Deloitte.

ガバナンス・リスク・コンプライアンス（GRC）ソフトウェア導入事例集

トーマツ.

目次

各事例の利用目的の関係を示しています

対応業務マトリクス

	ERM	情報セキュリティ	業種特有法令対応	ベンダー	ポリシー	インシデント	SOX	内部監査
事例①	◎		○					○
事例②			◎		○			○
事例③	◎	○					○	○
事例④		◎		○		○		○
事例⑤	◎				○	○		○
事例⑥	○		◎		○	○		○
事例⑦		○	◎				○	○
事例⑧							◎	○
事例⑨		○		◎		○		○
事例⑩			◎		○			○

【凡例】 ◎：GRCソフトウェア導入の際にターゲットとした業務
○：GRCソフトウェア導入により副次的に対応が可能な業務

事例概要一覧

事例概要一覧

事例No	業種	課題／改善ポイント	GRCソフトウェアで実現できたこと
1	製造業	1. 多角化した事業の複雑化したリスク、法規制対応 2. リスクの顕在化によるブランディングの低下	1. 経営者によるコミットメント 2. 将来的な変化を見据えたグループの管理階層の設定 3. グループ全体のリスクマネジメント、コンプライアンス関連情報の一元管理 4. 一元管理された情報の見える化
2	アミューズメント	1. コンプライアンスプログラムの多様化、複雑化による対応品質の維持 2. グループ全体のコンプライアンス強化	1. 各種コンプライアンスプログラムの要求事項を単一のポリシーとして整理（SOX、PCIDSS、SafeHarbor） 2. 制定したポリシーに基づく、推進部門と対象部署の業務フローの整理 3. 施策運用の効率化
3	食品	1. 組織の複雑化に伴うリスク・コンプライアンス要件の増加 2. Cクラスのタイムリーな情報把握（リスク対応状況など）	1. 中期計画等の意思決定に必要な情報についての内容とレポートスピードについての分析、マネジメントの同意と施策の統合 2. レポーティング手段としてGRCソフトウェアの活用
4	情報・通信	1. 複数のセキュリティ部門の独自管理により、全社的な管理ができない 2. 経営者へのレポーティングへ、各事業のリスク情報活用	1. 複数のセキュリティ部門のポリシーを統合と、全社共通の情報セキュリティ基準、法令対応基準の作成 2. 事業毎で分散しているリスク情報の一元管理 3. 全社共通基準の協業ベンダーへの運用の徹底

事例概要一覧

事例No	業種	課題／改善ポイント	GRCソフトウェアで実現できたこと
5	ネット通信販売	1. 事業毎にリスク評価基準がばらばら 2. 事業別のリスク情報収集に時間が掛かり、全社的な観点でのリスク管理ができない	1. 各事業で利用するリスク評価基準の全社統一化し、リスク管理レベルの均一化 2. リスク情報の集約化と、全社的な観点でのリスク管理の実現
6	保険	1. 自社独自のITインフラがうまく機能していない 2. リスク情報が複雑化し、全社レベルでの集約が困難 3. 非効率なリスク・コンプライアンス管理	1. 各国の事業拠点のリスク対応情報や法令対応情報を一元管理 2. リスク管理部門のオペレーションを自動化し、必要工数の削減 3. 全社のリスク情報閲覧、意思決定フローが行えるように柔軟なワークフローシステムの整備
7	クレジットカード	1. 複雑化・多様化するコンプライアンス管理業務の効率 2. リスク情報やコンプライアンス情報の全社レベルでの包括的な把握	1. 事業拠点ごとに行われて重複しているコンプライアンス対応業務の統合 2. リスク情報やコンプライアンス情報の一元管理

事例概要一覧

事例No	業種	課題／改善ポイント	GRCソフトウェアで実現できたこと
8	資源開発	1. SOX対応業務の強化・効率化 2. SOX対応状況の見える化 3. レポートのリアルタイム化	1. SOX対応に必要なデータの自動化 2. 業務プロセスの定義の共通化 3. システムへの入力タイミング等の方針や規律の徹底
9	配送事業	1. 情報セキュリティ関連のインシデントの増加 2. 外部委託先管理の強化	1. 情報セキュリティマネジメントPDCAサイクルのシステムライフサイクルプロセスへの組み込み 2. 外部委託先情報等の一元管理
10	保険	1. 事業拠点の業務プロセスの違いにより情報の集約が困難 2. グループ全体でSolvency Ⅱと各国ごとの法令対応にかかる膨大な工数	1. 各国で対応している法令対応の情報の集約によりオペレーションの集約 2. 統合要求事項に対応する重要リスクとコントロールの管理 3. 各事業拠点での個別カスタマイズが可能なグループ標準のレポート機能を確立と、管理レベルの均一化

個別導入事例

事例①:グローバル製造業A社(連結売上高:約1500億ドル)

概要:さまざまな事業をグローバルで展開している企業が、同一の組織階層でリスク、コンプライアンスに関する情報を統合し、全社の事業影響度の観点で「見える化」した。

背景

1. 製造業を中心に10以上の事業を全世界レベルで実施している中で、各事業や地域・国独自のものを含め自社が対応すべきリスクや法規制対応が複雑化していた
2. リスク事象(インシデントを含む)の発生による自社のブランディングの低下を懸念した経営陣の課題感からトップダウンで見直しを行った

目的

1. 自社の事業・組織の管理階層を設定し、その構造をもとにグループ会社、海外拠点を含めて、すべてのリスクマネジメント、コンプライアンスに関する情報を統合し、一元的に管理することを目指した
2. 一元的に管理をもとに施策の「見える化」を行い、全社への事業への影響度の観点で再整理することで、業務の効率化と管理の強化を行う

アプローチ

1. 経営者の意思決定として、企業グループ全体で、プロジェクトの継続的な推進へのコミットメントを行った
2. 将来的な変化も見据えてグループの事業、組織、グループ会社など、実際の事業構造にあわせた管理階層(ヒエラルキー)を決定
3. 決定した管理階層にあわせ、海外拠点、子会社を含むグループ全体で行っているリスクマネジメント、コンプライアンス関連の施策に関する情報の一元管理を実施
4. 一元管理された情報をもとに「見える化」を行い、各施策を事業影響度の観点で再整理し、効率性と強化の必要性の観点から見直しを実施

成果

1. 経営に関する情報を一元管理し、経営層が必要な単位で活用できることにより、経営層のリスク、コンプライアンスへの関心が高まり、結果的に全社レベルで意識や対応力が向上した
2. 統一された管理階層をもとに、経営への影響度の観点から、各施策を整理したことで、各施策の実施内容の過不足を一元的に把握できた
3. 施策横断的に情報を「見える化」することで、自社が対応すべきリスクに対し、各施策間での「重複」、「抜け・漏れ」を確認が可能となり、業務の効率性と強化の必要性の両面から各施策の見直しを実現した

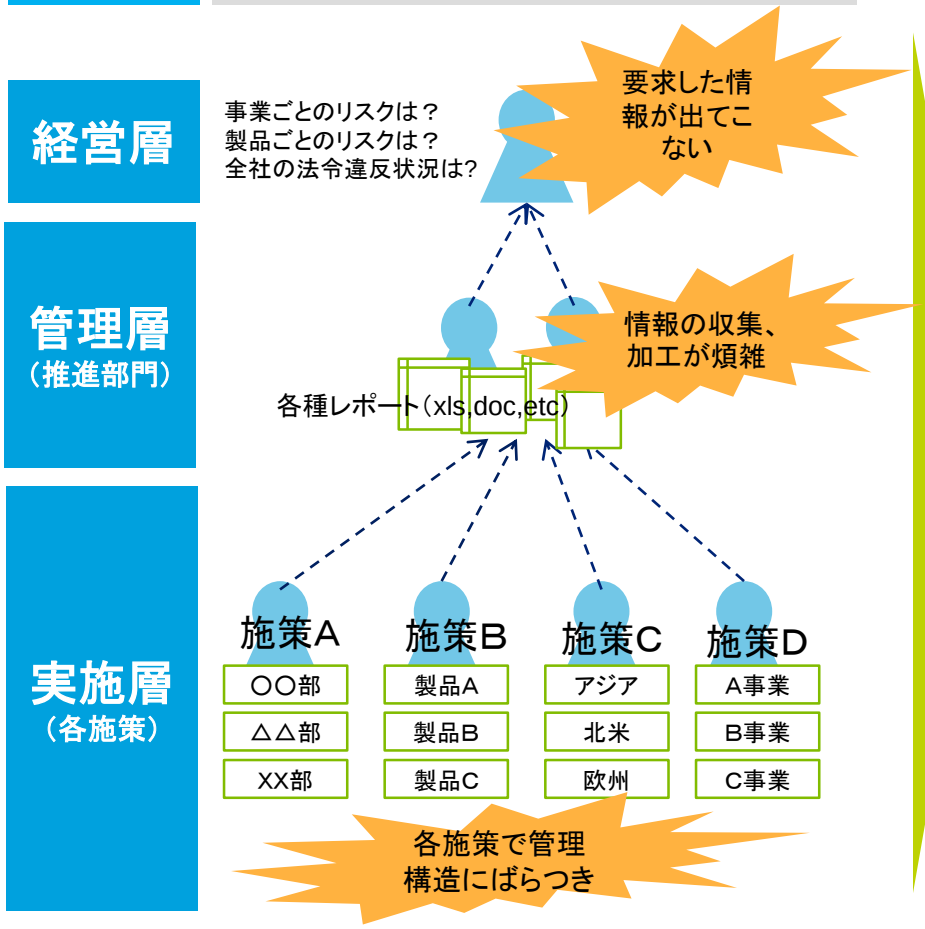
貴社で検討する上で参考にしていただきたいポイント

情報管理:自社の事業・組織の構造にあわせた施策横断的な管理階層(ヒエラルキー)の設定とそれに基づいた全施策の情報一元管理の実施
情報伝達:一元管理された情報をもとに施策横断的な観点でのモニタリングの実現(経営への影響度、業務効率性、実施体制の脆弱性等)

