

Insights on  
governance, risk  
and compliance

# SAP GRCソリューションによる リスク管理の変革

(GRC: Governance, Risk, and Compliance)

EYアドバイザリー・アンド・コンサルティング株式会社

The EY logo consists of the letters 'EY' in a bold, white, sans-serif font. A yellow chevron shape is positioned above the 'Y'.

Building a better  
working world

# 目次

はじめに .....	1
GRCの定義 .....	2
GRCテクノロジーの価値 .....	6
SAP GRCソリューションについて .....	8
SAP GRC Risk Management .....	9
SAP GRC Process Control .....	10
SAP GRC Access Control .....	11
まとめ .....	12



# はじめに

リスク管理は、いまや「その場限り・個別に都度対応」で対応すべき活動ではなく、企業の日常業務と統合された活動の一つです。外部リスク・内部リスクに対する管理がますます複雑化する一方で、ガバナンス・リスク・コンプライアンス(Governance, Risk, Compliance、以下「GRC」)に関する包括的かつ実用的な情報が求められています。従来型のリスク管理手法は機能、プロセス、手法、インフラ等が統一されておらず、こうした縦割型のリスク管理では、現在のさまざまな要求に対応することができなくなっています。多くの場合、リスク管理は業務面と財務面で大きな負担となっているのが実状であり、企業が中核事業の成長・変革に対応していく能力を阻害する要因となっています。

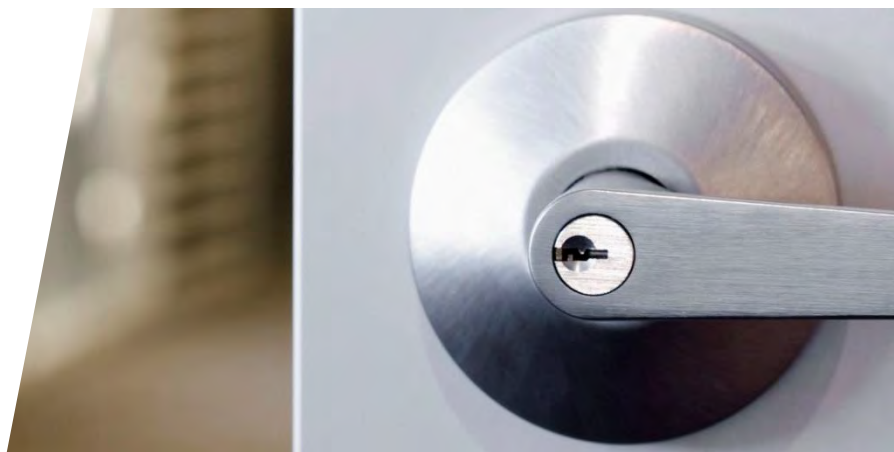
こうした状況に的確に対処するため、リーディングカンパニーは、テクノロジーを活用したGRC変革ソリューションの導入を推進し、下記の効果をあげています。

- ▶ 全社的なリスクの可視化、リスク緩和施策の明確化
- ▶ 手作業による管理プロセス比率を低下させることによる、リスク管理コストの削減
- ▶ 管理プロセスの標準化、簡素化、自動化、および一元化による効率性の向上

本冊子ではGRCの範囲について検討し、GRCテクノロジーがもたらす価値について解説した上で、SAP GRCがRisk Management(リスク管理)、Process Control(統制評価・自動化)、およびAccess Control(アクセス管理)をどのように支援するのかを説明します。

**GRCテクノロジーによる最適なソリューションは、費用対効果の高いリスク管理活動を日常業務に統合します。**

# GRCの定義



## GRCとは?

GRCは「ガバナンス、リスク、コンプライアンス」という三つの視点から、企業の統合的リスク管理を包括的に示す用語です。企業によって解釈が異なることがありますが、一般的にはコーポレート・ガバナンス、全社的リスクマネジメント(Enterprise Risk Management、以下「ERM」)、内部統制、法規制対応、および内部監査等の活動を対象にします。GRC活動は従来型の重複した非効率な活動を解消するべく、管理プロセス(組織構造・業務プロセス・システム・データ構造)に組み込まれる形で、統合される方向にあります。「全社横断的なリスク管理最適化」と言い換えることもできます。

「ガバナンス」により、リスク管理活動とビジネス戦略目標の整合性が向上します。下記のガバナンス活動により、説明責任と情報開示がより明確になり、重要度の高いリスクが浮き彫りにされ、意思決定プロセスが改善されます。

### 経営戦略関連

- ▶ 経営戦略・目標の設定
- ▶ 企業の文化・価値観の確立

### リスク関連

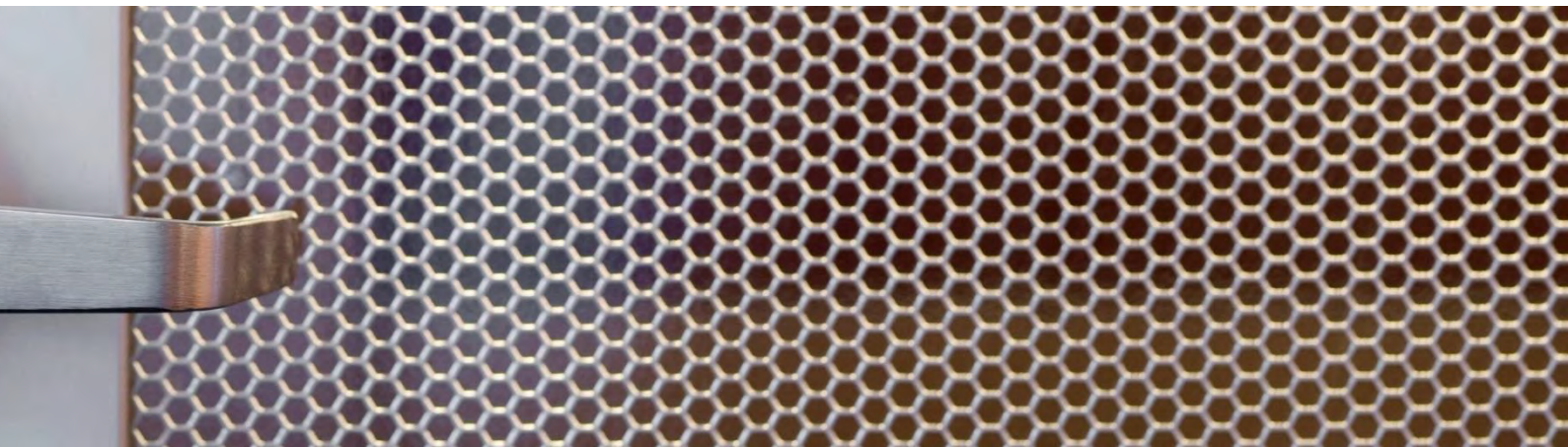
- ▶ リスクガバナンス機関の役割と責任の決定
- ▶ リスク許容度の決定
- ▶ 社内基準・社内規程の設定

