TOKIO MARINE

リスクマネジメント最前線

2025 | No.12

GRC（ガバナンス・リスク管理・コンプライアンス）のあり方

ビジネスリスク本部　青島　健二　上級主席研究員（専門分野：経営管理、業務/IT 改革、ERM）
ビジネスリスク本部　八代　慈瑛　研究員（専門分野：経営管理、リスク管理、経済安全保障）

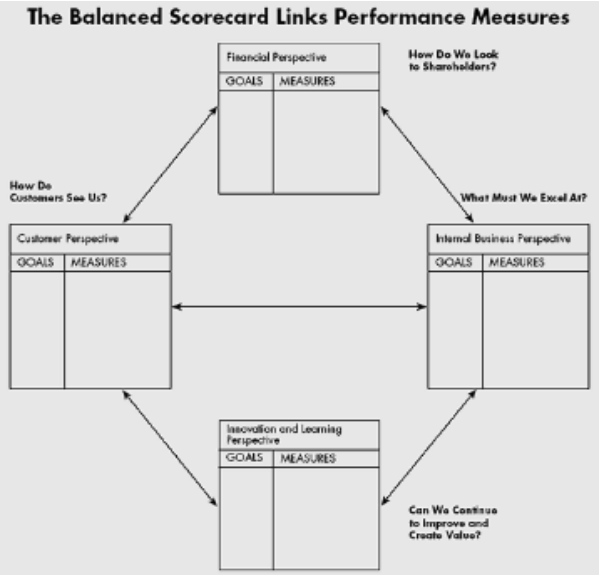
現在、社会からの様々な要請により、企業では GRC（ガバナンス・リスク管理・コンプライアンス）に関連する多くの委員会等が設置されている。一方で、これら委員会の活動は互いの領域がやや重複しており、またどの委員会もカバーしていない領域も存在する。そのような状況の中で、企業を揺るがすようなインシデントも起きており、GRC の取り組みの連携がその重要性を帯びている。本稿では欧米の取り組み事例を紹介しながら、GRC のあり方や GRC への移行方法について提言したい。

1. GRC（ガバナンス・リスク管理・コンプライアンス）連携の必要性

(1) バランスド・スコアカード・経営管理の枠組みにおける GRC の位置づけ

企業活動は、売上や利益、株主配当等、各種の経営目標を達成するために行われる活動といえる。この企業活動を評価するためのフレームワークとして、「バランスド・スコアカード（Balanced Scorecard：BSC）と呼ばれる手法があり、「財務」「顧客」「内部プロセス」「学習と成長」という 4 つの視点を用いる。1992 年にロバート・キャプラン（Robert Samuel Kaplan）とデビッド・ノートン（David P. Norton）両氏が Harvard Business Review 誌で発表した概念であるが、30 年以上が経過した現在においても、色あせることはない。

■　図 1　バランスド・スコアカード

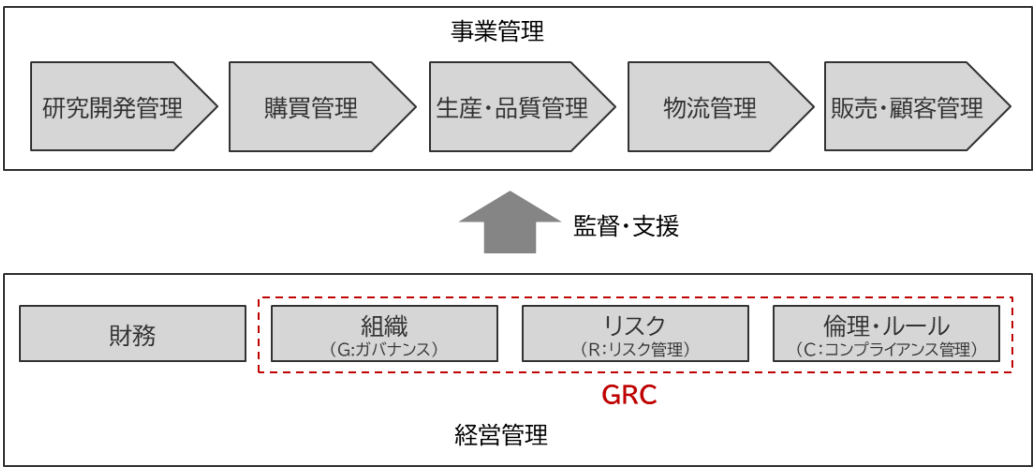


（出典：The Balanced Scorecard—Measures that Drive Performance Harvard Business Review）

