ACLホワイトペーパー

「データ主導型GRC」でリスクを管理する

ガバナンス、リスク管理、コンプライアンス(GRC)プロセスを統合し変革的価値を提供する段階的アプローチ

Dan Zitting, ACL CPO
John Verver, ACL顧問
翻訳監修：谷口 靖美, プロティビティ マネージングディレクタ

目次

概要 **3**

これらが組織にもたらす変化は? **3**

新たなリスク環境 3
ガバナンス、リスク、およびコンプライアンスの方法論の進化 3
テクノロジーによる機能強化 3

組織が目指すものは? **3**

GRCプロセスとテクノロジーの業務上のステークホルダー **4**

3つのディフェンスラインにおけるテクノロジーの活用不足 **4**

第3ディフェンスライン(内部監査)のリスク・コントロールテクノロジーの利用 5
第2ディフェンスライン(リスク、コンプライアンス、経理、IT)のリスク・コントロールテクノロジーの利用 5
第1ディフェンスライン(業務執行)のリスク・コントロールテクノロジーの利用 6

現在の状態から… **6**

…将来の状態へ:「データ主導型GRC」の導入 **6**

必要な機能: 6

GRC関連プロセスのデータ主導型方法論 **7**

ステップ1:シンプルで実務的なGRC方法論を設計する 7
ステップ2:コントロール検証でデータ分析を活用する 7
ステップ3:GRCとデータ分析の方法論を統合する 8
ステップ4:継続的モニタリングを強化してリアルタイムの洞察を得る 9
ステップ5:GRCと継続的モニタリング方法論を統合して「データ主導型GRC」とする 10

テクノロジーソリューション **10**

1. 統合的リスク評価 10
2. プロジェクト・コントロール管理 11
3. リスク・コントロールアナリティクス 11
4. ナレッジコンテンツ 11

GRCテクノロジーチェックリスト **12**

全てのディフェンスラインのリーダー向けの「価値を提供する」テクノロジー成熟モデル **13**

データ主導型GRCによるパフォーマンス管理強化 **14**

まとめ **15**

考慮すべき諸問題: 15

ACLについて **16**

「データ主導型GRC」でリスクを管理する

ガバナンス、リスク管理、コンプライアンス(GRC)プロセスを統合し変革的価値を提供する段階的アプローチ

概要

世界は変化し続けています。ほどんどすべての業界の新たなリスク環境は変わってしまいました。有効なリスクマネジメントの方法論も変わりました(内部監査、外部監査/コンサルティング、コンプライアンス、ERMなど、どの観点から見ても)。そして、テクノロジーそのものが変わりました。テクノロジーの利用者は、より低価格のより使いやすいテクノロジーから、より多くの価値を実現することを期待しています。

これらが組織にもたらす変化は?

新たなリスク環境

リスクは経営トップの関心事です。「変化のスピード」が共通要素となっている経済の中でリスクは迅速にシフトし、グローバル化と自動化がグローバル企業のコアバリューとイニシアチブを変える世界で、全く新しい形のリスクが出現しています。

ガバナンス、リスク、およびコンプライアンスの方法論の進化

不正、コンプライアンス、品質管理、ERM、財務諸表等のさまざまな監査機能に及ぶリスク・コントロール業務全体で、グローバルな組織は、より低いコスト(時間と費用の両方)でより多くのリスクをカバーする必要性を認識するようになり、これが方法論の改革と自動化を推進しています。

テクノロジーによる機能強化

企業IT分野におけるトップ調査会社であるガートナーによれば、クラウド、モバイル、データ、ソーシャルという4つの力の融合が、適切に設計された技術を使ってお互いに情報や情報を交換する際の、個人のエンパワメントを推進していることは明らかです[1]。多くの組織では、これらの3つの変化への組織の変化をうけて、リスク管理の統合的アプローチの開発へと向かう組織的取り組みは、まだ行われていません。今起きている変化を活用し、テクノロジーにとどまらず、人々、方法論、プロセスも含む新しいプログラムを開発する機会です。その目標は、全体的な戦略目的と業務目的に整合したリスク管理と変化への対応の有効性に関して、包括的かつダイナミックな視点を最高経営者に提供することです。

組織が目指すものは?

「**データ主導型GRC**」は、業務とテクノロジーの統合的方法論であり、組織パフォーマンスの信頼性を最大化しながら、新たなリスク環境に対処する機会を劇的に強化します。このペーパーでは、リスクとパフォーマンス管理の両面から変化を活用する重要な機会 — 監査やリスク管理活動の価値を最適化する統合的データ主導型GRCプロセスの構築、サポートツールや技術への投資 — などを考察します。

1 http://www .gartner .com/technology/research/nexus-of-forces/

GRCプロセスとテクノロジーの業務上のステークホルダー

内部監査人協会（IIA）の「有効なリスクマネジメントとコントロールにおける3つのディフェンスライン」モデルは、リスクマネジメントとコントロールにおける「誰が何を」という問題を具体的に取り扱っています。このモデルは、役割と責任から3つの機能を区別して説明しています[2]。

- リスクを管理するリスクオーナー部門（業務執行 – 「第1ディフェンスライン」）
- リスク監視部門（リスク、コンプライアンス、経理、IT – 「第2ディフェンスライン」）
- リスクについての独立したアシュアランス部門（内部監査 – 「第3ディフェンスライン」）

これらの3つのラインの包括的管理が、組織のガバナンスとガバナンス機関の広範な役割となります。

「従来の監査の役割はリスクとコンプライアンスへと拡大し、有効なリスクマネジメントの3つのディフェンスライン（業務管理、リスク管理とコンプライアンス業務、そして内部監査）をサポートするGRCテクノロジーへのニーズを創出しています。3つのディフェンスライン間のギャップの橋渡しが、組織全体のコミュニケーションの改善とGRC活動の統合にとって極めて重要です。」