「リスク」管理では、リスク管理活動をビジネス機能・業務プロセスに組み込むことにより、全社横断的な最適化を図ります。下記の活動を通じて、業績に影響を及ぼし得るリスク傾向が予測分析可能になり、リスクへの迅速な対応につながります。

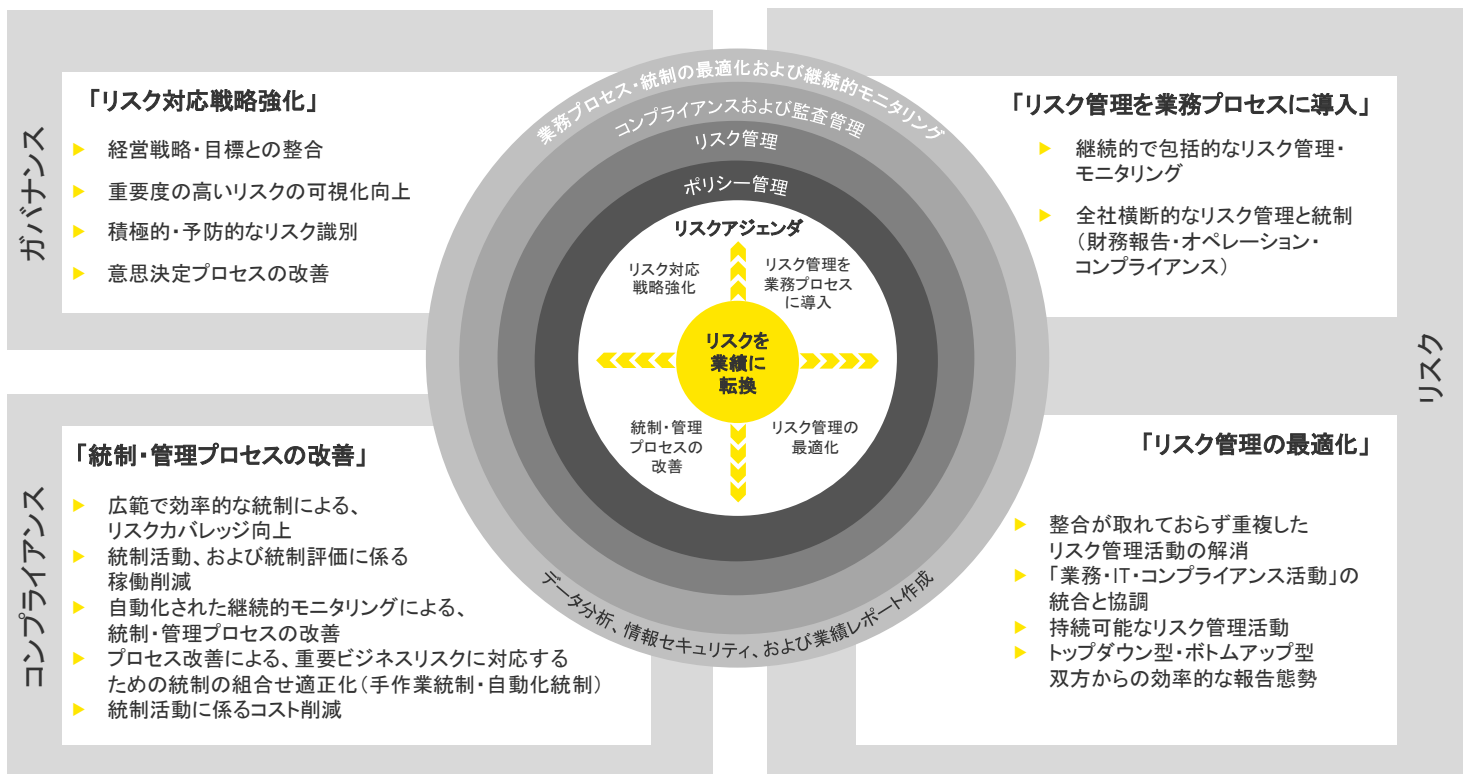
- ▶ ビジネス目標達成に影響するリスクの特定・評価
- ▶ リスク対応戦略の決定
- ▶ 統制活動の定義

「コンプライアンス」は、法規制対応・ビジネス上の要請に対応するための内部統制とその実施プロセスを整備し、運用促進を図ります。下記のコンプライアンス活動により、自動化統制・継続的モニタリングが日常の業務プロセスに統合され、結果としてリスクと統制の透明性が向上し、「リスクに対処されていない」業務が排除されます。

- ▶ 統制活動、社内規程、社内基準、およびコミットメントの遵守状況判定
- ▶ 課題管理、トラッキング、および是正



EYのリーディングプラクティスである「リスクアジェンダ」を下記に示します。この4要素で統合的GRCによるリスク管理を推進し、全社横断的GRCアプローチを提供します。



### 食品・飲料会社 (Global Fortune 100)

全社レベルで共通のリスク管理・統制の枠組みを策定し、重複する統制活動の可視化を行い、業務処理統制のライブラリ（データベース）を一元化した。SAPIに実装された90個以上の自動化統制を精査し、さらなる合理化および自動化を実現した。