4 つの視点の一つである「内部プロセス」は、株主や顧客を満足させるために、目標達成に貢献する社内の業務プロセスを構築・改善する評価視点であり、評価指標（KPI）としては、生産性向上、コスト削減等に関する管理指標を設定する。この点において、内部プロセスの視点とは「経営管理」そのものであると捉えることができる。

経営管理という用語に正式な定義は無いが、企業経営における管理にはコーポレート部門における「経営管理」と、事業部門における「事業管理」がある。このうち、コーポレート部門における、財務分野を除く管理分野が「GRC」に該当する部分であると本稿では定義する。

■ 図 2 経営管理における GRC の位置づけ



（筆者作成）

(2) 経営管理（GRC 部分）の歴史的発展とその結果生じている問題

GRC は、歴史的には 1930 年代のガバナンス（「所有と経営の分離」に関する研究と適用）に端を発している。その後、1950 年代に入りガバナンスから分化する形でリスク管理（損失低減のための「ロスコントロール」の活動）が萌芽し、1970 年代に入り、リスク管理から分化する形でコンプライアンス（汚職・腐敗防止の活動）が発展し始めた（表 1 参照）。大規模組織では現在、ガバナンス、リスク管理、コンプライアンスの各専門部門が独立して存在し、それぞれが個別に活動することが一般的である。

■ 表 1 経営管理における GRC の位置づけ

ガバナンス				リスク管理				コンプライアンス			
時代	年代	主要な出来事・制度	背景・特徴	時代	年代	主要な手法・制度	背景・特徴	時代	年代	主要な法制度・事件	背景・特徴
萌芽期	1930 年代	所有と経営の分離論	バーリ&ミーンズによる理論、株主と経営者の利害対立								
				伝統期	1950 年代	損害保険から派生するロスコントロール	火災・事故等の物理的リスクへの対応				
発展期	1970 年代	エージェンシー理論	株主利益の最大化、経営者監視の必要性	拡張期	1970 年代	統合的リスク管理の概念	財務リスクを含む包括的アプローチ	規制対応期	1970 年代	海外腐敗行為防止法（米国）	国際的な贈収賄防止の始まり
					1980 年代	VaR（Value at Risk）開発	金融リスクの定量化手法		1980 年代	インサイダー取引規制強化	証券市場の公正性確保

©2025 Tokio Marine dR Co., Ltd. All rights reserved.

<table>
<tr><th colspan="4">ガバナンス</th><th colspan="4">リスク管理</th><th colspan="4">コンプライアンス</th></tr>
<tr><td rowspan="4">制度化期</td><td>1990年代</td><td>キャドバリー報告書（英国）</td><td>取締役会の独立性、監査委員会設置</td><td rowspan="5">体系化期</td><td>1990年代</td><td>デリバティブリスク管理</td><td>金融工学の発達、複雑な金融商品への対応</td><td rowspan="3">制度整備期</td><td>1990年代</td><td>独占禁止法強化（日本）</td><td>公正取引委員会の権限拡大</td></tr>
<tr><td>2002年</td><td>SOX 法（米国）</td><td>エンロン事件後、内部統制強化</td><td>1998年</td><td>金融ビッグバン（日本）</td><td>金融規制の大幅緩和と監視強化</td></tr>
<tr><td>2003年</td><td>日本版 SOX 法検討開始</td><td>米国に追随した制度整備</td><td rowspan="3">企業責任期</td><td rowspan="2">2000年代</td><td rowspan="2">雪印、三菱自動車事件等（日本）</td><td rowspan="2">企業不祥事の続発、社会的責任の重視</td></tr>
<tr><td rowspan="4">強化期</td><td>2006年</td><td>金融商品取引法（日本）</td><td>内部統制報告制度導入</td><td>2004年</td><td>COSO-ERM フレームワーク</td><td>全社的リスク管理の標準化</td></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td></td><td></td><td></td><td rowspan="2">厳罰化期</td><td>2006年</td><td>会社法施行（日本）</td><td>内部統制システム構築義務</td></tr>
<tr><td rowspan="3">高度化期</td><td>2008年</td><td>リーマンショック後の規制強化</td><td>システミックリスクへの対応</td><td>2009年</td><td>公益通報者保護法施行（日本）</td><td>内部告発制度の法制化</td></tr>
<tr><td>2015年</td><td>コーポレートガバナンス・コード（日本）</td><td>攻めのガバナンス、社外取締役増加</td><td rowspan="2">2010年代</td><td rowspan="2">サイバーセキュリティリスク</td><td rowspan="2">デジタル化に伴う新たなリスク領域</td><td rowspan="2">グローバル化期</td><td rowspan="2">2010年代</td><td>GDPR（EU 一般データ保護規則）</td><td>個人データ保護の国際標準</td></tr>
<tr><td colspan="4" rowspan="2"></td><td colspan="2" rowspan="2"></td><td>贈収賄防止法の域外適用拡大</td><td>米国 FCPA、英国贈収賄防止法等</td></tr>
<tr><td>2020年代</td><td>パンデミックリスク、ESG リスク</td><td>COVID-19、気候変動等の新興リスク</td><td rowspan="2">デジタル対応期</td><td rowspan="2">2020年代</td><td>デジタルプラットフォーム規制</td><td>GAFA 規制、デジタル課税</td></tr>
<tr><td colspan="4"></td><td>ESG 関連規制</td><td>気候変動開示、人権デューデリジェンス</td></tr>
</table>

