ソリューション概要

Archer® IT & Security Risk Management

はじめに

組織は、何層ものファイアウォール、ウイルス対策、侵入防止システム、侵入検出システム、脆弱性スキャナー、セキュリティ ポリシー、ID 管理、物理的アクセス制御などを構築して、セキュリティ上の課題に取り組んでいます。これらの防御層は、基本的な防御を提供し、今日の脅威から保護するために必要ですが、層を重ねるにつれ、セキュリティ インフラストラクチャも複雑になります。このように複雑になると、セキュリティ リスクが発生する場所と、脅威が顕在化する速度を明確に調整することが困難になります。

セキュリティ機能にとっては、これらの防御層によって作成されたセキュリティ関連データの増加も課題となっています。すでに圧倒的な量になっているビジネス データも保護しなければならないためです。どのデータがビジネスにとって最も重要かをしっかりと理解していないために、IT チームとセキュリティ チームは、最も関連性の高いセキュリティ イベントの特定に苦労しています。

セキュリティは、今日のテクノロジーの移行によってますます影響を受けています。特に顕著なのは、クラウドおよび外部プロバイダーへのビジネス要素の移行です。企業が境界外に移行するビジネス クリティカルなプロセスとIT サービスが増えているため、セキュリティ制御は外部のステークホルダーに、完全にではなくとも、大きく依存することになります。このような第 3 のプラットフォームへの移行によって、セキュリティとコンプライアンスの両方の要件の課題は増加します。

絶えず変化する今日の脅威とインシデントによって、組織がサイバーリスクの増加にどのように対処するかに経営陣の関心が高まっています。これまで以上に、経営陣は、セキュリティリスク (評判の損害、財務的影響、規制に関連する損害) と、侵害またはその他のセキュリティ イベントの調査と解決の純コストについて懸念しています。

IT とセキュリティへのインサイトの提供

IT リスクとセキュリティ機能がテクノロジー関連のリスクを完全に把握して示すためには、複数の運用グループが協力して作業を調整する必要があります。セキュリティ ポリシーを、規制とビジネスの要件に合わせて調整する必要があります。脅威と脆弱性の管理プロセスは、増大する脅威に先んじるために機敏性を維持する必要があります。組織に対するアクティブな攻撃を迅速に特定し、危険にさらされた資産を保護するためには、アクティブかつ真摯にセキュリティ運用を行う必要があります。セキュリティ戦略は、革新的でコスト効率に優れたソリューションを実現するために、迅速さと巧妙さより多くを備えている必要があります。最後に、セキュリティ コンプライアンスによって、適切な制御が設計され、効果的に運用されているようにする必要があります。

Archer® IT & Security Risk Management のメリット

Archer IT & Security Risk Management を使用すると、可視性、分析、アクション、およびメトリックが強化され、セキュリティ機能が向上します。

GRC のコンテキストでのサイバーセキュリティ リスクの結び付け

今日のビジネス プロセスは相互に接続されているめ、組織には、急速に変化するサイバーセキュリティ リスクの複雑さと、広がっていく影響に効果的に対処する能力が必要です。Archer は、企業全体にわたって、セキュリティ プロセスとデータを、リスクとコンプライアンスの機能に結び付けることができます。そして、IT およびセキュリティ リスク機能によって、ビジネス リスクとIT リスクの関係を、ビジネスの重要度の観点から考慮して、担当とアカウンタビリティを確立し、IT とセキュリティのリスクを、ガバナンス、リスク、コンプライアンスのより広範なプログラムに結び付けることができます。

複数の次元でIT とセキュリティのリスク管理に取り組む

IT とセキュリティのリスクを効果的に管理するには、あらゆる種類のIT セキュリティ リスクを管理できるようにセキュリティ プログラムを編成する必要があります。企業のIT およびセキュリティ リスク プログラムは、ポリシー、標準、コンプライアンスから、脅威、脆弱性、攻撃に至るまで、複数の次元でリスク管理に取り組む必要があります。Archer は、IT チームとセキュリティ チームがプロセスを一元的に管理し、サイバー脅威に優先順位を付け、最新の脅威を完全に掌握できるようにします。