IIA事務総長兼CEO　**Richard Chambers**

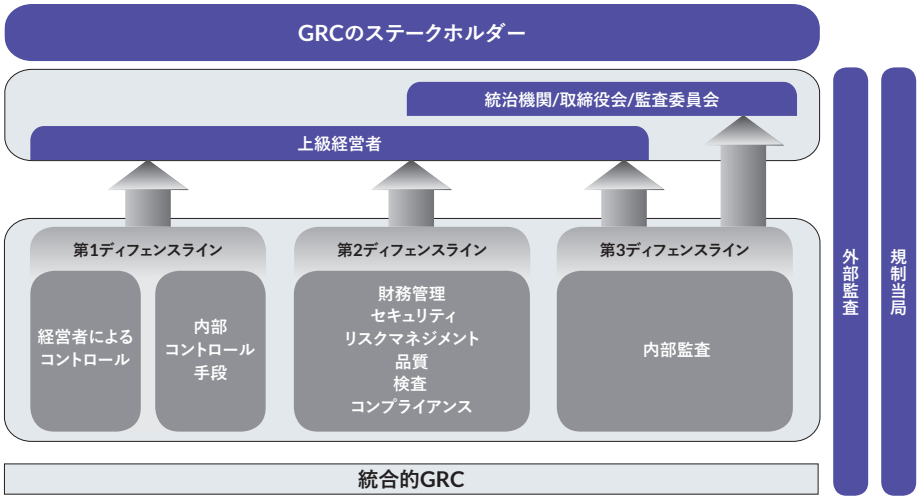

図1：IIA「3つのディフェンスライン」[3]

3つのディフェンスラインにおけるテクノロジーの活用不足

SOX施行以降、多くの組織でリスク・コントロールプロセスにおいて、テクノロジーの活用が始まりました。しかしながら、多くの組織でのリスク・コントロール関連業務では、テクノロジーは未だに部分的または単発的ソリューションとしてしか活用されていません。

2　内部監査人協会（2013）「効果的なリスク管理とコントロールの 3 つのディフェンスライン」
https://na .theiia .org/training/templates/Pages/The-Three-Lines-of-Defense-in-Effective-Risk-Management-and-Control .aspx

3　内部監査人協会から引用（2013）「効果的なリスク管理とコントロールの 3 つのディフェンスライン」
https://na .theiia .org/training/templates/Pages/The-Three-Lines-of-Defense-in-Effective-Risk-Management-and-Control .aspx

第3ディフェンスライン(内部監査)のリスク・コントロールテクノロジーの利用

内部監査人のサーベイでは、この10年間、内部監査人が直面する最も差し迫った問題の一つとしてテクノロジーのより有効な活用が、常に挙げられています。具体的には、監査分析、不正発見、および継続的監査におけるテクノロジーの必要性の増大がサーベイ回答に示されています。他のサーベイでも、監査部門内に十分なテクノロジーとデータ分析スキルが不足していることが示されています[4]。

テクノロジー利用の理由の多くは、監査プロセス自体をより有効かつ効率的にすると同時に、組織の他部門により多くの目に見える価値を提供したいという強い要望です。

この10年間、内部監査業務自体の役割が大きく変わりました。定期的監査と内部統制検証という従来型の内部監査は、リスク全般に対する経営プロセスの有効性の評価と報告が期待される内部監査に進化してきました。これには多くの場合、ビジネスプロセスにおけるリスクマネジメントとコンプライアンスや有効なコントロールシステムを維持していくためのベストプラクティスのガイダンスとコンサルティングをビジネス組織に提供することも含まれます。テクノロジーの利用は、これらのベストプラクティスで重要性を増している要素であり、場合によっては、内部監査が、アシュアランス目的でのテクノロジー利用経験に基づき、ビジネスのリスクマネジメントとコンプライアンスのプロセスに対し、インパクトが強く高い価値を持つテクノロジーの実践を指導することもできます。

内部監査部門がテクノロジーを活用する範囲はかなり多岐にわたります。ただし、内部監査が組織戦略において真に価値の高い有益なものとなるためには、その全体の改善が必要であることは、言うまでもありません。

専門職としての内部監査が、順調にテクノロジーを採用しているというわけではありません。最近の研究では、以下の数字が明らかになっています。

- 監査とドキュメント管理に特化したシステムを使用しているのは、内部監査部門の約40%に過ぎず、残りは、一般的なMicrosoft Office®と共有フォルダーに基づく、組織化されていないツールとプロセスを使用しています[5]。
- 個別のビジネスプロセスや業界の監査プログラムは、今まで使用していたプログラムと、さまざまな監査関係のウェブサイトで公開されているプログラムとを組み合わせて作られていることが多く、こうしたアプローチは、組織固有のリスクには対応できません。
- 次世代検証手法のうち、特にデータアナリティクスは、まだ十分に活用されていません[6]。

第2ディフェンスライン(リスク、コンプライアンス、経理、IT)のリスク・コントロールテクノロジーの利用

監査以外のリスクとコンプライアンス分野では、部門に特化したソフトウェアを使用している組織もありますが、大多数のユーザーは基本的なOfficeツールを使用して、リスクリストの維持、コントロールの文書化、そしてリスク評価を実施しています。より規模の大きい企業では、それぞれ異なる部門や業務に対して、それぞれ異なるテクノロジーとアプローチを使用していることは珍しくありません。こうしたアプローチは、共通のプラットフォームに基づいたものと比較すると、通常、より高コストであり、より低い効率性をもたらしています。

