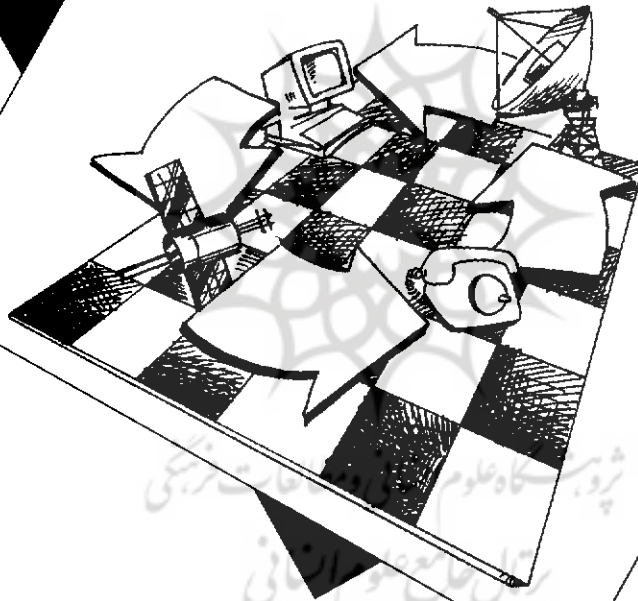


راهبری فناوری اطلاعات در سازمان

آیدا حقیقی

Haghighi aida@gmail.com



چکیده

مدیران ارشد سازمان تأثیر قابل توجهی را که فناوری اطلاعات می‌تواند روی موفقیت سازمان داشته باشد، درک کرده‌اند. مدیران امیدوارند که درک و شناخت خود را از روشهای مبتنی بر فناوری اطلاعات که به کار برده شده است و نیز احتمال به کار بردن موفقیت‌آمیز آن را برای کسب مزیت رقابتی افزایش دهند.

بنابراین هیئت مدیره و مدیران اجرایی نیاز دارند که مدیریت و نظارت روی IT را افزایش دهند، برای اینکه اطمینان یابند که IT سازمان، استراتژیها و هدفهای سازمان را دنبال می‌کند و برآورده می‌سازد. از اینرو راهبری فناوری اطلاعات (IT Governance = ITG) به عنوان بخش جدایی‌ناپذیر مدیریت سازمان در نظر گرفته می‌شود. این مقاله با هدف معرفی راهبری فناوری اطلاعات و دلایل اهمیت آن و آشنایی با چگونگی پیاده‌سازی آن تهیه شده است تا مدیران را در جهت به کارگیری راهبری فناوری اطلاعات در سازمانها یاری کند.

راهبری فناوری اطلاعات عبارتی است که برای توصیف اینکه چطور افراد برای مدیریت یک نهاد، فناوری اطلاعات را در سرپرستی، نظارت، کنترل و رهبری مورد توجه قرار می‌دهند، به کار برده می‌شود.

در این مقاله سعی بر آن شده است که رهبری فناوری اطلاعات معرفی شود و دلایل نیاز به آن در سازمانها برای نظارت و سرپرستی فعالیتهای مرتبط با فناوری اطلاعات شرح داده شود.

سازمانها نیاز دارند که به سمت فرایندگرایی حرکت کنند و آنچه که به سازمانها در این راه کمک کرده، آنها را پشتیبانی می‌کند فناوری اطلاعات است. فناوری اطلاعات ستون فقرات مهمی برای فرایندها است. برای اینکه فناوری اطلاعات در سازمانها وارد شود و همینطور برای ایجاد یکپارچگی و بهبود در سازمانها لازم است برای کنترل و نظارت روی آن، راهبری فناوری اطلاعات پیاده‌سازی شود.