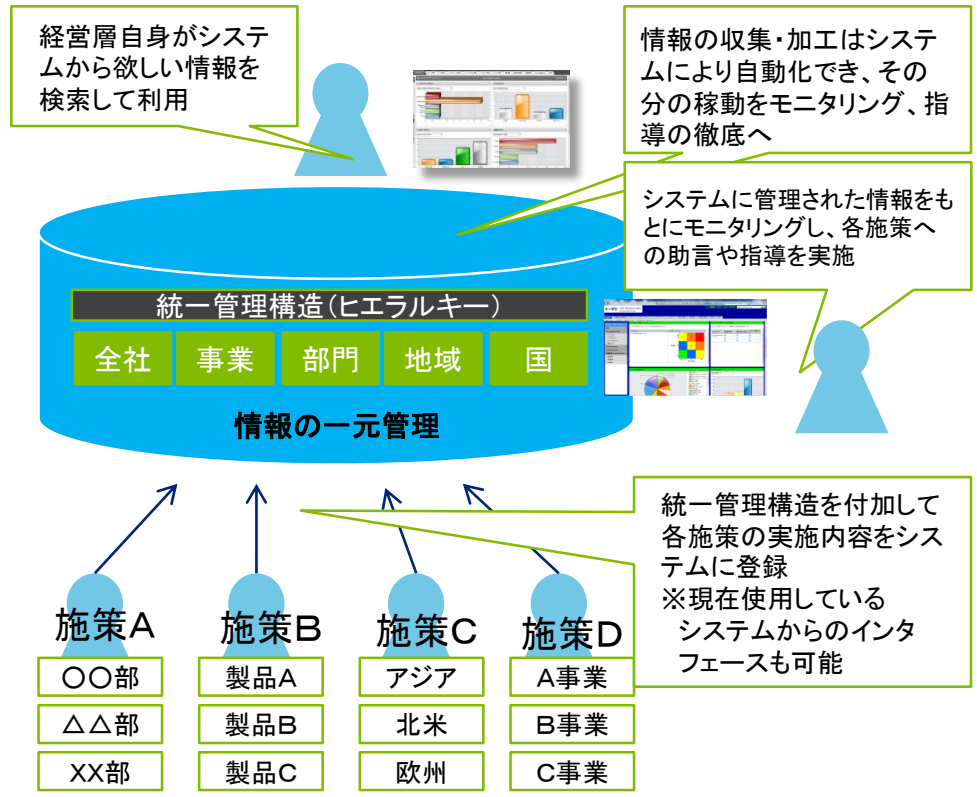
事例①:グローバル製造業A社　～効率化実施イメージ～

施策横断的な管理構造ヒエラルキーをもとにした情報の一元管理の実施

実施前　施策ごとで管理構造にばらつき



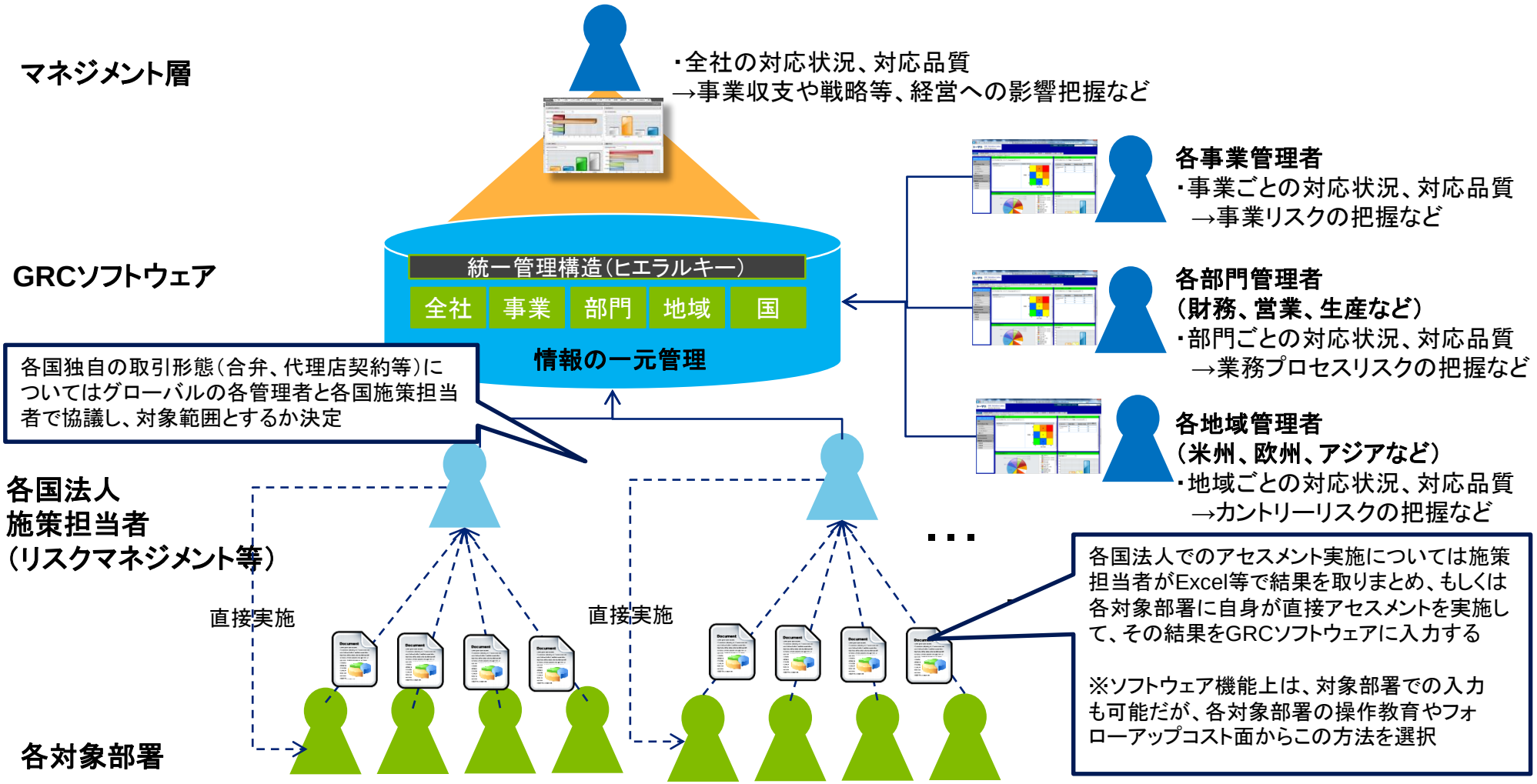
実施後　管理構造を統一して情報を一元管理



※本図は必ずしもA社の具体的な管理体制や施策を反映したものではありません

事例①:グローバル製造業A社　～GRCソフトウェア活用イメージ～

各国の施策担当者でGRCソフトウェアを利用　→主に対応内容の把握、とりまとめ、分析に活用



※本図は必ずしもA社の具体的な管理体制や施策を反映したものではありません

事例②：アミューズメントB社（連結売上高：約400億ドル）

概要：自社のブランディングの継続的な維持・強化を目的として、全世界に展開する複数の異なる事業部門に対するコンプライアンスプログラムを統合した。

背景

1. 自社が対応すべきコンプライアンスプログラムの多様化、複雑化により、各事業部門への負担が増大しており、各部門での対応品質維持に苦慮していた
2. 自社のブランド維持のために、各事業部門の負担を軽減しつつ、グループ全体のコンプライアンス強化を行う必要があった

目的

1. 独立して実施していた、SOX法対応（IT全般統制）とPCIDSSの整理
2. 自社保有ライセンス許諾に関するSafe Harbor管理のコンプライアンスプログラムを単一のフレームワークをもとに統合要求事項として整理し、共通アセスメントで複数の法令規制要求事項に対応できるようにする
3. これにより各事業部の負担軽減と全社としてのコンプライアンスの強化

アプローチ

1. 各コンプライアンスプログラム（SOX、PCIDSS、SafeHarbor）の要求事項を単一のポリシーとして整理した（特にエビデンスの重複の面を重視した）
   ※ 単なるポリシーの制定にとどまらず、それぞれの施策における各事業部へのアセスメント項目や収集するエビデンスの内容まで踏み込んだ
   ※ 各施策での要求事項の重複を排除するだけでなく、施策横断的に抜け・漏れを確認し、それらに対する要求事項、アセスメント項目を追加した
2. 制定したポリシーをもとに各施策の推進部門と対象部署での業務フローを整理した
3. 統合ポリシー、業務フローをGRCソフトウェアに実装し、施策運用の効率化を図り、その分各事業部との直接的なコミュニケーションを実施した

成果

1. 効率化：評価活動・エビデンス収集の効率化により、各施策推進部門と対象部門の負荷軽減が実現できた
2. 対応の強化：GRCソフトウェア（Archer）への情報一元管理により、発見事項（問題）の早期把握と解決の早期化を行った
3. 意識改革：効率化できたコンプライアンス担当者の時間をエンドユーザへのプログラム徹底とコミュニケーションの向上に活用することで、全社的な対応レベルの底上げを行った
   ※ さらに将来的に発生する対応すべき法令・規制対応にも、同ポリシーに収斂させることで継続的な効率化と対応力向上が期待される