（各種調査を踏まえ、筆者作成）

しかしながら、最近までそれぞれの領域について公的に定義されたものは存在せず、また、私的な機関（シンクタンクやコンサルティング会社、大学等）がそれぞれに定義している 3 つの領域の境目には違いがみられていた。そのため、各組織内において GRC それぞれの組織が活動を活性化していくと、ガバナンス担当部門とリスク管理担当部門、コンプライアンス担当部門との間に取り組み領域の重複がみられ、その現象は時に、現場部門に対して無用な負荷を与えるという弊害を起こすことがある。例えば、以下のような状況は、多くの組織において心当たりがあるのではないだろうか。

- **ガバナンス部門が毎年行う役員ヒアリングの中に、役員の法令順守性を確認する事項がある**（コンプライアンス領域と重複）
- **リスク管理部門が毎年行うリスクアンケートにおいては、法令違反に関するリスクシナリオとその影響度、発生頻度に関する回答を求めている**（コンプライアンス領域と重複）
- **コンプライアンス部門が実施する自主点検の項目内に、役員の裁量に関する確認事項が含まれている**（ガバナンス領域と重複）

©2025 Tokio Marine dR Co., Ltd. All rights reserved.

また、それら取り組みの成果は「売上増」というような目に見えるものとならないため、現場部門の中にはガバナンスとリスク管理、コンプライアンスそれぞれの組織活動が生み出す成果を懐疑的に捉え、GRC 組織からの依頼事項に対しある意味「適当」に対応している実態も存在する。それは本来経営管理の重要な一翼を担う GRC の形骸化につながりかねない状況を生み出している。

コラム：クレディ・スイス銀行で発生した“アルケゴス事件”[1]

アルケゴス事件とは、2021 年 3 月の富裕層向け資産管理会社「アルケゴス・キャピタル・マネジメント」（Archegos Capital Management）の破綻により世界の大手金融機関に総額約 100 億ドルの損失をもたらした事件である。この事件においてクレディ・スイス銀行では約 55 億ドルという財務的損失にとどまらず、組織全体の根本的な見直しを迫られることとなり、最終的には 2023 年に UBS による救済買収という結末につながる一因となった。同事件に関する同社の公式調査報告書は、ガバナンス・リスク管理・コンプライアンスの 3 機能が形式上は整備されていたものの相互に連動せず、縦割りのまま重複・断片化していた結果、組織全体としてリスクを把握・制御できなくなっていたという実態を指摘した。具体的には以下の通りである。

- ガバナンス：投資銀行部門およびリスク部門において「監督責任の十分な履行がなされず」「リスク報告のエスカレーションが欠如していた」と指摘されている。アルケゴス社との取引、リスク限度の逸脱は複数の委員会や管理組織で指摘されていたが、最終的な判断権限や監督主体が曖昧であったため、明確な統制が及ばなかった。これは、組織内でガバナンス機能が重層化しながらも接続されず、有効性が損なわれた結果といえる。
- リスク管理：アルケゴス社が恒常的に各種リスク限度（Potential Exposure 等）を逸脱していたにもかかわらず、是正措置が遅延・放置された事実が複数指摘されている。さらに、第一線である Prime Services Risk（PSR）と第二線である Credit Risk Management（CRM）の間には情報の壁が存在し、顧客の重要情報が共有されない状態にあった。このように、本来一体として機能すべきリスク管理が縦割り構造により分断され、実質的に機能不全へ陥っていたといえる。
- コンプライアンス：レピュテーショナルリスク審査（Reputational Risk Review）に欠陥があり、効果を発揮していなかった（flawed and ineffective）ことが指摘されている。アルケゴス社の過去のインサイダー取引事件を認識しつつ、将来取引に対する実質的な制限や条件を課すことなく承認が繰り返されていた。ここでもガバナンス・リスク管理・コンプライアンスの連携が不十分で、各機能が形式的に存在しながら互いに作用しない縦割りによる弊害が如実に表れている。