وضعیت ساختار IT در سازمانهای سده بیست و یکم

در سده بیست و یکم، سازمانها به سمت فرایندگرایی حرکت می‌کنند و توجه مدیران روی فرایندهای شرکت متمرکز شده است، در نتیجه فناوری اطلاعات، یک عامل توانمند برای این اطلاعات است. سازمانها برای افزایش یکپارچگی و استاندارد کردن فرایندها، افزایش سرعت روند جهانی شدن، بازسازی و تغییرات مکرر تجارت به فناوری اطلاعات نیازمندند. فناوری اطلاعات به فرایندگرا بودن سازمان کمک می‌کند. در این مسیر چهار فرایند و شش اصل مربوط به فناوری اطلاعات، سازمان را پشتیبانی می‌کنند. چندین سال پیش، مدیران اجرایی IT آروی سه فرایند اصلی، شامل برنامه‌ریزی، انتقال و عملیات، برای دستیابی به هماهنگی IT با تجارت متمرکز شدند اما تحلیل و آنالیز امروزه، چهار فرایند اصلی را برای سازمانهای IT مشخص کرده است که عبارتند از:

- توانایی ایجاد تغییرات سازمانی؛
قابلیتهای متداول فناوری اطلاعات،
تکنولوژیهای وب، بسته‌های نرم‌افزاری و ...

- ارائه راه‌حل برای الزامات استراتژیک؛
سفارشی کردن، درون سپاری، برون‌سپاری و ...

- اطمینان یافتن از خدمات زیر ساختی
که از نظر هزینه‌ای کارآمد می‌باشند؛ وجود

پایگاه‌های داده‌ای متمرکز و ...،

- مدیریت سرمایه‌های فکری؛ به
کارگیری دانشهای تخصصی.
شش اصل فناوری اطلاعات که برای
عملکرد مؤثر چهار فرایند یاد شده مهم
هستند عبارتند از:

- **طراحی معماری:** معماری IT مشخص
می‌کند که زیر ساخت چگونه ایجاد و
نگهداری خواهد شد.

- **مدیریت برنامه:** شامل مدیریت
راه‌حلهای کاربردی پویا و راه‌حلهایی که
باعث افزایش هم افزایی می‌شود.

- **مدیریت قراردادهای و منابع:** واحدهای
فناوری اطلاعات مسئول مذاکره و مدیریت
قراردادهای بسته شده با واحدهای تجاری
داخلی و قراردادهای خارجی هستند.

- **تحلیل و طراحی فرایند:** شرکتها برای
فرایندگرا شدن به مکانیزمهایی برای
شناسایی، تحلیل، ذخیره و ارتباط برقرار
کردن فرایندهای تجاری نیاز دارند.

- **مدیریت تغییر:** برای بهبود مستمر
فرایندها و پیاده‌سازی راه‌حلهای نرم‌افزاری
جدید.

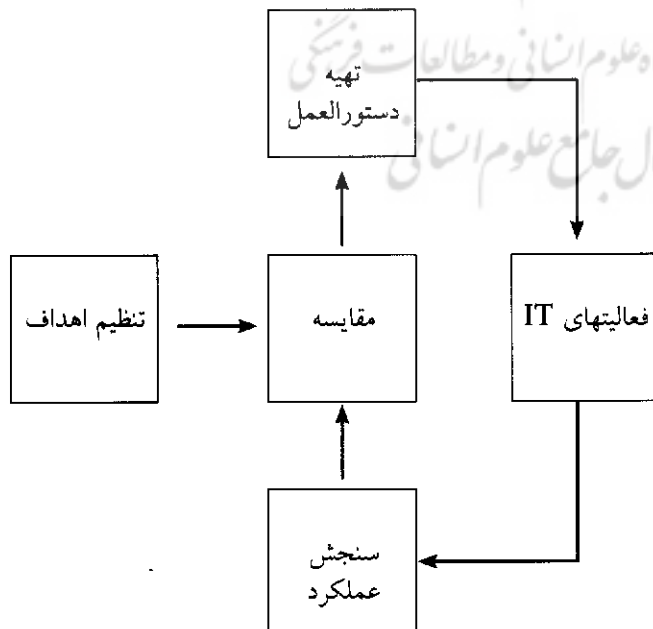
- **توسعه منابع انسانی ماهر در فناوری
اطلاعات:** اطمینان یافتن از وجود
متخصصین فناوری اطلاعات با مهارتهای
مورد نیاز.