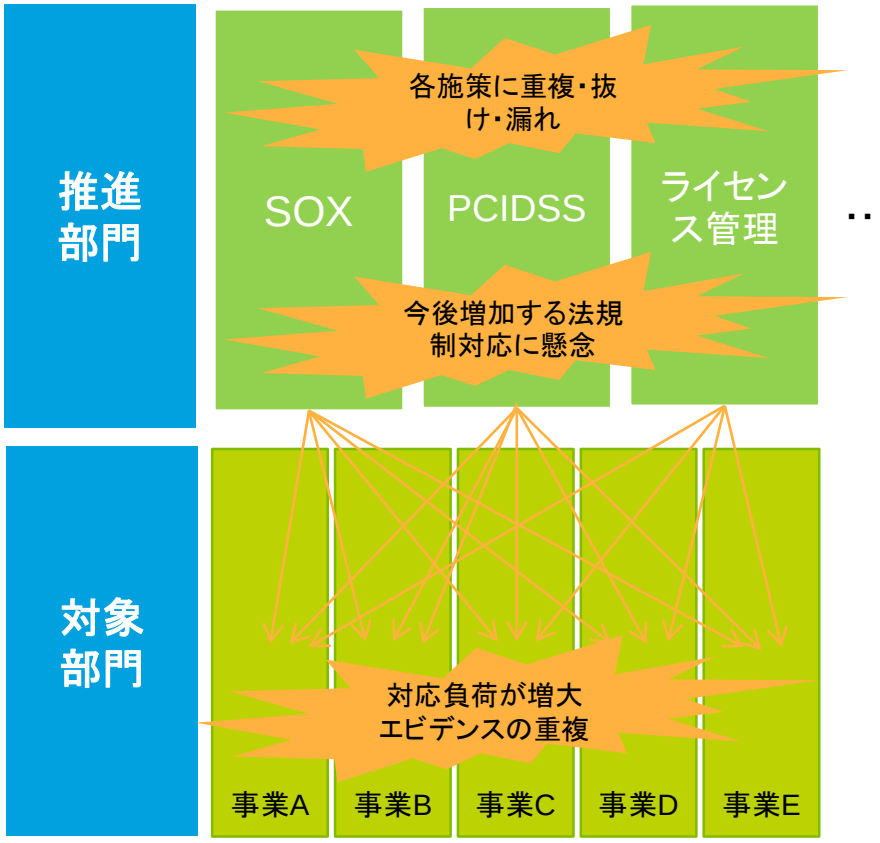
貴社で検討する上で参考にしていただきたいポイント

情報管理：各施策で重複する要求事項、アセスメント項目を統合要求事項として再整理し、可能な範囲で統合を行う
情報伝達：統合要求事項をもとに現行の各施策の対象と業務フローを見直し、1回のアセスメントで複数の施策に対応できるようにする。
GRCソフトウェアを活用することで、推進部門と対象部門の業務効率化を図り、効率化できた時間を各部門とのコミュニケーションにあてた

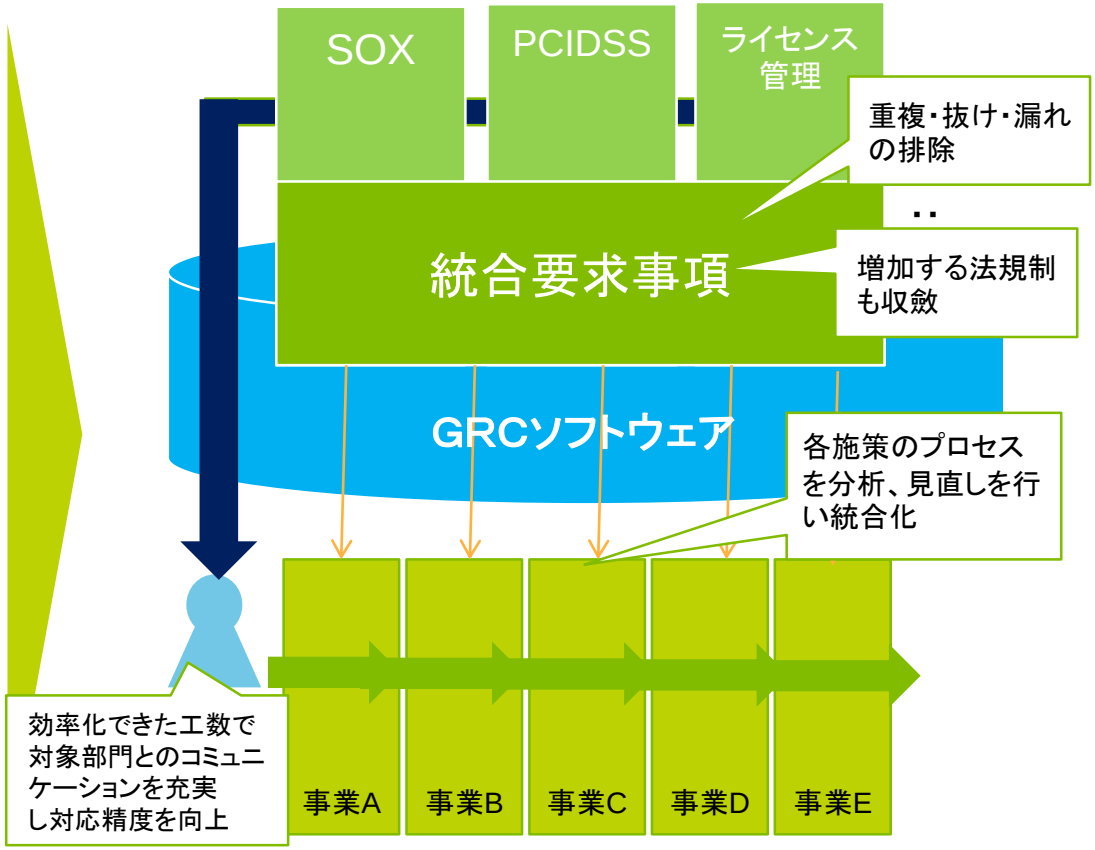
事例②:アミューズメントB社　～効率化実施イメージ～

施策横断的な統合要求事項をもとに施策自体の統合を実現

実施前　施策実施に対象部門の負荷が増加



実施後　統合要求事項をもとにした施策の統一



※本図は必ずしもB社の具体的な管理体制や施策を反映したものではありません

事例③：食品C社（連結売上高：約540億ドル）

概要：M&Aや合弁企業、さらにグローバル化など事業展開が複雑化する同社が経営層、各事業、地域・国の責任者に対する寄与を目的とし、リスクマネジメント等の施策を統合し、報告・意思決定の迅速化を図った。

背景

1. 組織体系の複雑化により、自社が対応すべきリスクやコンプライアンス要件が増加し、全体が見えにくい状況となっていた
2. 各事業、地域、国の責任者（Cクラス）が自身の職責で取り組むべきリスク、コンプライアンス対応状況を担当者に確認していたが、情報収集・加工に時間がかかり必要なタイミングで情報が入手できなかった

目的

1. 経営層及び各組織の責任者へ、有用な内容とスピードでの報告実施を目的として、それまで個別に実施していたさまざまなリスクマネジメント、コンプライアンス、ITセキュリティに関する施策を統合した
2. 経営上の意思決定に役立つ報告をタイムリーに実施することで、上層部にリスク、コンプライアンス対応の重要性を意識づけた

アプローチ

1. 中期計画等の戦略や経営層、各組織の責任者から発信されたメッセージをもとに、トップマネジメントが意識すべきリスク・コンプライアンスの内容と、それを経営上の意思決定に役立てるために必要な情報について、その内容と速さについて分析し、各マネジメントに同意を得た
2. 上記の内容と迅速性を確保するため、可能な限り施策の統合を行った
3. 経営層、各組織の責任者への迅速・正確な報告を行う手段の1つとして、GRCソフトウェアを活用した

成果

1. 20以上のリスクアセスメントプロセスを統合
2. 初年度で50%の対応コスト削減
3. 10以上の複雑な組織構造に対して統合管理を実現
4. 20以上の組織、40以上の事業部門に対してリアルタイムなレポート配信
5. 経営層へのリスク・コンプライアンス報告の迅速化

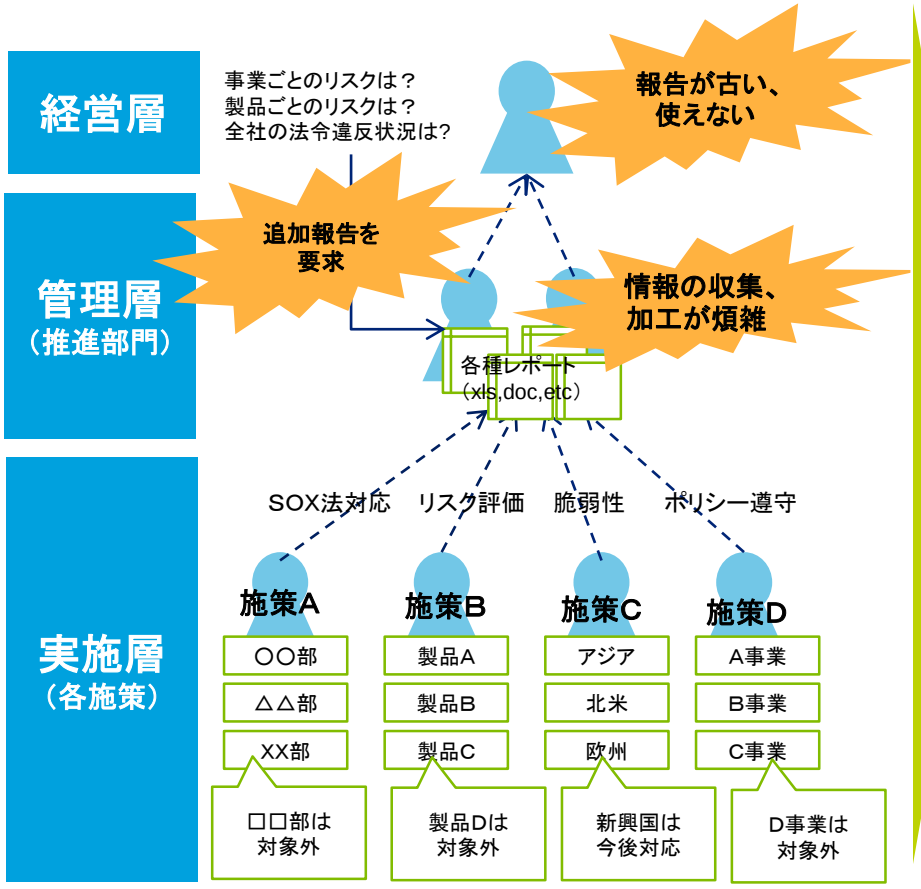
貴社で検討する上で参考にしていただきたいポイント

情報活用：経営に寄与する視点から情報の活用を促進する → Cクラスのニーズの把握とそれを実現するための報告の実現
情報管理：報告作成のための負荷の軽減→収集・加工に関する工数の削減

