第156回CFOセミナー　講演

企業における全社的なリスク管理を実現するためのGRCの最先端動向

2011年10月13日

新日本有限責任監査法人
シニア・パートナー
森本　親治

ERNST & YOUNG
Quality In Everything We Do

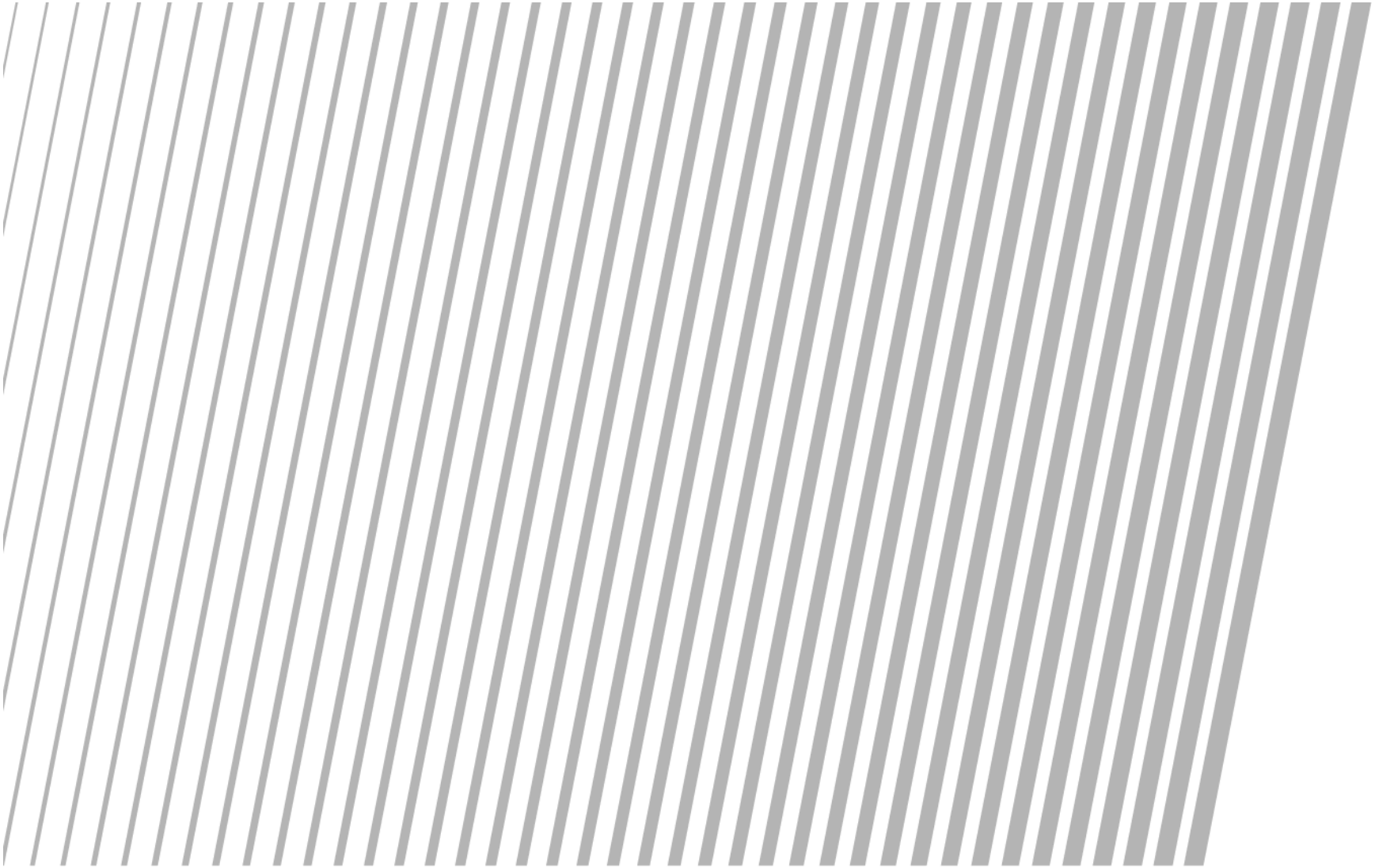
本資料の内容

1. GRCによる事業リスクの統合的管理の背景と概要

2. GRCツールを活用した統合的管理の事例紹介

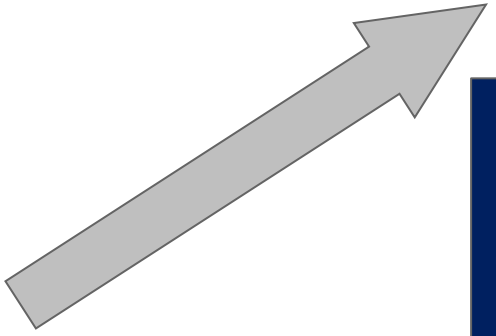
3. 他ツールとの関連情報の連携による機能拡張

1. GRCによる事業リスクの統合的管理の背景と概要



(1) SOX対応によるリスク管理の時代から攻めのリスク管理(全社的リスク管理)の時代へ

- これまでJ-SOXでカバーしてきた全社統制・IT全般統制から、事業継続管理や外部委託先管理、その他各種当局法令等に基づく管理等、組織全体で対象とすべきリスクの拡張を図ったものが全社的リスク管理であり、企業における事業活動の多様化・複雑化、国際的な事業展開の進展等に伴い全社的リスク管理を経営に活用する必要性が高まっているといえます。

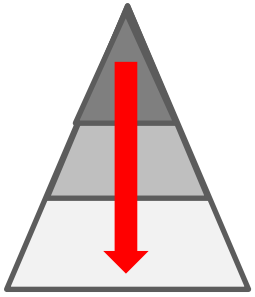


SOX対応	実現手段
・受動的リスク管理 ・財務報告リスクに限定 ・一過的関心	・経理、内部監査部中心の全社協力 ・文書化とテスト ・統一的評価枠 ・内部宣誓、経営者評価 ・外部監査

攻めのリスク管理	実現手段
・経営上の重要リスクを能動的に管理(ERMの概念) ・リスク＝経営課題 事業計画阻害要因 ・組織横断的、地域拠点横断的な複合リスクが中心課題 ・経営として永続課題 ・グローバル展開 規制複雑化 合併買収 競争環境激化等で必要性は益々上昇	・従来の組織統合、会議体、システムに留まらない組織間のリスク情報共有、統制活動の連携が不可欠(GRCの概念) ・統合管理主体の明確化 ・事業計画のPDCAサイクルへの組込み

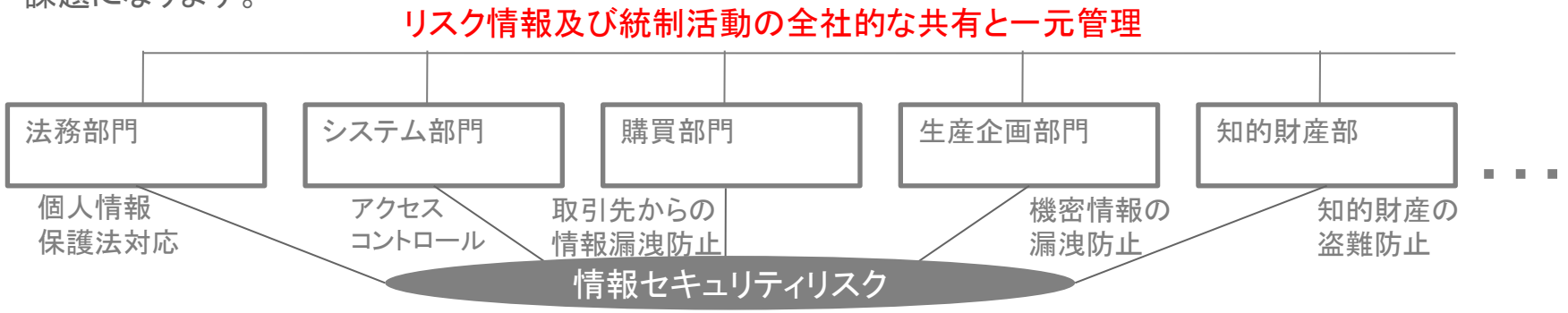
(2) GRCによる事業リスクの統合的管理とは

- グローバルに事業展開を行う企業では、規制強化や競争環境等に対してリスクマネジメントの実効を高めるため、従来の組織、会議体、システムによる統合的な管理態勢を、下記GRCの観点からさらに強化すべき時期に来ていると考えられます。多くの場合、事業単位の縦軸と地域統括の横軸のマトリックス組織での調整や、プロセスとリスク管理に関する本部と拠点間の権限委譲が課題になります。