با توجه به ساختارهای پیچیده‌ای که
سازمانهای IT در به کارگیری فناوری
اطلاعات داشتند و نیز با توجه به نیاز آنها
برای به کارگیری استانداردهای جدید یعنی
استفاده از استانداردهایی جامع و پیوسته
برای فرایندگرا تر بودن سازمانها و همچنین
برای ایجاد هماهنگی و یکپارچگی بین
فرایندها و هم با توجه به نیاز به تخصصهای
سیستمهای اطلاعاتی و آموزش کارکنان،
نیاز به کنترل و نظارت اقدامات مربوط به
فناوری اطلاعات در سازمان احساس
می‌شد که به این منظور راهبری فناوری
اطلاعات معرفی شد.

راهبری فناوری اطلاعات چیست؟

راهبری فناوری اطلاعات (ITG)
مسئولیت هیئت مدیره اجرایی است.
راهبری فناوری اطلاعات یک بخش
جدایی‌ناپذیر مدیریت سازمان، شامل
راهبری و سازماندهی ساختارها و فرایندها
است؛ تا اطمینان حاصل شود که فناوری
اطلاعات سازمان، هدفها و استراتژی
سازمان را پشتیبانی می‌کند و توسعه
می‌دهد یا نه؟

تجربه‌های منفی مدیران از به کارگیری
این فناوری، شامل از بین رفتن اعتبار، تأخیر
در ارائه خدمات، عدم کارایی فرایندهای



شکل ۱: تعاملات هدفها و فعالیتهای IT (منبع شماره ۲)

اصولی فناوری اطلاعات سازمان و شکست اولیه آن، سازمان را برآن داشت که راهبری فناوری اطلاعات را به کار گیرند و بنا به این دلایل بود که راهبری فناوری اطلاعات اهمیت پیدا کرد و در سازمانها به کار گرفته شد.

راهبری فناوری اطلاعات برای اطمینان یافتن از دستیابی عملکرد فناوری اطلاعات به هدفهای زیر به کار گرفته می‌شود:

- هماهنگی فناوری اطلاعات با سازمان و تحقق مزایای وعده داده شده.
- به کارگیری فناوری اطلاعات برای توانمند کردن سازمان برای استفاده از فرصتها و حداکثر کردن مزایا.
- به کارگیری منابع مربوط به فناوری اطلاعات به گونه‌ای مؤثر.
- مدیریت مناسب ریسکهای مرتبط با فناوری اطلاعات.

راهبری فناوری اطلاعات معمولاً در لایه‌های مختلف، با گزارش‌دهی سرپرستان به مدیران و مدیران به مدیران اجرایی و آنها نیز به هیئت مدیره، انحراف از هدفها را مشخص می‌کنند و در جهت رفع آنها اقدامات و دستورکارهای لازم با تأیید مدیریت انجام می‌شود. تعاملات هدفها و فعالیتهای مرتبط با فناوری اطلاعات از

دید راهبری آنها در شکل ۱ نمایش داده شده است و می‌توانند در لایه‌های مختلف در سراسر سازمان به کار برده شوند.

چرا راهبری فناوری اطلاعات اهمیت دارد؟

علت اینکه راهبری فناوری اطلاعات بسیار اهمیت دارد این است که اغلب، انتظارات با آنچه که در واقعیت رخ می‌دهد، منطبق نیستند، در نتیجه مدیریت روی موارد زیر باید انجام شود:

- به کارگیری امکانات فناوری اطلاعات با کیفیت مناسب و به موقع و با بودجه مناسب.
- کنترل و استفاده از فناوری اطلاعات برای بازگشت ارزشهای تجاری.
- به کارگیری فناوری اطلاعات برای افزایش بهره‌وری و کارایی در حالی که ریسکهای فناوری اطلاعات هم کنترل می‌شوند.

چه کسانی در سازمان درگیر راهبری فناوری اطلاعات هستند؟

مسئولیت راهبری فناوری اطلاعات در سازمانها در درجه اول به عهده مدیران اجرایی و هیأت مدیره است و سپس مدیران عامل باید ساختارهای سازمانی

را برای پشتیبانی از اجرا و پیاده‌سازی استراتژی فناوری اطلاعات، تهیه کنند و مدیران اطلاعات برای ایجاد پلی بین فناوری اطلاعات و تجارت و نیز کمیته‌های راهبری فناوری اطلاعات و سایر کمیته‌های مشابه نیز درگیر هستند.