# GRCの定義

## なぜ「GRC」なのか？

世界が急速に変化し続ける中、企業は業績向上のみならずリスク管理の適切な実施も外部から強く求められています。たった一度のリスク事象を回避できないだけで、企業の信用は著しく損なわれることがあります。

外部リスク・内部リスクに対する管理が複雑化する一方で、全社横断的に統合された包括的かつ実用的なGRC情報が求められています。従来型のリスク管理手法(サイロ化・縦割型)は機能、プロセス、手法、インフラ等が統一されておらず、今日の要求事項に即応することができなくなっています。リスク管理は多くの場合、業務面・財務面の負荷となっており、中核事業の成長・変革への対応能力を限定する要因となっています。

従来型のリスク管理手法では、内部監査、リスク管理、内部統制の各機能が個別最適を志向し、それにより全社横断的な連携・コミュニケーションに課題が生じ、結果としてリスク対応計画・業績管理が分断される事態を招いてきました。これからはそれを解消し、リスク管理を「漏れなくダブリなく」、価値創造的なものとするのが要求されています。一方でコスト削減圧力についても、昨今の厳しい経済環境下で高まっています。非効率な統制活動・コンプライアンス態勢による「隠れたコスト」を削減するために、全社レベル・事業部レベルで重複した作業を解消するべく、GRC機能の向上が求められています。

### 従来型GRC

#### サイロ化・縦割型 リスク管理

- ▶ リスクを把握・評価するための手法が部署間で統一されていない
- ▶ 職務分掌違反
- ▶ リスク識別の精度・正確性に対する、信頼欠如

#### 断片的活動

- ▶ 断片的で手作業による、都度でのレポート作成
- ▶ 統合化されたリスクヒートマップが作成できない
- ▶ 業績管理に直結するリスク・コンプライアンスに都度着目

#### 部分最適 プロセス

- ▶ リスク管理プロセス・統制標準化の欠如
- ▶ 重複した手作業によるリスク管理活動
- ▶ ビジネスに影響するほどのコスト

### 将来型GRC

#### 全社横断的 リスク管理

- ▶ リスク管理活動が組織横断的に一貫している
- ▶ リスク識別・リスク評価管理が一元化
- ▶ トップダウン型・ボトムアップ型双方でのリスク統合
- ▶ 複数部署にまたがるリスク管理が可能

#### 統合的活動

- ▶ 継続的なリアルタイムでのレポート作成
- ▶ 一元化・統合化されたリスクヒートマップ
- ▶ レポートからの詳細参照が容易(ドリルダウン機能)
- ▶ 重要ワークフローの自動化
- ▶ リスク管理に整合する権限グループ(ロール)の設定と権限付与

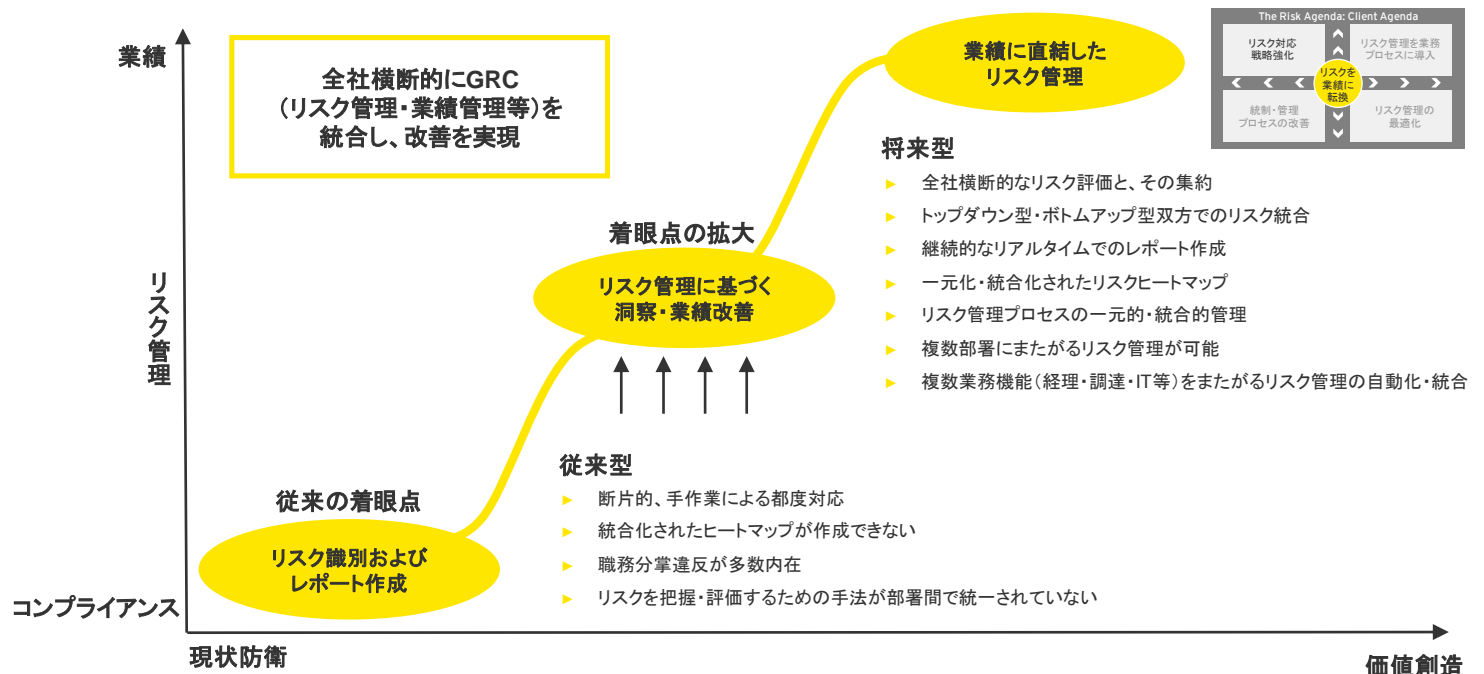
#### 全社最適 プロセス

- ▶ リスク管理プロセスの一元的・統合的管理
- ▶ 自動化されたリスク管理活動
- ▶ 重要ワークフローの自動化
- ▶ 合理的なコスト負荷

## テクノロジーが実現するGRC変革

テクノロジーを活用したGRC変革ソリューションがもたらす価値について、注目が集まっています。企業の各事業部はこれまで事業部ごとにリスク管理を実施していましたが、昨今では全社横断的なビジネス、リスク管理、財務報告、および資本政策の統合に向かいつつあります。それに伴うリスク管理活動の変革によって「将来を見据えた価値創造」「競争優位の実現」を可能とします。部署単位のリスク管理から全社横断的なリスク管理へとシフトすることで、リスクを意識するという企業文化が、重要な付加価値を創造する活動として全社レベルで促進されます。

