GRC (Quản trị, quản lý rủi ro và tuân thủ) là gì?

(GPLaw) - ***GRC*** *– Governance, Risk management and Compliance: Quản trị, quản lý rủi ro và tuân thủ là thuật ngữ bao gồm cách tiếp cận của một tổ chức thông qua ba hoạt động trên. Đây là một phương pháp tổng thể và tích hợp giúp các tổ chức quản lý các hoạt động then chốt của mình một cách hiệu quả và có hệ thống. Trong bối cảnh kinh doanh ngày nay, GRC không còn là một lựa chọn mà trở thành một yêu cầu then chốt đối với mọi doanh nghiệp muốn duy trì tính minh bạch, giảm thiểu rủi ro và đảm bảo tuân thủ các quy định pháp luật.*

1. Tổng quan về GRC:

GRC là một thuật ngữ bao gồm cách tiếp cận của một tổ chức thông qua ba hoạt động sau: Quản trị, Quản lý rủi ro và Tuân thủ.

Nghiên cứu học thuật đầu tiên về GRC được xuất bản vào năm 2007, trong đó GRC được chính thức định nghĩa là "tập hợp các khả năng tích hợp cho phép tổ chức đạt được các mục tiêu một cách đáng tin cậy, giải quyết sự không chắc chắn và hành động một cách liêm chính". Nghiên cứu đề cập đến các hoạt động chung "giữ cho công ty đi đúng hướng" được thực hiện trong các bộ phận như kiểm toán nội bộ, tuân thủ, rủi ro, pháp lý, tài chính, công nghệ thông tin, nhân sự cũng như các ngành nghề kinh doanh, bộ phận điều hành và chính hội đồng quản trị.

Quản trị, quản lý rủi ro và tuân thủ là 03 (ba) khía cạnh liên quan nhằm đảm bảo tổ chức đạt được các mục tiêu một cách đáng tin cậy, giải quyết sự không chắc chắn và hành động một cách liêm chính. Quản trị là sự kết hợp của các quy trình do giám đốc (hoặc ban giám đốc) thiết lập và thực hiện, được phản ánh trong cơ cấu của tổ chức cũng như cách tổ chức được quản lý và dẫn dắt để đạt được mục tiêu. Quản lý

rủi ro là dự đoán và quản lý những rủi ro có thể cản trở tổ chức đạt được mục tiêu một cách đáng tin cậy trong điều kiện không chắc chắn. Tuân thủ đề cập đến việc tuân thủ các ranh giới bắt buộc (luật pháp và quy định) và các ranh giới tự nguyện (chính sách, thủ tục của công ty…).

GRC là một nguyên tắc nhằm đồng bộ hóa thông tin và hoạt động trong quản trị cũng như tuân thủ để hoạt động hiệu quả hơn, cho phép chia sẻ thông tin hiệu quả, báo cáo hoạt động hiệu quả hơn và tránh sự chồng chéo lãng phí. Mặc dù được giải thích khác nhau ở nhiều tổ chức khác nhau, GRC thường bao gồm các hoạt động như quản trị doanh nghiệp, quản lý rủi ro doanh nghiệp (ERM) và việc tuân thủ luật pháp và quy định hiện hành của doanh nghiệp.

Các tổ chức đạt đến quy mô cần có sự kiểm soát phối hợp đối với các hoạt động của GRC để hoạt động hiệu quả. Mỗi lĩnh vực trong số ba lĩnh vực này tạo ra thông tin có giá trị cho hai lĩnh vực còn lại và cả ba lĩnh vực này đều tác động đến cùng công nghệ, con người, quy trình và thông tin.

Sự trùng lặp đáng kể về nhiệm vụ phát triển khi quản trị, quản lý rủi ro và tuân thủ được quản lý độc lập. Các hoạt động GRC chồng chéo và trùng lặp tác động tiêu cực đến cả chi phí vận hành và ma trận GRC. Ví dụ: mỗi dịch vụ nội bộ có thể được kiểm tra và đánh giá bởi nhiều nhóm hàng năm, tạo ra chi phí rất lớn và kết quả không đồng đều.

