نتایج بکارگیری مدل مرجع COBIT در عارضه‌یابی فرآیندهای مدیریت IT شرکت ملی حفاری ایران با رویکرد بلوغ فرآیندی

مرتضی علاالدینی[۱]، علی دقایقی[۲]

دانشجوی کارشناسی ارشد، فناوری اطلاعات و مدیریت، دانشگاه صنعتی امیرکبیر (پلی‌تکنیک تهران) ـ کارشناس شرکت مهندسی نرم‌افزاری گلستان
تهران، ایران
m.alaeddini@aut.ac.ir

[۲] کارشناسی ارشد فناوری اطلاعات و مدیریت، دانشگاه صنعتی امیرکبیر (پلی‌تکنیک تهران)، رئیس کارگروه فن‌آوری اطلاعات و ارتباطات و رئیس اداره فن‌آوری اطلاعات
شرکت ملی حفاری ایران
اهواز، ایران
daghayeghi@nidc.com

Abstract

Nowadays, owing to the fact that information is regarded as one of the most important enterprise assets and strategic resources, IT management method is an imperative basis in enterprise planning. The need for assurance about the value of IT, the management of IT-related risks and increased requirements for control over information are now understood as key elements of enterprise governance.

In this paper, we are going to introduce COBIT as an internal control framework and to show how to use this framework for evaluating current situation of IT organization's processes in National Iranian Drilling Company (NIDC). This framework uses a six-level maturity model for benchmarking and recognition necessary improvements in IT based on which presented by Software Engineering Institute (SEI). Finally we will propose a method to define NIDC's IT goals and metrics and also will offer a solution to prepare a plan for upgrading maturity level of processes and to define required roles to execute these processes and achieve required maturity level.

Keywords

COBIT, IT governance, corporate governance, internal control framework, maturity model, National Iranian Drilling Company (NIDC), IT process, IT goal, IT metric

چکیده

امروزه اطلاعات از مهمترین دارایی‌ها و منابع استراتژیک هر سازمان است. به همین دلیل، نحوه مدیریت فناوری اطلاعات، یکی از ارکان مهم برنامه‌ریزی سازمانی بوده، نیاز به تضمین ارزش فناوری اطلاعات، مدیریت مخاطرات مرتبط با آن و کنترل اطلاعات، به عنوان عناصر کلیدی در رهبری هر سازمان محسوب می‌شوند.

در این مقاله، پس از معرفی اجمالی چارچوب کنترل داخلی COBIT، چگونگی استفاده از این چارچوب برای ارزیابی وضعیت موجود فرآیندهای سازمان متولی فناوری اطلاعات در «شرکت ملی حفاری ایران» با کمک مدل بلوغ ۶ سطحی ارایه شده از سوی «مؤسسه مهندسی نرم‌افزار (SEI)» که COBIT آن را برای انجام مطالعات تطبیقی و شناسایی بهبودهای ضروری در حوزه فناوری اطلاعات مورد استفاده قرار می‌دهد، ذکر گردیده است. در پایان نیز روشی برای تعیین اهداف و شاخص‌های کارآیی IT «شرکت ملی حفاری ایران» و نیز راهکاری برای تهیه برنامه‌ای جهت ارتقای سطح بلوغ فرآیندها و تعیین نقش‌های لازم برای اجرای این فرآیندها در شرکت و رسیدن به سطح بلوغ مورد انتظار بر اساس چارچوب مذکور، پیشنهاد گردیده است.

کلمات کلیدی

COBIT، حاکمیت فناوری اطلاعات، حاکمیت سازمانی، چارچوب کنترل داخلی، مدل بلوغ، شرکت ملی حفاری ایران، فرآیند IT، هدف IT، شاخص کارآیی IT

۱- مقدمه

امروزه اطلاعات جزو مهمترین دارایی‌ها و منابع استراتژیک هر سازمان به حساب می‌آید. به همین دلیل، نحوه مدیریت فناوری اطلاعات، به عنوان یکی از ارکان مهم برنامه‌ریزی سازمانی محسوب می‌شود. آنچه که امروزه آن را به عنوان مدیریت فناوری اطلاعات می‌شناسیم، در واقع طراحی ساختار، تشکیلات، وظایف و مسؤولیت‌ها، فرآیندها و نظام‌هایی است که اجرای آنها در سازمان برای بهره‌برداری بهینه از منابع و دارایی‌های اطلاعاتی و فناوری اطلاعات، ضروریست.

در اغلب سازمان‌ها و مؤسسات بزرگ، فناوری اطلاعات به عنوان یکی از باارزش‌ترین دارایی‌های مجموعه محسوب می‌گردد. سازمانی موفق است که به ارزش واقعی این دارایی پی برده، بتواند در دستیابی به منافع ذینفعان خود، از آن استفاده کند. نیاز به تضمین ارزش‌های فناوری اطلاعات، مدیریت مخاطرات مرتبط با آن و کنترل اطلاعات، امروزه به عنوان عناصر کلیدی در حاکمیت سازمانی[1] محسوب می‌شوند [1]. همین ارزش، ریسک و کنترل، هسته حاکمیت فناوری اطلاعات[2] را تشکیل می‌دهند.

حاکمیت فناوری اطلاعات یک جنبه از چارچوب وسیع حاکمیت سازمان ـ که توسط سازمان همکاری و توسعه اقتصادی[3] (OECD) در رابطه با حاکمیت اشخاص حقوقی تشریح گردیده است ـ محسوب می‌شود [2]. حاکمیت فناوری اطلاعات بر عهده مدیران اجرایی سازمان بوده، شامل مدیریت، ساختاردهی به سازمان و فرآیندهایی برای اطمینان از حرکت فناوری اطلاعات در راستای استراتژی‌ها و اهداف سازمان است [1]. حاکمیت مؤثر فناوری اطلاعات سازمان را در دستیابی به سه هدف حیاتی، یعنی انطباق با قوانین و مقررات، برتری عملیاتی و مدیریت بهینه ریسک‌ها، قارد می‌سازد [3] و می‌تواند سازمان را در زمینه اطمینان از پشتیبانی اهداف توسط IT، بهبود سرمایه‌گذاری در زمینه IT و مدیریت مخاطرات و فرصت‌های مرتبط با IT یاری دهد [1].