راهبری فناوری اطلاعات چه فعالیتهایی را پوشش می‌دهد؟

راهبری روی پنج سطح اصلی در سازمان تمرکز دارد که در شکل ۲ نشان داده شده است.

دو مورد از پنج سطح اصلی خروجی هستند که عبارتند از:

- انتقال ارزش: تمرکز روی بهینه‌سازی مخارج و ایجاد ارزش فناوری اطلاعات. منظور از انتقال ارزش اعتباری است که سازمان از به کارگیری فناوری اطلاعات کسب می‌کند.

- مدیریت ریسک: حفاظت از دارایی‌های مربوط به فناوری اطلاعات، بهبود اشتباهها و عدم انطباقها و پیوستگی و دوام عملیات و استمرار آنها.

سه مورد از پنج سطح اصلی، محرکهایی هستند که برای دستیابی به خروجیها لازمند که عبارتند از:

- تعیین و تنظیم استراتژی: با تمرکز روی هماهنگی استراتژی فناوری اطلاعات با راه‌حلهای تجاری.

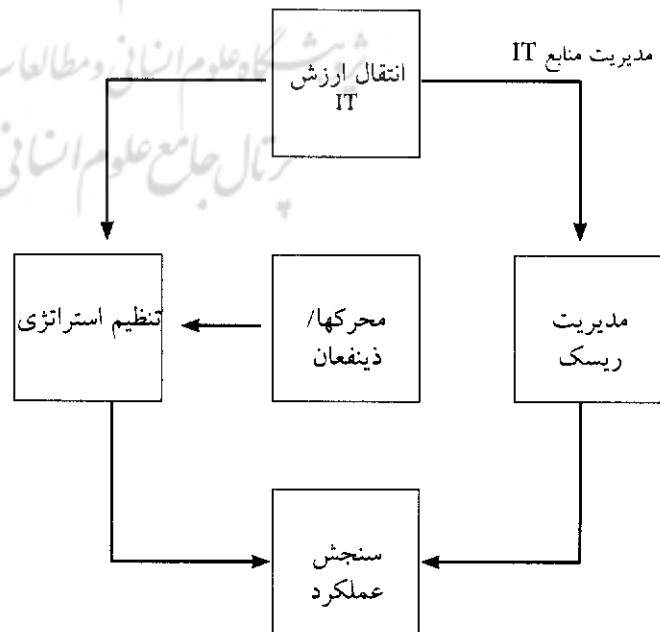
- مدیریت منابع: بهبود دانش و زیرساختهای فناوری.

- ارزیابی و سنجش عملکرد: پیگیری خروجی پروژه (آنچه که تحویل داده می‌شود) و نظارت بر خدمات فناوری اطلاعات.

هیچ یک از چهار عامل اول، بدون وجود عامل ارزیابی و سنجش عملکرد نمی‌تواند به خوبی مدیریت شود.

پس از معرفی راهبری فناوری اطلاعات به سازمان، برای شروع اجرا و پیاده‌سازی راهبری فناوری اطلاعات، برای اینکه مشخص شود که سازمان در چه وضعیتی قرار دارد، استفاده از چک لیستهای مربوطه که پنج عامل یاد شده را در نظر می‌گیرد، روش مؤثری است.

برای اجرای کامل راهبری فناوری اطلاعات، استانداردهای مختلفی مثل:



شکل ۲. سطوح تمرکز ITG

(COBIT= Control Objective For Information & Related Technology) Turnbull و Cadbury, میان آنها، COBIT که توسط مؤسسه IT Governance تهیه شده است و به گونه بین المللی به عنوان یک مدل خوب برای کنترل اطلاعات، IT و ریسکهای مرتبط پذیرفته شده و برای پیاده سازی و ممیزی راهبری فناوری اطلاعات انتخاب شده است.