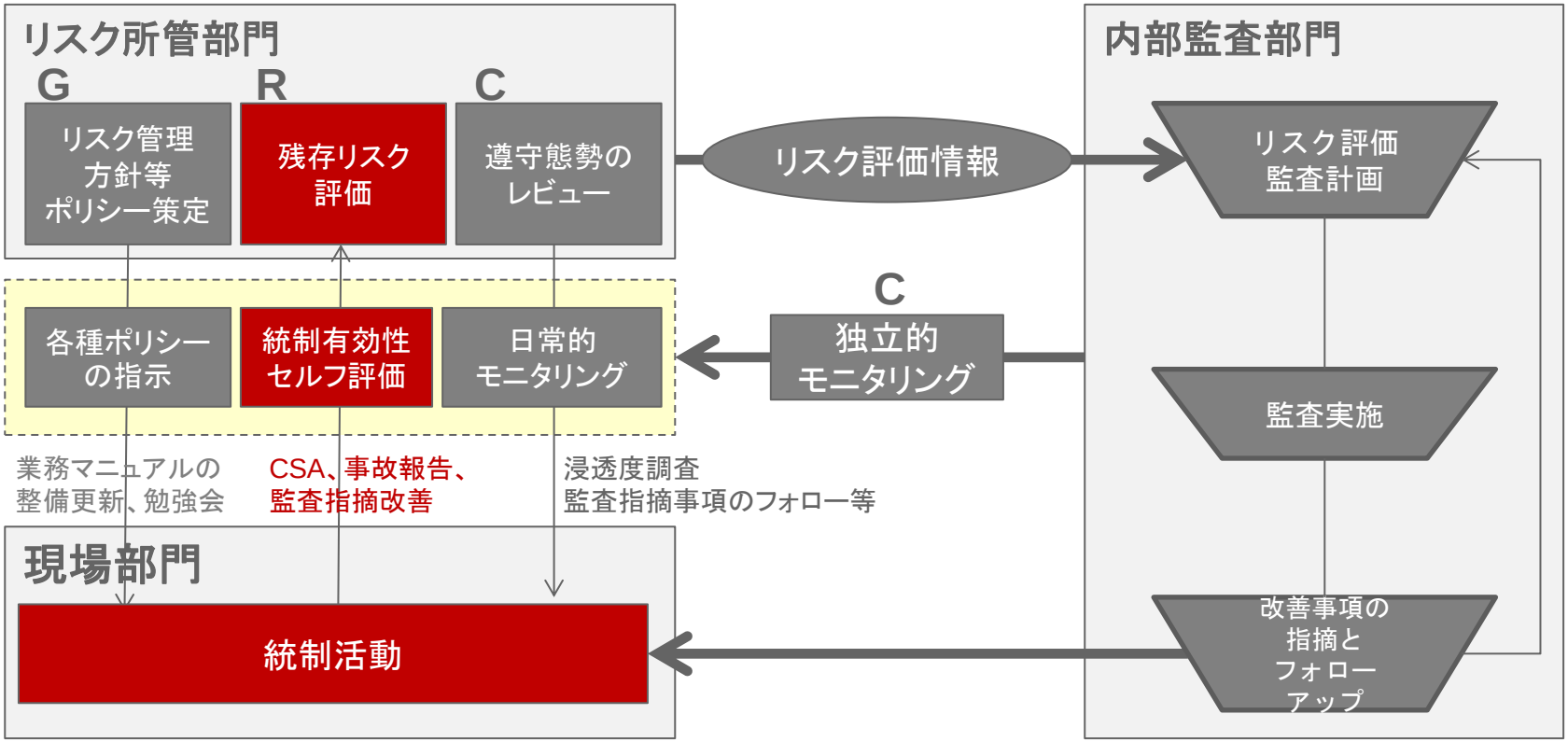
Governance	法令やグループ方針・ルールを徹底させる態勢
Risk	各組織・業務・プロセスにおけるリスクの評価、統制活動
Compliance	現場でのリスクの統制が所定の基準、方法に遵守して実施されていることのモニタリング

- 事業リスクの統合的管理とは、会社組織の各々のリスク所管部署においてバラバラに対応しがちであった、リスク管理項目について、リスク情報及び統制活動を全社的に共有し、首尾一貫して重複なく効率的に管理を行う考え方です。多くの場合、組織横断型の調整統括をどの部署が行い、PDCAサイクルをどう回すかが課題になります。



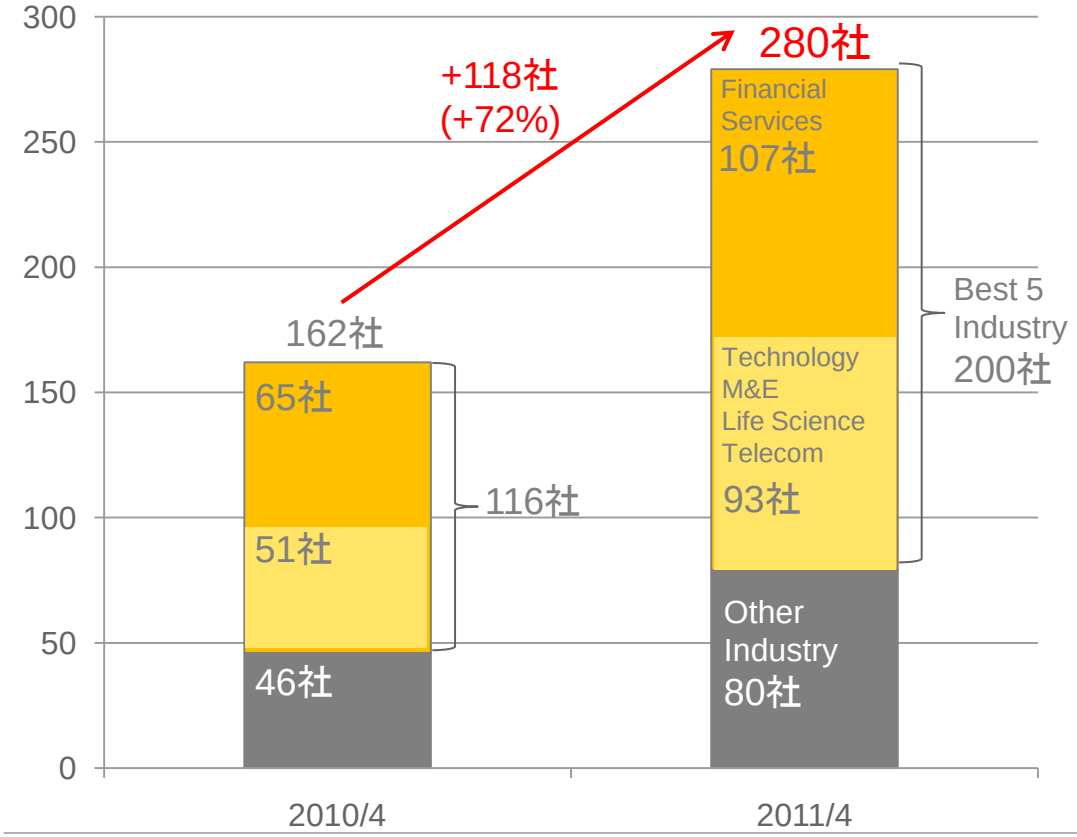
(3) GRCの実効性を最大化させるアプローチの要点

- GRCの実効性をグループレベルで向上しようとすれば、Cに関するリスク所管部門、内部監査部門の機能強化も重要ですが、その前提となるRの信頼性を高めるため、現場部門にリスク管理の当事者意識を持たせることがより重要です。こうしたアプローチの推進策として、欧米大手企業を中心にGRCツールの導入が急速に進展しています。



(4) 代表的GRCツールであるRSA Archerの導入実績

■ 代表的なGRCツール「RSA Archer」を例に挙げると米国での導入実績が近年、Fortune500の大企業を中心として飛躍的な増加傾向にあり、また産業別の集計を見た場合には下記の通り、金融業を始めとした特定の産業において、導入が先行している状況が窺えます。