می‌دانیم که سازمان‌ها ناگزیر به ارضای نیازمندی‌های کیفیت، اعتبار و امنیت اطلاعات خود در رابطه با همه دارایی‌هایشان هستند. همچنین مدیریت سازمان باید به صورت بهینه از منابع در دسترس IT، شامل برنامه‌های کاربردی، اطلاعات، زیرساخت و نیروی انسانی، استفاده نماید [1]. برای انجام این مسؤولیت‌ها و به منظور دستیابی به اهداف مورد نظر، مدیریت سازمان ناگزیر است که به وضعیت معماری سازمان خود از منظر IT واقف بوده، در مورد حاکمیت و کنترل مورد نیاز، تصمیم‌گیری کند.

شرکت ملی حفاری ایران یکی از سازمان‌های زیرمجموعه وزارت نفت است که با هدف افزایش توان رقابتی خود و ورود به بازارهای جهانی، تصمیم به برنامه‌ریزی استراتژیک در حوزه‌های مختلف کسب و کار اصلی و پشتیبانی خود گرفته و یکی از این حوزه‌ها، حوزه فناوری اطلاعات است. با این نگاه، جایگاه IT در سازمان از یک فراهم‌کننده اطلاعات به یک جزء ضروری از استراتژی سازمان [4]، ارتقا خواهد یافت. نیاز این شرکت در زمینه فناوری اطلاعات، شناخت و عارضه‌یابی وضعیت کنونی در ابعاد مختلف فرآیندی، اطلاعاتی، عملیاتی و زیرساختی و همچنین تصویر وضع مطلوب فناوی اطلاعات شرکت و برنامه‌ریزی برای رسیدن به این وضع بر اساس استراتژی‌ها و اهداف فناوری اطلاعات است.

بدین منظور پروژه‌ای تحت عنوان «تدوین معماری سازمانی فناوری اطلاعات و ارتباطات» توسط این شرکت تعریف و اجرا گردیده که هم‌اکنون فاز شناخت آن به پایان رسیده است. در حوزه شناسایی وضع موجود و طراحی وضع مطلوب سازمان متولی فناوری اطلاعات در شرکت ملی حفاری ایران، نیاز به مدل مرجعی که بتواند پوشش‌دهنده همه نیازهای IT شرکت باشد و به عنوان نقشه راه، مورد استفاده قرار گیرد، ضروری بوده، از طرفی این مدل باید بتواند چارچوبی را برای کنترل و ممیزی فعالیت‌های مطلوب که در آینده انجام خواهند شد نیز فراهم نماید.

۱-۱- چرا به چارچوب کنترلی نیاز است؟

مدیریت ارشد هر سازمان به طور فزاینده برای تحقق دستاوردهای مهم اطلاعات در موفقیت سازمان خود می‌کوشد. مدیران به دلایل زیر می‌خواهند از برآورده شدن اهداف فناوری اطلاعات در سازمانشان آگاه شوند [1]:

- دستیابی به اهداف
- حصول اطمینان از یادگیری و سازگاری
- مدیریت خردمندانه مخاطراتی که سازمان با آنها روبروست
- شناسایی فرصت‌ها و استفاده از آنها

سازمان‌های موفق، علاوه بر شناسایی مخاطرات و بهره‌گیری از منافع فناوری اطلاعات، راه‌هایی نیز برای انجام موارد زیر می‌یابند [1]:

- هم‌سو کردن استراتژی‌های IT با استراتژی‌های کسب و کار
- ایجاد اطمینان در سرمایه‌گذاران و ذینفعان از این بابت که سازمان، مخاطرات آینده را پیش‌بینی نموده است
- تسری استراتژی‌ها و اهداف IT در سازمان
- کسب سود از سرمایه‌گذاری IT

- فراهم نمودن ساختارهای سازمانی که پیاده‌سازی استراتژی‌ها و اهداف را تسهیل می‌کنند
- ایجاد روابط سازنده و مؤثر میان کسب و کار و IT با شرکای بیرونی
- اندازه‌گیری کارآیی IT

۱-۲- چه کسی به چارچوب کنترلی نیاز دارد؟

از خصوصیات یک چارچوب کارآ و مناسب برای حاکمیت و کنترل حوزه مورد نظر، خدمت‌رسانی به انواع ذینفعان داخلی و خارجی سازمان است. این ذینفعان عبارتند از [1]:

- ذینفعان داخلی علاقمند به خلق ارزش از طریق سرمایه‌گذاری IT؛ شامل کسانی که در رابطه با سرمایه‌گذاری تصمیم می‌گیرند، افرادی که در مورد نیازمندی‌ها تصمیم‌گیری می‌کنند و کسانی که سرویس‌های IT را به کار می‌برند
- ذینفعان داخلی و خارجی فراهم‌کننده سرویس‌های IT؛ شامل مدیران سازمان و فرآیندهای IT، فراهم‌کنندگان امکانات و کسانی که سرویس‌ها را راه‌اندازی می‌کنند
- ذینفعان داخلی و خارجی با نقش‌های حساس و نظارتی؛ شامل مسؤولان امنیتی، افرادی با دسترسی‌های خاص و تهیه‌کنندگان سرویس‌های امنیتی

۱-۳- ویژگی‌های یک چارچوب کنترل IT چیست؟

برای پاسخگویی به نیازهای حاکمیت فناوری اطلاعات، چارچوب مورد نظر باید [1]:

- برای همسو کردن اهداف IT با کسب و کار، روی کسب و کار تمرکز کند.
- به منظور تعریف محدوده و ساختار وظایف و اختیارات، فرآیندگرا باشد.
- با تجارب موفق پیشین و استانداردهای موجود در زمینه IT سازگار باشد.
- از زبان مشترک و قابل فهم برای تمامی ذینفعان برخوردار باشد.
- به وسیله تحکم استانداردهای حاکمیت سازمان، در برآورده ساختن نیازمندی‌های قانونی، کمک نماید.

با توجه به مطالب یادشده، یکی از نیازهای اساسی هر سازمان ـ که طبعاً سازمان‌های داخلی کشور ما نیز از آن مستثنی نیستند ـ در اختیار گرفتن و استفاده از چارچوب و روشی برای کنترل فناوری اطلاعات در آن سازمان است.

