

COBIT Framework Defect Cover Using Val IT and Risk IT to Implement IT Governance in Organization

پوشش ضعف چارچوب COBIT با استفاده از چارچوب های Val IT و Risk IT جهت برقراری حاکمیت فناوری اطلاعات در سازمان

Reza Parvizi, Zahra Rasti, Seyed Raouf Khayami

Abstract — *Today information is the most important asset and strategic resources of any organization. For this reason, information technology management, was one of the organizational planning pillars programs need to ensure the value of information technology, risk management and control information associated with it, as a key element to leadership in any organization. In this article we are going through various frameworks, COBIT, Risk IT, and Val IT frameworks to examine. business and IT are Two pillars of the organizations, To choice Framework for IT management we should consider alignment of business and goals. The framework provided help to the senior management in a framework for controlling alignment business architecture and information systems to the objectives of the organization that it was the outcome frameworks COBIT, Risk IT, and Val IT, such as investment Technology in the desired position, risk management, life cycle forecast establish a common language between IT and business executives and IT managers, validation and evaluation activities to maximize profits. COBIT have some bugs, to cover this Defect we suggest that use Val IT and Risk IT parallel to COBIT, in fact those framework are Complementary with COBIT that can to form IT Governance in Organization in conclusion Alignment goals and business¹.*

Keywords — COBIT, Val IT, Risk IT, IT governance, business and goals alignment.

چارچوب برای کنترل همراستایی معماری کسب و کار و سیستم های اطلاعاتی نسبت به اهداف سازمان ارائه نماید که این مهم از طریق دستاورد چارچوب های COBIT، Risk IT و Val IT از قبیل: سرمایه گذاری فناوری در جایگاه مطلوب، مدیریت ریسک، پیش بینی چرخه حیات فناوری اطلاعات و برقراری زبان مشترک میان مدیران کسب و کار و مدیران فناوری اطلاعات، اعتبارسنجی و ارزیابی فعالیت ها و دسترسی به سود حداکثری، حاصل می گردد. COBIT ضعف هایی هم دارد، ما در این مقاله جهت پوشش ضعف COBIT استفاده از چارچوب های Val IT و Risk IT در کنار COBIT پیشنهاد می کنیم که نقش مکمل را برای چارچوب COBIT ایفا می کنند تا حاکمیت فناوری اطلاعات در سازمان شکل گیرد و منتج به همسویی کسب و کار و اهداف سازمان گردد. کلمات کلیدی COBIT، Val IT، Risk IT، حاکمیت IT، همسویی اهداف با کسب و

۱. چکیده

امروزه اطلاعات از مهمترین داراییها و منابع استراتژیک هر سازمان است. به همین دلیل، نحوه مدیریت فناوری اطلاعات، یکی از ارکان مهم برنامه ریزی 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 می - شوند. در این مقاله ما قصد داریم از بین چارچوب های مختلف، چارچوب های COBIT، Risk IT و Val IT را مورد بررسی قرار دهیم. دو رکن اساسی در سازمان ها کسب و کار و فناوری اطلاعات است، این امر می طلبد که چارچوب انتخابی برای مدیریت فناوری اطلاعات همراستایی این دو مقوله را موجب گرداند، در واقع چارچوب های ارائه شده کمک شایانی به مدیران ارشد در انتخاب یک

¹ R. Parvizi is postgraduate student in the Department of Electronic Learning, Shiraz University, Shiraz, Iran (e-mail: re.parvizi@gmail.com).

Z. Rasti is undergraduate student in the Shiraz University of Technology, Shiraz, Iran (e-mail: Zahra_rasti@yahoo.com).

S.R. Khayami is with the Department of Information Technology, Shiraz University of Technology, Shiraz, Iran (e-mail: Khayami@sutech.ac.ir).

ندادن بعد ریسک و بعد ارزش سازمان محقق سازد، موسسه دو چارچوب برای رفع این نقیصه COBIT معرفی کرده است. برای ارزیابی و مدیریت ریسکهای فناوری اطلاعات نیاز به چارچوبی است که سطح قابل قبولی از ریسک را ارائه داده، استراتژیهای برای کاهش، از بین بردن یا گذر از ریسکها تدوین کند (Risk IT). Val IT راهنماییهای مدیریتی برای کمک به سازمان در برپایی و مدیریت فرایند های مدیریت ارزش در محیط خود ارائه می کند.