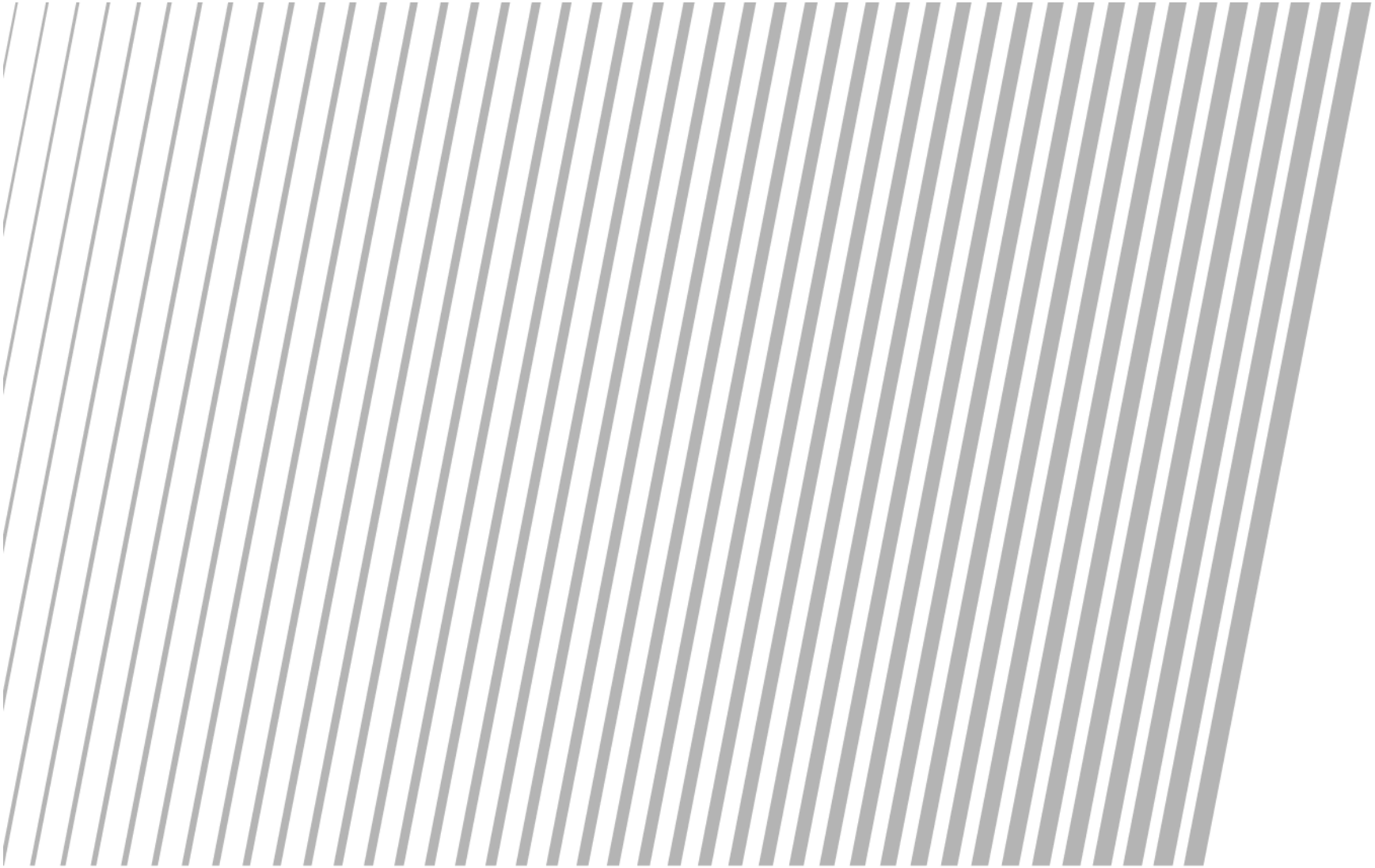
※ 産業別の導入事例は下記の通りです。

- **Financial Services…107社(2010年：65社)**
- **Technology…30社(19社)**
- **Media & Entertainment…23社(14社)**
- **Life Science…21社(9社)**
- **Telecommunication…19社(9社)**
- **Government…16社**
- **Energy…12社**
- **Retail…9社**

