فاصله میان تصمیم و اجرا – *کاربرد چارچوب COBIT 5 در مدیریت ریسک سازمانی*

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

در هر سازمانی به دلیل عوامل داخلی و خارجی متعدد به منظور حفظ جایگاه رقابتی در بازار و رسیدن به اهداف، پیاده‌سازی فرایند مدیریت ریسک سازمانی[1] امری ضروری محسوب می‌شود. افزون بر این، به دلیل الزام در اعمال پیوسته و مداوم نظرات ذینفعان در مورد وضعیت ریسک در کل سازمان و نهادینه‌سازی فرهنگ ریسک، اجرایی نمودن این فرآیند اهمیت می‌یابد. فاصله میان تصمیم‌گیری در این زمینه و اجرایی نمودن آن از اصلی‌ترین مسائل در پیاده‌سازی مدیریت ریسک است. چراکه اکثر مدیران در انتخاب چارچوب و متدولوژی مناسب مدیریت ریسک مشکلات اساسی دارند.

هیئت مدیره، مدیران عامل، مدیران کسب‌وکار و فناوری اطلاعات و متخصصان ریسک در کل سازمان نیازمند راهنمایی هستند تا بتوانند فرآیند مدیریت ریسک را با توجه به شرایط داخلی و خارجی سازمان خود، به صورت گام به گام و موثر اجرا نمایند. بنابراین لازم است تا با استفاده از به‌روش‌ها[2] و چارچوب‌های رایج، این فاصله را به حداقل رساند و راهنمایی برای مدیران و سایر مخاطبان فراهم نمود. چارچوب COBIT می‌تواند ابزاری مناسب برای کاستن این فاصله باشد و به اجرایی نمودن فرآیند مدیریت ریسک کمک شایانی نماید. در شکل 1 تعدادی از پرسش‌های رایج در این مسیر به همراه پاسخ آن‌ها در این مقاله نشان داده شده است.

[1] Enterprise Risk Management (ERM)
[2] Best practice

COBIT چارچوبی برای توسعه، پیاده‌سازی، نظارت و بهبود حاکمیت[3] و مدیریت فناوری اطلاعات است. در نگاه نخست این چارچوب زبان مشترکی به منظور برقراری ارتباط میان مدیران کسب‌وکار و مدیران فناوری اطلاعات جهت رسیدن به درک مشترک از مقاصد و اهداف یکدیگر است؛ و در نگاه عمیق‌تر، در حقیقت این امکان را می‌دهد تا به اهداف عملیاتی نظام حاکمیتی و مدیریتی در سازمان دست یافت، یعنی:

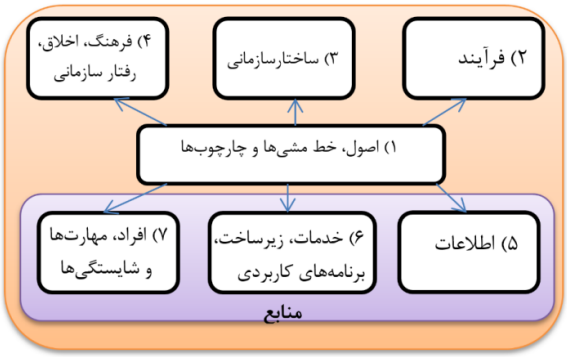
"خلق ارزش از طریق ایجاد حفظ تعادل میان تحقق منافع، مدیریت ریسک و بهینه‌سازی منابع"

جایگاه ریسک در این هدف می‌تواند نمایان‌گر این موضوع باشد که مدیریت ریسک در خلق ارزش برای هر سازمانی نقش به‌سزایی داشته و یک فعالیت مجزا نبوده و در تعامل با سایر فعالیت‌ها در حوزه تحقق منافع و بهینه‌سازی منابع، باعث خلق ارزش خواهد شد.

این چارچوب در حوزه مدیریت ریسک، راهنمای انتها به انتها و متدولوژی لازم برای ارزیابی و پاسخگویی به ریسک ارائه می‌دهد. COBIT 5 به ایجاد دید دقیق‌تر نسبت به ریسک‌های کنونی و آینده در سازمان و مشخص نمودن مسئولیت‌های مربوط به ریسک در کل سازمان کمک می‌نماید. همچنین نمونه‌های عملی از سناریوهای رایج را در حوزه فناوری اطلاعات در قالب پروفایل‌های ریسک معرفی نموده است.

چارچوب COBIT 5 تمامی 11 اصل مدیریت ریسک در استاندارد ISO 31000 را با 5 اصل و 7 توانمندساز[4] پوشش می‌دهد. همچنین تمامی جنبه‌های موجود در چارچوب و فرآیند مدیریت ریسک تعریف شده در استاندارد ISO 31000، در مدل فرآیندی COBIT 5 نیز وجود دارد.