次の表は、リスクやコンプライアンス機能に対して個別に対応していた従来型GRCから出発し、GRC変革を成功させるまでの道筋を示したものです。GRC変革に関するリーディングプラクティス（先行事例）を参照・導入することによって、企業は全社横断的に統合され成熟したGRC管理を実現できます。リーディングプラクティスでは「守り・防衛」のリスク管理にとどまらず、ビジネス価値創出に貢献する高度なリスク管理を志向します。



# GRCテクノロジーの 価値



従来型GRCにおける関連テクノロジーは、個別課題に対応するソリューション提供を目的としていました(内部監査サポート、統制文書管理等)。一方、今日のリーディングカンパニーは、複数課題への統一的対応を目的としてGRCテクノロジーを活用しています。これまでの一般的な企業はサーベンス・オクスリー法(SOX法)等、特定規制の遵守を念頭に置いていましたが、リーディングカンパニーは包括的なGRC活動により、監査対応・法規制対応・ITガバナンス・業績改善・ポリシー管理に対応しています。それゆえ「一元化されたデータベースの構築」「データ分析の有効活用」が今まで以上に重要となっています。

多くの企業がGRCテクノロジー活用による経営戦略目標の追求・新たな価値創造に取り組むとともに、リスク管理活動・管理プロセスの実効化・統合化・最適化を図っています。GRCテクノロジーは急速に普及しており、リーディングカンパニー各社による採用が進んでいます。GRCテクノロジーは全社共通のリスク管理概念を用い、各管理プロセスの整合性、統合性を高めることによって、コスト効率、イノベーション、効果的なワークフローの実現を図ります。GRCテクノロジーは、ガバナンス、リスク管理、コンプライアンス、プロセス改善を一体化したソリューションです。

GRCテクノロジーは下記の活動を通じて、リスク管理水準を大幅に向上させます。

- ▶ 内部統制・各種管理プロセスの自動化と標準化
- ▶ リスク管理と統制に関するデータを、統一された形式で管理
- ▶ 全社横断的なリスク管理・コンプライアンス管理情報の参照(リスクダッシュボード)
- ▶ リスク管理と統制に関する、リアルタイムの情報生成・レポート作成
- ▶ リスク兆候情報の把握と分析、それに対する判断のサポート
- ▶ 組織全体に周知徹底されたワークフロー

## 医薬・医療会社(Global Fortune 500)

世界各地域の2,000以上に及ぶ業務処理統制を合理化し300にまで削減。自動化により大幅なコスト削減を実現した。SAP GRC Access Controlを世界規模で導入した結果、監査手続が大幅に改善され、社内外で実施されている評価業務が大幅に効率化された。





## GRCテクノロジー選定プロセス

株主価値の追求におけるリスク管理の重要性増大に対応して、ベンダー各社はより包括的で柔軟性の高いGRCソリューションを提供しています。こうしたソリューションを導入した企業は、リスク管理プログラムの改善・リスク管理プロセスの成熟度向上に短期間で成功しています。

リスク管理を経営戦略に統合させ得る最適なGRCテクノロジーの選定に、下記チェックリストをご活用ください。



- ▶ 会社概要、市場での地位、および実績
- ▶ 長期的な製品戦略
- ▶ 競争力
- ▶ パートナー企業
- ▶ 既存顧客
- ▶ 導入手法
- ▶ 研修体制
- ▶ ソフトウェアライセンス形態、リリース戦略、保守サービス

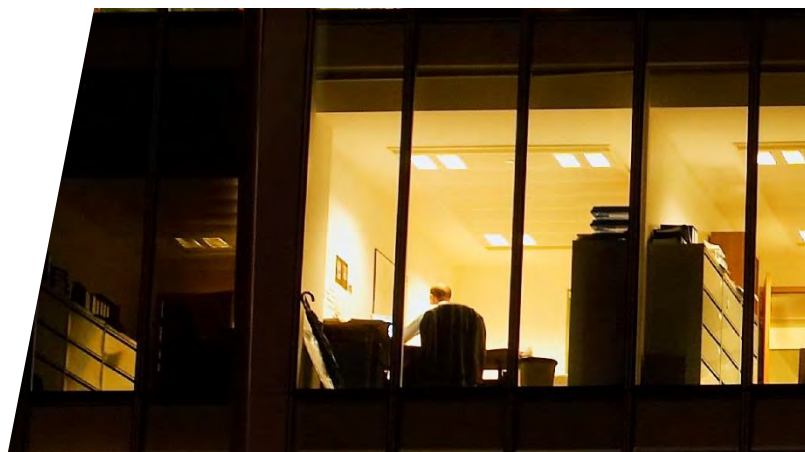
- ▶ 製品機能
- ▶ データ・リポジトリ管理 (統合的データベース)
- ▶ レポート作成能力
- ▶ ワークフロー管理
- ▶ 発見事項レビュー、対応とそれに対する承認のトラッキング機能
- ▶ リスク管理機能
- ▶ 監査管理機能
- ▶ 統制モニタリング機能
- ▶ データ分析機能

- ▶ 提供ベンダー・製品の情報
- ▶ 技術的アーキテクチャ
- ▶ 性能・拡張性
- ▶ プロダクト戦略
- ▶ モバイル機器の活用、リモートアクセス
- ▶ ソフトウェア保守モデル
- ▶ 情報セキュリティ