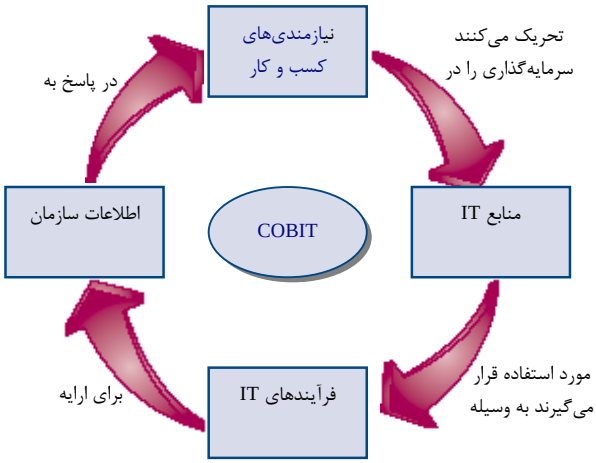
پروژه CobiT که امروزه در سراسر جهان توسط سازمان‌های مختلفی بکار گرفته می‌شود ـ و همین امر مهر تأییدی بر آن است ـ تجارب موفق مدیریتی را در زمینه امنیت و کنترل فناوری اطلاعات بیان می‌کند [5] و از این حیث، استفاده از آن برای کنترل حوزه فناوری اطلاعات در سازمان، دارای ارزشی ویژه خواهد بود.

۲- CobiT، یک چارچوب کنترلی

مؤسسه ITGI (با نشانی اینترنتی www.itgi.org) در سال ۱۹۹۸ با هدف پیشبرد مطالعات بین‌المللی در زمینه هدایت و کنترل فناوری اطلاعات در سازمان‌ها تأسیس گردیده است. بدین منظور و برای کمک به برآورده ساختن این هدف، مؤسسه ITGI مبادرت به انتشار استانداردها و دستورالعمل‌هایی در قالب یک سری کتب و مقالات، منابع الکترونیکی و مطالعات موردی نموده که یکی از این استانداردها چارچوب CobiT است. ویرایش جدید این استاندارد در سال ۲۰۰۷ و با نام CobiT 4.1 انتشار یافته است. این چارچوب دارای ویژگی‌های منحصر به فردیست که آن را از سایر روش‌ها و چارچوب‌های موجود در زمینه مدیریت فناوری اطلاعات، متمایز می‌سازد. در ادامه، نگاهی گذرا به این ویژگی‌ها شده است.

۲-۱- تمرکز روی کسب و کار

اصلی‌ترین خصوصیت CobiT تمرکز آن روی کسب و کار است. چارچوب CobiT نه فقط برای فراهم‌کنندگان سرویس‌های IT، کاربران و ممیزان، بلکه بیشتر برای مدیران و صاحبان کسب و کار، طراحی شده است.

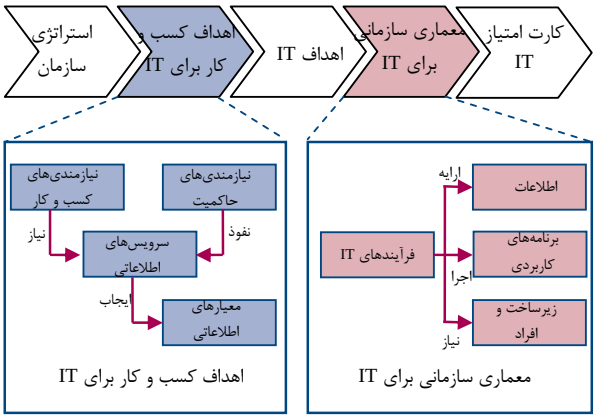


شکل (۱): پایه اصلی CobiT [1]

همان طور که در شکل (۱) نیز نشان داده شده، چارچوب مذکور بر این پایه استوار است که سازمان باید برای فراهم نمودن اطلاعاتی که برای دستیابی به اهدافش به آنها نیاز دارد، با استفاده از مجموعه‌ای ساخت‌یافته از فرآیندها در زمینه مدیریت و کنترل منابع IT، سرمایه‌گذاری کند. مدیریت و کنترل اطلاعات را می‌توان قلب این چارچوب دانست؛ چرا که به سازمان اطمینان می‌دهند در راستای پاسخگویی به نیازمندی‌های کسب و کار خود حرکت کند [1].

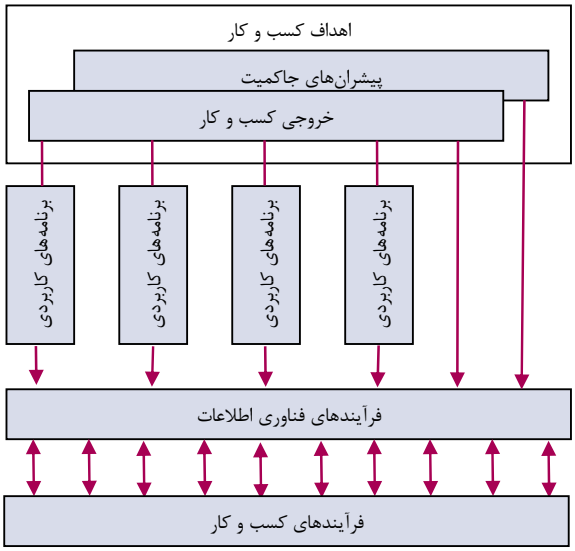
برای نیل به اهداف کسب و کار، اطلاعات باید با معیارهای کنترلی خاصی تطبیق یابد. این معیارهای اطلاعاتی در COBIT عبارتند از [1]:

- اثربخشی[۴]؛ مربوط به وابستگی اطلاعات به فرآیندهای کسب و کار و ارایه بموقع، صحیح، منسجم و کاربردی اطلاعات
- کارآیی[۵]؛ مرتبط با فراهم کردن اطلاعات از طریق استفاده بهینه (اقتصادی و سودبخش) از منابع
- محرمانگی[۶]؛ در رابطه با جلوگیری از دسترسی غیر مجاز به اطلاعات حساس
- یکپارچگی[۷]؛ مربوط به دقت، صحت و اعتبار اطلاعات مطابق با انتظارات کاری سازمان
- دسترس‌پذیری[۸]؛ مربوط به در دسترس بودن اطلاعات در زمان مورد نیاز
- انطباق[۹]؛ مربوط به سازگاری اطلاعات با قوانین، مقررات و سیاست‌های سازمان
- قابلیت اعتماد[۱۰]؛ مرتبط با فراهم نمودن اطلاعات مناسب برای مدیریت در راستای انجام وظایف مدیریتی



شکل (۲): تعریف اهداف و معماری سازمانی IT [1]

وقتی قرار است فناوری اطلاعات سرویس‌هایی برای حمایت از استراتژی‌های سازمان ارایه کند، باید مالکیت و جهت‌گیری نیازمندی‌ها آشکار بوده، درک روشنی از این سرویس‌ها و چگونگی ارایه آنها، وجود داشته باشد. شکل (۲) نشان می‌دهد که چگونه استراتژی‌های سازمان می‌توانند به وسیله کسب و کار به اهداف مرتبط با IT ترجمه شوند.



