(استقرار یکپارچه GRC در بانک‌ها و موسسات مالی

نگاهی متفاوت در تحقق اهداف سازمانی)

نوش‌آفرین مومن واقفی مدیر ریسک و امنیت اطلاعات شرکت خدمات انفورماتیک
زهرا ذکائی کارشناس ارشد ریسک و امنیت اطلاعات شرکت خدمات انفورماتیک

امروزه سازمان‌ها خصوصا بانک‌ها و موسسات مالی از یک سو با افزایش ریسک‌های کسب و کار، عملیاتی، اعتباری، نقدینگی، انطباق و... مواجه هستند؛ و از سوی دیگر چگونگی راهبری(حاکمیت) و مدیریت فعالیت‌های سازمان همراستا با نیازهای ذی‌نفعان، مقررات، بازار و فرهنگ سازمان در کنار پیشرو بودن در بهره‌گیری از فناوری و کسب مزیت‌های رقابتی به عنوان چالش پیش روی در همه صنایع و از جمله صنعت بانکی می‌باشد. در مسیر کسب‌وکار امروز خصوصاً در حوزه صنعت بانکی با سه روند قابل توجه مواجه هستیم که لازم است در راهبری و مدیریت سازمان مورد توجه جدی قرار گیرد.

- افزایش هزینه‌ها در انطباق با قوانین و الزامات (هزینه‌های متغیر و غیر قابل پیش بینی)
- افزایش حجم، سرعت و پیچیدگی در کسب وکار (تغییرات در روند کسب‌وکار و خصوصا تغییرات در حوزه‌های جدید فناوری اطلاعات نظیر شبکه‌های اجتماعی، رایانش ابری، ابرداده ها، و ...)
- افزایش انتظارات ذی‌نفعان (انتظار بهره‌وری حداکثری همراه با شفافیت در چگونگی رسیدن به این سطح بهره وری)

در میان روندهای ذکر شده، مساله انطباق با الزامات خصوصا" در صنعت بانکی از اهمیت بالایی برخوردار است. در بحث ریسک‌های انطباق، بانک‌ها و موسسات مالی ملزم به انطباق با الزامات و قوانین مرجع از جمله قوانین ضدپول‌شویی (AML)، Basel، PCI و سایر استانداردهای بین المللی مرتبط در این حوزه و همچنین قوانین وضع شده توسط قانون‌گذار در داخل کشور در حوزه صنعت بانکی از جمله قانون پولی و بانکی کشور، قانون تنظیم بازار، قانون عملیات بانکی بدون ربا و ... هستند. با وجود آن که استقرار و نگهداشت این استانداردها و قوانین و نیز انطباق با آن‌ها هزینه‌های بسیار زیادی برای بانک‌ها و موسسات مالی به همراه دارد، اما عدم رعایت آن‌ها نیز منجر به جرایم سنگین و خدشه به اعتبار بانک‌ها و موسسات شده که خسارات جبران ناپذیری در حوزه کسب و کار محسوب می‌شود.

پس از بحران‌های مالی سال 2008 و شناسایی علل موثر بر آن، سازمان‌ها و صنایع مختلف با تغییر جدی رویکرد قانون‌گذاران مواجه شدند. پس از آن مدیریت هزینه‌های مربوط به انطباق بطور قابل توجهی افزایش یافته و این روزها به دغدغه اصلی صاحبان کسب وکار تبدیل شده است. قابل توجه است که به دنبال رکود اقتصادی سال 2008، مجموع جرائم سالیانه موسسات ارائه دهنده خدمات مالی در انگلیس، در طی 5 سال از 26 میلیون پوند به بیش از 474 میلیون پوند رسید. همچنین طبق گزارشی از موسسه اقتصاد لندن، مجموع جرائم 10 بانک برتر جهانی صرفاً در سال 2009 حدود 157 میلیارد پوند ارزیابی شده بود. بنابراین نادیده گرفتن سونامی انطباق با الزامات و عدم لحاظ تغییرات سریع قوانین که علت ریشه ای آن بدلیل رشد سریع فناوری‌ها در صنایع است، منجر به خسارات هنگفتی برای سازمان‌ها، بانک‌ها و موسسات مالی خواهد شد.