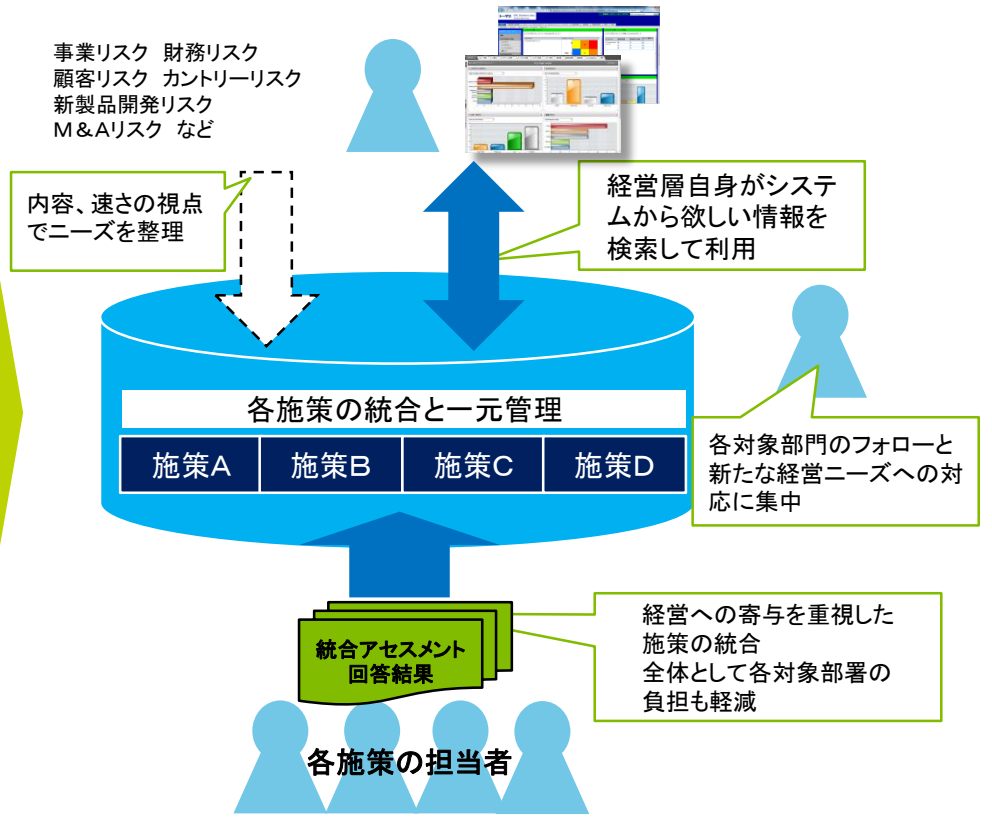
事例③:食品C社　～効率化実施イメージ～

経営に寄与する報告を実現するための情報活用の実現

実施前　経営陣、事業責任者のニーズにあわせた報告ができていない



実施後　経営への寄与の視点で施策を統合し効率化を実現



※本図は必ずしもC社の具体的な管理体制や施策を反映したものではありません

事例④:グローバル情報・通信業D社（連結売上高:約600億ドル）

概要:多数の事業で分散した社内情報を1つのITインフラにより統合し、全社的な基準を統一することによって、経営者への全社レベルでのリスク情報のレポーティングを可能した。

背景

1. 複数のセキュリティ部門で独自の情報セキュリティ基準に基づいたリスク対応を行っており、全社的な視点での管理ができていなかった
2. 経営者へのレポーティングを行う際に、分散した個別事業ごとのリスク情報を効果的に活用することができていなかった（事業間でのリスクの比較などを行うことができなかった）

目的

従来まで基準が別々で分散した状態で有効活用できていなかったリスク情報を、全社共通のITインフラ整備と情報一元化により、全社レベルで取りまとめ、経営者へ事業毎でのリスク情報、リスク対応状況を効果的にレポーティングする。

アプローチ

1. 複数のセキュリティ部門で使用されている情報セキュリティ基準や法令事項を統合し、全社共通の情報セキュリティ基準、法令事項を作成した
2. 分散している各事業の情報（ITリスクやインシデント情報、等）を全社共通の情報セキュリティ基準、法令事項に対応する形で1つのITインフラ上で統合した
3. 外部会社（協業ベンダー等）に対しても全社で統一した情報セキュリティ基準の適用、および継続運用を徹底した

成果

1. 複数のセキュリティ部門で別々の情報セキュリティ基準に基づいて対応を行っていたものを全社的に統一することによって、今まで非効率であったリスク対応活動を効率的に実施することが可能になった

2. 多事業でのリスク情報を集約するITインフラを整備することによって、各事業でのリスク情報を迅速に把握し、経営者へのレポートティングが可能になったことで、影響度の高いリスクへの対応速度を加速化させた

貴社で検討する上で参考にしていただきたいポイント

情報管理:各種基準（セキュリティ基準、等）を全社レベルで統一することによって、リスク対応レベルの均一化と高度化が可能
情報活用:全社共通のITインフラを整備することによって、経営者が求める情報（リスク情報、等）を迅速に収集・活用することが可能

事例④:グローバル情報・通信業D社　～統合イメージ～

事業毎に分散していた各種情報の一元管理の実施

実施前　重要なリスク情報を分散して管理

経営層
管理層
各種事業部

・事業間でのリスクの比較
・リスク対応の優先度
・リスク対応状況のモニタリングが迅速に行えない。

全社レベルでのリスク情報が得られない

情報の粒度、精度が分散

ソフトウェア販売事業	ゲーム事業	アプリケーション開発事業	ハードウェア販売事業
情報資産	クレジットカード情報	ログ監視	情報資産
個人情報	ログ監視	情報資産	インシデント(バグ)
契約情報	インシデント(バグ)	インシデント(バグ)	契約情報

各事業で情報管理体制にばらつき

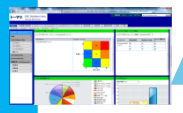
実施後　リスク情報を一元化し有効活用

経営者に全社レベルでレポートティングし、経営判断の迅速化

・重要リスクに対する経営層の意思決定を伝達

各種情報を全社的に管理

情報資産 / 個人情報 / 契約情報 / インシデント(バグ) / ソースコード



共通基準に基づく情報の一元管理

・各事業へのリスク対応指示
・リスク対応状況のモニタリング

ソフトウェア販売事業	ゲーム事業	アプリケーション開発事業	ハードウェア販売事業
情報資産	クレジットカード情報	ログ監視	情報資産
個人情報	ログ監視	情報資産	インシデント(バグ)
契約情報	インシデント(バグ)	インシデント(バグ)	契約情報

※本図は必ずしもD社の具体的な管理体制や施策を反映したものではありません

事例⑤：海外ネット通信販売業E社 （売上高：約35億ドル）

概要：リスク情報管理を統一のITインフラで行い、全社的なリスク評価基準の整備とリスク対応フローの確立、モニタリングを行った

背景

1. リスク評価基準が事業部毎に異なり、重要度の意味合いや発生可能性などの定義にばらつきがあった
2. リスク情報が複数のシステムで管理され、収集に時間が掛かっていた。
3. 全社リスク、個別リスクを関連付けずに管理され、全社的なリスク管理ができていなかった

目的

1. 全社統一のリスク評価基準の作成を行い、リスク管理レベルの均一化を図る
2. 分散したリスク情報を1つのITインフラで統一し、情報活用の迅速化を図る（一貫したリスク対応フローの確立と対応状況の可視化）

アプローチ

1. 各事業部で適応しているリスク評価基準を全社レベルで統一化し、リスク管理レベルの均一化を行う
2. 全社共通のITインフラを整備し、リスク情報管理の基盤の確立
3. 各事業部で発生する細かなリスク情報（インシデント情報、等）を集約することによって、全社的なリスクの把握と対応を行う

成果

1. 単一のITインフラに集約されたリスク情報をもとに、全社で統一されたリスク評価基準、およびリスク対応フローを作成し、リスク管理レベルの均一化とモニタリングの効率化を図ることができた
2. 各事業部で日々発生する個別リスクを集約・評価することで、全社で対応しなければいけないリスクの選定と対応を迅速化するこができた