テクノロジーを活用した効果的な検証方法は、通常、利用されず、検討も行われていません。事実、第2のディフェンスラインは多くの場合、アンケート調査のような質問ベースの方法に強く依存しています。こうした方法は、組織におけるリスクの実際の兆候の識別には効果が低いことが証明されています。事業組織がトランザクションの調査またはモニタリングに分析用ソフトウェアを使用している場合は、その多くは、このソフトウェアには、標準的なクエリツールか、一般的なビジネスインテリジェンス(BI)テクノロジーが使われています。BIツールは、概要レベルの情報や傾向を提供する場合には優れてい

4 プライスウォーターハウスクーパース(年間号)「内部監査専門職の状態の調査」
5 AuditNet (2012)「監査人によるテクノロジー使用の状態」
6 AuditNet (2012)「監査人によるテクノロジー使用の状態」、プライスウォーターハウスクーパース(年間号)「内部監査専門職の状態の調査」

ますが、このツールで問題の根本原因を探るのは困難です。また、これらのツールは、詐欺やエラーの発生を防止するための機能や例外のフラグを立てる機能はありますが、発生する典型的な問題のトランザクションを効果的に抽出するには十分ではありません。

第1ディフェンスライン(業務執行)のリスク・コントロールテクノロジーの利用

第1ディフェンスラインの業務執行機能は、特定の要注意分野では優れたテクノロジーを使う(例:経理部門における継続的トランザクション モニタリング テクノロジー)場合もありますが、ビジネス基幹システムを有効なコントロールとして過度に信頼しているのが通常の傾向です。
大規模ERPや他のシステムベンダーは内部コントロールの不備を防ぐ広範な能力を有しているように見えますが、実際には、これらのシステムは大規模かつ複雑であり、内部コントロールはシステム導入時に十分考慮されていないのが通常です。例えば、ERPシステムをより効率的に稼働できるように、特定のコントロール設定をオフにすることは少なくありません。
共通の独立した方法論とテクノロジープラットフォームを活用し、第2および第3ディフェンスラインと連携した、リスクマネジメントとコントロールモニタリングの統合的連携アプローチは、経営者の主要なリスク低減達成に、最も効果的です。

現在の状態から…

さまざまなテクノロジーがさまざまなGRC関連プロセスにばらばらに適用されている状況から考えると、共通の方法論とサポートツールセットを統合した新たなアプローチが必要であることは明確です。テクノロジーをリスク・コントロールプロセスに組み込む機会には、大きく2種類あります。

1. GRC機能関係者全員を、同じ方法論と同じテクノロジープラットフォームに揃えることによって、組織の連携と価値を推進する(例:水平的成熟度の成長)。
2. リスク・コントロールプロセスの全ての使用ツールのテクノロジー能力を統合することによって、組織の能力と価値を推進する(例:垂直的成熟度の成長)

…将来の状態へ:「データ主導型GRC」の導入

リスク・コントロール機能の戦略的目標の価値が最大化された未来の状態は、リスク・コントロール関連プロセスに対する「データ主導型」アプローチによって達成されるでしょう。

「データ主導型GRC」とは、経営レベルまたは取締役会レベルの戦略リスクを、取引レベルの事業データ分析によりリアルタイムで評価およびモニターするために、テクノロジーツールを活用する方法論のことです。

必要な機能:

- 主要な戦略リスクに係る現場のコントロールを確実に識別する
- 組織内の経験的証跡(データ等)を使用してコントロールを検証する(質問、サンプリングなどの不確かな検証方法は使用しない)
- それらの検証をスケジュール化および自動化し、定期的検証により関連コントロールの継続評価を行う
- 検証のリアルタイム結果を直接コーポレートリスクとリンクさせ、リアルタイムの組織的リスク評価を推進する

GRC関連プロセスのデータ主導型方法論

GRC関連機能領域全体にデータ主導型能力を構築する（そして通常もテクノロジーを効果的に活用する）近道は、基礎となる方法論を単純明確にすることです。それにより、異なる業務や組織の関係者が共通の場でプロセス視点から作業できるようになります。一つ一つの段階を踏んでこの方法論を構築することが、データ主導型GRC成功の要です。

ステップ１：シンプルで実務的なGRC方法論を設計する

監査、コンプライアンス、ERM、品質、セキュリティなど全てのGRC機能において、リスク、コントロール、検証、および検証結果を定義する基本プロセスを設定する必要があります。さらに、そのプロセスは、経営陣および取締役会レベルでのコーポレートリスクの課題に直接結びついていなければなりません。

このプロセスは、戦略的レベルでコーポレートリスクを識別し、客観的な「潜在的影響」と「発生可能性」の基準で評価することから始まります。この最初のリスク評価に基づき、適切なリスク軽減達成のために、各種の機能領域（監査、コンプライアンスなど）をまたぐ組織計画を策定します。この計画は、残余リスクを許容レベルへと下げるためのプロジェクトや施策を識別する必要があります。

軽減計画策定後、各プロジェクト内の具体的な主要目標を定めると、これらの目標の達成に脅威を与える戦術レベルのリスクが浮き彫りとなるでしょう。これらの戦術的リスクを軽減するコントロールを識別する必要があります。最後に、これらのコントロールの検証を設計し実行しなければなりません。

図2：基本的GRCプロセスフロー

ステップ２：コントロール検証でデータ分析を活用する

ステップ1は、リスク評価、コントロール定義、および検証の実行という単純な統合プロセスの設定でした。GRCの基本です。

主要リスクの評価と軽減の基本的プロセスを定めた次は、一般的に組織の最大の弱点となる、コントロールの有効性を評価する真に有効な検証の実行になります。簡単に言えば、「あなたは、自分が知らないということを知らない」ことが課題です。今日の動きの速い世界では、コントロールの不備や、以前には認識されなかったリスクの発生を簡単に見逃してしまいます。

