protiviti
Face the Future with Confidence

2021年3月4日「テクノロジーリスク調査結果からみる2021年のIT監査のポイント」ご質問とプロティビティの回答

No.	頂いたご質問	Protiviti回答
1	テクノロジーリスク評価を行う際に、外部環境の変化としてどのようにして情報を収集するのがよいでしょうか。参考になる情報源などありますか。	テクノロジーリスクについて外部環境の変化を捉える場合、セミナーでご紹介したようなコンサルティング会社が発行する調査レポートやメールマガジンの購読、経済産業省や金融庁が発信するテクノロジーに関連するレポートを確認し情報を収集する、また、法令や基準の改正が影響するケースもあるため、法改正が自社の情報システムに影響を与えないか検討するなどがあります。
2	クラウドのベンダーモニタリングですが、監査として見るのが一般的なのでしょうか。	監査としてはクラウドサービスの重要度に応じて、手続きを実施するかどうか判断することになります。一律でベンダーのモニタリングを実施するのではなく、企業活動にとって重要なクラウドサービスを提供するクラウドベンダーを対象にモニタリングを実施することが望まれます。 なお、ベンダーのモニタリングに係る手続としては、下記の2点が考えられます。 ①継続的に契約しているベンダーに対して、契約更新のタイミングや、もしくは年次など定期のタイミングで、委託先企業自体や委託先のシステム環境等を評価する手続 ②保守運用を委託しているベンダーに対して、月次や週次など定期のタイミングで、委託先から提供を受けているサービス内容を評価する手続
3	今回は話に挙がりませんでしたが、ITのリスク評価を、システムを使って管理するような事例はありますか。	ITのリスク評価は、GRCツールと呼ばれるもので管理可能です。GRCツールにて、識別したITリスクを登録し、リスク毎に発生可能性や影響度などの測定結果を登録することで、高リスク領域を特定することが可能になります。 また最近では、リスクに紐づくKRI（リスク指標）となるデータを特定し、このKRIにしきい値を設定することで、データに連動して自動的にリスクを評価するという仕組みをGRCツールで構築している会社もあります。
4	テクノロジーリスクの3位「法規制の遵守」は、具体的にどのような内容（最近の事例など）になりますか。	今回のサーベイでの定義は「新たなコンプライアンス要件や変更点を特定し、コンプライアンス要件を満たすためにタイムリーに対応するためのプロセスと管理が不十分であること。また、継続的なコンプライアンスの監視と報告が不足していること」としておりますが、海外ではGDPRやCCPA、日本では個人情報保護法の改正が最近の事例となります。なお、監査では新たな法規制がITに与える影響を捉えるプロセスや、これらの法規制の要請に対しITが適時・適切に対応ができる状態となっているか検証します。
5	トップダウン形式とボトムアップ形式のどちらを適用するか選ぶ場合の判断基準があれば教えてください。	トップダウン形式では、経営戦略や外部環境の変化を考慮してリスクベースで評価を行うため、監査対象とするITリスクについて経営陣への理解が得やすくトレンドを反映した評価が出来る、というメリットがあります。また、ボムアップ形式では、システム、アプリケーション、プロジェクト等の現在のIT資産や統制をベースに評価をするため、漏れなく評価を実施できるというメリットがあります。 それぞれの長所を活かして組み合わせて実施することが理想的ですが、IT監査でシステム管理態勢が整備され、システム自体も安定稼働していることが確認できているようでしたら、トップダウン形式での評価をお勧めします。
6	競争優位を確保するためのプラスのリスク評価についてですが、例えばどのような分析になるでしょうか。例を教えてください。	金融庁の「金融機関のITガバナンスに関する実態把握結果（事例集）」ではITリスクの着眼点の例として、「新技術を導入しないことによる機会損失リスクの見極め」が機会損失も対象としたリスク評価を事例として紹介されています。