چارچوب COBIT

در سالهای اخیر بدیهی است که به یک چارچوب مرجع برای کنترل و امنیت در خبرهای فناوری اطلاعات نیاز است، همچنین نیاز بیشتری وجود دارد برای اینکه کاربران از ارائه خدمات فناوری اطلاعات، از راه ممیزی خدمات ارائه شده توسط گروه های داخلی و شخص ثالث، اطمینان حاصل کنند. همچنین برای دستیابی به مزیت رقابتی و کارآمد بودن از نظر هزینه با تکیه بر تکنولوژی، برای دستیابی به موفقیت در مدیریت سازمان و مدیریت فناوری اطلاعات و نظارت و ارزیابی بر عملکرد سازمان، برای برآورده کردن هدفها و الزامات تجاری در جهت پاسخگویی به نیازها، از چارچوب مرجع به نام COBIT استفاده می شود. تعاریفی که در چارچوب COBIT باید در نظر گرفته شود، عبارتند از:

- کنترل: خط مشی ها، روشهای اجرایی، فعالیتها و ساختارهای سازمانی که طراحی شده اند، برای ایجاد اطمینان از اینکه هدفهای تجاری برآورده خواهند شد و از حوادث نامطلوب جلوگیری کرده، یا کاهش و یا اصلاح خواهند شد.

- هدفهای کنترل فناوری اطلاعات: بیان نتایج یا طرح مطلوبی که از راه پیاده سازی روشهای اجرایی، کنترل یک فعالیت خاص، به دست خواهد آمد.

- راهبری فناوری اطلاعات: ایجاد ارتباطات و فرایندها برای هدایت و کنترل سازمان برای دستیابی به هدفهای سازمان برای ایجاد ارزش افزوده یا ایجاد تعادل و توازن ریسکهای حاصل از به کارگیری فناوری اطلاعات و فرایندهای آن.

هدف اصلی پروژه COBIT، توسعه خط مشیهای واضح و مدلهای مناسب برای امنیت و کنترل فناوری اطلاعات، برای



راهبری فناوری اطلاعات یک بخش جدایی ناپذیر مدیریت سازمان، شامل راهبری و سازماندهی ساختارها و فرایندها است.

چارچوب COBIT در سه سطح در نظر گرفته شده است: در سطح پایین، فعالیتها و وظایفی وجود دارند که برای دستیابی به نتایج قابل اندازه گیری مورد نیاز هستند. فعالیتها یک چرخه عمر دارند در حالی که وظایف بیشتر گسسته هستند.

سپس فرایندها در یک لایه بالاتر به عنوان مجموعه ای از فعالیتها و وظایف تعریف شده اند. در بالاترین سطح که بیشتر مورد توجه COBIT است، فرایندها در یک حوزه جمع آوری شده اند.

بنابراین چارچوب COBIT از نظر مفهومی می تواند از سه بعد در نظر گرفته شود: ۱- معیارهای اطلاعات؛ ۲- منابع فناوری اطلاعات؛ ۳- فرایندهای مربوط به فناوری اطلاعات. این سه بعد در مکعب COBIT به صورت شکل ۴ نشان داده شده است.

چهار حوزه گسترده ای که در COBIT در نظر گرفته شده اند عبارتند از: برنامه ریزی و سازماندهی، ایجاد و پیاده سازی، تحویل و پشتیبانی، نظارت.

بدین گونه که در حوزه برنامه ریزی و سازماندهی، استراتژی و تاکتیکها و نگرانیهای مربوط به شناسایی IT را می توان برای دستیابی به هدفهای تجاری به بهترین شکل جمع آوری کرد. در حوزه ایجاد و پیاده سازی برای شناخت و ایجاد استراتژی فناوری اطلاعات، امکانات باید شناسایی، توسعه یافته و یا ایجاد شوند. در حوزه تحویل و پشتیبانی، تحویل به موقع و ارائه خدمات مورد نیاز، مورد توجه قرار می گیرد و فرایندهای پشتیبانی مورد نیاز باید راه اندازی شوند. در حوزه نظارت، تمامی فرایندهای IT لازم است که به طور منظم از نظر کیفیت و مطابقت با الزامات کنترل، مورد ارزیابی قرار گیرند.