最終的に調査報告書は、アルケゴス事件が個別の不正によるものではなく、「組織横断的なリスク管理・監督の欠陥によって生じた」と結論付けている。すなわち、G・R・C 各機能が独立に整備されながら、その接続・統合が不十分であったため、複雑化したリスクを全体として把握できず、重大な損失へとつながったのである。

[1] 参考文献：UNITED STATES SECURITIES AND EXCHANGE COMMISSION, REPORT OF FOREIGN PRIVATE ISSUER PURSUANT TO RULE 13a-16 OR 15d-16 UNDER THE SECURITIES EXCHANGE ACT OF 1934 ,July 29,2021

©2025 Tokio Marine dR Co., Ltd. All rights reserved.

2．MECE(Mutually Exclusive and Collectively Exhaustive) な GRC 体制の実現

(1) 筆者の考える GRC の定義

ガバナンス、リスク管理、コンプライアンスについて、内部監査の国際機関である内部監査人協会（IIA：The Institute of Internal Auditors）は、2024 年 9 月に発行した「グローバル監査基準」（The Global Internal Audit Standards）内で以下のように定義した。ガバナンスは事業目標達成のために組織体を最適化する取り組み、リスク管理は事業目標達成のための組織体の取り組みを担保する取り組み、コンプライアンスは事業目標達成の前提として組織体が遵守する取り組みであるとするこの定義は、比較的分かりやすい。

- **ガバナンス**
  組織体の目標達成に向けて、組織体の活動について、情報を提供し、指揮し、管理し、及びモニタリングするために、プロセスと組織構造を併用して実施すること。
- **リスク管理**
  組織体の目標達成に関し合理的なアシュアランスを提供するために、発生する可能性のある事象又は状況を、識別、評価、管理、コントロールするプロセス。
- **コンプライアンス**
  法令、規制、契約、方針、手続及びその他の要求事項を遵守すること。

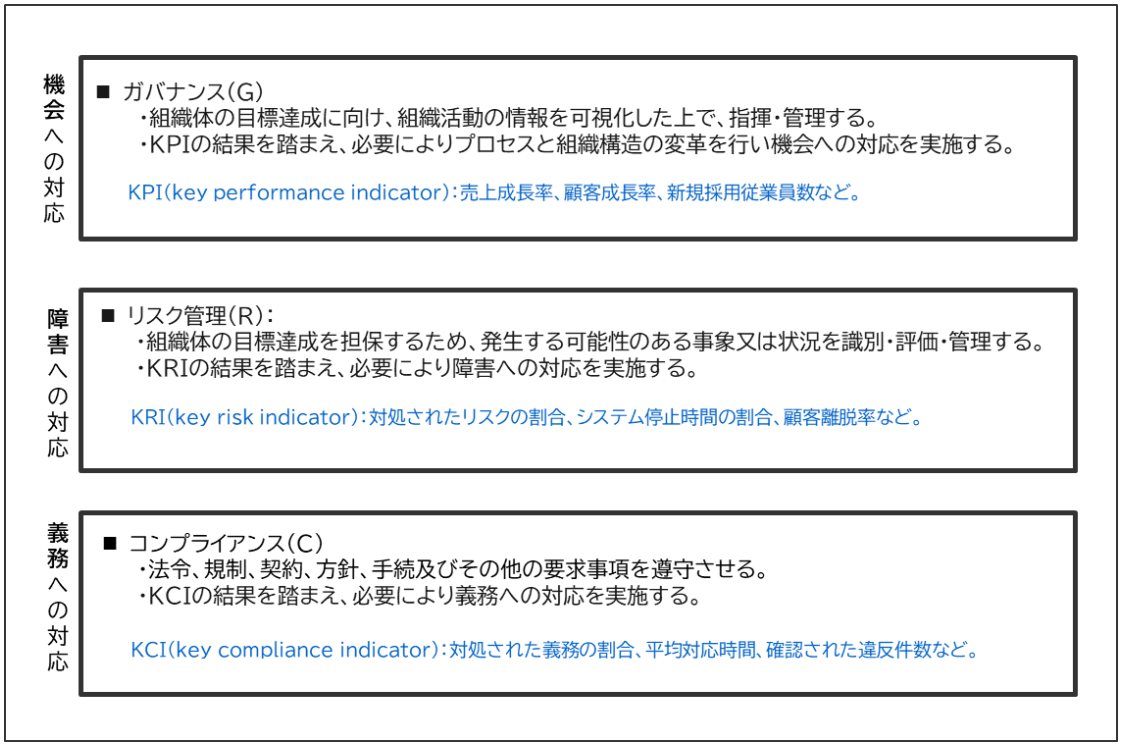
また、2007 年に企業のガバナンス・リスク管理・コンプライアンスを統合的に管理する概念として GRC を提案した米国の NPO 法人・OCEG（the Open Compliance and Ethics Group）は、効果測定の観点で GRC それぞれの活動を以下の関係性で整理した。