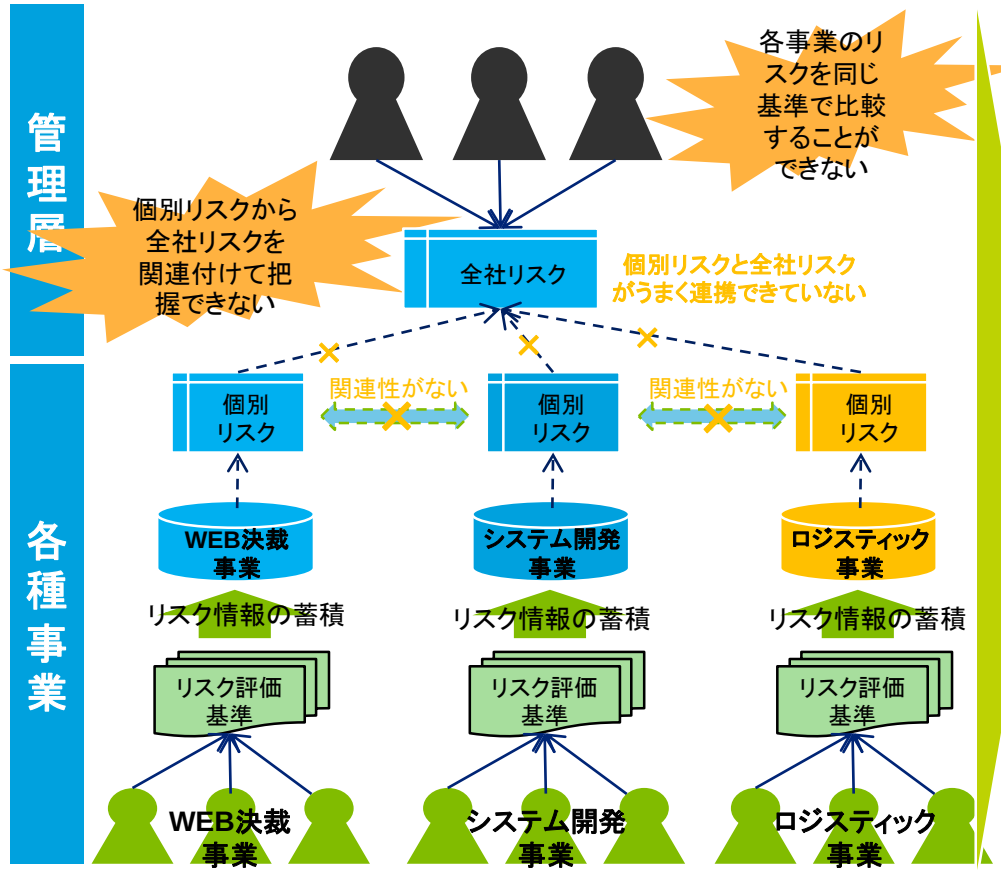
貴社で検討する上で参考にしていただきたいポイント

情報管理：リスク評価基準を全社レベルで統一することによって、リスク対応レベルの均一化と高度化が可能

事例⑤：海外ネット通信販売業E社　～統合イメージ～

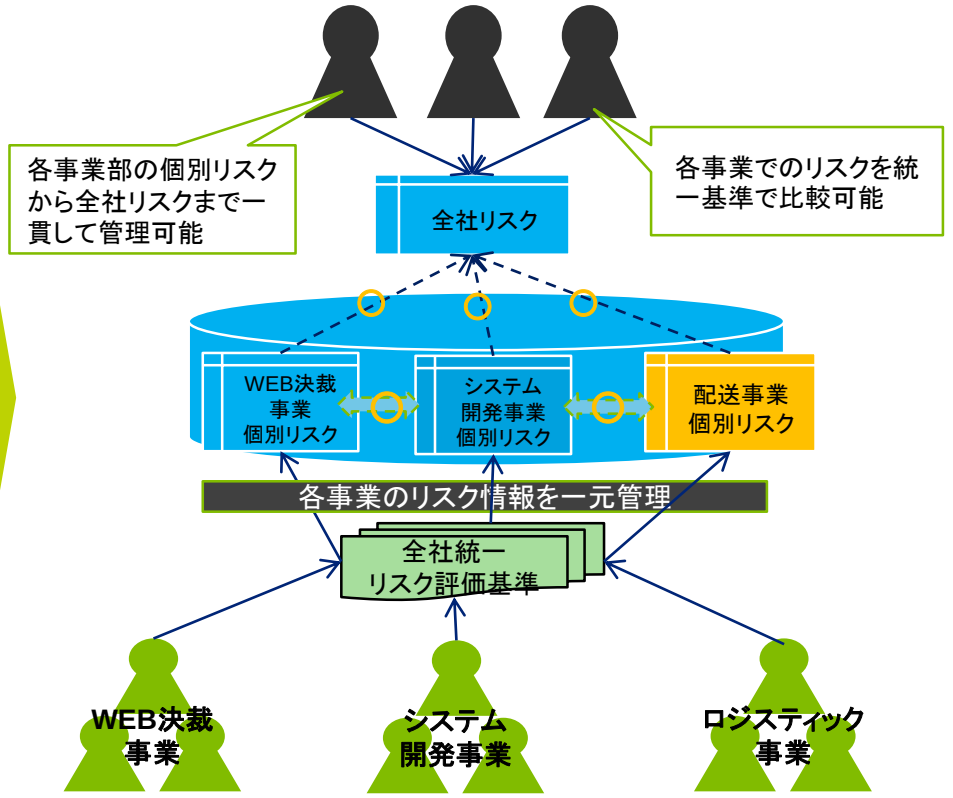
事業毎に異なるリスク評価基準を統合

実施前　事業毎にリスク評価基準に違いがあり別々のITインフラで情報管理を行っていた



事業毎のリスク管理体制

実施後　リスク評価基準、リスク情報を同じITインフラ上で統一管理した



※本図は必ずしもE社の具体的な管理体制や施策を反映したものではありません

事例⑥：保険会社F社 （総資産：約200億ドル）

概要：各国でのリスク情報、法令対応情報を一元管理し、管理部門のオペレーションを自動化することによって、コンプライアンス管理の高度化を図った。

背景

1. 従来、自社独自のITインフラを導入していたがうまく機能していなかった
2. 20ヶ国以上の事業拠点で独自のリスク対応や各国特有の法令対応を行っており、リスク情報が複雑化し全社レベルでの集約が困難であった
3. 経営者へのレポート機能が確立されておらず、意思決定から各国現場へのフィードバックに時間が掛かり、非効率なリスク管理、コンプライアンス管理を行っていた

目的

1. 各国で行っているリスク対応や法令対応に関する情報を一元管理しモニタリング可能な運用を行うことで、全社でのコンプライアンス対応状況の透明性を確保する
2. 共通の管理システム（レポート機能や承認機能を含む）を導入することで、経営者の意思決定プロセスを迅速に行う

アプローチ

1. 全社共通のITインフラを整備し、各国の事業拠点のリスク対応情報や法令対応情報を一元管理できるようにした
2. リスク管理部門でのリスク情報収集・モニタリングなどのオペレーションをシステムにより自動化して、必要工数の削減を行った
3. ITインフラ上で各国のリスク情報を確認し、かつ意思決定フローも同一のシステム上で行えるように柔軟なワークフローシステムを整備した

成果

1. 管理部門のオペレーションを自動化することにより、工数削減（月10時間以上）が可能になり余剰工数を管理体制の強化へ回すことができた
2. 各国の情報を一元管理することによって、新たな法令対応が発生した場合に修正が必要な規程、リスク対応基準を迅速にアップデートすることができた
3. 共通のITインフラ上でリスク情報のレポートから現場へのフィードバックが可能になり、経営者の意思決定を迅速に行い全社レベルでのコンプライアンス管理体制の改善が可能になった

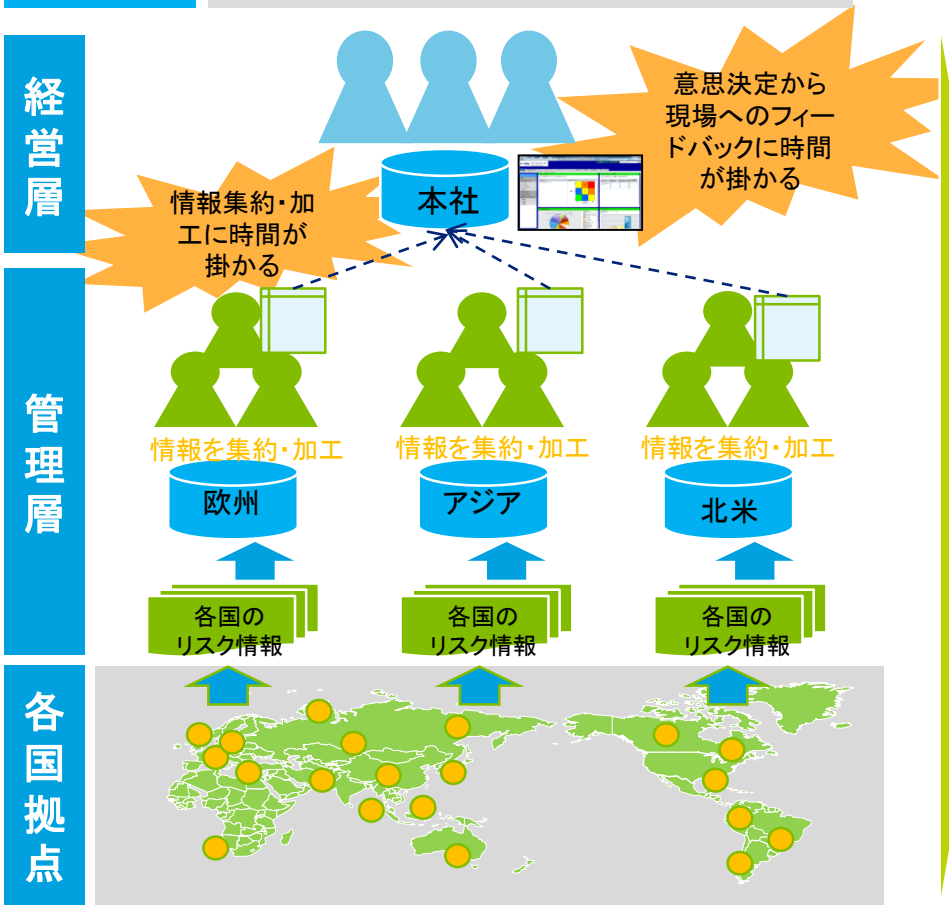
貴社で検討する上で参考にしていただきたいポイント

情報管理：国別の法令対応、リスク情報などを一元管理することによって、管理部門の対応工数の削減が可能
情報伝達：新たな法令対応やリスクが発生際、ワークフローシステムの活用により全社の規程修正や、リスク管理が迅速に行うことが可能
情報活用：共通のITインフラを導入することによって、経営者へのレポート、現場へのフィードバックを迅速に行い、管理レベルの高度化が可能