コントロールの不備の発生およびコントロールギャップの存在に対してより有効な洞察を得るためには、次世代検証手法を活用しなければなりません。

次世代検証手法とは、基本的にはテクノロジーツールを活用するコントロール検証です。質問、観察、サンプルチェックなどの手作業による従来型の監査と評価方法は、信頼性の高い信頼区間を求める際には、統計的に失敗することが証明されています。自動化された検証は、実質的に価値のない問題の調査に費やされる時間も回避します。　次世代検証手法は、システムと実際のデータソースの分析に基づいています。この検証手法には、トランザクションデータ分析、全数検査、自動化ITインフラ、アプリケーション評価ツール、統計的データ動向アナリティクス、活動監視ツールその他が含まれます。

データ主導型GRC方法論のステップ2は、優れた「真実を語るソース」（優れたデータなど）で優れた検証を実施することに主眼を置いています。これは、次のようにテクノロジーを駆使することで達成されます。

1. 関連データを抽出する
2. 完全性を検証し分析を準備する
3. 事前に策定されたビジネスルールに基づき分析する
4. 潜在的例外事象を含む結果を得る（例：コントロールの不備の発生やコントロールのギャップの存在を示すレッドフラグ）

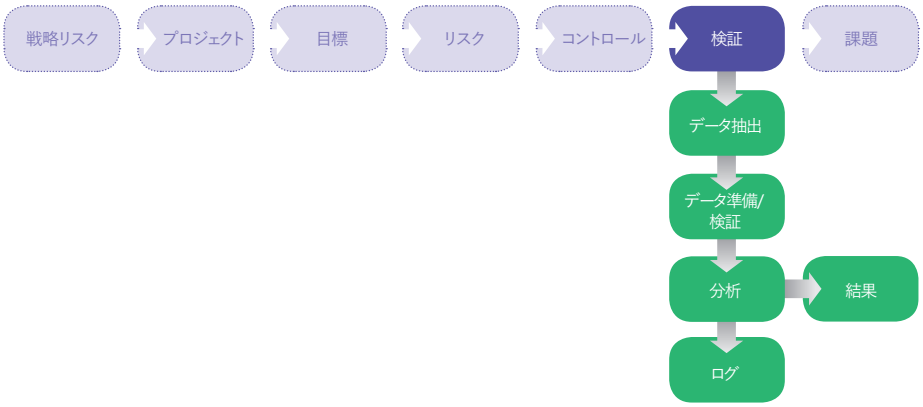

図3：データ分析を使用したコントロール検証の方法論

ステップ2の分析は、過去の証跡に適用したとき、より良いカバー範囲とよりよい信頼区間を得られるように設計されなければなりません。

ステップ3：GRCとデータ分析の方法論を統合する

ステップ3では、組織は、次世代アナリティクス手法とGRCプロセスとの戦略的統合を始めます。理想的には、このフェーズでは、組織のリスク・コントロール関連機能組織が、次世代検証により50%以上をカバーするなどの、必要なカバー範囲の標準化に着手します。また、次世代検証のレポートを全体的な問題管理プロセスに直接統合し、結果と問題を示す経営ダッシュボードを提供し、戦略的リスクレベルのビジュアルなレポートを提供します。

リスク・コントロールプロセスにおける次世代検証の戦略的統合は、リスク軽減の適用範囲が大幅に改善され、裏付けのある検証可能なレポート、そして、組織における明確なリスク表明による経営適合性の改善をもたらします。

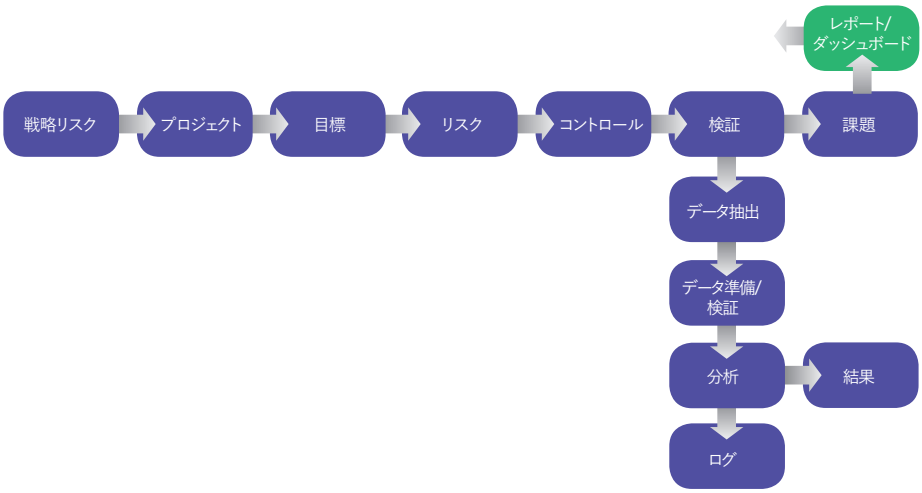

図4：統合的GRCとデータ分析方法論

ステップ 4：継続的モニタリングを強化してリアルタイムの洞察を得る

次世代検証、特にデータアナリティクスの活用に続いて、価値提供強化の次のステップは、今日の現実経済のスピードにあった実行です。リスクや経営問題について、年次または四半期で開示し報告するだけでは、少なくとも経営陣や取締役会レベルのステークホルダーの観点からは不十分です。検証は自動化し、連続的に実行する必要があります。現在利用できるテクノロジーを使えば、容易に統合的GRCとデータ分析を構築し、それを自動化して準リアルタイムでの継続的監査またはモニタリングを推進できます。