- **ガバナンス**（の結果としてのパフォーマンス）
  機会への対応がどの程度うまくいっているかの評価指標として、KPI(key performance indicator)を用いる。例えば、売上成長率、顧客成長率、新規採用従業員数等。
- **リスク管理**
  障害への対応がどの程度うまくいっているかの評価指標として、KRI(key risk indicator)を用いる。例えば、対処されたリスクの割合、システム停止時間の割合、顧客離脱率等。
- **コンプライアンス**
  義務への対応がどの程度うまくいっているかの評価指標として、KCI(key compliance indicator)を用いる。例えば、対処された義務の割合、平均対応時間、確認された違反件数等。

これらを踏まえ、筆者においては GRC の関係性を図 3 の通り整理したい。これが、MECE(Mutually Exclusive and Collectively Exhaustive（お互いに重複せず、全体を網羅する)）となる GRC の定義と考える。

©2025 Tokio Marine dR Co., Ltd. All rights reserved.

■ 図 3 筆者の考える GRC の関係性



(筆者作成)

(2) 3 ラインディフェンスの思想下での GRC 組織統合

3 ラインディフェンスとは、2013 年に IIA と COSO（トレッドウェイ委員会支援組織委員会：Committee of Sponsoring Organizations of the Treadway Commission）が共同で公表したもので、現在、この概念は企業における管理一般の概念として展開されており、GRC の各領域においても多くの大企業では以下のように 3 ラインディフェンスが実践されている。

