ちに伝達され、実施されている。
 - セキュリティテスト、インシデントの根本原因の分析およびリスクを積極的に発見することで、継続的にプロセスを改善している。
 - 組織全体で、セキュリティプロセスと技術の統合が図られている。
 - セキュリティ管理に関する測定指標が計測、収集、周知されている。
 - マネジメント層は、これらの測定結果を用いて、セキュリティ計画を継続的に改善している。

この項目に関して検討された対策は広範囲にわたり、本書の範囲を超えている。ただし、次の点については検討に値する。

- 認証の取得、独立した評価、自己評価などを含む、ISO 27000 の考え方の利用。
- セキュリティ戦略の立案。現実的には、IT インフラと、ソーシャルエンジニアリングなどの社会的インフラに関連するすべての要素について、発生する可能性がある事象をモニタリングすることは不可能である。モニタリングの対象とすべき、インフラと関連する事象を識別する必要がある。
- 事象の種類を分類すべきである。最も重要な事象は、携帯電話とEメールで、特定の部門に報告されるであろう。それほど重要でない事象は、個別あるいは日次のサマリーレポートとして、Eメールによって報告されるであろう。最も重要性の低い事象は、記録されないか、ログは取っても報告の対象とはならない、または、傾向分析のために定期的なサマリーレポートとして報告されるかのいずれかであろう。
- セキュリティパッケージの欠陥の発覚など、内部不正に利用される可能性のある外部事象のモニタリング。

COBIT では、検討対象となる測定指標の例として、以下の項目を挙げている。ただし、実際に使用される測定指標は、組織によって異なるものである。

- セキュリティ要件を満たしていないシステムの数
- アクセス違反の疑いのあるおよび実際のアクセス違反の数とタイプ
- 職務分掌違反の数
- パスワード標準を遵守していないユーザの割合

- 阻止された悪意のあるコードの数とタイプ
- モニタリングすべきセキュリティイベントのタイプの確認とタイプごとの発生頻度
- 使われていないアカウントの数とタイプ
- 許可されていないIPアドレスとポートの数、拒否されたトラフィックタイプの数
- 侵害されて失効となった暗号鍵の割合
- 許可、取り消し、リセット、変更されたアクセス権の数

これらの指標には、測定可能な達成目標、および達成目標への進捗を示す指標が含まれる。

DS9 構成管理

DS9 の内容は、以下のとおりである。

ハードウェアとソフトウェアの構成のインテグリティを確保するには、正確かつ網羅された構成管理用リポジトリの作成と保守が必要である。このプロセスには、初期構成情報の収集、ベースラインの設定、構成情報の検証と監査、および必要に応じた構成管理用リポジトリの更新が含まれる。効果的な構成管理により、システムの可用性が向上し、本番システムでの課題が最小限に抑えられ、課題を速やかに解決できるようになる。

達成目標の設定にあたっては、CoBIT の成熟度レベルが参照された。関連性があるとみなされた成熟度レベルとその内容は、次の通りである。

- 成熟度 4—管理され、測定可能である
 - 構成管理の必要性が組織内のすべてのレベルで認識されており、優れた実践基準の継続的な改善が図られている。
 - 手順と標準が周知され、研修に組み込まれている。逸脱について、モニタリング、追跡、および報告されている。
 - 自動化ツール(プッシュ技術など:ブロードキャストされる情報をクライアント側で解釈、表示する技術の総称)が標準の施行と安全性の向上に活用されている。
 - 構成管理システムはほとんどのIT資産に対応しており、適切なリリース管理と配付コントロールを可能にしている。
 - 物理的検証に加え、例外分析が一貫して実施されており、例外の根本原因が調査されている。
- 成熟度 5—最適化
 - ベースラインに関する監査レポートには、各装置の修理、保守、保証、アップグレード、および技術評価に必要な、ハードウェア/ソフトウェアに関するデータが記載されている。
 - 許可されていないソフトウェアのインストールを制限する規則が徹底して施行されている。
 - 資産について追跡し、個々のIT資産をモニタリングすることで、これらの資産を保護し、盗難、誤用、悪用を未然に防止している。

以下のような対策が考えられる。

- ライセンスのない、または、許可されていないソフトウェアの使用やコピー — サーバとワークステーションを定期的に調査し、許可されていない、またはライセンスを受けていない可能性のあるソフトウェアやファイルタ

IPを特定する。

- ワークステーションの盗難、または許可されていない装置の接続 — ワークステーションは、一元管理されたワークステーションの一覧表と比較し、相違を調査する。ネットワークに接続される全ての装置を対象とした標準規格を整備し、適用する。例えば、自宅のコンピュータは、認定された最新のアンチウイルスソフトをインストールしなければならない、などの対策が含まれる。

CoBIT では、検討対象となる測定指標の例として、以下の項目を挙げている。ただし、実際に使用される測定指標は、組織によって異なるものである。

- 不適切な資産構成に起因するビジネス上のコンプライアンスに関する問題の数
- 構成管理用リポジトリと実際の資産構成との間で確認された相違の数
- リポジトリ内の、購入済ライセンスと所在不明ライセンスの割合

そのほかに、以下の測定指標も検討に値する。

- インストールされたライセンス製品の数
- サーバでのみ使用されるべきライセンス製品が、ワークステーションにインストールされている数
- 標準外の製品のインストール数、およびライセンスを受けていない可能性のある製品のインストール数
- 地域別や部門別の報告

付録Ⅷ—参考文献

Accord Implementation Group (Operational Risk) (AIGOR), “Observed Range of Practice in Key Elements of Advanced Measurement Approaches (AMA),” October 2006

Bank Systems and Equipment, “Basel II Converges With Business Performance,” October 2004

Basel Committee on Banking Supervision, Principle 1—Framework for Internal Control Systems in Banking Organisations, September 1998

Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards, June 2006, www.bis.org/publ/bcbs107.htm

Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, February 2003, www.bis.org/publ/bcbs91.htm

BearingPoint, “Basel II Operational Risks,” June 2005

BearingPoint, “Data Quality: A Stumbling Block to Basel Compliance,” March 2006

British Standards Institution (BSI), BS 25999-1 “Business Continuity Management,” 2006

British Standards Institution (BSI), PAS 77 “IT Service Continuity Management,” 2006

Business Continuity Institute (BCI), Good Practice Guidelines for Business Continuity Management, 3rd Edition, 2007

COSO, Enterprise Risk Management—Integrated Framework, September 2004, www.coso.org/publications.htm

International Organization for Standardization (ISO), ISO 27001 “Information Security Management Systems—Code of Practice,” 2006

IT Governance Institute, COBIT 4.1, USA, 2007 (Source of figure 14.)

IT Governance Institute, IT Control Objectives for Sarbanes-Oxley, 2nd Edition, 2006 (Source of figure 8.)

Joint Forum, “High-level principles for Business Continuity,” August 2006

KPMG Financial Services, “Basel II—A Closer Look: Managing Operational Risk,” 2003 (Source of figures 4 and 13.)

Office of Government Commerce (OGC), IT Infrastructure Library® (ITIL), UK

Paisley Consulting, “The Case for Operational Risk Management,” February 2006

PricewaterhouseCoopers, “Basel II: Making It Work for You,” March 2004

Symantec, “Risk Management Challenge and Basel II,” May 2006