場合により、このレベルのモニタリングを維持する責任を、第2、第3のディフェンスラインから、業務執行レベルに渡すこともできるでしょう。この場合でも、内部監査またはその他のリスク・コントロール機能組織は、モニタリング検証の結果をレビューし、必要なアシュアランスを得ることができます。自動化スケジューリング、例外事象の調査、およびトランザクション（取引）結果の視覚化を、単純に階層化することで、モニタリング成果がリスク・コントロールのアーキテクチャ全体に直接リンクします。これにより、実際の活動からのデータ証跡に基づいた、事業機能組織のリスクマネジメントの有効性をレビューする継続的プロセスが可能になります。その結果、たとえば、追加的な監査手順の実行や、より効果的なコントロールシステムの実施など、すべてのステークホルダーが適切な対応を行うことができます。

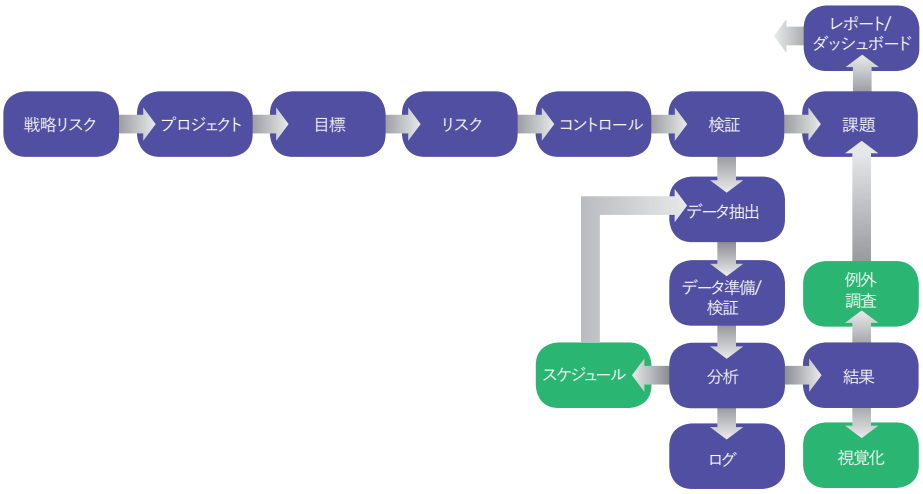

図5：データ アナリティクスの継続的監視への拡大（緑色で表示）

ステップ 5：GRCと継続的モニタリング方法論を統合して「データ主導型GRC」とする

最後は、データ主導型GRC方法論を使ってコンプライアンスを達成する重要なステップです。このステップ5では、継続的モニタリング活動で得られた結果を、適合するリスク・コントロール管理とリンクさせます。識別された問題の量、価値、および傾向は、各プロセスまたはテクノロジーに対応したルールに自動的にフィードバックされ、その結果、戦略的リスクレベルのリスク評価を導き、潜在的な影響度と発生可能性に関して、これらのリスクのデータインジケータがどこに位置するかを正確に反映させます。これが、データ主導型GRCを可能にするプロセス全体の重要な段階です。実行されたすべての作業が、経営陣および取締役会を、以前は分からなかったリスクレベルを軽減する有意義なリアルタイムの意思決定へと導くことができ、結果、組織パフォーマンスの信頼性を最適化できるフェーズです。データ主導型プログラム方法論の完全な統合を成功させる鍵は、スコアカードやルールを策定して、組織において戦略的課題を導くようなリスクを引き起こす好ましくない活動の限界値を客観的かつ定量的に定義することです。以下は、このプロセス全体を図示したものです。

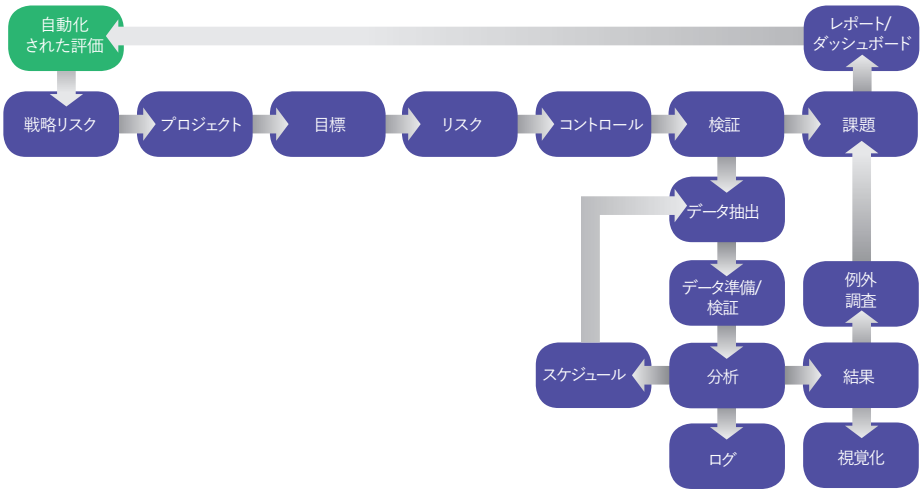

図6：エンドツーエンドの統合的データ主導型GRC方法論

テクノロジーソリューション

データ主導型GRCは、テクノロジープラットフォームなくしては達成できません。テクノロジープラットフォームは、上記の各ステップをサポートすることに加え、組織の広範なテクノロジー環境を直接統合して、客観的評価に必要なデータを取得し、GRC活動を推進します。テクノロジーの視点から、データ主導型GRC方法論で主要ステップを有効にするために、4つの主要素が必要です。

1. 統合的リスク評価

統合的リスク評価テクノロジーは、戦略的リスクの一覧と、それらの管理状況評価を維持管理します。このテクノロジーは、組織の最も上級の専門家がGRCプロセスに参加するためのインターフェースとして、経営陣にとって関連性があり、使用可能なツールでなければなりません。このテクノロジーは、リスク軽減の取り組みの優先度を設定し、各ディフェンスラインによって策定される対応・プロジェクト計画検討を推進します。