از طرف دیگر در فضای رقابتی کسب‌وکار امروزی، نیاز به تفکر آینده‌نگر در بحث ریسک به عنوان یک ضرورت جدی با توجه به تغییرات سریع فناوری‌ها و تاثیرات آن‌ها بر صنایع مختلف از جمله صنعت بانکی، مطرح است. مشابه با نوآوری‌های انجام شده در صنعت خودرو که سیستم جلوگیری از برخورد در خودروهای مدرن تعبیه می‌شود و به راننده قدرت تصمیم‌گیری و مدیریت بهینه ریسک را می‌دهد، صنعت بانکی نیز بیش از هر صنعت دیگر نیازمند استقرار فرایندها و سیستم‌های مرتبط جهت ایجاد امکان تصمیم‌گیری سریع، صحیح و بهینه است. این مهم جز با استقرار صحیح فرایندها و ساختارهای مرتبط با حاکمیت سازمانی، مدیریت بهینه ریسک و انطباق با الزامات ممکن نیست.

در بسیاری از بانک‌ها و موسسات مالی فعالیت‌های مرتبط با این سه حوزه‌ی مهم یعنی حاکمیت، مدیریت ریسک و انطباق توسط نقش‌های مختلف و در سطوح مختلف سازمانی ازجمله هیئت مدیره، مدیر عامل، مدیر ریسک، مدیر مالی، مدیر عملیات، ممیزان، واحد حقوقی و ... در قالب رویه‌ها و اقدامات مختلفی در سراسر سازمان انجام می‌شود. این فعالیت‌ها به تفکیک در ادامه تشریح شده‌اند:

حاکمیت (Governance): مجموعه‌ای از فرآیندهای تعریف و هدایت شده توسط هیأت مدیره و مدیران ارشد که در ساختار سازمان، نحوه هدایت و مدیریت سازمان و نحوه دستیابی سازمان به اهدافش انعکاس می‌یابد.

فعالیت‌هایی در حوزه حاکمیت (Governance) قرار می‌گیرد که این اطمینان را بوجود آورد که انتظارات ذی‌نفعان به درستی ارزیابی شده، استراتژی‌ها و برنامه‌های مناسب در نظر گرفته شده است و اطلاعات مدیریتی مهم و بحرانی ارائه شده به تیم ارشد اجرایی، به حد کافی شفاف، کامل و صحیح است و مکانیزم‌های کنترلی

برای اطمینان از اینکه استراتژی‌ها، راهبردها و دستورالعمل‌های ابلاغ شده بطور موثر و صحیح در همه لایه‌های سازمان اجرا می‌شوند، وجود دارد.

مدیریت ریسک: مدیریت ریسک کاربرد سیستماتیک سیاست‌های مدیریتی، رویه‌ها و فرایندهای مربوط به فعالیت‌های شناسایی، تحلیل، ارزیابی و کنترل ریسک در سازمان در سطوح مختلف استراتژیک تا عملیاتی می‌باشد. مدیریت ریسک مجموع فرآیندهایی است که برای شناسایی، تحلیل و پاسخگویی به ریسک‌هایی که تحقق اهداف سازمان را تحت تاثیر قرار می‌دهد استقرار می‌یابد. پاسخگویی به ریسک‌ها می تواند با پذیرش، اجتناب، کنترل یا انتقال ریسک‌ها صورت گیرد و ریسک‌ها می‌توانند انواع مختلفی از جمله ریسک‌های مالی، فناوری اطلاعات، امنیت، اعتباری، انطباق و ... باشند. با مدیریت صحیح ریسک، سازمان این قابلیت را پیدا می‌کند که ریسکی را بپذیرد که سازمان‌های دیگر نمی‌توانند بپذیرند و این برای سازمان مزیت رقابتی است. در بحث مدیریت ریسک توجه خاص مدیران ارشد به مشخص نمودن سطح ریسک مورد پذیرش سازمان و حصول اطمینان از اینکه راه‌کارهای مقابله با ریسک‌ها بصورت کافی لحاظ شده و اضافی غیر موثر، غیر ضروری و بی هدف نمی باشد امر مهمی است.

