ماهنامهٔ انجمن انفورماتیک ایران
(فعلاً هردوماه یکبارمنتشرمی شود.)

گزارش کامپیوتر

سال سی و ششم، آذر و دی ۱۳۹۳، شمارهٔ ۲۱۸، ۴۰۰۰ تومان

صاحب امتیاز: انجمن انفورماتیک ایران
مدیر مسئول و سردبیر: ابراهیم نقیب‌زاده مشایخ

مقاله‌ها و گزارشهای تالیفی یا ترجمه خود را برای گزارش کامپیوتر بفرستید. مطالب ارسالی را با خط خوانا (یا ماشین شده) بر یک روی کاغذ بنویسید فاصله کافی برای افزودن اصلاحات ویرایشی در بین خط‌ها و حاشیه در نظر بگیرید. در صورت ارسال مطلب ترجمه شده، یک نسخه از اصل مطلب را نیز ارسال دارید. شکلها باید با روان‌نویس مشکی ترسیم و به‌صورت آماده چاپ ارسال شوند. مطالب ارسالی پس فرستاده نمی‌شوند.

مسؤولیت مطالب گزارش کامپیوتر با نویسندگان است و لزوماً نشان‌دهنده نظر انجمن انفورماتیک ایران نیست. ذکر نام شرکتها و محصولات در مطالب گزارش کامپیوتر برای ارائه اطلاع به خوانندگان است و نباید به معنی تائید انجمن از آنها تلقی شود.

سازمان آگهی‌ها: مهناز خاوندکار
تلفکس : ۸۸۳۲۸۴۱۷-۲۱
حروفچینی : تارتن سامانه
لیتوگرافی: نگارین پرتو ۷۷۵۳۰۳۰۷
چاپ علوی تهران : ۶۶۷۰۱۵۲۷
خ جمهوری ، ۳۰ تیر ، کوچه مصری پور ، پلاک ۲۵۶

اعضای هیئت تحریریه و ویراستاران علمی

تهران، خیابن طالقانی غربی، روبروی سینما عصر جدید، ساختمان پزشکان صدف، طبقه اول، واحد ۵

محتوای این شـماره از گزارش کامپیوتر، عمدتاً به مقالات ارایه شده در سـومین همایش «راهبری و مدیریت فناوری اطلاعات» اختصاص یافته اسـت. سـابقه این همایش، که توسط «سـازمان نظام صنفی رایانه‌ای اسـتان تهران» برگزار می‌شـود، به سـال ۱۳۹۱ برمی‌گردد. کمیسیون اسـتاندارد و تدوین مقررات سـازمان نظام صنفی رایانه‌ای استان تهران حسب ماموریت‌های محوله و در مسیر اطلاع‌رسانی استانداردهای حوزه فناوری اطلاعات، در سال ۱۳۹۱ اقدام به طرح‌ریزی و اجرای این سلسله همایش‌ها کرد.

ایـن همایش تلاش می‌کند که موضوعـات حاکمیتی و راهبری فناوری اطلاعات را در سطح سازمان‌ها تبیین کرده و علاوه بر آن، تجارب داخلی را در سطح گسترده‌تری اطلاع‌رسانی کند. طبق طرح اولیه، برگزاری این همایش به‌صورت سالانه، و هر سال با یک موضوع مشخص، برنامه‌ریزی شد. نخستین همایش در اسفند ماه سال ۱۳۹۱ با موضوع «اصول و مبانی راهبری سـازمانی فناوری اطلاعات» و دومین همایش در آذر ماه سـال ۱۳۹۲ با موضوع «ارتقاء ظرفیت کارفرمایی در تعریف و اجرای پروژه‌ها و خدمات فناوری اطلاعات» برگزار شد. سومین همایش که در دی ماه اجرا می‌شود، موضوع آن «ممیزی فناوری اطلاعات» است. انجمن انفورماتیک ایران به دلیل سابقه همکاری خود با سازمان نظام صنفی رایانه‌ای استان تهران، از ابتدای شـکل‌گیری این همایـش، از آن حمایت کرده و حامی معنوی آن بوده است.

سازمان‌های مختلف حسب نیازهای کسب‌وکاری خود طی سال‌های اخیر اقدام به پیاده‌سـازی انواع پروژه‌های فناوری اطلاعات کرده‌اند. اکثر این پروژه‌ها در بخشـی از سازمان و با هدف تحقق اهدافی از کسب‌وکار اجرا شده است. عدم حصول موفقیت پروژه (از دیدگاه سازمان و نه پروژه‌ای) در سازمان، و به تبع آن هدر رفتن سرمایه‌گذاری انجام شده، مدیریت ارشد را با شرایط ویژه‌ای مواجه کرده است. سوال مشخص این است که در چه حوزه‌ای باید سرمایه‌گذاری کرد که به تحقق اهداف کسب‌وکاری سازمان کمک کند؟ این سوال اصلی، منجر به ایجاد مفهومی به نام حاکمیت یا راهبری فناوری اطلاعات (IT Governance) منجر شد.

راهبری فناوری اطلاعات، به عنوان فرآیندی تعریف شـده که اطمینان می‌دهد سـازمان، فناوری اطلاعات را به شکلی موثر، اثربخش، و کارا در راستای توان‌مندسازی خود، به‌منظور تحقق اهداف کسب‌وکار، استفاده می‌کند. بر همین اسـاس، راهبری فناوری اطلاعات به موضوعاتی مانند ارزیابـی، انتخاب، اولویت‌بندی، تامین بودجه، برای سـرمایه‌گذاری‌های متضاد فناوری اطلاعات می‌پردازد.

مخاطبیـن اصلی موضوعات راهبری فناوری اطلاعات، لایه‌های مدیریت ارشـد و تصمیم‌ساز سازمان‌ها است؛ بر خلاف مدیریت فناوری اطلاعات که اساسـاً موضوعی است فنی و به مدیران فناوری اطلاعات برمی‌گردد. مدیریت ارشـد به دنبال تعریف پروژه‌هایـی مبتنی بر فناوری اطلاعات، است که سازمان متبوع خود را از حیث درآمدی، جایگاهی، و رقابتی ارتقا داده و ارزش افزوده‌ای را برای آن به ارمغان بیاورد. از سـوی دیگر، ابعاد مالی استفاده از فناوری اطلاعات هم برای این لایه از مدیران مهم است: چه سرمایه‌گذاری‌هایی و با چه توجیهی، باید در حوزه به‌کارگیری فناوری اطلاعات انجام شـود؟ سرمایه‌گذاری‌های قبلی چه منفعت یا دستاوردی برای سازمان داشته است؟

در حالی که مدیریت فناوری اطلاعات، مدیریت اجرای یک پروژه بخشی و محدود در سـازمان اسـت، راهبری فناوری اطلاعات درصدد «توزیع» قابلیت‌های آن در سرتاسـر سـازمان و در مسـیر اهداف سازمانی است. راهبری فناوری اطلاعات در سـازمان، ارتباط با مفاهیمی مانند اهداف، ماموریت، چشم‌انداز، و راهبرد داشته و طیف گسترده‌ای از افراد ذی‌ربط (از مدیریت ارشد تا مدیر عامل تا هیئت‌مدیره تا سهام‌داران تا ذی‌نفعان) را دربرمی‌گیرد. پیادسازی یک سـاختار برای راهبری فناوری اطلاعات، درگیر موضوعات مهمی مانند هم‌سـویی راهبری، ارایه ارزش، مدیریت منابع، مدیریت مخاطره، و هم‌سـویی با کسب‌وکار است. به همین دلیل است که پیاده‌سازی ساختار و سازمان راهبری فناوری اطلاعات به‌مراتب پیچیده‌تر از پیاده‌سازی یک پروژه خاص در این حوزه است.

«ممیزی فناوری اطلاعات» مفهومی است در راهبری فناوری اطلاعات که هدف آن درک درسـت وضعیت اسـتفاده از فنـاوری اطلاعات در سازمان، شـناخت نقاط قوت و ضعف، و ایجاد شرایطی برای بهبود (بر اسـاس این فناوری) اسـت. در مقالاتی که خواهد آمد، تجارب برخی سازمان‌ها و نهادها در باب این موضوع، که در همایش مذکور ارایه شده، آمده است.

اخبار انجمن

مسئولان جدید انجمن

هیئت مدیرهٔ جدید انجمن در نخستین جلسهٔ خود در تاریخ ۹۳/۰۷/۳۰، مسئولان جدید انجمن را به شرح زیر برگزید:

- آقای ابراهیم نقیب‌زادهٔ مشایخ، رئیس هیئت مدیره
- آقای دکتر اسلام ناظمی، نایب رئیس هیئت مدیره
- آقای مهندس محمدحسن محوری، خزانه‌دار انجمن
- آقای دکتر علیرضا باقری، دبیر انجمن
- آقای دکتر محمد گنج‌تابش، عضو هیئت مدیره
- آقای مهندس سعید امامی، عضو علی‌البدل هیئت مدیره
- آقای دکتر علی فرخی، عضو علی‌البدل هیئت مدیره

انتخاب سرپرستان کمیته‌های انجمن

هیئت مدیرهٔ جدید انجمن، در نخستین جلسهٔ خود، سرپرستان کمیته‌های مختلف انجمن را به شرح زیر انتخاب کرد:

۱- آقای ابراهیم نقیب‌زادهٔ مشایخ، سرپرست کمیتهٔ انتشارات

۲- آقای دکتر محمد گنج‌تابش، سرپرست کمیتهٔ آموزش

۳- آقای مهندس سعید امامی، سرپرست کمیتهٔ عضویت و روابط عمومی

۴- آقای مهندس علیرضا ماهیار، سرپرست کمیتهٔ گردهمایی‌های علمی

اتمام چاپ اول کتاب کار برنامه‌نویسان

با استقبال زیادی که از سوی جامعهٔ فناوری اطلاعات کشور و به ویژه برنامه‌نویسان جوان از کتاب «کار برنامه‌نویسان» به عمل آمد، چاپ اول این کتاب در کمتر از یک سال و نیم پس از انتشار به پایان رسید.

لازم به ذکر است که این کتاب که توسط آقای ابراهیم نقیب‌زادهٔ مشایخ به فارسی ترجمه شده است، در اسفند ۱۳۹۱ با حمایت مالی شرکت‌های پویا و همکاران سیستم به چاپ رسید. اینک انجمن برای تجدید چاپ این کتاب همچنان نیازمند حمایت مالی است. از شرکت‌ها و مؤسساتی که مایلند در این زمینه یاری‌رسان انجمن باشند تقاضا می‌شود با دفتر انجمن (۳-۸۸۸۶۱۴۲۱) تماس بگیرند.

بدیهی است نام شرکت به عنوان حامی مالی در پشت جلد کتاب درج خواهد شد.

چاپ کتاب «پایان کار غول‌ها»

کتاب «پایان کار غول‌ها» که تا کنون ترجمهٔ هفت قسمت آن در شماره‌های متوالی گزارش کامپیوتر به چاپ رسیده و مورد استقبال وسیع خوانندگان این نشریه قرار گرفته است، تا قبل از پایان سال جاری از سوی انجمن انفورماتیک ایران به چاپ خواهد رسید.

انجمن برای چاپ این کتاب نیاز به حامی مالی دارد. بدین وسیله از کلیهٔ اعضای حقوقی انجمن که مایلند در هزینهٔ چاپ این کتاب مشارکت نمایند تقاضا می‌شود با دفتر انجمن تماس بگیرند. بدیهی است نام شرکت یا شرکت‌هایی که در این زمینه به انجمن یاری رسانند در پشت جلد کتاب درج خواهد شد و تعدادی نسخهٔ رایگان از این کتاب در اختیارشان قرار داده خواهد شد.

این کتاب می‌تواند بهترین هدیهٔ نوروزی از

طرف شـرکت‌ها و سازمان‌ها به کارشناسان و کارمندانشان باشد.

اخبار شاخه‌های دانشجویی انجمن

برگـزاری سـخنرانی علمـی در دانشگاه تهران

شاخهٔ دانشجوئی انجمن در دانشکدهٔ ریاضی، آمار و علـوم کامپیوتر دانشـگاه تهران، یک سـخنرانی علمـی در تاریـخ ۲۵ آذر ۹۳ در محل سـالن هشـترودی آن دانشکده برگزار کرد. سخنران این جلسه آقای سپهر لرستانی و موضوع سخنرانی «چرا لینوکس؟» بود.

آقای لرستانی در ابتدای سخنان خود به این نکته اشـاره کرد که شـاید در سـال ۱۹۹۰، زمانی که لینوس توروالدز اولین نسخه از کد کوچـک خود به نام لینوکـس را ایجاد کرد، کسی حتی تصوّر این را هم نمی‌کرد که روزی این محصول به رقیبی سرسـخت برای سایر سیسـتم عامل‌های تجاری تبدیل شـود. وی سپس به تفصیل به بیان ویژگی‌های سیستم عامل لینوکس و مقایسـهٔ آن با سایر سیستم عامل‌های مطرح بـازار پرداخت و ضمن ارائهٔ آمارهایی از به‌کارگیری این سیستم عامل، به چند دلیل برای مهاجرت به لینوکس اشـاره کرد.

در پایان این سـخنرانی که با استقبال خوبی از سـوی دانشـجویان روبـرو شـده بـود به پرسش‌های حاضران پاسخ داده شد.

شـاخهٔ دانشـجوئی انجمن انفورماتیک ایران بدین وسـیله از آقای سـپهر لرسـتانی برای قبـول دعـوت انجمن بـرای برگـزاری این سخنرانی صمیمانه قدردانی می‌نماید.

برگزاری دوره‌های تخصصی برای سازمان‌ها

گروه تخصصـی «راهبری و مدیریت خدمات فناوری اطلاعات» انجمـن انفورماتیک ایران آمادگـی برگـزاری دوره‌هـای زیـر را برای کارشناسان سازمان‌های مختلف در محل آن سازمان دارد.

۱. کارگاه نیـم روزه تدویـن توافقنامه‌هـای سطح خدمات
۲. کارگاه یـک روزه طراحـی و اسـتقرار پیشخوان خدمات
۳. کارگاه نیم روزه طراحی کاتالوگ خدمات
۴. کارگاه یک روزه ابزارهای مدیریت خدمات فناوری اطلاعات
۵. کارگاه نیـم روزه برونسـپاری خدمـات و محصولات فناوری اطلاعات
۶. کارگاه نیم روزه همسوسـازی IT با کسب وکار (IT Alignment) از طریق COBIT5
۷. کارگاه یک روزه راهبری فناوری اطلاعات (IT Governance) از طریق COBIT5
۸. کارگاه یک روزه راهبری فناوری اطلاعات (IT Governance)
۹. کارگاه نیم روزه مدیریت تدوام کسـب و کار ISO2012:22301
۱۰. کارگاه نیم روزه راهبری فناوری اطلاعات و ITBSC
۱۱. کارگاه نیم روزه تدوین استراتژی خدمات فناوری اطلاعات
۱۲. کارگاه یک روزه مدیریت خدمات فناوری اطلاعات
۱۳. کارگاه سه روزه ITIL V3 Foundation 2011
۱۴. کارگاه یـک روزه مدیریـت مخاطـرات فناوری اطلاعات
۱۵. کارگاه سه روزه دوره جامع COBIT5
۱۶. کارگاه نیـم روزه توسـعه نیازمندی‌هـا مبتنی بر چارچوب CCMI-ACQ و استاندارد ISO/IEC29148:2011

ویژگی‌های این کارگاه‌ها عبارتند از :

- مشارکت گروهی، بحث و انجام سناریو، حل نمونه آزمون‌های امتحانی
- استفاده از مثال‌های مرتبط با حوزه فعالیت هر کسب وکار
- برگـزاری دوره حداقل توسـط دو مدرس دارای مدرک بین‌المللی
- برگزاری دوره در محل سازمان متقاضی
- ارائه مدرک شرکت در دوره از سوی انجمن انفورماتیک ایران
- ارائه مستندات آموزشی

علاقه‌منـدان مـی تواننـد بـا دفتـر انجمن انفورماتیـک ایـران(۳-۸۸۸۶۱۴۲۱) و یـا نشانی پسـت الکترونیکی member@isi.org.ir تماس بگیرند.

اخبار ایران

سـمپوزیوم بین‌المللـی هـوش مصنوعی و پردازش علائم

انجمن کامپیوتر ایران و دانشـگاه فردوسـی مشهد، نخستین سمپوزیوم بین‌المللی هوش مصنوعـی و پردازش علائـم (AISP2015) را در تاریـخ ۱۲ تا ۱۴ اسـفند ۱۳۹۳ در محل دانشکدهٔ مهندسی کامپیوتر دانشگاه فردوسی برگزار می‌کنند.

علاقه‌منـدان برای دریافت اطلاعات بیشـتر می‌تواننـد بـه وبـگاه همایـش به نشـانی http://aisp2015.um.ac.ir مراجعه کنند.

بیستمین کنفرانس سالانهٔ انجمن کامپیوتر ایران

بیسـتمین کنفرانـس ملـی سـالانهٔ انجمن کامپیوتـر ایران از ۱۲ تا ۱۴ اسـفند ۱۳۹۳ در دانشـگاه فردوسی مشـهد برگزار خواهد شـد. ایـن کنفرانـس در دو بخـش مقالات عادی و پوسـتری برگزار می‌شود و تأکید آن بر جنبه‌های بنیادی، کاربـردی، راهبردی و توسـعه‌ای است که از سـودمندی خاص در سطح کشور برخوردارند.

محورهـای علمی این کنفرانـس به قرار زیر است:

- مهندسی نرم‌افزار
- الگوریتم‌ها و نظریهٔ محاسبات
- هوش مصنوعی و پردازش‌های هوشمند
- شبکه‌های کامپیوتری و سیستم‌های انتقال داده
- سیسـتم‌های عامـل، پـردازش مـوازی و سیستم‌های توزیع شده
- امنیت اطلاعات
- سیستم‌های دیجیتال و معماری کامپیوتر
- فناوری اطلاعات

علاقه‌منـدان بـرای آگاهی از تاریخ ارسـال مقالات و پیشـنهاد کارگاه می‌توانند به وبگاه کنفرانس به نشانی http://csicc2015.um.ac.ir مراجعه کنند.

نخسـتین همایش سیسـتم‌های حمل و نقل هوشمند جاده‌ای

سـازمان راهـداری و حمل و نقـل جاده‌ای، نخستین همایش سیسـتم‌های حمل و نقل هوشمند جاده‌ای (ITS) را در دی ماه ۱۳۹۳ برگزار می‌کند.

محورهای این همایش عبارتند از:

- سیاست‌های کلی و راهبردها در ITS
- مدیریت هوشمند ایمنی و کنترل ترافیک
- اطلاع‌یابی، اطلاع‌رسانی و مدیریت سفر
- زیرساخت‌های مشترک
- تکنولوژی و تجهیزات
- مدیریت و تجربیات اجرای پروژه‌های ITS
- ارتقاء الگوهای رفتاری

همچنین برگزاری نمایشگاه جانبی به منظور عرضهٔ دستاوردهای علمی و فنی در خصوص موضوع همایش پیش‌بینی شده است.

علاقه‌منـدان برای دریافت اطلاعات بیشـتر می‌تواننـد بـه وبـگاه همایـش به نشـانی www.itscongress.rmto.ir مراجعه کنند.

اخبار جهان

رابین ویلیامز در صدر جستجوی گوگل

براسـاس آنچه مردم دنیا در گوگل جستجو کرده‌اند، خودکشـی رابین ویلیامز، هنرپیشهٔ آمریکایـی، بیش از هر چیز دیگری در سـال ۲۰۱۴ اذهـان جهانیان را بـه خود معطوف کرده است.

واکنش به مرگ ویلیامز در ماه آگوسـت، در صدر جسـتجوی گوگل در سال ۲۰۱۴ قرار گرفته و رویدادهـای مهمی چون جام‌جهانی فوتبال، ویروس ابولا، گم شـدن پرواز شمارهٔ ۳۷۰ هواپیمایـی مالزی در ماه مارچ و چالش سطل یخ (موج فیلم‌های ویدیویی در اینترنت بـرای جمـع‌آوری کمک مالی و آگاه‌سـازی عمومی دربارهٔ بیماری ALS) را پشـت سـر گذاشته است.

سـایر عناوین پرجسـتجو عبـارت بوده‌اند از بازی تلفنـی «Flappy Bird»، گـروه افراطی داعـش، کارتون «Frozen» شـرکت دیزنی و المپیک زمستانی روسیه.

مرگ رابیـن ویلیامـز، جام‌جهانـی فوتبال، ویـروس ابـولا و چالش سـطل یـخ در بین موضوعاتی که در سـال جاری در فیسـبوک بیشـتر از همه مورد بحث قـرار گرفته‌اند نیز وجـود دارند. فیسـبوک هفتهٔ گذشـته این فهرست را منتشر کرد.

رتبه‌بندی گوگل بیش از هر چیز دیگر گویای این اسـت که مردم به چه چیزی بیشتر فکر کرده‌انـد زیرا از هر سـه جسـتجوئی که در اینترنـت به عمل می‌آیـد، دوتایش از طریق گوگل صورت می‌گیرد.

در فهرسـت بیشترین جسـتجوهای یاهو در سـال ۲۰۱۴، ویروس ابولا در صدر قرار دارد. این فهرسـت گویای این است که وبگاه یاهو بیشتر علاقه‌مندان به تفریحات و سرگرمی‌ها را به خود جلب می‌کند زیرا پس از ابولا، شش جسـتجوی برتر بعدی به نام‌های هنرپیشه‌ها تعلّق دارد. بـازی ویدیویی «Minecraft» (که محبوبیتش باعث شـد که مایکروسـافت در اوایل امسال آن را ۲/۵ میلیارد دلار خریداری کند)، کارتون «Frozen» و آیفون ۶، لیسـت ۱۰ جستجوی برتر یاهو را تکمیل کرده‌اند.

جویشـگر بینگ مایکروسـافت به جای آن کـه بیشـترین جسـتجوها را در کلّ اعلام کند، فهرسـتش را به موضوعـات مختلف تقسـیم کرده و اعلام کرده در هر موضوع، بیشترین جستجو مربوط به چه بوده است. براساس این فهرسـت موضوعی، در زمینهٔ ورزش، لبرون جیمز بسکتبالیسـت NBA، در زمینـهٔ چهره‌هـای سرشـناس هنری، کیم کارداشـیان، در زمینهٔ مقصد سفرهای تفریحـی، کشـور کاسـتاریکا، و در زمینهٔ موسـیقی، بیانسه، بیشـترین جستجوها را داشته‌اند.

آسوشیتدپرس، ۱۶ دسامبر ۲۰۱۴

دنیای بدون گذرواژه

چه خوب می‌شـود اگر بتوانیـم گذرواژه‌ها را کنار بگذاریم و آن‌ها را با زیسـت سـنجه‌ها (بیومتریـک) و رمـز- نشـانه‌های (توکـن) برگرفتـه از تلفن‌هـای هوشـمند جایگزین بسـازیم. اتحادیـهٔ فیدو که ائتلافی اسـت از بسیاری از شرکت‌های بزرگ و نامدار فناوری، مشخصات نهایی این کار را منتشر کرد.

برنامه‌های فیدو شامل دو طرح UAF(چارچوب احـراز هویـت عمومـی) و U2F (عامل دوم عمومی) می‌باشـد امّا به عقیدهٔ کارشناسان، این دو طـرح، پایان کار رمز عبورها نیسـت بلکه آن‌ها را دور از نظر نگاه می‌دارد.

از بیـن دو اسـتانداردی کـه اتحادیهٔ فیدو ایجاد کرده اسـت، U2F بیشـتر نظرها را به خود جلب کرده اسـت. این استاندارد، روش سازگاری برای پیاده‌سـازی احراز هویت دو عاملی فراهم می‌سازد، بدون آن که نیاز باشد هیچکدام از دو عامل، یک عنصر خاص باشد. ایـن مدل، از آنچه اکنون وجود دارد بسـیار انعطاف‌پذیرتر اسـت. امّا خبر بد این اسـت که U2F فرض می‌کند که کاربر ابتدا توسـط سـازوکار دیگری احراز هویت شـده اسـت و سـپس قرارداد U2F وارد عمل می‌شـود و آن سازوکار دیگر در ۹۸ درصد موارد چیزی نیست جز گذرواژه.

شـرکت‌های سرشناسـی در اتحادیـهٔ فیدو حضـور دارنـد کـه از آن جمله می‌تـوان به مایکروسـافت، گوگل، پِی پَل، مسـترکارد و بانـک آمریکا اشـاره کرد. برخـی از آن‌ها به کارگیری استانداردهای فیدو را آغاز کرده‌اند. به طور مثال، پِی پَل و سامسونگ از استاندارد UAF بـرای پرداخت‌هـا اسـتفاده کرده‌اند و گوگل از U2F برای ورود کاربرد.

اینفو ورلد، ۱۲ دسامبر ۲۰۱۴

پذیـرش بیـت کویـن توسـط مایکروسافت

مایکروسـافت گزینهٔ پرداخت جدیدی را در فروشـگاه‌های برخط خود راه‌انـدازی نموده و آن چیـزی نیسـت جـز بیت کویـن. این

پول رمزگذاری شده می‌تواند برای خرید برنامه‌های کاربردی (app)، بازی‌ها و سایر محتویات دیجیتال از فروشگاه‌های برخط ویندوز، ویندوز فون و اکس‌باکس، به کار گرفته شود. البته در حال حاضر خرید مستقیم با بیت کوین امکان‌پذیر نیست، بلکه از آن می‌توان برای افزودن پول به یک حساب مایکروسافت در آمریکا استفاده کرد و بعد از آن حساب به خرید محصولات پرداخت.

مایکروسافت هشدار داده است که خرید با بیت کوین شاید روش ساده‌ای نباشد. با وجودی که تراکنش‌های بیت کوینی قاعدتاً باید بلافاصله پردازش شوند امّا به کاربران توصیه شده است که در صورتی که چنین نشد، تا دو ساعت صبر کنند. همچنین، پولی که با بیت کوین به حساب اضافه می‌شود قابل برگشت دادن نیست.

این خدمت در حال حاضر فقط در آمریکا در دسترس کاربران است. مایکروسافت با پذیرش بیت‌کوین به لیست بلند بالایی از سایر شرکت‌ها که عرضهٔ گزینهٔ بیت کوین را برای پرداخت آغاز کرده‌اند، پیوست.

آی‌دی‌جی نیوز، ۱۱ دسامبر ۲۰۱۴

تلویزیون‌های کوانتومی ال‌جی

شرک کره‌ای ال‌جی، تلویزیون‌های جدیدی با فناوری پیشرفته را از اوایل سال ۲۰۱۵ به بازار عرضه خواهد کرد که قیمتش از تلویزیون‌های OLED (دیود نورافشان) ارزان‌تر خواهد بود. این تلویزیون‌ها از فناوری نقطهٔ کوانتومی استفاده می‌کنند.

این فناوری، فیلمی از بلورهای نورافشان نازک را در نمایشگرهای بلور مایع (LCD) معمولی به کار می‌گیرد و بدین ترتیب، کیفیت تصویر را بهبود می‌بخشد. ال‌جی اعلام کرده است که تلویزیون‌های ۵۵ اینچی و ۶۵ اینچی نقطهٔ کوانتومی با کیفیت بسیار بالا را در ماه ژانویه در نمایشگاه لاس‌وگاس عرضه خواهد کرد.