شکل (۳): مدیریت منابع IT برای نیل به اهداف IT [1]

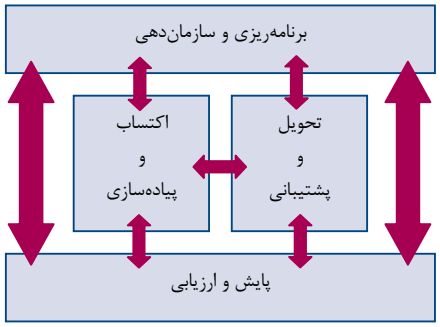
ساختار IT سازمان باید با تعریفی روشن از فرآیندها و نیز با استفاده از منابعی نظیر مهارت افراد و زیرساخت‌های فناوری، در جهت این اهداف توسعه داده شود [1]. در شکل (۳) به طور خلاصه نشان داده شده است که برای دستیابی به اهداف IT چگونه باید منابع IT توسط فرآیندهای IT مدیریت شوند.

۲-۲- فرآیندگرا

این چارچوب برای پایش و مدیریت فعالیت‌های IT، یک مدل فرآیندی مرجع و یک زبان قابل فهم را برای تمامی کارکنان سازمان فراهم می‌کند. همچنین COBIT چارچوبی را برای برقراری ارتباط میان سرویس‌دهندگان، یکپارچه‌سازی تجارب موفق مدیریتی و اندازه‌گیری و پایش کارآیی فناوری اطلاعات، تهیه می‌نماید.

برای رهبری مؤثر فناوری اطلاعات در سازمان لازمست که فعالیت‌ها و خطرات IT به دقت شناسایی گردند. این موارد عموماً در حوزه‌های برنامه‌ریزی، ساخت، اجرا و پایش، خود را نشان می‌دهند [1]. به همین منظور مطابق شکل (۴)، چارچوب COBIT حوزه‌های زیر را برای بررسی در سازمان پیشنهاد داده است:

- برنامه‌ریزی و سازمان‌دهی[۱۱] (PO): جهت‌گیری ارایه راهکار (AI) و سرویس‌دهی (DS) را تعیین می‌کند.
- اکتساب و پیاده‌سازی[۱۲] (AI): راهکارهایی را ارایه و آنها را به سرویس تبدیل می‌کند.
- تحویل و پشتیبانی[۱۳] (DS): راهکارها را دریافت و برای کاربران نهایی، قابل استفاده می‌کند.
- پایش و ارزیابی[۱۴] (ME): همه فرآیندها را به منظور اطمینان یافتن از پیروی جهت‌گیری ارایه شده، پایش می‌کند.

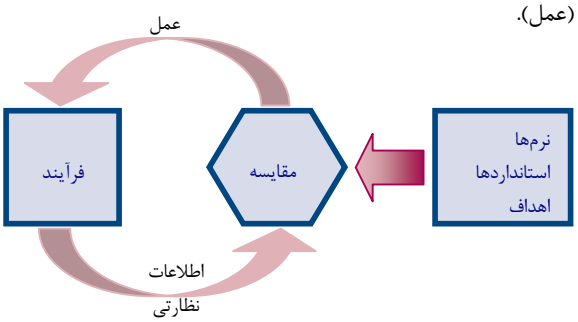


شکل (۴): وابستگی حوزه‌های چهارگانه در COBIT [1]

۲-۳- کنترل‌محور

کنترل به شکل سیاست‌ها، رویه‌ها، تجارب و ساختارهای سازمانی طراحی شده برای تضمین دستیابی به اهداف کسب و کار و پیشگیری یا تشخیص و اصلاح رخدادهای نامطلوب در نظر گرفته می‌شود [1]. با دید کنترل و ممیزی، سازمان‌ها باید نسبت به استقرار سیستم‌های کنترلی در همه ابعاد فناوری اطلاعات خود، نظیر مدیریت امنیت اطلاعات [6] یا مدیریت پروژه و ریسک‌های ناشی از آن، مبادرت ورزند. پس از این که چنین سیستم‌های کنترلی در سازمان مستقر شدند، کارآیی کنترل باید توسط رویه‌های ممیزی مورد اندازه‌گیری قرار گیرد [6].

در شکل (۵) مدل استانداردی برای نظارت نشان داده شده است. این مدل بر اساس اصول آشکار این تمثیل بنا شده که وقتی دمای اتاق (استاندارد) برای سیستم گرمایشی (فرآیند) تنظیم شده است، سیستم دایماً دمای پیرامون اتاق (اطلاعات نظارتی) را کنترل می‌کند (مقایسه) و به سیستم گرمایشی برای بالا یا پایین بردن دما اخطار می‌دهد (عمل).



شکل (۵): مدل نظارت [1]

در واقع می‌توان COBIT را مدلی برای مدیریت فناوری اطلاعات دانست که بر پایه دو مدل کنترل داخلی اصلی استوار است؛ «مدل کنترل عملیات جامع[۱۵]» و «مدل کنترل تمرکز بر فناوری اطلاعات[۱۶]» [6]. این چارچوب با متعادل ساختن ریسک و هدایت و کنترل معیارها و شاخص‌ها، سازمان را در دستیابی به اهدافش یاری می‌رساند. بر این اساس، سیستم کنترل‌های داخلی سازمان در سه سطح بر فناوری اطلاعات اثر دارد [1]:

- در سطح «مدیریت اجرایی»، اهداف کسب و کار تعیین شده، سیاست‌گذاری‌ها صورت گرفته، راجع به چگونگی استقرار و مدیریت منابع سازمان برای اجرای استراتژی‌ها تصمیم‌گیری می‌شود. در این حالت، کنترل کلی به وسیله یک کمیته تخصصی در سطح سازمان صورت می‌گیرد.
- در سطح «فرآیند کسب و کار»، فعالیت‌های کسب و کار خاص کنترل می‌شوند.
- برای «پشتیبانی» از فرآیندهای کسب و کار، فناوری اطلاعات به ارایه سرویس‌های IT (معمولاً سرویس‌های مشترک میان فرآیندهای کسب و کار) مبادرت می‌ورزد. در این حالت، همه فعالیت‌های خدمات IT تحت نظارت قرار می‌گیرند که این نظارت‌ها با نام کنترل‌های عمومی IT شناخته می‌شوند.