ビジネス コンテキストとプロセス有効化をつなぐ

今日のIT リスクとセキュリティ リスクの管理には、データの速度とフィードだけでなく、さらに多くの要素が関わっています。テクノロジーの問題によって組織全体が深刻なリスクにさらされる可能性があるため、ビジネスの観点からIT リスクを理解する必要があります。ビジネスとIT の連携を確保することによって、IT とセキュリティのリスク管理プログラムで、ビジネスの安全性を維持するために必要な対処を容易にすることができます。RSA ArcherIT & Security Risk Management により、リスクを特定して効果的かつ効率的にエスカレーションするプロセスを確立することで、人とテクノロジーのギャップが埋められます。

Archer it & Security Risk Management

最新のIT およびセキュリティの脅威は、今日の複雑なビジネスに広がっています。Archer IT & Security Risk Management によって、お客様のビジネスにとって重要な資産を特定し、セキュリティのポリシーと標準を確立して伝達することができます。また、攻撃を検知して対応し、セキュリティの不備を特定して修復するとともに、明確なIT リスク管理のベスト プラクティスを確立することができます。

Archer IT & Security Risk Management によって、リスク管理の成熟までの行程におけるお客様固有のビジネス ニーズに対応する、さまざまなユース ケースが提供されます。

問題管理

Archer Issues Management を、セキュリティ、リスク、またはコンプライアンス関連のユースケースに適用することにより、セキュリティ インシデント、内部統制の障害または欠陥、注意またはエスカレーションを必要とする例外により発生する問題の把握と統合が行われます。Archer Issues Management によって、組織は、社内および社外の監査所見、法令順守の問題、管理により自己識別された問題をカタログ化し、問題解決のためのアカウンタビリティを確立し、責任および期限と照合して修復計画を追跡することができます。堅牢なレポート機能により、すべてのレベルの経営陣と取締役会は、未解決の問題、優先度、および修復のタイムラインの範囲全体を容易に把握することができます。

IT セキュリティ ポリシー プログラム管理

Archer IT & Security Policy Program Management を使用すると、外部の規制の義務を文書化し、体系的なレビューと承認のプロセスを確立することができます。また、規制による義務の変化を追跡し、ビジネスへの影響を理解し、対応に優先順位を付けることができます。

IT 統制保証

Archer IT Controls Assurance は、すべてのIT 資産にわける統制のパフォーマンスを評価してレポートし、統制の評価と監視を自動化する機能を提供します。一元化されたシステムを実装して、コンプライアンス レポート作成用にIT 資産をカタログ化し、IT 統制を文書化するための記録システムを構築することができます。IT 統制をテストするための合理化されたプロセスとワークフローにより、手作業による統制のための標準化された評価プロセスを導入し、自動化されたシステムからのテスト結果を統合することができます。コンプライアンス評価の際に特定された問題は一元化されているため、コンプライアンスのギャップについて追跡してレポートを作成することができます。ギャップの修復作業は文書化して監視し、コンプライアンスの差異を確実かつ適時に解決することができます。

サイバー リスクの定量化

Archer Cyber Risk Quantification は、サイバーセキュリティ イベントに関する、組織の財務リスクを定量化します。Cyber Risk Quantification のユース ケースによって、CIOSO は、ビジネスと財務への影響に基づいてリスク軽減作業の優先順位を付け、取締役会および経営幹部に、財務面でのサイバーリスクの影響を伝えることができます。この財務データを活用すれば、組織は、リスクとセキュリティ対策への投資について、十分な情報を基に意思決定を行えます。

サイバー インシデントおよび侵害対応

Archer Cyber Incident & Breach Response により、組織とIT の資産を一元的にカタログ化し、ビジネス コンテキストを確立してインシデントの優先順位付けを推進することができます。また、宣言されたインシデントの効果的なエスカレーション、調査、解決のために設計されたプロセスを実装できます。このユース ケースは、チームが、定義されたインシデント対応およびトリアージ手順に従って効率的に作業し、データ侵害に備えることができるように設計されています。