همانطور که پیش از این گفته شد، COBIT5 هفت دسته توانمندساز را در بر می‌گیرد:



- اصول، خطمشی‌ها و چارچوب‌ها
- فرآیند
- ساختار سازمانی
- فرهنگ، رفتار سازمانی و اصول اخلاقی
- اطلاعات
- سرویس‌ها، زیرساخت و برنامه‌های کاربردی
- افراد، مهارت‌ها و شایستگی‌ها

تمامی این توانمندسازها در هر دو لایه حاکمیت و مدیریت ریسک کاربرد دارند. هدف اصلی از پیاده‌سازی چارچوب COBIT 5 استفاده از این 7 توانمندساز برای تصحیح، تسهیل و تسریع فرآیند مدیریت ریسک است که در ادامه به تفکیک بررسی می‌شوند.

[3] Governance
[4] Enabler

1. اصول، خطمشی‌ها و چارچوب‌ها

اصول ریسک بر سیستماتیک بودن، به موقع و نظام‌مند بودن فرآیند مدیریت ریسک تمرکز دارد تا بتواند نتایج قابل‌اطمینان و قابل مقایسه را ارائه دهد. برای تهیه راهنمایی بیشتر به منظور عملی نمودن اصول مدیریت ریسک، به مجموعه‌ای از خط مشی‌ها نیاز است. برای نمونه خط‌مشی مدیریت ریسک باید در برگیرنده حاکمیت ریسک، چارچوب مدیریت ریسک، نقش‌ها و مسئولیت‌ها و دامنه اجرای این فرآیند باشد. خط‌مشی‌های امنیت اطلاعات، تداوم کسب‌وکار، تقلب، تغییرات، کنترل داخلی و ... از نمونه‌های دیگری هستند که در اجرایی نمودن مدیریت ریسک نقش مهمی دارند.

2. فرآیندها

در چارچوب COBIT 5 در دامنه‌های حاکمیت و مدیریت به طور مجموع 37 فرآیند معرفی شده است. در این میان یک فرآیند در دامنه حاکمیت و دیگری در دامنه مدیریت، به صورت اختصاصی به موضوع مدیریت و کنترل ریسک می‌پردازد. برای پشتیبانی دو فرآیند کلیدی مذکور، 12 فرآیند دیگر ازجمله پایش و ارزیابی سیستم کنترل داخلی، پایش و ارزیابی انطباق با الزامات بیرونی، مدیریت استراتژی و ... معرفی شده است. تمامی این فرآیندها به همراه اقدامات، ورودی/خروجی‌ها و معیارهای سنجش عملکردشان به کارایی فرآیند مدیریت ریسک کمک می‌نماید.

3. ساختارهای سازمانی

در چارچوب COBIT 5 نقش‌های مختلفی تعریف شده است که 5 ساختار اصلی از میان آن‌ها موثرترین نقش‌ها در مدیریت ریسک محسوب می‌شوند. کمیته مدیریت ریسک سازمانی که متشکل از افرادی چون CEO[5]، CIO[6]، COO[7]، CISO[8]، CFO[9] و CRO[10] می‌شود موظف به جهت‌دهی مدیریت ریسک در کل سازمان بوده. این کمیته باید به صورت منظم به هیئت مدیره گزارش ارائه نماید و برای تسهیل فرآیند مدیریت ریسک اقداماتی از قبیل تفویض اختیار به مالکان ریسک را انجام دهد. گروه مدیریت ریسک سازمانی نیز از دیگر ساختارهای تعریف شده موثر است که شامل مدیران ریسک، تحلیل‌گران ریسک و سایر متخصصان در حوزه امنیت و کسب‌وکار هستند. این گروه موظف به اجرای مراحل مختلف شناسایی، تحلیل و برخورد با ریسک با همکاری مالکان فرآیندها است. واحدهای ممیزی و انطباق نیز از دیگر ساختارهایی هستند که در راستای پایش وضعیت کنترل‌های داخلی و انطباق با الزامات به واحد مدیریت ریسک اطلاعات و گزارش ارائه می‌نمایند.

4. فرهنگ، رفتار سازمانی و اصول اخلاقی

رفتارهای سازمانی نقش موثر در استقرار و نگهداشت فرهنگ مبتنی بر ریسک دارد که این رفتارها در سطوح مختلف از جمله سطح مدیریتی، متخصصان ریسک و عمومی طبقه‌بندی می‌شود. برای نمونه

---

5 Chief Executive Officer
6 Chief Information Officer
7 Chief Operating Officer
8 Chief Information Security Officer
9 Chief Financial Officer
10 Chief Risk Officer

کارمندان باید اهمیت کاهش ریسک در سازمان را درک کرده و بدانند که کنترل ریسک باعث بالا بردن ارزش نقش آن‌ها در سازمان می‌شود. از طرف دیگر متخصصان ریسک باید رابطه دوطرفه در طول انجام فرآیند مدیریت ریسک با ذینفعان داخلی داشته باشند و اطمینان حاصل نمایند که آگاهی‌رسانی در زمینه ریسک به صورت کامل انجام شده و دو طرف به درک مشترکی از اهداف یکدیگر رسیده‌اند. در سطح بالاتر نیز مدیران باید جهت انجام اقدامات لازم برای پاسخگویی به ریسک، سطوح اختیارات لازم را به کارمندان تفویض نمایند. تمام این رفتارهای سازمانی می‌توانند توسط قوانین داخلی، مکانیزم‌های پاداش و افزایش آگاهی‌رسانی، به صورت هدفمند کنترل شوند.