■ **第一線**

現場部門（例：事業部、工場、営業所等）における管理

■ **第二線**

管理部門における、第一線に対する管理、指導

■ **第三線**

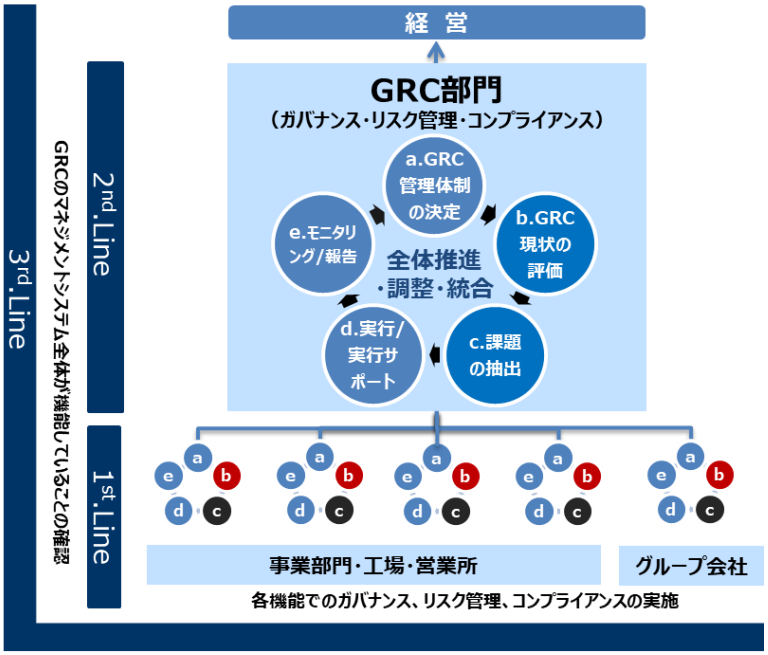
第一線と第二線の全体が経営管理体制として問題が無いことの確認、指摘

第一線（現場部門）、及び第三線（内部監査部門）は一意であるが、日本において問題なのは第二線が一意でなく複線化していることにある。第二線に「経営管理部門」や「内部統制部門」「リスク管理部門」「法務部門」「コンプライアンス部門」が乱立し、時に重複した管理・指導を行っていることが非効率を生み出しており、管理・指導の受け手である第一線に無用な負担を強いている傾向がみられる。また、第三線が内部監査を行う上でも、第二線の職掌が不明瞭なために、起きている問題はどこの部門に起因している問題であるのか指摘しきれないといった状況や、例えば生成 AI 等新たな技術が出現した際に第二線のどこが管理のガイドラインを発するべきであるのかを即時に決められず、いつまで経っても現場が利用することができないといった

©2025 Tokio Marine dR Co., Ltd. All rights reserved.

状況が生まれている。したがって、第二線における GRC 関係組織を一元化することによって、望ましい GRC 体制が実現するものと筆者は考える。

■ 図４　筆者の考える、望ましい GRC 体制



（筆者作成）

(3) 欧米における GRC 普及の背景とそれを支えるツール

一方で、それまでＧ・Ｒ・Ｃの各担当部門がそれぞれの体制、手法、様式等を用いて実行してきた状況を統合するにあたり、主導権争いや統合の拒絶等、当該組織間における様々な抵抗が生まれるのは想像に難くない。この障壁に対し欧米では、第三線である内部監査部門が、複線化している第二線の問題を課題として経営に提起するとともに複線化している第二線を単線にするためのツールの存在が GRC の実現を担保し GRC 体制への移行を後押ししているように思われる。例えば、米国の GRC ツールの一つである AuditBoard[2]は、その名の通り監査部門からのツール導入を企図して名づけられており、監査部門から導入が始まり、そこから第二線、第一線へとツールの共同利用の範囲を広げ、最終的にツールドリブンで GRC 統合が進む結果をもたらしているようである。GRC ツールの世界市場は今や 440 億ドル（約 6 兆円）の市場規模に拡大しているが、GRC ツールには以下のようなベネフィットが存在することもその背景にあると推察する。

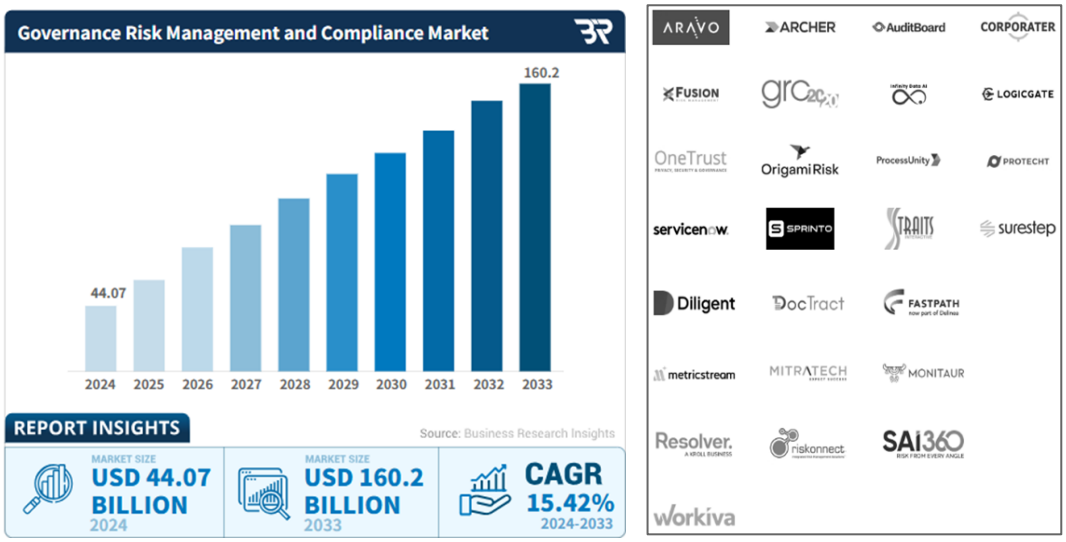
- **特にグループ会社を 100 社以上有するような大企業においては、EXCEL 等による労働集約的な手法での管理をツールによる管理に切り替えることにより、担当スタッフがより価値の高い業務（組織改革の検討やリスク対策の立案等）に集中できる。**
- **GRC 各分野におけるアンケート等が標準化、統合化されるため収集されたデータの整理・分析が容易となる。また、各分野でアンケートを行うことが無くなるため、現場部門へ強いる負担が軽減する。**

[2] AuditBoard の採用企業は Estée Lauder Companies、United Bankshares, Inc.、University of Calgary、Ascot Group など大手企業が多い。

©2025 Tokio Marine dR Co., Ltd. All rights reserved.