Cách tiếp cận GRC bị ngắt kết nối cũng sẽ ngăn tổ chức cung cấp các báo cáo điều hành GRC theo thời gian thực. GRC cho rằng cách tiếp cận này, giống như một hệ thống giao thông được quy hoạch kém, mỗi tuyến đường riêng lẻ sẽ hoạt động nhưng mạng lưới sẽ thiếu những phẩm chất cho phép chúng phối hợp hiệu quả với nhau.

Nếu không được tích hợp, nếu được giải quyết theo cách tiếp cận "silo" truyền thống, hầu hết các tổ chức sẽ phải duy trì số lượng yêu cầu liên quan đến GRC không thể quản lý được do những thay đổi trong công nghệ, tăng cường lưu trữ dữ liệu, toàn cầu hóa thị trường và tăng cường quy định.

2. Các khái niệm cơ bản:

Quản trị (Governance): Mô tả phương pháp quản lý tổng thể thông qua đó các nhà điều hành cấp cao chỉ đạo và kiểm soát toàn bộ tổ chức, sử dụng kết hợp thông tin quản lý và cơ cấu kiểm soát quản lý phân cấp. Hoạt động quản trị đảm bảo rằng: thông tin quản lý quan trọng đến được với đội ngũ điều hành là đầy đủ, chính xác và kịp thời để cho phép đưa ra quyết định quản lý phù hợp và cung cấp các cơ chế kiểm soát để đảm bảo rằng: các chiến lược, chỉ đạo và hướng dẫn từ ban quản lý được thực hiện một cách có hệ thống và hiệu quả.

Quản lý rủi ro (Risk management): Là tập hợp các quy trình qua đó ban quản lý xác định, phân tích và khi cần thiết ứng phó một cách thích hợp với những rủi ro có thể ảnh hưởng bất lợi đến việc thực hiện các mục tiêu kinh doanh của tổ chức. Phản ứng đối với rủi ro thường phụ thuộc vào mức độ nghiêm trọng được nhận thức và liên quan đến việc kiểm soát, tránh, chấp nhận hoặc chuyển chúng cho bên thứ ba, trong khi các tổ chức thường xuyên quản lý nhiều loại rủi ro, ví dụ: rủi ro công nghệ, rủi ro thương mại/tài chính, rủi ro bảo mật thông tin…

Tuân thủ (Compliance): Có nghĩa là tuân thủ các yêu cầu đã nêu. Ở cấp độ tổ chức, điều này đạt được thông qua các quy trình quản lý trong đó xác định các yêu cầu áp dụng (ví dụ như được xác định trong luật, quy định, hợp đồng, chiến lược và chính sách), đánh giá tình trạng tuân thủ, đánh giá rủi ro và chi phí tiềm ẩn của việc không tuân thủ đối với chi phí dự kiến để đạt được sự tuân thủ, từ đó ưu tiên, tài trợ và bắt

đầu mọi hành động khắc phục được coi là cần thiết. Quản lý tuân thủ đề cập đến việc thực hiện hành chính nhằm cập nhật tất cả các tài liệu tuân thủ, duy trì tính phổ biến của các biện pháp kiểm soát rủi ro và tạo ra các báo cáo tuân thủ.

Nhận thức về nghĩa vụ đề cập đến khả năng tổ chức nhận thức được tất cả các nghĩa vụ bắt buộc và tự nguyện của mình, cụ thể là luật liên quan, yêu cầu chế định, quy tắc ngành và tiêu chuẩn tổ chức, cũng như các tiêu chuẩn về quản trị tốt, các thông lệ tốt nhất, đạo đức và các quy định được chấp nhận chung. sự mong đợi của cộng đồng. Các nghĩa vụ này có thể là tài chính, chiến lược hoặc hoạt động khi hoạt động bao gồm các lĩnh vực đa dạng như an toàn tài sản, an toàn sản phẩm, an toàn thực phẩm, sức khỏe và an toàn nơi làm việc, bảo trì tài sản.

3. Phân khúc thị trường GRC:

Chương trình GRC có thể được thiết lập để tập trung vào bất kỳ lĩnh vực riêng lẻ nào trong doanh nghiệp hoặc GRC được tích hợp đầy đủ có thể hoạt động trên tất cả các lĩnh vực của doanh nghiệp bằng cách sử dụng một khuôn khổ duy nhất.

GRC tích hợp đầy đủ sử dụng một bộ tài liệu kiểm soát cốt lõi duy nhất, được ánh xạ tới tất cả các yếu tố quản trị chính đang được giám sát. Việc sử dụng một khuôn khổ duy nhất cũng có lợi ích là giảm khả năng thực hiện các hành động khắc phục trùng lặp.