2. プロジェクト・コントロール管理

プロジェクト・コントロール管理システム（狭義には監査管理システム、または eGRC システムと言われることもあります）によって、各リスク・コントロール機能組織は、必要に応じて識別されたリスク軽減のためのプロジェクト計画を構築できます。プロジェクトの内容は、戦術レベルのリスク、そのリスクを低減するコントロール、そしてそのコントロールを評価する検証に分けられます。これは、組織の戦略目標の達成にはどのデータが検証やモニターされるべきかを整理し、組織の内部コントロール環境および関連するドキュメンテーションと評価のバックボーン（背骨）となります。

3. リスク・コントロールアナリティクス

統合リスク評価がデータ主導型 GRC プログラムの頭脳であり、プロジェクト・コントロール管理がバックボーン（背骨）であるならば、リスク・コントロールアナリティクスは心臓と肺となります。客観的意思決定を行うために、組織環境を対象としてすべての必要なデータを集め、フィルターにかけ、処理したうえで、脳に送り返すためには、アナリティクスツールセットが不可欠です。このツールセットは、リスク・コントロールアナリティクスに合わせて調整され、フィルタリングと処理機能が異常を特定するために最適化され、同時に膨大な数のデータに対処しながら、時間の経過とともに傾向を示せることが重要です。

4. ナレッジコンテンツ

ナレッジコンテンツは、すべてのテクノロジー要素に関連し、さまざまな形式で提供され、組織の広範なリスク領域をカバーする方法論を実行し自動化するために必要なリスク、コントロール、検証、およびデータについて特化したナレッジです。ナレッジコンテンツは、個別のリスク・コントロール目標に従って取得される必要があり、次のような項目を含みます。

- 特定のビジネス プロセス、課題、または全社レベルのリスク領域に対応するリスク・コントロールテンプレート
- 複数のコンプライアンス要件を、実践し検証できるコントロールの単一セットにする統合的プライアンスフレームワーク
- 特定の主要コーポレートシステムにアクセスし、評価に必要なデータセットを抽出するデータエクストラクタ（例: SAP を使用する組織では、特定のバージョンの SAP から固定資産データの完全なセットを取得し、固定資産に関連するコントロールの検証を要求する）
- 特定のデータセットを取り込み、そのデータセットの中のどのトランザクションがルール違反なのかを評価し、発生したコントロールの不備を示す、データ分析のルールセット（またはアナリティクスのスクリプト）

完全に統合されたデータ主導型 GRC 方法論に対する、統合されたリスク・コントロールテクノロジープラットフォームを構成する主要テクノロジーのマッピングは次のとおりです。

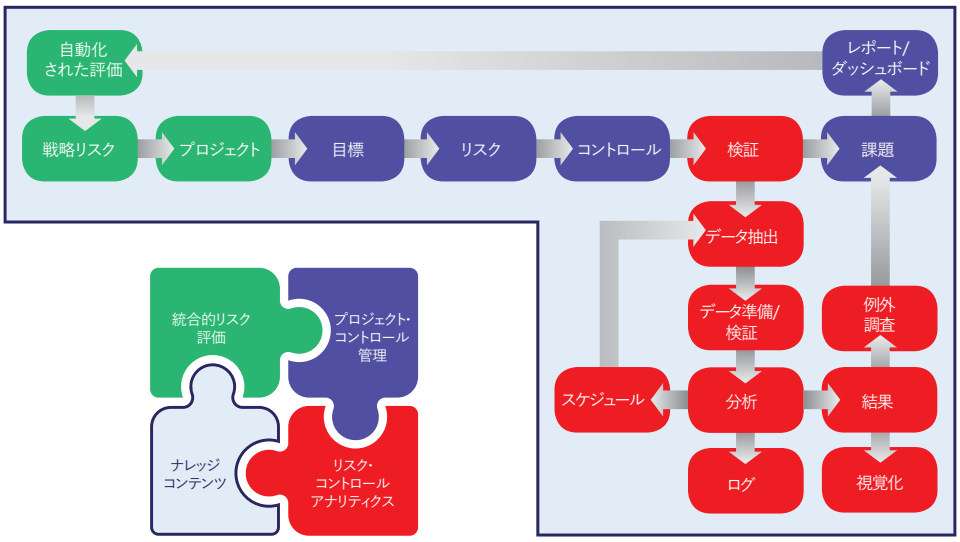

図7：データ主導型GRC方法論の統合的GRCテクノロジープラットフォームへのマッピング

テクノロジープラットフォームを評価する場合に、このジグソーパズルの各ピースは他のピースと直接統合していることが必要不可欠です。そうでない場合は、結果を手動で集計する必要があり、これは手間がかかるだけでなく、一貫性がなく、整理もできません。そもそも、データ主導型GRC方法論に違反したものになります。