۳. حوزههای اصلی راهبری فناوری اطلاعات

حوزههای اصلی راهبری فناوری اطلاعات موضوعاتی را تشریح می کنند که مدیریت اجرایی برای هدایت فناوری اطلاعات در سازمان نیازمند بررسی این موضوعات است. [2] مدل فرایندی COBIT بر حوزههای اصلی راهبری فناوری اطلاعات نگاشت میشود، و پلی میان آن چه مدیران عملیاتی بدان نیاز دارند و مدیران اجرایی برای هدایت سازمان خواستارند ایجاد میکنند. حوزههای اصلی راهبری فناوری اطلاعات به شرح زیر است:



شکل (۲) حاکمیت فناوری اطلاعات [۷]

همراستایی استراتژیک: این حوزه متمرکز بر تضمین ارتباط طرح و برنامه های کسب و کار و فناوری اطلاعات، و همراستا سازی عملیات فناوری اطلاعات با عملیات سازمانی است. ارزش افزایی: این حوزه درباره ایجاد ارزش توسط فناوری اطلاعات و همچنین تمرکز بر بهینه سازی هزینه ها و دستیابی به ارزشی منحصر به فرد از فناوری اطلاعات است.

مدیریت منابع: این حوزه پیرامون سرمایه گذاری بهینه در منابع فناوری اطلاعات (کاربردها، اطلاعات، زیرساخت و نیروی انسانی) است. بهینه سازی دانش و زیر ساخت، یکی از مباحث کلیدی این حوزه میباشد. مدیریت مخاطره: این حوزه مستلزم آگاهی نسبت به مخاطرات توسط واحدهای سازمانی ارشد، درک الزامات سازگار پذیری، شفافیت پیرامون مخاطرات سازمانی و تفویض مسئولیتها و وظایف مخاطرات در سازمان است. مدیریت عملکرد: این حوزه نحوه پیاده سازی راهبرد، انجام پروژه، استفاده از منابع، عملکرد فرآیندهای فناوری اطلاعات و ارائه خدمات را دنبال کرده و بر این مقولات نظارت میکند [1]

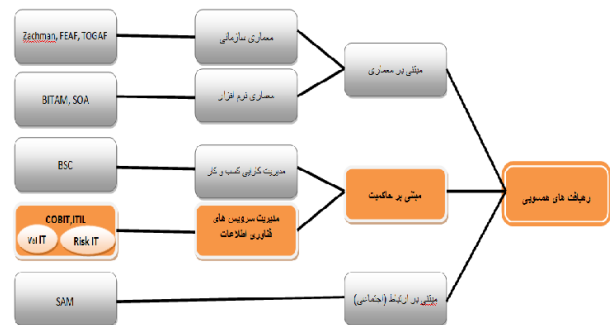
۴. رابطه COBIT با میزان بلوغ

مدیران ارشد سازمان همواره در صدد هستند که بدانند فناوری اطلاعات در سازمانش چگونه هدایت میشود برای دانستن این مطلب باید به طریقی سطح بلوغ فناوری اطلاعات در سازمان ارزیابی گردد. در چارچوب COBIT مدلسازی بلوغ بر اساس نوعی ارزیابی سازمانی بنا شده است. که بین سطح عدم وجود (۰) و

کار.

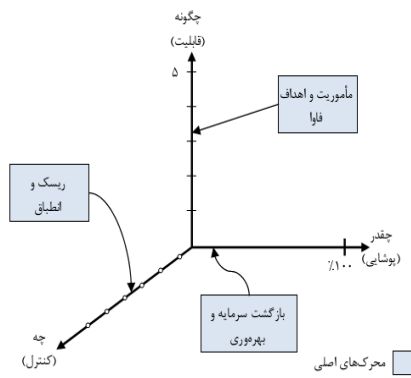
۲. مقدمه

برای بقا و موفقیت سازمان مدیریت موثر اطلاعات و مباحث مرتبط با فناوری اطلاعات (IT) بسیار مهم و حیاتی است. سازمان باید اطلاعات مورد نیاز خود را برای دارایی، کیفیت، اعتبار و امنیت برآورده نماید. رشد روزافزون فناوری اطلاعات از یک سو، و تغییرات محیط کسب و کار سازمانی مانند حرکت به سوی جهانی شدن، عوامل و پشیران های موثری هستند که سازمانها را مجبور به تغییر می نمایند. بخشهای فناوری اطلاعات سازمانها نیز برای پشتیبانی از تغییرات مذکور ملزم به توسعه و بروزرسانی سیستمهای خود می باشند. [5] به همین دلیل بیشتر سازمان ها شروع به پیاده سازی سیستم های نظارت و حاکمیت IT نموده اند تا اهداف فناوری اطلاعات و کسب و کار با هم همسو گردد. که انواع را در شکل (۱) مشاهده می کنید.