چگونه COBIT را به سازمان معرفی می کنید؟

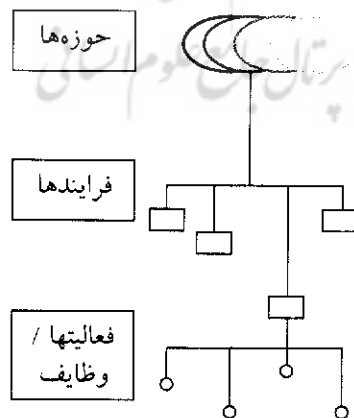
COBIT معمولاً فعالیتهای تأیید شده ای را برای مدیریت و کنترل منابع اطلاعاتی و فناوری اطلاعات، ایجاد می کند. COBIT برای سه گروه طراحی شده است:

- برای مدیران: COBIT کمک می کند که تعادل را بین ریسکهای سرمایه گذاری و کنترل آنها در اغلب محیطهای غیر قابل

تأیید جهانی توسط سازمانهای تخصصی، دولتی و تجاری است. هدف COBIT برآورده کردن هدفهای تجاری است.

اصول چارچوب COBIT

COBIT مدلی است برای راهبری فناوری اطلاعات. مفهوم اساسی چارچوب COBIT آن است که کنترل روی فناوری اطلاعات از راه توجه به اینکه اطلاعات باید هدفها یا الزامات تجاری را پشتیبانی کند، ایجاد می شود.



شکل ۳: سطوح چارچوب COBIT (منبع ۳)

پیش‌بینی برقرار می‌کند.

- برای کاربران: COBIT کمک می‌کند که اطمینان یافتن از امنیت و کنترل خدمات IT ارائه شده، توسط گروه‌های داخلی و شخص ثالث.

- برای ممیزان: COBIT کمک می‌کند که مستند کردن و ارائه نظرات و عقایدشان در مورد کنترل‌های داخلی فناوری اطلاعات برای اطلاع و آگاهی مدیران، مؤثر باشد. در نتیجه برای معرفی COBIT در یک سازمان باید آن را به سه گروه افراد یاد شده در سازمان معرفی کنیم و آنها را از فواید COBIT آگاه سازیم.

برای پذیرش COBIT چه کسانی باید تحت تاثیر قرار گیرند؟

COBIT در اصل، یک چارچوب برای مدیران فناوری اطلاعات و ارتباطات یک سازمان است. بنابراین، مدیران به ویژه ایجادکنندگان خط مشی فناوری اطلاعات نقش مهمی را در پذیرش و ایجاد COBIT

در سازمان ایفا می‌کنند.

علاوه بر مدیران عامل، مدیران اطلاعات و کمیته‌های راهبردی، افراد کلیدی دیگری شامل مدیران اجرایی، صاحبان فرایندهای تجاری و مدیران اصلی نیز باید COBIT را بپذیرند.

چرا یک سازمان باید COBIT را بپذیرد؟ دلایلی که مدیران و تصمیم‌گیرندگان اصلی را به پذیرش COBIT تشویق می‌کند، عبارتند از:

۱. به دلیل مشکلات تجربه شده توسط سازمانها.
۲. نیاز مدیران به نظارت بر منابع سازمان.
۳. با کنترل منابع فناوری اطلاعات، هزینه کل ارائه خدمات آن ممکن است کاهش یابد.
۴. COBIT ترس و نگرانی و عدم اطمینان مدیران را نسبت به برآورده نشدن هدفهای تجاری کاهش خواهد داد.
۵. اطمینان یافتن از اینکه سازمان مطابق با

قوانین کاربردی و قابل اجرا است.

۶. ایجاد و برقراری ارتباطات بهبود یافته بین مدیران، کاربران و ممیزان با به کارگیری COBIT.