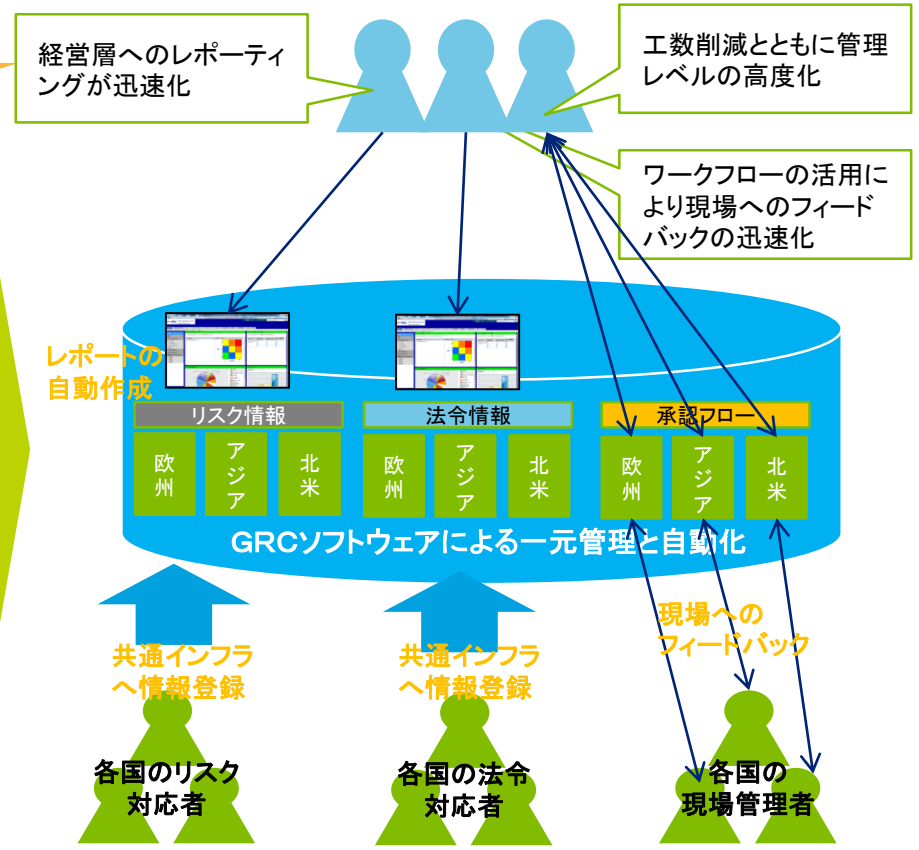
事例⑥：保険会社F社　～マネジメントレポート自動化イメージ～

各国の情報をITインフラで統合し、マネジメントレポート作成を自動化

実施前　各国の情報収集からレポート作成に時間が掛かり、非効率な状態であった



実施後　各国からの情報を元に、レポート作成を自動化し、管理層の工数削減を実現した



※本図は必ずしもF社の具体的な管理体制や施策を反映したものではありません

事例⑦：クレジットカード事業G社（連結売上高：約300億ドル）

概要：グローバル展開している企業がGRCソフトウェアを導入し事業拠点ごとのコンプライアンス対応業務を統合・整理することで、
コンプライアンス管理業務を強化・効率化した。

背景

1. コンプライアンス対応業務が複雑化・多様化する中で、グローバル展開している複数の事業拠点がそれぞれ別々にコンプライアンス管理業務を行っていたため、全社レベルの観点からコンプライアンス管理が行えず、重複する業務などもあり非効率であった
2. リスク情報やコンプライアンス情報を管理するシステムも各事業拠点で別々であったため、リスク情報やコンプライアンス情報を全社レベルで包括的に把握することが困難であった

目的

1. 事業拠点ごとにそれぞれ行われているコンプライアンス対応業務を統合し、コンプライアンス管理業務の効率化を図る
2. 事業拠点ごとに別々のシステムに入力していたリスク情報やコンプライアンス情報を一元管理し、全社レベルで包括的に把握できるようにする

アプローチ

1. 事業拠点ごとに行われて重複しているコンプライアンス対応業務を統合するために、GRCソフトウェアを導入するとともに、システムへの入力者やプロセスオーナー等の業務プロセスを全社レベルでの観点から整理し、事業拠点間や部門間の役割を明確にした
2. リスク情報やコンプライアンス情報を全社レベルで包括的に把握するために、PCI DSS（クレジット業界におけるグローバルセキュリティ基準）やSOX等のコンプライアンス情報を全事業拠点共通のGRCソフトウェアに一元管理し、入力されたリスク情報やコンプライアンス情報を紐付けて、事業拠点ごとの比較や、事業拠点にまたがって共通に認識されるリスクを見える化した

成果

1. 全社レベルでの観点から業務プロセスを整理し、事業拠点間や部門間の役割を明確にしたため、業務の重複が統合され、コンプライアンス管理業務が効率化した
2. リスク情報やコンプライアンス情報が全社共通のGRCソフトウェアで一元管理されたため、データの紐付けが容易となり、リスク情報やコンプライアンス情報を全社レベルで包括的に把握することができるようになった

貴社で検討する上で参考にしていただきたいポイント

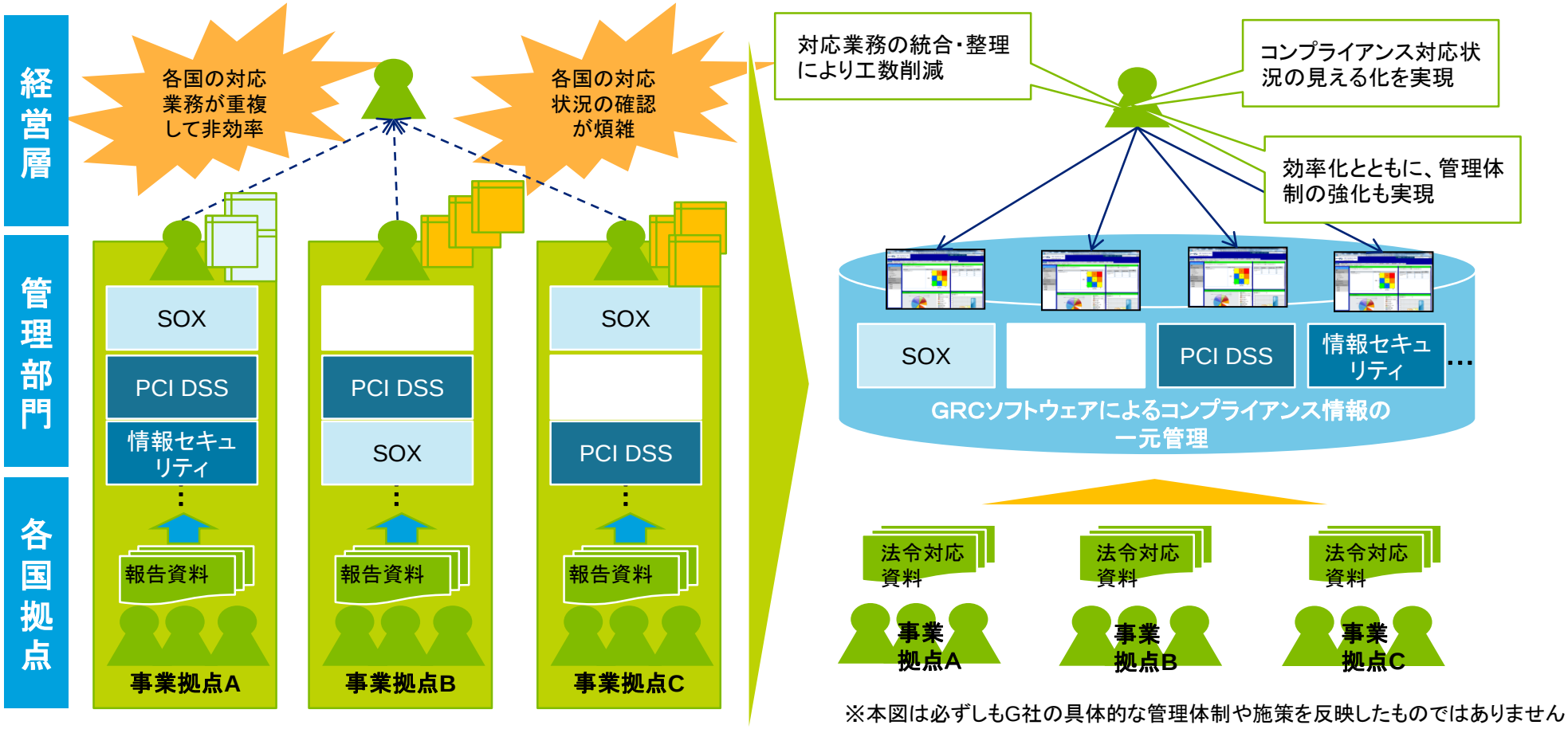
情報管理：GRCソフトウェアを導入することで情報を一元管理することができ、リスク情報やコンプライアンス情報の紐付けが容易となる
情報伝達：全社共通のシステムに情報が集約されるため、リスク管理やコンプライアンス管理の状況を全社レベルで包括的に把握できる

事例⑦：クレジットカード事業G社　～統合・整理イメージ～

各国の事業拠点のコンプライアンス対応業務を統合・整理

実施前　各国のコンプライアンス対応業務が複雑化し、全社レベルで管理できていない

実施後　各国事業拠点の業務を統合・整理し、全社レベルでのコンプライアンス管理を実現した



※本図は必ずしもG社の具体的な管理体制や施策を反映したものではありません

事例⑧：資源開発H社（連結売上高：約280億ドル）

概要：SOX対応を手作業で行っていた企業が、GRCソフトウェアを導入してSOX対応の強化・効率化を実現した。

背景

1. SOX対応における事業拠点の選定や重要な勘定科目の特定等の業務がすべて手作業で行われていた
2. 各拠点の業務プロセスの定義にばらつきがあり、評価結果の拠点間比較が困難であった
3. 四半期単位での内部統制自己評価結果等のレポートをリアルタイムに閲覧することができず、ビジネス環境の変化に対応するための経営の迅速な意思決定に役立たなかった

目的

1. GRCソフトウェアを導入することで、SOX対応に必要なデータを自動化させ、SOX対応の効率化を図る
2. 業務プロセスの定義の共通化を図り、SOX対応を見える化する
3. SOX対応の強化・効率化により、SOX対応に関連するレポートをリアルタイムに提供して経営の迅速な意思決定に役立てる

アプローチ

1. 各事業拠点で共通のGRCソフトウェアを使用して、今まで様々な形式で作成されていたSOXの文書を均一化し、各事業拠点の財務情報を紐付けることでSOX対応に必要なデータを自動化し、事業拠点の選定や重要な勘定科目を特定する業務を効率化させた
2. SOX対応の過程を見える化するために、業務プロセス及びサブプロセスの定義を共通化し、同一事業については複数の拠点にまたがっても同じ視点で見られるように業務フローを整理した
3. リアルタイムでのレポート閲覧を可能とするために、評価活動は複数の事業拠点で同一時期に実施する等、方針や規律を作り徹底した

成果

1. 各拠点から収集するデータの均一化・紐付けにより、SOX対応が効率化された
2. SOX対応が見える化されたことにより、内部統制の有効性や信頼性が向上した
3. SOX対応における方針や規律の徹底により、SOX対応に関連する情報をリアルタイムに取得できるようになった
   例1） SOX対応の現場で必要な情報がリアルタイムで取得できるため、推進部門に不備等の重要情報がタイムリーに伝達されるようになった
   例2） 経営層が望むレポートをリアルタイムに閲覧できるため、経営の迅速な意思決定に役立てることができた