۲-۴- قابل اندازه‌گیری

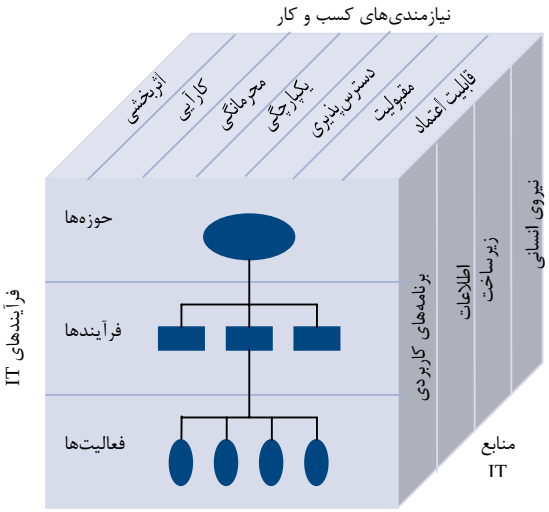
نیاز اساسی هر سازمان، شناخت وضعیت سیستم‌های IT آن سازمان و تصمیم‌گیری در رابطه با سطح مدیریت و کنترل لازم می‌باشد. برای تصمیم‌گیری صحیح، این پرسش برای مدیریت مطرح می‌شود که تا چه حد باید پیش رفت و آیا هزینه‌های صورت گرفته با سود مورد انتظار، تراز خواهد شد یا نه.

هر سازمان باید بداند در چه وضعیتی قرار دارد، در چه جاهایی بهبود لازم است و باید از چه ابزاری برای پایش این بهبود استفاده کند. چارچوب COBIT با فراهم کردن موارد زیر، به این امور رسیدگی می‌کند [1]:

- مدل‌های بلوغ برای انجام مطالعات تطبیقی و شناسایی بهبودهای ضروری
- اهداف و شاخص‌های کارآیی فرآیندهای IT که نشان می‌دهند فرآیندها چگونه اهداف IT و کسب و کار را برآورده می‌سازند
- اهداف فعالیت برای کارآیی مؤثر فرآیند

۳- معرفی مدل مرجع فرآیندها در COBIT

چنان که گفته شد، «منابع IT توسط فرآیندهای IT و به منظور دست‌یابی به اهداف IT که پاسخگوی نیازهای کسب و کار هستند، مدیریت می‌شوند». این عبارت مبنای چارچوب COBIT است و می‌توان آن را به صورت مکعبی که در شکل (۶) نشان داده شده، در نظر گرفت. این مکعب به مکعب COBIT معروف است.



شکل (۶): مکعب COBIT [1]

همان طور که در شکل (۶) نشان داده شده است، این چارچوب ۳۴ فرآیند عمومی فناوری اطلاعات را در چهار حوزه که پیشتر ذکر شدند، تقسیم‌بندی می‌کند و انجام هر فرآیند را منوط به اجرای تعدادی فعالیت می‌داند. نکته مهم این است که COBIT به جای بیان چگونگی کارها بیشتر روی این امر تمرکز دارد که چه کارهایی باید انجام شود. بنابراین می‌توان آن را یکپارچه‌ساز تجارب و پژوهش‌های حاکمیت IT با مدیریت اجرایی، مدیریت IT و کسب و کار، حاکمیت، کارشناسان تضمین و امنیت و کارشناسان ممیزی و کنترل دانست [1].

جدول (۱) فهرست فرآیندهای عمومی فناوری اطلاعات را از دید چارچوب COBIT نشان می‌دهد.

جدول (۱): فهرست فرآیندهای IT در چارچوب COBIT

حوزه	شناسه فرآیند	عنوان فرآیند
برنامه‌ریزی و سازمان‌دهی	PO1	تدوین برنامه استراتژیک IT
	PO2	تدوین معماری اطلاعات
	PO3	تعیین جهت‌گیری فناوری
	PO4	تعریف فرآیندها، سازمان و روابط IT
	PO5	مدیریت بر سرمایه گذاری در IT
	PO6	ارتباط دادن اهداف مدیریتی و جهت‌گیری‌ها
	PO7	مدیریت منابع انسانی IT
	PO8	مدیریت کیفیت
	PO9	ارزیابی و مدیریت ریسک‌های IT
	PO10	مدیریت پروژه‌ها
اکتساب و پیاده‌سازی	AI1	تعیین راهکارهای اتوماسیون
	AI2	تهیه و نگهداری نرم‌افزارهای کاربردی
	AI3	تهیه و نگهداری زیرساخت فناوری
	AI4	عملیاتی کردن راهکارها
	AI5	تهیه منابع IT
	AI6	مدیریت تغییرات
	AI7	اجرا و معتبرسازی راهکارها و تغییرات
تحویل و پشتیبانی	DS1	تعریف و مدیریت سطوح سرویس
	DS2	مدیریت خدمات شخص ثالث
	DS3	مدیریت کارآیی و ظرفیت منابع
	DS4	استمرار سرویس‌ها
	DS5	مدیریت امنیت
	DS6	شناسایی و تخصیص هزینه های سرویس‌ها
	DS7	آموزش کاربران
	DS8	مدیریت میز سرویس‌ها و رویدادها
	DS9	مدیریت پیکربندی
	DS10	مدیریت مشکلات
	DS11	مدیریت داده
	DS12	مدیریت محیط فیزیکی
	DS13	مدیریت عملیات
پایش و ارزیابی	ME1	پایش و ارزیابی کارآیی IT
	ME2	پایش و ارزیابی کنترل داخلی
	ME3	انطباق با نیازمندیهای خارجی
	ME4	ایجاد رهبری IT

در چارچوب COBIT هر فرآیند دارای شناسنامه‌ایست که این موارد در آن درج شده است:

- شرح فرآیند
- ارتباط فرآیند با نیازمندی‌های کسب و کار
- منابع فناوری اطلاعات مورد نیاز برای اجرای فرآیند
- اهداف کنترلی فرآیند
- ورودی‌ها و خروجی‌های فرآیند
- فعالیت‌ها (گام‌های فرآیند) و ارتباطشان با افراد و نقش‌های مختلف سازمان
- اهداف و شاخص‌های کارآیی
- مدل بلوغ فرآیند

با استفاده از این شناسنامه می‌توان سطح بلوغ فرآیند مورد نظر را در سازمان مورد سنجش قرار داد و برای بهبود آن در آینده، برنامه‌ریزی کرد.