### 石油・ガス会社 (Global Fortune 500)

全世界のSAPインスタンス20個を対象としてSAP GRC Access Controlを導入することでアクセス管理プロセスを世界規模で標準化し、統制環境を強化した。標準化の結果、アクセス管理プロセスの効率性は20~30%改善された。それまでの担当者の手作業による事後的・発見的な対応から、職務分掌を明確にした予防的統制、および実効的なアクセスログのチェックに比重が移り、リスク管理が大きく改善された。

# SAP GRC ソリューションについて

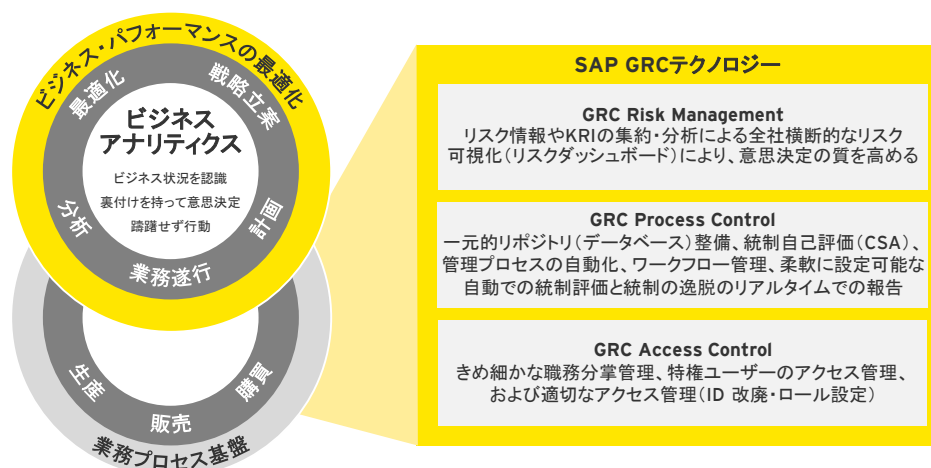


今日では多くのITベンダーがGRCテクノロジー関連ソリューションを提供しています。本冊子ではSAP社が提供するGRCテクノロジーと関連ソリューションを取り上げます。

- ▶ **SAP GRC Risk Management** (リスク管理)は、リスク情報やKRI(Key Risk Indicator)の集約・分析による全社横断的なリスク可視化(リスクダッシュボード)により、意思決定の質を高めます
- ▶ **SAP GRC Process Control** (統制評価・自動化)は、一元のリポジトリ(データベース)整備、統制自己評価(Control Self Assessment: CSA)、管理プロセスの自動化、ワークフロー管理、柔軟に設定可能な自動での統制評価と統制の逸脱のリアルタイムでの報告を可能にします
- ▶ **SAP GRC Access Control** (アクセス管理)は、きめ細かな職務分掌管理、特権ユーザーのアクセス管理、および適切なアクセス管理(ID改廃・ロール設定)を可能にします

次ページ以降では、上記のうち3つについて説明します。

(SAP GRC Risk Management、SAP GRC Process Control、SAP GRC Access Control)



**SAP GRC Risk Management**

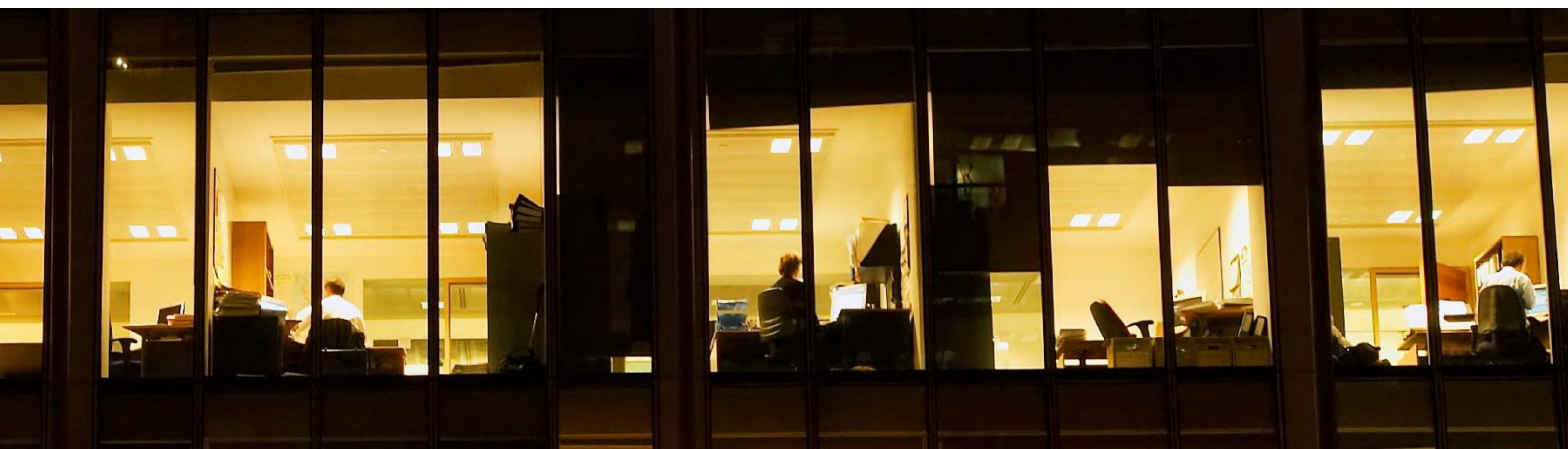
- ▶ リスク管理と戦略を統合
- ▶ リスク分析・リスク緩和のための再利用可能なフレームワーク
- ▶ 戦略目標ごとのKRIを継続的にモニタリング

**SAP GRC Process Control**

- ▶ 社内規程・法規制対応にかかわる継続的な統制モニタリングを自動化
- ▶ システム横断的なコンプライアンス情報可視化・レポジットリによる、複合的管理の効率化