貴社で検討する上で参考にしていただきたいポイント

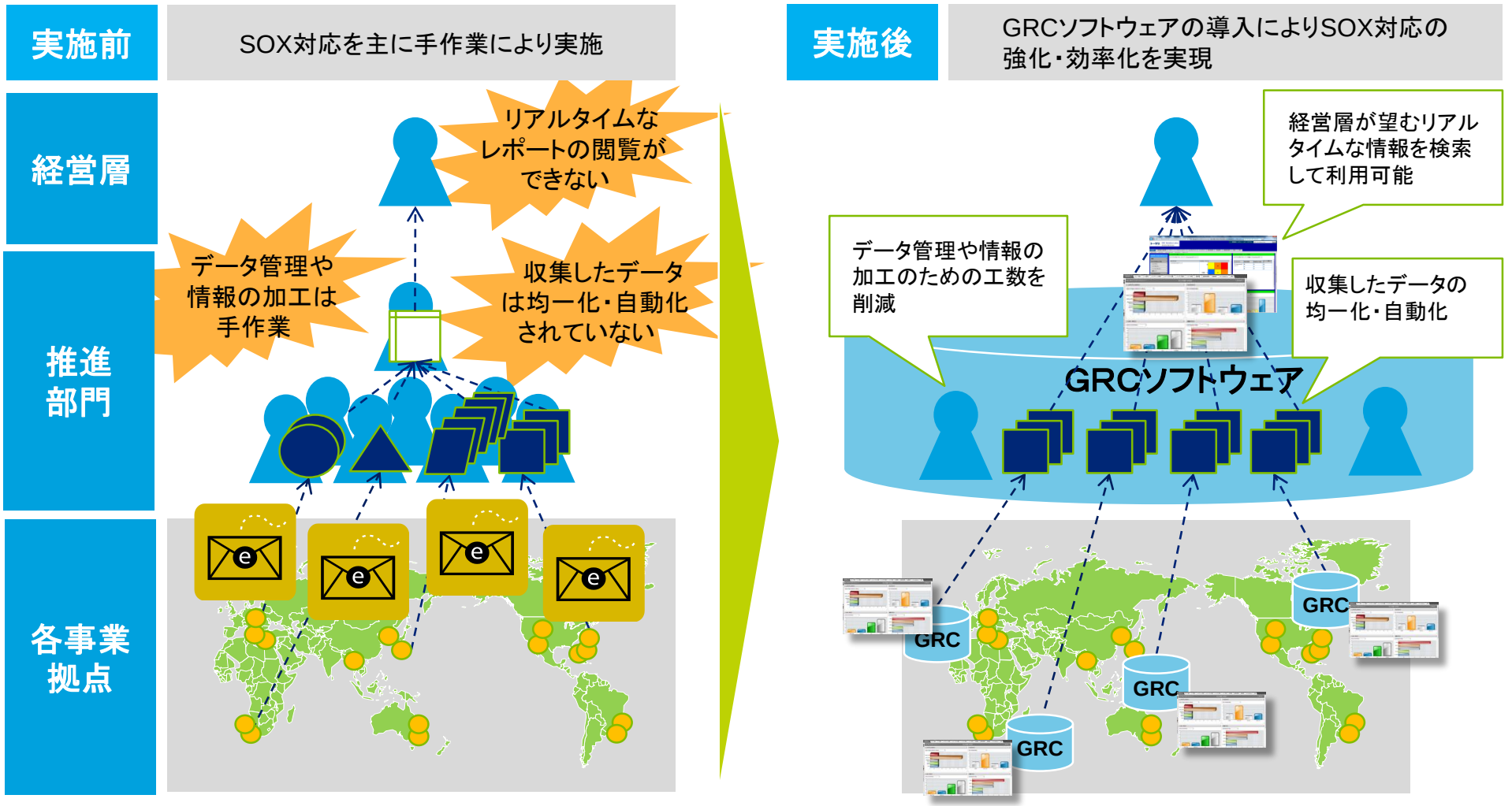
情報管理：GRCソフトウェアを導入することにより、グローバル展開している各拠点から収集したデータが均一化され、レポート作成のためのデータ管理・加工に関する工数を削減することができる
情報伝達：SOX対応が見える化されることにより、地理的に離れた対象部署、子会社等の実態の把握が可能となる
情報活用：作成されるレポートはリアルタイムに提供され、分析を行うことでリスクを未然に防ぐことが可能となる

事例⑧：資源開発H社　～SOX対応の強化・効率化実施イメージ～

SOX対応を強化・効率化するための情報管理の実現

実施前　SOX対応を主に手作業により実施

実施後　GRCソフトウェアの導入によりSOX対応の強化・効率化を実現



※本図は必ずしもH社の具体的な管理体制や施策を反映したものではありません

事例⑨：配送事業I社（連結売上高：約700億ドル）

概要：電子配送のビジネス戦略を強化している企業が、GRCソフトウェアを導入して外部委託先管理の強化を図り、ITリスクを事前把握し、予防措置を行うことで情報セキュリティ関連のインシデントが減少した。

背景

1. 情報セキュリティマネジメントが徹底されていなかったため、情報漏えい等のITリスクが事前に把握できず、顕在化してから対処していた
2. 電子配送は外部委託先への依存度が高いが、外部委託先管理スキルが低かったため、ITリスクを十分に把握できず、ステークホルダーに対してITリスクへの対応状況を説明することができていなかった

目的

1. ITリスクが顕在化してから事後対応を行うのではなく、ITリスクを事前に把握し予防措置を講じる
2. ITシステムの構築における外部委託先管理を徹底し、ITリスクの状態を包括的に認識してステークホルダーへの説明責任を果たす

アプローチ

1. 網羅的かつタイムリーにITリスクを把握するために、情報セキュリティマネジメントのPDCAサイクルをシステムライフサイクルプロセスに組み込んだ
2. ITリスクへの対応状況を包括的に認識するために、GRCソフトウェアを導入して、外部委託先の企業情報、外部委託先との契約情報、インシデント情報等を一元管理した
   - 一元管理された様々な情報をITリスクに対応するための優先度の決定に利用した
   - 把握したITリスクへの対応状況や予防措置をITリスクと紐付けて継続的なモニタリングを行った

成果

1. 情報セキュリティマネジメントを徹底して事前にITリスクを把握することで予防措置を講じることができ、情報セキュリティ関連のインシデントが減少した
   - 構築したITシステムの脆弱性やセキュリティホールが減少した
   - 外部委託先への依存度が高いシステムの品質を一定レベルに担保することができるようになった
2. 外部委託先管理を強化したことにより、ITリスクをどう把握しどう対処しているかをステークホルダーに説明できるようになった

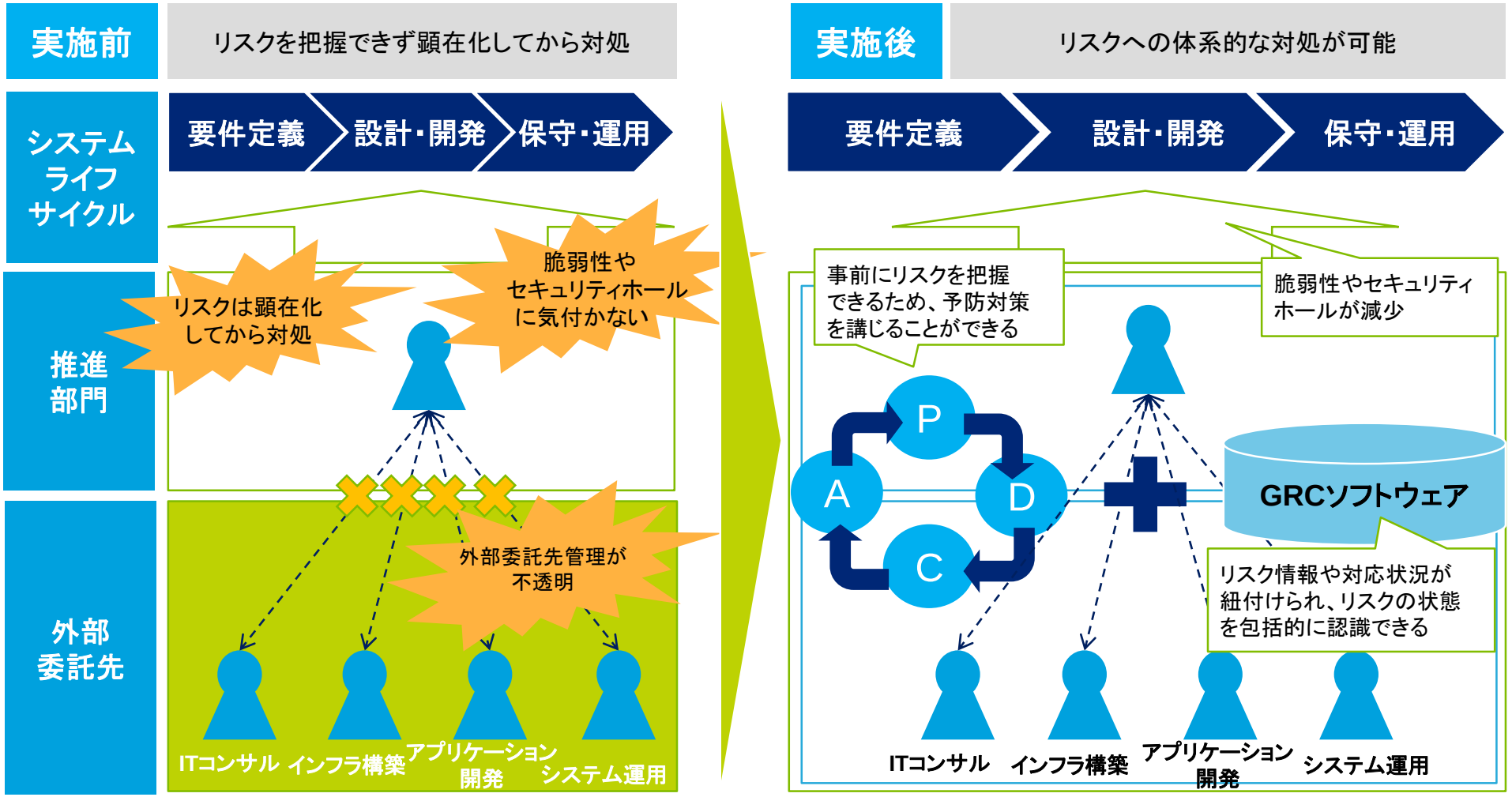
貴社で検討する上で参考にしていただきたいポイント

情報管理：GRCソフトウェアの導入により、外部委託先の企業情報、外部委託先との契約情報、インシデント情報等の関連付けが容易となり、把握したITリスクの優先順位の決定や対応状況の継続的なモニタリングに役立つ