۴- بلوغ فرآیندی در COBIT

مدیران ارشد سازمان همواره در صدد هستند که بدانند فناوری اطلاعات در سازمانشان چگونه هدایت می‌شود. برای دانستن این مطلب باید به طریقی سطح بلوغ IT در سازمان ارزیابی گردد. در چارچوب COBIT مدلسازی بلوغ بر اساس نوعی ارزیابی سازمانی بنا شده است که بین سطح عدم وجود (۰) و بهینه (۵) رتبه‌بندی می‌شود. این رتبه‌بندی بر اساس مدل بلوغ پیشنهادی مؤسسه مهندسی نرم‌افزار[۱۷] در ارتباط با سنجش سطح بلوغ قابلیت توسعه نرم‌افزار، صورت می‌گیرد [1]. سطوح مختلف بلوغ در مدل یاد شده، همان طور که در شکل (۷) نشان داده شده است، به صورت زیر دسته‌بندی می‌شوند:

- سطح ۰ ـ عدم وجود[18]: فقدان هرگونه فرآیند؛ سازمان حتی متوجه نشده است که باید کاری انجام دهد.
- سطح ۱ ـ ابتدایی/ فاقد عمومیت[19]: مدرکی دال بر توجه سازمان نسبت به موضوع وجود دارد؛ اما هیچ فرآیندی استاندارد نیست و فقط کارهایی فاقد عمومیت، موردی و یا شخصی اجرا می‌شوند.
- سطح ۲ ـ تکرارپذیر اما شهودی[20]: فرآیندها تا حدی توسعه یافته‌اند که رویه‌های مشابه توسط نقش‌های مشابه انجام می‌شوند. در این سطح، هیچ گونه آموزش رسمی داده نشده، ارتباطی با رویه‌های استاندارد وجود ندارد و مسؤولیت بر عهده اشخاص است. به دلیل وابستگی زیاد به دانش اشخاص، بروز خطا نیز محتمل است.
- سطح ۳ ـ فرآیند تعریف شده[21]: رویه‌ها استاندارد، مستند و با آموزش مرتبط شده‌اند. انجام موارد مذکور بسیار ضروریست؛ با این حال شناسایی انحرافات بعید به نظر می‌رسد. رویه‌ها از سطح بالایی برخوردار نبوده، صرفاً جنبه تشریفاتی دارند.
- سطح ۴ ـ مدیریت شده و قابل اندازه‌گیری[22]: مدیریت سازمان به پایش و ارزیابی مطلوبیت رویه‌ها پرداخته، هرجا به نظر آید که اجرای فرآیندها مؤثر نیست، وارد عمل می‌شود. فرآیندها تحت بهبود مستمر قرار داشته، منجر به ارایه تجارب موفق می‌شوند. اتوماسیون و ابزار به شکل محدود و تکه‌تکه بکار می‌روند.
- سطح ۵ ـ بهینه[23]: فرآیندها در سطح تجارب موفق دیگر سازمان‌ها، بر مبنای نتایج بهبود مستمر و مدل‌سازی بلوغ، پالایش شده‌اند. فناوری اطلاعات به صورت یکپارچه و به منظور خودکارسازی گردش کارها، فراهم آوردن ابزار ارتقای کیفیت و سرعت بخشیدن به تطابق سازمان با تغییرات، مورد استفاده قرار می‌گیرد.

شکل (۷): نمایش گرافیکی مدل‌های بلوغ [1]

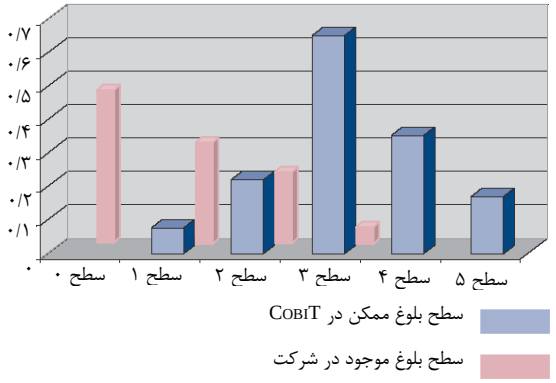
مزیت یک مدل بلوغ اینست که به مدیریت سازمان امکان می‌دهد تا به سادگی بتواند وضعیت سازمان را درک نموده، در صورتی که به بهبود کارآیی نیاز داشته باشد، بتواند نکات مبهم این امر را دریابد [1].

۵- بکارگیری COBIT در شرکت ملی حفاری

طی انجام پروژه «تدوین معماری سازمانی فناوری اطلاعات و ارتباطات» در شرکت ملی حفاری ایران، در فاز شناخت وضعیت موجود فناوری اطلاعات و ارتباطات، علاوه بر تشریح فرآیندهای استاندارد برای یک سازمان متولی مدیریت IT و همچنین ارایه روشی برای ارزیابی و سنجش بلوغ این فرآیندها در شرکت، وضعیت موجود مدیریت فناوری اطلاعات شرکت شامل فرآیندها، سرمایه‌گذاری، نیروی انسانی و پروژه‌های IT، مورد ارزیابی قرار گرفته است.

در این رابطه، پس از شناخت جایگاه کنونی IT (شامل ساختار سازمانی و شرح وظایف) در شرکت ملی حفاری ایران، ۳۴ فرآیند عمومی یادشده در چارچوب COBIT مورد شناسایی قرار گرفته‌اند. همچنین بر اساس مصاحبات انجام شده با مدیران واحدهای متولی IT در شرکت و مشاهدات به عمل آمده از روند اجرای فرآیندها، سطح بلوغ هریک از فرآیندهای موجود بر اساس رهنمودهای ذکر شده در شناسنامه هریک از فرآیندها در چارچوب مذکور، اندازه‌گیری شده است.