Khi được xem xét dưới dạng các khu vực GRC riêng lẻ, các tiêu đề riêng lẻ phổ biến nhất được coi là: (i) GRC Tài chính (Financial GRC), (ii) GRC Hoạt động (Operational GRC), (iii) GRC Sức khỏe và an toàn lao động (Work Health and Safety - WHS GRC), (v) GRC Công nghệ thông tin (Information Technology - IT GRC), và: (vi) GRC Pháp lý (Legal GRC).

GRC tài chính: liên quan đến các hoạt động nhằm đảm bảo hoạt động chính xác của tất cả các quy trình tài chính, cũng như tuân thủ mọi nhiệm vụ liên quan đến tài chính.

GRC vận hành: liên quan đến tất cả các hoạt động vận hành như an toàn tài sản, an toàn sản phẩm, an toàn thực phẩm, sức khỏe và an toàn tại nơi làm việc, bảo trì tài sản tuân thủ công nghệ thông tin.

WHS GRC: một tập hợp con của GRC hoạt động, liên quan đến tất cả các hoạt động an toàn và sức khỏe tại nơi làm việc

IT GRC: một tập hợp con của GRC hoạt động, liên quan đến các hoạt động nhằm đảm bảo rằng: tổ chức công nghệ thông tin hỗ trợ các nhu cầu hiện tại và tương lai của doanh nghiệp và tuân thủ tất cả các nhiệm vụ liên quan đến công nghệ thông tin.

GRC pháp lý: tập trung vào việc gắn kết cả ba thành phần này thông qua bộ phận pháp lý và giám đốc tuân thủ của tổ chức. Tuy nhiên, điều này có thể gây hiểu nhầm vì ISO 37301 đề cập đến các nghĩa vụ bắt buộc và tự nguyện và việc tập trung vào GRC hợp pháp có thể gây ra sự thiên vị.

Tuy nhiên, AICD (Viện Giám đốc Công ty Úc) chia rủi ro thành 03 (ba) nhóm siêu lớn: (i) Rủi ro tài chính, (ii) Rủi ro hoạt động, (iii) Rủi ro chiến lược.

Các nhà phân tích không đồng ý về cách xác định các khía cạnh này của GRC như các loại thị trường. Gartner đã tuyên bố rằng thị trường GRC rộng lớn bao gồm các lĩnh vực sau: (i) GRC tài chính và kiểm toán, (ii) Quản lý GRC công nghệ thông tin, (iii) Quản lý rủi ro doanh nghiệp.

Họ tiếp tục chia thị trường quản lý IT GRC thành các khả năng chính này.
(i) Thư viện điều khiển và chính sách,
(ii) Phân phối và phản hồi chính sách,
(iii) Công nghệ thông tin Kiểm soát việc tự đánh giá và đo lường,
(iv) Kho lưu trữ tài sản công nghệ thông tin,
(v) Bộ sưu tập điều khiển máy tính chung (GCC) tự động,
(vi) Quản lý khắc phục và ngoại lệ,
(vii) Báo cáo,
(viii) Bảng điều khiển tuân thủ và đánh giá rủi ro công nghệ thông tin nâng cao,
(ix) Nhà cung cấp sản phẩm GRC

Sự khác biệt giữa các phân khúc phụ của thị trường GRC rộng lớn thường không rõ ràng. Với một số lượng lớn các nhà cung cấp tham gia vào thị trường này gần đây, việc xác định sản phẩm tốt nhất cho một vấn đề kinh doanh nhất định có thể là một thách thức. Do các nhà phân tích không hoàn toàn đồng ý về phân khúc thị trường, việc định vị nhà cung cấp có thể làm tăng thêm sự nhầm lẫn.

Do tính chất năng động của thị trường này, mọi phân tích về nhà cung cấp thường lỗi thời ngay sau khi được công bố.

Nhìn rộng ra, thị trường nhà cung cấp có thể được coi là tồn tại trong ba phân khúc:
(i) Giải pháp GRC tích hợp (lợi ích đa quản trị, toàn doanh nghiệp),
(ii) Giải pháp GRC cụ thể theo miền (lợi ích quản trị duy nhất, toàn doanh nghiệp),
(iii) Giải pháp điểm cho GRC (liên quan đến quản trị toàn doanh nghiệp hoặc rủi ro toàn doanh nghiệp hoặc tuân thủ toàn doanh nghiệp nhưng không kết hợp với nhau).