**SAP GRC Access Control**

- ▶ 組織全体で整合した、継続的な「アクセス管理」
- ▶ 自動化されたアクセス関連リスク分析・緩和による、情報保全・不正防止



## SAP GRC Risk Management

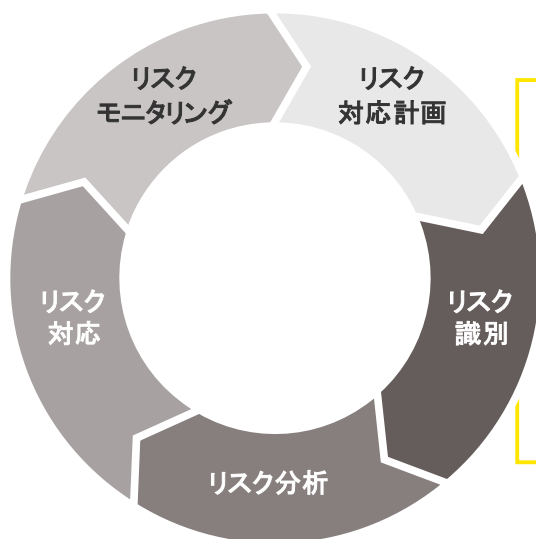
SAP GRC Risk Managementは、企業が直面する多様なリスクを把握・管理するための統合的アプローチを提供します。主な目的は、意思決定の質を高めることです。さらに、リスク間の相互作用を経営者が事前に認識できるようにすることで、予測できたかもしれない事象によって企業が不測の事態に陥る可能性を低減させます。

SAP GRC Risk Managementの特長

- ▶ **リスク対応計画** 経営戦略立案から業務プロセスまで、包括的なリスクと統制の管理を可能にします。これにより経営戦略、財務報告、オペレーション、コンプライアンスといったそれぞれの場面でのリスク管理に一貫性を持たせることができます

- ▶ **リスク識別** 将来の不確実性に積極的に対処するため、全社横断的にリスクを特定し、その発生可能性を数値化します。予防的な警告が発せられることで、リスクが自動的に特定され、優先順位が付けられます。法規制への対応がより確実に行われることになり、信用低下や損失発生といった事態を避けることができます
- ▶ **リスク分析** GRCツール機能がリスクの正確かつ素早い分析を可能にすることで、意思決定プロセスが改善され、リスクモデルの実効性と効率性が向上します
- ▶ **リスク対応** リスクに素早く対応するための施策(「低減」「保有」「回避」「移転)を導入することで、マイナスの影響を最低限にします
- ▶ **リスクモニタリング** リスクが業績に及ぼす影響をモニタリングし、可視化します。これにより、実効的なレポート機能・ワークフローを実現します

SAP GRC Risk Management(SAP GRC RM)の導入により、リスク管理モデルの主要4項目(リスクガバナンス、リスク管理、リスク統合、業務プロセス管理への適用)を網羅することができます。



### SAP GRC RMの機能は下記のとおりです

- ▶ 共通のリスク定義(リスクプロファイル、リスク選好、リスク許容度、対応戦略、対象範囲等)
- ▶ リスクリポジトリの構築と分類
- ▶ リスク評価プロセスの自動化
- ▶ リスクヒートマップの一元化、統合化
- ▶ リスクの相互関連付け・シミュレーション
- ▶ プロセスを一気通貫したワークフローによる、自動化されたリスク管理

# SAP GRCソリューションについて

## SAP GRC Process Control

SAP GRC Process Control は、内部統制モデル（自動化統制、手作業統制、統制評価/承認ワークフロー）および内部統制に対するコンプライアンスのモニタリングの双方を自動化します。省力化を図るとともに、経営者評価業務に対する信頼感を向上させます。

- ▶ **統制リポジトリ一元化** 内部統制モデルの管理業務・文書化プロセスを一元化し、リポジトリ（データベース）を作成します。設定やマスターデータの更新も早期に識別することができます
- ▶ **統合** ビジネス・IT・コンプライアンスの統合と協調を促進します。内部統制が全社的な業務として組み込まれ、より適切な役割を果たします
- ▶ **自動化** 継続的な統制監視（Continuous Control Monitoring: CCM）態勢が自動化・整備されることによって、コンプライアンス違反のレポートがリアルタイムで作成され、内部統制に対するコンプライアンスが担保されます。このような自動レポート作成機能により、「人為的ミス」の要因が取り除かれ、内部統制の

効率性が高まり、「統制の有効性」への信頼性が向上します。コンプライアンス対応コスト（投入時間、投入人員）が削減されること、および監査効率が向上することで、業務プロセス管理に係る「手作業」が最小限に抑えられます

- ▶ **定期的・継続的なモニタリング** 事前に設定したルールに基づき「統制からの逸脱」可能性をリアルタイムで通知します（例：通常想定していない例外的な生産変更を特定し、警告を発することで不正が生じている可能性を示唆する）。業務プロセスに統合された統制はトランザクションを「全件」監視するため、評価の有効性が向上します。また、統制の標準化とポリシーの適切な管理により、業務の効率性を高めます。さらに適切な統制の整備・現状分析による統制見直しを行えば、より高い効率性を実現できます。内部監査が行き届かなかつたことで発生する損失を回避できます
- ▶ **システム間の可視性** 複合的管理を効率的かつ全社横断的に実施するために、コンプライアンス情報が一元化されたりポジトリ（データベース）が構築されます。業務プロセスに関連するリスク発生の可能性が可視化され、全社横断的な統制評価を行うことができます

SAP GRC Process Controlを導入することで、業務の協調性と透明性が向上し、コンプライアンス活動とリスク管理活動の自動化を実現することができます。