شرکت ژاپنی سونی تا کنون تنها فروشندهٔ عمدهٔ تلویزیون بود که مدل‌های نقطهٔ کوانتومی را عرضه می‌کرد. یکی از جذابیت‌های این تلویزیون‌ها قیمت پایین‌ترشان نسبت به تلویزیون‌های OLED است. برای مثال، یک تلویزیون ۶۵ اینچی OLED در کره به قیمت نزدیک به ۱۱ هزار دلار عرضه می‌شود در حالی که تلویزیون مشابه نقطهٔ کوانتومی سونی ۳۸۰۰ دلار قیمت دارد.

شرکت سامسونگ نیز اعلام کرده است که فناوری نقطهٔ کوانتومی یکی از فناوری‌هایی است که این شرکت روی آن کار می‌کند. تحلیل‌گران بازار انتظار دارند که سامسونگ نیز در سال آینده به عرضهٔ این‌گونه تلویزیون‌ها بپردازد.

شرکت ال‌جی پس از سامسونگ، دومین تولیدکنندهٔ تلویزیون در جهان است.

رویترز، ۱۵ دسامبر ۲۰۱۴

شکایت دو کارمند از سونی

دو کارمند سابق سونی علیه آن شرکت دادخواستی را تقدیم دادگاه کرده‌اند و ادعا کرده‌اند که سونی حفاظت لازم را از اطلاعات شخصی آن‌ها در جریان حملهٔ رایانه‌ای ماه نوامبر به عمل نیاورده است. این دو نفر از سونی تقاضای غرامت کرده‌اند و هزاران کارمند سابق و فعلی این شرکت نیز در صورت تمایل می‌توانند به این دو بپیوندند.

در این دادخواست آمده است: «سونی علیرغم ضعف‌های شناخته شده‌ای که سال‌ها وجود داشت به ایمن‌سازی سیستم‌های رایانه‌ای، کارسازها و دادگان‌های خود نپرداخته زیرا براساس یک تصمیم مدیریتی، خطر از دست دادن اطلاعات براثر رخنه‌گری را پذیرفته بوده است.»

مدیریت سونی در هفتهٔ گذشته، طی نامه‌ای خطاب به کارمندان خود اعلام کرد که اطلاعاتی که ممکن است از دست رفته باشد شامل نام، نشانی، شمارهٔ امنیت اجتماعی، شمارهٔ گواهی نامهٔ رانندگی، شمارهٔ گذرنامه، اطلاعات حساب بانکی، اطلاعات کارت اعتباری، شناسهٔ کاربری و گذرواژهٔ رایانه و جزئیات حقوق کارمندان می‌باشد.

کامپیوتر ورلد، ۱۶ دسامبر ۲۰۱۴

توقف فروش اپل در روسیه

اپل فروش‌های برخط آیفون، آی‌پد و سایر محصولات خود را در روسیه به خاطر کاهش ارزش پول آن کشور متوقف کرد. کاهش قیمت نفت و تحریم‌های غرب باعث کاهش ۶۰ درصدی ارزش روبل شده‌اند. شرکت اپل اعلام کرده است که ناپایداری روبل، قیمت‌گذاری محصولاتش در روسیه را غیرممکن ساخته است.

آسوشیتدپرس، ۱۶ دسامبر ۲۰۱۴

چاپ سه‌بعدی در خدمت درمان سرطان

دانشمندان انگلیسی به استفادهٔ تازه‌ای از چاپ سه‌بعدی پرداخته‌اند. آن‌ها مدل‌های مشابه بخش‌هایی از بدن که گرفتار سرطان شده را با چاپگرهای سه بعدی چاپ می‌کنند تا پزشکان به طور دقیق‌تری بتوانند تومورها را هدف قرار دهند.

این آخرین نمونه از به‌کارگیری این فناوری نوپدید در امر پزشکی است. تا کنون از این فناوری در ساخت برخی پیوندهای پزشکی (ایمپلنت) استفاده شده است.

چاپ سه بعدی از طریق لایه‌گذاری مواد، شیء سه بعدی را به وجود می‌آورد. شرکت‌های خودروسازی و صنایع فضایی از آن برای تولید پیش نمون‌ها (پروتوتایپ) و نیز ایجاد ابزارهای خاص، مدل‌ها و برخی قطعات استفاده می‌کنند.

در امر پزشکی، چاپ سه‌بعدی توسط دندان پزشکان برای ساخت آرواره و دندان و برخی پیوندها استفاده می‌شود و جراحان استخوان نیز از آن برای تولید استخوان لگن استفاده کرده‌اند. در سال گذشته، دانشمندان آمریکایی موفق شدند گوش انسان را از سلّول‌های گاو به کمک چاپ سه‌بعدی رشد دهند.

کاربـرد جدید چاپ سـه بعـدی در درمان سـرطان شـامل چاپ سـه بعدی «شـبح» تومورها و اعضاء بدن بر پایهٔ تصاویر سـی‌تی اسکن گرفته شده از بیماران در حین درمان اسـت. این نمونه‌های پلاسـتیکی سـپس با مایع پر می‌شـود تا پزشـکان بتوانند به طور دقیق جریان داروهای رادیواکتیو را مشاهده کنند. این داروها، داروهایی هسـتند شـامل مـواد رادیواکتیو که به صورت وریدی تزریق می‌شوند. مشـکلی که در حال حاضر وجود دارد، انتخاب میزان دقیق داروست به نحوی که برای از بین بردن سـلّول‌های سـرطانی کافـی باشـد و به بافت‌های سـالم آسـیب نرساند. مدل‌سـازی دقیق به پزشکان امکان می‌دهد تا در آینده به کمک چاپ سه بعدی، میزان دقیـق داروی مصرفی را تعیین کنند. نکتهٔ مهم این است که مدل تولید شده برای هر شـخص متفاوت خواهد بود و پزشـکان براسـاس آن می‌توانند میـزان مصرف دارو را بـرای هر بیمار به طـور اختصاصی تعیین کنند.

رویترز، ۱۶ دسامبر ۲۰۱۴

سـخت‌گیری چین به شرکت‌های آمریکایی

در سـال جـاری میـلادی، دولـت چیـن محدودیت‌های زیادی را بر روی شـرکت‌های فناوری خارجی درون مرزهایش اعمال کرده اسـت. رئیس جمهـوری جدید این کشـور، ژی‌جین‌پینـگ، سیاسـت‌های جدیـدی را اعلام کرده که هدفش تقویت صنایع فناوری داخلـی چین و محافظـت از آن‌ها در مقابل تهدیدهای امنیت رایانه‌ای است.

شـرکت‌های اینترنتی آمریکایی مدت‌هاست که به دلیل قوانین سـفت و سـخت سانسور در چیـن، بـرای کار کـردن در این کشـور مشـکل دارند، امّا در سال ۲۰۱۴ این چالش به سایر صنایع فناوری مانند نرم‌افزار، شبکه، ریزپردازنده‌ها و ابزارهای امنیتی نیز گسترش یافته است.

شـرکت کلـکام ممکـن اسـت بـا پرداخت میلیاردهـا دلار جریمـه به خاطـر چگونگی مجوّزدهی به حـق اختراعش در چین روبرو گردد. مایکروسافت نیز ممکن است با جریمهٔ مشـابهی به خاطر نحوهٔ توزیع نرم‌افزار روبرو شـود. این موضوع پـس از آن بالا گرفت که ادوارد اسـنودن ادعا کرد که آمریکا از طریق مسـیریاب‌های شـبکه و سـایر تجهیزات به جاسوسی از کسب و کارهای چینی می‌پردازد. ژی‌جیـن پینگ در ماه فوریـه اعلام کرد که «بدون امنیـت رایانه‌ای، امنیـت ملّی وجود نخواهد داشـت» و یک کمیتهٔ دولتی را برای حفاظت کشـور در مقابل تهدیدهای رایانه‌ای تشـکیل داد. سـه ماه بعد، دولت چین اعلام کرد که یک سیسـتم بازبینی درسـت کرده اسـت که تمام محصولات فنـاوری اطلاعات را از نظـر تهدیدات امنیتی بررسـی می‌کند و شـرکت‌هایی کـه نتوانند از ایـن بازبینی عبور کنند، از فروش محصولاتشـان در چین جلوگیری خواهد شد.

یک دهه قبل، شـرکت‌های فنـاوری چینی از همتایـان آمریکایـی خـود بسـیار عقب بودند امّا امروز نام‌هایـی چون ژیائومی، لنوو و هـواوی بر بازار داخلی چین تسـلّط دارند. نشـان‌های تجاری (برند) داخلی، ۸۷ درصد بازار تلفن‌هـای هوشـمند و ۹۱ درصد بازار رایانه‌های رومیزی را در اختیار دارند.

شـرکت‌های آمریکایی نگران این هستند که اگر به دلیل قوانین جدید، بازار را به همتایان چینی خود واگـذار کنند، بازسـتانی آن در آینده برایشان خیلی دشوار خواهد بود.

با وجـود محدودیت‌های تازه، نقاط روشـنی نیز امسال برای فروشندگان آمریکایی وجود داشـت. مایکروسافت سـرانجام توانست پس از برداشـته شـدن ممنوعیت سـیزده ساله فروش پیشانه‌های (کنسـول) بازی خارجی، بـه فروش اکس‌باکـس در چین بپـردازد. و لینکداین (LinkedIn) نیز در ماه فوریه با یک وبگاه محلّی وارد بازار چین شـد. البته در هر دو مورد، شرکت‌ها باید قوانین سانسور چین را رعایـت کنند. به طور مثال، مایکروسـافت قـادر نخواهد بود بازی‌های خشـن‌تر خود را به فروش برسـاند و لینکدایـن نیز پیام‌های انتقادی از دولت چین را برای کاربران چینی مسدود کرده است.

کامپیوتر ورلد، ۱۶ دسامبر ۲۰۱۴

برنامـهٔ کاربـردی بـرای کنتـرل سلامتی

گروهی از کارمندان سـابق گوگل با انتشـار یک برنامهٔ کاربردی (app) رایگان، قصد دارند دانش پزشـکی مردم جهان را افزایش دهند. این کار از طریق یک آزمون بهرهٔ هوشی (IQ) انجام می‌گیرد.

این برنامهٔ کاربردی که Hi.Q نام دارد و برای آیفون و آی‌پد اپل عرضه شده است شامل ده هزار سـؤال در ۳۰۰ موضـوع مختلف، مانند حساسـیت غذایی، سـلامت دوران کودکی و کنتـرل وعدهٔ غذایی می‌باشـد. پس از آن که کاربـر آزمون را انجام داد، میزان تجربه و آگاهیش در زمینه‌های مختلف پزشکی را به تفکیک دریافت خواهد کرد.

سرپرسـت این پروژه، مونجال شـاه است که شـرکت قبلیش Like.com را در سال ۲۰۱۰ بـه گـوگل فروخـت. او می‌گویـد داده‌های اولیه نشـان می‌دهد که ارتباطـی قوی بین «سـواد» بهداشـتی و چاقی وجـود دارد. او عقیده دارد که تولید دسـتگاه‌های پوشیدنی برای ردگیری وضعیت سـلامتی و تندرستی، بسـیار زودهنگام بوده است. مطالعات جدید نشان می‌دهد که یک سوم کسانی که از این دستگاه‌ها خریداری کرده‌اند، پس از شش ماه آن‌ها را کنار گذاشته‌اند.

تیم Hi.Q عقیده دارند که نخستین گام برای آن که مـردم به طور روزانـه درگیر موضوع سلامتی‌شـان گردند، «دانـش کمیّت‌پذیر» است.

مونجال شـاه که برای این پروژه شـرکت تازه‌ای را تأسـیس کـرده می‌گوید تاکنون ۲۵۰ هزار نفر از نسخهٔ آزمایشی این برنامهٔ کاربـردی اسـتفاده کرده‌انـد. ۸۴ درصد کسـانی که این آزمون را انجام داده‌اند زن بوده‌اند و بین ۳۰ تا ۶۰ سـال داشته‌اند. او می‌گوید از مشاورهٔ پزشکان متخصص برای

تنظیم پرسش‌های آزمون استفاده کرده است.

رویترز، ۱۵ دسامبر ۲۰۱۴

کار در شرکت‌های غیرفناوری

وبگاه شغلی Glassdoor مطابق معمول هر سال، فهرست بهترین ۵۰ محل کار در آمریکا در سال بعد (۲۰۱۵) را منتشر کرد. این فهرست، رتبه‌بندی سالانهٔ شرکت‌هایی با حداقل ۱۰۰۰ کارمند است و بر پایهٔ نظرخواهی از کارمندان تهیه می‌شود. فهرست امسال شامل ۱۴ شرکت فناوری است و در صدر آن شرکت گوگل قرار دارد. امّا وضعیت برای سایر شرکت‌های بزرگ فناوری به این خوبی نیست. برخی از آن‌ها رتبه‌های پایین‌ترین را نسبت به سال قبل به دست آورده‌اند و بعضی دیگر به کلّی از فهرست خارج گشته‌اند.

گوگل در فهرست سال گذشته در مکان هشتم قرار داشت که امسال به مکان نخست صعود کرده است. اپل نیز از رتبهٔ ۳۵ به رتبهٔ ۲۲ آمده است. شرکت مَت ورکز، سازندهٔ نرم‌افزار مَت‌لب و سایر نرم‌افزارهای رایانش ریاضی، نیز چند پله صعود داشته است و از مکان ۲۲ به ۱۹ ارتقاء یافته است. شرکت‌های فناوری که تازه وارد این فهرست شده‌اند عبارتند از اِنویدیا(رتبهٔ ۶)، ادوبی (رتبهٔ ۱۸) و زیلو (رتبهٔ ۳۳).

براساس فهرست منتشر شدهٔ امسال، کار در شرکت‌های بزرگ فناوری به خوبی سال قبل نیست. در سال ۲۰۱۴، ۲۲ شرکت فناوری در فهرست بهترین ۵۰ محل کار قرار داشتند که امسال به ۱۴ شرکت تقلیل یافته‌اند. در بین شرکت‌های فناوری که رتبه‌شان در فهرست ۲۰۱۵ کاهش یافته می‌توان به لینکداین (از رتبهٔ ۳ به ۲۳)، فیسبوک (از رتبهٔ ۵ به ۱۳) و اوربیتز (از رتبهٔ ۹ به ۴۲) اشاره کرد. شرکت‌های بزرگی که در فهرست ۲۰۱۴ قرار داشتند و از فهرست ۲۰۱۵ خارج شده‌اند، عبارتند از توئیتر (رتبهٔ ۲ در ۲۰۱۴)، ردهت (رتبهٔ ۲۳)، رَک اسپیس (رتبهٔ ۳۰)، اینتل (رتبهٔ ۳۳)، سیتریکس (رتبهٔ ۳۸)، eBay (رتبهٔ ۴۹) و سیلزفورس (رتبهٔ ۵۰).

۱۷ شرکت جدیدی که امسال وارد فهرست شده‌اند به صنایع مختلفی چون خدمات کسب و کار، حسابداری، زیست فناوری، تولید، بهداشت، رسانه، ساختمان، کشاورزی و غذایی تعلّق داشته‌اند.

انتشار فهرست ۲۰۱۵ ممکن است باعث شود سایر کسب و کارها دست بالاتری برای استخدام کارمندان ماهر و بااستعداد پیدا کنند.

آی‌تی ورلد، ۱۶ دسامبر ۲۰۱۴

ماشین «شبح» برای هدایت رانندگان

شرکت جگوارلندرور از پروژهٔ پژوهشی خود پرده برداشت: یکی نمایشگری که به راننده نمای ۳۶۰ درجه‌ای از بیرون خودرو می‌دهد و دیگری یک ماشین «شبح» که در جلوی خودرو حرکت می‌کند و راننده باید آن را دنبال کند.

ماشین شبح یک وسیلهٔ کمک ناوبری است که برای جاده‌های شلوغ طراحی شده است. راننده نمای یک خودرو را در جلو خودروی خود می‌بیند و بدون آن که نیاز به دیدن علائم جاده داشته باشد، فقط آن خودرو فرضی را تا مقصد دنبال می‌کند.

این شرکت خودروسازی انگلیسی همچنین بر روی ساخت یک سقف شفاف مجازی کار می‌کند که به راننده نمای ۳۶۰ درجه از بیرون خودرو را نشان می‌دهد. این فناوری از طریق دادن یک صفحهٔ نمایشگر در روی هر ستون سقف در داخل خودرو عمل می‌کند. این صفحات، فیلم‌های ویدیویی را از دوربین‌های پوشش دهندهٔ زوایای خارج از خودرو که معمولاً به دلیل ستون‌های سقف کور شده‌اند، نمایش می‌دهند. پیاده‌ها، دوچرخه‌سوارها و سایر وسایل نقلیه، دور تا دور خودرو قابل مشاهده خواهند بود. هنگامی که خودرو به تقاطع می‌رسد، سیستم به طور خودکار، ستون سقف چپ یا راست را شفاف می‌سازد.

کامپیوتر ورلد، ۱۶ دسامبر ۲۰۱۴

فیزیک کوانتومی در خدمت احراز هویت

پژوهشگران در هلند با استفاده از فیریک کوانتومی، کارت‌های اعتباری و کارت‌های شناسایی ضدّ تقلّب ساخته‌اند. این رویکرد که آن‌ها آن را احراز هویت امن کوانتومی (QSA) نامیده‌اند، بر روی ذرات منفرد نور، یا فوتون، و قابلیت آن‌ها برای رمزگذاری داده‌ها به نحوی که رخنه‌گران نتوانند اطلاعات را شناسایی کنند، تمرکز دارد. این فناوری از یک خاصیت فوتون‌ها که به آن‌ها اجازه می‌دهد در آن واحد به نحو مؤثری در چند جا قرار داشته باشند، بهره می‌گیرد. این پدیده در فیزیک کوانتومی توصیف شده است.

پژوهشگران در دانشگاه توئنته و دانشگاه فناوری آیندهوون یک کارت اعتباری را با لایهٔ نازکی از رنگ سفید شامل میلیون‌ها ذرهٔ نانو پوشش داده‌اند. هنگامی که نور به ذرات نانو برخورد می‌کند، این سو و آن سو می‌رود تا در نهایت خارج گردد و در این فرایند، الگوی یگانه‌ای تولید می‌کند که به موقعیت دقیق ذرات در رنگ بستگی دارد. کارت‌ها در سیستم توسط نحوه‌ای که نور را منعکس می‌کنند «ثبت» می‌شوند.

برای احراز هویت کارت، ماشین بانک نوری را به رنگ روی کارت می‌تاباند که برای هر تراکنش یگانه است. در صورتی که الگوی نور ظاهر شد، کارت قابل احراز هویت می‌گردد. بنا بر خاصیت فیزیک کوانتومی، تلاش برای مشاهدهٔ فرایند پرسش و پاسخ بین کارت‌خوان و کارت، باعث خراب شدن اطلاعات می‌گردد. به گفتهٔ پژوهشگران، حتی اگر یک نفر اطلاعات کاملی از چگونگی ساخت کارت داشته باشد، فناوری به او اجازه ساخت یک کپی از آن را نمی‌دهد. ذرات نانو بسیار ریزند و تعداد زیادی از آن‌ها وجود دارد که باید با دقت بسیار زیاد قرار داده شوند. در کاربردهای واقعی، به جای رنگ که نرم و در مقابل حرارت و رطوبت ناپایدار است از سرامیک استفاده خواهد شد.

آی‌دی‌جی نیوز، ۱۶ دسامبر ۲۰۱۴

پارک کردن خودرو با ساعت هوشمند

شرکت خودروسازی بی‌ام‌و یک سیستم دستیار پارک خودرو تولید کرده که به کمک آن شما دیگر نیاز ندارید خودتان به پارکینگ بروید خودرو خودش جایی برای پارک کردن پیدا خواهد کرد. این ویژگی که توسط یک ساعت هوشمند قابل کنترل است در نمایشگاه بین‌المللی CES در ماه ژانویه به نمایش گذاشته خواهد شد.

راننده از خودرو پیاده می‌شود و دستیار پارک را بر روی تلفن هوشمندش فعّال می‌سازد. حسگرهای نصب شده در خودرو به اضافهٔ نقشه‌های دیجیتال پارکینگ، ویژگی‌های ساختاری پارک خودرو را تشخیص می‌دهند و از موانع غیرمنتظره، مانند خودروهایی که به طرز ناصحیحی پارک کرده‌اند، دوری می‌کنند. پس از آن که خودرو در فضای مناسب پارک شد، خودش را قفل می‌کند.

راننده می‌تواند با فراخوانی خودرو باعث شود که خودرو خودش از پارکینگ خارج شود و جلو پای راننده بایستد.

کنترل کاملاً خودکار خودرو از طریق ترکیب حسگرها و نقشه‌های دیجیتال، دستاورد مهمی است. این کار، وابستگی به سیستم‌های مکان‌یاب جغرافیایی (GPS) را که برای پارکینگ‌های چند طبقه به قدر کافی دقیق نیستند، از بین می‌برد.

حسگرها که نمای ۳۶۰ درجه دارند، هنگامی که راننده داخل خودرو است نیز برای جلوگیری از تصادف در محیط‌های با دید کم به کار می‌آیند.

آی‌دی‌جی نیوز، ۱۶ دسامبر ۲۰۱۴

پرداخت حق اشتراک مجلّه تایم با بیت کوین

شرکت انتشاراتی تایم که ناشر بیش از ۹۰ روزنامه و مجلّه است اعلام کرد که بیت کوین را به‌عنوان گزینه‌ای برای پرداخت حق اشتراک تعدادی از عناوینش می‌پذیرد. مجلات فورچون، Health، تراول پلاس و This Old House نخستین عناوینی هستند که پول دیجیتال را برای پرداخت حق اشتراک می‌پذیرند.

در اوایل امسال، پول دیجیتال رسماً توسط جری براون، فرماندار کالیفرنیا، به‌عنوان پول معتبر در این ایالت پذیرفته شد. این در حالی است که وضعیت در کشورهای دیگر متفاوت است. به طور مثال، در استرالیا پول‌های دیجیتال مانند بیت کوین در دست ارزیابی هستند و در چین، هر نوع معامله با بیت کوین ممنوع است.

زد دی نت، ۱۷ دسامبر ۲۰۱۴

زبان‌های جدید تابعی

افق برنامه‌نویسی تابعی با دو زبان جدیدی که در دست تهیه است، رو به گسترش می‌باشد. این دو زبان یکی استریم (Streem) است که توسط بنیان‌گذار زبان روبی طراحی شده و دیگری موچی (Mochi) که شبیه پایتون است.

زبان استریم که زادهٔ فکر یوکی هیرو ماتسوموتو، خالق زبان روبی است، یک زبان نوشتاری همروند است که بر پایهٔ یک مدل برنامه‌نویسی مشابه با پوسته (شِل) و تحت تأثیر روبی، ارلانگ و سایر زبان‌های برنامه‌نویسی تابعی بنا شده است.

به گفتهٔ ماتسو موتو هنوز خیلی کار تا عرضهٔ نسخهٔ الف (آلفا) این زبان باقی مانده و او از این که هم‌اکنون بسیاری دربارهٔ این زبان صحبت می‌کنند شگفت زده شده است. به گفتهٔ وی زبان استریم برای پردازش متن و برنامه‌نویسی وب مناسب خواهد بود. استریم زبان‌های تابعی را در محیط‌های پویا به کار می‌بندد. در خواستی می‌رسد، وضعیت داده‌ها تغییر می‌کند و تابعی برای اجرا فراخوانده می‌شود. این الگوی کار در زبان استریم خواهد بود.

زبان موچی ترکیبی از مفاهیم تابعی و پویاست. در واقع یک زبان برنامه‌نویسی با نوع‌بندی پویا برای برنامه‌نویسی تابعی است. مفسّر آن به زبان پایتون ۳ نوشته شده و برنامهٔ نوشته شده به موچی را به کد بایتی پایتون ۳ ترجمه می‌کند. قواعد نحوی آن نیز شبیه پایتون است و کلان دستورهایی (مکرو) شبیه کلان دستورهای لیسپ دارد. نویسندهٔ این زبان، یاشوشی ایتو است.

اینفو ورلد، ۱۵ دسامبر ۲۰۱۴

جایزهٔ گوگل برای اینترنت اشیاء

اگر ایده‌ای دربارهٔ چگونگی کار اینترنت اشیاء (IoT) دارید، می‌توانید آن را برای گوگل بفرستید و چنانچه ایدهٔ شما به قدر کافی خوب باشد، گوگل به شما جایزهٔ نقدی خواهد داد.

گوگل به عنوان بخشی از تلاش‌های تازه برای تولید فناوری‌های بیشتری برای اینترنت اشیاء، بودجهٔ قابل ملاحظه‌ای در نظر گرفته که در اختیار پژوهشگران این حوزهٔ نوپای رایانش بگذارد.

منظور از اینترنت اشیاء، اتصال تمام دستگاه‌ها به هم از طریق اینترنت است که تحقق آن نیاز به کار بر روی سیستم‌های ناهمگن و متصل به هم دارد و ملاحظات خاصی برای امنیت و محرمانگی آن باید به عمل آید. بنابر پیش‌بینی سیسکو تا سال ۲۰۲۰ بیش از ۵۰ میلیارد شیء به هم متصل خواهند شد.

گوگل دو دسته جایزه برای کار در زمینهٔ اینترنت اشیاء در نظر گرفته است. دستهٔ اول برای تیم‌های بزرگ‌تر است و گوگل بین ۵۰۰ تا ۸۰۰ هزار دلار در صورت تکمیل پروژه به آن‌ها می‌پردازد. دستهٔ دوم که به پروژه‌های کوچک‌تر تعلّق می‌گیرد بین ۵۰ تا ۱۵۰ هزار دلار است. این جایزه‌های نقدی به راه‌حل‌های جدید و ابتکاری در زمینه‌های رابط کاربری و تولید برنامه، امنیت و محرمانگی،و سیستم‌ها و قراردادها (پروتکل) پرداخت می‌گردد.

تاریخ ارسال طرح‌ها تا ۲۱ ژانویهٔ ۲۰۱۵ خواهد بود.

آی‌دی‌جی نیوز، ۱۲ دسامبر ۲۰۱۴

قانون ساکس (SOX) و چارچوب کوبیت (COBIT): سیر تحولی ممیزی فناوری اطلاعات

سید علی آذرکار
شرکت مهندسی پدیدپرداز، کمیسیون استاندارد و تدوین مقررات، سازمان نظام صنفی رایانه‌ای استان تهران
پست الکترونیکی: ali.azarkar@pdpsoft.com

مقدمه

در این مقاله سعی شده تا ریشه‌های تاریخی و ضرورت‌های ممیزی فناوری اطلاعات ارایه شود. هدف از این مقاله، چگونگی شکل‌گیری موضوع «ممیزی فناوری اطلاعات» و هم‌چنین بررسی چارچوب کوبیت، به عنوان نقشه‌راهی برای پیاده‌سازی اصول راهبری و ممیزی فناوری اطلاعات است.

راهبری فناوری اطلاعات، اصولاً به نحوه استفاده از فناوری اطلاعات در پشتیبانی و حمایت از فرآیندهای کسب‌وکار سازمان‌ها می‌پردازد. از آن‌جا که اولاً موضوع راهبری فناوری اطلاعات با سایر راهبردهای سازمان در تعامل بوده و ثانیاً، به دلیل تنوع و گستردگی استفاده، باعث تحول بنیادین در کسب‌وکار (از طریق ارایه راهکارها و سازوکارهای جدید) شده، مخاطبین این حوزه نوعاً مدیران ارشد و اجرایی سازمان‌ها هستند.