5. اطلاعات

انواع مستندات و گزارش‌های مربوط به ریسک مانند پروفایل ریسک، نقشه ریسک، شاخص‌های کلیدی ریسک، طرح تبادلی اطلاعات ریسک و ... از جمله اطلاعاتی هستند که باید به‌موقع، کامل و صحیح در اختیار افراد قرار گیرد؛ چراکه تصمیم‌گیری‌های مبتنی بر ریسک بر اساس این اطلاعات اتخاذ می‌گردند. برای نمونه پروفایل ریسک باید شامل ثبت اطلاعات کامل سناریوی ریسک، تحلیل آن، طرح‌های برخورد با ریسک، تاریخچه آن و فاکتورهای موثر در شناسایی و تحلیل ریسک (KRI) باشد. تمامی این اطلاعات زیر نظر CRO، توسط مالکان فرآیند، CIO، CISO و کارشناسان مربوط به آن‌ها تهیه و تولید می‌شوند.

6. سرویس‌ها، زیرساخت و برنامه‌های کاربردی

سرویس‌هایی مانند مدیریت برنامه‌ها و پروژه‌ها، مدیریت بحران و مدیریت رخداد می‌توانند نمونه‌هایی از سرویس‌های موثر در مدیریت ریسک محسوب شوند. پایگاه دانش و منابع اطلاعاتی به‌روز نیز می‌توانند زیرساخت مناسبی برای اجرایی نمودن این فرآیند باشند. همچنین ابزارهای GRC[11]، ابزار مناسب تحلیل ریسک، ابزار مدیریت تداوم کسب‌وکار و ابزارهای گزارش‌دهی و تبادل اطلاعات، در کارایی و اثربخشی فرآیند مدیریت ریسک نقش موثری دارند.

7. افراد، مهارت‌ها و شایستگی

مهارت‌های مدیریتی، قدرت تحلیل ریسک، روابط اجتماعی مناسب جهت تبادل اطلاعات و رسیدن به درک مشترک در رابطه با ریسک‌ها، تاثیرگذاری بیشتر بر طرف مقابل و مهارت‌های فنی کافی از ملزومات اجرای فرآیند مدیریت ریسک در سازمان هستند. نقش‌های مختلف در این فرآیند باید دارای سطح کافی از مهارت‌های ذکرشده باشند تا انتظار کارایی و اثربخشی بیشتر مدیریت ریسک را داشت.

ناگفته نماند که قابلیت‌های هر توانمندساز در تعامل با سایر توانمندسازها و در کنار آن‌ها، تکامل می‌یابد. بنابراین باید برنامه‌ای جهت استقرار و اجرای تمامی آن‌ها به صورت موازی و گام به گام در سازمان، در نظر گرفته شود. با این حال برداشتن هر گام صحیح در این مسیر، چه بسا کوچک، می‌تواند در طول زمان فاصله میان درک اهمیت مدیریت ریسک و اجرایی نمودن آن در سازمان را کاهش داده و موجب خلق ارزش گردد.

11 Governance, Risk and Compliance

توانمندسازها در کوبیت نقش اهرم‌های کنترلی را دارند که مدیریت ارشد اجرایی در پنل کنترل سازمان در اختیار دارد. ضعف در هر یک از این توانمندسازها در سازمان باعث عدم قطعیت در تحقق اهداف سازمانی و به تعبیر دیگر ریسک سازمانی می‌گردد. بدیهی است اگر مدیران ارشد سازمان بستر و زیرساخت مناسبی بر اساس توانمندسازهای مطرح شده در سازمان فراهم نمایند، به طور ضمنی، ریسک‌های سازمان نیز کاهش یافته و مدیریت می شوند و اثربخشی حاصل از به‌کارگیری فرآیند مدیریت ریسک سازمانی و دستاوردهای اجرای آن در سازمان مورد توجه قرار خواهد گرفت.

متاسفانه در اغلب سازمان‌ها، بین سیاست‌ها و روش‌های مدیریتی و بهره‌گیری از چارچوب‌ها و استانداردها در عمل رویکرد مناسب اجرایی لحاظ نشده است و این امر باعث کاهش اثربخشی تصمیمات مدیریتی و نیز عدم موفقیت در استقرار سیستم‌ها و استانداردهای مدیریتی می‌گردد. برطرف کردن این شکاف در تصمیم و اجرا جز با نهادینه‌سازی دانش مدیریت مبتنی بر ریسک و تغییر نگرش در میان مدیران ارشد سازمان ممکن نیست. مدیریت اثربخش در هر حوزه‌ای و از جمله حوزه مدیریت ریسک سازمانی نیازمند تحول جدی نگرش‌های مدیریتی در سازمان بر اساس الگوهای موفق است. در اولین گام باید این دانش در مدیران ایجاد شود که مدیریت ریسک باعث سرعت و دقت در تصمیمات سازمانی می شود.

منابع

COBIT for risk-ISACA
ISO 31000:2009 – Risk Management