主要活動		機能		
承認・レポート	分析・レポート作成	認証取得、サインオフ、監査証拠の提供	<ul style="list-style-type: none"> <li>▶ 統制活動、統制評価、発見事項、是正の状況を、プロセス・ポリシー・地域・勘定科目を横断して、インタラクティブに提供。複数様式での出力にも対応可能</li> <li>▶ ポリシー管理、ISO等の認証管理</li> </ul>	
モニタリング	発見事項のモニタリング	発見事項の是正	<ul style="list-style-type: none"> <li>▶ 「統制からの逸脱」および関連する影響について、ほぼリアルタイムで通知</li> <li>▶ ワークフローを活用したモニタリング活動・発見事項への対応</li> </ul>	
統制評価	自動化統制の評価	手作業統制の評価	総合評価	<ul style="list-style-type: none"> <li>▶ 統制テスト計画の柔軟な立案</li> <li>▶ 継続的統制モニタリング（CCM）用の、120超のスクリプト・カスタマイズ可能なSAPクエリ/レポートをERPに統合</li> </ul>
スコアリング	重要性に基づく分析	リスク評価	戦略評価戦略	<ul style="list-style-type: none"> <li>▶ 組織、業務プロセス、および統制の一元化マップ</li> <li>▶ リスク評価ユーティリティ、カスタマイズ可能な統制評価戦略の定義</li> </ul>
設定・管理	統制環境	法規制対応、社内規程管理、および監査対応	全社横断的統合	<ul style="list-style-type: none"> <li>▶ 複数基準・法規制に対応可能なコンプライアンス支援（経営戦略・財務報告・オペレーション・ITリスク）</li> </ul>

## SAP GRC Access Control

SAP GRC Access Control は、アプリケーションへのアクセス権に関する統制モデルを自動化する複数のツールで構成されています。それは、職務分掌 (Segregation of Duties: SoD) 違反を発見し解消する "get clean" と、プロセスの自動化によって将来にわたり職務分掌違反の防止を維持する "stay clean" という大きな二つの仕組みによって実現されます。

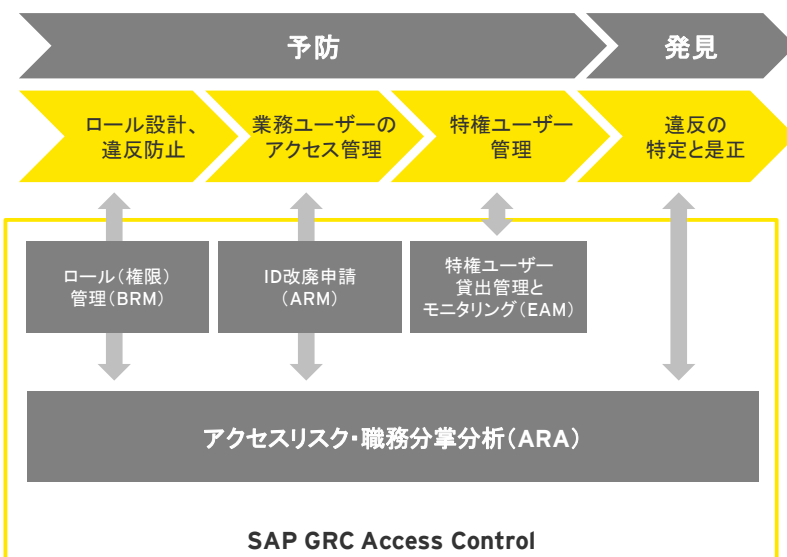
SAP GRC Access Control は、以下のアクセス管理の4大機能を有しています。

1. リスク分析・是正  
(Access Risk Analyzer: ARA)
2. 全社的なロール(権限)管理  
(Business Role Management: BRM)
3. 特権ユーザー管理  
(Emergency Access Management: EAM)
4. コンプライアンスを考慮したアクセス権管理(ID改廃)  
(Access Request Management: ARM)

SAP GRC Access Control の機能は下記のとおりです。

- ▶ **ロール(権限)管理の一元化** トランザクションコード単位での職務分掌ルールライブラリ等、厳密なコンプライアンスを可能にするロール管理を一元化・統合化します
- ▶ **アクセス状況モニタリングと統制** 特権ユーザー管理をモニタリングとレポート機能によって自動化。特権ユーザーによるアプリケーション操作が想定外であり、不正アクセスの可能性を示唆している場合は、ログレビュー・警告表示により特定可能です
- ▶ **自動化** ユーザー自身によるアクセス権要求 (ID発行依頼)、承認者による承認プロセス等について、ワークフローによりプロセスを一気通貫に自動化可能になります
- ▶ **コンプライアンス** 継続的なアクセス管理(アクセス認証を含む)によって、職務分掌の全社横断的な管理を支援します
- ▶ **情報保護** アクセス権に係るリスクの分析とその是正を自動化することによって、不正の発生を回避し、より確実に情報を保護します

SAP GRC Access Control (SAP GRC AC) の導入により、アクセス管理の4大要素の実現を可能にします。



### SAP GRC ACの特長

- ▶ 業務に即した、コンプライアンスを考慮したロール設計・ロール定義
- ▶ 特権ユーザーの統合的モニタリングとレポート体制
- ▶ ユーザー自身によるアクセス要求、および承認者による承認プロセス
- ▶ トランザクションコードに基づく、職務分掌ルールの一元的ライブラリ
- ▶ 不正アクセスを素早く特定、アクセス要求シナリオのシミュレーション可能
- ▶ ワークフローにより自動化された、一連のアクセス管理

# まとめ

GRCテクノロジーは、価値創造、コスト削減、リスク管理・業績管理の向上を支援します。GRCテクノロジーを導入することで、業務プロセスの自動化、標準化、合理化が可能になります。リスクとコンプライアンスに関する情報が全社横断的に可視化され、必要な情報をリアルタイムで分析することができます。GRCテクノロジーは貴社の意思決定に大きく貢献します。貴社GRCテクノロジー成熟度を評価するため、下記のチェックリストをご活用ください。

## GRC Risk Management

- 経営戦略からビジネスプロセスまで一貫してリスク管理と統制が整合し、統合されているか
- リスク管理を一元化しているか(経営戦略・財務報告・オペレーション・コンプライアンス)
- リスクモデルの実効性・効率性を向上させているか
- 業績に対するリスクの影響について、可視性を向上させているか
- 新たな法規制に対して追加の対策が行われ、信用低下や損失発生 の予防策が取られているか
- 透明性を確保するために、全社横断的にリスクを事前に特定し、リスク発生可能性を定量化しているか
- 意思決定プロセスを改善させるために、レポート機能ワークフローを効果的に設定しているか
- 自動的な事前警告・対処によりリスクが特定され、優先順位付けされているか
- リスクによるマイナスの影響を予防するため、リスク緩和活動やリスク発生時の即応体制が整えられているか