組み込みのワークフローとレポート作成機能により、セキュリティ マネージャーは、最も差し迫った問題に集中し、プロセスを合理化することができます。宣言されたインシデントの調査に関連する問題は、一元化されたポータルで追跡して管理することができるため、全体の把握とレポート作成が可能です。インシデントがデータ侵害にエスカレーションされた場合は、より広範なビジネスに役立つ事前構築済みワークフローと評価機能により、セキュリティ チームと連携して適切に対応できます。

IT セキュリティ脆弱性プログラム

Archer IT Security Vulnerabilities Program は、Big Data アプローチにより、リスクの高い脅威を特定して優先順位を付けるセキュリティチームを支援します。資産のビジネス コンテキスト、実用的な脅威インテリジェンス、脆弱性評価の結果、包括的なワークフローの組み合わせにより、IT セキュリティ リスクをプロアクティブに管理できます。IT 資産に、完全なビジネス コンテキスト オーバーレイを使用してカタログを付けることができるため、スキャンおよび評価の作業のより適切な優先順位付けが可能になります。この統合された脆弱性調査プラットフォームにより、IT セキュリティ アナリストは警告を実施し、脆弱性スキャンの結果を調べ、発生した問題を分析することができます。強力で柔軟なルール エンジンによって、新たな脅威、対応が遅れている問題、ビジネス ニーズの変化が浮き彫りになります。既知の脆弱性リスクを、適用されたビジネス コンテキストに関連付ける機能によって、応答と修復の作業に優先順位を付け、大きなギャップの解消にかかる時間を短縮し、コストを削減することができます。

IT リスク管理

Archer IT Risk Management を使用すると、IT リスク管理のために、組織の要素とIT 資産をカタログ化できます。このユース ケースには、IT リスクをカタログ化するリスク登録、IT 向けの構築済みリスク評価、構築済みの脅威評価手法、IT 統制を文書化するカタログが含まれています。RSA Archer Issues Management は、リスク アセスメントから生じるギャップと所見を管理するためにも含まれています。

IT リスクを明確に把握することにより、評価プロセスを合理化し、IT リスクの特定を迅速化し、適時にレポートを作成できます。リスクと内部統制を結び付けることで、IT 管理要件の伝達と相関が容易になるため、コンプライアンスのギャップを解消し、リスク軽減戦略を改善することができます。この機動性の高いリスク管理フレームワークによって、ビジネスにおける要件の変化に遅れることなく対応し、影響が最大のIT リスクにリソースを集中することができます。

PCI 管理

Archer PCI Management を使用すると、ペイメント カード インダストリー（PCI）のコンプライアンス プロセスの合理化と評価の自動化を行い、準拠に必要な労力を削減することができます。組織のプロジェクト管理アプローチでPCI コンプライアンス プログラムをすばやく開始し、継続的な評価を効率的に実施することができます。また、体系的なレポートを作成し、リスクの管理と軽減に必要な可視性を得ることができます。Archer PCI Management は、他のRSA Archer のGRC ソリューションと完全に統合されているため、効率的で持続可能なPCI コンプライアンス プログラムを実装し、容易に結果をまとめて、より広範な企業リスクおよびコンプライアンス パフォーマンス メトリックを通知することができます。

