海外金融機関のGRC（Governance・Risk・Compliance）対応の現状と方向性

改正個人情報保護法の全面施行、経済安全保障推進法が成立するなど、国内におけるGRC関連の整備が進められてきた。野村総合研究所（NRI）が実施した海外金融機関のGRCへの取り組み状況によると、ツール開発や組織構築における工夫、そして重要リスクの再確認への姿勢が伺われる。

昨年、改正個人情報保護法が全面的に施行され、経済安全保障推進法が成立するなど、GRC（Governance・Risk・Compliance）関連の規制が整備された。この機会にNRIが米国・欧州の金融機関（11行）に対し、Cutter Associates社と共同して実施したGRCの取り組み状況に関するインタビュー調査について紹介することとしたい。調査はコスト、ツール、組織の3つの項目に分けて実施し、GRCの現状と現在注目されている点を探ることに重点を置いている。

コンプライアンス・コストは3%

GRCへの取り組みは企業活動全般に及ぶため、GRCコスト自体を正確に把握することは難しい。そこで、今回のインタビュー調査ではGRC予算の大部分を占めるコンプライアンス・コストについて調査した。

まず、コストの水準だが、ある大手金融機関の場合、コンプライアンス・コストは「総営業コストの3%」となっていた。これは、欧州委員会が10年に一度、金融機関に対して行っている調査においても同様の傾向となっている。

同委員会の調査によると、このコストのうち、30%弱が監督当局向け報告のデータ収集作業となっている。30%という水準は決して少ないものではなく、また、今後、規制が強化されるにしたがって、コストが増加する可能性があることに留意すべきだろう。

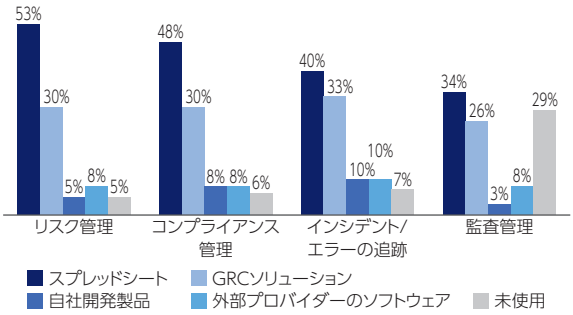
ここ数年、金融機関側は、このコスト削減に取り組んできており、例えば、リスク管理とコンプライアンス管理のプロセスを統合するといった工夫や内部統制とエラー検出を自動化する仕組みを導入するなど、複雑化する規制への対応を強化している。今回のインタビュー調査においても、「今後数年間、GRCプロセスの自動化や高度な分析を可能とする新しい技術の導入などに、より多くの支出を見込んでいる」ということを確認している。

課題山積のGRCツールの活用

次はGRCのモニタリング・分析などのツールの活用状況だが、今回の調査に先立ちCutter Associatesが2019年に行った調査によると、多くの金融機関でGRCツールが使用されているものの、1つの製品で完遂はしておらず、自社開発製品と外部プロバイダーのソフトウェアが混在している。また、各作業において手作業入力のスプレッドシートが多用されていることも判明している（図表）。こうしたソフトの混在や手作業による管理はリスクの分類や関連リスク発見の障害となっているだけでなく、変化する規制やビジネスプロセスの影響を把握することを困難にしている。

今回のインタビュー調査において、上記の課題への対応として、多くの金融機関が現在のGRCツールやサービスについて「再評価する」としており、今後、ツール

図表　GRCツールの利用状況



(出所) Cutter Research Survey on GRC practices, 2019

の開発が進むものと思われる。また、今後、GRCツールの活用方針について問うと、「GRC関連データのデータ戦略、データ収集、データアーキテクチャの整備が重要である」といった回答が寄せられている。今回は具体的なモニタリングやデータ分析手法についてまで調査していないものの、経営層において高い関心が伺われた。

GRCの組織構築の方向性

GRCを担当する組織は、企業規模により人員配置（人数、勤務形態など）、外部リソースの活用状況が大きく異なるが、国内金融機関と同様に、いずれもいわゆる「3つの防衛線モデル（業務執行部門、管理部門＝リスク・コンプラ管理、内部監査部門）」を踏襲している。

ただ、最近では第2線レベルの管理部門でリスクとコンプライアンスを切り離す動きがあり、今回の調査でも、ある大手金融機関はガバナンスの枠組みの再構築の主要な要素としてコンプライアンス機能をリスク機能から分離することを挙げている。この金融機関では、現在、CCO（Chief Compliance Officer）は、グループCEOの直属の独立した役員として位置づけられており、CCOはCRO（Chief Risk Officer）と共にリスク監視の責任を負い、両者はリスクフレームワークの中でそれぞれのチームを率いる形態をとっている。

また、気候変動リスクやESG関連の法規制を考慮したGRC組織の構築が進んでいることも大きな特色となっている。今回、インタビュー調査に参加した大手金融機関のほとんどが、ESGリスクを評価するためのフレームワークを検討しており、既存のERM委員会の権限にESGリスクを加えるか、もしくは企業内に専門のチームを新たに設置するなどの対策がとられている。

なお、インタビュー調査に参加した中小金融機関において十分なGRCに対応する組織がなく、内部監査機能やCCOの外部のコンサルに委託を検討する例も散見された。米国では、CCO経験者だけを集めたGRC専門のコンサル会社も登場している。

コスト、ツール、そして組織構築の動向についてふれたが、最近の新たな動きとしてコンダクトリスクへの対応も注目される。リモートワーク環境が拡大するにつれてプライバシー侵害や社員の不正行為によるコンダクトリスクの顕現化が懸念されている。インタビュー調査対象のほとんどの金融機関においても、これまで注力してきたサイバーセキュリティ・情報セキュリティリスク、サードパーティ・サプライヤーリスク、AMLなどに加え、このコンダクトリスクへの関心が高くなっている。

インタビュー項目の一つである「GRCの取り組みの中で何を優先させるか」の問いに対し、ある大手金融機関の今年度（2022年）の重点項目として「ハイブリッドな勤務形態に起因するコンダクトリスクの増加、および遠隔地の従業員の監督と監視に関する新たなリスクと課題への対応」が挙げられていた。特に、遠隔地の従業員を中心としたリスクと、それが組織全体のリスクフレームワークにどのように適合するかについて引き続き検討していくとのことであった。前述のESGリスクに加え、改めて重要なリスクとして認識すべきであろう。

Writer's Profile

土師 佐和子 Sawako Haji
金融ガバナンスプラットフォーム企画部
エキスパート
専門はITガバナンス、GRCS全般
focus@nri.co.jp