⋮

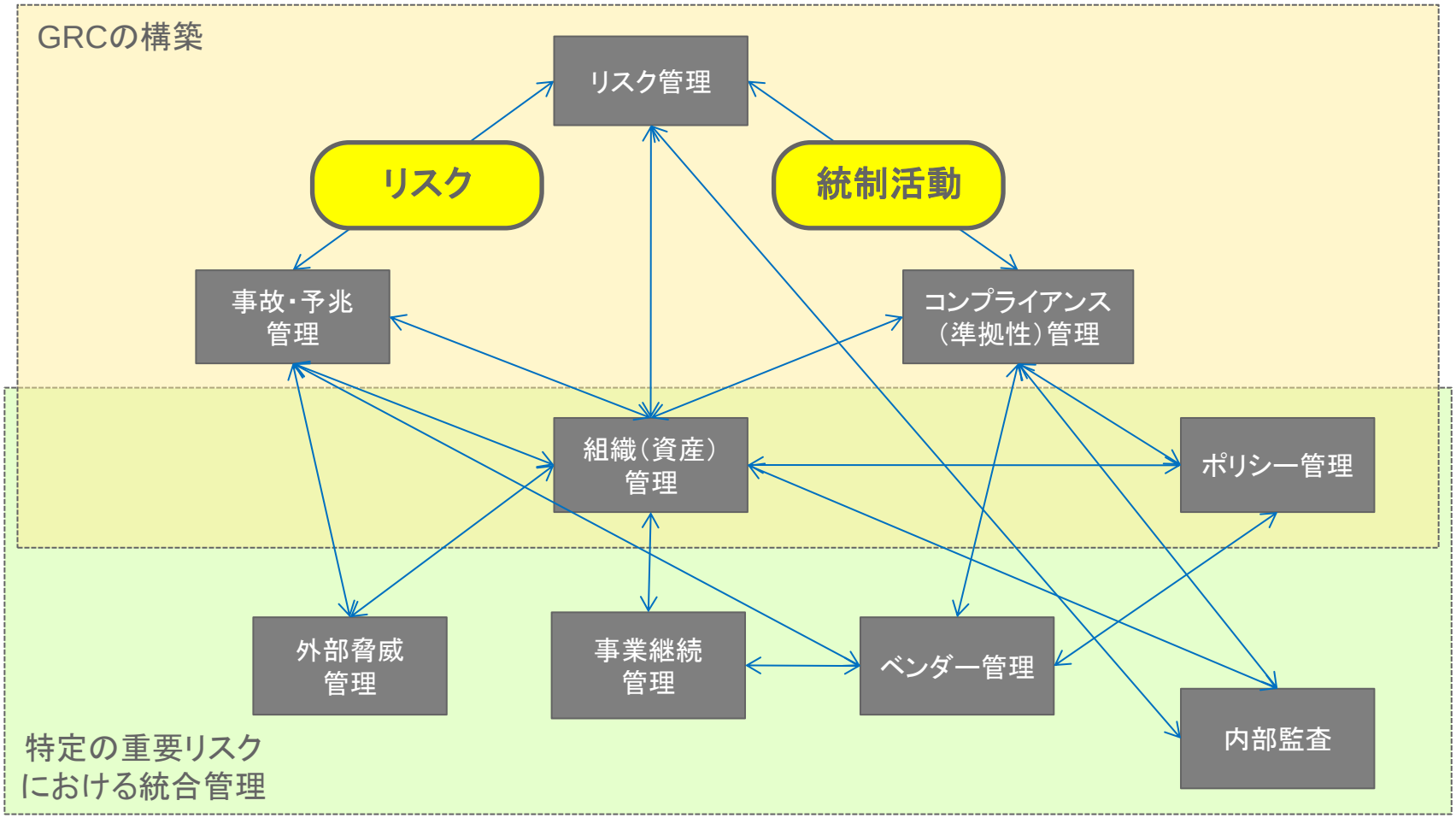
導入企業には大手日本企業も3社含まれます。

2. GRCツールを活用した統合的管理の事例紹介



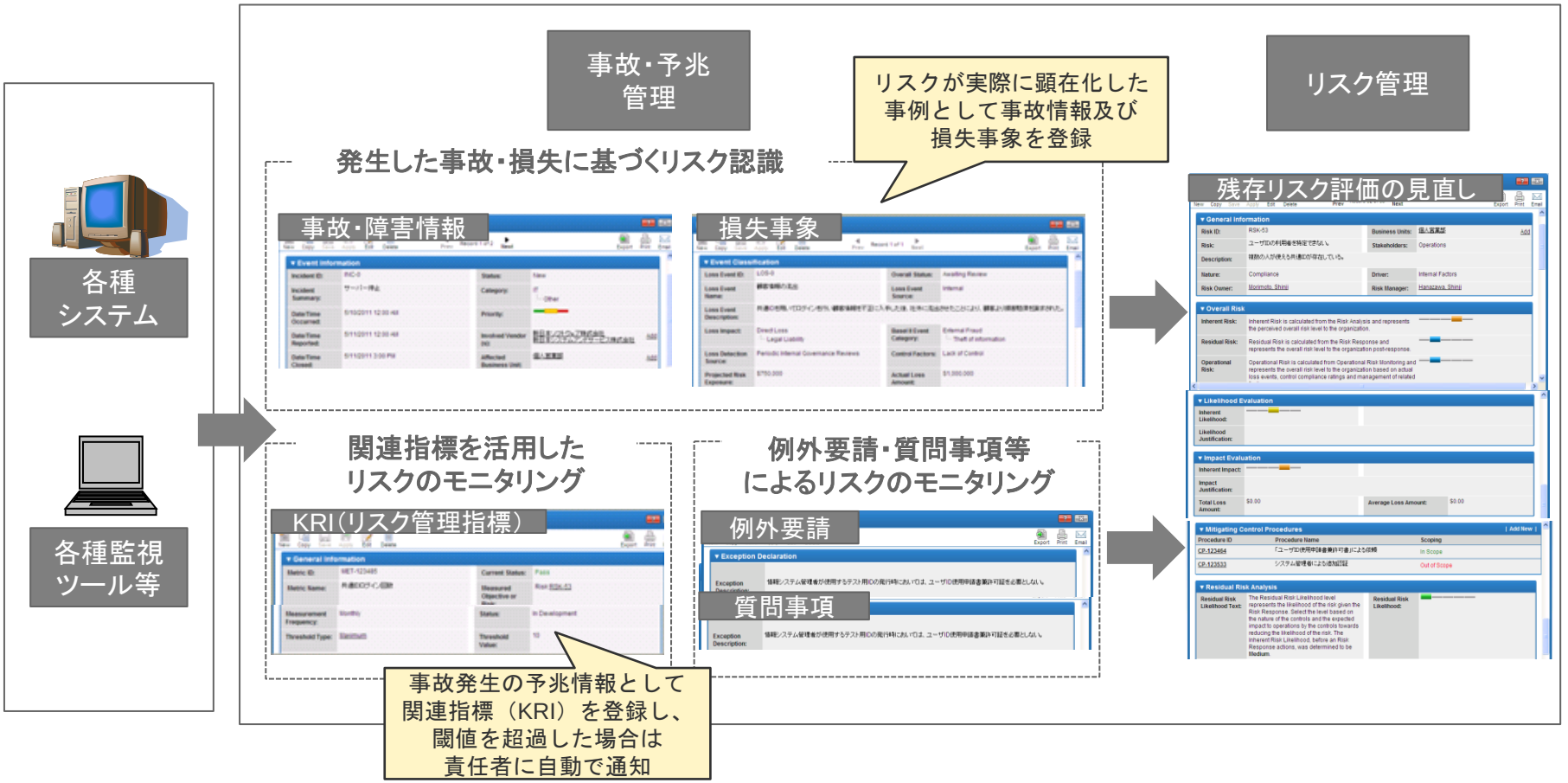
(1) GRCツールにおける情報連携の体系図

■ GRCツールの特筆すべき特徴はモジュール間、さらには他ツールとの情報連携により機能を拡張できる点にあり、到達したいと考える目標やレベルに応じてリスク管理の効率化や高度化を図ることが可能となります。



①事故・予兆情報を活用したリスク管理の高度化
GRCツールの活用における具体的なイメージ

- GRCツールと各種システム及び監視ツールと連携させて、顕在化した事故事例や損失事象、KRIや例外要請等の情報をリスクの評価（予兆管理）に活用することにより、実態に基づいたリスクシナリオの更新と精度の高い残存リスクの評価及びリスクの顕在化防止が可能となります。



①事故・予兆情報を活用したリスク管理の高度化
GRCツールの活用事例　～大手国際物流会社

事故・予兆管理　リスク管理

- **当社の概要**
  世界220ヶ国、従業員29万人を擁する大手国際物流会社

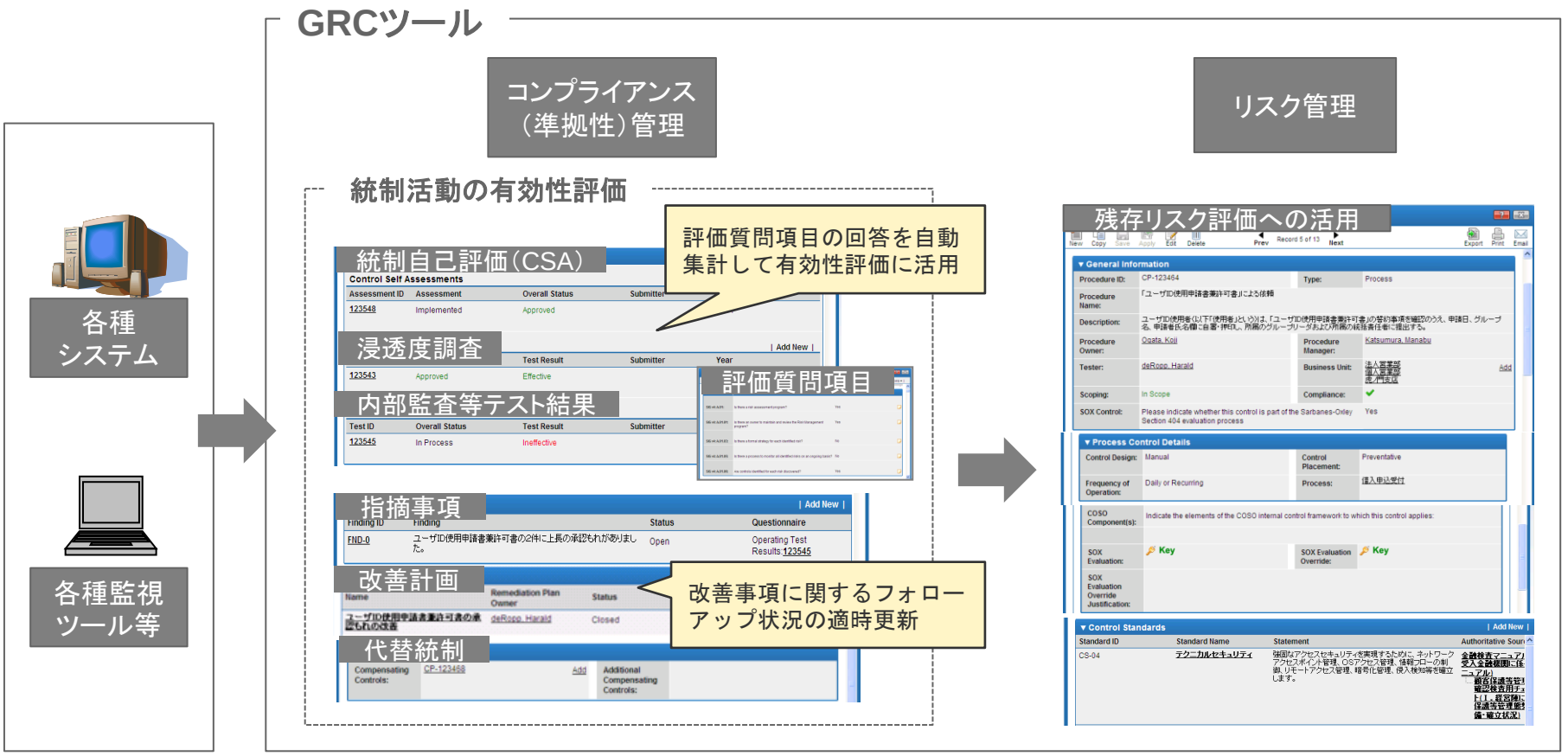
- **課題**
  - 集荷・配送状況等に関する顧客からの照会、決済情報エラー、監査指摘事項等事故に繋がり得る潜在的なリスク事象について統合管理されておらず、未然に防止しえた事故が実際に発生していた。
  - 事故情報が事象によってバラバラに管理されているために、全社レベルでの事故情報のレポーティングに多大な業務負荷が掛かっていた。

- **解決策**
  - 事故に繋がり得る予兆情報を外部システムから取り込み、リスク評価プロセスに組み入れ、評価結果に応じたアクションプランを策定できるよう、リスク管理の仕組みを精緻化した。
  - あらゆる事故情報を一元管理し、リスク要因別など様々な切り口で分析して迅速に報告できる基盤を構築することにより、事故およびその対応情報を組織毎のパフォーマンス評価に統合した。

- **ツール導入による実現効果**
  - 予兆情報に基づくアクションプランの新たな策定や見直しが迅速かつ適切に実施できるようになった結果、統制活動の実効性が向上し、事故発生件数が減少した。
  - 報告作成がシステム化されたことによって、月間約250時間の報告作成作業時間が削減された。