نتایج این ارزیابی نشان می‌دهد که هم‌اکنون سطح بلوغ IT در شرکت ملی حفاری ایران ـ که از میانگین امتیازهای بلوغ تک‌تک فرآیندها حاصل گردیده ـ برابر ۱/۱۲ است. بر اساس این ارزیابی، ۴۷٪ فرآیندهای کنونی IT شرکت دارای سطح بلوغ صفر، ۲۹٪ دارای سطح بلوغ یک، ۲۱٪ دارای سطح بلوغ دو و تنها ۳٪ فرآیندها دارای سطح بلوغ سه هستند. سطوح بلوغ چهار و پنج در شرایط کنونی شرکت، مشاهده نشده‌اند. مقایسه این مقادیر با آنچه که خود چارچوب COBIT به عنوان سطوح بلوغ ممکن یک فرآیند معرفی می‌کند، در نوع خود می‌تواند جالب باشد. این نتایج در شکل (۸) با یکدیگر مقایسه شده شده‌اند.



شکل (۸): مقایسه سطوح بلوغ ممکن برای فرآیندها در COBIT [1] و سطوح بلوغ فرآیندهای کنونی در شرکت ملی حفاری ایران

همچنین مقایسه‌ای میان سطوح بلوغ در حوزه‌های مختلف نشان می‌دهد که حوزه «برنامه‌ریزی و سازمان‌دهی» با نمره ۱/۴۰ بیشترین و

حوزه «پایش و ارزیابی» با نمره ۰/۴۸ کمترین سطح بلوغ را در میان حوزه‌های فرآیندی فناوری اطلاعات دارا هستند. این در حالیست که بالغ‌ترین حوزه فناوری اطلاعات در شرکت ملی حفاری ایران، در شرایط حاضر، امتیازی کمتر از ۲ کسب نموده است.

در این مطالعات، سطح بلوغ فرآیندهای کلیدی فناوری اطلاعات شرکت ملی حفاری ایران، یعنی فرآیندهایی که با عوامل کلیدی موفقیت[۲۴] در ارتباطند، نیز به طور جداگانه مورد ارزیابی قرار گرفته است. بر خلاف انتظار، این مقدار برابر ۱/۱۳ است که تنها به میزان ۰/۰۱ از مقدار مشابه برای همه فرآیندها بیشتر است. این مقدار نشان از عدم بلوغ و توجه کافی به فرآیندهای کلیدی فناوری اطلاعات همچون سایر فرآیندهای غیر کلیدی این حوزه در شرکت دارد. نتیجه‌ای که از این مقایسه می‌توان گرفت، عدم شناخت دقیق این شرکت از عوامل کلیدی موفقیت خود و به تبع، فرآیندهای کلیدی در حوزه‌های مختلف است که فناوری اطلاعات نیز یکی از این حوزه‌هاست.

۶- نقشه راه آینده شرکت ملی حفاری

پیاده‌سازی حاکمیت فناوری اطلاعات در شرکت ملی حفاری ایران هنوز مراحل اولیه خود را طی می‌کند و تا حصول نتیجه کامل، راهی طولانی باقی است. طبق برنامه پروژه، پس از کسب شناخت از وضعیت کنونی مدیریت IT در شرکت ملی حفاری ایران، ابتدا باید سند راهبردی IT شرکت تدوین گردد و سپس بر اساس اهداف و چشم‌انداز فناوری اطلاعات تدوین شده در این سند، فرآیندهای مطلوب IT تعیین و سطح بلوغ مورد انتظار برای آنها مشخص گردد.

یکی از روش‌هایی که عموماً برای تعیین عناصر استراتژیک فناوری اطلاعات در سازمان و تهیه سند راهبردی IT مورد استفاده قرار می‌گیرد، همراستاسازی استراتژیک [7] است. لازم به ذکر است که COBIT نگاه ویژه‌ای به این رویکرد داشته، چنان که پیشتر نیز ذکر شد، تأکید خاصی بر همسویی فناوری اطلاعات با کسب و کار سازمان دارد. همسویی استراتژی‌های IT با استراتژی‌های کسب و کار، مدیران سازمان را نسبت به تحویل بموقع و تحت بودجه مشخص دستاوردهای IT، کسب وظیفه‌مندی و سود مناسب، تعادل سرمایه‌گذاری IT در میان سیستم‌های پشتیبانی موجود و سیستم‌های مورد نیاز برای ایجاد مزایای رقابتی در آینده، تصمیم‌گیری در مورد تمرکز روی منابع IT، پیشبرد استراتژی‌های رقابتی، بهبود رضایتمندی مشتریان و تضمین نگاهداشت ایشان، مطمئن می‌سازد [2].

بدین منظور، در یکی از پیوست‌های این چارچوب، پیوندی میان اهداف کسب و کار با اهداف متصور برای IT از دید COBIT برقرار شده است که از این موضوع می‌توان برای تعیین اهداف فناوری اطلاعات در شرکت ملی حفاری ایران استفاده کرد. شاخص‌های کارآیی مرتبط با هر هدف فناوری اطلاعات نیز در این چارچوب بیان گردیده‌اند.

در پیوست دیگری از چارچوب یادشده، ارتباط میان اهداف و فرآیندهای IT بر اساس آنچه که در شناسنامه فرآیندهای COBIT ذکر شده، مشخص گردیده است. پس از تعیین اهداف فناوری اطلاعات در شرکت ملی حفاری ایران با توجه به شرایط و اولویت‌ها و همچنین پس از مشخص شدن سطح بلوغ مطلوب برای فرآیندهای IT، باید فرآیندهای مرتبط با این اهداف شناسایی شوند و برنامه‌ریزی برای ارتقای سطح بلوغ این فرآیندها به مقدار مورد نظر، صورت گیرد. با این اوصاف، بهبود و ارتقای سطح بلوغ سایر فرآیندها که فاقد ارتباط با اهداف فناوری اطلاعات شرکت هستند، در اولویت‌های بعدی قرار خواهد گرفت.

پس از تعیین اولویت فرآیندهای مطلوب، باید نقش‌های مجری هر فرآیند در چارچوب COBIT با پست‌های سازمانی موجود در سازمان تطبیق داده شوند. در صورت عدم وجود نقش‌های مورد نظر در سازمان، باید پست‌های سازمانی جدیدی همراه با شرح وظایف مدون، برای پوشش دادن نقش‌های مورد نظر، در سازمان در نظر گرفته شوند. برای تعیین شرح وظایف این پست‌ها می‌توان از مجموعه فعالیت‌های مرتبط با فرآیندهای مطلوب به همراه نحوه تعامل نقش مورد نظر با این فعالیت‌ها بهره برد. این نحوه‌های تعامل در COBIT به صورت مسؤول انجام[۲۵] (R)، مسؤول پاسخگو[۲۶] (A)، مشاور[۲۷] (C) یا آگاه[۲۸] (I) مشخص شده‌اند.

۷- نتیجه

این مقاله با همکاری شرکت ملی حفاری ایران نگاشته شده و نحوه بکارگیری چارچوب کنترل داخلی COBIT در شناخت و عارضه‌یابی فرآیندهای کنونی حوزه فناوری اطلاعات این شرکت، در آن تشریح گردیده است.

شرکت ملی حفاری ایران با نگاه ارتقای جایگاه فناوری اطلاعات از یک فراهم‌کننده اطلاعات در شرکت به یک جزء غیر قابل تفکیک از استراتژی سازمان، مبادرت به تعریف و انجام پروژه‌ای تحت عنوان «تدوین معماری سازمانی فناوری اطلاعات و ارتباطات» نموده است که هم‌اکنون مراحل اولیه خود را پشت سر می‌گذارد. در این پروژه با توجه به نیازهای شرکت و میل آن به حرکت به سوی حاکمیت فناوری اطلاعات، COBIT به عنوان استاندارد و مدل مرجعی که شرکت را در شناسایی وضع موجود و طراحی وضع مطلوب سازمان متولی فناوری اطلاعات خود یاری دهد و بتواند در آینده نیز به عنوان چارچوبی برای کنترل و ممیزی فرآیندهای این سازمان عمل کند، انتخاب شده است.

اگرچه ممکن است بکارگیری این چارچوب و مدل بلوغ فرآیندی آن در شرکت ملی حفاری ایران، منعکس‌کننده نتایج مأیوس‌کننده‌ای

از وضعیت و بلوغ کنونی فناوری اطلاعات در این شرکت باشد، ولی می‌توان امیدوار بود که شرکت مذکور با استفاده از رویکرد مبتنی بر همسویی بین فناوری اطلاعات و کسب و کار که از پایه‌های اصلی این چارچوب است، بتواند در تدوین استراتژی‌ها و اهداف فناوری اطلاعات خود به موفقیت‌های عمده دست یابد. پس از تدوین استراتژی‌ها و اهداف فناوری اطلاعات در شرکت نیز می‌توان با کمک COBIT فرآیندهای مطلوبی را برای تحقق این اهداف، طراحی و اجرای این فرآیندها را در شرکت مورد کنترل، پایش و ارزیابی قرار داد و بدین نحو در بهبود مستمر این فرآیندها کوشید.

پس از اتمام این پروژه و تشکیل بدنه و ساختار اصلی سازمان متولی فناوری اطلاعات در شرکت ملی حفاری ایران، در رابطه با چگونگی اجرای فرآیندهای این سازمان، شرکت می‌تواند از سایر روش‌ها و استانداردهای مرتبط با فناوری اطلاعات نظیر ITIL یا ISO17799 نیز استفاده نماید.

سپاسگزاری

در پایان لازم می‌دانم از آقایان مهندس دقایقی و مهندس رشیدی، ریاست ادارات خدمات رایانه‌ای و مخابرات شرکت ملی حفاری ایران که در جمع‌آوری اطلاعات مورد نیاز، همکاری کامل نمودند و از هیچ کمکی دریغ نکردند، صمیمانه تشکر کنم. همچنین از زحمات آقایان دکتر سیروس و مهندس صبور طینت که با راهنمایی‌های ارزنده خویش در رفع اشکالات شناخت وضع موجود شرکت و شکل‌گیری این مقاله یاری‌ام کردند، سپاسگزارم.

مراجع

[1] IT Governance Institute (www.itgi.org), *Control Objectives for Information and related Technology (COBIT)*, Ver 4.1, USA, ITGI, Apr 2007.

[2] Hardy G., *Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges*, Information Security Technical Report, Vol. 11, pp. 55-61, Elsevier Ltd., 2006.

[3] Robinson, N., *IT excellence starts with governance*, Journal of Investment Compliance, Vol. 6 No. 3, pp. 45-49, Emerald Group Publishing Limited, 2005.

[4] Luthy, D., Forcht, K., *Laws and regulations affecting information management and frameworks for assessing compliance*, Information Management & Computer Security, Vol. 14 No. 2, pp. 155-166, Emerald Group Publishing Limited, 2006.

[5] Misra, S. C., Kumar, V., Kumar, U., *A strategic modeling technique for information security risk assessment*, Information Management & Computer Security, Vol. 15 No. 1, pp. 64-77, Emerald Group Publishing Limited, 2007.

[6] Hong, K. S., Chi, Y. P., Chao, L. R., Tang, J., H., *An integrated system theory of information security management*, Information Management & Computer Security, Vol. 11 No. 5, pp. 243-248, Emerald Group Publishing Limited, 2003.

[7] Henderson, J. C., Venkatraman, N., *Strategic Alignment: Leveraging information technology for transforming organizations*, IBM Systems Journal, Vol. 32, No. 1, 1993.

---

[1] Enterprise/Corporate Governance
[2] IT Governance
[3] Organisation for Economic Co-operation and Development (OECD)
[4] Effectiveness
[5] Efficiency
[6] Confidentiality
[7] Integrity
[8] Availability
[9] Compliance
[10] Reliability
[11] Plan and Organise (PO)
[12] Acquire and Implement (AI)
[13] Deliver and Support (DS)
[14] Monitor and Evaluate (ME)
[15] Holistic Operation Control Model
[16] Focus on Information Technology Control Model
[17] Software Engineering Institute (SEI)
[18] Non-existent
[19] Initial/Ad Hoc
[20] Repeatable but Intuitive
[21] Defined Process
[22] Managed and Measurable
[23] Optimised
[24] Key Success Factor (KSF)
[25] Responsible
[26] Accountable
[27] Consulted
[28] Informed