شکل (۱) رهافت های همسویی با اندکی تغییر [۱۱]

برای انجام دادن این مسئولیت ها و همچنین برای دستیابی به اهداف خود، مدیریت باید وضعیت سیستم های IT خود را درک کند و تصمیم بگیرد که چه ساز و کار و ابزار کنترل را فراهم نماید برای دستیابی به موفقیت در مدیریت سازمان و مدیریت فناوری اطلاعات و نظارت و ارزیابی بر عملکرد سازمان، از چارچوبی مرجع به نام COBIT استفاده می شود. پروژه کوبیت که امروزه در سراسر جهان توسط سازمان های مختلفی بکار گرفته میشود، تجارب موفق مدیریتی را در زمینه امنیت و کنترل فناوری اطلاعات بیان میکند و از این حیث، استفاده از آن برای کنترل حوزه فناوری اطلاعات در سازمان، دارای ارزشی ویژه خواهد بود. [3] COBIT یکی از مورد قبول ترین چارچوب های معتبر بین المللی در حوزه حاکمیت فناوری اطلاعات است که شامل مجموعه ای از بهترین کارکردها برای مدیریت فناوری اطلاعات است. در سال های اخیر مدیران ارشد به اهمیت فناوری اطلاعات در موفقیت سازمانها بیش از پیش پی برده اند. آنان به این امر واقف شده اند که می بایست در رابطه با نحوه راهبری فناوری اطلاعات در سازمان آگاهی لازم را داشته باشند. در راستای پاسخگویی به اهدافی نظیر برقراری ارتباط با الزامات سازمان، بهره گیری از یک مدل مشخص، شناسایی منابع اصلی، تعریف اهداف کنترلی مدیریتی و... چارچوبی به نام COBIT ایجاد شد که از ویژگی های اصلی آن می توان به تمرکز بر کسب و کار، فرایند محوری، بر پایه کنترل و با قابلیت اندازه گیری اشاره نمود. جهت گیری کسب و کار موضوع اصلی COBIT است که فقط برای کاربران و حسابرسان طراحی نشده است بلکه مهمتر از آن به عنوان راهنمایی جامع برای صاحبان فرایند مدیریت و کسب و کار است. [8] با این وجود COBIT به تنهایی نمی تواند حاکمیت فناوری اطلاعات را به دلیل پوشش



شکل (۳) سه بعد بلوغ [۶]

- آگاهی و ارتباط
- سیاستها، برنامه‌ها و روالها
- ابزارها و خودکارسازی
- مهارتها و تخصص
- مسئولیت و پاسخگویی
- تنظیم اهداف و یادگیری [6]

۵. رزیابی و مدیریت ریسکهای فناوری اطلاعات

Risk IT یک چارچوب کاملی است که ریسک سازمان را پوشش می دهد و فرایند ها و فعالیت ها را ارزیابی می نماید. همتراز و مکمل COBIT است و حق این را دارد که ارزش رسانی به شرکت را داشته باشد. در حالی که COBIT مجموعه ای را برای کنترل Risk IT و فرایند های فناوری اطلاعات فراهم می کند . Risk IT چارچوبی به منظور شناسایی و مدیریت ریسک برای سازمان فراهم می کند. سازمانها از Risk IT می توانند برای افزایش مدیریت ریسک استفاده نمایند همچنین آن دسته از سازمان هایی که COBIT را به عنوانی چارچوبی برای سازمان خود انتخاب کرده اند (یا در حال انتخاب هستند) اتصال و هارمونی بسیار مفیدی را بین این دو پیدا خواهند کرد. چارچوب Risk IT به سه حوزه: حاکمیت ریسک، ارزیابی ریسک و واکنش ریسک تقسیم می شود ، که هر حوزه شامل سه فرایند می باشد:

حاکمیت ریسک:

- ایجاد و نگهداری یک دید از ریسک های رایج
- یکپارچگی با مدیریت ریسک سازمان
- تصمیم گیری کسب و کار با آگاهی از ریسک

ارزیابی ریسک:

- جمع آوری داده
- تحلیل ریسک
- نگهداری پروفایل (نمایه) ریسک

پاسخ ریسک:

- مدیریت ریسک
- واکنش به رخداد
- شمرده کردن ریسک

بهینه (۵) رتبه بندی می شود. این رتبه بندی براساس مدل بلوغ پیشنهادی موسسه مهندسی نرم افزار در ارتباط با سنجش سطح بلوغ قابلیت توسعه نرم افزار صورت می گیرد. سطوح به صورت زیر دسته بندی میشوند:

سطح ۰ - عدم وجود ۲: فقدان هرگونه فرایند؛ سازمان حتی متوجه نشده است که باید کاری انجام بدهد.

سطح ۱- ابتدایی/فاقدعمومیت ۳: مدرکی دال بر توجه سازمان نسبت به موضوع وجود ندارد، اما هیچ فرآیندی استاندارد نیست و فقط کارهای فاقد عمومیت، موردی و یا شخصی انجام می شوند .

سطح ۲-تکرارپذیر اما شهودی ۴: فرآیندها تا حدی توسعه یافته اند که رویه های مشابه توسط نقش های مشابه اجرا می شوند . در این سطح ،هیچ گونه آموزش رسمی داده نشده است، ارتباطی با رویه های استاندارد وجود ندارد و مسئولیت برعهده اشخاص است. به دلیل وابستگی زیاد به دانش اشخاص، بروز خطا نیز محتمل تر است.

سطح ۳-فرآیند تعریف شده ۵: رویه ها استاندارد، مستند و با آموزش مرتبط شده اند .انجام موارد مذکور بسیار ضروری است با این حال شناسایی انحرافات بعید به نظر می رسد . رویه ها از سطح بالایی برخوردار نبوده ،صرفا جنبه تشریفاتی دارند .

سطح ۴-مدیریت شده و قابل اندازه گیری ۶: مدیریت سازمان به پایش و ارزیابی مطلوبیت رویه ها پرداخته ،هر جا که به نظر آید که اجرای فرآیندها موثر نیست ،وارد عمل می شود .فرآیندها تحت بهبود مستمر قرار داشته ،منجر به ارائه تجارب موفق می شوند ، خودکار سازی و ابزار به شکل محدود و جزئی ای به کار می روند. سطح ۵-بهینه ۷: فرآیندها در سطح تجارب موفق دیگر سازمان ها ، بر مبنای نتایج مستمر و مدلسازی بلوغ ،پالایش شده اند. فناوری اطلاعات به صورت یکپارچه و به منظور خودکار سازی گردش کارها، فراهم آوردن ابزار ارتقای کیفیت و سرعت بخشیدن به تطابق سازمان با تغییرات مورد استفاده قرار می گیرد. [4]

۱. ابعاد بلوغ هر فرآیند

ابعاد بلوغ هر فرایند چنان که در شکل (۳) نیز نشان داده شده، شامل سه مورد قابلیتها (چگونه)، پوشایی(چقدر) و کنترل (چه) است. هر یک از این ابعاد توسط محرکهایی تغییر وضعیت مییابند و بر این اساس، امتیاز بلوغ فرایند های مختلف در سازمان سنجیده میشود. محرکهایی هر بعد نیز در شکل (۳) نمایش داده شده اند.

اما آنچه که مدل بلوغ فرایندی COBIT بر آن تمرکز دارد تنها قابلیت بوده، بعد پوشایی را Val IT و بعد کنترل را Risk IT پوشش می دهند. در طراحی مدل بلوغ کنونی این چارچوب، مشخصه های زیر مد نظر قرار گرفته اند:

² Non-existent

³ Initial/Ad Hoc

⁴ Repeatable but Intuitive

⁵ Defined Process

⁶ Managed and Measurable

⁷ Optimised

هزینه‌ها، امکان محاسبه صحیح ارزش ایجاد شده توسط سرویس‌های فناوری اطلاعات وجود نداشته و باعث ایجاد سؤالاتی از قبیل موارد زیر می‌گردد:

- به چه دلیل دپارتمان فناوری اطلاعات قادر به ارائه سطح بالاتری از سرویس نمی‌باشد؟
- به چه دلیل بودجه زیادی به دپارتمان فناوری اطلاعات اختصاص داده می‌شود؟
- هزینه پیاده‌سازی و به‌کارگیری این سیستم جدید چقدر می‌باشد؟

چارچوب Val IT به عنوان چارچوب مدیریت و سرمایه‌گذاری فناوری اطلاعات با تمرکز در سه حوزه‌ی راهبری ارزش، مدیریت پورتفولیو و مدیریت سرمایه‌گذاری روشی بهتر را برای کنترل و نظارت بر هزینه‌ها و پروژه‌های فناوری اطلاعات در یک سازمان ارائه می‌دهد. [9]

آ. دلایل رویکرد سازمان به پیاده‌سازی Val IT

- مدیریت سرمایه‌گذاری‌های فناوری اطلاعات به صورت پورتفولیوهای سرمایه‌گذاری کسب و کار
- ایجاد ارزش از طریق سرمایه‌گذاری‌های مرتبط به فناوری اطلاعات
- مدیریت سرمایه‌گذاری‌های فناوری اطلاعات در طول چرخه حیات آنها
- شناسایی، ارزیابی و مدیریت طبقه‌بندی‌های مختلف سرمایه‌گذاری
- تعریف و نظارت بر شاخص‌های کلیدی ارزش و اقدام در مقابل انحراف از وضع مطلوب

راهنمایی‌های مدیریتی Val IT

- Val IT راهنمایی‌های مدیریتی برای کمک به سازمان در برپایی و مدیریت فرایند‌های مدیریت ارزش در محیط خود ارائه می‌کند. این راهنمایی‌ها به سؤالات معمول مدیریت پاسخ می‌دهد
- چگونه بایستی همه فرایندهای مدیریت ارزش را به هم مرتبط کرد؟
 - فعالیت‌های اصلی که بایستی انجام داد یا بهبود بخشید چیست؟
 - نقش‌ها و وظایفی که برای فرایندهای مدیریت ارزش موفق لازم است، چیستند؟
 - چگونه باید فرایندهای مدیریت ارزش را سنجید و مقایسه کرد؟
 - شاخص‌های کارایی خوب چیست؟

۷. نتیجه‌گیری

فناوری اطلاعات یک بخش جدایی‌ناپذیر از کسب و کار است و راهبری آن یک بخش جدایی‌ناپذیر 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 چارچوب برای اجرا و پیاده‌سازی راهبری، مثل COBIT لازم است. COBIT به واسطه فراهم‌آوری چارچوبی مناسب، از راهبری فناوری اطلاعات پشتیبانی کرده و از این طریق تضمین می‌کند که اولاً فناوری اطلاعات و کسب و کار همراستا هستند و فناوری اطلاعات موجب توانمندی کسب و کار و افزایش منافع سازمان می‌گردد. ثانیاً مخاطرات فناوری اطلاعات به صورت مناسبی مدیریت می‌شود. با



چارچوب Risk IT [10]

- توصیف: برای ارزیابی و مدیریت ریسک‌های فناوری اطلاعات نیاز به چارچوبی است که سطح قابل قبولی از ریسک را آرایه داده، استراتژی‌هایی برای کاهش، از بین بردن یا گذر از ریسکها تدوین کند. بر این اساس، هر تأثیر بالقوه‌ای که به وسیله عوامل پیش‌بینی نشده ممکن است در اهداف کسب و کار سازمان - که بر تصمیمات حوزه فناوری اطلاعات اثر می‌گذارد - روی دهد، باید تعیین، تحلیل و ارزیابی شود. [10]
- هدف اصلی این فرآیند: تحلیل و ابلاغ ریسک‌های فناوری اطلاعات و تأثیرات بالقوه آنها بر فرآیندها و اهداف کسب و کار است.
- منابع:

- برنامه‌های کاربردی
- اطلاعات
- زیرساخت
- افراد

۶. مشاوره و پیاده‌سازی چهارچوب سنجش ارزش خدمات فناوری

اطلاعات VAL IT

ارچوب وال آی تی، چارچوب کاملی است که ارزش سازمان را پوشش می‌دهد، این چارچوب مکمل COBIT است و ارائه ارزش به سازمان حق آن است. در حالی که COBIT تضمین می‌کند که فناوری اطلاعات به طور موثر اقدام به افزایش و حداکثر رساندن سود سرمایه‌های فناوری نماید، وال آی تی به سازمان در تصمیم‌گیری بهتر در مورد مکان سرمایه‌گذاری می‌نماید با این تضمین که سرمایه‌گذاری با استراتژی کسب و کار سازگار باشد. [9] سرویس‌های فناوری اطلاعات اغلب به عنوان سرویس‌های حیاتی در سازمان محسوب می‌گردند. با این وجود افزایش کاربران فناوری اطلاعات، تکنولوژی‌های جدید و سایر پیچیدگی‌های این سرویس‌ها موجب افزایش هزینه این سرویس نسبت به سرویس‌های دیگر می‌باشد. بنابراین سازمان‌ها اغلب یا نمی‌خواهند یا نمی‌توانند بودجه لازم برای سرویس‌های فناوری اطلاعات را فراهم نمایند. در نتیجه این پیچیدگی‌ها و افزایش

استفاده از این چارچوب کنترلی میتوان معیاری را برای سنجش جایگاه فعلی سازمان تعیین نمود در همین راستا روشی برای تصمیم گیری مناسب به نحوه عملکرد و حرکت سازمان نیز مشخص نمود. COBIT چارچوبی است که در آن بیشتر به چیسستی کارها پرداخته شده تا چگونگی انجام آنها و از این رو به نظر می رسد که در سطوح استراتژیک کارایی بیشتری داشته باشد تا در سطوح تاکتیکی و عملیاتی. ضعف عمده دیگر از این چارچوب بجز مورد فوق، ضعف در تعیین ساختارها و حقوق تصمیم گیری در حوزه فناوری اطلاعات است. گذشته از این موارد، در معرفی فرایندها و تعیین سطح بلوغ آنها COBIT چارچوبی کاربردی و پذیرفته شده در سطح بین المللی است و برای همسوسازی فناوری اطلاعات با اهداف کسب و کار و مدیریت مخاطرات مناسب میباشد. نظرات مدیران و پژوهشگران حوزه حاکمیت فناوری اطلاعات نیز موید این مطلب است. علاوه بر چارچوب COBIT جهت پوشش ارزشهای سازمان و ریسک های سازمان می توان از چارچوب های مکمل Risk IT و Val IT بهره برد. برای همسویی فناوری اطلاعات و کسب و کار سازمان موضوع حاکمیت فناوری اطلاعات مطرح است، که جهت شکل گیری حاکمیت فناوری اطلاعات به صورت جامع بحث مدیریت کارایی کسب و کار و مدیریت سرویس های اطلاعاتی با هم مد نظر قرار گیرد که خود یک بررسی، پژوهش و مجالی دیگر را می طلبد، امید آنکه با دستیابی به این مهم حاکمیت فناوری اطلاعات، همراستایی فناوری اطلاعات با کسب و کار و اهداف سازمانی را به ارمغان آورد.

REFERENCES

- 1 Haghshenas M. Evaluation of Information Technology Functionality in Organization with COBIT controlling Framework. Computer Reporting, 2009; 41.
- 2 Alaedini M. Information Governance and COBIT Framework Role in Its Implementation, MSc Seminar, Amirkabir University, 2009.
- 3 Alaedini M, Daghyeghi A. Results of Using COBIT Reference Model in IT Management Processes in National Iranian Drilling Company with Process Maturity Approach, Strategic Management Academy, Tehran, 2008.
- 4 Amid A, Edalatpour A. Model for Evaluation of Management Maturity of Information Technology Projects: Case Study on TRE Company. Proceeding of 25th International Conference on Electricity, Tehran, 2010.
- 5 Khayami, SR. Organization Analysis and Architecture. PhD Thesis, Shiraz University, 2009.
- 6 IT Governance Institute (www.itig.org). Control Objective for Information and Related Technology (COBIT), ver 4.1, USA, 2007.
- 7 COBIT Transforming Enterprise IT. 2009, Available at: www.isaca.org.
- 8 www.isaca.org/CobIT
- 9 www.isaca.org/valit
- 10 www.isaca.org/riskit
- 11 Kazman R, Chen HM. Aligning Business Models. Business and IT Architectures. 2002; 2.