انطباق(Compliance): مجموع فرایندهای مدیریتی که در سطح سازمان مشخص می‌کند نیازها و الزامات قابل اعمال چیست،.وضعیت تطابق با الزامات و ریسک‌های مربوطه را شناسایی می‌کند، هزینه بالقوه عدم انطباق را در برابر هزینه قابل پیش‌بینی برای رسیدن به انطباق برآورد نموده و بر اساس این اطلاعات اولویت-دهی، اختصاص بودجه و تعیین فعالیت اصلاحی مورد نیاز را برای رسیدن به انطباق مشخص می‌کند. Compliance در صنعت بانکی انطباق با الزامات ابلاغ شده است که می‌تواند سیاست‌ها، فرآیندها، قوانین یا دستورالعمل‌های داخلی و خارجی صنعت بانکی (کشوری یا بین المللی)، استراتژی‌ها، تعهدات قراردادی، تعهدات و قول‌های داده شده به ذی‌نفعان و نظایر آن باشد. برخی از این الزامات در صنعت بانکی عبارتند از:

- قوانین تعیین شده توسط سازمان‌های قانون‌گذاری و نظارتی در کشور نظیر بانک مرکزی
- قوانین و الزامات جهانی مانند Basel و PCI DSS
- تعهدات قراردادی، تعهدات و وعده‌های داده شده به ذی‌نفعان
- الزامات شرکت‌ها وسازمان‌های بالاسری
- کنترل‌های مشخص شده از طرف حسابرسان
- کنترل‌های مشخص شده از طرف ممیزان داخلی و خارجی

تا اینجا سه حوزه حاکمیت، ریسک و انطباق بصورت مجزا مطرح شد. ترکیبی از مفاهیم مطرح شده در این حوزه ها، در مفهوم GRC به صورت همگرا در مباحث مدیریتی شناخته شده است. ایجاد رویکرد یکپارچه و متمرکز در حاکمیت و مدیریت فرایندهایی نظیر حاکمیت اطلاعات (Information Governance)، مدیریت ریسک، مدیریت کارآیی، مدیریت امنیت، انطباق، ممیزی و ... که به عنوان زیرمجموعه‌ای از فعالیت‌های در نظر گرفته شده در مفهوم GRC مطرح هستند، به عنوان مزیت رقابتی در سازمان‌ها مطرح می‌شود. سازمان‌ها تا وقتی کوچک هستند شاید با رویکردهای قدیمی بتوانند به حیات خود ادامه دهند؛ اما وقتی سازمان بزرگ می‌شود کنترل هماهنگ شده بین کلیه فعالیت‌های ذکر شده در این حوزه ها لازم است تا سازمان بتواند موثر و بهره ور ادامه مسیر دهد. بدین منظور در چند سال اخیر در سطح بین‌المللی استقرار مفهوم یکپارچه GRC به عنوان مزیت رقابتی مورد توجه قرار گرفته است.

GRC یکپارچه مانند چتری است که رویکرد سازمان را در حوزه فعالیت‌های این محورها بصورت هماهنگ پوشش می‌دهد. این رویکرد کمک می‌کند که اطلاعات در این حوزه‌ها به اشتراک گذاشته شوند و با تصمیم‌گیری‌های موثر و درست از موازی‌کاری‌های بسیار در سازمان و اتلاف منابع جلوگیری شود. فعالیت‌های ذکر شده در هر کدام از این حوزه‌ها برای حوزه‌های دیگر اطلاعات ارزشمند فراهم می‌کنند تا در نهایت خروجی بهینه که رسیدن به استقرار مفهوم GRC در سازمان است امکان پذیر گردد.