## GRC Process Control

- 自動化統制・モニタリング活動について、SAPへの実装可能性について分析・検討しているか
- 例外的業務・取引について、業務部門が発見・防止・監視・承認できるか
- 事前に決定したルールに基づいた発見事項がリアルタイムで通知され、効率的な対応が可能か
- 統制の自動化によって、監査対応、文書化、および発見事項管理にかかる時間を大幅に低減したか
- 内部統制モデル管理の労力時間が、全社的に減少したか
- 内部統制評価の実施について、残存リスクに応じて、費用対効果の高いリソース組合せを確立しているか
- 従来型の事後的・発見的な内部統制モデルから、即応的・予防的なモデルに変革したか
- 財務報告プロセス・業務プロセスを最適化しているか(統制の信頼性・有効性の向上)

## GRC Access Control

- 職務分掌の診断が、リアルタイムで行われているか
- 重要なトランザクションコード実行・ユーザー活動のモニタリングは、リアルタイムで行われているか
- 統制リポジトリ(データベース)・リスクを表示する「リスクダッシュボード」は一元化されているか
- 職務分掌において、違反(権限競合)が発生するリスクを予防しているか
- 複数の異なるデータオーナーによる承認行為が、自動化・統合化されているか
- アクセス管理は、全てのアプリケーション横断的に最適化されているか(ID改廃、権限付与・修正)
- ロール(権限)・プロファイルの管理が「ベストプラクティス」に準拠しているか、ロール・プロファイルに関する定義・文書化・作成・評価・維持が、全て管理プロセスで一貫しているか
- 特権ユーザー管理・モニタリングは自動化され、事後確認可能か

## より深く知るには？

「Insights on governance, risk and compliance」は、IT・ビジネスリスクに関連した課題・機会に焦点を当てたシリーズです。これらは最新の論点に基づいてタイムリーに解説されています。GRC理解の一助として、価値ある考察を提供いたします。

### Risk Management



#### 『Turning risk into results: enabling risk management with SAP GRC』

SAP GRCが実現可能とする「リスク管理」を取り上げます。マーケット認識、改善機会、導入メリットとともに、想定する着手ポイントについて解説します。



#### 『The future of Internal audit is now: increasing relevance by turning risk into results』

「経営戦略と内部監査との整合」に焦点を当てます。リスク成熟度の向上施策により、業績向上への貢献を志向します。

### Process control



#### 『Turning risk into results: enabling compliance and process management with SAP GRC』

SAP GRCが実現可能とする「コンプライアンス・業務プロセス管理の最適化」を取り上げます。SAPが提供する業務プロセス・統制分析機能による、リアルタイムでの状況把握について解説します。



#### 『Smart Control: transforming controls to reduce cost, enable growth and keep the business safe』

業務プロセスの価値・コスト・リスクに合致した内部統制を整備・運用することで、企業は競争力を高めることができます。それにより変化を的確に予測し、機敏な対応を可能にします。

### Access control



#### 『Turning risk into results: enabling access management with SAP GRC』

SAP GRCが可能とする「アクセス権管理」を取り上げます。費用対効果が高く、効率的に継続可能なアクセス権管理が、一元化・標準化・自動化・他モジュールとの連携によってどのように実現され得るかを解説します。



#### 『A risk-based approach to segregation of duties』

IT全般統制・業務処理統制における「リスクベース方法論」について解説します。管理が容易で、費用対効果の高いアプローチをもたらします。

## EYについて

EYは、アシュアランス、税務、トランザクションおよびアドバイザリーなどの分野における世界的なリーダーです。私たちの深い洞察と高品質なサービスは、世界中の資本市場や経済活動に信頼をもたらします。私たちはさまざまなステークホルダーの期待に応えるチームを率いるリーダーを生み出していきます。そうすることで、構成員、クライアント、そして地域社会のために、より良い社会の構築に貢献します。

EYとは、アーンスト・アンド・ヤング・グローバル・リミテッドのグローバル・ネットワークであり、単体、もしくは複数のメンバーファームを指し、各メンバーファームは法的に独立した組織です。アーンスト・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。詳しくは、[ey.com](http://ey.com) をご覧ください。

## EY Japanについて

EY Japanは、EYの日本におけるメンバーファームの総称です。新日本有限責任監査法人、EY 税理士法人、EY トランザクション・アドバイザリー・サービス株式会社、EY アドバイザリー・アンド・コンサルティング株式会社などから構成されており、各メンバーファームは法的に独立した法人です。詳しくは [www.ejapan.jp](http://www.ejapan.jp) をご覧ください。

## EY アドバイザリー・アンド・コンサルティング株式会社について

EY アドバイザリー・アンド・コンサルティング株式会社はEYの日本におけるメンバーファームです。さまざまな分野の専門性を有するプロフェッショナルがグローバルに連携し、企業が抱える経営課題に対し、最先端かつグローバルな視点と実行力で最適なアドバイザリーサービスを総合的に提供いたします。詳しくは [www.ejapan.jp/advisory](http://www.ejapan.jp/advisory) をご覧ください。

© 2017 EY Advisory & Consulting Co., Ltd. All Rights Reserved.

ED None

本書は一般的な参考情報の提供のみを目的に作成されており、会計、税務およびその他の専門的なアドバイスを行うものではありません。EY アドバイザリー・アンド・コンサルティング株式会社および他の EY メンバーファームは、皆様が本書を利用したことにより被ったいかなる損害についても、一切の責任を負いません。具体的なアドバイスが必要な場合は、個別に専門家にご相談ください。

## サービスに関するお問い合わせ

EY アドバイザリー・アンド・コンサルティング株式会社

お問い合わせフォームへ  
(ここをクリックしてください)