- **取締役や執行役に報告するための UI（User Interface）がより簡素となり、GRC における現状を経営が一瞥して判断できるようになる。**
- **コミュニケーションツールとしての機能を使用すると、問題が顕在化した際の関係者間での共有・対策検討がよりスムーズに進むようになる。**

■ 図 5　GRC ツールの市場規模（左）と参入ベンダー（右）



（出所：https://www.businessresearchinsights.com）

■ 図 6　AuditBoard のツールイメージ（左から、ガバナンス、リスク管理、コンプライアンスに関する画面）

（出所：https://auditboard.com/）

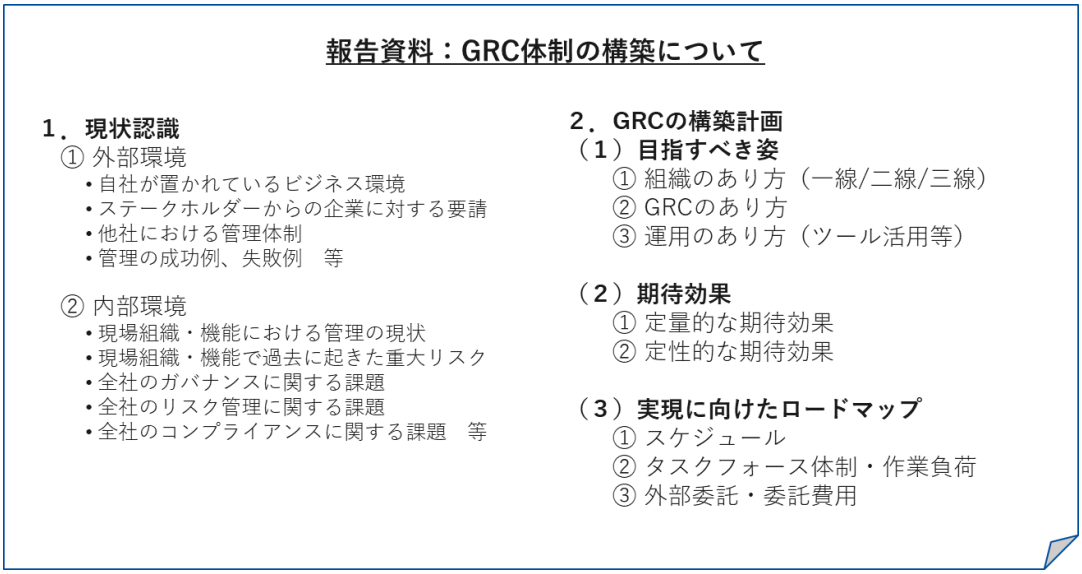
3．GRC 組織への移行にむけた手順

(1) GRC 体制のグランドビジョン策定

繰り返しになるが、それまでＧ・Ｒ・Ｃの各担当部門がそれぞれの体制、手法、様式等を用いて実行してきた状況を統合するにあたり、主導権争いや統合の拒絶等、当該組織間における様々な抵抗が生まれるのは想像に難くない。ボトムアップで GRC 統合を推進するのは極めて困難であるといえるため、早い段階で経営に上申し、承認を得ることが重要といえる。そのためにはまず、従来の組織体制における問題点を洗い出し、新たな GRC 体制によってその諸問題が解決されることを説明しなければならない。具体的には、以下のようなアジェンダで経営に説明する必要がある。

©2025 Tokio Marine dR Co., Ltd. All rights reserved.

■　図 7　GRC 体制の構築に関する経営への上申資料（目次）



（筆者作成）

なお、経営を説得する上で最も重要となる期待効果は、以下の視点等により整理されるべきものである。

- **第二線において、G・R・Cに関連する部門間重複が解消されることによる工数・コスト削減効果と、重複感の解消により余裕が生まれた各担当がさらなるガバナンス向上、リスク対策の検討、コンプライアンスの新規施策等の高価値を新たにアウトプットすることによる企業全体における生産性向上、コスト削減効果**
- **第一線において、G・R・C各部門から要求される対応事項が一元化されることによる工数・コスト削減効果と、それら社内工数・コストをプロフィットセンターとしての本来業務に向けられることで期待される業績への効果**
- **第三線である内部監査の相手である第二線が単線化することによる、第三線における問題点の鮮明化・指摘精度の向上**
- **GRC ツール内でのダッシュボード機能提供による、経営における問題把握、意思決定のアジャイル化**