در بسیاری سازمان‌ها این فعالیت‌ها بصورت ایزوله و غیر هماهنگ دنبال می‌شوند، در حالی که ریسک‌های سازمان مرتبط با هم و در بسیاری حوزه‌ها مشترک هستند. در نتیجه برنامه‌ریزی و مدیریت سیلویی این فعالیت‌ها و فرایندها، ریسک‌های جدیدی نیز در کسب و کار سازمان بوجود می آید. این نکته حائز اهمیت است که هر سه این حوزه‌ها روی فرآیندها، اطلاعات، نیروی انسانی و فناوری های مشابه در سازمان تمرکز دارند و در صورت عدم هماهنگی و یکپارچگی در اجرای آن‌ها با استهلاک جدی منابع سازمان مواجه می‌شویم. برای نمونه، هزینه‌های پایش و ممیزی، علاوه بر نتایج نامرتبط و اتلاف وقت واحدهای ممیزی شده، جزء اولین مشکلات سازمان‌هایی است که رویکرد پراکنده و غیر مرتبط در GRC دارند و باعث می‌شود که مدیران ارشد سازمان در زمان مناسب به اطلاعات و گزارشات لازم دسترسی نداشته باشند. به عنوان مثال، در مدل غیر یکپارچه ، هر فرایند و سرویس داخلی و یا سرویس ارائه شده به مشتریان سازمان در برابر یک سری دستورالعمل‌ها، قوانین و استانداردها توسط چندین گروه و مسئول در سازمان بصورت غیر اثربخش بازرسی می‌شوند و خروجی این ممیزی‌ها که بایستی ورودی واحد مدیریت ریسک و انطباق در سازمان باشد بطور موثر در اختیار این واحد قرار نمی‌گیرد.

اجرای مدل یکپارچه GRC، نیازمند تعریف و ایجاد ارتباطات شفاف میان نقش‌ها و مسئولیت‌ها در این فرایندها می‌باشد. همچنین برای پیشبرد این فرایندهای در هم آمیخته لازم است از ابتدا قبل از هر اقدامی یک نقطه مرجع در ساختار و فرایندهای مدیریت سازمان تعیین و منابع اطلاعاتی مشترک ایجاد شوند. برای پیاده‌سازی یکپارچه مفهوم GRC، بررسی و مطالعه چارچوب‌ها و استانداردهای این حوزه ضروری است. با پیاده‌سازی صحیح GRC، انتظار می‌رود که تصمیمات جامع‌تر و مبتنی بر ریسک به منظور کاهش هزینه‌ها و افزایش بهره‌وری سازمان‌ها و بانک‌ها مورد توجه قرار گیرد.

در این مدل یکپارچه، نیازمندی‌ها و انتظارات ذی‌نفعان در بالاترین سطح از اطلاعات ورودی، شناسایی و ارزیابی شده و باید به سطوح مختلف در اهداف سازمانی تبدیل شوند. به منظور تحقق این اهداف و نیازمندی‌ها باید استراتژی‌ها، ساختار، افراد، مهارت ها، فرآیندها، فناوری و زیرساخت‌های مختلف به کار گرفته شوند. در ادامه باید اهداف کنترلی از جمله در حوزه مدیریت اطلاعات، مدیریت کارآیی، مدیریت ریسک و سایر بخش‌های عملیاتی سازمان تعیین شده و به منظور دستیابی به آن‌ها کنترل‌های عمومی و اختصاصی آن صنعت به کار گرفته شود. از طرف دیگر باید ریسک‌ها و فرصت‌های حاصل از عدم قطعیت در تحقق اهداف سازمانی نیز ارزیابی شوند. در تمام این مراحل باید بحث انطباق با الزامات داخلی و خارجی را به عنوان حدود اصلی تعیین راهکارها در نظر داشت تا عدم انطباقی که ریسک آن شناسایی نشده است، صورت نگیرد. در نهایت با انجام ممیزی‌های لازم، نتایج به صورت مستقیم و یا سلسه مراتبی در اختیار تمام واحدهای ذی‌ربط قرار می‌گیرد تا اقدامات اصلاحی لازم برای هرگونه عدم انطباق را مورد توجه قرار دهند. در صورت ایجاد این نگاه جامع و یکپارچه در اطمینان از تحقق اهداف سازمان ضمن پرداختن به عدم قطعیت‌ها در چارچوب الزامات و قوانین، می‌توان ادعا نمود که GRC به صورت یکپارچه در سازمان مستقر شده است.