GRCテクノロジーチェックリスト：

- **一元化されたプロジェクトとコントロールの文書化：**
  プロジェクト・コントロール管理システムが組織内に設定され、リスク・コントロールと、コントロールの有効性を維持、評価するための手法が文書化されている。
- **継続的リスクモニタリング：**
  継続的トランザクション モニタリングと継続的コントロール モニタリングを管理するリスク・コントロールアナリティクスが、重要なビジネスプロセス領域で実行され、例外事象を識別し、プロジェクト・コントロール管理システムに統合されたリスク指標のダッシュボードを提供している。
- **マネジメント活動との統合：**
  プロジェクト・コントロール管理システムは、統合リスク評価計画システムに直接接続し、リーダーが、組織のディフェンスライン全体のリスク低減施策を行うべき重要分野を判断する際に用いられている。
- **リスク コントロール マトリックス 検証計画：**
  リスク低減施策のための各プロジェクトでは、吟味されたリスク コントロール マトリックスにより、重要な戦術リスクと低減コントロールを識別している。次世代検証手法を活用した検証計画が設定され、コントロールの有効性についてのアシュアランスを提供している。
- **自動コントロール検証：**
  適切な場合には、検証は、安全で一元化されたリポジトリーに維持されたアナリティクスにリンクします。アナリティクスは、繰り返し自動的に実行され、識別された結果はレビューと解決策のために自動的に転送され、リスク・コントロール構造にリンクしている。
- **分析主導型の改善とリスク評価：**
  すべての検証手法を通じて識別特定された結果は、自動的に改善活動と、戦略レベルの組織的リスクに対する影響度と発生可能性の評価につながっている。
- **リスク ダッシュボード：**
  監査とコンプライアンス活動の状態は、監査、コンプライアンス、および上級管理職により、関連リスクエクスポージャーと取り組み中の問題についての最新状況を提供するダッシュボードを使ってモニターしている。

全てのディフェンスラインのリーダー向けの「価値を提供する」テクノロジー成熟モデル

ここまで、データ主導型GRC方法論とそのアプローチに必要なテクノロジーに基づいたプログラム開発の各段階を見てきました。完全に統合されたテクノロジーを使用することで、GRCプロセス自体の効率と、全社に確立されているリスク管理手順とコントロールシステムの有効性に大幅な向上が見られるはずです。

我々は、この方法論を通じての適切なテクノロジーソリューションの適用を通して、5つのレベルの成熟能力があることを特定しました。

1. 基本的GRCプロセス
2. リスク・コントロールデータ分析
3. 統合的GRC＋データ分析
4. 全社的継続的モニタリング
5. データ主導型GRCプロセス

以下のモデルは、これらの先進的能力が、すべてのディフェンスラインで、それぞれの業務アプリケーションに関して適合するかを説明したものです。多くの組織のGRCを調査すると、基本的GRCプロセスは、一般に、第3ディフェンスライン（内部監査）と一部の第2ディフェンスラインの業務に構築されています。また、データ分析が一部実行されていますが、通常は、第3ディフェンスラインだけで実行され、GRCプロセスから切断された状態か、GRCプロセスには手作業でしか連結されていません。これらは重要な活動であるものの、この場当たり的なアプローチでは、最新のテクノロジーで可能な方法と比較すると、組織には限定的な戦術的価値しか提供できません。

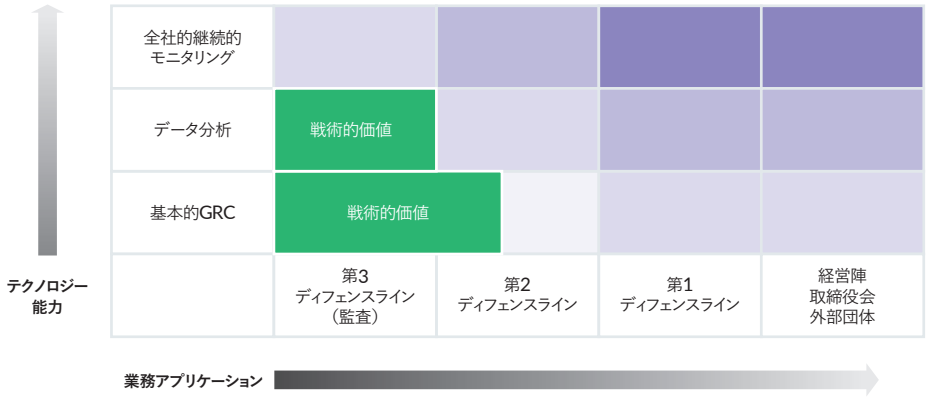

図8：現在の状態

専任のGRC専門家が、組織のGRCプロセスを積極的に改善し、ディフェンスライン全体が協調し始めると、高い価値のGRCプログラムに進化します。データ分析とGRCプロセス検証が統合され、リスク・コントロール関連機能に統合的GRCとデータ分析が達成されると、組織の戦略的レベルでインパクトの高い価値の高い結果が出始めます。ディフェンスライン全体のコントロールモニタリングと改善の取り組みを自動化する、強力な全社的継続的モニタリングプログラムに対しても同様のことが言えます。

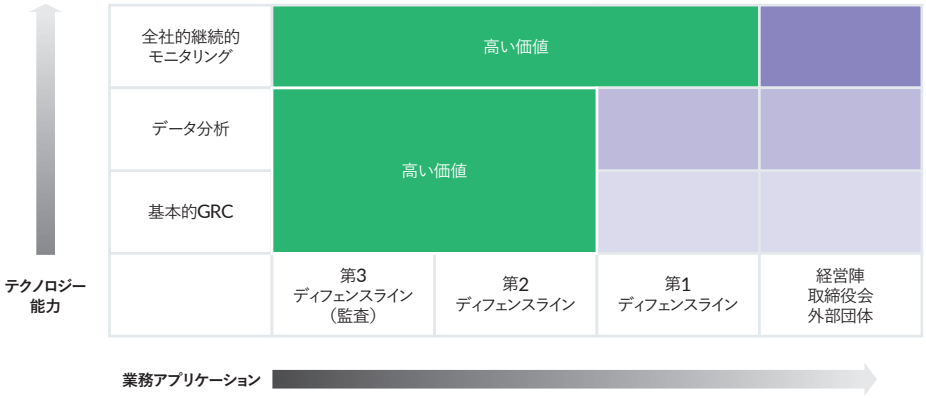

図9：高パフォーマンスGRCプログラム

データ主導型GRCによるパフォーマンス管理強化

データ主導型GRCはリスクだけに関するものではありません。これは、コーポレートパフォーマンス管理活動全体の中核にもなります。プログラム、人、およびテクノロジーが、成熟し統合されてデータ主導型GRC機能を達成し、組織全体に適用されると、すぐに変革の価値が生まれ、プログラムはしばしば上級管理職と取締役会の組織パフォーマンス管理活動の基盤となります。