(2) GRC 組織への変革ステップ

先述したグランドビジョン作成から、経営への上申を終え、GRC 体制の構築/再構築を経て最終的に GRC 体制の運用を開始するまでのステップは以下の通りである。

【ビジョン】GRC 体制のグランドビジョン策定

・外部環境、内部環境に関する調査・分析を行い、GRC 体制への移行による効果を検討・試算する。また、既存のG・R・C体制を統合化された GRC 体制へ移行するための計画を策定し、経営に上申する。

©2025 Tokio Marine dR Co., Ltd. All rights reserved.

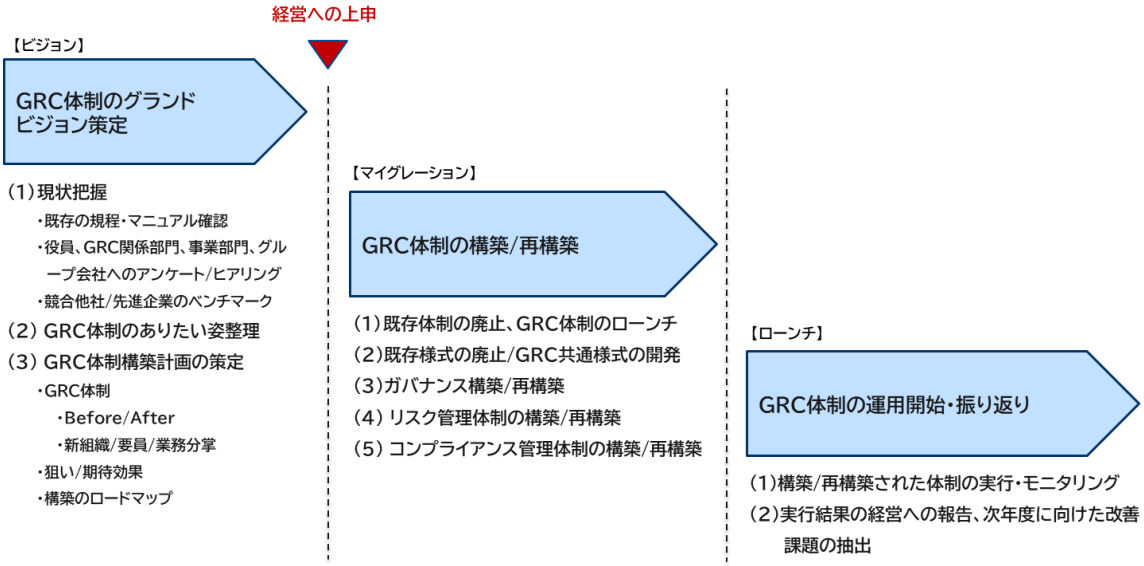
【マイグレーション】GRC 体制の構築/再構築

・GRC 体制への移行に関する経営の承認を取り付けた後に、移行計画に従って既存体制・業務・様式を廃止し新たな体制・業務・様式を構築する。

【ローンチ】GRC 体制の運用開始・振り返り

・構築された体制の運用を開始するとともに運用状況のモニタリングを行い、経営に報告する。また、GRC 統合後に起きている問題を把握し、次年度課題として解消のための対策を検討する。

■ 図 8　GRC 組織への変革ステップ（俯瞰図）



（筆者作成）

4．まとめ

近年、GRC（ガバナンス、リスク管理、コンプライアンス）各取り組みの重複はサステナビリティや人権、サイバーセキュリティ、さらには経済安全保障といった個別取り組みの必要性も相まってさらに混沌としている。そのような個別取り組みを実行するにあたっては、闇雲に新たな内部プロセスを作るのではなく、GRC という統合化された枠組みの中での実行を念頭に置くことが MECE な管理部門を維持するキーポイントと考える。G・R・C の統合化は既に国内でも大手製造業を中心にはじまっており、今後のトレンドになっていくものと筆者は考える。

[2025 年 12 月 9 日発行]

東京海上ディーアール株式会社

ビジネスリスク本部　青島 健二　上級主席研究員
ビジネスリスク本部　八代 慈瑛 研究員
〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23F
Tel. 03-5288-6594 www.tokio-dr.co.jp

©2025 Tokio Marine dR Co., Ltd. All rights reserved.