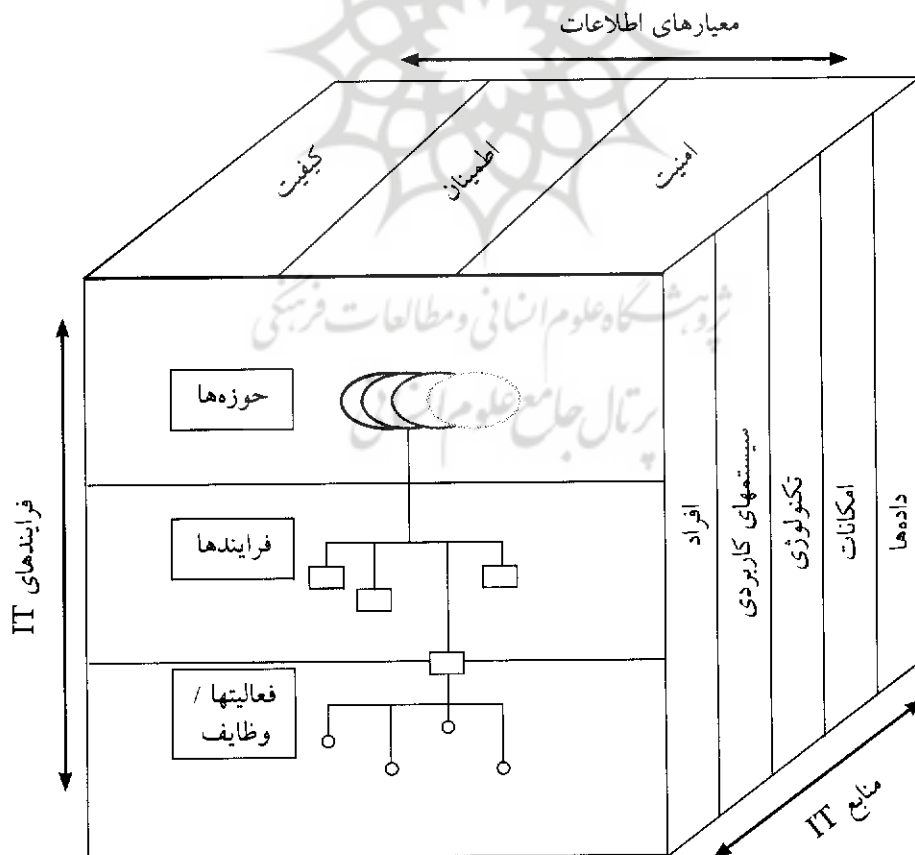
۷. COBIT چارچوبی را برای شناسایی ریسکهای مرتبط با فناوری اطلاعات و ارزیابی و کنترل آنها ارائه می‌نماید.

۸. برخی سازمانها با به کارگیری COBIT، ممیزیهای یکپارچه و سراسری، خود را بهبود داده‌اند منبع شماره ۴.

حوزه و محدودیتهای COBIT چه هستند؟

برای اینکه COBIT به طور موفق اجرا شود، هر کسی باید بداند که COBIT چیست، برای چه به کار برده می‌شود و چه کاری می‌تواند انجام دهد؟ در این زمینه چندین نکته وجود دارد:

۱. COBIT روشی جدید برای تفکر است.
۲. COBIT چارچوبی است که باید متناسب با سازمان باشد.



شکل ۴: مکعب COBIT

۳. COBIT باید به عنوان یک منبع مدیریت، کنترل و ممیزی به کار برده شود.
 ۴. کارکنان اصلی باید برای دستیابی به یک پیاده‌سازی موفق، از COBIT آگاه باشند و آموزش ببینند.

چگونه COBIT را در سازمانتان اجرا کنید؟

پذیرش موفق COBIT به آموزش احتیاج دارد. پس از معرفی COBIT در سازمان، برای اجرای آن، ابتدا مسئولان اصلی باید آشنایی کامل نسبت به آن داشته باشند و آن را بپذیرند. پس از تأیید، لازم است که COBIT در نظامنامه، خط مشی و روشهای اجرایی به عنوان یک مدل مناسب مشخص شود و سپس از راه فرمهای نام برده شده در زیر، ارزیابی ریسک و برنامه‌ریزی ممیزی انجام گیرد. فرمها عبارتند از:

- فرم فعالیتهای پیش ممیزی: شناسایی اینکه آیا فعالیتهای ممیزی مرتبط با فرایند فناوری اطلاعات در حوزه پیش از ممیزی قرار می‌گیرد؟ این فرم توسط تیم ممیزی تکمیل می‌شود.

- فرم خلاصه گزارش بخش: شناسایی فرایندهای مربوط به فناوری اطلاعات که با اهمیت بیشتری مورد توجه قرار گیرند. این فرم توسط مدیران بخشها تکمیل می‌شود.