برای استفاده بهینه از فناوری اطلاعات، مدیران نیاز دارند درک درستی از فرصت‌ها و تهدیدهای ایجاد شده توسط فناوری اطلاعات داشته، زمینه بهره‌گیری از فرصت‌ها را فراهم آورده، مخاطرات مربوط به استفاده از فناوری اطلاعات را کاهش یا مهار کرده، و در نهایت، تاثیر استفاده از آن را بر کسب‌وکار ارزیابی کنند. بنابراین، فناوری اطلاعات و به‌کارگیری آن باید مانند سایر عوامل سازمانی، «کنترل» شود.

تاریخچه اجمالی قانون‌گذاری کنترل‌های داخلی

موضوع «کنترل» در سازمان‌ها، ریشه در «کنترل‌های مالی» یا به عبارت وسیع‌تر، «کنترل‌های داخلی» سازمان دارد. از آن‌جا که بسیاری از سامانه‌های کنترل داخلی مستقیماً به پردازش تراکنش‌ها (مالی) مرتبط است، حسابداران اولین مشارکت‌کنندگان اصلی در حصول اطمینان از مناسب بودن کنترل‌ها بوده‌اند.

نیاز به ایجاد سامانه‌هایی برای کنترل داخلی در سازمان، متاسفانه ریشه در رسوایی‌های مالی برخی شرکت‌های بزرگ بین‌المللی در دهه‌های گذشته داشته، که منجر به از دست دادن اعتماد مردم به بازار سرمایه و بنگاه‌های اقتصادی شد. مهم‌ترین وقایعی که به لحاظ تاریخی در زمینه قانون‌گذاری در مباحث کنترل داخلی مطرح بوده، به شرح زیر است [۱]:

- اولین شوک به بازار بورس در سال ۱۹۲۹ در ایالات متحده آمریکا وارد شد، که ماحصل یک تقلب مالی جهانی بود. پس از آن، دولت ایالات متحده دو قانون را با هدف بازگرداندن اعتماد مردم به بازار بورس تهیه و مصوب کرد. اولین قانون در سال ۱۹۳۳ (با نام «قانون اوراق بهادار»[1]) و دومی در سال ۱۹۳۴ با نام («اوراق بهادار بورس یا SEC»[2]) به تصویب رسید. به تبع قانون دوم، استانداردهایی برای ممیزی تدوین شد. این قانون هم‌چنین شرکت‌های تجاری عام را مکلف به ممیزی توسط ممیزان مستقل می‌کند.

قانون حق‌طبع[3]: این قانون- که نسخ مختلفی هم داشت- نرم‌افزار و سایر دارایی‌های معنوی را به جمع مواردی در قوانین حفظ حق‌طبع، اضافه کرد.

1- Securities Act
2- Securities and Exchange Commission
3- Copyright

- قانـون رفتار فاسـد خارجـی (FCPA)[4]: ایـن قانون که در سـال ۱۹۷۹ مصوب شـد، به دلیل افشـای نقش مدیران در دادن رشوه و حق‌السـکوت به سازمان‌های خارجی از محل منابع مالی سازمان بـود. در این قانون شـرکت‌هایی که تحت قانون SEC ثبت شـده بودند، ملزم شـدند که سوابق دربرگیرنده تراکنش‌ها و جایگاه مالی سـازمان را نگهداشته و سامانه‌ای برای کنترل‌های داخلی، با هدف ارایه اطمینان از تحقق اهداف سازمانی، ایجاد و نگهداری کنند.
- کمیته سازمان‌های حامی[5]: این کمیته پس از رسوایی شرکت S&L، در دهه ۱۹۸۰ شکل گرفت. این کمیته با نام COSO شناخته می‌شود. این کمیته به دلیل شناسایی نیاز به ایجاد کنترل‌های سخت‌گیرانه داخلی، تصمیـم گرفت مدلی اثربخـش برای کنترل‌های داخلـی (از دیدگاه مدیریت) ایجاد کند. خروجی این کمیته مدلی با نام COSO بود.

بحـث تقلب‌هـای مالی تـا اوایـل دهه ۲۰۰۰ هـم ادامه داشـت. در نتیجـه چندین رسـوایی بزرگ مالی چندین شـرکت بـزرگ (مانند WorldCom و Enron)، و تحمیل خسـارات زیاد به سـهام‌داران، فشـار زیادی بر کنگره آمریکا با هدف محافظت از عامه مردم در قبال این‌گونه رویدادها و اتفاقات، وارد شد. این فشار منجر به تصویب قانونی در سال ۲۰۰۲ شـد که توسط دو سناتور با نام‌های ساربنس[6] (سناتور دمکرات از ایالـت مریلند) و آکسـلی[7] (سـناتور جمهوریخـواه از ایالت اوهایو) تدویـن و در ۳۰ ژوئیـه ۲۰۰۲ پس از تصویب سـنا، به امضای جورج دبلیـو بوش، رئیس جمهوری آمریکا رسـید. این قانون که هم‌اکنون با نام تهیه‌کنندگان، آن به ساکس (SOX) معروف است، از تلاش‌ها برای جلب اعتماد عمومی به بازارهای سـرمایه حمایت و پشتیبانی می‌کند. علاوه بر آن، در این قانون روش‌هایی برای راهبری شرکتی (سازمانی)، کنترل‌های داخلی و کیفیت ممیزی نیز طرح شـده است. به طور ویژه، ایـن قانون از شـرکت‌های عمومی درخواسـت می‌کند که سـامانه‌ای مناسـب برای مدیریت و پایش کنترل‌های داخلی بتعریف شده ر روی فرآیند تهیه گزارش‌های مالی، پیاده‌سازی و نگهداری کنند.

۳- قانون ساکس

این قانون دارای بخش‌های متعددی است که به نقش مدیریت سازمان برای ایجاد و مراقبت از کنترل‌های داخلی می‌پردازد. دو بخش از این قانون، منشأ ایده‌هایی است که بعداً در مدل‌ها و چارچوب‌های مربوط به ممیزی فناوری اطلاعات به‌کار گرفته شد. این دو بخش در ادامه به اجمال بیان شده است -[۲-۳].

۳-۱- بخش ۴۰۴

بخش ۴۰۴ از قانون ساکس، با عنوان «ارزشیابی مدیران از کنترل‌های داخلی»، مدیریت شـرکت‌های عمومی را ملزم می‌کند که اثربخشـی کنترل‌های داخلی خود را ارزیابی و در گزارش سالانه خود موارد زیر را مد نظر قرار دهند:

- درک گردش‌کار تراکنش‌ها، شامل ابعاد فناوری اطلاعات
- ارزیابی اثربخشـی طراحی و اجـرای کنترل‌های منتخب داخلی، با رویکردی مبتنی بر مخاطره
- ارزیابی تقلب‌های بالقوه در سامانه‌ها و ارزیابی کنترل‌هایی که برای پیشگیری یا کشف آن طراحی شده
- ارزیابی و جمع‌بندی کفایـت کنترل‌ها بر روی فرآیند گزارش‌دهی صورت‌های مالی
- ارزیابی کنترل‌هایی در گستره سازمان که متناظر اجزای چارچوب COSO است.

طبـق این بخـش، مدیریت شـرکت، مدیـران اجرایـی و مالی باید فعالیت‌های زیر را انجام دهند:

- ارایه اظهارنامه‌ای مبتنی بر تعهد مدیریت برای تعریف و نگهداشت کنترل‌های داخلی قابل قبول بر روی گزارش‌دهی مالی هر سازمان
- ارایـه اظهارنامه که چارچوب مورد اسـتفاده مدیریـت برای انجام ارزیابی‌های مورد نیاز در مورد اثربخشـی کنترل‌های داخلی تعریف شده برگزارش‌دهی مالی را معرفی کند.
- ارزیابی اثربخشی کنترل‌های داخلی تعریف شده بر روی گزارش‌دهی مالی، در سـال مالی اخیر، به همراه یـک اظهارنامه صریح دال بر اثربخش بودن این کنترل‌ها
- ارایه اظهارنامه در خصـوص ارزیابی مدیریتِ کنترل داخلی تعریف شـده بر روی گزارش‌دهی مالی که توسـطِ یک موسسه ثبت‌شده حسابرسی عمومی تایید شده باشد، این موسسه باید جزء موسساتی باشـد که ممیزی اظهارنامه‌های مالی را که در گزارش‌های سـالانه منتشر می‌شوند برعهده دارند.
- ارایه مسـتند نتیجه‌گیری درباره اثربخش بودن کنترل‌های داخلی تعریف شده بر روی گزارش‌دهی مالی به صورت کتبی.
- متعهد شـدن مدیریت به رفع نقاط ضعف گزارش شـده بر اساس ممیزی تا پایان سـال مالی بعـدی (در صورتی‌که نقطه ضعفی در زمینه کنترل‌های داخلی بر اساس ممیزی در سازمان مشخص شود مدیریت علاوه بر تعهد به رفع آن اجازه اعلام فرآیند کنترل داخلی را به عنوان یک فرآیند تاثیرگذار ندارد.).

این بخش هم‌چنین اشاره می‌کند که: تهیه‌کنندگان گزارش‌های مالی ملزم به انتشـار اطلاعات مربوط به محدوده و کفایت سـاختار کنترل داخلـی و رویه‌ها برای گزارش‌دهی مالی در گزارش‌های سـالانه خود هسـتند. این اطلاعات باید هم‌چنین اثربخشـی این گونه کنترل‌ها و رویه‌ها را ارزشیابی کند.

۴- بخش ۳۰۲

طبق بخش ۳۰۲ قانون سـاکس، با عنوان «مسـئولیت شرکتی برای

4- Foreign Corrupt Practices Act
5- Committee of Sponsoring Organizations (COSO)
6- Paul S. Sarbanes
7- Michael G. Oxley

گزارش‌های مالی»، مدیریت سازمان با مشارکت مدیران اصلی اجرایی و مالی:

- تایید می‌کنند که مدیران، مسئول ایجاد و نگهداری کنترل‌های داخلی بر روی گزارش‌های مالی هستند.
- تاییـد می‌کنند که مدیران این‌گونـه کنترل‌ها بر روی گزارش‌های مالی را طراحی کرده یا طراحی با نظارت آن‌ها انجام می‌شود. هدف این کنترل‌ها، حصول اطمینان از تضمین معقول نسـبت به قابلیت اطمینـان گزارش‌های مالی و تهیـه صورت‌های مالی برای مصارف خارجی، طبق اصول پذیرفته شده حسابداری، است.
- هـر تغییر در کنترل داخلی سـازمان مرتبط با گزارش‌گیری مالی، کـه در مقطع مالی قبلی رخ داد و بر این کنترل‌ها اثرگذار بوده (یا احتمال آن وجود دارد که اثرگذار باشد) باید افشا شود.
- هنگامـی که علت یک تغییر در کنتـرل داخلی گزارش‌دهی مالی، اصلاح یـک منطقه ضعـف مهـم و تعیین‌کننده اسـت، مدیریت مسـئولیت دارد که تعیین کند آیا علت تغییر و مقتضیات پیرامونی آن آن‌قـدر حیاتی بوده که ضرورت داشـته باشـد در مورد این‌که تغییر گمراه کننده نیست، روشنگری شود.

بخش ۳۰۲ هم‌چنین اشـاره می‌کند که: مدیر ارشد اجرایی (CEO) و مدیر ارشد مالی (CFO) تصدیق می‌کنند که صورت‌های مالی واقعی، کامل و دقیق بوده و کنترل‌های کافی برای گزارش‌دهی مالی و افشـا (ی غیرمجاز) وجود دارد.

این فعالیت‌ها در ارزیابی فصلی و سالانه انجام می‌شود.

۴-۱- استاندارد AS 5

در سـال ۲۰۰۳، هیات نظارت بر حسابداری شرکت‌های سهامی عام (PCAOB)[8] اسـتاندارد کلیدی AS 2 را منتشر کرد که پیشران اصلی برای ممیزی اثربخشـی قانون سـاکس بود. این اسـتاندارد در سـال ۲۰۰۷ با استاندارد AS 5 جایگزین شد.

اسـتاندارد AS 5 نیازمندی‌های ممیزی را سـاده کرده و یک دیدگاه بـالا به پاییـن مبتنی بر مخاطرات را برای طراحـی و اجرای ممیزی کنترل‌های داخلی ارایه می‌کند. تمرکز این استاندارد بر روی آزمودن اثربخشـی کنترل‌های سازمانی اسـت که گرایش به مخاطرات ذاتی سازمان دارند [۲].

۵- چارچوب کوبیت

هدف بسـیاری از سازمان‌ها بهبود رشد و توسـعه مزیت‌های رقابتی، هم‌زمان با اسـتفاده از فنـاوری اطلاعات به‌منظـور افزایش راندمان، انعطاف‌پذیری و نوآوری اسـت. پیش‌نیاز این‌گونه راهبردها، درک یک مفهوم «کیفی» از فناوری اطلاعات و تعریف اهداف کنترلی به منظور تضمین این مفهوم کیفی است.

اهـداف کنترلی برای اطلاعات و فناوری‌های وابسـته، که به اختصار COBIT[9] نامیده می‌شـود، چارچوبی اسـت که توسط موسسه ایساکا (ISACA)[10] بـرای راهبری و مدیریت فناوری اطلاعات در سـازمان‌ها ارایه شـده اسـت. این چارچوب در واقع به مدیران ارشـد سازمان‌ها کمک می‌کند تا خلأ بین الزامات کنترلی، موضوعات فنی، و مخاطرات کسـب‌وکاری را پر کنند. علاوه بر آن، راهبری فناوری اطلاعات را از طریق هم‌سو کردن اهداف کسب‌وکاری با اهداف و فرآیندهای فناوری پشتیبانی می‌کند.

چارچوب کوبیت توسط موسسـه راهبری فناوری اطلاعات (ITGI)[11] که ارتباط نزدیکی با ایساکا دارد، تهیه و منتشر می‌شود. در حالی که ایسـاکا بیشـتر درگیر هدایت موضوع ممیزی فناوری اطلاعات است، این موسسـه بر روی تحقیق و توسـعه قواعد متمرکز اسـت. ایساکا هم‌چنیـن ارایه‌دهنده مـدرک ICSA[12] (ممیز تایید صلاحیت شـده سامانه‌های اطلاعاتی) به متخصصین است.

سوالاتی که در ذهن مدیریت ارشد سازمان در حوزه فناوری اطلاعات وجود داشـته که این چارچوب در صدد پاسـخ‌گویی به آن‌ها اسـت، عبارت است از:

- آیا سازمان فناوری اطلاعات کارهای مفیدی انجام می‌دهد؟
- آیا کارها به طریق درست انجام می‌شود؟
- آیا کارها به طریق درست به پایان می‌رسد؟
- آیا سازمان از این کارها بهره‌مند می‌شود؟

بـر این اسـاس، چارچـوب کوبیت تـلاش کرده تـا اسـتانداردها و بهروش‌های صنعـت را در حوزه‌های زیر به‌کار گرفته و یکپارچه کند (شکل شماره ۱) [۴]:

- هم‌سویی راهبردی فناوری اطلاعات با اهداف کسب‌وکاری
- خلق ارزش از محصولات و خدمات جدید
- مدیریت مخاطره
- مدیریت منابع
- مدیریت کارایی

به‌طور مشخص، این چارچوب از استانداردهایی مانند ISO/IEC 27002 و ISO/IEC 27001 و چارچوب‌هایـی دیگـری مانند ITIL و PMBOK استفاده می‌کند.

ایـن چارچوب راهنمایـی را برای مدیریت اجرایـی، با هدف راهبری فناوری اطلاعات در سازمان، ارایه می‌دهد:

- استفاده از ابزارهای موثرتر فناوری اطلاعات برای پشتیبانی اهداف کسب‌وکاری
- ایجاد شفافیت بیشتر و قابلیت بهتر پیش‌بینی برای هزینه‌های کلی چرخه عمر فناوری اطلاعات
- کسـب اطلاعات زمان‌مندتر و با قابلیت اطمینان بیشـتر از فناوری اطلاعات

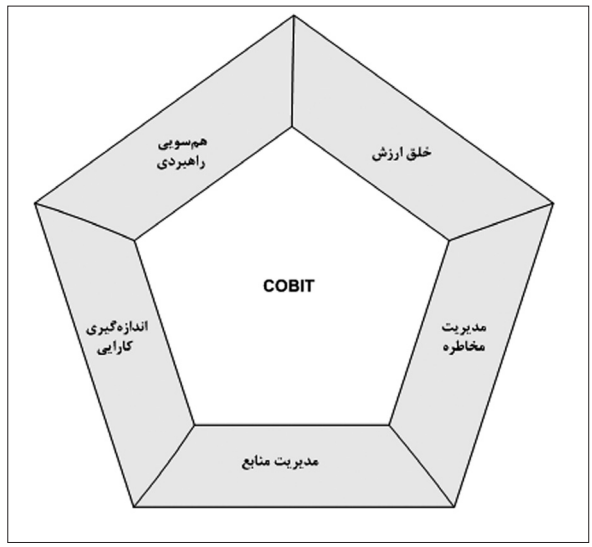
8- Public Company Accounting Oversight Board

9- Control Objectives for Information and Related Technology

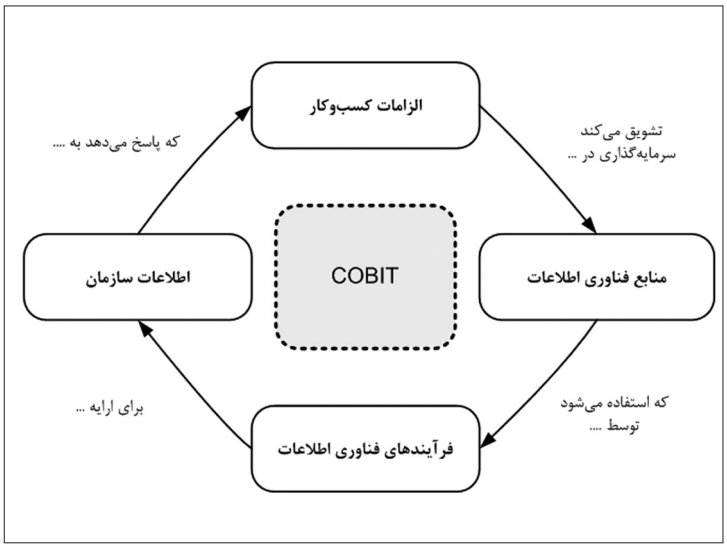
10- Information Systems Audit and Control Association

11- Information Technology Governance Institute

12- Certified Information Systems Auditor



شکل ۱: ابعاد چارچوب کوبیت



شکل ۲: اصول اولیه چارچوب کوبیت [۴]

خدمات با کیفیت‌تر فناوری اطلاعات و پروژه‌های موفق بیشتر
مدیریت اثربخش‌تر مخاطرات مربوط به فناوری اطلاعات
این چارچوب، فرآیندها، اهداف و هم‌چنین معیارهای مربوط را تعریف و نقش‌ها و مسئولیت‌ها را نیز در قبال فعالیت‌های پیش‌بینی شده، ارایه داده و تشریح می‌کند. اصول اولیه این چارچوب، در شکل شماره ۲ نشان داده شده است [۴].

۵-۱- سیر تحولی چارچوب

سیر کلی تحول این چارچوب، از زمان ارایه اولیه آن در سال ۱۹۹۶، به شرح زیر است:

- سال ۱۹۹۶: ارایه ویرایش ۱
- سال ۱۹۹۸: ارایه ویرایش ۲ با اضافه کردن کلمه «کنترل»
- سال ۲۰۰۰: ارایه ویرایش ۳ با عنوان «راهنمای مدیریت»
- سال ۲۰۰۳: ارایه یک ویرایش برخط
- سال ۲۰۰۵: ارایه ویرایش ۴
- سال ۲۰۰۷: ارایه ویرایش ۴/۱
- سال ۲۰۱۲ (ژوئن): ارایه ویرایش ۵
- سال ۲۰۱۲ (دسامبر): ارایه سند تکمیلی چارچوب کوبیت برای امنیت اطلاعات
- سال ۲۰۱۳: ارایه سند تکمیلی، چارچوب کوبیت برای تضمین

۵-۲- اجزای چارچوب

این چارچوب دارای اجزای زیر است:

- چارچوب: سازمان‌دهی اهداف راهبری فناوری اطلاعات و تجارب برتر، به تفکیک دامنه‌ها و فرآیندهای فناوری اطلاعات، و برقراری ارتباط آن با الزامات کسب‌وکار
- توصیف فرآیندی: ارایه یک مدل فرآیندی مرجع و یک زبان مشترک برای تمامی افراد در سازمان؛ این فرآیندها به حوزه‌های مسئولیتی طرح‌ریزی، ساخت، اجرا و پایش نگاشت می‌شود.
- اهداف کنترلی: ارایه مجموعه کاملی از الزامات سطح بالا برای لحاظ کردن توسط مدیریت با هدف کنترل اثربخش هر فرآیند فناوری اطلاعات
- راهنماهای مدیریتی: کمک به تفویض مسئولیت‌ها، توافق بر روی اهداف، اندازه‌گیری کارایی، و نمایش ارتباطات درونی با سایر فرآیندها
- مدل‌های بلوغ: ارزشیابی بلوغ و قابلیت به ازای هر فرآیند با هدف کمک به رفع خلاءها

۵-۳- سطوح پایش و ارزیابی

چارچوب کوبیت، ابزاری را برای پایش[۱۳] و ارزیابی[۱۴]، با هدف دسترسی به اهداف سازمان، فراهم کرده و بر این اساس، سطوح زیر را تعریف می‌کند [۵]:

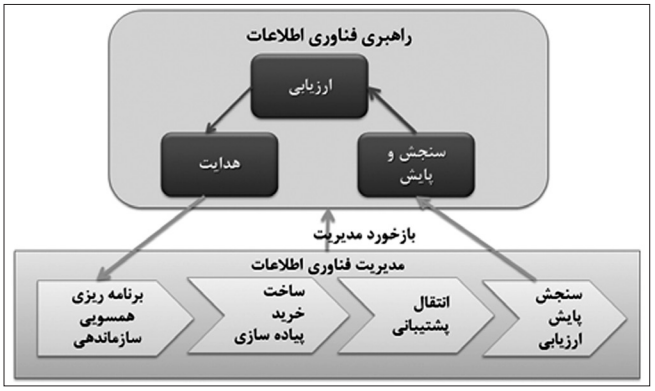
- سطح ۰: عدم وجود
- سطح ۱: پایش و ارزیابی کارایی فناوری اطلاعات
- سطح ۲: پایش و ارزیابی کنترل‌های داخلی
- سطح ۳: حصول اطمینان از تطابق با مقررات
- سطح ۴: ارایه راهبری فناوری اطلاعات

در زمان ارزیابی خدمات فناوری اطلاعات (سطح ۱) موارد زیر باید مدنظر قرار گیرد:

- در چه گستره‌ای، فرآیندهای کسب‌وکار توسط تمهیدات فناوری اطلاعات پشتیبانی می‌شود؟
- خدمات فناوری اطلاعات چه کمکی به تحقق اهداف راهبردی کسب‌وکار سازمان می‌کند؟
- آیا خدمات ارایه شده توسط فناوری اطلاعات، سازگاری و انطباق با قوانین سازمان دارد؟

در سطح ۲، یکی از حوزه‌های مهم پایش (استفاده از ابزارهای مناسب

13- Monitoring
-14Evaluation



شکل ۳: سطوح فرایندی کوبیت۵

بـرای) اندازه‌گیری و میزان انحراف از کنترل‌های داخلی و گزارش آن به مدیریت هدف است. ویژگی‌های اصلی پایش عبارت است از:

- تطابق با قوانین و مقررات
- کارایی فرآیندهای فناوری اطلاعات
- امنیت اطلاعات
- تبعیت از نقاط کنترلی برای مدیریت تغییر
- تبعیت از توافق سطح خدمت (SLA)

سطح ۳ نوعاً یک فرآیند مستقل بازنگری، اطمینان سازگاری و تطابق بـا قوانین و مقررات را به‌دسـت می‌دهد. این کار از طریق ایجاد یک منشور ممیزی و درگیر کردن یک ممیز مستقل انجام می‌شود.

هدف سطح ۴ کنترل تهیه گزارش‌هایی است که به شکل شفاف نشان می‌دهد که آیا طرح‌های فناوری اطلاعات پیاده‌سـازی شده یا خیر، و نحوه پیاده‌سازی را تشریح می‌کند.

۶- چارچوب کوبیت [۵]

انجمن کنترل و ممیزی سیستم‌های اطلاعاتی[15] که وظیفهٔ طراحی و پایش چارچوب شـناخته شده کوبیت را به‌عهده دارد، با جمع‌آوری پیشـنهادهای حاصل از اجرای چارچوب کوبیت ۴ توسط متخصصین فاوا به ارزیابی، پایش و بهبود این چارچوب اقدام و نسـخه جدید این چارچوب را تحت عنوان چارچوب کوبیت ۵ ارایه کرد. این نسـخه بر اساس ترکیب قابلیت‌های نسخه چهارم با قابلیت‌های چارچوب ارزش فنـاوری اطلاعـات[16] و چارچوب مخاطره فنـاوری اطلاعات[17] تدوین شده است. جزئیات فرآیندها و فازهای کلیدی چارچوب کوبیت ۵ در جدول شماره ۱ ارایه شده است [۶].

در ایـن چارچوب برخلاف نسـخه چهـارم، حوزهٔ راهبـری از حوزه مدیریت جدا شـده اسـت. حوزه مدیریت همچون نسخه چهارم این چارچوب شـامل برنامه‌ریزی، ایجاد، راه‌اندازی و نظارت است و حوزه راهبری شامل فعالیت‌ها و مهارت‌هایی است که به ارزیابی انتخاب‌های راهبردی کمک می‌کند، مسـیر را برای پیاده‌سـازی فاوا و رسیدن به خروجی مناسـب همـوار می‌کند و ایجاد ارزش افـزوده، وجود روابط شـفاف با ذینفعان، بهینه‌سازی منابع، بهینه‌سـازی مخاطره و ایجاد چارچـوب راهبری را تضمیـن می‌کند. تفکیک راهبـری از مدیریت در چارچـوب کوبیت۵، درک بهتـری از فرآیندهایی از نوع راهبری را برای سـازمان‌ها ایجاد می‌کند. در نسخه پنجم این چارچوب، فرآیند راهبری در سـطح بالاتری از مدیریت نقـش هدایت، پایش و ارزیابی مستمر فرآیندهای مدیریتی را بر عهده دارد. این فرآیندها راهبردهای موردنیاز اجرا را تعریف کرده و با سـنجش مسـتمر، تضمین می‌کنند که فعالیت‌های انجام شـده در سطح مدیریت در راستای راهبردهای تدوین شده باشند و بر اسـاس دریافت بازخورد از اجرای تصمیمات، فرآیند تدوین راهبرد اصلاح می‌شود.

- این چارچوب حاوی ۷ توانمندسـاز و ۵ اصل اسـت که در ادامه به توصیف آن‌ها می‌پردازیم [۷].