これは過度に理想的のように見えるかも知れませんが、既にこの方向に進んでいる複数の部門にまたがる統合的GRCプログラムはあります。このようなプログラムは、リスク管理における変革の価値の提供を通じて、戦略目標を達成する全社的な業績管理を進歩させる組織を支援してきました。

図10：変革型GRCプログラム

まとめ

データ主導型GRCを通じた変革的価値の提供に向けた組織の動きを支援するために、監査またはリスクマネジメントのリーダーは何ができるでしょうか？

考慮すべき諸問題：

- リスク・コントロール関連機能組織（監査、リスク管理、コンプライアンス他を含む）のリーダーは、組織的戦略を策定し、統合的テクノロジーアプローチの根本的価値を認識します。
  - 監査、リスク管理、およびコンプライアンス活動において、連結も統合もされていないテクノロジーの断片的な使用では、インパクトが高い価値の提供や、総体的費用対効果の改善は困難です。
  - 統合的テクノロジープラットフォームは、内部監査の独立性を侵すことはありません。
- データ主導型GRC方法論は、行く行くは組織リスクを管理する必要性を証明し、最終的には全社的パフォーマンス管理の基礎になることを証明するでしょう。
- リスク・コントロールテクノロジープラットフォームの統合は、多くのメリットを提供しますが、無用な複雑性はありません。
  - 大量の計画、構成、およびメンテナンスを要する大規模かつ複雑なシステムには、総体的な費用対効果は望めません。
  - 方法論とテクノロジーは、それぞれを実行する適切なアプローチによりシンプルになります。
- テクノロジーは、リスク管理とGRC戦略全体の基礎として検討すべきです。
  - 真の「データ主導型」GRCプロセスを達成するためには、思考とアプローチの大きなシフトが必要です。
  - リソース計画と予算では、こうしたことを十分に考慮する必要があります。

アシュアランス、リスク管理、およびコントロールにおける効率の高いデータ主導型プロセスを持つ組織が、優れたビジネスパフォーマンスを示す組織となることは明らかです。

ACLは、世界中の何千ものお客様と連携してきた20年もの経験を活用し、変革型GRCをサポートする詳細な事柄および方法論に加え、データ主導型GRCモデル内の各ステップでパフォーマンスを最適化するプロセスと手順を開発してきました。

貴社がテクノロジーをGRCプロセスに最善の形で統合する方法の無料評価については、1-888-669-4225まで電話でお問い合わせいただくか、www.acl.comをご覧ください。

Dan Zitting　CPA、CISA、GRCPは、ACLの最高製品責任者（CPO）であり、先進的テクノロジー活用の提唱者です。特に、GRC関連の専門職と組織パフォーマンス管理の変革におけるクラウド、モバイル、データ分析と可視化、およびソーシャルテクノロジーを推進しています。

John Verver　CA、CISA、CMCは、ACLの顧問であり、監査、リスク管理、コンプライアンス、および継続的モニタリングのテクノロジーの役割を長年にわたり提唱しています。

ACLについて

ACLは、監査とリスク管理を変革するテクノロジー ソリューションを提供します。ソフトウェアと専門的コンテンツの組み合わせにより、ACLは、リスクの特定と軽減、利益の保護、およびパフォーマンスの促進を行う強力な内部コントロールを実現します。監査とリスク管理の地平を拡大し、優れた戦略的ビジネス価値を提供可能とする、という強い願いで推進されているACLは、結果を出し、適用を簡素化し、使いやすさを改善するテクノロジーを開発し、提唱しています。ACLの統合製品群には、クラウドベースのガバナンス、リスク管理とコンプライアンス(GRC)ソリューション、および主力製品であるデータアナリティクス製品があります。これらの製品は、監査とリスク管理の不可欠な要素をすべて組み合わせたものであり、経営幹部レベルから、最前線の監査とリスク管理の専門職、およびビジネス最前線の管理者まで、組織の全てのレベルでシームレスに使用されています。強化されたレポートとダッシュボードは、重要な事項への集中を実現できる、透明性とビジネスコンテクストを提供します。さらに、30年の経験とコンサルティング アプローチを有することで、迅速かつ効果的な実装を徹底し、お客様はビジネスの具体的な結果を低リスクかつ迅速に実現できます。当社は、全世界の14,000社以上のお客様(Fortune500社の89%が含まれます)のコミュニティに積極的に参加し、当社の最善の構想を発信しています。数例をご紹介いたします。
オンラインで www.acl.com からご覧ください。

プロティビティについて

プロティビティは、企業のリーダーが自信をもって未来に立ち向かうために、高い専門性と客観性のある洞察力や、お客様ごとに的確なアプローチを提供し、ゆるぎない最善の連携を約束するグローバルコンサルティングファームです。20ヶ国、70を超える拠点で、プロティビティとそのメンバーファームはクライアントに、ガバナンス、リスク、内部監査、経理財務、テクノロジー、オペレーション、データ分析におけるコンサルティングサービスを提供しています。プロティビティは、Fortune 1000の60%以上、Fortune Global 500の35%の企業にサービスを提供しています。また、成長著しい中小企業や、上場を目指している企業、政府機関等も支援しています。プロティビティは、1948年に設立され現在S&P500の一社であるRobert Half International (RHI)の100%子会社です。

protiviti®
Face the Future with Confidence