②一貫した統制活動の有効性評価とモニタリング
GRCツールの活用における具体的なイメージ

- 統制自己評価(CSA)や浸透度調査、内部監査等テスト結果等を活用した統制活動の有効性評価（規程に対する準拠性の確認）や例外要請の申請、指摘事項を通じた改善のフォローアップまでツール上のワークフロー機能を用いて、グローバルで首尾一貫したコンプライアンス状況の管理を行うことができます。



②一貫した統制活動の有効性評価とモニタリング
GRCツールの活用事例　～大手航空会社

コンプライアンス（準拠性）管理　リスク管理

- **当社の概要**
  年間搭乗者数1億6,000万人を誇る国際航空会社

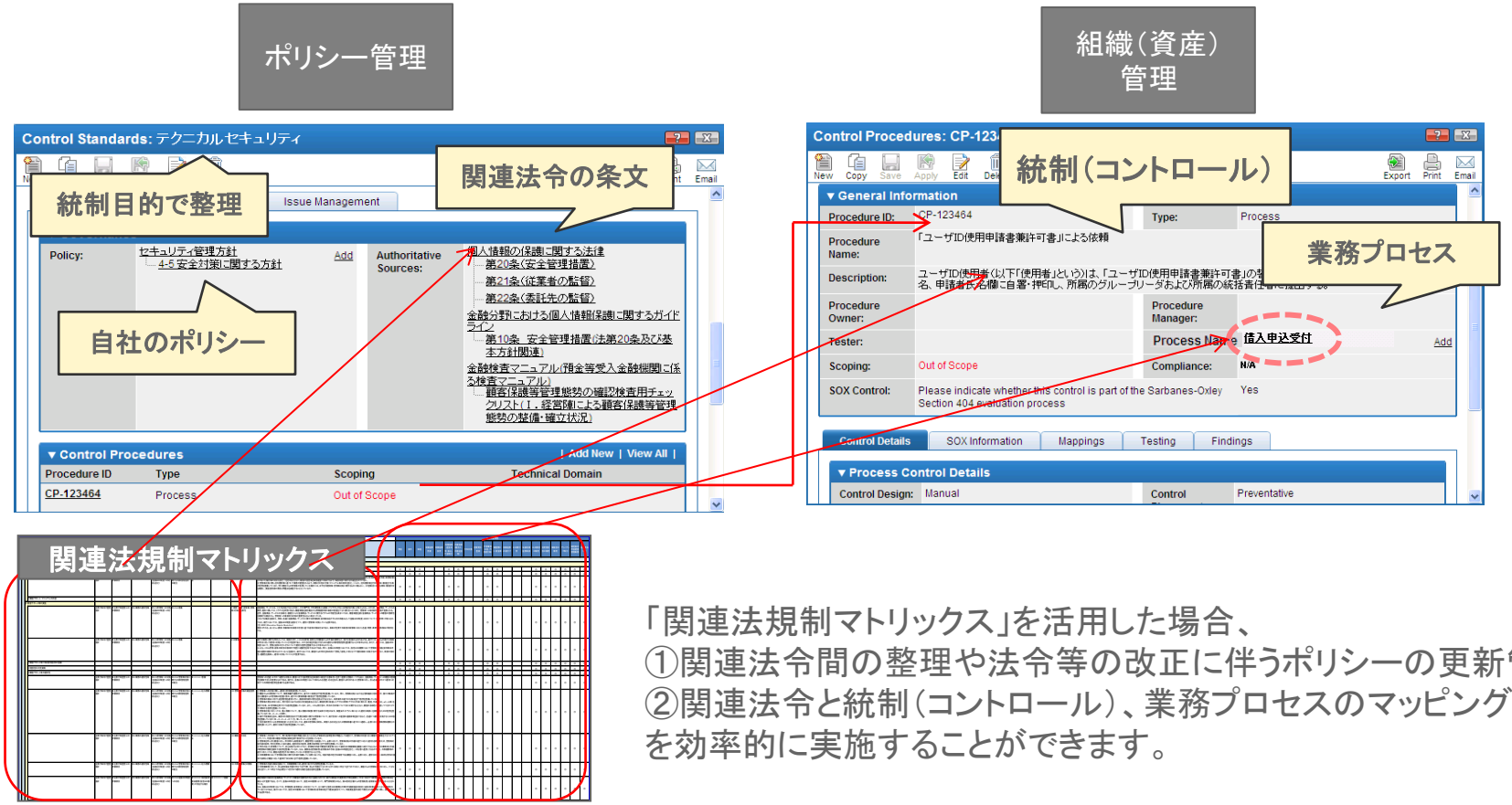
- **課題**
  - 各種ポリシーの遵守状況に関するモニタリングが十分に行われていなかったため、各現場における統制活動に対する意識が不十分であった。
  - 各部門間で設定した統制活動のレベルにバラ付きがあり、モニタリング活動の効率性と実効性が阻害されていた。

- **解決策**
  - 統一的に遵守状況のチェック項目をデータベース化し、遵守状況の統制自己評価（CSA）の実施による自主点検を現場で実施した。（日常的モニタリング）
  - 内部監査部門にて統制活動の有効性テスト・発見事項のフォローアップを一元的に管理することで網羅的に対応を行う体制を整えた。
    （独立的モニタリング）

- **ツール導入による実現効果**
  - 現場側においてポリシー管理の遵守に対する意識が向上した。
  - 統制に対するモニタリング活動を部門横断的に実施できるようになった結果、全社的な観点から統制活動の有効性の把握が行えることとなり、リスク管理における効率性が大幅に向上した。

③網羅的かつ効率性の高い規制対応の実現
GRCツールの活用における具体的なイメージ

- GRCツールを活用したポリシー管理を行うことにより、グループ全体で遵守すべき関連法令等に対して、自社のポリシーが網羅的かつ適切に整備されていることが確認できます。
  また、組織や業務プロセスごとに遵守すべき規程や統制活動を明確にすることで現場への浸透が促進でき、効率的な規制対応の実現が可能となります。



「関連法規制マトリックス」を活用した場合、
①関連法令間の整理や法令等の改正に伴うポリシーの更新管理
②関連法令と統制（コントロール）、業務プロセスのマッピング
を効率的に実施することができます。

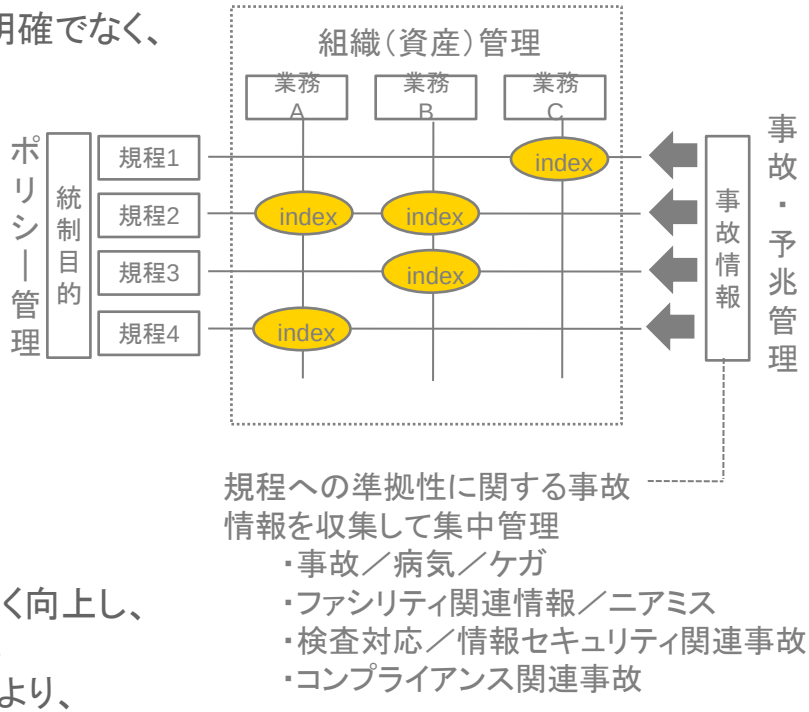
③網羅的かつ効率性の高い規制対応の実現
GRCツールの活用事例　～大手精密機器会社

ポリシー管理 | 組織（資産）管理 | 事故・予兆管理

- **当社の概要**
  世界各地に生産・販売拠点を有する大手精密機器会社

- **課題**
  - 社内の各種ポリシーが業務と関連付けて管理されておらず、従業員のポリシーに対する理解が十分に得られていなかった。
  - 実際の事故の発生に基づき修正すべきポリシーが明確でなく、同様の事故が頻発していた。