情報伝達：情報セキュリティマネジメントのPDCAサイクルと組み合わせることにより、外部委託先との関係に伴うリスクやその対応状況を見える化できる

事例⑨:配送事業I社　～外部委託先管理の実施イメージ～

GRCソフトウェアを利用した外部委託先管理の実現



※本図は必ずしもI社の具体的な管理体制や施策を反映したものではありません

事例⑩：保険会社J社 （総資産：約200億ドル）

概要：共通ITインフラを活用して、グループ全体のオペレーションの集約化により、法令対応レベルの均一化と管理工数の適正化を実現した。

背景

1. 個々の事業拠点によって事業規模の違いや異なる商品・販売プロセスが存在して、情報の集約が困難であった
2. グループ全体での統一的な法令対応（Solvency Ⅱ）と各国ごとの細かな法令対応に膨大な工数を割いていた

目的

1. グループ全体での複雑なオペレーションを集約して、各種法令の運用工数を削減する（業務上の損失とデータの把握、各法令で共通した重要リスクに対応するコントロールの整備・運用）
2. 共通ITインフラで情報の一元管理を行い、グループ標準のレポート体系を確立するとともに個々の事業拠点でのカスタマイズを可能にする

アプローチ

1. 各国で対応している法令対応の情報集約（統合要求事項の作成）を行い、複雑なオペレーションの集約を図った
2. 共通のITインフラ上で統合要求事項に対応する重要リスクとコントロールを管理した
3. グループ全体で標準的なレポート機能を確立し、管理レベルを均一化するとともに、各事業拠点での個別カスタマイズが可能な柔軟性を持たせた

成果

1. 共通ITインフラへの情報とオペレーションの集約により、グループ全体でSolvency Ⅱへの規制対応に必要な管理レベルを達成することができた
2. グループ標準のレポート機能により、管理者による効率的なモニタリングを可能にし、グループ全体での管理工数の適正化ができた
3. 新たな規制が発生しても、従来のシステム環境、対応プロセスの変更なく柔軟に対応することが可能になった（工数の過度な増大を防ぐことができた）

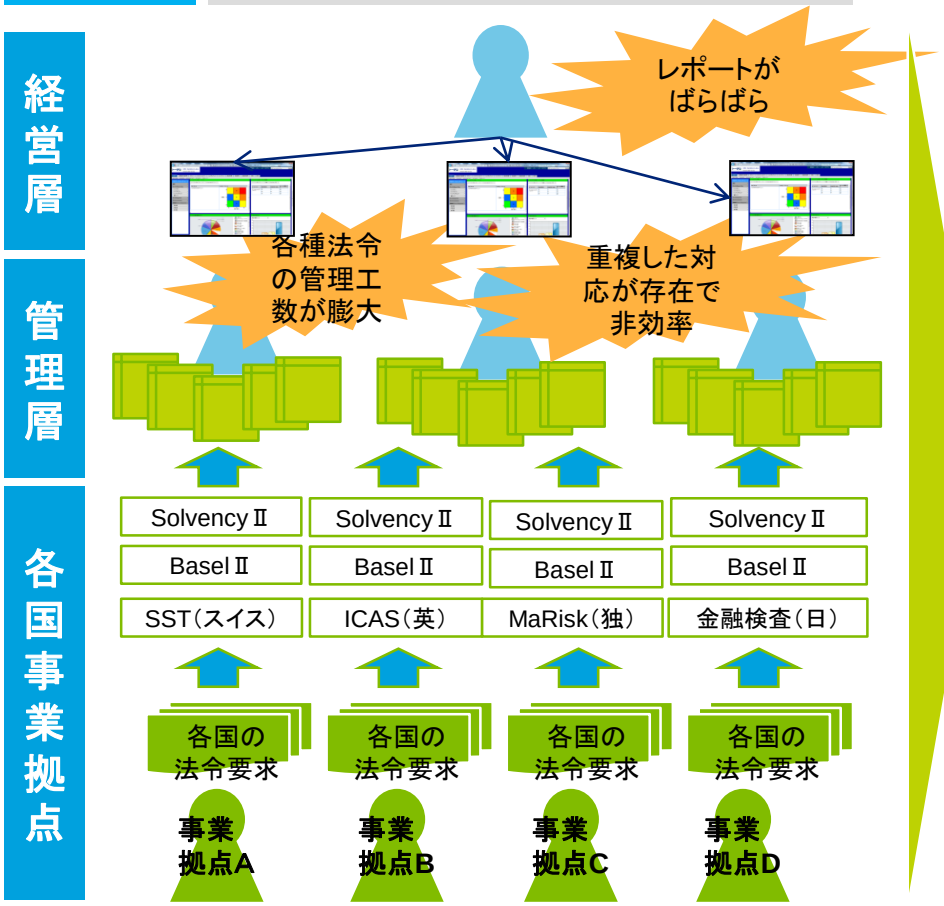
貴社で検討する上で参考にしていただきたいポイント

情報管理：国別の法令対応へのオペレーションを集約することで、法令対応レベルの均一化を実現した。
情報伝達：共通のITインフラによるグループ標準のレポート機能で、管理者による管理工数の適正化を図ることができた。
情報活用：新たな規制に対応するオペレーションも、従来の統合要求事項を柔軟に活用にすることで、過度な工数の増大を防ぐことができた。

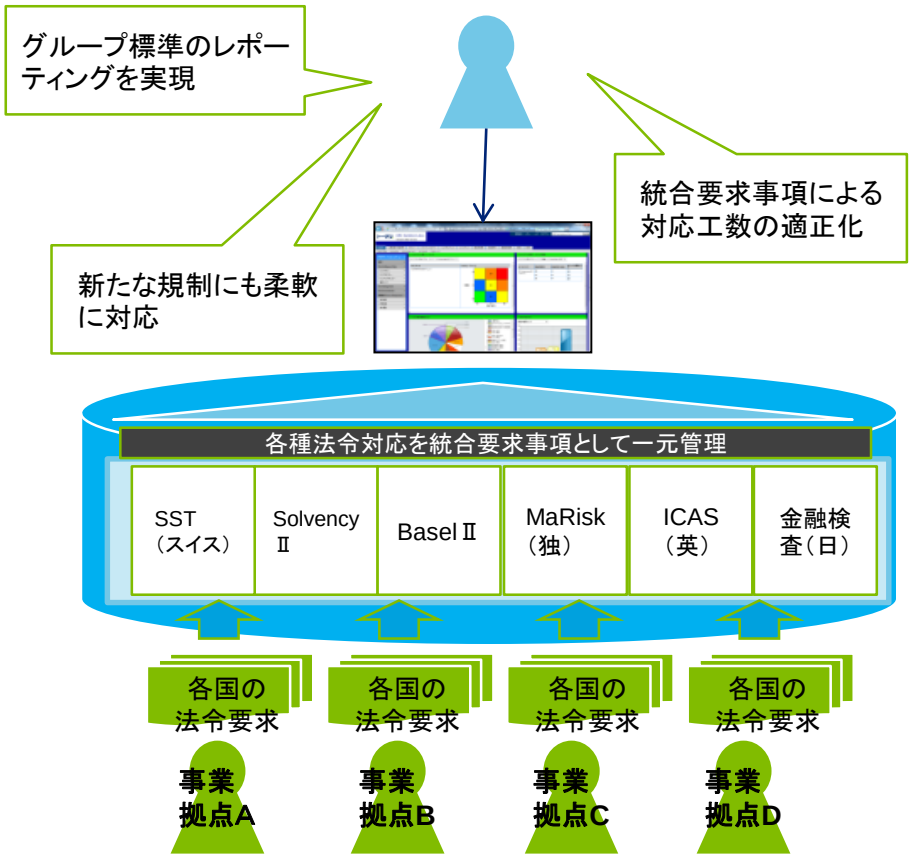
事例⑩：保険会社J社　～オペレーション集約化イメージ～

オペレーション集約化の実現

実施前　各国独自の法令対応により非効率な管理を行っていた



実施後　統合要求事項と標準レポートの整備により管理工数の適正化を実現した



※本図は必ずしもJ社の具体的な管理体制や施策を反映したものではありません

Deloitte. トーマツ.

トーマツグループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームおよびそれらの関係会社（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング株式会社、デロイト トーマツ ファイナンシャルアドバイザリー株式会社および税理士法人トーマツを含む）の総称です。トーマツグループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各社がそれぞれの適用法令に従い、監査、税務、コンサルティング、ファイナンシャルアドバイザリー等を提供しています。また、国内約40都市に約7,800名の専門家（公認会計士、税理士、コンサルタントなど）を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はトーマツグループWebサイト（www.deloitte.com）をご覧ください。

Deloitte（デロイト）は、監査、税務、コンサルティングおよびファイナンシャル アドバイザリーサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150ヵ国を超えるメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを提供しています。デロイトの約200,000名におよぶ人材は、“standard of excellence”となることを目指しています。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）およびそのネットワーク組織を構成するメンバーファームのひとつあるいは複数を指します。デロイト トウシュ トーマツ リミテッドおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。その法的な構成についての詳細はwww.deloitte.com/jp/aboutをご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

有限責任監査法人トーマツ 東京事務所エンタープライズ リスク サービスは、2006年2月8日、監査法人として初めて情報セキュリティマネジメントの国際規格であるISO/IEC27001の認証を取得しました。
2009年4月1日には、デロイト トーマツ リスク サービス株式会社をこの認証範囲に含めております。

IS 501214 / ISO (JIS Q) 27001

有限責任監査法人トーマツ 東京事務所におけるBCP/BCMサービス提供部門およびデロイト トーマツ リスクサービス株式会社は、2011年3月11日に事業継続マネジメントシステムの規格であるBS25999-2:2007の認証を取得し、2013年2月19日に国際規格であるISO22301:2012の認証を取得しました。

BCMS 568132 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited