حسابرسی و کنترل فناوری اطلاعات:

مقایسه اجمالی بین چارچوب کوبیت ۴/۱ و کوبیت ۵

دکتر علیرضا سروش

مقدمه

انجمن حسابرسی و کنترل سیستمهای اطلاعاتی[۱] (ISACA) در کار نظارت، کنترل و اطمینان‌بخشی **فناوری اطلاعات** (IT) پیشتازی جهانی است که همایشهای بین‌المللی، دوره‌های آموزشی و یک شبکه دانش جهانی را پشتیبانی مالی و پرورش و معرفی **حسابرس رسمی سیستمهای اطلاعاتی**[۲] (CISA)، **مدیر رسمی امنیت اطلاعات**[۳] (CISM)، **متخصص نظام راهبری فناوری اطلاعات سازمان**[۴] (CGEIT) و **متخصص کنترل سیستمهای اطلاعاتی و ریسک**[۵] (CRISC) را در سطح جهان رهبری می‌کند و حسابرسی سیستمهای اطلاعاتی کاربردی و استانداردهای کنترل را در سطح جهانی توسعه می‌دهد. **کوبیت**[۶] (COBIT)، چارچوبی ارائه‌شده توسط **موسسه نظام راهبری فناوری اطلاعات**[۷] (ITGI) و راه‌اندازی‌شده توسط انجمن حسابرسی و کنترل سیستمهای اطلاعاتی برای حسابرسی، کنترل و راهبری فناوری اطلاعات است. کوبیت چارچوب جامعی از هدفهای کنترلی است که به حسابرسان فناوری اطلاعات، مدیران عامل و مدیران فناوری اطلاعات کمک می‌کند که سیستمهای فناوری اطلاعات خود را درک کرده و تصمیم بگیرند چه سطح امنیت و کنترلی کافی است. کوبیت، شامل رهنمودهای مدیریتی برای پر کردن شکافهای میان ریسکهای کسب‌وکار، نیازهای کنترلی و موضوعهای فنی است. یک مجموعه ابزار پشتیبانی است که این امکان را به مدیران می‌دهد که شکاف بین نیازهای کنترلی، موضوعهای فنی و ریسکهای کسب‌وکار را پر کنند. این ابزار جدید به تعیین فرایندهای نظارتی کسب‌وکارها با استفاده از **عوامل حیاتی موفقیت**[۸] (CSFs)، **شاخصهای کلیدی هدف کلان**[۹] (KGIs) و **شاخصهای کلیدی عملکرد**[۱۰] (KPIs) کمک می‌کنند. ماموریت آن تحقیق، توسعه، انتشار و ترویج یک مجموعه بین‌المللی، معتبر و به‌روز از هدفهای کلی کنترل فناوری اطلاعات پذیرفته‌شده برای استفاده روزمره به‌وسیله مدیران کسب‌وکار، مشاغل فناوری اطلاعات و مشاغل اطمینان‌بخشی است. اولین نسخه از کوبیت توسط موسسه نظام راهبری فناوری اطلاعات در سال ۱۹۹۶ عرضه شد. در سال ۱۹۹۸ و در نسخه دوم، «رهنمودهای مدیریتی» به آن افزوده شد. در سال ۲۰۰۰، نسخه سوم به‌صورت کاملتری ارائه شد. در سال ۲۰۰۳، یک نسخه اینترنتی در دسترس قرار گرفت. در دسامبر سال ۲۰۰۵، نسخه اولیه چاپ چهارم با افزودن بخش نظام راهبری فناوری اطلاعات عرضه شد. در ماه مه ۲۰۰۷، نسخه تجدیدنظرشده آن نسخه ۴/۱ چاپ شد. نسخه کوبیت ۵ برای ارائه در سال ۲۰۱۲ زمانبندی شده بود که پس از ارائه پیش‌نویس آن در سال ۲۰۱۱، در آوریل سال ۲۰۱۲ و پس از به‌روزآوری، ارائه شد. کوبیت ۵ به یکپارچگی چارچوبهای کوبیت ۴/۱، چارچوب **وال آی تی ۲/۰** (Val IT 2.0) و چارچوب **آی تی ریسک** (IT Risk) می‌پردازد و همچنین، به میزان درخورتوجهی **الگوی کسب‌وکار برای امنیت اطلاعات**[۱۱] (BMIS) و **چارچوب اطمینان‌بخشی فناوری اطلاعات**[۱۲] (ITAF) را ترسیم می‌کند (سروش، ۱۳۹۱). در این مقاله، قصد داریم به‌صورت اجمالی به مقایسه تفاوتهای میان کوبیت ۴/۱ و کوبیت ۵ بپردازیم.

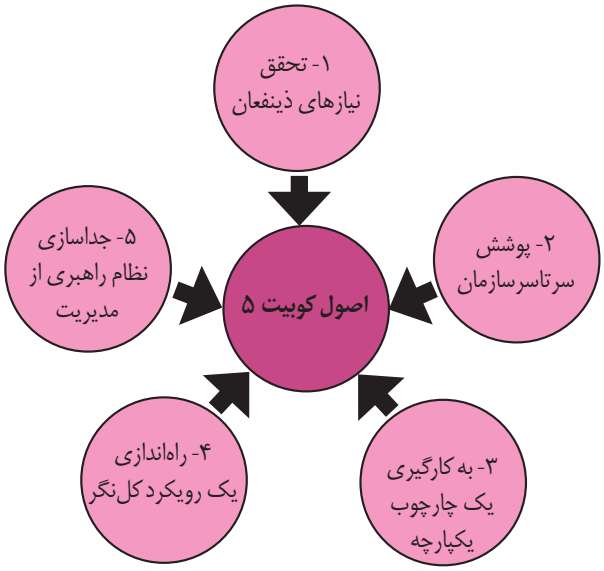
چارچوب کوبیت

ایـن چارچـوب شـیوه‌های مناسـب در کل چارچـوب فرایند و حـوزه را فراهـم می‌کند. جهتگیـری کسـب‌وکار کوبیت از پیونـد هدفهای کسـب‌وکار بـا هدفهای فنـاوری اطلاعات، ایجاد سـنجه‌ها و الگوهای رشد برای سـنجش موفقیت آنها و شناسـایی مسئولیتهای همبسته با کسـب‌وکار و افراد درگیر در فراینـد فناوری اطلاعات اسـت. تمرکز فرایند کوبیت ۴/۱ به‌وسـیله یک الگوی فرایندی نشان داده می‌شود که فناوری اطلاعات را به چهار حوزه (طرحریزی و سازماندهی، اکتساب و اجـرا، تحویـل و پشـتیبانی، و نظـارت و ارزیابـی) و ۳۴ فرایند همراسـتا با حوزه‌های مسـئولیتی طرح‌ریزی، ایجاد، اجـرا و نظارت تقسـیم می‌کند. هر فرایند به همـراه ورودیها و خروجی‌هـای فراینـد، فعالیتهای کلیـدی فرایند، هدفهای فراینـد، سـنجه‌های عملکـردی و یـک الگوی رشـد اولیه تعریف شـده است. چارچوب نظام راهبری فناوری اطلاعات با تعریـف و تنظیم هدفهای کسـب‌وکار با هدفهـای فناوری اطلاعات و فرایندهای فناوری اطلاعات پشـتیبانی می‌شود. به‌علاوه، کوبیت، چارچوب مورد استفاده بیشتر شرکتها برای تطبیق با ساربنز-آکسـلی است. شرکتهایی که در ایالات‌متحد تجـارت می‌کنند بایـد از قانون ساربنز-آکسـلی ۲۰۰۲ پیروی کنند (سـروش، ۱۳۹۱). در ادامه، بـه توصیف کلی کوبیت ۵ می‌پردازیـم و بهبودهایـی را که در آن نسـبت به کوبیت ۴/۱ ایجاد شده است به اختصار بیان می‌کنیم.

بهبودها در کوبیت ۵

کوبیـت ۵، محـک جدیـدی بـرای وظایـف، سـازمانها و ارائه‌کننـدگان خدمـات فنـاوری اطلاعـات اسـت. کوبیت ۵، مرحلـه بعـدی تکاملی در تعریـف چارچوب مدیریـت فناوری اطلاعات برای پشـتیبانی عملیات کسـب‌وکار سـازمان اسـت که عـلاوه بر نمایش نیازهای عملیاتی، دسـتیابی به هدفهای راهبردی را ممکن می‌سـازد. امـروزه، اطلاعات و فناوریهای مرتبط بیش از پیش نیاز به راهبری، مدیریت و عملیاتی شدن از طریق یک الگوی فرایندی یکپارچه به روشی کل‌نگر داشته که پوشـش کاملی از نقشـها، مسـئولیتها و رویه‌های مورد نیاز را فراهـم می‌کنـد (IT Governance Network, 2011). بهبودهای چشـمگیری در کوبیت جهت اسـتقرار آن به‌عنوان الگویـی برای نظام راهبـری فناوری اطلاعات شـرکت ایجاد شـده اسـت. **تصویر ۱**، اصول جدید **نظام راهبری فناوری اطلاعات سـازمان**[۱۳] (GEIT) در کوبیت ۵ را نشـان می‌دهد (ISACA, 2012).

تصویر ۱- اصول کوبیت ۵



چارچوبهای وال آی‌تی و آی‌تی ریسک مبتنی بر این اصول هستند. بازخوردها نشان داده که اصول به سادگی درک‌پذیرند و در متن سازمان قرار می‌گیرند و امکان کسب ارزش از راهنمای پشتیبانی‌کننده را کاراتر می‌سازند. همچنین، **استاندارد ایزو/آی‌ایی‌سـی ۳۸۵۰۰** (ISO/IEC 38500)، اصول را برای دسـتیابی به سـود بازاری همان کار به یکدیگر پیوند می‌دهد؛ اگرچه این اصول در این استاندارد و کوبیت ۵ یکسان نیستند.

به علاوه، کوبیت ۴/۱، **توانمندسـازها**[۱۴] را نداشـت، البته آنهـا به‌صورت واضـح یا مفهومی وجود داشـتند؛ اما تحت نام توانمندسـازها شناخته نمی‌شدند. **تصویر ۲**، توانمندسازها در کوبیت ۵ را نشان می‌دهد (ISACA, 2012).

همان‌طـور کـه در **تصویـر ۲** دیـده می‌شـود، اطلاعات، زیرسـاخت، نرم‌افزارهـای کاربردی (خدمات) و افـراد (افراد،

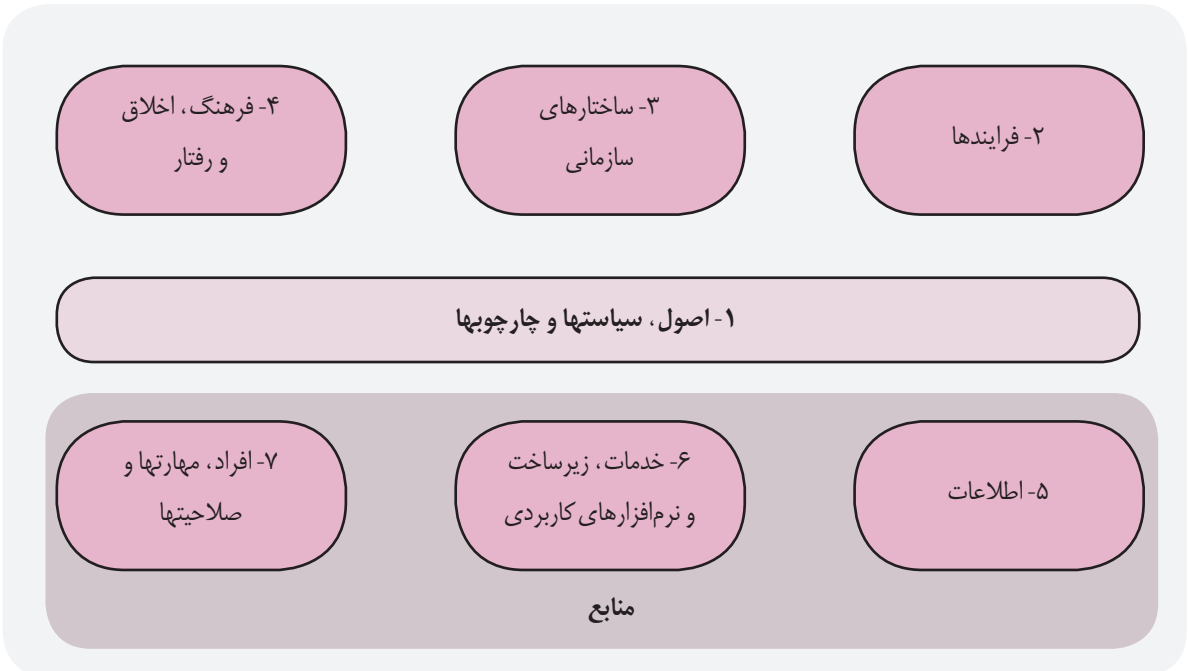
مهارتها و صلاحیتها) منابع کوبیت ۴/۱ بودند. اصول، سیاستها و چارچوبها در تعداد کمی از فرایندهای کوبیت ۴/۱ ذکر شده بودند. فرایندها بر استفاده از کوبیت ۴/۱ متمرکز بودند. ساختار سازمانی از طریق نقشهای **مسئول**، **پاسخگو**، **مشاور و مطلع**[۱۵] (RACI) و تعریفهایشان استنتاج شده بود. موارد مربوط به فرهنگ، اخلاق و رفتار نیز در تعداد کمی از فرایندهای کوبیت ۴/۱ ذکر شده بودند (ISACA, 2012).

براساس تحقیقی در سال ۲۰۱۱، کوبیت در سطحی بالاتر قرار می‌گیرد و با شیوه‌های مناسب و سایر استانداردهای فناوری اطلاعات همچون **کوزو**[۱۶] (COSO)، **مدرک آی‌تی‌آی‌ال**[۱۷] (ITIL)، **ایزو/آی‌ایی‌سی ۱۷۷۹۹** (ISO/IEC 17799)، **ایزو/آی‌ایی‌سی ۲۰۰۰۰** (ISO/IEC 20000)، **پیکره دانش مدیریت پروژه**[۱۸] (PMBOK)، **یکپارچگی مدل بلوغ قابلیت**[۱۹] (CMMI)، **چارچوب معماری گروه باز**[۲۰] (TOGAF) و **شورای آزمون موسسه‌های مالی فدرال**[۲۱] (FFIEC) به‌صورت دقیق تنظیم و هماهنگ شده است.

در این تحقیق، نگاشتی از مقایسه فرایندهای کوبیت ۴/۱ با سایر استانداردها صورت گرفته است. نتایج نشان می‌دهد که کوزو تنها ۲۴ فرایند، مدرک آی‌تی‌آی‌ال تنها ۱۶ فرایند، ایزو/آی‌ایی‌سی ۱۷۷۹۹ تنها ۲۴ فرایند، ایزو/آی‌ایی‌سی ۲۰۰۰ تنها ۲۵ فرایند، پیکره دانش مدیریت پروژه تنها ۵ فرایند، یکپارچگی مدل بلوغ قابلیت تنها ۱۱ فرایند، چارچوب معماری گروه باز تنها ۵ فرایند، **کنترلهای امنیتی توصیه‌شده برای سازمانها و سیستمهای اطلاعاتی فدرال** NIST (800-53) نیز تنها ۱۱ فرایند از ۳۴ فرایند کوبیت را پوشش می‌دهند. در میان چارچوبها و استانداردهای موجود، تنها شورای آزمون موسسه‌های مالی فدرال کلیه ۳۴ فرایند کوبیت را پوشش می‌دهد؛ اما دو حوزه اکتساب و اجرا و تحویل و پشتیبانی از گستردگی و عمق کمتری نسبت به کوبیت برخوردار است (ISACA, 2012).

علاوه بر این، برخلاف نسخه قبلی آن (کوبیت ۴/۱) و مدرک **آی‌تی‌آی‌ال نسخه ۳** (ITIL V3)، چارچوب کوبیت ۵ هر سه سطح چارچوب نظام راهبری فناوری اطلاعات را

تصویر ۲- توانمندسازها در کوبیت ۵



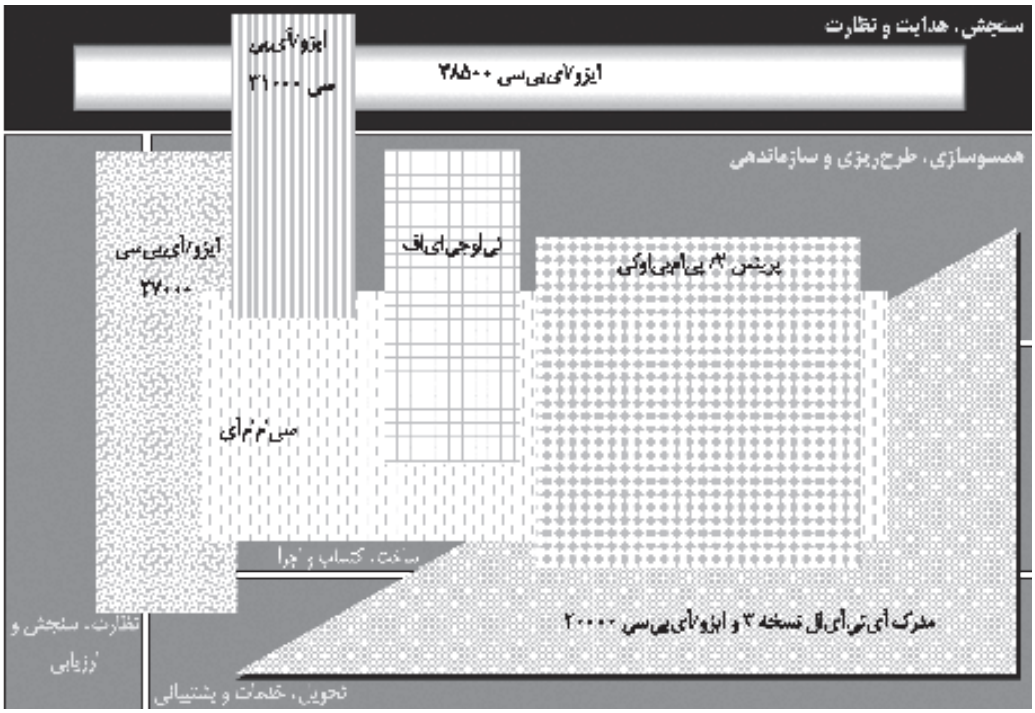
نشـان می‌دهـد. هم کوبیـت ۴/۱ و هم مـدرک آی‌تی‌آی‌ال نسـخه ۳، الگوهایی فرایندی هسـتند که رویه‌هـای فناوری اطلاعـات را در سـطح عملیاتـی مبتنـی بـر منبـع مفیدی از رویه‌های مناسـب تشـریح می‌کنند. به هر حال، کوبیت ۴/۱ و مدرک آی‌تی‌آی‌ال نسـخه ۳ رویه‌های مدیریتی لازم برای هدایـت را نداشـته و از منابع فناوری اطلاعـات به‌طور کارا و اثربخـش اسـتفاده نمی‌کنند. به‌علاوه، کوبیـت ۴/۱ و مدرک آی‌تـی‌آی‌ال نسـخه ۳ فرایندهـای نظـام راهبـری شـرکت لازم بـرای هدایـت و کنترل اسـتفاده از فنـاوری اطلاعات را تشـریح نمی‌کنند (IT Governance Network, 2011). **تصویر۳**، میزان پوشـش کوبیت ۵ شامل سایر استانداردها و چارچوبها را نمایش می‌دهد (ISACA, 2012).

همان‌طور که در **تصویر۳** مشـاهده می‌شـود، در کوبیت ۵ سعی شده است که کلیه روشهای موجود در سایر استانداردها و چارچوبها در نظر گرفته شوند تا چارچوب حاصل پوشش‌دهنده کل فرایندهای فناوری اطلاعات سازمان و به‌روز و کامل باشد. بهبودهـا در کوبیت ۵ شـامل بازسـازی تشـریح فرایندها، شناسـایی رویه‌هـای اساسـی واقعـی در هر فرایند و تشـریح فعالیتهای کلیدی در هر رویه اساسـی اسـت. آبشـار هدفهای کلان در کوبیـت ۵ جهت پشـتیبانی نیازهـای ذینفعان دوباره بررسـی و به‌روز شـده اسـت. مهمتریـن تغییـر در کوبیت ۵، سـازماندهی مجدد چارچوب از یک الگـوی فرایندی فناوری اطلاعات به یک چارچوب نظـام راهبری فناوری اطلاعات با مجموعه‌ای از رویه‌های نظام راهبری برای فناوری اطلاعات، یک سیسـتم مدیریتی بـرای بهبود مـداوم فعالیتهای فناوری اطلاعـات و یک الگـوی فرایندی همراه با رویه‌های اساسـی است (IT Governance Network, 2011).

ارتقا از کوبیت ۴/۱ به کوبیت ۵

کوبیت ۵ (کوبیت ۴/۱ به‌علاوه چارچوب وال آی‌تی و چارچوب آی‌تی ریسـک) براسـاس الگوی فرایندی که پیـش از این در نسخه‌های قبلی کوبیت تعریف شد، ایجاد شده است. تغییری تکاملی اسـت کـه فرایندهـای موجـود را از طریـق ترکیب و تخصیـص مجدد رویه‌هـا در محـدوده فرایندهـای موجود و

تصویر ۳- میزان پوشش کوبیت ۵ شامل سایر استانداردها و چارچوبها



در کوبیت ۵ سعی شده است که کلیه روشهای موجود در سایر استانداردها و چارچوبها در نظر گرفته شوند تا چارچوب حاصل پوشش‌دهنده کل فرایندهای فناوری اطلاعات سازمان و به‌روز و کامل باشد

در نظـر گرفتن فرایندهـا و رویه‌های اضافی بـرای مدیریت و راهبری فناوری اطلاعات به‌صورت معقولی توجیه کرده اسـت (IT Governance Network, 2011).

پیـش از ایـن، سـازمانها در سـطح بلـوغ حداقـل ۲ (اندازه‌گیری‌شـده با استفاده از ایزو ۱۵۵۰۴) با ارتقای به‌نسبت آسانی روبه‌رو می‌شدند. اگرچه، احتمال دارد سازمانها در سطح بلوغ ۱ در ارتقا از کوبیت ۴/۱ به کوبیت ۵ با چالش روبه‌رو شوند. سـازمانهایی که در حال حاضر در سـطح بلوغ ۱ یا کمتر (یعنی بدون فرایندهای به‌درستی تعریف‌شده) عمل می‌کنند، ممکن اسـت آن را آسـانتر یافته و با صرف هزینه بیشتری کوبیت ۵ را انتخاب و از نو با اسـتفاده از چارچوب جدید کوبیت ۵ آغاز کنند (IT Governance Network, 2011).

البته، در جایی که سـازمان سـرمایه‌گذاریهای چشـمگیری را در اجـرای فرایندهای کوبیت ۴/۱ انجام داده، ممکن اسـت مطلـوب باشـد که ابتدا ایـن عملیات قبل از ادغـام فرایندهای کوبیـت ۴/۱ برای همسوسـازی با فرایندهـای کوبیت ۵ کامل شـود. تصویـر ۴، الگـوی مرجع فراینـدی کوبیت ۵ را نشـان می‌دهد (ISACA, 2012).

همان‌طـور که در **تصویر ۴** مشـاهده می‌شـود، فرایندهای نظام راهبری فناوری اطلاعات از فرایندهای مدیریت فناوری اطلاعات سازمان جدا شده‌اند. از این‌رو، برای بیشتر سازمانها معرفی سیسـتم مدیریتی و چارچوب نظام راهبری کاملاً جدید خواهـد بود. شـرط لازم کار این اسـت که مدیـران رویکردی سـاختاریافته را جهت چگونگی طرح‌ریزی، سازماندهی، اداره و کنتـرل منابع و ارائه عملکرد مورد نیاز تدوین کنند. در بخش بعد، به‌صورت تفصیلی‌تر به تشـریح تغییرهای ایجادشـده در فرایندهای کوبیت خواهیم پرداخت.

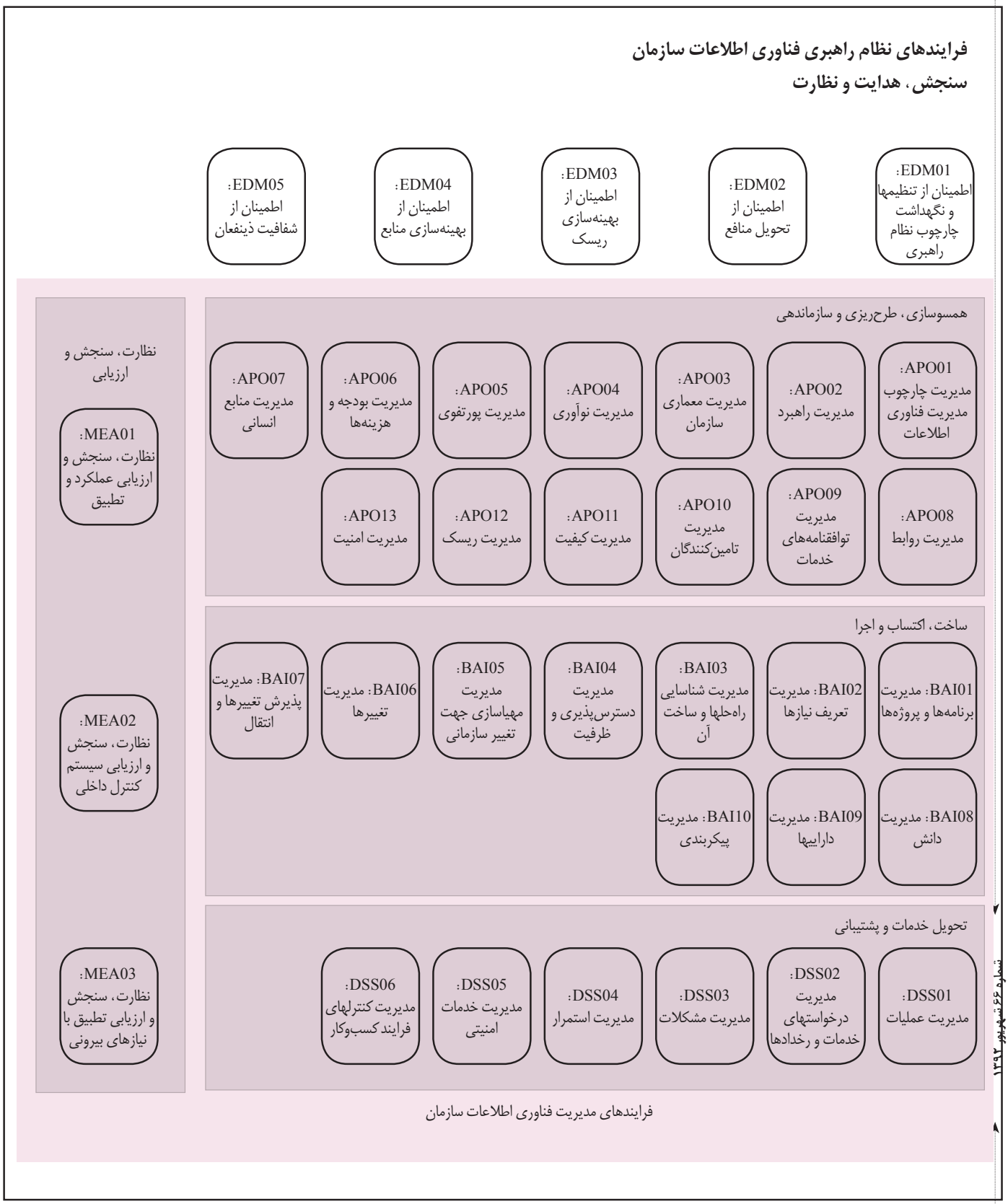
خلاصه تغییرهای کوبیت ۴/۱ به کوبیت ۵

در کوبیت ۵، پنج فرایند نظام راهبری جدید معرفی شـده اسـت کـه رویکردهای نظام راهبری کوبیت ۴/۱، چارچوب وال آی‌تی و چارچوب آی‌تی ریسـک را به‌کار بسـته و بهبود می‌دهد. این راهنما به سازمانها در پالایش و تقویت بیشتر رویه‌ها و فعالیتهای نظـام راهبری فنـاوری اطلاعات سـازمان در سـطح مدیریت اجرایـی کمـک می‌کنـد. از یکپارچگـی نظام راهبـری فناوری اطلاعات سـازمان با رویه‌هـای موجود نظام راهبری سـازمان پشـتیبانی کرده و با ایزو/آی‌یی‌سی ۳۸۵۰۰ همسو می‌شود. در ادامه، مقایسـه‌ای بین فرایندهای کوبیت ۴/۱ و کوبیت ۵ انجام گرفته و تغییرهای ایجادشده به‌صورت طبقه‌بندی‌شده بیان شده است (IT Governance Network, 2011).

* فرایندهای کوبیت ۴/۱ که در کوبیت ۵ دوباره جایابی شـده یا تغییر نام داده شده‌اند، عبارتند از:

- **پـی‌او۰۱** (PO01) بـه **ای‌پـی‌او۰۲** (APO02) (مدیریت راهبرد)
- **پـی‌او۰۲** (PO02) بـه **ای‌پـی‌او۰۳** (APO03) (مدیریت معماری سازمان)
- **پـی‌او۰۸** (PO08) بـه **ای‌پـی‌او۱۱** (APO11)(مدیریت کیفیت)

تصویر ۴- الگوی مرجع فرایندی کوبیت ۵



فرایندهای مدیریت فناوری اطلاعات سازمان

• **پی‌او۰۹** (PO09) به **ای‌پی‌او۱۲** (APO12) (مدیریت ریسک)

• **پی‌او۱۰** (PO10) به **بی‌ای‌آی۰۱** (BAI01) (مدیریت برنامه‌ها و پروژه‌ها)

• **ای‌آی۰۱** (AI01) به **بی‌ای‌آی۰۲** (BAI02) (مدیریت تعریف نیازها)

• **ای‌آی۰۵** (AI05) به **ای‌پی‌او۱۰** (APO10) (مدیریت تامین‌کنندگان)

• **ای‌آی۰۶** (AI06) به **بی‌ای‌آی۰۶** (BAI06) (مدیریت تغییرها)

• **ای‌آی۰۷** (AI07) به **بی‌ای‌آی۰۷** (BAI07) (مدیریت پذیرش تغییرها و انتقال)

• **دی‌اس۰۱** (DS01) به **ای‌پی‌او۰۹** (APO09) (مدیریت توافقنامه‌های خدمات)

• **دی‌اس۰۳** (DS03) به **بی‌ای‌آی۰۴** (BAI04)(مدیریت دسترس‌پذیری و ظرفیت)

• **دی‌اس۰۴** (DS04) به **دی‌اس‌اس۰۴** (DSS04) (مدیریت استمرار)

• **دی‌اس۰۹** (DS09) به **بی‌ای‌آی۱۰** (BAI10) (مدیریت پیکربندی)

• **دی‌اس۱۰** (DS10) به **دی‌اس‌اس۰۳** (DSS03) (مدیریت مشکلات)

• **ام‌ایی۰۱** (ME01) به **ام‌ایی‌ای۰۱** (MEA01) (نظارت، سنجش و ارزیابی عملکرد و تطبیق)

• **ام‌ایی۰۲** (ME02) به **ام‌ایی‌ای۰۲** (MEA02) (نظارت، سنجش و ارزیابی سیستم کنترل داخلی)

• **ام‌ایی۰۳** (ME03) به **ام‌ایی‌ای۰۳** (MEA03) (نظارت، سنجش و ارزیابی تطبیق با نیازهای بیرونی)

* فرایندهای کوبیت ۴/۱ که در کوبیت ۵ ادغام شده‌اند، عبارتند از:

• **ای‌آی۰۲** (AI02) با **ای‌آی۰۳** (AI03) (اکتساب و نگهداری نرم‌افزار کاربردی با اکتساب و نگهداری زیرساخت فناوری) ادغام و **بی‌ای‌آی۰۳** (BAI03) حاصل شده است.

• **ای‌آی۰۵** (AI05) با **دی‌اس۰۲** (DS02) (مدیریت تدارک منابع با مدیریت خدمات شخص ثالث) ادغام و **ای‌پی‌او۱۰** (APO10) حاصل شده است.

• **دی‌اس۰۶** (DS06) با **پی‌او۰۵** (PO05) (شناسایی و تخصیص هزینه‌ها با مدیریت سرمایه‌گذاری) ادغام و **ای‌پی‌او۰۶** (APO06) حاصل شده است.

• **دی‌اس۰۷** (DS07) با **پی‌او۰۷** (PO07) (تعلیم و تربیت کاربران با مدیریت منابع انسانی) ادغام و **ای‌پی‌او۰۷** (APO07) حاصل شده است.

• بخشی از **دی‌اس۰۹** (DS09) با **دی‌اس۰۸** (DS08) (مدیریت پیکربندی با مدیریت رخدادها و میز خدمت‌دهی) ادغام و **دی‌اس‌اس۰۲** (DSS02) حاصل شده است.

• بخشی از **دی‌اس۱۱** (DS11)، **دی‌اس۱۲** (DS12) و **دی‌اس۱۳** (DS13) با بخش عمده‌ای از **دی‌اس۰۵** (DS05) (مدیریت داده‌ها، مدیریت محیط فیزیکی و مدیریت عملیات با اطمینان از امنیت سیستم‌ها) ادغام و **دی‌اس‌اس۰۵** (DSS05) حاصل شده است.

• بخشی از **دی‌اس۱۱** (DS11) و **دی‌اس۱۲** (DS12) با بخش عمده‌ای از **دی‌اس۱۳** (DS13) (مدیریت داده‌ها و مدیریت محیط فیزیکی با مدیریت عملیات) ادغام و **دی‌اس‌اس۰۱** (DSS01) حاصل شده است.

* فرایندهای کوبیت ۴/۱ که از کوبیت ۵ حذف یا در سایر فرایندها تقسیم شده‌اند، عبارتند از:

• **پی‌او۰۳** (PO03) در **ای‌پی‌او۰۱** (APO01)، **ای‌پی‌او۰۲** (APO02)، **ای‌پی‌او۰۳** (APO03)، **ای‌پی‌او۰۴** (APO04)

• **دی‌اس۰۸** (DS08) به **دی‌اس‌اس۰۲** (DSS02) (حذف میز خدمات مطابق با مدرک آی‌تی‌آی‌ال نسخه ۳)

• **دی‌اس۱۱** (DS11) در **دی‌اس‌اس۰۱** (DSS01)، **دی‌اس‌اس۰۴** (DSS04)، **دی‌اس‌اس۰۵** (DSS05) و **دی‌اس‌اس۰۶** (DSS06)

• **دی‌اس۱۲** (DS12) در **دی‌اس‌اس۰۱** (DSS01) و **دی‌اس‌اس۰۵** (DSS05)

* فرایندهای جدید در کوبیت ۵، عبارتند از:

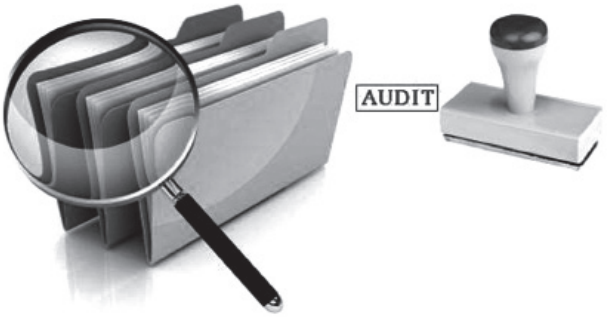
• **ایی‌دی‌ام۰۱** (EDM01): تنظیم و نگهداشت چارچوب نظام راهبری (بخشی از **پی‌او۰۳** (PO03) و **ام‌ایی۰۴** (ME04))

• **ایی‌دی‌ام۰۲** (EDM02): اطمینان از تحویل منافع (بخشی از **پی‌او۰۱** (PO01) و امایی ۰۴)
• **ایی‌دی‌ام۰۳** (EDM03): اطمینان از بهینه‌سازی ریسک (بخشی از **پی‌او ۰۶** (PO06)، **پی‌او۰۹** (PO09) و امایی۰۴)
• **ایی‌دی‌ام۰۴** (EDM04): اطمینان از بهینه‌سازی منابع (بخشی از امایی۰۴)
• **ایی‌دی‌ام۰۵** (EDM05): اطمینان از شفافیت ذینفعان (بخشی از امایی۰۴)
• **ایی‌پی‌او۰۱** (APO01): مدیریت چارچوب مدیریت فناوری اطلاعات(بخش اندکی از **پی‌او۰۲** (PO02)، **پی‌او۰۳** (PO03)، **پی‌او۰۷** (PO07)، **پی‌او۰۹** (PO09) و بخش عمده‌ای از **پی‌او۰۴** (PO04)، **پی‌او۰۶** (PO06))
• **ای‌پی‌او۰۴** (APO04): مدیریت نوآوری (بخشی از **پی‌او۰۳** (PO03))
• **ای‌پی‌او۰۵** (APO05): مدیریت پورتفوی (بخشی اندکی از **پی‌او۰۱** (PO01) و **پی‌او۰۵** (PO05))
• **ای‌پی‌او۰۸** (APO08): مدیریت روابط (بخش اندکی از **پی‌او۰۴** (PO04))
• **ای‌پی‌او۱۳** (APO13): مدیریت امنیت (بخشی از **دی‌اس۰۵** (DS05))
• **بی‌ای‌آی۰۸** (BAI08): مدیریت دانش (بخش عمده‌ای از

جدول ۱- معادلهای کوبیت ۵ نسبت به معیارهای اطلاعاتی کوبیت ۴/۱

معیارهای اطلاعاتی کوبیت ۴/۱	معادل کوبیت ۵
اثربخشی	اطلاعات کارا خواهد بود؛ اگر نیازهای مصرف‌کننده اطلاعات را که از اطلاعات برای کار مشخصی استفاده می‌کند، محقق سازد. اگر مصرف‌کننده اطلاعات بتواند کار را با اطلاعات انجام دهد، آنگاه اطلاعات کاراست. این مطابق با هدفهای کلان کیفیت اطلاعات یعنی مقدار مناسب، ارتباط، درک‌پذیر بودن، تفسیرپذیر بودن و بیطرفی است.
کارایی	درحالی‌که اثربخشی، اطلاعات را به‌عنوان محصول در نظر می‌گیرد، کارایی بیشتر به فرایند کسب و استفاده از اطلاعات مربوط می‌شود؛ از این‌رو، از منظر «اطلاعات به‌عنوان یک خدمت» نگاه می‌کند. اگر اطلاعاتی که نیازهای مصرف‌کننده اطلاعات را محقق می‌کند به روشی ساده کسب و استفاده شود (یعنی، منابع اندکی را به کار بگیرد- تلاش فیزیکی، تلاش شناختی، زمان و پول)، آنگاه استفاده از اطلاعات کارا خواهد بود. این مطابق با هدفهای کلان کیفیت اطلاعات یعنی باورپذیری، دسترسی، سادگی عملیات و شهرت است.
یکپارچگی	اگر اطلاعات یکپارچگی دارد، آنگاه بدون خطا و کامل است. این مطابق با هدفهای کلان کیفیت اطلاعات یعنی تمامیت و دقت است.
اطمینان‌پذیری	اغلب، اطمینان‌پذیری مترادف با دقت در نظر گرفته می‌شود؛ هر چند، می‌توان گفت که اطلاعاتی درخور اطمینان است که صحیح و معتبر باشد. اطمینان‌پذیری در مقایسه با یکپارچگی، غیرعینی‌تر است، بیشتر به ادراک مربوط می‌شود و فقط واقعی نیست. مطابق با هدفهای کلان کیفیت اطلاعات یعنی باورپذیری، شهرت و بیطرفی است.
دسترس‌پذیری	دسترس‌پذیری، یکی از هدفهای کلان کیفیت اطلاعات تحت عنوان دسترسی و امنیت است.
محرمانگی	محرمانگی، مطابق با هدف کلان کیفیت اطلاعات در دسترس طبقه‌بندی شده است.
تطبیق	تطبیق بدین معنی است که اطلاعات باید با ویژگیهایی که به‌وسیله هر هدف کلان مربوط به کیفیت اطلاعات که براساس نیازها پوشش داده می‌شود، مطابقت داشته باشند. تطبیق با مقررات، بیشتر مواقع یک هدف کلان یا احتیاج به استفاده از اطلاعات است؛ نه آنقدر مربوط به کیفیت ذاتی اطلاعات.

مهمترین تغییر در کوبیت ۵ سازماندهی مجدد چارچوب از الگوی فرایندی فناوری اطلاعات به چارچوب نظام راهبری فناوری اطلاعات با مجموعه‌ای از رویه‌های نظام راهبری برای فناوری اطلاعات سیستم مدیریتی برای بهبود مداوم فعالیتهای فناوری اطلاعات و الگوی فرایندی همراه با رویه‌های اساسی است



ای‌آی۰۴ (AI04))

• **بی‌ای‌آی۰۵** (BAI05): مدیریت مهیاسازی جهت تغییر سازمانی (بخش اندکی از **ای‌آی۰۴** (AI04) و **ای‌آی۰۷** (AI07))

• **بی‌ای‌آی۰۹** (BAI09): مدیریت داراییها (بخش اندکی از **دی‌اس۱۳** (DS13))

• دی‌اس‌اس۰۶: مدیریت کنترلهای فرایند کسب‌وکار (بخشی از دی‌اس۱۱ و پی‌او۰۴)

علاوه بر این موارد، **شیوه‌های کلیدی مدیریت**[۲۲] چارچوب وال آی‌تی در فرایندهای ایی‌دی‌ام۰۱، ایی‌دی‌ام ۰۲، ای‌پی‌او۰۱، ای‌پی‌او۰۲، ای‌پی‌او۰۵، ای‌پی‌او۰۶، **ای‌پی‌او۰۷** (APO07)، **بی‌ای‌آی۰۱** (BAI01) و **بی‌ای‌آی۱۰** (BAI10) و شیوه‌های کلیدی مدیریت چارچوب مدیریت ریسک در فرایندهای ایی‌دی‌ام۰۱، ایی‌دی‌ام۰۳، ایی‌دی‌ام۰۴، ایی‌پی‌او۰۷، **ای‌پی‌او۱۲** (APO12) در کوبیت ۵ افزوده شده‌اند.

به این ترتیب، اکنون فرایندهای کوبیت۵ کل کسب‌وکار و فعالیتهای فناوری اطلاعات را پوشش می‌دهند؛ به‌طوری که پوشش جامعتر و کاملتری از رویه‌های انعکاس فراگیر نوع استفاده از فناوری اطلاعات در کل سازمان ارائه می‌کنند. همچنین، میزان درگیری، مسئولیتها، پاسخگوییهای ذینفعان کسب‌وکار در استفاده از فناوری اطلاعات را واضحتر و شفافتر می‌سازد (ISACA, 2012).

مقایسه بین الگوی اطلاعاتی کوبیت ۵ و معیارهای اطلاعاتی کوبیت ۴/۱

چگونگی ارتباط ۷ معیار اطلاعاتی کوبیت ۴/۱ (اثربخشی، کارایی، یکپارچگی، قابلیت اطمینان، دسترس‌پذیری، محرمانگی و تطبیق) با ابعاد و طبقه‌های کیفیت اطلاعات در راه‌اندازهای اطلاعاتی کوبیت ۵ نیز معادلسازی شده است. **جدول ۱** شامل دو ستون است که ستون اول هر یک از ۷ معیار اطلاعاتی کوبیت ۴/۱ و ستون دوم، معادلهای کوبیت ۵ یعنی هدفهای کلان راه‌انداز اطلاعاتی متناظر را نشان می‌دهد.

این جدول نشان می‌دهد که کلیه معیارهای اطلاعاتی کوبیت ۴/۱، توسط کوبیت ۵ پوشش داده می‌شوند؛ اگرچه، الگوی اطلاعاتی کوبیت ۵ امکان تعریف مجموعه‌ای از معیارهای اضافی را نیز به‌منظور افزودن ارزش به معیارهای کوبیت ۴/۱، می‌دهد (ISACA, 2012).

اجرای کوبیت ۵

کوبیت ۵، دربرگیرنده یک الگوی عملیاتی و یک زبان مشترک برای کلیه بخشهای کسب‌وکار درگیر در فعالیتهای فناوری اطلاعات است. همچنین، چارچوبی را برای سنجش و پایش عملکرد فناوری اطلاعات، یکپارچه‌سازی بهترین رویه‌های مدیریتی، نظام راهبری و برقراری ارتباط با ذینفعان فراهم می‌کند. چارچوب کوبیت ۵ شامل یک الگوی مرجع فرایندی است و فرایندهای نظام راهبری و مدیریتی را تعریف و تشریح می‌کند. الگوی مرجع فرایندی، کلیه فرایندهای بر پا شده در سازمان در رابطه با فعالیتهای فناوری اطلاعات را به‌عنوان یک الگوی مرجع مشترک و درک‌پذیر برای مدیران کسب‌وکار و فناوری اطلاعات عملیاتی، شامل می‌شود (IT Governance Network, 2011).

فعالیتهای کوبیت ۵، معادل با رویه‌های کنترلی کوبیت ۴/۱ و رویه‌های مدیریتی چارچوب وال آی‌تی و چارچوب آی‌تی ریسک هستند. کوبیت ۵، هدف و مفاهیم سنجش مشابهی را همچون کوبیت ۴/۱، چارچوب وال آی‌تی و چارچوب آی‌تی ریسک دنبال می‌کند. اما اینها به هدفهای سازمان، هدفهای مرتبط با فناوری اطلاعات و هدفهای فرایند که منعکس‌کننده نمایی از سطح سازمان هستند، تغییر نام داده می‌شوند. کوبیت ۵، نمونه‌هایی از هدفهای کلان و سنجه‌ها را در سطوح عملی سازمان، فرایندی و مدیریتی ارائه می‌کند. این تغییری است که نسبت به کوبیت ۴/۱، چارچوب وال آی‌تی و چارچوب آی‌تی ریسک ایجاد شده است؛ زیرا آنها باید یک سطح پایینتر می‌رفتند. کوبیت ۵، ورودی‌ها و خروجی‌ها را برای هر رویه مدیریتی فراهم می‌کند؛ درحالی‌که کوبیت ۴/۱ تنها این موارد را در سطح فرایند فراهم می‌کرد. همچنین، راهنمای تفصیلی اضافی را برای طراحی فرایندها جهت در نظر گرفتن محصولات کاری حیاتی و کمک به یکپارچگی فرایند داخلی فراهم می‌کند (ISACA, 2012).

کوبیت ۵، رویکرد **الگوسازی بلوغ قابلیت**[۲۳] (CMM) را برای کوبیت ۴/۱، چارچوب وال آی‌تی و چارچوب آی‌تی ریسک ادامه نمی‌دهد. کوبیت ۵، با یک رویکرد ارزیابی قابلیت فرایند جدید مبتنی بر **ایزو/آی‌ایی‌سی ۱۵۵۰۴** (ISO/IEC 15504) و **برنامه ارزیابی کوبیت**[۲۴] که پیش از این برای کوبیت ۴/۱ به‌عنوان راهکار دیگری مطابق با رویکرد الگوسازی بلوغ قابلیت برپا شده است، پشتیبانی می‌شود. رویکردهای مبتنی بر الگوسازی بلوغ قابلیت به کار گرفته‌شده برای چارچوبهای کوبیت ۴/۱، چارچوب وال آی‌تی و چارچوب آی‌تی ریسک با رویکرد ایزو/آی‌ایی‌سی ۱۵۵۰۴ همساز نیستند؛ زیرا این روشها از مقیاسهای اندازه‌گیری و ویژگیهای متفاوتی استفاده می‌کنند. خواسته کاربران کوبیت ۴/۱، چارچوب وال آی‌تی و چارچوب آی‌تی ریسک ادامه دادن با رویکرد مبتنی بر الگوسازی بلوغ قابلیت است. آنها به عنوان رویکردی موقتی یا دائمی می‌توانند از راهنمای کوبیت ۵ استفاده کنند؛ اما باید جدول ویژگی عمومی کوبیت ۴/۱ را بدون الگوهای بلوغ سطح بالا به کار گیرند (ISACA, 2012).

نتیجه‌گیری

با این احوال می‌توان گفت که الگوی فرایندی کوبیت ۵، الگویی کامل و جامع است که سازمان باید آن را پس از گرفتن نیازهای داخلی کسب‌وکار، فشارهای خارجی کسب‌وکار و انتظارهای مختلف ذینفعان سازمان و وظیفه فناوری اطلاعات با نیازهای خاص خودش متناسب کند.

اجرای کوبیت ۵ با تعیین اینکه کدام علاقه‌های ذینفعان اولویت دارند، انتظارهای آنها چه چیزهایی است، قابلیتهای کاری فناوری اطلاعات برای براورده‌سازی این انتظارها چیست و چه کسی برای انجام آن پاسخگو است و موارد از این دست، آغاز می‌شود. شرط لازم تحقق این موضوع، کسب دانش درباره فرایندهای اساسی و سیستم مدیریتی خواهد بود

کوبیت ۵
دربرگیرنده یک الگوی عملیاتی
و یک زبان مشترک برای
کلیه بخشهای کسب‌وکار
درگیر در فعالیتهای فناوری اطلاعات است
همچنین چارچوبی را برای
سنجش و پایش عملکرد فناوری اطلاعات
یکپارچه‌سازی بهترین
رویه‌های مدیریتی
نظام راهبری و برقراری
ارتباط با ذینفعان فراهم می‌کند

که بتوانـد کار فناوری اطلاعات را در خصوص تحویل خدمات و عملکرد مورد انتظار، پشـتیبانی نمایـد(IT Governance Network, 2011). به‌علاوه، اجرای کوبیت ۵ موضوعهایی همچـون تثبیـت موقعیـت نظام راهبـری فنـاوری اطلاعات سـازمان در سازمان، اتخاذ مراحل ابتدایی به‌سوی بهبود نظام راهبری فناوری اطلاعات سـازمان، چالشـهای اجرا و عوامل موفقیـت، راه‌انـدازی تغییر رفتاری و سـازمانی مرتبط با نظام راهبری فناوری اطلاعات سازمان، اجرای بهبود دائمی شامل مدیریت برنامه و راه‌اندازی تغییر، استفاده از کوبیت ۵ و اجزای آن را پوشش می‌دهد.

پانوشتها:

1- Information Systems Audit and Control Association (ISACA)
2- Certified Information Systems Auditor (CISA)
3- Certified Information Security Manager (CISM)
4- Certified in the Governance of Enterprise IT (CGEIT)
5- Certified in Risk and Information Systems Control (CRISC)
6- Control Objective for Information and Related Technology (COBIT)
7- Information Technology Governance Institute
8- Critical Success Factors (CSF)
9- Key Goal Indicators (KGI)
10- Key Performance Indicators (KPI)
11- Business Model for Information Security (BMIS)
12- Information Technology Assurance Framework (ITAF)
13- Governance of Enterprise IT (GEIT)
14- Enablers
15- Responsible, Accountable, Consulted and Informed (RACI)
16- Committee of Sponsoring Organization
17- IT Infrastructure Library (ITIL)
18- Project Management Body of Knowledge (PMBOK)
19- Capability Maturity Model Inegration (CMMI)
20- The Open Group Architecture Framework (TOGAF)
21- Federal Financial Institutions Examination Council (FFIEC)
22- Key Management Practices
23- Capability Maturity Modeling
24- COBIT Assessment Programme

منابع:

- سـروش علیرضـا، **ضرورت حسابرسـی فنـاوری اطلاعـات در هزاره جدید**، همایش ملی حسابداری و حسابرسی، دانشگاه سیستان‌وبلوچستان، زاهدان، ایران، ۱۳۹۱، صص ۴۱۳-۳۹۷
- ISACA, **COBIT 5: A Business Framework for the Governance and Management of Enterprise IT**, 2012
- ISACA, **COBIT Mapping: Overview of International IT Guidance**, 3rd Edition, 2011
- ISACA, **Comparing COBIT 4.1 and COBIT 5**, www.isaca.org/COBIT/Documents/Compare-with-4.1.pdf, 2012
- IT Governance Network, **Summary of Differences between COBIT 4.1 and COBIT 5**, http://www.qualified-audit-partners.be/user_files/COBIT5forAuditors/Summary_of_differences_between_COBIT_4_1_and_COBIT_5___2012___IT_Governance_Network.pdf, 2011