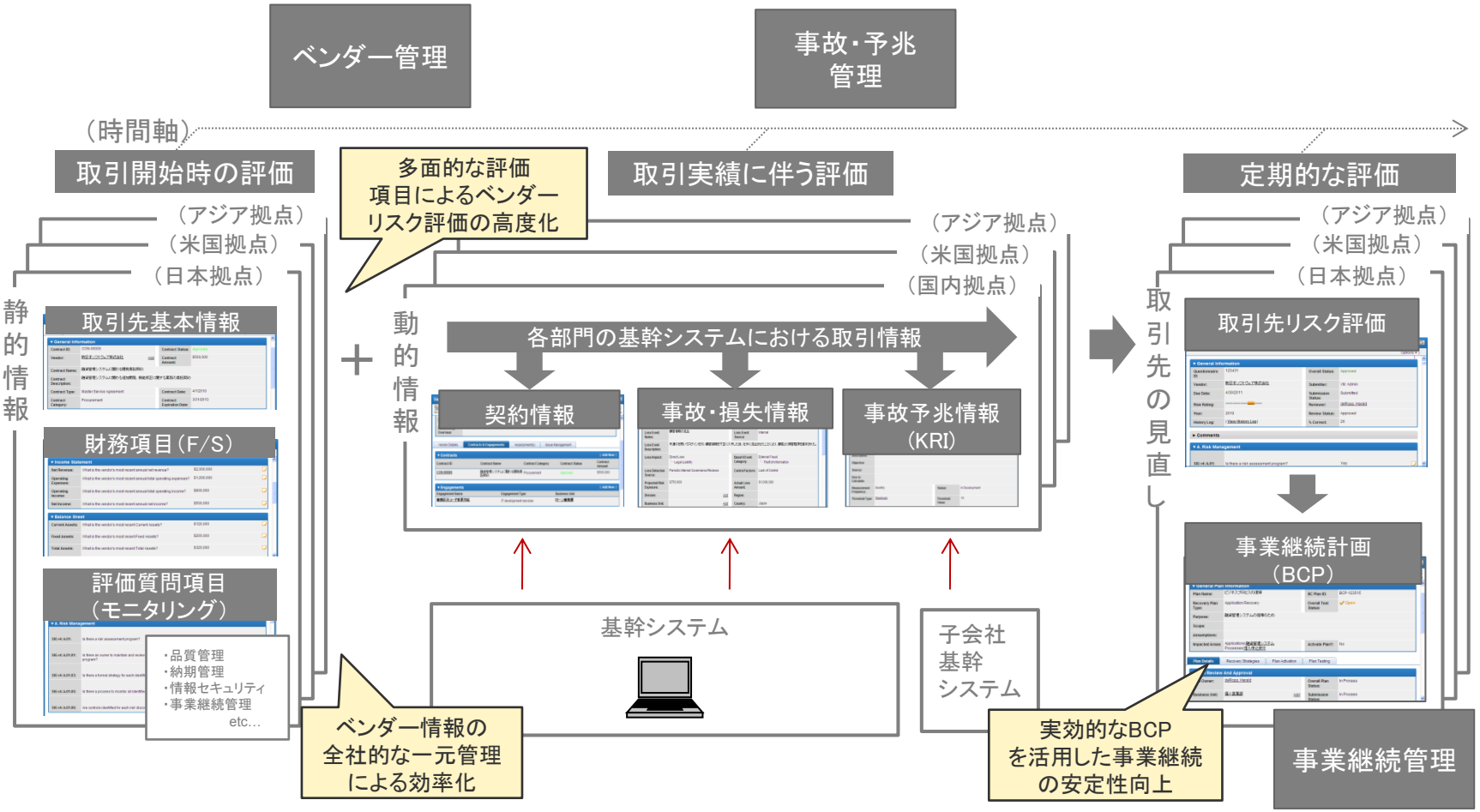
- **解決策**
  - 各従業員が必要なポリシーを容易に参照できるよう、ポリシーの階層化・Index付け・検索機能・相互参照機能を導入した。
    また業務とポリシーを関連付けて管理することにより、参照すべきポリシーを検索できるようにした。
  - 実際に発生した事故を関連するポリシーに紐付け、ポリシーの見直しができるよう仕組みを構築した。



- **ツール導入による実現効果**
  - ポリシーの電子化により利便性、検索容易性が大きく向上し、社員の理解度及びポリシーの遵守状況が改善した。
  - 事故情報とポリシーとの関連付けが行われたことにより、事故の再発防止に大幅な改善が図られた。

④取引先管理の全社的な最適化
GRCツールの活用における具体的なイメージ

- GRCツールでは各拠点に点在したベンダー情報を全社一元的に集約し、多面的な評価項目にて効率的かつ高度なベンダーリスクの評価を行うことで、ベンダー管理の最適化を支援することが可能です。



④取引先管理の全社的な最適化
GRCツールの活用事例　～大手ネット小売会社

- **当社の概要**
  世界で95百万人以上の利用者を有する大手ネット小売会社

ベンダー管理 | 事故・予兆管理 | 事業継続管理

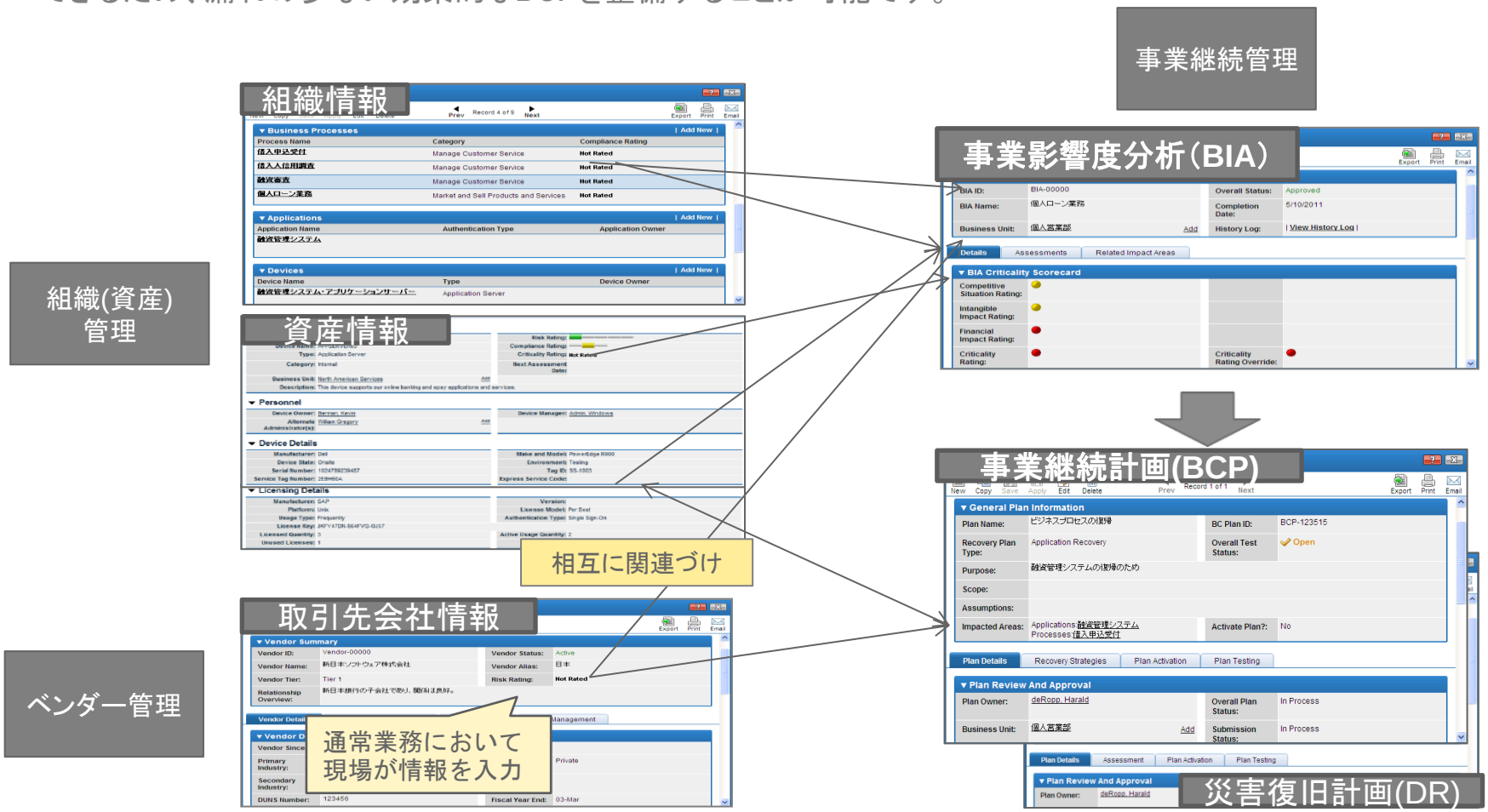
- **課題**
  - ベンダー（商品納入元、各種業務委託先など）が著増しており、各取引先の業務実態やリスク状況の把握のための情報収集に多大な負荷がかかっていた。
  - ベンダーの情報セキュリティや事業継続における管理体制を把握しておらず、ベンダーリスク評価が万全に行えている状況ではなかった。