- فرم ارزیابی ریسک: کمک به تیم ممیزی در شناسایی فرایندهای مربوط به فناوری اطلاعات در جایی که ریسک وجود خواهد داشت. این فرم توسط تیم ممیزی یا مدیران یا به طور مشترک تکمیل می‌شود.

- فرم گروه‌های مسئول: برای شناسایی کسانی که هر فرایند مربوط به فناوری اطلاعات را انجام می‌دهند و کسانی که مسئول نهایی هر فرایند هستند. این فرم توسط تیم ممیزی با مشارکت مدیران بخش ممیزی شونده تکمیل می‌شود.

انجام ممیزی با استفاده از COBIT
 پس از برنامه‌ریزی، فرایند ممیزی براساس گامهای زیر انجام می‌گیرد:

۱. تعیین نوع ممیزی: نوع ممیزی مورد

مسئولیت راهبری فناوری اطلاعات در درجه اول به عهده هیئت مدیره است و سپس مدیران عامل و مدیران اطلاعات در این فعالیت نقش دارند.



۴. انجام ممیزی: ممیزی مطابق راهنمای ممیزی COBIT انجام می‌گیرد.

۵. نوشتن گزارش ممیزی: نوشتن نتایج با تمرکز روی هدفهایی که برآورده شده‌اند و هدفهایی که برآورده نشده‌اند (منبع شماره ۴).

نتیجه‌گیری

فناوری اطلاعات یک بخش جدایی ناپذیر از تجارت است و راهبری آن یک بخش جدایی ناپذیر از مدیریت سازمان است. در راهبری فناوری اطلاعات نقشها و مسئولیتها باید به طور واضح مشخص شوند و کمیته‌هایی مثل کمیته راهبری (در سطح اجرایی) و کمیته استراتژی (در سطح مدیریتی) تشکیل شده، سپس یک طرح برای اجرا و پیاده‌سازی راهبری، مثل COBIT لازم است. برای انجام راهبری کارهای زیر باید انجام گیرد:

- تهیه چارچوب سازمانی مدیران
- هماهنگی استراتژی فناوری اطلاعات با هدفهای تجاری،
- شناخت ریسکها،
- تعریف و شناسایی سطوح فرایند،
- شناسایی عدم انطباقها و مغایرتها،
- توسعه استراتژیهای بهبود،
- ارزیابی نتایج.

این کارها تا بهبود کامل تکرار می‌شود. □

منابع:

1. Brown, Carol and Jeanne W. Ross, 1999, The IT organization of the 21st century: Moving to a Process-Based orientation.
2. Board Briefing on IT Governance IT Governance Institute - 2003
3. COBIT 3rd Edition- Audit Guidelines, IT Governance Institute - July 2000
4. COBIT 3rd Edition- Implementation Tool Set, IT Governance Institute - July 2000

• آیدا حقیقی: کارشناس صنایع و کارشناس ارشد تحلیل سیستم‌ها در منطقه ۳ عملیات انتقال گاز شرکت ملی گاز ایران

نیاز برای بخشی که باید ممیزی شود را انتخاب کنید. انواع ممیزیهایی که ممکن است انجام شوند، عبارتند از: مالی، عملکرد، مطلوبیت و ...

۲. تعیین هدفهای ممیزی: بعد از انتخاب نوع ممیزی، زمان آن است که هدفهای کنترل COBIT برای دستیابی به بینش و آگاهی بیشتر فرایندهای مربوط به فناوری اطلاعات انتخاب شده برای این ممیزی به کار گرفته شود.

۳. توسعه و برنامه‌ریزی ممیزی: در صورتی که یک برنامه ممیزی وجود داشته باشد، آن برنامه با راهنمای ممیزی COBIT مقایسه می‌شود و اگر برنامه ممیزی وجود نداشته باشد، از راه راهنمای ممیزی COBIT یک برنامه ممیزی تهیه می‌شود. در این گام فعالیتهای زیر انجام می‌شود: مقایسه هدفهای ممیزی با هدفهای کنترل COBIT. مقایسه برنامه ممیزی با برنامه ممیزی COBIT، افزودن فعالیتهای ممیزی پیشنهاد شده از راه نظامنامه‌ها و راهنماهای سازمانی و قانونی.