۶-۱- توانمندسازها

توانمندسـازها بر اسـاس تعریف کوبیت۵ معیارهایی هسـتند که به صـورت انفرادی و یـا ترکیبی بر روی این‌که آیـا راهبری و مدیریت فناوری اطلاعات سـازمان قابل انجام اسـت یا خیر، تاثیر می‌گذارند. هدایت‌کننده توانمندسـازها اهداف تعریف شـده در سطوح متفاوت آبشـار اهداف اسـت. در کوبیت۵، ۷ گروه توانمندساز وجود دارد [۷] که عبارت است از:

- اصول، خط‌مشـی‌ها و چارچوب‌ها: وسیله‌ای برای ترجمهٔ رفتارهای مطلوب به راهنماهای عملی به منظور مدیریت روزانه فعالیت‌ها.
- فرآیندهـا: مجموعه‌ای سـازمان یافته از فعالیت‌هـا و وظایف برای دسـتیابی بـه اهداف معیـن که مجموعـه‌ای از خروجی‌هـا را در پشتیبانی از تحقق اهداف سازمانی ایجاد می‌کند.
- سـاختارهای سـازمانی: بخش‌های کلیـدی تصمیم‌گیری در یک سازمان است.
- فرهنگ، اخلاق و رفتار سازمانی: بخش غیررسمی سازمان که عامل موفقیت کلیدی در فعالیت‌های مدیریتی و راهبری است.
- اطلاعـات: مجموعه اطلاعات تولید شـده در سـازمان برای حفظ حرکت و راهبری صحیح سازمان.
- خدمات، زیرسـاخت‌ها و برنامه‌های کاربردی: بخش‌فناوری سازمان که سازمان را با پردازش فناوری اطلاعات و خدمات تجهیز می‌کند.
- افـراد، مهارت‌هـا و توانایی‌ها: بـرای انجام کامل همـه فعالیت‌ها، تصمیم‌گیری درست و انجام بهبودسازمانی مورد نیاز است.

اصول کوبیت [۵]

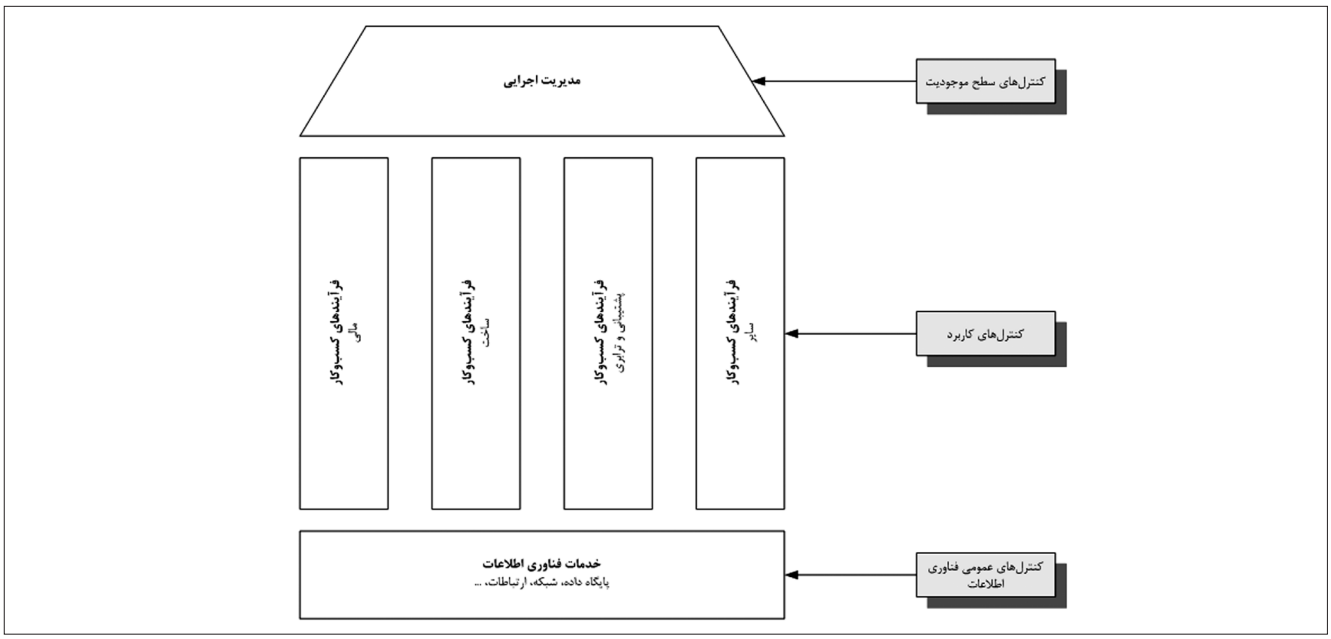
کوبیت۵ بر اساس ۵ اصل زیر استوار است [۷].

- اصل ۱ فراهم آوردن نیازهای ذی‌نفعان: فلسـفه وجودی سازمان‌ها خلق ارزش برای ذی‌نفعان خود اسـت. آنچه که در این خلق ارزش اهمیت دارد برقراری تعادل میان تحقق مزایا، بهینه‌سازی مخاطرات و اسـتفاده صحیح از منابع اسـت. کوبیت۵ تمام فرآیندهای مورد

15- Information Systems Audit and Control Association
16- Value IT
17- Risk IT

جدول ۱: فرست فرایندهای کوبیت۵

	مجموعه فرآیند	فرآیند	مخفف
فرآیندهای راهبری	ارزیابی، سنجش و پایش	تضمین ایجاد چارچوب راهبری و پایش بر اساس آن	EDM01
		تضمین ایجاد ارزش افزوده	EDM02
		تضمین بهینه سازی مخاطره	EDM03
		تضمین بهینه سازی منابع	EDM04
		تضمین وجود روابط شفاف با ذینفعان	EDM05
فرآیندهای مدیریت	همسوسازی، برنامه‌ریزی و سازماندهی	مدیریت چارچوب مدیریت فناوری اطلاعات	APO01
		مدیریت راهبرد	APO02
		مدیریت معماری سازمانی	APO03
		مدیریت نوآوری	APO04
		مدیریت سبد برنامه‌ها۱	APO05
		مدیریت بودجه و هزینه	APO06
		مدیریت منابع انسانی	APO07
		مدیریت روابط	APO08
		مدیریت توافقات خدمت	APO09
		مدیریت تامین کنندگان	APO10
		مدیریت کیفیت	APO11
		مدیریت مخاطره	APO12
		مدیریت امنیت	APO13
	ساخت، خرید و عملیاتی ساختن	مدیریت برنامه ها و پروژه ها	BAI01
		مدیریت تعریف نیازمندی ها	BAI02
		مدیریت تعریف راه حل و ساخت	BAI03
		مدیریت در دسترس بودن و ظرفیت	BAI04
		مدیریت فعال‌سازی تغییرات سازمانی	BAI05
		مدیریت تغییرات	BAI06
		مدیریت پذیرش تغییر و انتقال	BAI07
		مدیریت دانش	BAI08
		مدیریت دارایی‌ها	BAI09
		مدیریت پیکربندی	BAI10
	تحویل، خدمت و حمایت	مدیریت عملیات	DSS01
		مدیریت رخدادها و درخواسته‌ای خدمات	DSS02
		مدیریت مشکلات	DSS03
		مدیریت استمرار	DSS04
		مدیریت خدمات امنیتی	DSS05
		مدیریت کنترلهای فرآیندهای کسب‌وکار	DSS06
	پایش، سنجش و ارزیابی	پایش، سنجش و ارزیابی کارایی و تطبیق	MEA01
		پایش، سنجش و ارزیابی کنترل های داخلی سیستم	MEA02
		پایش، سنجش و ارزیابی میزان اجابت درخواست‌های خارجی	MEA03



شکل ۴: اجزای عمومی سازمان و کنترل‌های آن [۲]

نیاز برای حمایت از خلق ارزش کسب‌وکار، با استفاده از فناوری اطلاعات را فراهم می‌کند.

- اصل ۲ دربرگیرنده تمام سازمان: کوبیت۵ راهبری فناوری اطلاعات را با راهبری سازمانی یکپارچه می‌سازد. این چارچوب تنها بر کارکرد فناوری اطلاعات تمرکز نداشته، بلکه با اطلاعات و فناوری‌های مرتبط به عنوان دارایی‌های حیاتی سازمانی برخورد می‌کند. این چارچوب تمامی توانمندسازهای مدیریت و راهبری فناوری اطلاعات را به صورت جامع و در سراسر سازمان، در نظر می‌گیرد و تمامی نقش‌ها و فرآیندهای داخل یک سازمان را پوشش می‌دهد.
- اصل ۳ به‌کارگیری چارچوب یکپارچه واحد: استانداردها و چارچوب‌های متعددی مرتبط با فناوری اطلاعات تدوین و ارایه شده است. که هر یک پوشش‌دهنده زیرمجموعه‌ای از فعالیت‌های حوزه فناوری اطلاعات هستند. کوبیت ۵ به عنوان چارچوبی فراگیر برای مدیریت و راهبری فناوری اطلاعات سازمان مورد استفاده قرار می‌گیرد. این چارچوب همسو با استانداردها و سایر چارچوب‌های سطوح کسب‌وکاری و سازمانی است.
- اصل ۴ ایجاد رویکردی کل نگر: راهبری و مدیریت فناوری اطلاعات، نیازمند رویکردی جامع است. کوبیت۵ با تعریف توانمندسازها که در بخش قبل به آن اشاره شد، امکان پیاده‌سازی یک سیستم مدیریت و راهبری جامع فناوری اطلاعات را میسر می‌سازد.
- اصل ۵ تمایز راهبری و مدیریت: کوبیت۵ مطابق شکل شماره ۳ تمایز آشکاری بین مدیریت و راهبری فناوری اطلاعات قایل است. در این چارچوب واژه های راهبری و مدیریت به صورت ذیل تعریف می‌شوند.

راهبری تضمین می‌کند که تحقق اهداف سازمانی به‌وسیله موارد ذیل امکان‌پذیر است:

۱- سنجش نیازهای ذی‌نفعان، شرایط و گزینه‌ها.

۲- تعیین جهت حرکت سازمان از طریق اولویت بندی و تصمیم‌گیری.

۳- پایش کارایی، انطباق و پیشرفت در رابطه با اهداف و جهت‌گیری توافق شده سازمان.

مدیریت: مدیریت شامل فرآیندهای برنامه‌ریزی، ساخت، انتقال و پایش است تا فعالیت‌های روزانه اولا همسو با جهت‌گیری تعریف شده در حوزه راهبری بوده و ثانیا تحقق اهداف سازمانی را تضمین کنند.

۷- اجزای عمومی سازمان

طبق تعریفی که کوبیت از سازمان ارایه می‌دهد [۲]، اجزایی را به شکل عام برای آن متصور شده که در شکل شماره ۴ نشان داده شده است. متناظر با هر کدام از این اجزا نیز کنترل‌هایی تعریف شده که در ادامه، به اجمال توضیح داده می‌شود.

۷-۱- کنترل‌های سطح موجودیت

این کنترل‌ها، آهنگ و فرهنگ سازمان را تنظیم می‌کند. کنترل‌های فناوری اطلاعات سطح موجودیت، بخشی از محیط کلی کنترل سازمان به حساب می‌آید. این کنترل‌ها شامل موارد زیر است:

- راهبردها و طرح‌ها
- سیاست‌ها و رویه‌ها
- فعالیت‌های مدیریت مخاطرات
- آموزش و تعلیم

جدول ۲: نگاشت کنترل‌های سطح موجودیت و فرآیندهای کوبیت۵

.کنترل‌های سطح موجویت ساکس (AS 5)	مرجع کوبیت (نسخه ۵)
حصول اطمینان از تنظیم و نگهداری چارچوب راهبری	EDM01
حصول اطمینان از بهینه‌سازی مخاطره	EDM03
حصول اطمینان از شفافیت برای سهامدار	EDM05
مدیریت چارچوب مدیریت فناوری اطلاعات	APO01
مدیریت راهبرد	APO02
مدیریت منابع انسانی	APO07
مدیریت کیفیت	APO11
مدیریت مخاطره	APO12
پایش، ارزیابی، و ارزشیابی کارایی و انطباق	MEA01
پایش، ارزیابی، و ارزشیابی سامانه کنترل داخلی	MEA02
پایش، ارزیابی، و ارزشیابی انطباق با الزامات خارجی	MEA03

- تضمین کیفیت
- ممیزی داخلی

۷-۲- کنترل کاربرد

کنترلی است که در فرآیندهای کسب و کاری محصولات کاربردی که مستقیماً اهداف کنترلی مالی را پشتیبانی می‌کند، تعبیه شده است. اهداف کنترلی شامل موارد زیر است:

- کامل بودن
- دقت
- وجود داشتن/ صلاحیت
- ارایه/ افشا

۷-۳- کنترل‌های عمومی فناوری اطلاعات

کنترل‌هایی که در فرآیندهای فناوری اطلاعات، که یک محیط عملیاتی قابل اطمینان را فراهم کرده و عملیات اثربخش کنترل‌های کاربرد را پشتیبانی می‌کند، تعبیه شده است. نمونه‌هایی از این کنترل‌ها، شامل موارد زیر است:

- توسعه برنامه
- تغییرات برنامه
- دسترسی به برنامه‌ها و داده‌ها
- عملیات رایانه‌ای

۸- ارتباط قانون ساکس و چارچوب کوبیت

قانون ساکس مدیران ارشد سازمان‌ها را صراحتاً موظف به ایجاد، ارزیابی، و پایش اثربخشی کنترل‌های داخلی تعریف شده بر روی گزارش‌دهی مالی می‌کند. برای بسیاری از سازمان‌ها، نقش فناوری اطلاعات در تحقق اهداف آن‌ها حیاتی است بنابراین سازمان‌ها نیازمند حضور نماینده فناوری اطلاعات در تیم‌های مربوط به اجرای قانون ساکس، با هدف تضمین این‌که کنترل‌های فناوری اطلاعات،

جدول ۳: نگاشت کنترل‌های عمومی فناوری اطلاعات و فرآیندهای کوبیت۵

کنترل‌های عمومی فناوری اطلاعات ساکس (AS 5)	مرجع کوبیت (نسخه ۵)
مدیریت توافقات خدمت	APO09
مدیریت تامین‌کنندگان (شامل قراردادهای برون سپاری)	APO10
مدیریت امنیت	APO13
مدیریت تعریف نیازمندی‌ها	BAI02
مدیریت شناسایی راه‌حل و ساخت	BAI03
مدیریت دسترس‌پذیری و ظرفیت	BAI04
مدیریت تغییرات	BAI06
مدیریت پذیرش تغییرات و انتقال	BAI07
مدیریت پیکربندی	BAI10
مدیریت عملیات	DSS01
مدیریت رخدادها و درخواست‌های خدمات	DSS02
مدیریت مشکلات	DSS03
مدیریت استمرار	DSS04
مدیریت امنیت خدمات	DSS05
مدیریت کنترل‌های فرآیندهای کسب وکار	DSS06

کنترل‌های عمومی، و کنترل‌های کاربرد وجود داشته و اهداف برنامه انطباق را پشتیبانی می‌کنند.

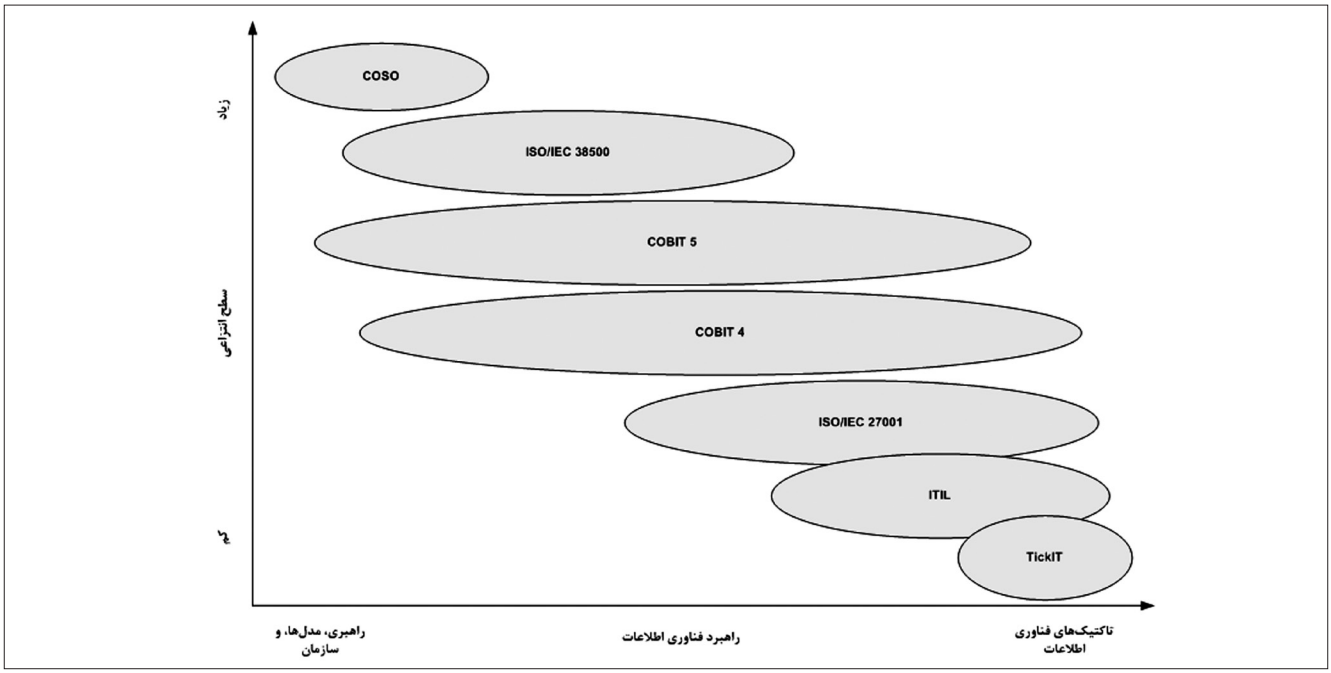
محیط کنترل فناوری اطلاعات، مرتبط با کنترل‌های سطح موجودیت بوده که در استاندارد AS 5 تعریف شده است. این محیط در برگیرنده فرآیند راهبری فناوری اطلاعات، پایش و گزارش‌دهی است. فرآیند راهبری فناوری اطلاعات، شامل طرح‌ریزی راهبردی سامانه‌های مدیریت اطلاعات، فرآیند مدیریت مخاطرات فناوری اطلاعات، انطباق و مدیریت مقررات، و استانداردها، رویه‌ها و سیاست‌های فناوری اطلاعات است. پایش و گزارش‌دهی با هدف هم‌سو کردن فناوری اطلاعات با نیازمندی‌های کسب‌وکار لازم است.

ساختار راهبری فناوری اطلاعات باید به نحوی طراحی شود که فناوری اطلاعات ارزش افزوده‌ای را به کسب‌وکار اضافه کرده و علاوه بر آن، مخاطرات فناوری اطلاعات نیز عنوان شده باشد. این ساختار راهبری، هم‌چنین در برگیرنده یک ساختار سازمانی فناوری اطلاعات، که تحقق اهداف سازمان را پشتیبانی و ارتقا می‌دهد، خواهد بود.

۹- کوبیت۵ و قانون ساکس

اشاره شد که استاندارد AS 5 به عنوان ابزاری برای ممیزی پیاده‌سازی قانون ساکس ارایه شده است. در این استاندارد وزن قابل توجهی به کنترل‌های سطح موجودیت (شامل کنترل‌های فناوری اطلاعات) داده شده است. ۱۱ فرآیند کوبیت ۵ با کنترل‌های سطح موجودیت مرتبط هستند. نگاشت بین این ۱۱ فرآیند و کنترل‌های موجودیت مرتبط با آن‌ها در جدول شماره ۲ ارایه شده است [۲].

دسته بعدی کنترل‌ها، کنترل‌های عمومی فناوری اطلاعات هستند



شکل ۵: جایگاه مدل‌ها/استانداردهای راهبری فناوری اطلاعات [۷]

نگاشت بین کنترل‌های پیشنهادی عمومی فناوری اطلاعات از قانون ساکس در استاندارد AS 5 و نسخه ۵ چارچوب کوبیت در جدول شماره ۳ نشان داده شده است.

برای پوشش کنترل‌های کاربردی کوبیت۵ یک فرآیند منحصر به‌فرد به نام مدیریت کنترل‌های فرآیندهای کسب‌وکار (DSS06)وجود دارد. این فرآیند شامل مفاد اهداف کنترلی برای کنترل‌های کاربردی است[۲].

۱۰- ارتباط با سایر استانداردها

از آن‌جا که معمولاً موضوعات «مدیریت فناوری اطلاعات» و «راهبری فناوری اطلاعات» به درستی تفکیک نشده و جایگاه هر کدام روشن نمی‌شود، استاندارد ISO/IEC 38500:2008 که توسط سازمان جهانی ایزو ارسال ۲۰۰۸ منتشر شده، تلاش دارد تا از یک نگاه سازمانی، جایگاه «راهبری فناوری اطلاعات» را مشخص کند. این استاندارد به اجمال در همین شماره از نشریه گزارش کامپیوتر بررسی و مرور شده است. ارتباط بین چارچوب‌ها و استانداردهای حوزه راهبری فناوری اطلاعات و سطح عملیاتی هر کدام در شکل شماره ۵ ارایه شده است [۸].

۱۱- جمع‌بندی

ممیزی فناوری اطلاعات موضوعی است که در ۱۴ سال اخیر تکامل بسیار یافته است. شروع مطرح شدن این موضوع ریشه در رسوایی‌های مالی شرکت‌های بزرگ آمریکایی داشته است. این رسوایی‌های مالی زمینه ساز تصویب قانونی به نام قانون ساکس در ایالات متحده آمریکا شد. این قانون شامل الزامات راهبری شرکتی (سازمانی)، کنترل‌های داخلی و کیفیت ممیزی است.

اهداف کنترلی اطلاعات و فناوری‌های وابسته، که به اختصار کوبیت نامیده می‌شود، چارچوبی است که توسط موسسه ایساکا برای راهبری و مدیریت فناوری اطلاعات در سازمان‌ها ارایه شده است. این چارچوب در واقع به مدیران ارشد سازمان‌ها کمک می‌کند تا خلأ بین الزامات کنترلی، موضوعات فنی، و مخاطرات کسب‌وکاری را پر کنند. علاوه بر آن، راهبری فناوری اطلاعات را از طریق هم‌سو کردن اهداف کسب‌وکاری با اهداف و فرآیندهای فناوری پشتیبانی می‌کند. در این مقاله مفاد قانونی ۴۰۴ و ۳۰۲ این قانون که ارتباط با ممیزی فناوری اطلاعات دارند ارایه شده است و سپس نحوه تحقق الزامات قانون ساکس با استفاده از فرایندهای کوبیت ۵ مورد بررسی قرار گرفته است.

مراجع

مراجعی که در تدوین این مقاله از آن‌ها استفاده شده، به شرح زیر است:
[1] James A. Hall, Information Technology Auditing and Assurance, Third Edition, South-Western Cengage Learning, Mason, OH, 2011.
[2] IT Control Objectives for Sarbanes-Oxley, ISACA, Rolling Meadows, IL, 2014.
[3] Jill Gilbert Welytok, Sarbanes-Oxley for Dummies, Wiley Publishing, Inc, 2006
[4] Robert R. Moeller, Sarbanes-Oxley Internal Controls, John Wiley & Sons, Hoboken, NJ, 2008.
[5] Sabine Schöler et al., COBIT and the Sarbanes-Oxley Act, Galileo Press, Boston, MA, 2007[6] COBIT5 Enabling Process, ISACA, 2012
[7] COBIT5 a Business Framework for the Governance and Management of Enterprise IT, ISACA, 2012[8] Steven De Haes and Wim Van Grembergen, "COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities", Journal of Information Systems, Vol. 27, No. 1, Spring 2013, pp. 307–324

نقش ممیزی درپیاده‌سازی راهبری فناوری اطلاعات در سازمان‌های بزرگ

مرتضی ترک تبریزی
مدیر امور فناوری اطلاعات بانک ملت
پست الکترونیکی: m.tabrizi@bankmellat.ir

اکبر دهقانی
مشاور مدیر امور فناوری اطلاعات بانک ملت
پست الکترونیکی: ak.dehghani@bankmellat.ir

عیسی جبارزاده
کارشناس اداره کل فناوری اطلاعات بانک ملت
پست الکترونیکی: e.jabbarzadeh@bankmellat.ir

چکیده

امروزه استفاده از فناوری اطلاعات برای کلیه سازمان‌های بزرگ امری ضروری و اجتناب‌ناپذیر است، چرا که با گسترش فعالیت‌ها و تغییرات سریع فناوری، لازم است که سازمان‌ها از انعطاف‌پذیری لازم برخوردار باشند، و این امر محقق نمی‌شود مگر در سایه استفاده از فناوری اطلاعات. در حال حاضر، فناوری اطلاعات به صورت گسترده‌ای در سازمان‌های بزرگ مورد استفاده قرار می‌گیرد؛ بنابراین کسب‌وکار سازمان‌ها کاملاً وابسته به فناوری اطلاعات است. از این‌رو یکی از دغدغه‌های مهم ذینفعان اصلی این سازمان‌ها، فناوری اطلاعات بوده و باید از انجام صحیح مسایل مربوط به آن اطمینان حاصل کرد. تحقق این امر مهم، شدیداً وابسته به پیاده‌سازی دیسیپلین‌های (نظام‌های) راهبری (یا حاکمیت) و مدیریتی فناوری اطلاعات در سازمان‌های بزرگ خواهد بود. در این نوشتار سعی بر آن است که پس از بررسی چالش‌ها و مشکلات پیش روی یک مدیر در سازمانی مانند بانک، و با استفاده از رهنمودهای ممیزی و حسابرسی فناوری اطلاعات، امکان پیاده‌سازی راهبری فناوری اطلاعات پس از رفع مشکلات یاد شده ایجاد شود.

واژه‌های کلیدی: ممیزی و حسابرسی، راهبری فناوری اطلاعات، نظام‌های مدیریتی، فناوری اطلاعات

مقدمه

رشد روز افزون استفاده از فناوری اطلاعات در سازمان‌ها و بخصوص در سازمان‌های مالی (بانک‌ها و موسسات مالی) باعث ایجاد وابستگی بسیار قابل توجهی میان فرآیندهای سازمان و فناوری اطلاعات شده، به‌طوری‌که گاهی حتی نمی‌توان آن‌ها را از هم تفکیک کرد. از این رو، نظام‌های راهبری و مدیریتی فناوری اطلاعات بسیار حایز اهمیت بوده و لازم است که سازمان‌ها در اسرع وقت به پیاده‌سازی آن‌ها اقدام کنند. اهمیت به‌کارگیری این نظام‌ها در سازمان‌های بزرگ به‌قدری مهم و حیاتی است که پیشنهاد می‌شود که قبل از انجام هرکار دیگری در فناوری اطلاعات سازمان، این مقوله مهم پیاده‌سازی شود؛ چرا که منافعی که یک سازمان، به ویژه یک سازمان مالی، به دلیل عدم پیاده‌سازی صحیح فناوری اطلاعات از دست می‌دهد، به مراتب ارزش‌مندتر است.

از آن‌جایی که استفاده نادرست از فناوری اطلاعات می‌تواند مانع کارایی و رقابت سازمان‌ها شود، یا آن‌ها را در معرض مخاطرات ناشی از عدم مطابقت با قوانین و مقررات قرار دهد، فرآیندهای مربوط به ممیزی فناوری اطلاعات باید به‌کار گرفته شده تا راهنمای وسیعی را در بخش مدیریتی در خصوص راهبری در اختیار سازمان‌ها قرار دهند. بانک ملت نیز از این قاعده مستثنی نیست؛ به‌این معنا که برای استفاده کارا از فناوری اطلاعات باید از استانداردها و نظام‌های راهبری و مدیریتی موجود در زمینه فناوری اطلاعات و نیز رهنمودهای کارا و اجرایی حسابرسی فناوری اطلاعات استفاده کرد.

هدف

نظام‌های راهبری و مدیریت فناوری اطلاعات در سازمان بزرگی چون بانک ملت، با دیدی کلان و جامع به بررسی مفاهیم فناوری اطلاعات در سطوح مختلف سازمانی می‌پردازد. این نظام‌ها، با استقرار صحیح ممیزی و پیاده‌سازی رهنمودهای آن، به مثابه یک نقشه‌راه برای بانک به حساب آمده و می‌تواند بین کلیه ساختارها، برنامه‌ها و پروژه‌های این حوزه در سازمان یکپارچگی ایجاد کند؛ از این رو بانک را در تخصیص بودجه، اولویت‌بندی طرح‌ها و توسعه یاری کرده و مخاطرات پروژه‌های فناوری اطلاعات را تا حد زیادی کاهش می‌دهد.

ممیزی صحیح فناوری اطلاعات به هیئت‌مدیره بانک کمک خواهد کرد تا استفاده از آن را ارزیابی، هدایت و پایش کنند. نتایج حاصل از این ممیزی، مدیران بانک را در مسیر اطمینان از متابعت با وظایف در خصوص پذیرش استفاده از فناوری اطلاعات و داشتن راهبری فناوری اطلاعات یاری می‌کند. مدیران ارشد بانک ملت نیز در صدد هستند با اجرای صحیح فرآیندهای ممیزی فناوری اطلاعات چراغ راهی را پیش‌رو قرار داده تا مسیر پیاده‌سازی راهبری فناوری اطلاعات هموارتر و نتایج به‌دست آمده، اجرایی‌تر شود.

چالش‌های پیش روی مدیر فناوری اطلاعات

خدمات تشکیل‌دهنده سبد فناوری اطلاعات به ۴ دسته تقسیم می‌شود:

۱- راهبردی (برای دستیابی به مزیت رقابتی)

۲- اطلاعاتی (برای ارایه اطلاعات به مدیر)

۳- مبادلاتی (برای پردازش مبادلات و کاهش هزینه‌ها)

۴- زیرساختی (برای ارایه نرم‌افزارهایی که ظرفیت استفاده از فناوری اطلاعات را گسترش دهد) [۱]

این چهار دسته، سازمان را در رسیدن به سه هدف: کمینه‌سازی مخارج، رشد تجاری، و کارایی سازمان یاری می‌دهد. خدمات مرتبط با فناوری اطلاعات می‌تواند تاثیر راهبردی بر سازمان داشته و از این رو قادر است جهت‌گیری راهبردی سازمان‌ها را تغییر دهد. امّا در این مسیر یک مدیر فناوری اطلاعات با مشکلات فراوانی پیش‌رو بوده، که برخی از آن‌ها عبارت است از:

درخواست‌های ضربتی با قید فوریت

درخواست سامانه‌های مشابه

درخواست ایجاد مزیت رقابتی برای محصولات

افزایش رضایت‌مندی مشتریان از خدمات ارایه شده

کاهش هزینه‌های کسب‌وکار در حوزه خدمات

افزایش امنیت لایه‌های مختلف خدمات

افزایش پایداری خدمات ارایه شده از سمت سازمان

سازوکارهای هم‌سویی راهبردی

پایش یکپارچه کلیه فعالیت‌ها

پاسخگویی سریع به در خواست‌های ارایه شده از سمت کسب‌وکار

تعدد مراکز تماس (Call Center)

یکپارچه کردن تغییرات نرم‌افزاری و مدیریت آن

تولید سامانه‌های مورد نیاز در حوزه‌های مختلف بانک به دلیل وجود افراد علاقه‌مند و فعال به تولید نرم‌افزار، خارج از بدنه فناوری اطلاعات

مستندسازی فرآیندها و انتشار دانش برای مقاصد آموزشی (مدیریت دانش)

تامین نیروی انسانی متخصص در فناوری اطلاعات

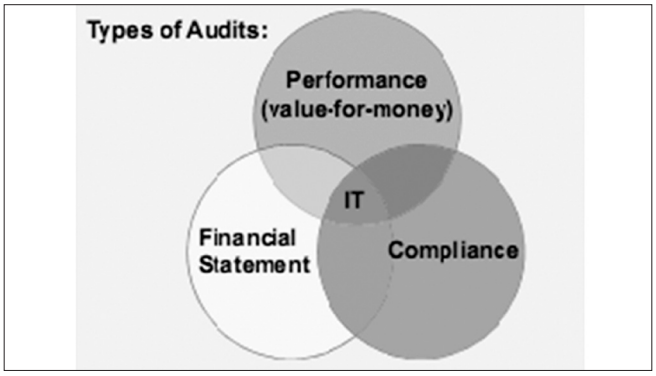
...

ممیزی فناوری اطلاعات

فناوری اطلاعات در سازمان‌ها نیازمند کنترل و نظارت بوده، و این کنترل مستلزم آگاهی از تغییرات رخ داده در سازمان و وضعیت کسب‌وکاری آن در اثر ورود فناوری اطلاعات و به ویژه مخاطرات

جدول ۱: اقدامات بانک ملت در خصوص چالش‌های موجود

ملاحظات	اقدامات بانک ملت	چالش‌های حوزه فناوری اطلاعات
استقرار IT Governance	پیاده سازی استانداردهای COBIT و ITIL و ISO27001	افزایش امنیت و پایداری لایه‌های مختلف سرویس و خدمات از سمت بانک
Data Mining	ایجاد Data Warehouse	عدم وجود مرکز مدیریت و ذخیره دیتاهای تولید شده در کل شبکه بانک
استقرار دفتر PMO	اجرای پروژه EPM	نیاز به پاسخگویی سریع به در خواست‌های کسب و کار/ ایجاد مزیت رقابتی برای محصولات / زمانبندی پروژه ها
ارتقاء حوزه فناوری اطلاعات	مرکزتعالی فناوری اطلاعات	عدم وجود نیروی انسانی و تیم های بین وظیفه ای متخصص
استقرار مدیریت دانش	مستند سازی کلیه فرآیندها و اقدامات	عدم وجود مستندات فرآیندها و انتشار دانش برای مقاصد آموزشی
ایجادمرکزتماس یکپارچه ملت	تجزیه و تحلیل تماس های دریافتی مدیریت مراکز تماس	تعدد مراکز ارتباط و امداد مشتریان (Call Center)
راه اندازی سامانه‌های جامع مالی	یکپارچه کردن رویه ها و فرآیندهای مربوطه	کاهش هزینه‌های کسب و کار در حوزه سرویس‌ها و خدمات



شکل۱: ممیزی فناوری اطلاعات

ناشی از این تغییرات است. در نتیجه، کنترل فناوری اطلاعات امری خطیر است و خود، باید قابل کنترل باشد تا از کفایت آن اطمینان حاصل شود. در این راستا سازمان باید به‌منظور اجرای فرآیندهای کنترلی خود از خدمات «حسابرسان مستقل» خود بهره‌گیرد تا همسویی فناوری اطلاعات با منافع خود را تحت کنترل و نظارت داشته باشد [۴]. برای این منظور و در راستای پیاده‌سازی بخشی از ارکان نظام نوین بانکداری در بانک ملت و اجرای مستمر فرآیند ممیزی، کمیته‌ای تحت نظارت هیئت‌مدیره و کمیته حسابرسی در سال ۱۳۸۹ تشکیل و به انجام وظیفه مشغول شد. ممیزی فناوری اطلاعات یکی از اصلی‌ترین وظایف این کمیته بوده که شامل بررسی کنترل‌های داخلی در حوزه فناوری اطلاعات و بانکداری الکترونیکی است (شکل شماره ۱). در این واحد سعی بر آن است که پس از شناخت کلیه فرآیندهای مربوط به فناوری اطلاعات، مخاطرات پیش‌رو را در اختیار فناوری اطلاعات قرار داده و پیشنهادهای قابل اجرا برای بهبود فرآیندهای ممیزی شده را در اختیار مدیریت این اداره قرار دهد. این پیشنهادها علاوه بر اجرایی بودن باید موجب افزایش کارایی و اثربخشی شده و صرفه اقتصادی نیز داشته باشد. در مسیر پیاده‌سازی و اجرای مراحل کنترلی در سازمان، مشکلاتی پیش‌رو است که عبارت است از (جدول شماره ۱):

عدم ارایه اطلاعات توسط لایه مدیریتی، و به تبع آن، عدم پذیرش و مقاومت توسط بدنه فناوری اطلاعات

عدم مستندسازی فرآیندها

عدم تمرکز کارها و فعالیت‌های سازمانی

عدم وجود مدیریت جامع گزارش‌ها، و فقدان واحد جامع برای تهیه گزارش‌های آماری

عدم پیاده‌سازی مدیریت دانش

حال بانک ملت در حوزه ممیزی فناوری اطلاعات در دو مرحله اقداماتی را به انجام رساند:

در مرحله اول ممیزی فناوری اطلاعات (IT Audit) بانک ملت به عنوان نخستین بانک ایرانی موفق به اخذ گواهینامه سیستم مدیریت امنیت اطلاعات (ISMS مبتنی بر استاندارد ISO/IEC ۲۷۰۰۱:۲۰۰۵) برای خدمت «بانکداری اینترنتی» از شرکت DNV یکی از شرکت‌های معتبر بین‌المللی در زمینه صدور گواهینامه‌های استانداردهای ISO در سال ۱۳۹۰ شد.

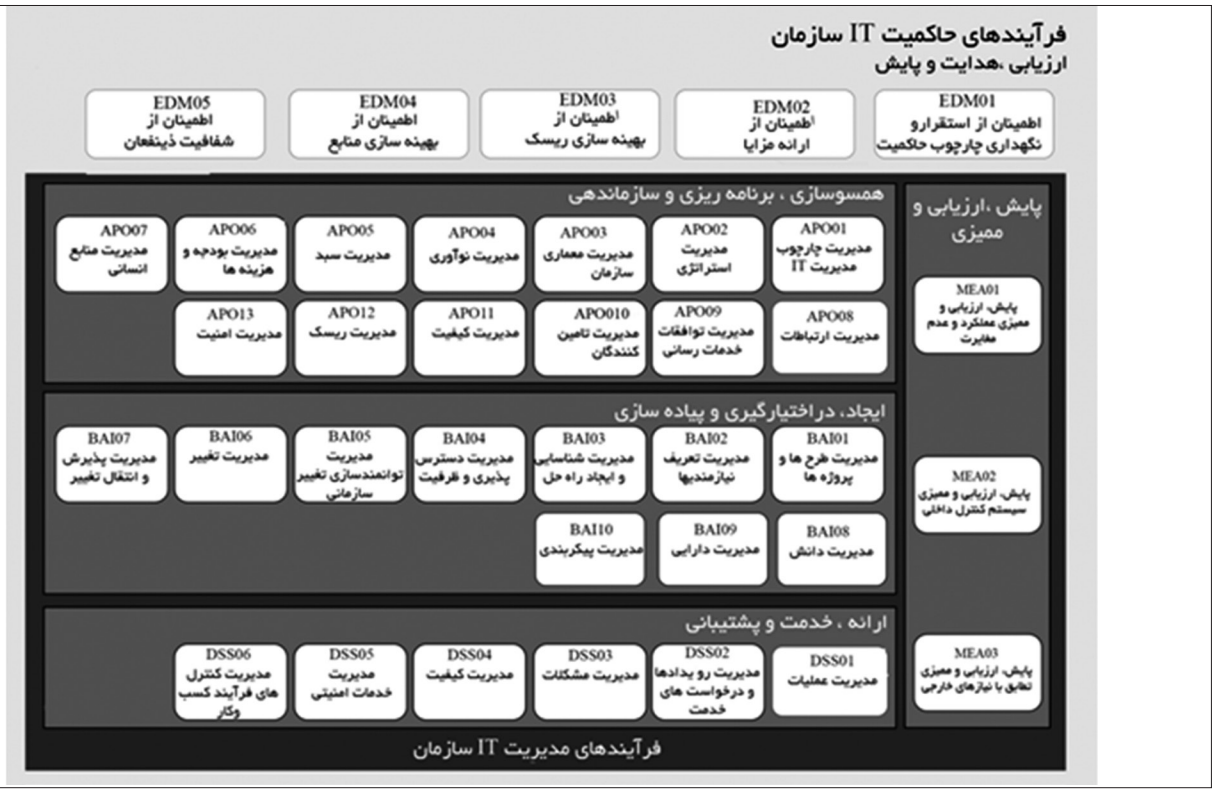
مرحله دوم پروژه ممیزی فناوری اطلاعات با استقرار حسابرسان خبره در سال ۱۳۹۲ در اداره کل فناوری اطلاعات آغاز شد. در این مرحله پروژه‌هایی نظیر امنیت نرم‌افزار، کنترل کیفیت پروژه‌های نرم‌افزاری، استانداردهای فناوری اطلاعات، پایگاه داده‌ها، تامین و پشتیبانی تجهیزات سخت‌افزاری، امنیت زیرساخت و ... مورد ممیزی قرار گرفت.

که بر این اساس و با توجه به چرخه دمینگ (شکل ۳) مراحل عملیاتی و اجرایی در بانک ملت عبارت است از:

۱- تدوین راهبردها، سیاست‌ها و برنامه‌های حوزه فناوری اطلاعات

۲- تشکیل کارگروه های تخصصی و تیم تحقیق و توسعه در حوزه فناوری اطلاعات

۳-استقرار استانداردهای روزآمد دنیای بانکداری در حوزه امنیت اطلاعات، مدیریت دانش، بانکداری الکترونیکی و ...



شکل ۲: فرایندهای حاکمیت فناوری اطلاعات در سازمان

۴- ایجـاد و پیاده‌سـازی دفاتـر مدیریت پروژه، راهبـری فناوری اطلاعات، انبار داده و ...(جدول شماره ۲)

راهبری فناوری اطلاعات

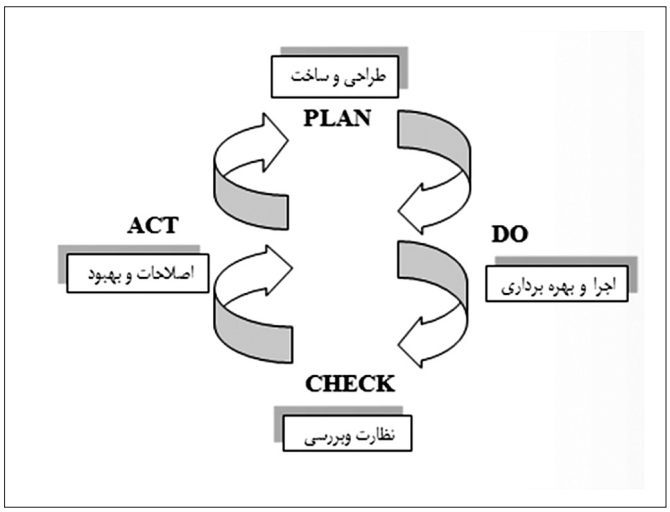
راهبـری فناوری اطلاعـات[1]، مجموعـه‌ای از قواعد و رویه‌ها اسـت کـه تعیین می‌کنـد تصمیم‌گیری درباره سـرمایه‌گذاری در فناوری اطلاعـات چگونـه انجام گیرد، بـرای اجرای ایـن تصمیمات چگونه نظارت شود، نتایج این تصمیمات چگونه اندازه‌گیری و ارزیابی شود، و تصمیم‌گیرنـدگان چگونه باید پاسـخگو باشـند. بـه عبارت دیگر، راهبری فناوری اطلاعات مسـئولیت مدیران سـازمان برای رهبری، و ایجاد سـاختارها و فرآیندهای سازمانی است که اطمینان می‌دهد فناوری اطلاعات در راستای راهبردها و اهداف سازمان حرکت می‌کند (شـکل شـماره ۲). دو نکته کلیـدی در راهبری فنـاوری اطلاعات، تصمیم‌گیرنـدگان (حـق تصمیم‌گیـری) و چگونگـی تصمیم‌گیری (فرآیندها و رویه‌ها) در رابطه با فناوری اطلاعات است [۲].

راهبری فناوری اطلاعات برای حصول اطمینان از دستیابی عملکرد فناوری اطلاعات به هدف‌های زیر به‌کار گرفته می‌شود:

هماهنگـی فناوری اطلاعات با سـازمان و تحقق مزایای وعده داده شده،

به‌کارگیـری فناوری اطلاعـات برای توانمند کردن سـازمان برای استفاده از فرصت‌ها و بیشینه‌کردن مزایا

1- IT Governance



شکل ۳: چرخه عملیاتی ممیزی فناوری اطلاعات

به‌کارگیری اثربخش منابع مربوط به فناوری اطلاعات

مدیریت مناسب مخاطرات فناوری اطلاعات

جمع‌بندی و فعالیت‌های آتی

پیاده‌سـازی اثربخش و کارای اسـتانداردها و تجارب موفق جهانی رمز موفقیت و بقای سـازمان‌ها در بازار رقابتی کنونی اسـت. برای پیاده‌سـازی این اسـتانداردها و تجارب موفق، راهبری و مدیریت سـازمان بایـد به صـورت چتری بر ایـن امر نظارت داشـته، تا از

جدول ۲: اقدامات بانک ملت در خصوص ممیزی فناوری اطلاعات

کارگروه/کمیته/کمیسیون/شورا	اهم وظایف
کارگروه نظام پیشنهادات یا بهبود مستمر	بررسی و جوابگوئی به پیشنهادات همکاران در خصوص امور مرتبط با اداره کل
کمیته پدافند غیرعامل	بررسی مسائل امنیتی
کمیته نظارت بر پروژه‌های توسعه و فناوری (هیأت نظارت)	تسهیل و هماهنگی اقدامات اجرایی مرتبط با ایجاد و راه‌اندازی سیستم متمرکز بانک‌داری و توسعه بانک‌داری الکترونیکی
کمیته راهبری امنیت	بررسی امنیتی موضوعات ارجاع شده به کمیته و اتخاذ تصمیم در راستای بهبود و ارتقاء امنیت تبادل اطلاعات در سطح بانک
کارگروه تخصصی بانک جامع اطلاعات مشتریان	ساماندهی وضعیت بانک جامع اطلاعات مشتریان و رفع مغایرت از اطلاعات تسهیلات ، اعتبارات اسنادی و ضمانتنامه هالی ریالی و ارزی ارسالی به مراجع برون سازمانی
کارگروه پروژه ملی کارت هوشمند سوخت	تأمین تجهیزات سخت‌افزاری مورد نیاز
کمیته راهبرد	سیاست‌گذاری راهبردی فناوری اطلاعات
کارگروه پژوهش	بررسی موارد پژوهشی در امور فناوری اطلاعات
کارگروه انبار و اموال	سامان بخشی به کلیه موارد مربوط به اموال بانک
کارگروه تکنولوژی	همسوسازی استراتژیهای فناوری اطلاعات و کسب و کار بانک ملت
کمیته‌ی بررسی شرایط انتصاب انفورماتیک	بررسی صلاحیت فنی و تخصصی متقاضیان اشتغال و ادارات انفورماتیک

پیاده‌سازی اثر بخش آن‌ها مطمئن شود. تحقق این مهم منوط به استفاده مناسب از نظام‌های فناوری اطلاعات و نظارت از طریق ممیزی فناوری اطلاعات است که می‌تواند بر کسب‌وکار سازمان اثر مستقیم داشته باشد. فناوری اطلاعات یک بخش جدایی‌ناپذیر از کسب‌وکار است و راهبری آن یک بخش جدایی‌ناپذیر از مدیریت سازمان. در راهبری فناوری اطلاعات نقش‌ها و مسئولیت‌ها باید به‌طور واضح مشخص شده و کمیته‌هایی مثل کمیته راهبری (در سطح اجرایی) و کمیته راهبردی (در سطح مدیریتی) تشکیل شود. پس از آن، یک استفاده از چارچوب برای اجرا و پیاده‌سازی راهبری فناوری اطلاعات، مثل COBIT لازم است. بانک‌ها و موسسات مالی نیز از این امر مستثنی نبوده، بلکه حتی رقابت بر سر بقا در این‌گونه سازمان‌ها بیشتر شده است. بنابراین، سازمانی موفق خواهد بود که از مزایای رقابتی که فناوری اطلاعات ایجاد می‌کند، به بهترین نحو در راستای اهداف و کسب‌وکاری خود استفاده کند. برای انجام راهبری کارهای زیر باید انجام گیرد:

تهیه چارچوب سازمانی مدیران

هماهنگی راهبردی فناوری اطلاعات با اهداف کسب‌وکاری

شناخت مخاطرات

تعریف و شناسایی سطوح فرآیندی

شناسایی عدم انطباق‌ها و مغایرت‌ها

توسعه راهبردهای بهبود

ارزیابی نتایج

این کارها تا بهبود کامل تکرار می‌شود.

حال نقشه‌راه بانک ملت در زمینه پیاده‌سازی راهبری فناوری اطلاعات به شرح زیر است:

- مرحله اول: شناخت وضعیت فعلی فناوری اطلاعات
- مرحله دوم: شناخت وضعیت مطلوب فناوری اطلاعات
- مرحله سوم: تدوین طرح مهاجرت به وضعیت مطلوب فناوری اطلاعات
- مرحله چهارم: ارایه مدل هم‌سوسازی راهبردهای فناوری اطلاعات و کسب‌وکار
- مرحله پنجم: تعیین سازوکارهای اندازه‌گیری هم‌سویی (سطح بلوغ)

مراجع

1- Guldentops, E. (2007). “What is in our IT portfolio?” Information Systems Control Journal, Vol. 5, pp. 20-21.

2- Sandrino-Arndt, B. (2008). “People, portfolios and processes: the 3p model of IT Governance”, Information Systems Control Journal, Vol. 2, pp 36-40

3-www.ago.gov.sg

4- Zarrella, E. (2008). “You can’t outsource control”. Information Systems Control Journal, Vol. 6, pp 5-6.

5- Board Briefing on IT Governance IT Governance Institute – 2003

مصاحبه با آقای مهندس انتظاری دبیر شورای عالی فضای مجازی

پرسش: همانطور که مستحضرید قوانین، مقررات و آیین‌نامه‌ها به صورت مستقیم یا غیرمستقیم بر ارایه‌دهندگان دولتی یا خصوصی خدمات و محصولات فناوری اطلاعات تاثیرگذار بوده و در برخی موارد چالش‌های جدی را برای آن‌ها به‌وجود آورده است و آن‌ها را از ارتقاء خدمات خود همگام با پیشرفت فناوری باز داشته است و منجر به کیفیت نه چندان قابل قبول محصولات و خدمات در حوزه فناوری اطلاعات در کشور شده است

با توجه به جایگاه حاکمیتی شورای عالی فضای مجازی نسبت به بدنه اجرایی فناوری اطلاعات در کشور و از آن‌جا که یکی از فرآیندهای اصلی در ساختارهای حاکمیتی ممیزی است، لطفا لزوم پرداختن به موضوع پایش و ممیزی قوانین، مقررات و آیین‌نامه‌های فناوری اطلاعات به عنوان یکی از وظایف شورا را بیان کنید.

پاسخ: به بحث بسیار مهمی اشاره کردید که از ابتدای قبول این مسئولیت توسط بنده یکی از دغدغه‌ها بوده است و از همان نخستین روزها با آن مواجه بوده‌ایم. لازم به ذکر است موضوع ممیزی فناوری اطلاعات در سطح بنگاه با ممیزی فناوری اطلاعات در سطح ملی تفاوت بسیار زیادی دارد. در سطح ملی نه تنها حوزه وسیع‌تر و ذی‌نفعان متنوع‌تر هستند بلکه ابعاد و ماهیت موضوع کاملاً متفاوت است. شاید تفاوت این دو بحث را بتوان مشابه تفاوت اقتصاد خرد و کلان دانست. در نتیجه انجام اقدامات در این حوزه نیاز به تامل و برنامه‌ریزی کلان‌تری دارد زیرا از یک طرف باید منافع ملی مدنظر قرار گیرد و از طرف دیگر منافع بنگاه‌های اقتصادی خرد که در این حوزه فعالیت دارند. در واقع قوانین از یک سو باید منافع ملی و ارتقاء سطح فناوری اطلاعات کشور را مدنظر قرار دهند و از طرف دیگر نباید به گونه‌ای باشند که این قوانین برای بنگاه‌های اقتصادی خرد تهدید حساب شده و آن‌ها به منظور حیات خود ناگزیر از قانون گریزی باشند. عدم وجود بستر قانونی مناسب، سبب شده است که با وجود بهره‌گیری از نیروی انسانی مجرب وضعیت ما در رتبه‌بندی‌های جهانی وضعیت مناسبی نباشد. به عنوان مثال در بحث صادرات نرم‌افزار جایگاه ما جایگاه ارزنده‌ای نیست. پس از جشنواره کارآفرینی دانشگاه شریف، متخصصین یکی از شرکت‌های ارایه‌کنندگان خدمات و محصولات فناوری اطلاعات که در کسب و کار خود بسیار موفق بوده و به ارایه صادرات نرم‌افزار می‌پرداخت عنوان کردند که ما برای بقای کسب و کارمان همه فعالیت‌هایمان را به اصطلاح عامیانه «زیرآبی» انجام می‌دهیم هر

چند تمایل ما به بحث رعایت قوانین، آیین‌نامه‌ها و بخش‌نامه‌هاست اما در پاره‌ای از موارد پیروی از آن‌ها به معنای توقف کسب و کار است. مثال‌هایی از این دست بسیار است.

در بحث‌های ملی تاکنون جلسات متعددی با سازمان تجارت، گمرک، اتحادیه صادرکنندگان نرم‌افزار برای بررسی چالش‌ها داشته‌ایم.

بنابراین موضوع که شما مطرح کرده‌اید بسیار مهم است. کشور ما در حوزه فناوری اطلاعات در حال ورود به فضای مجازی با همه ابعاد آن است. در کشور یک ناهمگونی در پرداختن به این ابعاد وجود دارد. دربرخی از این ابعاد به سرعت پیشرفته‌ایم در صورتی که در سایر بخش‌ها نه‌تنهاحرکتی نداشته‌ایم بلکه اصلا به آن فکر هم نکرده‌ایم. بنده فضای مجازی را کلان‌تر از فناوری اطلاعات می‌دانم. در این فضا علاوه بر فناوری اطلاعات بحث‌های امنیتی، اقتصادی، توسعه، زیرساختی و ... مطرح است و لازم است به همه این ابعاد فکر شود و اقدامات در تمامی این حوزه‌ها متوازی صورت گیرد که متاسفانه هنوز در فضای مجازی، در سطح کلان ملی، نگرش جامع بین همه دستگاه‌های ذی‌نفع آن وجود ندارد. این عدم فهم مشترک در سطح مدیران ارشد و حتی مدیران میانی هم وجود دارد.

علاوه بر آن در بحث ممیزی باید به دنبال تضمین باشیم. مثالی از ماهواره برایتان بزنم. در ماهواره بخشی به نام تضمین محصول وجود دارد. در بحث‌های تضمین از یک سو تا تمامی مولفه‌ها به درستی کار نکنند محصول یا خدمت ارایه نمی‌شود. و از سوی دیگر در صورت شکستِ فرآیند تضمین نقطه ایجادکننده شکست قابل شناسایی است. اگر بخواهیم سرمایه‌گذاری کشور تاثیرگذار و موفق باشد و کشور به هدف خود برسد لازم است نگاه ما به ممیزی همان نگاه تضمین عنوان شده باشد. اعتقاد بنده آن است که ضرورت ممیزی در بحث کلان بسیار بیشتر

از ممیزی در بحث بنگاه‌هاست و حتی اگر ممیزی در سطح کلان به درستی کار کند ممیزی بنگاه را نیز تحت تاثیر قرار می‌دهد.

پرسش: به نکته خوبی اشاره کرده‌اید. جالب است که نگرش شما در زمینه ممیزی و تضمین همان چیزی است که در چارچوب‌های جهانی مطرح در این حوزه مانند COBTT 5 به آن اشاره شده است. در مستندات جدید COBTT 5 for assurance بحث ممیزی و تضمین در بسیاری موارد با هم به‌کار برده شده است. حتی به جای واژه تجربه فرآیندی[1] جایگزین واژه اهداف کنترلی[2] شده است. هر دو این موارد نشان از این موضوع دارد که در ادبیات بین‌المللی هدف از ممیزی بهبود است و نه رفتارهای بازخواستی و تنبیهی اما دغدغه برخی از سازمان‌ها در اجرای فرآیند ممیزی به عنوان یک فرآیند داخلی آن است که نتایج حاصل از ممیزی اهرم فشاری در دست نهادهای بالادستی شود و با این بیم فرآیند ممیزی داخلی نیز حذف می‌شود. و به مجرد حذف آن قطعاً بهبود مستمر سازمان نیز حذف می‌شود به نظر شما در سطح ملی چه تدابیری می‌توان اندیشید تا این تغییر نگاه به ممیزی از یک فرآیند بازدارنده به یک فرآیند مستمر داخلی و لازمه ارتقا سازمان میسر شود؟

پاسخ: به نظر بنده نکته اول در این زمینه عدم وجود سازوکار مناسب برای پایش و ممیزی در سطح ملی و بنگاه است. کلیه سرمایه‌گذاری‌های سازمانی و صرف هزینه‌ها در جهت دستیابی به اهداف و دستاوردهای از پیش تعیین شده‌ای است. اگر فرآیندی که در این زمینه تحقق یافته جوابگو نیست لازم است پایش و ارزیابی شده، علل عدم تحقق اهداف مشخص شود. متاسفانه هم‌اکنون در کشور ممیزی در هیچ یک از دو سطح مالی و بنگاهی اتفاق نمی‌افتد. هم اکنون سازوکار مناسبی برای پایش و ممیزی، حتی در حد شرکت‌ها هم وجود ندارد. در بحث ملی موضوع نظارت در مورد پروژه‌های ملی بسیار مطرح است اما در این زمینه با مقاومت‌های بسیار زیادی روبرو هستیم. نظر بنده لزوم ممیزی طرح‌های کلان ملی و رسیدگی به مواردی است که تعهدات، نقض شده و سپس تلاش در جهت درمان سریع آن‌ها است. اگر در حوزه‌ای حتی هزینه‌های کلانی صرف کرده‌ایم ولی هنوز نتیجه نگرفته‌ایم و افق آن کار هم امیدوارکننده نیست بهتر است آن طرح‌ها را متوقف کنیم.

به نظر بنده اگر سیستم ممیزی فراگیر شود موضوع تغییر نگاهی که شما به آن اشاره کردید اتفاق می‌افتد لزوم این بحث همه‌گیر شدن ممیزی مخصوصاً در حوزه طرح‌ها و پروژه‌های ملی و پایش مستمر آن هاست. موضوع ممیزی در سطح ملی از وظایف شورای عالی فضای مجازی است. بین شورای عالی فضای مجازی، شورای انقلاب فرهنگی و شورای امنیت تفاوت‌های وظیفه‌ای وجود دارد. وظیفه اصلی شورای امنیت ملی رفع تهدیدات امنیتی در ابعاد وسیع ملی است. شورای انقلاب فرهنگی در بحث نظارتی وارد نشده است. تفاوت شورای عالی فضای مجازی با دو شورای عنوان شده وجود مرکز ملی فضای مجازی به عنوان بازوی اجرایی این شوراست. وظیفه اصلی مرکز ملی فضای مجازی «مواجهه فعال» است. «مواجهه فعال» بدان معناست که اگر مسئولیتی که آن را متعهد شده بودیم، تحقق نمی‌یابد فعالانه ورود کنیم. در این مرکز در حال تدوین برنامه‌ریزی کلان و نظارت کلان هستیم.

در زمینه نظارت مستمر بر طرح‌ها و پروژه‌های کلان ملی و اصطلاحا Observe آن‌ها بحث بسیار مهمی است که می‌توان آن را «دیده‌بانی» یا «پایش و سنجش» یا «رصد» ترجمه کرد. به نظر بنده مساله رصد یا دیده‌بانی پروژه‌های ملی لازم است توسط یک نهاد مستقل یا بهتر است بگوییم یک NGO که منافع مستقیمی در این زمینه ندارد انجام شود. نظام صنفی رایانه‌ای، سازمان بسیار مناسبی برای اجرای این وظیفه دیده‌بانی و رصد است زیرا اولاً سازمان دولتی نیست که به صورت مستقیم از این موضوع منتفع شود و ثانیاً یک کسب و کار خصوصی محدود هم نیست که تنها منافع محدودی را مدنظر داشته باشد و از زوایای محدود قضیه را نظاره کند. بنابراین به نظر بنده نظام صنفی باید رصد یا دیده‌بانی پروژه‌ها و طرح‌های ملی را در دستور کار خود قرار دهد و با توجه به ماهیت مستقل بودن آن می‌تواند در این راستا بسیار تاثیرگذار باشد. ورود سازمان نصر به این حوزه نه تنها باعث می‌شود جایگاه کلیه شرکت‌های خصوصی حوزه فناوری اطلاعات ارتقا یابد بلکه باعث تثبیت جایگاه ملی این سازمان مردم نهاد می‌شود.

پرسش: چالش‌های ممیزی فناوری اطلاعات را در حوزه‌پروژه‌های ملی، فرآیندهای سازمانی و حتی فرآیندهای ملی که نیاز به یکپارچگی دارند چه می‌دانید؟ و به نظر شما برای آن‌ها چه راهکارهایی می‌توان طراحی کرد تا بتوان تاثیر آن‌ها را کاهش داد و یا آن‌ها را حذف کرد؟

پاسخ: به نظرم بزرگترین چالش ما در این حوزه نشات گرفته از این موضوع است که ما وارد تحولات جدید می‌شویم ولی نظام برنامه‌ریزی، بودجه‌ریزی و تخصیص اعتبار ما قدیمی است. خیلی هم قدیمی است. یکی از بحث‌هایی که در حکمرانی فضای مجازی ما به دنبال آن هستیم همین موضوع است که بسیار هم با مقاومت روبروست اما یکی از بحث‌های کمک کننده به این موضوع، اصلاح فرآیندها، بخصوص در حوزه ارجاع کار و تقسیم کار ملی است. تخصیص بودجه هر یک از قراردادها به شرطی صورت گیرد که ممیزی پروژه به عنوان یکی از فرآیندهای قرارداد نیز لحاظ شده و هزینه‌های آن دیده شود با وجود دشوار بودن این موضوع و نیاز به کار اطلاع‌رسانی و شفافیت در نهادهای مختلف به نظر می‌رسد باید با حساسیت این موضوع دنبال شود.

پرسش: بحثی که معمولاً پس از ممیزی مطرح می‌شود نحوه اشتراک‌گذاری دانش و انتقال تجربه از پروژه‌های موفق به سایر پروژه‌ها و از سازمان‌های برتر به سایر سازمان‌هاست. منظورم دقیقاً این است که پس از انجام ممیزی و شناخت سازمان‌های برتر با چه تدابیری می‌توان تجربه و دانش آن‌ها را ارایه کرد تا سازمان‌هایی با سطح بلوغ پایین‌تر ولی مشتاق، بتواند درس‌های لازم را بیاموزد؟

پاسخ: در مسایل این چنین باید به دنبال رویکرد برد-برد بود بدین معنا که منافع شرکت‌هایی که تجارب برتری دارند و شرکت‌هایی که خواهان آموزش این تجارب هستند هر دو لحاظ شود. در این زمینه ما نیازمند بحث فرهنگ‌سازی هستیم.

کلام آخر:

ورود به بحث‌های ملی ابعاد و پارامترهای متفاوت و ذی‌نفعان گسترده دارد لذا لازم است با نگاه یکپارچه و کلان‌نگر دنبال شود. در این راستا حضور یک سازمان مستقل که به عنوان ممیز طرح‌ها و پروژه‌های ملی را رصد کرده و فعالیت‌ها را گزارش دهد بسیار تاثیرگذار است. توصیه من به سازمان نصر ورود به حوزه دیده‌بانی و رصد این موارد است.

1- Process Practice
2- Control Objective

برنامه‌ریزی حرکت به سمت بهبود بر اساس فرصت‌های شناسایی شده در ممیزی‌های فناوری اطلاعات

(مورد کاوی: سازمان فناوری اطلاعات و ارتباطات شهرداری تهران)

شباهنگ سلیمانی
سازمان فناوری اطلاعات و ارتباطات شهرداری تهران - رئیس دایره سیستم‌ها و تشکیلات
پست الکترونیکی: Soleymani_sh@tehran.ir

مینا سادات فرخی
سازمان فناوری اطلاعات و ارتباطات شهرداری تهران - کارشناس دایره سیستم‌ها و تشکیلات
پست الکترونیکی: farokhi_m@tehran.ir

خلاصه

امروزه با توجه به پیشرفت فناوری اطلاعات و به‌کارگیری آن در بخش‌های مختلف دولت، به منظور ارتقای بهره‌وری و سطح خدمت‌رسانی، سازمان‌هایی که خدمات مبتنی بر فناوری اطلاعات ارایه می‌دهند بیش از پیش به حرکت در مسیر دستیابی به اهداف دولت الکترونیکی توجه می‌کنند. از طرفی، پیاده‌سازی استانداردهایی از قبیل ایزو ۲۰۰۰۰ در زمینه مدیریت خدمات فناوری اطلاعات، که در راستای دستیابی به اهداف کسب‌وکار و خواسته‌های مشتریان در حوزه فناوری اطلاعات تدوین شده، نقش شایانی در دستیابی به این اهداف دارد. با توجه به این‌که پیاده‌سازی استانداردهای مدیریتی در سازمان‌ها با چالش‌های بسیاری روبرو است، رفع آن‌ها و بهبود در ارایه خدمت به مشتریان، نیازمند انجام اقدامات و ممیزی‌های مستمر است.

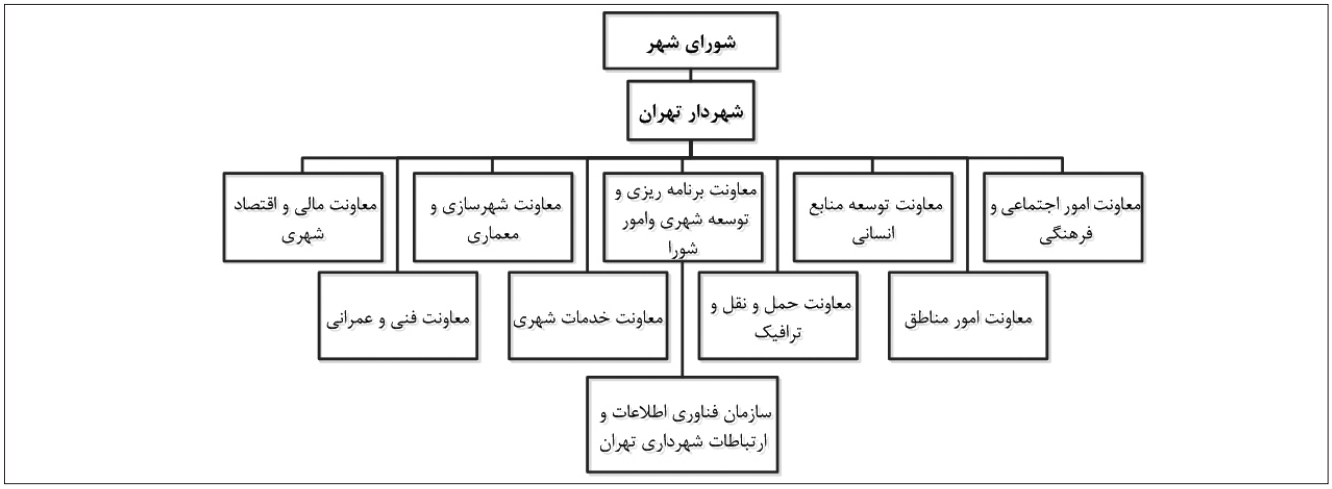
واژه‌های کلیدی: ITIL - ایزو ۲۰۰۰۰ - ممیزی فناوری اطلاعات

هدف

قصد این تحقیق آن است تا با بررسی تجارب موفق و ناموفق کسب شده در زمینه ممیزی‌های فناوری اطلاعات انجام شده در سطح سازمان فناوری اطلاعات و ارتباطات شهرداری تهران، راهکارهایی برای بهبود در پیاده‌سازی فرآیندهای استاندارد ایزو ۲۰۰۰۰، افزایش کیفیت خدمت ارایه شده به مشتری و پیرو آن ارتقای میزان رضایت‌مندی مشتریان، ارایه شود.

تعاریف

چارچوب ITIL: به عنوان کتابخانه‌ای از بهترین افکار، الگوها و



شکل ۱: جایگاه سازمان فناوری اطلاعات و ارتباطات در شهرداری تهران

به‌روش‌ها (Best Practice) برای مدیریت خدمات فناوری اطلاعات شناخته می‌شود. این چارچوب نگاهی نوین به فرآیندهای راهبردی، طراحی، ارایه، پشتیبانی و بهبود داشته و مورد توجه بسیاری از سازمان ها در سطح دنیا در حوزه مدیریت خدمات فناوری اطلاعات است. چارچوب مذکور به سازمان‌ها این امکان را می‌دهد که بهترین شیوه‌های شناخته شده در حوزه خدمات فناوری اطلاعات را در سازمان خود پیاده‌سازی و اجرا کرده و فعالیت‌های این حوزه را با نیازهای کسب‌وکاری خود هم‌سو کنند. [۵]

استاندارد ایزو ۲۰۰۰۰: اولین استاندارد در زمینه مدیریت خدمات فناوری اطلاعات است که توسط سازمان جهانی استاندارد (ایزو) منتشر شده است. این استاندارد با رویکردی فرایندگرا، در جهت دستیابی به اهداف کسب‌وکار و خواسته‌های مشتریان در حوزه فناوری اطلاعات تدوین شده است. نکته قابل توجه در این استاندارد استفاده از چارچوب ITIL است. [۵]

ممیزی: فرآیندی سیستماتیک، مستقل و مدون برای کسب شواهد ممیزی و ارزیابی مبتنی بر واقعیت آن به منظور تعیین میزان برآورده شدن معیارهای ممیزی. [۶]

نمودار RACI : واژه RACI مخفف ۴ نقش اصلی است: Responsible (شخص یا افرادی که مسئولیت انجام کاری را عهده‌دار است)؛ Ac-countable (تنها فردی که پاسخگوی هر وظیفه است)؛ Consulted (افرادی که با آن‌ها مشورت شده و/یا نظر آن‌ها اخذ می‌شود)؛ و Informed (افرادی که در طول پیشرفت فرآیند/فعالیت باید از حیث اطلاعاتی بروز باشند). از این ماتریس برای مشخص کردن ارتباطات بین فرآیندها و کارکردها استفاده می‌شود. [۱]

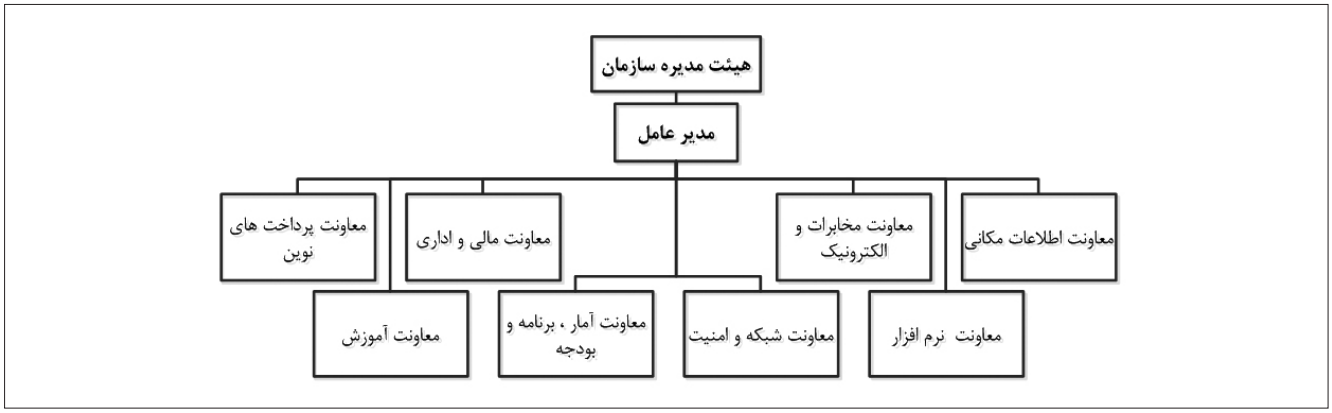
پایگاه داده مدیریت پیکره‌بندی (CMDB): پایگاه داده مدیریت پیکره‌بندی یا (Configuration Management Database)، پایگاه‌داده‌ای است که به منظور ذخیره سوابق پیکره‌بندی در چرخه عمر آن‌ها به‌کار برده شده، و مشخصات و روابط هر یک از اقلام با یکدیگر را ثبت و نگهداری می‌کند. [۴]

معرفی سازمان فناوری اطلاعات و ارتباطات شهرداری تهران («سازمان»)

شهرداری تهران متشکل از ۹ معاونت بوده که سازمان فناوری اطلاعات و ارتباطات شهرداری تهران زیرمجموعه معاونت «برنامه‌ریزی و توسعه شهری و امور شوراها» است (رجوع شود به شکل ۱).

همان‌طور که در شکل ۲ مشاهده می‌شود، سازمان نیز از ۸ معاونت تشکیل شده و خدمات و محصولاتی که توسط آن تولید، توسعه و پشتیبانی می‌شود به شرح زیر است:

- تامین تجهیزات سخت‌افزاری کامپیوتر و پشتیبانی آن
- تامین و پشتیبانی تجهیزات ویژه و برق اضطراری
- طراحی، تولید و تامین نرم‌افزارهای تخصصی مورد نیاز شهرداری تهران و پشتیبانی آن‌ها
- نصب و راه‌اندازی شبکه‌های LAN و WAN و پشتیبانی آن
- ارایه تجهیزات باسیم و بی‌سیم و نصب، راه‌اندازی و پشتیبانی آن
- تهیه انواع نقشه‌ها و تصاویر ماهواره‌ای در مقیاس‌های مختلف، تولید اطلاعات مکانی و هم‌چنین تعریف و اجرای پروژه‌های تحقیقاتی در حوزه اطلاعات مکانی
- ارایه خدمات مربوط به استفاده از کارساز و تامین، نصب و راه‌اندازی کارسازهای مورد نیاز در سطح شهرداری تهران
- تهیه آمارنامه‌های شهرداری تهران و شهر تهران
- طراحی و اجرای آموزش‌های مربوط به حوزه فناوری اطلاعات و ارتباطات، برای سازمان‌ها، شرکت‌ها، ادارات کل، و مناطق شهرداری تهران
- چاپ فرم‌های درخواستی مشتریان، ورود داده، فیش‌گیری و اتوماسیون اداری
- ارایه خدمات امنیتی
- نظارت بر خدمات، شبکه و امنیت (پایش)
- مدیریت پایگاه‌داده‌ها
- تامین نیازهای آموزشی کارکنان و ارائه آموزش‌های هدف‌مند در



شکل ۲: نمودار سازمان فناوری اطلاعات و ارتباطات شهرداری تهران (معاونت ها)

داخل سازمان به منظور از بین بردن فاصله شایستگی کارکنان سازمان

- کنترل و نظارت بر پرداخت‌های نوین (شامل پرداخت‌های اینترنتی، موبایلی، و پرداخت‌های خرد)

با توجه به تنوع و گستردگی خدمات و محصولات ارایه شده توسط سازمان و نیاز به توسعه و پشتیبانی آن‌ها، پیاده‌سازی و وجود استانداردهایی از جمله ایزو ۲۰۰۰۰ بسیاری ضروری و حیاتی است.

معرفی مشتریان و رویکرد سازمان نسبت به آن‌ها

سازمان وظیفه ارایه خدمات فناوری اطلاعات و ارتباطات به مشتریان ذیل را دارد:

- مناطق ۲۲گانه
- معاونت‌ها
- ادارات کل
- سازمان‌ها
- شرکت‌ها

این سازمان به عنوان متولی ارایه خدمات مذکور با رویکرد ارتقاء سطح رضایت‌مندی مشتریان و از طریق شناسایی انتظارات و حساسیت‌های آنان، به استفاده از خدمات فناوری اطلاعات، رویکردهای زیر را مد نظر داده است:

- فراهم‌سازی فرهنگ مشتری‌مداری در سازمان
- ارایه خدمات با کیفیت مناسب و در زمان توافق شده
- کاهش هزینه خدمات ارایه شده
- بهبود خدمات ارایه شده
- برقراری ارتباط مناسب با مشتریان به‌منظور اخذ نظرات، پیشنهادات و شکایات آن‌ها و رسیدگی به آن‌ها

مرکز سامانه مدیریت شهری ۱۳۷ به عنوان یکی از مشتریان سازمان

مرکز سامانه مدیریت شهری زیر مجموعه سازمان بازرسی، و از مشتریان سازمان بوده و به عنوان خدمت انتخابی پیاده‌سازی استاندارد ایزو ۲۰۰۰۰ در سازمان مد نظر قرار گرفته، که در ادامه به تشریح آن پرداخته می‌شود.

برای اولین بار تلفن خدماتی ۱۳۷ به عنوان پل ارتباطی بین مردم و شهرداری و با هدف دریافت پیام شهروندان در خصوص مسایل شهری در سال ۱۳۷۹ به صورت یک صندوق صوتی پیام گیر ایجاد شد. مرکز مزبور در بدو تأسیس، شبانه‌روزی و به‌صورت سیستم گویا مبادرت به ضبط تماس و درخواست‌های شهروندان کرده، و پیام‌های سامانه در ساعات اداری برای پیگیری به مناطق ابلاغ می‌شد. در مهر ماه سال ۱۳۸۱ مرکز ارتباطات مردمی که زیر نظر اداره کل روابط عمومی و بین‌الملل شهرداری تهران اداره می‌شد، جایگزین سیستم پیام‌گیر شهر شد. این مرکز در سوم دی ماه سال ۱۳۸۴، با توجه به گسترش درخواست‌های مردمی، با به‌کارگیری دانش فناوری اطلاعات جایگزین روش قبلی شده و به تدریج مرکز ارتباطات مردمی به مرکز هدایت و کنترل، ساماندهی و رسیدگی به معضلات شهری، شناخت مشکلات شهری و پل ارتباطی بین شهروندان و شهرداری تحت عنوان «مرکز سامانه مدیریت شهری ۱۳۷» ارتقا یافت.

حوزه‌های درخواست‌های سرویس ۱۳۷، عبارت است از:

- فرهنگی و اجتماعی
- خدمات شهری
- فنی و عمرانی
- حمل و نقل و ترافیک
- شهرسازی و معماری

اهداف مرکز ۱۳۷

۱. تحقق سیستم واحد مدیریت شهری
۲. ایفای نقش موثرتر در تحقق شهر الکترونیکی
۳. افزایش سطح مشارکت شهروندان در اداره امور شهر و بالا بردن احساس رضایت عمومی از شهرداری تهران به عنوان نهادی خدمت‌رسان

جدول ۱: ماتریس تعاملات اهداف ایزو ۲۰۰۰۰ و اهداف دولت الکترونیکی [۲]

اهداف ایزو ۲۰۰۰۰ / اهداف دولت الکترونیکی	بهبود روابط با مشتریان از طریق تبعیت از سطح توافقات خدمت انجام شده در خصوص کیفیت خدمات ارایه شده	تشریح جزئیات خدمات ارایه شده در قالب کاتالوگ خدمات به زبان مشتری	مدیریت کیفیت و هزینه‌های خدمات ارایه شده به نحوی بهتر و اثربخش‌تر	بهبود روند ارتباطی فاوا از طریق هدایت صحیح کانال‌های ارتباطی	ارایه شفاف هزینه خدمات و در نتیجه درک بهتر مشتریان از میزان هزینه‌های کلی عملیاتی
خدمت‌دهی یکپارچه، ساده، کارآمد و مطابق میل شهروندان	*	*	*		*
کاهش هزینه ارایه خدمات			*		*
انعطاف‌پذیری در اداره دولت				*	
کیفیت مطلوب تصمیم‌گیری‌های دولت			*		
تسهیل ارتباط بین سازمان‌های دولتی و اتوماسیون اداری				*	
مشارکت موثر شهروندان در فعالیت‌های اقتصادی				*	
افزایش ارتباط شهروندان و حکومت	*	*		*	

۴. ماشینی کردن نظام پاسخگویی به شهروندان تهرانی نسبت به معضلات و نیازمندی‌های اعلامی به شهرداری
۵. هدف‌مند کردن ماموریت‌های شهرداری و جلوگیری از اتلاف وقت، هزینه، نیروی‌انسانی و تجهیزات شهری
۶. استفاده از فناوری اطلاعات و ارتباطات در راستای تحقق شهر الکترونیک

مأموریت‌های مرکز سامانه مدیریت شهری ۱۳۷

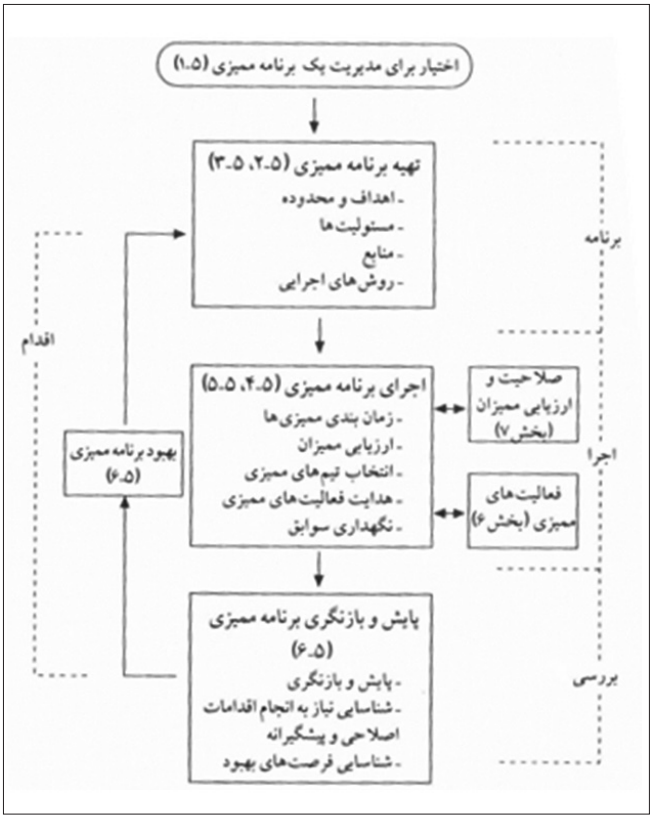
- ایجاد پل ارتباطی بین شهرداری و شهروندان
- هماهنگی و هدایت توان اجرایی برای رفع سریع و فوری مشکلات ملموس در سطح شهر با بهره‌گیری کلیه امکانات و تجهیزات
- پیگیری عملیاتی و میدانی، نظارت دقیق بر اجراء و صحت عمل، بازرسی هوشمندانه برای پاسخ‌گوئی صحیح و موثر به پیام‌های شهروندان
- ایجاد زمینه جلب مشارکت عمومی شهروندان و کارکنان مرکز سامانه با تبلیغات، اطلاع‌رسانی و آموزش همگانی برای اعتلا و ارتقاء ابعاد زندگی شهری در تهران
- دریافت درخواست‌های شهروندان و پاسخگویی و ارایه خدمات به صورت شبانه‌روزی و بدون وقفه
- بهره‌گیری از درخواست‌های ثبت شده مردمی در سامانه ۱۳۷ و تحلیل داده‌های آماری به منظور برنامه‌ریزی دقیق به‌منظور رفع معضلات شهری و بهبود روش‌های موجود در انجام ماموریت‌های محوله

پیاده‌سازی استاندارد ایزو ۲۰۰۰۰ برای خدمت ۱۳۷

در ابتدا، قبل از پرداختن به استقرار و نحوه پیاده‌سازی استاندارد فوق برای خدمت ۱۳۷، هدف سازمان از پرداختن به این استاندارد بر اساس اهداف دولت الکترونیکی بیان می‌شود. نحوه تعامل اهداف استاندارد ایزو ۲۰۰۰۰ و دولت الکترونیکی در جدول ۱ قابل مشاهده است.