از مزایای ایجاد چنین دید کلانی در سازمان‌ها و نهادینه‌سازی و استقرار مدل یکپارچه GRC می‌توان به مواردی نظیر کاهش فاصله میان فرآیندهای مدیریت ریسک و انطباق، کاهش فعالیت‌های تکراری و موازی و جلوگیری از فرسودگی منابع سازمانی، کاهش اثرات منفی مدیریت سیلویی و ناهماهنگ در سازمان، افزایش توانایی در ارائه اطلاعات مناسب برای هیات مدیره و مدیران ارشد، افزایش توانایی در جمع‌آوری سریع تر و موثرتر اطلاعات، کاهش هزینه‌ها و و ... اشاره نمود.

رهبران امروزی نیاز دارند تا به بالاترین سطح از ابزارها، فناوری‌ها و فرآیندها در سازمان دسترسی داشته باشند تا بتوانند سازمانی رقابتی را هدایت کنند. قطعاً هنوز هم می‌شود با فرم‌ها و برگه‌ها و در سیلوهای

پراکنده سازمان را مدیریت کرد، همانطور که یک بندباز ریسک‌های حرفه‌اش را مدیریت می کند. اما این نکته مشابه آن است که همچنان روش‌ها و رفتارهای مدیریتی دهه 1960 را بکار ببریم و این دیدگاه در دنیای امروز جز سردرگمی و از دست دادن فرصت ها، سازمان را به کجا خواهد رساند؟ قطعاً به سطحی از عملکرد و بهره‌وری که برای رقابت در کسب و کار امروز مورد نیاز است نخواهیم رسید.

در دنیای کسب و کار امروز سازمان‌هایی موفق هستند که مدیران آن‌ها بتوانند با سرعت و چابکی، تصمیم‌گیری‌های درست و موثر داشته باشند. متاسفانه رویکرد مدیریتی در اغلب سازمان‌ها و بانک‌ها در ایران این است که می‌خواهند با تکنیک‌ها، ابزارها، دانش، منابع و تفکر قدیمی ولی با چابکی مورد نیاز دنیای امروز حرکت کنند و در این حالت در هر لحظه سازمان را به سمت ریسک‌های جدی کسب و کار سوق می دهند.

سازمان‌های پیشرو، رهبرانی متعهد به ایجاد کسب‌وکارهای چابک، تاب‌آور، مطمئن و رقابتی دارند. دربین این رهبران، پیشروترین در تفکر مدیریتی، آنهایی هستند که دریافته‌اند استقرار رویکرد GRC بصورت یکپارچه در سازمان کلید موفقیت در کسب و کار امروزی است. چراکه این رویکرد منجر به سودآوری، قانون‌مندی، کارآمدی، و هماهنگی بیشتر سازمان شده و در نتیجه ضمن همراستایی کلیه فعالیت ها جهت تحقق اهداف سازمان با کسب آگاهی بالاتر، به شیوه‌ای مدرن، واکنشی سریعتر برای استفاده از فرصت‌ها نشان خواهند داد.