7	13ページの色別の意味合いをもう少し詳しく教えてください。	今回のセミナー内で特に説明をしたリスクを対象に色分けをしております。「サイバー脅威」はいずれの産業でも上位であったため色分けしております。また、その他の色分けをしているリスクは全体のTop10リスクに含まれなかったものの、産業別に分類した場合に当該産業のTop10リスクにランクインしたリスクです。
8	重複する箇所が多いため、J-SOXのIT統制評価との棲み分けはどうすれば良いでしょうか。	J-SOXとITリスク評価の棲み分けに関するご質問と理解いたしました。 まずJ-SOXは一般的に、財務諸表に関連するシステムを対象にシステム開発・運用、セキュリティ等に係る統制状況を評価いたしますが、ITリスク評価は、IT戦略やITガバナンス、サイバーセキュリティといった比較的大きなテーマの他、ITトレンドや経営陣が気になるテーマも含めてリスクシナリオを想定し、発生可能性と影響度を評価の軸にしてテーマごとにリスクの大小を識別いたします。 要約しますと、J-SOXは財務諸表に係るシステムを対象とする限定的な保証を目的としており、一方、ITリスク評価は社内の全リスク領域に対するリスクの大小の識別を目的としています。
9	クラウドサービスの監査はサービスプロバイダーが情報を開示しない部分が多く、必要な評価ができない可能性が高いと感じています。効果的な対応方法があれば教えてください。	クラウドサービスプロバイダーは、受託業務に係る内部統制が適切に構築されていることを証明する目的で「SOC報告書」を用意し、利用者に提供することが増えていますので、「SOC報告書」を入手してクラウドサービスプロバイダーを評価するのも一案です。また、一定のセキュリティ水準を担保することを目的に、最低限確認が必要な項目をチェックシートにまとめ、クラウドサービスの利用前にチェックする社内ルールとすることも有用です。確認が必要な項目の例は、以下のようなものがあります。 ・プロバイダーの経営状況／SLAの有無／データの格納場所／データセンターの物理的セキュリティ／データのバックアップ体制／システムの冗長性／各種モニタリングと報告の有無等々
10	リモートワーク監査を行う場合のポイントについて、もう少し詳しく教えてください。	リモートワークにおける情報セキュリティ対策は、「ルール」、「人」、「技術」の３点の組み合わせによって実現されます。従いまして、監査においてもこの３点を対象に検証を行うことが重要になります。想定されるセキュリティ対策については、総務省テレワークガイドラインが参考になりますので、ご参照ください。（https://www.soumu.go.jp/main_content/000545372.pdf） また、弊社が発行しております、「リモートワークにおけるサイバーセキュリティの取り組み」もご参照いただければ幸いです。 （https://www.protiviti.com/JP-jp/insights/work-home-cybersecurity-practices）
11	ITリスク評価の進め方としては、トップダウン形式とボトムアップ形式のどちらを採用することが多いのでしょうか。	金融業界では金融庁の検査項目への対応として、IT資産への自己評価が定着していることもあり、ボトムアップ形式で実施されているケースが多くありましたが、最近ではトップダウンの評価を取り入る事例も多くなっています。 それぞれのアプローチのメリットや選択基準についてはNo5を参照ください。
12	M365のアプリケーションでIT監査的に最も注目すべきものがありますか。OneDriveなどでしょうか。	ご質問のOne Driveは、IT監査で注意すべきアプリケーションの一つです。 その他、組織で良く使われているOutlook、SharePoint、Teamsも同様です。 SharePoint：格納されている情報の重要性に応じて、アクセス権が付与されているか、特に、退職した従業員や契約が終了した委託業者のアクセス権が残存していないか、 Teams：外部のアプリケーションと連携（アドオン）して利用することも可能ですので、そのアドオンが組織のセキュリティポリシーに従って制御されているか、と言った観点も注意が必要です。

13	リスク評価シートの参考になるものがあれば、ご紹介ください。	弊社では、以下のような項目で構成されたリスク評価シートを使用しています。 ・リスクタイトル（例：IT戦略や投資計画等） ・リスクシナリオ ・会社における現在の状況 ・リスクを引き起こす要素、発生可能性、根拠 ・リスクが発生した場合のビジネスへの影響度 ・発生可能性と影響度から算出した固有リスクのスコア　等 ご参考になれば幸いです。