وضعیت پیاده‌سازی استاندارد ایزو ۲۰۰۰۰ در سازمان

سازمان در سال ۱۳۹۱ برای اولین بار در ایران موفق به اخذ گواهینامه ایزو ۲۰۰۰۰ شد. ممیزی داخلی این استاندارد در همین سال توسط



شکل ۳: نمایش جریان فرآیند مدیریت یک برنامه ممیزی [۳]

مشـاورین پیاده‌سازی این استاندارد انجام، و در روزهای پایانی همین سـال توسط موسسـه کیفیت و انطباق کیهان پویا (آقای Sudarshan Mandyam) ممیـزی نهایی انجـام و گواهینامه ایزو ۲۰۰۰۰ از مرجع اعتباردهنده ISC اسـترالیا بر روی خدمت ۱۳۷ (دامنه پیاده‌سـازی استاندارد) دریافت شد.

به منظور حفظ و نگهداری سـامانه فـوق، کمیته‌ای با عنوان «کمیته راهبری ایزو ۲۰۰۰۰» تشکیل و از میان اعضای آن ۳ نفر برای شرکت در دوره ممیـزی ایزو ۲۰۰۰۰ انتخـاب، و ممیزی داخلی مرحله دوم سازمان، به‌صورت کاملاً داخلی و بدون استفاده از مشاور انجام شد.

در خرداد ماه سال ۱۳۹۲ نیز ممیزی مراقبتی استاندارد ایزو ۲۰۰۰۰ توسـط شـرکت اعتباردهنده برگزار (یکی از تفاوت‌هـای این دوره با دوره قبل ممیزی خارجی اسـتفاده از ممیـزان ایرانی در روند انجام ممیزی مراقبتی بـود) و نتیجه نهایی ممیزی مذکور نیز تنها با اعلام یک عدم انطباق جزئی پایان یافت.

جریان فرآیند مدیریت برنامه یک ممیزی

جریـان فرآیند مدیریـت یک برنامه ممیزی همان‌طور که در شـکل ۳ نشـان داده شـده،، کاربرد روش طرح‌ریزی، اجرا، بررسـی، و اقدام (PDCA) را در فرآیند ممیزی نشان می‌دهد.

تجارب ارایه شـده در ایـن مقاله مربوط به حوزه «بررسـی» فرآیند ممیزی بوده و به اقدامات مربوط به پایش و بازنگری وضعیت موجود، شناسایی اقدامات اصلاحی و پیشگیرانه مورد نیاز و فرصت‌های بهبود پرداخته می‌شود. در ادامه، اقدامات اصلاحی شناسایی شده به مرحله اجرا رسیده و مجدداً نتایج اثربخشی آن مورد بررسی قرار می‌گیرد.

شناسایی فرصت‌های بهبود، انجام اقدامات اصلاحی مورد نیاز و ارایه نتایج آن

با توجه به ممیزی‌های انجام شـده و موارد مشـاهده شـده به منظور رفع عدم انطباق‌ها و ایجاد بهبود در عملکرد سـامانه، اقداماتی توسط سـازمان انجام شده که به آن‌ها اشـاره خواهد شد. لازم به ذکر است در ابتدای هر مورد، به مشـکل مشاهده شده توسط ممیزین پرداخته شده و سپس به اقدامات انجام شده بر روی موضوع و نتیجه آن اشاره شده است:

۱- عـدم وجود یکپارچگی در سـوابق تهیه شـده در فرآیندهای ایزو ۲۰۰۰۰

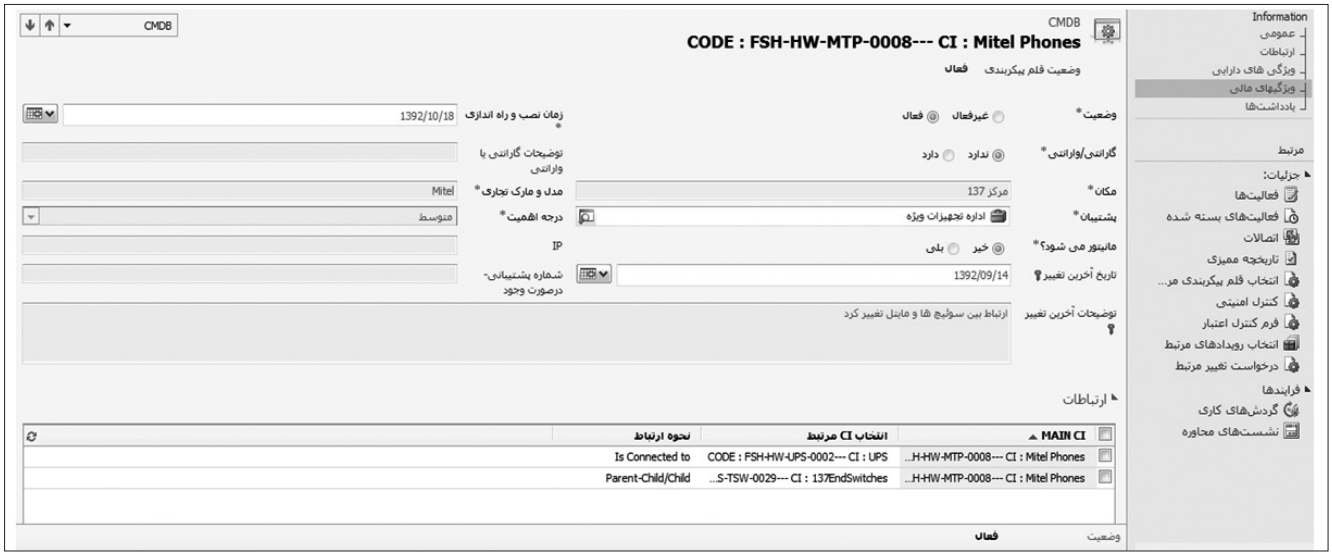
مواردی هم‌چون «عدم ارایه شواهد و یا ارایه شواهد ناکافی در جلسات ممیزی»، «دشواری پیگیری رفع عدم انطباق‌ها با توجه به تعدد آن‌ها و پیچیدگی فرآیندها»، «عدم وجود سوابق مربوط به اطلاع‌رسانی در خصـوص به تأخیر افتادن زمان ارایه محصول در بعضی از پروژه های نرم افزاری»، «عدم تکمیل سـوابق امکان‌سنجی و برآورد هزینه ارایه خدمات در تعدادی از پروژه‌ها» و «عدم وجود هماهنگی مناسب بین واحدهای فنی و امور مشـتریان» سبب شـد تا یکپارچه‌سازی سوابق در برنامـه کاری قـرار گیرد. پس از انجام بررسـی‌های لازم، مکانیزه کردن این موضوع در دستور کار قرار گرفت. امکان ثبت مواردی مانند درخواسـت تغییر، ارزیابی تامین‌کنندگان، درخواست اقدام اصلاحی/ پیشـگیرانه، نظرسنجی از مشتریان، شکایات مشتریان در این سامانه فراهم شـد. هم‌چنین پایـگاه داده مدیریت پیکره‌بنـدی نیز در این سـامانه ایجاد، و خصوصیات هر قلم پیکره‌بندی، ارتباطات آن با سایر اقـلام و ویژگی‌های دارایی و امنیتی آن‌ها نیز در سـامانه ثبت شـد. نمونه‌ای از اطلاعات مربوط به یکی از اقلام پیکره‌بندی ثبت شـده در سامانه، در شکل ۴ نشان داده شده است.

یکی دیگر از قابلیت‌های ایجاد شـده، استفاده از مفهوم ACCOUNT-ABLE در نمودار RACI، به منظور مشـخص شـدن شخص پاسخگو (ستون «صاحب» در شکل ۵) به ازای هر درخواست است.

اقدامـات صورت گرفته در ایـن مورد منجر یکپارچگـی فرآیندهای اسـتاندارد ایزو ۲۰۰۰۰ شده تا جایی که به عنوان یکی از نقاط قوت سیستم در ممیزی‌های بعدی اعلام شد.

۲- تأخیر در پاسخگویی به درخواست‌های تغییر سرویس

در راسـتای ارتقای کیفیت خدمت‌رسـانی به مشـتریان و به منظور بهبود زمان رسـیدگی به درخواسـت‌های ثبت شـده، روش ارسـال



شکل ۴: نمونه‌ای از اطلاعات یک قلم پیکره‌بندی در پایگاه داده مدیریت پیکره‌بندی

شکل ۵: درخواست‌های ثبت شده

سلسله مراتبی (Hierarchical Escalation) بر اساس چارچوب ITIL از طریق سامانه راه‌اندازی شد. بدین صورت که در صورت عدم پیگیری و انجام درخواست، به صورت خودکار نامه هشدار (همانند شکل ۶) را به مسئولین ذیربط و مدیران بالاتر ارسال می‌کند.

در نتیجه انجام این فعالیت، سازمان شاهد ارتقای کیفیت خدمت‌رسانی به مشتریان بوده و علاوه بر آن، میانگین زمان پاسخگویی به درخواست‌ها به میزان ۸۰ درصد بهبود داشته است.

۳- عدم ثبت کلیه مستندات مربوط به نشر نرم‌افزارها

به منظور ثبت مستندات و سوابق نشر نرم‌افزار، انجام کلیه تغییرات در سامانه مدیریت نشر نرم‌افزار در دستور کار قرار گرفته و پیمانکار توسعه نرم‌افزار ملزم به ثبت آن‌ها در سامانه شده است. در شکل ۷ تغییرات ثبت شده در سامانه نشر مشاهده می‌شود.

در نتیجه اقدام صورت گرفته تعداد عدم انطباق‌های مرتبط با مستندات نشر نرم‌افزارها کاهش پیدا کرد.

با سلام و احترام

تکمیل فرم امکان سنجی یا برآورد هزینه با مشخصات زیر به تاخیر افتاده است :

عنوان فرصت فروش : درخواست شبکه منطقه ۰۲-ساختمان اصلی

نام مشتری : منطقه ۰۲

زمان گذشته شده ایجاد فرم (برحسب روز) : ۱۱

زمان گذشته شده از یادآوری به مسئول انجام (برحسب روز) : ۳

زمان گذشته شده از یادآوری به رییس دایره (برحسب روز) : ۳

شکل ۶: نمونه‌ای از نامه هشدار ارسال شده

اقدامات و فرهنگ‌سازی‌های انجام شده

در راستای بهبود برخی از موارد مشاهده شده در ممیزی‌ها، اقداماتی به‌منظور فرهنگ‌سازی و ارتقای سطح دانش کارکنان سازمان صورت

#	کد فعالیت	کد تغییر	عنوان	شرح	نوع تغییر	تاریخ انجام	نسخه پکیج	وضعیت	فرم جاری	تاریخ ایجاد
1	3738	5053	رفع اشکالات نسخه قبلی در ثبت پیام		جدید	1393/5/26	03.01.09	پایان یافته	تایید نهایی تغییر	1393/5/26
2	3738	5054	ثبت پیام پیرو برای اداره پردازش		جدید	1393/5/26	03.01.09	پایان یافته	تایید نهایی تغییر	1393/5/26
3	3738	5055	اضافه کردن تاریخ و ردیف در قسمت تغییرات پیام		جدید	1393/5/26	03.01.09	پایان یافته	تایید نهایی تغییر	1393/5/26
4	3738	5056	دکمه alt		جدید	1393/5/26	03.01.09	پایان یافته	تایید نهایی تغییر	1393/5/26
5	3738	5057	آدرس در فهرست پیامها		جدید	1393/5/26	03.01.09	پایان یافته	تایید نهایی تغییر	1393/5/26
6	3738	5058	فیلتر کانال دریافت		جدید	1393/5/26	03.01.09	پایان یافته	تایید نهایی تغییر	1393/5/26

شکل ۷: تصویری از سامانه نشر

جدول ۲: جدول ارزیابی عملکرد اعضای کمیته راهبری ایزو ۲۰۰۰۰

ردیف	عنوان شاخص	وزن	میزان شاخص		
۱	حضور در جلسات دعوت شده	۲۰	فعال = ۱۰۰	غیرفعال = ۰	نیمه فعال = ۷۰
۲	انجام فعالیتهای واگذار شده در زمان تعیین شده	۳۵	فعال = ۱۰۰	غیرفعال= ۰	نیمه فعال = ۵۰
۳	انجام فعالیتهای ذکرشده در روش اجرایی	۲۰	فعال = ۱۰۰	غیرفعال= ۰	نیمه فعال = ۵۰
۴	آشنایی با روشهای اجرایی و مستندات مرتبط	۱۰	فعال = ۱۰۰	غیرفعال= ۰	نیمه فعال = ۵۰
۵	رفتار مسئولانه در برخورد با پیگیری کنندگان	۱۰	مناسب = ۱۰۰	متوسط = ۵۰	ضعیف = ۰
۶	ارائه پیشنهادات بهبود	۵	فعال = ۱۰۰	غیرفعال= ۰	نیمه فعال = ۵۰

گرفته که همانند قسمت قبلی در ابتدا عنوان مشکل ذکر شده و سپس راهکارهای رفع آن اعلام شده است:

۱- تأخیر در رفع عدم انطباق‌های ممیزی و عدم انجام آن‌ها در زمان تعیین شده

به منظور پیگیری رفع عدم انطباق‌های ممیزی و انجام فعالیت‌های مربوط، «کمیته راهبری ایزو ۲۰۰۰۰» تشکیل شد. در ابتدا با توجه به تعداد کم اعضای پروژه و تیم کمیته راهبری، اقدامات مورد نیاز در زمان مناسب انجام نمی‌پذیرفت. به منظور بهبود عملکرد کمیته، اقدام به برگزاری دوره آموزشی برای کارکنان و افزایش سطح دانش آنان شد. افزایش تعداد افراد پروژه از ۸ نفر به ۳۹ نفر، اضافه کردن افراد مسئول در کنار افراد پاسخگو و برگزاری کمیته راهبری به صورت منظم منجر به رفع عدم انطباق‌ها در مدت زمان کوتاه‌تری شد که از نتایج آن می‌توان به ثبت تنها یک عدم انطباق در ممیزی مراقبتی اشاره کرد.

۲- تأخیر در انجام فعالیت‌های تغییر در خدمت

یکی از تفاوت‌های اصلی پیاده‌سازی استاندارد ۲۰۰۰۰ با سایر استانداردها، ماهیت کاملاً فرآیندی آن بوده و برای این منظور باید از سیستم‌های انگیزشی در پیشبرد پروژه استفاده می‌شد. در ابتدا با توجه به عدم ارزیابی عملکرد اعضای کمیته، انجام فعالیت‌های تغییر در خدمت با تاخیر مواجه شد. لذا سازوکاری بر اساس جدول ۲ تدوین و به‌صورت ماهانه ارزیابی اعضاء انجام و در قالب اضافه کار به آن‌ها پاداش تعلق گرفت. این امر با توجه به علاقه‌مند شدن اعضای کمیته به انجام فعالیت‌ها در زمان تعیین شده، در حوزه انجام فعالیت‌های تغییر خدمت، تاثیر داشت.

۳- پایین بودن میزان رضایت‌مندی مشتری و عدم وجود برنامه برای افزایش آن

یکی از دلایل پایین بودن میزان رضایت مشتریان پس از بررسی

شکل ۸: نمونه‌ای از فرم رضایت سنجی از مشتریان

انجام شده، اســتفاده از مدیر تغییر و مدیر تأمین‌کنندگان (بر اساس ITIL در سرویس ۱۳۷) در جلسات با مشتری، و هم‌چنین عدم دعوت از مشتری در جلسات آموزشی مربوط به ITIL بود، که می‌توان از آن به عنوان یک تجربه ناموفق ذکر کرد. لذا به‌منظور رفع مورد مذکور از یکی از افراد اداره هماهنگی و امور مشــتریان سازمان استفاده کرده و پس از ارایه آموزش، از فرد به عنوان مدیر روابط کسب‌وکار بهره گرفته شــد. پس از آن، جلسات با مشــتری با حضور مسئول مشتری، مدیر تغییر و مدیر تأمین‌کنندگان برگزار شــد. هم‌چنین کارکنان مشتری در کلیه جلسات و مراحل پیاده‌سازی (جلسات آموزشی، جلسات حل مسئله و ...) دخیل شــدند. نتیجه اقدامات انجام شده، افزایش میزان رضایت‌مندی مشتریان بوده است. لازم به ذکر است رضایت مشتریان مطابق شــکل ۸ بر اســاس خود اظهاری و از طریق ســامانه مدیریت ارتباط با مشتری اندازه‌گیری شده و می‌شود.

۴- به تأخیر افتادن اخذ تأییدیه‌های عدم انطباق‌های ممیزی

در دوره‌های پیشــین ممیزی داخلی، اکثر واحدهای سازمان حاضر به امضای عدم انطباق‌ها نبودند. به منظور رفع این مشــکل، مقرر شد در صورت رفع عدم انطباق‌ها، در گــزارش ممیزی تنها عدم انطباق‌های باز آورده شود. نتیجه اقدام صورت گرفته بهبود در سرعت تأیید عدم انطباق‌ها و رفع آن‌ها بوده است.

۵- مقاومــت اکثــر واحدهــا در مقابــل پیاده‌ســازی فعالیت‌هــای سامانه‌ای

برگزاری جلســات متعدد با معاونت‌های مختلف ســازمان و هم‌چنین تســهیل فعالیت‌هــای معاونت با پیاده‌ســازی ســامانه‌های مدیریتی مختلف، منجر به اخذ حمایت معاونت‌های تخصصی ســازمان شــده تا آن‌جــا که یکی از معاونت‌های فنی پیشــنهاد پیاده‌ســازی ســایر سیستم‌های مدیریتی از جمله ایزو ۲۷۰۰۱ را ارایه کرده است.

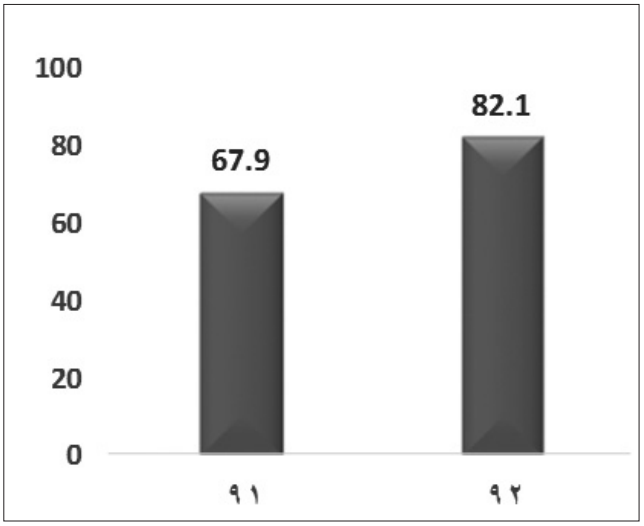
جمع‌بندی و فعالیت‌های آتی

- یکی از روش‌های مناســب و اثربخش به منظور ممیزی فعالیت‌های تخصصی فناوری اطلاعات، اســتفاده از ممیزی خودکار و بر اساس شاخص‌های ارایه شده به نرم‌افزار است.

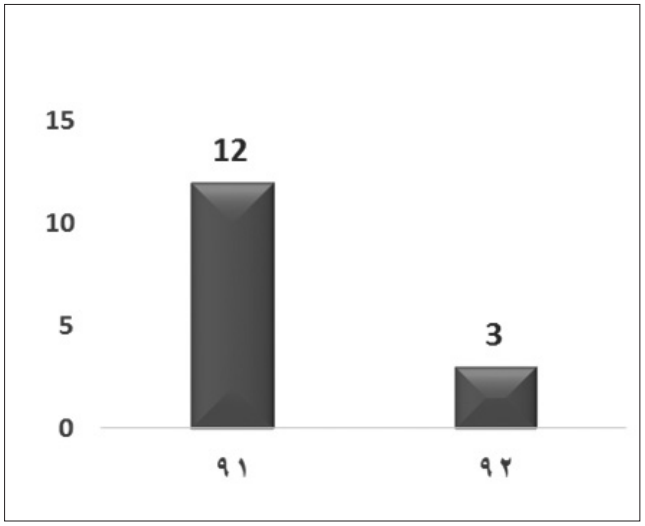
- با توجه به تغییرات زیاد فناوری فناوری اطلاعات، لزوم انجام تغییر در ســامانه‌های مدیریتی پیاده‌سازی شده در سازمان‌ها و هم‌چنین نحوه کنترل فرآیندهای ســازمانی بیش از پیش احســاس می‌شود. این ســامانه‌ها در تســهیل و کنترل دقیق‌تر فرآیندها و فعالیت‌ها، بسیار تاثیرگذار هستند.

پیرو اقدامات صورت گرفته، سازمان شاهد بهبودهای قابل ملاحظه‌ای بوده که می‌توان از میان آن‌ها، به اشکال ۹ ، ۱۰ و ۱۱ اشاره کرد.

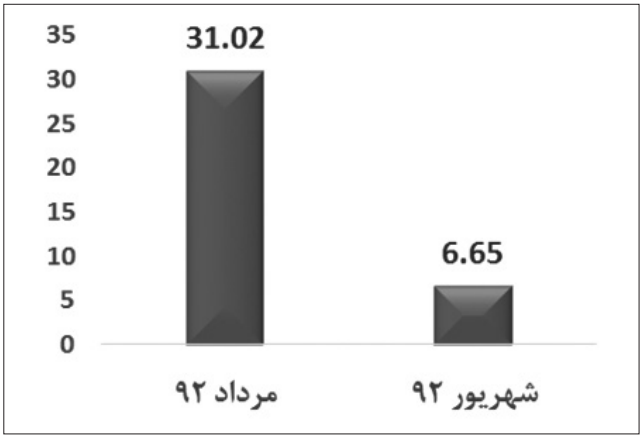
همان‌طــور که ملاحظه می‌شــود، میزان رضایت‌مندی مشــتریان در حــدود ۱۴ درصد افزایش یافته اســت. هم‌چنین تعــداد دفعات عدم پایبنــدی به توافقات درج شــده در SLA (توافقنامه ســطح خدمت) و میانگین زمان پاســخگویی به درخواســت‌ها و رویدادها کاهش پیدا کرده است.



شکل ۹: نمودار میزان رضایت‌مندی مشتریان (درصد)



شکل ۱۰: نمودار تعداد دفعات عدم پایبندی به توافقات موجود در SLA



شکل ۱۱: نمودار میانگین زمان پاسخگویی به درخواست ها و رویدادها (روز کاری)

مراجع

1. ITIL V3 – SERVICE STRATEGY BOOK
2. toseeh.medilam.ac.ir
۳. استاندارد ایزو ۱۹۰۱۱
4. ITIL V3 – SERVICE TRANSITION BOOK
5. http://www.datissystem.com/%DA%AF%D9%88%D8%A7%D9%87%DB%8C%D9%86%D8%A7%D9%85%D9%87-%D9%87%D8%A7%DB%8C-%DA%AF%D9%88%D9%86%D8%A7%DA%AF%D9%88%D9%86/iso20000/
۶. استاندارد ایزو ۹۰۰۰

پایان کار غول‌ها

به آگاهی خوانندگان پاورقی «پایان کار غول‌ها» می‌رساند که چاپ قسمت ششم آن به دلیل حجم بالای مطالب مربوط به سومین همایش راهبری و مدیریت خدمات فناوری اطلاعات، در این شماره امکان پذیر نشد.

توان‌مندسازی ممیزی با IT GRC

فریدالدین مهروانی بهبهانی
مدیرعامل شرکت اینفوامن
پست الکترونیکی: f.behbahani@infoamn.com

بر کسی پوشیده نیست که فرآیند ممیزی جزیی اساسی در ساختارهای راهبری و مدیریت فناوری اطلاعات بوده، و نقش ممیزی از بررسی صرف انطباق یا عدم‌انطباق با مجموعه‌ای از الزامات، به سرعت به سوی عاملی کلیدی در نیل به بهبود سازمان در حال تغییر است. اجرای اثربخش ممیزی فناوری اطلاعات چالش‌هایی با خود به همراه داشته که می‌تواند اثربخشی و کارایی آن را دچار مخاطره کند. در این مقاله به چهار چالش اشاره شده است. وجود ساختار راهبری، مدیریت مخاطرات و انطباق فناوری اطلاعات (IT GRC) می‌تواند به صورت مناسبی چالش‌های شمرده شده برای ممیزی فناوری اطلاعات را کاهش داده و اثربخشی آن را بهبود بخشد.
واژه‌های کلیدی: ممیزی فناوری اطلاعات، IT GRC، راهبری فناوری اطلاعات

نقش ممیزی در راهبری و مدیریت فناوری اطلاعات

واژه «ممیزی» که در زبان فارسی به عنوان معادل واژه انگلیسی Audit به کار می‌رود، ریشه تاریخی قابل تاملی دارد. واژه انگلیسی Audit در اصل از Audītus لاتین مشتق شده که معنای آن «شنیدن و گوش فرادادن» است. مفهوم ممیزی (مانند بسیاری مفاهیم مدیریتی دیگر) در ابتدا در حوزه مالی و برای سنجش میزان صحت، جامعیت و شفافیت گزاره‌های مالی و حسابداری به کار گرفته شد. کما این‌که در ادبیات فارسی نیز با ظهور دولت مدرن و ساخت‌یافته شدن موضوع مالیات، این واژه و مفهوم راه خود را به افواه عموم گشود.

می‌توان این گونه پنداشت که ممیزی جزء بدیهی هر نظام مدیریت و پایش، یا هر چارچوب الزام‌آور سازمانی و نهادی است. از آن‌جا که نظام پایش و مدیریت مالی در اصل اساسی نهادها و سازمان‌ها وجود داشت، موضوع ممیزی نیز در بدو امر در همین حوزه نمود یافت. در روند تکاملی و با شکل‌گیری دیگر نظام‌های مدیریتی سازمانی و نهادی، همراستا با نیاز مدیران و ذینفعان برای پایش عملکرد این نظام‌ها، مفهوم ممیزی نیز بسط یافته و نقش خود را در سنجش میزان انطباق عملکرد با مجموعه چارچوب‌های مختلف و در زمینه‌های مختلف گسترش داده است.

با گسترده‌تر شدن مفهوم و موضوع ممیزی، همزمان ماموریت آن نیز تغییر یافت. هم‌اکنون انتظار از گزارش‌های ممیزی چیزی بیش از بیان انطباق یا عدم انطباق در یک موضوع یا در برابر الزامات یک چارچوب است؛ بلکه انتظار می‌رود ممیز بتواند با ارایه نظر و زاویه نگاه خود (که به عنوان یکی از اصول اولیه، «مستقل» انگاشته می‌شود)

برای بهبود و اثربخشی بیشتر مدیریت و راهبری سازمان نیز راهگشا باشد.