- **解決策**
  - 各取引先に対してアクセスIDを付与、質問票に直接回答を記入させるようにした。
  - 情報セキュリティ体制や事業継続計画に関する質問項目に追加することで情報を収集し、また顧客情報の漏洩といった事故情報も統合的に管理を行うことで、ベンダーリスク評価の精緻化を図った。

- **ツール導入による実現効果**
  - 従来6カ月程度かかっていた取引先情報収集プロセスが約2カ月に短縮された。またベンダーから直接最新の情報が入手できるようになったことで、効率的な取引先評価が行えるようになった。
  - ベンダーリスク評価及び改善措置の対応状況等が一元的に管理でき、モニタリング活動の実効性が高まった。またリスク評価の結果を活用して、外部委託先も範囲に含めたより精度の高い事業継続計画の作成に着手することができた。

⑤実効性の高い事業継続計画(BCP)の策定
GRCツールの活用における具体的なイメージ

■災害時におけるサプライチェーンの安定性向上のためには、実効性の高いBCPの作成が鍵です。
GRCツールでは各現場で入力を行った取引先の評価や資産の配置などのきめ細かい情報を集約的に利用できるため、漏れの少ない効果的なBCPを整備することが可能です。



⑤実効性の高い事業継続計画(BCP)の策定
GRCツールの活用事例　～大手ネット小売会社

組織（資産）管理 | ベンダー管理 | 事業継続管理

- **当社の概要**
  世界で95百万人以上の利用者を有する大手ネット小売会社

- **課題**
  - 組織・資産の異動が頻繁に発生する上、1,000を超える外部取引先が部署毎にバラバラに管理されていたため、BCPの更新が適時に行われず、BCPの信頼性が低下していた。
  - BCPの内容が業務影響度などのリスク評価結果や計画の妥当性テスト結果を反映したものになっておらず、BCPの実効性に問題があった。

- **解決策**
  - 組織、業務プロセス、資産、ベンダーなどの各情報を、BCPと常時連携させることにより、リアルタイムでBCP情報の更新を行える仕組みを構築した。
  - 業務影響度評価等のリスク評価情報、BCPのテスト結果や発見事故情報をツール上で一元管理し、必要なBCP更新と自動的に紐付けができるようにした。

- **ツール導入による実現効果**
  - BCPの内容が常に最新の組織・業務プロセス・資産・ベンダーの情報を反映することができるようになったことにより、現場でのBCP浸透度が向上、災害発生時の初動対応が迅速化した。
  - 業務影響度評価など最新のリスク状況を反映したBCPが維持されるようになり、緊急時に現場で適用可能な内容となった。

(2) GRCツールの導入プロジェクト事例紹介 ～大手エレクトロニクス会社におけるグローバル展開(1/2)

1.目的

- リスク及び統制活動の単一ツールにおける統合
- 効率性の改善　　業務における自動化／冗長性の削減／優先順位付け
- 機能の徹底　　可視性／説明責任／標準化
- 統合の強化　　部門・グループ横断的な情報連携

2.導入拠点

米国統括会社を中心に在米拠点の子会社に対して同時に導入し、稼働を開始。
その後ヨーロッパ、アジアパシフィック及び日本にグローバル展開を行う予定。

3.導入における代表的な活用業務とスケジュール

- 昨年9月にプロジェクトを開始。段階的に活用業務を拡張している。

年度	2011	2012	2013以降
業務	・グローバルポリシー管理 ・ローカルポリシー管理 ・組織（資産）管理 ・情報セキュリティ管理 ・事業継続管理	・ベンダー管理 ・法令遵守管理 (セルフ評価)	・外部脅威管理 ・事故障害管理 ・環境(ISO)法令遵守管理 ・ITガバナンス管理 (アプリケーション統合化及び標準化)

- 上記順位付けは、導入を行ったモジュール毎の対象業務の重要性・移行データ等を考慮した結果。

(2) GRCツールの導入プロジェクト事例紹介 ～大手エレクトロニクス会社におけるグローバル展開(2/2)

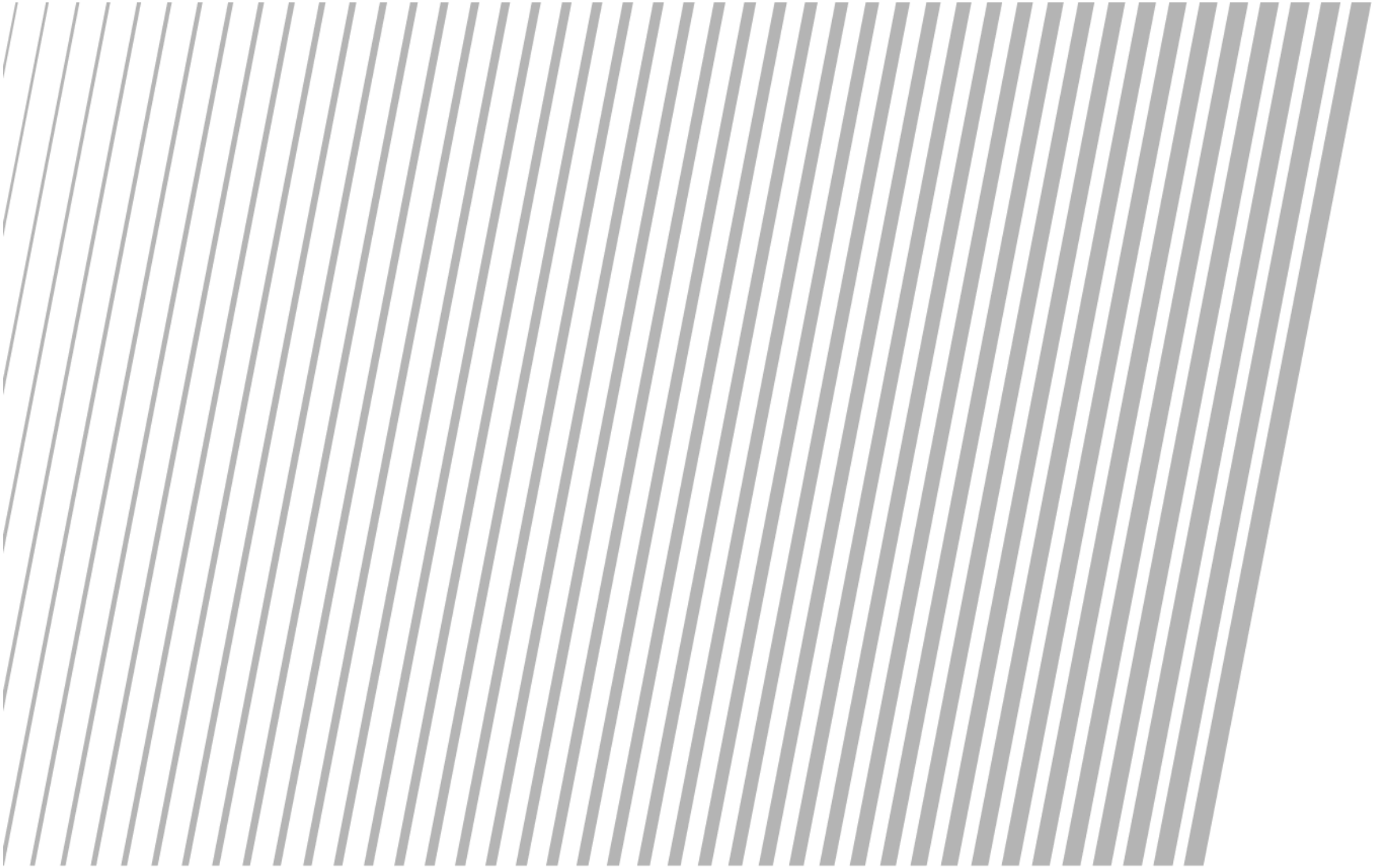
4.導入プロジェクト体制

- 米国法人の内部統制担当部署が主導でプロジェクトを組成。
- 同部の "VP, Americas Region Risk Officer" がリーダーとなり、専任メンバー約10名を含めて約40名程度が関与中。
- 2011年5月以降下期にかけてはグループ各社でのカットオーバー、モジュール追加のため要員を70～80人規模に増強予定（主に兼務メンバー）