Các giải pháp GRC tích hợp cố gắng thống nhất việc quản lý các khu vực này thay vì coi chúng như những thực thể riêng biệt. Một giải pháp tích hợp có thể quản lý một thư viện trung tâm về các biện pháp kiểm soát tuân thủ nhưng vẫn quản lý, giám sát và trình bày chúng theo mọi yếu tố quản trị. Ví dụ: theo cách tiếp cận theo miền cụ thể, có thể tạo ra ba phát hiện trở lên đối với một hoạt động bị hỏng. Giải pháp tích hợp nhận ra đây là một bước đột phá liên quan đến các yếu tố quản trị được ánh xạ.

Các nhà cung cấp GRC theo miền cụ thể hiểu được mối liên hệ mang tính chu kỳ giữa quản trị, rủi ro và tuân thủ trong một lĩnh vực quản trị cụ thể. Ví dụ: trong quá trình xử lý tài chính - rủi ro sẽ liên quan đến việc thiếu biện pháp kiểm soát (cần cập nhật cách quản trị) và/hoặc thiếu sự tuân thủ (hoặc chất lượng kém) của biện pháp kiểm soát hiện có. Mục tiêu ban đầu là tách GRC thành một thị trường riêng biệt đã khiến một số nhà cung cấp bối rối về việc thiếu chuyển động.

Người ta cho rằng, việc thiếu đào tạo chuyên sâu trong một lĩnh vực về mặt kiểm toán, cùng với sự thiếu tin tưởng vào kiểm toán nói chung sẽ gây ra rạn nứt trong môi trường doanh nghiệp. Tuy nhiên, có những nhà cung cấp trên thị trường, mặc dù vẫn duy trì hoạt động theo miền cụ thể nhưng đã bắt đầu tiếp thị sản phẩm của họ.

4. Kho dữ liệu GRC và kinh doanh thông minh:

Các nhà cung cấp GRC với khung dữ liệu tích hợp hiện có thể cung cấp các giải pháp kinh doanh thông minh và kho dữ liệu GRC được xây dựng tùy chỉnh. Điều này cho phép đối chiếu và phân tích dữ liệu có giá trị cao từ bất kỳ số lượng ứng dụng GRC hiện có nào.

Việc tổng hợp dữ liệu GRC bằng cách sử dụng phương pháp này mang lại lợi ích đáng kể trong việc xác định sớm rủi ro và cải thiện quy trình kinh doanh (và kiểm soát kinh doanh).

Các lợi ích khác của phương pháp này bao gồm (i) nó cho phép các ứng dụng hiện có, chuyên dụng và có giá trị cao tiếp tục mà không có tác động (ii) các tổ chức có thể quản lý quá trình chuyển đổi dễ dàng hơn sang phương pháp tiếp cận GRC tích hợp vì thay đổi ban đầu chỉ là thêm vào lớp báo cáo, và: (iii) nó cung cấp khả năng thời gian thực để so sánh và đối chiếu giá trị dữ liệu trên các hệ thống mà trước đây không có sơ đồ dữ liệu chung.

5. Nghiên cứu GRC:

Mỗi nguyên tắc cốt lõi - Quản trị, Quản lý rủi ro và Tuân thủ - bao gồm bốn thành phần cơ bản: (i) Chiến lược, (ii) Quy trình, (iii) Công nghệ, (iv) con người.

Khẩu vị rủi ro của tổ chức, các chính sách nội bộ và quy định bên ngoài của tổ chức tạo thành các quy tắc của GRC. Các nguyên tắc, thành phần và quy tắc của chúng hiện sẽ được hợp nhất theo cách tích hợp, tổng thể và toàn tổ chức (ba đặc điểm chính của GRC) - phù hợp với các hoạt động (kinh doanh) được quản lý và hỗ trợ thông qua GRC. Khi áp dụng cách tiếp cận này, các tổ chức mong muốn đạt được các mục tiêu: hành vi đúng đắn về mặt đạo đức và cải thiện hiệu quả cũng như hiệu quả của bất kỳ yếu tố nào có liên quan.