IT 規制管理

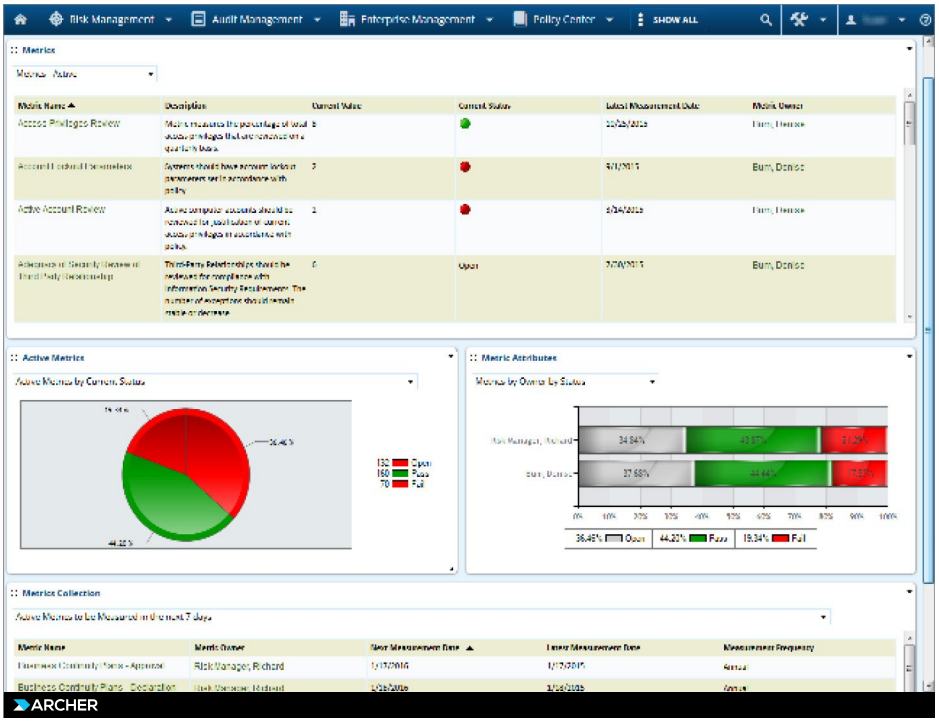
Archer IT Regulatory Management には、IT 環境と機密データ環境に影響を及ぼす外部の規制義務を文書化するために必要なツールと機能が用意されています。これが、ビジネスとIT のコンプライアンス リスクの変化に組織が対応するための、機敏性のあるポリシー フレームワークの基盤となります。組織は、体系的なレビューと承認のプロセスを確立して、規制義務の変化を追跡し、ビジネスへの影響を理解し、対応に優先順位を付けることができます。その後、企業が順守しなければならない規制とその他のコンプライアンス要件について、正確なガイダンスを、経営幹部およびIT 部門に迅速に提供できます。IT コンプライアンス要件と内部統制のつながりを強化することにより、ギャップを縮小し、ビジネスに影響を与えるIT 関連の問題について、経営幹部がより詳細なインサイトを得ることができます。

情報セキュリティ管理システム

Archer Information Security Management System では、お客様のISMS を迅速に精査し、レポートおよび認定のための適用宣言書を文書化します。また、情報資産、アプリケーション、ビジネス プロセス、デバイス、施設などの情報セキュリティ管理システム（ISMS）に関連する個々のリソースをカタログ化することも、関連するポリシー、標準、リスクを文書化して維持することもできます。このように情報セキュリティ管理システムを一元化することにより、資産間の関係を把握し、インフラストラクチャへの変更を管理することが容易になります。アセスメント時に指摘された問題は一元的に追跡することができ、ギャップの改善作業を一貫して文書化し、監視することにより、効率的に対処できるようになります。

まとめ

Archer IT & Security Risk Management によって、セキュリティへのビジネス リスクベースのアプローチが提供されるため、今日のセキュリティの脅威、調整が不十分なセキュリティ対策、運用上のセキュリティ コンプライアンス障害のリスクを軽減できます。セキュリティのビジネス コンテキストを確立し、セキュリティのポリシーと標準を文書化して管理することができます。また、攻撃を検知して対応し、セキュリティの脆弱性を特定して修復することができます。



Archerについて

Archerは、統合リスク管理（IRM）ソリューションのリーディングプロバイダーであり、お客様の戦略的意思決定と業務回復力の向上を、ビジネスとITの両方の影響を主軸に行う定性・定量分析をサポートする近代技術プラットフォームにより可能にします。 GRCソフトウェアの真のパイオニアとして、Archerは、従来の業務運営リスクからESGのような新しい問題に至るまで、お客様がリスクとコンプライアンスの領域を管理できるよう支援することに唯一専念しています。 リスク管理業界で20年以上の実績を持つArcherの顧客基盤は、世界最大の純粋なリスク管理コミュニティの1つであり、Fortune 500企業の50%以上を含む1,200以上の顧客を有しています。

www.ArcherIRM.com