5.今後のグループ内展開に関して

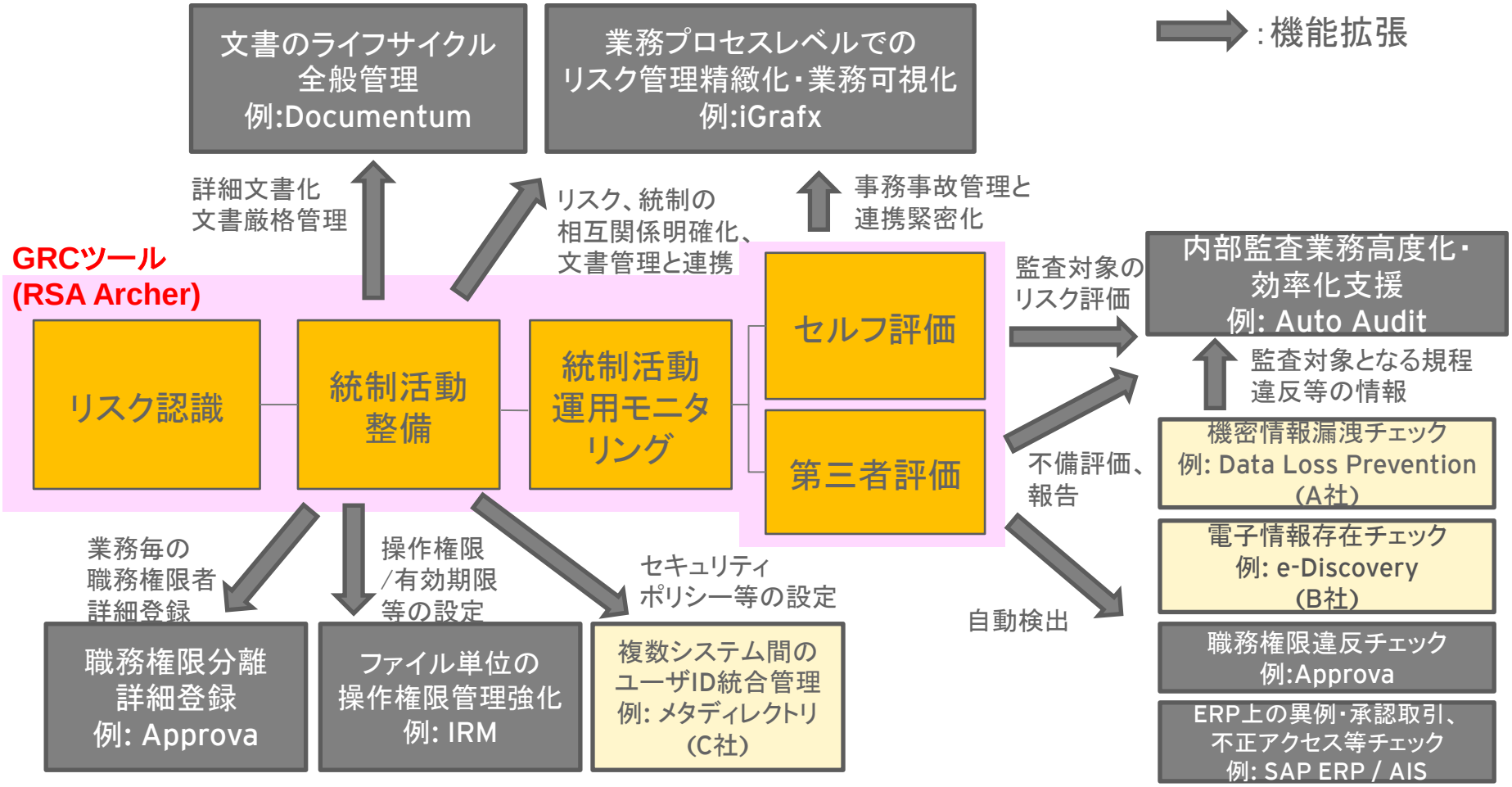
- これまで製品売上増に直接寄与しないリスク管理業務に対する投資は、なかなか経営陣の理解を得られなかったが、現在は震災影響もあってリスク管理の重要性を経営陣に訴求し易い環境になっている。
- 本社グローバルリスク管理本部としては、リスク管理フレームワークの社内啓蒙を進めることも重要なミッションと考えている。
- 当面は本社グローバルリスク管理本部自身がArcherの機能理解を図ると共に、USでの稼働状況を十分に見極めたうえでグループ内にどう効率的に展開出来るか、対象事業部門などを検討していく予定である。

3. 他ツールとの関連情報の連携による機能拡張



(1)GRCツールの機能拡張によるリスク管理の全体像

- GRCツールの特筆すべき特徴として、他ツールと情報を連携して機能拡張を行える柔軟性の高さが挙げられており、こうした複合ソリューションによりリスク管理の高度化を図ることが可能です。



(2)大手グローバル日系企業のコンプライアンス取り組み状況

■ リスクマネジメント上の諸課題に対処する場合、様々な事業リスクの中でも、まず法令遵守態勢のグローバルな浸透・徹底から着手する企業が多くみられます。最近では各種ツール等を効率的に活用し、コンプライアンスリスクの管理を図る取組みも始まっています。

A社（エレクトロニクス・エンタテイメント）

- 規制対応、情報セキュリティ、ベンダー管理、予兆・事故情報の一元管理を強化するため、US地域統括会社主導の下で、GRC統合リスク管理ツールを各事業ドメインに一斉導入中。
- 情報セキュリティに関しては、ISO27001とCOBITをベースに従来、130項目に亘るグローバルポリシー・スタンダードを整備し、環境変化と社会的要請、残存リスクの変化に応じて、現在全面見直しを検討中。
- また電子媒体以外のセキュリティを強化するため、GRCツールに加えて情報漏洩防止に特化したツール(DLP)も導入検討中。

B社（エレクトロニクス）

- 海外子会社におけるカルテル再発防止体制を強化するため、法人営業部門内におけるコンプライアンスチーム主導の下で、電子情報調査分析・開示用ツール(e-Discoveryツール)を導入しており、またGRCツールの導入も検討中。
- 国内事業部における60万件のメールについて法令違反に関係性の深い数千件に絞り込みを行えるようツールによる検証を実施中。

C社（ゼネコン）

- 同時進行する3000余りの国内外の現場工事に関する三次、四次の協力会社を含めたコンプライアンス、情報セキュリティの強化を図るため、権限認証の集中管理ツール（メタディレクトリ）を導入し、メール添付ファイルの自動暗号化も完了。8000社の協力会社と機密保持契約を締結済。

講師紹介

森本　親治 （金融アドバイザリー部　シニアパートナー）
GRC アドバイザリー業務責任者

Eメール:morimoto-shnj@shinnihon.or.jp
Tel:03-3503-1954（代表）

【専門分野】リスクマネジメント GRC ERM、内部統制、US/J-SOX, ERP導入、内部監査整備、
2006年新日本監査法人（現、新日本有限責任監査法人）入所。大手監査法人、東証一部上場流通業常務取締役、有力外資系流通業マネジメントディレクター、大手コンサルティングファームにおけるディレクター 流通消費財事業部長、リスクマネジメントリーダーを経て、現在に至る。
メガバンクを中心とした金融業、自動車、電機、食品、商社等の様々な業界に、US/J-SOX対応、リスクマネジメント、組織設計、ビジネスプロセス改革、業績改善、ERP導入システム開発、サプライチェーン最適化、営業改革等の支援業務を提供。内部統制統括部長を経て、現在はJapan Area GRC Champion、金融アドバイザリー部Markets 副担当、自動車業部会　専門委員及びメガバンクグローバルアカウント チーム　アドバイザリーサービス　ライン責任者としてサービス提供に従事している。
神戸大学経営学部卒業。日本CFO協会主任研究委員。

（著書等）『企業改革法が変える内部統制プロセス』（日経BP社）、『内部統制の落とし穴完全ガイド」』（日経BP社）、『在庫管理のポイント』（創己塾出版社）、『FASS検定　公式テキスト　経営会計』（日本CFO協会　監修）他、寄稿多数
（講演）日経フォーラム、CFOフォーラム（日本CFO協会主催）、日本内部監査協会セミナー、SAPフォーラム、IBMフォーラム等でERM、SOX対応、グループ経営等に関し、講演（最近3年間で22回）
（資格）公認会計士（JCPA）