زمینه و حوزه مدیریت و راهبری فناوری اطلاعات نیز در رابطه با نقش و عملکرد ممیزی از گفته‌های پیشین مستثنی نیست و چه بسا نظر به روند سریع حرکت و رشد در این زمینه، موارد و مسایل پیش گفته، در آن به‌صورتی پررنگ‌تر نمود پیدا می‌کند. از این رو، می‌توان انتظار داشت که اولاً ممیزی فناوری اطلاعات برای موفقیت و اثربخشی نظام‌های مدیریت و راهبری فناوری اطلاعات نقشی کلیدی داشته، و ثانیاً ممیزی در این حوزه نه تنها برای بررسی انطباق با الزامات، بلکه به عنوان یکی از ارکان اساسی پیشرفت و بهبود مستمر مورد توجه باشد.

معرفی IT GRC

راهبری (Governance) فناوری اطلاعات مفهومی است که به صورت سریعی پدیدار گشته و به مسئلهٔ مهمی در فناوری اطلاعات بدل شد. زمان دقیق شکل‌گیری این مضمون روشن نیست؛ در سال ۱۹۹۸ موسسه راهبری فناوری اطلاعات (ITGI) به‌منظور بسط و توسعه مفهوم راهبری فناوری اطلاعات بنیان نهاده شد. در متون آکادمیک و تخصصی، مقاله‌هایی که در عنوان آن‌ها عبارت راهبری اطلاعات به کار رفته باشد از اواخر دهه ۱۹۹۰ پدیدار شد. در گزارش موسسه گارتنر (Gartner) از سال ۲۰۰۳ عبارت «بهبود راهبری فناوری اطلاعات» به عنوان یکی از ده اولویت اول مدیران ارشد اطلاعات (CIO) ظاهر گردید (که در آن سال در رتبه سوم قرار گرفت). طبق تعریف موسسه ISACA[1]، «راهبری» عبارت است از حصول اطمینان از این‌که «نیازها، شرایط و گزینه‌های مختلف ذی‌نفعان مورد بررسی قرار گرفته، تا اهداف متعادل و مورد توافق سازمانی تعیین شود، جهت‌گیری‌ها از طریق تعیین اولویت‌ها و اتخاذ تصمیم‌های مورد نیاز انجام گیرد و پایش عملکرد و انطباق در مقایسه با جهت‌گیری‌ها و اهداف توافق شده صورت پذیرد.» در اساس، نقش راهبری، توان‌مندسازی بالادستان برای پایش و کنترل رفتار عوامل زیردست آن‌ها است.

درک این موضوع که دخیل بودن کسب‌وکار در راهبری فناوری اطلاعات حیاتی است، به تدریج منجر به تغییر مفهوم «راهبری فناوری اطلاعات (ITG)» به «راهبری سازمانی فناوری اطلاعات (GEIT)» شد. راهبری سازمانی فناوری اطلاعات بخشی از راهبری سازمانی یک بنگاه بوده، و به تعریف و پیاده‌سازی فرآیندها، ساختارها و سازوکارهای ارتباطی در سازمان می‌پردازد که همزمان پرسنل فناوری اطلاعات و سازمان را قادر سازد مسئولیت‌های خود در قبال همراستایی کسب‌وکارفناوری اطلاعات و ایجاد ارزش کسب‌وکار از طریق سرمایه‌گذاری در فناوری اطلاعات ایفا کنند.

1- Information Systems Audit and Control Association

مفهوم GRC[2] و به تبع آن IT GRC، از تجمیع اقدامات سازمان در سه حوزه راهبری (Governance) مدیریت مخاطرات (Risk Management) و انطباق (Compliance) شکل گرفت. در واقع پس از معرفی هر یک از این سه مفهوم و بلوغ نسبی آن‌ها در فضای اجرایی و عملیاتی سازمان‌ها، تداخل و اشتراک حوزه‌های زیادی بین این سه مفهوم مشاهده شد که مشوق تجمیع هرسه زیر یک چتر با عنوان GRC شد. در مدل‌ها و نظام‌های جدیدتری که خصوصاً در حوزه IT Governance و IT Security Governance پیشنهاد شده، (مانند ISO/IEC 38500:2008 و ISO/IEC 27014:2013) دو حوزه دیگر (مدیریت مخاطرات و انطباق) نیز به صورت ضمنی یا عینی مورد اشاره و استفاده قرار گرفته است. در عین حال که GRC به عنوان مفهومی سازمانی در شکل نظری آن قابل اشاره و استناد است، در بسیاری موارد اشاره به GRC در واقع اشاره به مجموعه‌ای از سازوکارها، ابزارها و نظام‌ها است که وظیفه مدیریت و پیشبرد سه حوزه درهم تنیده فوق را به عهده دارد.

عملکردهای اساسی که در یک ساختار IT GRC عموماً موجود است، شامل ارزیابی و مدیریت مخاطرات، مدیریت رخدادها، مدیریت ممیزی، سنجش عملکرد و اثربخشی، مدیریت سیاست‌ها و اسناد و مدیریت انطباق می‌شود که به صورت یکپارچه و با ارتباط به هم، به تحقق اهداف راهبری، مدیریت مخاطرات و انطباق سازمانی یاری می‌رساند.

چالش‌های ممیزی و نقش IT GRC در مقابله با آن‌ها

در فضای شدیداً متغیر و در حال حرکت کسب‌وکارهای امروزی، ممیزی فناوری اطلاعات (و همچنین سایر حوزه‌های ممیزی به صورت اعم) با مسایلی روبرو است که اثربخشی، عملکرد و ارزش افزایی آن را با چالش مواجه می‌کند. عدم توجه به چنین چالش‌هایی می‌تواند در طولانی مدت باعث کم‌رنگ و کم‌وزن شدن ممیزی فناوری اطلاعات شده، آن را از اولویت‌های مدیریتی سازمان خارج کرده و یا بدل به مراسمی تشریفاتی کند که از روح، جوهره و عملکرد اصلی خود تهی شده است. در ادامه، به برخی از چالش‌های عمده ممیزی فناوری اطلاعات پرداخته شده و دلیل بروز چالش و هم‌چنین تبعات و اثرات آن شرح داده می‌شود. در هر مورد نقشی که IT GRC می‌تواند در مقابله با آن چالش و به تبع آن توانمندسازی ممیزی داشته باشد، شرح داده خواهد شد.

تعیین دامنه و برنامه ممیزی

منابع سازمانی عموماً محدود بوده و با توجه به فضای رو به تزاید رقابت‌های کسب‌وکاری و فشار ذینفعان، استفاده بهینه از این منابع یکی از دغدغه‌های اصلی مدیران است؛ منابع صرف شده برای ممیزی

2- Governance, Risk and Complance

نیز از این قاعده مستثنی نیست. بخصوص که برای انجام ممیزی علاوه بر صرف مستقیم منابع نسبتاً خبره و پرهزینه (تیم ممیزی)، به صورت غیرمستقیم نیز منابعی در سازمان صرف شده که خود هزینه بالایی برای سازمان به همراه دارد؛ عموماً در خلال ممیزی‌ها واحد، حوزه یا فرآیند تحت ممیزی نیز به‌منظور همراهی در ممیزی، پاسخ به پرسش‌ها، ارایه شواهد و اسناد مثبته، بحث و بررسی وضعیت یافته‌ها، تعیین اقدامات اصلاحی، پیگیری و اجرای آنها و نهایتاً گزارش وضعیت اقدامات به متولیان امور درگیر می‌شوند. این درگیری و صرف وقت و منابع می‌تواند منجر به کاهش کارایی در حوزه تحت ممیزی (دست کم به صورت موقت) شود. لذا هزینه اجرای ممیزی برای سازمان به هیچ وجه اندک نیست و، نتیجتاً، لازم است استفاده از این ابزار به صورتی کاملاً حساب شده و بر اساس یک تخمین قابل قبول از میزان فایده (ارزش افزوده) انجام ممیزی برنامه‌ریزی شود.

به‌سادگی قابل پیش‌بینی است که در صورت عدم توازن مثبت ارزش افزوده به هزینه‌های ممیزی، این ابزار جذابیت خود را برای سازمان از دست خواهد داد. در چنین شرایطی مقاومت و ناهماهنگی احتمالی ممیزی‌شوندگان برای عدم مشارکت در ممیزی و پیگیری یافته‌های آن، نمی‌تواند با حمایت مدیریت سازمان جبران شده و به احتمال زیاد واحدها و فرآیندها ترجیح خواهند داد به انجام «کارهای مهم‌تر» روزانه خود بپردازند.

میزان ارزش افزوده ممیزی را می‌توان با دو پارامتر مدل سازی نمود: نخست کیفیت اجرای ممیزی از منظر ارایه یافته‌ها و توصیه‌های صحیح و اثربخش است که می‌تواند متضمن ایجاد ارزش افزوده در حوزه تحت ممیزی باشد؛ و عامل دیگر، میزان وزن و اهمیت حوزه و دامنه تحت ممیزی برای کسب‌وکار سازمان است. مواردی که می‌تواند عامل نخست را تقویت کند، فعلاً در این بخش تحت بررسی قرار نمی‌گیرد. لیکن در مورد انتخاب دامنه ممیزی می‌توان وزن واهمیت یک حوزه، فرآیند یا سامانه را برای کسب‌وکار سازمان از دو منظر مورد بررسی قرار داد. منظر نخست سهمی از عواید کسب‌وکاری (ارزش) است که توسط آن حوزه، فرآیند یا سامانه تولید می‌شود و منظر دیگر، مخاطراتی است که در صورت عدم عملکرد صحیح در آن محدوده می‌تواند برای کسب‌وکار ایجاد شود. بنابراین، در صورتی که هدف تشخیص و تعیین وزن و اهمیت دامنه تحت ممیزی از دید کسب‌وکار باشد، وجود یک مدل ارزیابی مخاطرات می‌تواند بر اساس میزان مخاطرات تشخیص داده شده برای یک فرآیند، سامانه یا یک حوزه سازمانی اطلاعات کافی را در اختیار بگذارد. در عین حال در صورت وجود مدلی برای ارزیابی و مدیریت مخاطرات، امکان افزایش ریزدانگی (Granularity) در ممیزی نیز فراهم می‌شود؛ زیرا حتی در مورد یک سامانه یا فرآیند لزوماً تمامی اقدامات انطباقی یا کنترل‌های کاهش مخاطرات دارای وزن و اهمیت همسان برای کسب‌وکار نیست. تواتر و عمق بیشتر ممیزی برای بررسی اقدامات و کنترل‌هایی لازم است که یا برای مقابله با مخاطرات شدیدتر طرح ریزی شده و یا در سوابق خود نشانه‌هایی از عدم موفقیت در اجرا و یا عدم انطباق را نشان می‌دهد.

از آنجا که در یک نظام IT GRC، مدل ارزیابی و مدیریت مخاطرات به عنوان عنصری اساسی وجود دارد، می‌توان با بهره‌گیری از اطلاعات به دست آمده از ارزیابی و مدیریت مخاطرات، برنامه‌های ممیزی را به صورتی دقیق‌تر و براساس میزان واقعی اهمیت دامنه تحت ممیزی برای کسب‌وکار سازمان برنامه‌ریزی کرد. ممیزی‌هایی که با چنین برنامه‌ریزی اجرا شود علاوه بر دارا بودن نسبت هزینه به فایده بالاتر، می‌تواند به صورت مناسبی به سازوکار مدیریت مخاطرات سازمان نیز بازخورد دهد.

اثبات اهمیت یافته‌ها و نیل به ادبیات مشترک با ممیزی‌شوندگان

ممیزی اساساً بر مبنای یک چارچوب مرجع شکل می‌گیرد که امکان قضاوت در خصوص یافته‌ها را برای ممیز فراهم کند. چارچوب‌های مرجع عموماً بر مبنای الزامات قانونی، استانداردها، بهروش‌ها و یا خط مشی‌ها و ضوابط درون سازمانی شکل می‌گیرد. در بسیاری موارد در قضاوت میزان انطباق با چارچوب‌های مرجع بین ممیزان و ممیزی‌شوندگان اختلاف نظرهایی بروز می‌کند. در صورتی که به ذات چارچوب‌های مرجع دقت شود، قابل پیش‌بینی است که چنین اختلافاتی محتمل است؛ اگر چارچوب مرجع یک استاندارد باشد، با توجه به ذات عمومیت و قابلیت استفاده استانداردها در شرایط و سازمان‌های گوناگون، شکل و نحوه بیان الزامات یا پیشنهادها در این اسناد به گونه‌ای است که لزوماً جزئیات اقدامات یا مصادیق واقعی یا ملموس هر الزام را بیان نمی‌کند. به این ترتیب، فضای تعبیر و تفسیر و هم‌چنین امکان برداشت‌های متفاوت از یک گزاره ایجاد خواهد شد. در خصوص بهروش‌ها، عموماً مسئله این است که چه سطحی از تبعیت «مورد نیاز» سازمان است و یا این‌که منافع متصور از آن با هزینه‌های تحمیلی قابل رقابت است یا خیر. به این ترتیب، در بسیاری موارد، اقناع ممیزی‌شونده در خصوص وجود یک عدم انطباق، فرصت بهبود و ... منوط به بحث و چالش ممیز با ممیزی‌شونده و تابع میزان قدرت و نفوذ طرفین است.

این مسئله به صورت عمومی‌تر می‌تواند منجر به ضعیف شدن قابلیت اثبات «اهمیت» (Materiality) یافته‌های ممیزی شود. در این حالت، یافته‌هایی که ذاتاً «صحیح» است-یعنی بر مبنای قضاوت صحیحی از تفاوت وضع موجود با چارچوب مرجع ثبت شده است-برای سازمان وزن و اهمیت کافی پیدا نمی‌کند؛ به این دلیل که یا توصیف و تعبیر از چارچوب مرجع متفاوت است و یا کسب‌وکار نمی‌تواند ارتباط کافی مابین یافته‌ها و توصیه‌ها با اولویت‌های سازمانی برقرار کند.

مشکل پیش گفته، اساساً در مورد سیاست‌ها و الزامات درون سازمانی کمتر رخ می‌دهد؛ زیرا در خصوص اهمیت و نحوه انطباق با این الزامات

حداقل اختـلاف بین طرفین ممیزی وجود دارد. لیکن همان‌گونه که قبلاً اشاره شد در بسیاری ممیزی‌ها، انتظار از خروجی ممیزی نه‌تنها مقایسـه وضعیت عملکرد سـازمان با الزامات داخلی (یا بیرونی)، که نشـان دادن فرصت‌های بهبود یا میزان فاصله با بهروش‌ها و تجربیات موفق است. در چنین شـرایطی دو عامل می‌تواند به پذیرش یافته‌ها و توصیه‌های ممیزی توسـط ممیزی‌شـونده یاری رساند. عامل اول، سـطح توان‌مندی، تجربه و تسـلط ممیز به حوزه ممیزی اسـت که به صورت مسـتقیم (در کیفیت نگارش، اسـتناد و توصیف یافته‌ها و توصیه‌هـا) و هم‌چنین غیر مسـتقیم (در شـکل ارتباطی فرد به فرد ممیز با ممیزی‌شـوندگان) دارای تأثیر خواهد بود. عامل دیگر امکان ارتبـاط دادن یافته‌هـا و توصیه‌ها به یک مدل و الگو اسـت که برای سـازمان قابل لمس و نیز برای مدیریت و تصمیم‌گیران سازمان قابل تحلیل، از منظر هزینه و فایده، باشد.

در راسـتای تقویت عامل اخیر، وجود سـاختار مدیریت مخاطرات در یک نظام IT GRC، می‌تواند به عنوان یک مرجع استناد برای مقایسه فوایـد و ارزش افـزوده توصیه‌های ممیزی به کارگرفته شـود. چنین مرجعی امکان مقایسـه توصیه‌ها و یافته‌هـای جدید با اقدامات قبلی سازمان را فراهم کرده و هم‌چنین به مخاطبان ممیزی کمک می‌کند تا یافته‌ها و توصیه‌ها را در بافتار (Context) مناسب کسب‌وکاری درک کند. به علاوه، ارتباط و همبستگی ممیزی با نظام IT GRC به شکلی که بیان شـد، به‌تدریج باعـث غنای مجموعه کنترل‌ها، سیاسـت‌ها و الزامـات داخلی سـازمان خواهد شـد. این امر به نوبـه خود، علاوه بر کمک به IT GRC و ممیزی، سـازمان را به سـوی بلوغ راهبری و مدیریت هدایت می‌کند.

تعدد و تکثر منابع اطلاعاتی مورد نیاز ممیزی

در سـازمان‌های مدرن و خصوصاً در زمینه‌هایی که فناوری اطلاعات نقش بیشـتری در آن ایفا می‌کند، تعداد و پراکندگی منابع اطلاعاتی، سوابق و شواهدی که می‌تواند برای ممیزی مورد بررسی و استناد قرار گیـرد به صورت روزافزونی در حال افزایش اسـت. به صورت معمول، این اسـناد و مدارک در منابـع مختلف و متنوعی نگهداری شـده و لزوماً ارتباط سیسـتماتیکی بین چنین اطلاعاتی نیز برقرار نیست. به عنوان مثال، اطلاعات مربوط به تغییراتی که در سـامانه‌های فناوری اطلاعات مجاز شـده–در صـورت وجود- در سـامانه‌های مدیریت و خودکارسـازی فرآیندهای مدیریت فاوا نگهداری می‌شود. اطلاعات و سـوابق رخدادها در سـامانه‌های مختلف از سامانه ثبت رخداد (Incident Register) تا سـامانه‌های مدیریت رویـداد (Log Management) و هم‌چنین احتمالاً سـامانه‌های کشـف و مقابله با نفـوذ (IDS/IPS) قابل یافتن اسـت. اطلاعات مخاطرات شناسـایی شـده و کنترل‌های امنیتی پیاده‌سـازی شده در سامانه‌ای دیگر (در صورت وجود سامانه مدیریت مخاطرات) قابل ردیابی اسـت، اطلاعات مالی و بودجه‌ای در سـامانه‌های حسـابداری نگهداری می‌شـود و روال‌ها و سیاست‌های سـازمان در سـامانه‌های دیگری (یا حتی به صورت اسناد منفک) در سازمان تصویب، ابلاغ و توزیع می‌شود.

اگر چه از منظر عملکردی، هر یک از این اطلاعات مربوط به حوزه‌های متفاوتـی بوده و متولیان خاص خـود را دارد، برای انجام یک ممیزی کامل و دقیق فناوری اطلاعات لازم است تجمیع و همبستگی بین این اطلاعات برقرار شـده تا روند ممیزی (Audit Trail) به صورت مناسبی شـکل گیرد. حتی به صورت سـاده‌تر نیز برای مقایسه سیاست‌های سازمان، اقدامات برنامه‌ریزی شده برای انطباق با سیاست‌ها و وضعیت جاری سامانه‌ها، یک ممیز نیاز دارد اطلاعاتی از زمینه‌ها و سامانه‌های مختلف و متفاوت را جمع آوری کند. مسلماً تجمیع چنین حجمی از اطلاعات پراکنده علاوه بر صرف زمان ممیز و ممیزی‌شـوندگان (و به تبع آن تحمیل هزینه به سـازمان)، نیازمند آشنایی و تسلط ممیزان بر هر یک از سـامانه‌های اشاره شده است تا بتوانند اطلاعات مناسب و صحیح را از آن اسـتخراج کرد. چنین مهارت‌هایی ممکن است نزد برخی ممیزان باتجربه یافت شود، اگرچه با تعدد روز افزون سامانه‌ها و ابزارهایی که برای کاربردهای فوق استفاده می‌شود، کمتر متخصصی را می‌توان یافت که بر تمامی این ابزارها تسـلط داشـته باشـد. این مشکل علاوه بر تأثیر منفی بر کارایی ممیزی، می‌تواند کیفیت یافته‌ها را نیز متأثر سازد.

راهـکاری کـه می‌تواند مسـئلهٔ فوق را تـا حد زیـادی کاهش دهد بهره‌برداری از نظامی اسـت که کلیه اطلاعـات مورد نیاز را به‌صورت مرتبط با هم نگهداری کند؛ به‌گونه‌ای که به‌طور مثال برای یک دارایی سـازمان، اطلاعات مربوط به مخاطرات شناسـایی شده، کنترل‌های پیاده‌سازی شـده و در دست پیاده‌سازی، رخدادهای به‌وقوع پیوسته، تغییراتی که آن دارایی را متأثر کرده، خط مشی‌ها و روال‌های سازمانی که نحوه پیکره‌بندی و بهره‌برداری از آن دارایی را بیان می‌کند و...، به صورت منسـجم از آن قابل استخراج باشد. چنین اطلاعاتی برای یک ممیز مجرب امکان بررسـی یک موضوع خاص را از زوایای مختلف و هم‌چنیـن امکان صحه‌گذاری دقیق‌تر و قرار دادن یک یافته یا توصیه در بافتار مناسـب را فراهـم می‌کند. این ویژگی یـک عنصر کلیدی بیشتر راهکارهای معتبر IT GRC است.

پیگیـری وضعیت یافته‌هـا و اقدامات اصلاحی مورد نیاز

ممیزی، فرآیندی اسـت که از برنامه‌ریزی، تا اجرا و ارایه گزارش و پس از آن تا طرح‌ریزی اقدامات مورد نیاز بسـتن عدم انطباق‌ها و یا بهره‌برداری از توصیه‌ها و نهایتاً تعقیب اقدامات تا رسـیدن به نتیجه مطلوب را در بر می‌گیرد. تمرکز صرف بر قسمت ملموس‌تر و احتمالاً فعال‌تر ممیزی (اجرای ممیزی و ارایه یافته‌ها) منجر به از دست رفتن یا کم اثر شدن بخش بسیار مهم ممیزی که پیگیری

اقدامات ناشـی از ممیزی است خواهد شـد. در سازمان‌هایی که ممیزی به عنوان یک عملکرد سـازمانی تثبیت شده است (تحت نـام واحد ممیزی، تضمین کیفیت یـا....) بخش عمده‌ای از وقت ممیزان مصروف پیگیری عملیاتی و اجرایی شدن اقدامات و احیاناً میزان پیشـرفت پروژه‌های تعریف شـده متناظر می‌شود؛ این امر در مورد ممیزی‌هایی که توسـط یک بدنه خارج از سازمان انجام شـده باشـد عموماً بسـیار ضعیف‌تر صورت می‌پذیرد. با توجه به این‌کـه این پیگیری‌ها در بسـیاری مواقع جنبـه اضافی و جانبی بـر کار اصلی متولیان پیگیری و اجـرای اقدامات را دارند، تمایل زیادی برای حرکت به سـمت شکل‌گرایی و سطحی شدن وجود خواهد داشـت. هم‌چنین از منظر مدیران و راهبران سازمان (بدنه راهبری) اثر اجرای این اقدامات و یا تبعات تأخیر در اجرای آن‌ها بر شاخص‌های اساسی سـازمانی مغفول می‌ماند. به عبارت دیگر امکان رصد تحقق و هم‌چنین اثر بخشی اقدامات ناشی از ممیزی برای ذینفعان در سطوح مختلف فراهم نمی‌شود.

برای پاسـخ به این مسـئله، IT GRC می‌تواند با یکپارچه نمودن یافته‌های ممیزی با وظایف دیگر محول شـده از برنامه‌های دیگر (مانند مدیریت مخاطرات، پروژه‌های راهبری و ...) از دو جهت به پیگیری و شفاف‌سازی نتیجه اقدامات ناشی از ممیزی یاری رساند. از آن‌جا که موضوع برنامه‌ریزی و مدیریت وظایف بخشـی اساسی از نظام IT GRC به شمار می‌رود، با گنجاندن اقدامات برنامه‌ریزی شده در نظام مدیریت برنامه و وظایف IT GRC امکان تسهیل اجرا و پیگیـری آن در مجموعه‌ای واحد بـرای متولیان فراهم خواهد شد. از سـوی دیگر، با مرتبط کردن یافته‌های ممیزی و اقدامات ناشـی از آن بـا برنامه‌های دیگر، IT GRC امکان ایجاد شـفافیت برای ذینفعان سازمانی از اثرات و مخاطرات بازبودن یا بسته شدن یک اقدام ناشـی از ممیزی بر اهداف سـازمان فراهم می‌شود. به عنوان مثال، اثر یافته‌های ممیزی بر اهداف کسب‌وکاری می‌تواند در داشـبورد کلان مخاطرات سـازمانی نمایش داده شود. به این ترتیب علاوه بـر امکان رصد کردن دقیق‌تـر اقدامات و برنامه‌ها، تعهد و پشـتیبانی لایه‌های مختلف سازمان امکان نمود بیشتری پیدا خواهد کرد.

مراجع

Erik T. Heidt; "Achieving IT GRC Success", GARTNER Technical Professional Advice, 10 May 2013

Vasant Raval, Greg Dyche; "Seven Myths of Information Governance", ISACA Journal, vol. 4, 2012

French C Aldwell, John A. Wheeler; "Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms", GARTNER, 24 September 2013

آشنایی با «انجمن علمی حسابرسی فناوری اطلاعات ایران»

حسابرسی فناوری اطلاعات رویکردی است که حرفه حسابرسی برای حفظ جایگاه و اثربخشی خود در محیط‌های مبتنی بر فناوری اطلاعات از آن بهره می‌گیرد. حسابرسی فناوری اطلاعات که گاهی تحت عناوین دیگری نظیر حسابرسی سیستم‌های اطلاعاتی، حسابرسی سیستم‌های کامپیوتری و حسابرسی کامپیوتر نیز از آن نام برده می‌شود عبارت است از: «بررسی و آزمون مستقل رکوردهای اطلاعاتی و فعالیت‌ها به منظور ارزیابی کفایت کنترل‌های داخلی سیستم‌های کامپیوتری برای حصول اطمینان به رعایت سیاست‌ها، روش‌ها و رویه‌های عملیاتی مصوب، و پیشنهاد اطلاحات لازم در کنترل‌های داخلی».

حسابرسی فناوری اطلاعات علاوه بر کمک به حسابرسان در به‌کارگیری موثر فنون مختلف کامپیوتری به منظور استخراج و تحلیل شواهد الکترونیکی، و نیز ارایه پیشنهادهای حرفه‌ای برای کنترل موثر دارایی‌ها و فعالیت‌های حوزه فناوری اطلاعات به مدیریت، خدمات فنی مستقلی را برای کمک به حسابرسان داخلی و مستقل غیر فناوری اطلاعات فراهم می‌کند. برخی از خدمات متداول حسابرسان فناوری اطلاعات در حوزه‌های مختلف عبارت است از:

(۱) بررسی رعایت قوانین و مقررات، سیاست‌ها، استانداردها و رویه‌های مربوط به خدمات فناوری اطلاعات سازمان‌ها و شرکت‌ها، مفاد قراردادهای مرتبط با خدمات فناوری اطلاعات و غیره

(۲) بررسی چگونگی مدیریت و استفاده از منابع اطلاعاتی (سخت‌افزار، نرم‌افزار، پرسنل)

(۳) بررسی امنیت فیزیکی و منطقی مراکز داده، انبارهای ذخیره‌سازی تجهیزات و رسانه‌های ذخیره‌سازی

(۴) ارزیابی انواع کنترل‌های عمومی و کاربردی سیستم‌های اطلاعاتی مانند کنترل تغییر نرم‌افزار، چرخه‌عمر پیاده‌سازی سیستم، و غیره،

(۵) بررسی چگونگی برنامه‌ریزی برای تداوم فعالیت‌های شرکت و بازیابی پس از توقف‌های غیر مترقبه

با توجه به نقش و اهمیت روز افزون حسابرسی فناوری اطلاعات، انجمن‌ها و کمیته‌های علمی و نیز تشکل‌ها و مجامع متعدد حرفه‌ای حسابرسی فناوری اطلاعات از بیش از ۳ دهه گذشته در کشورهای پیشرو ایجاد، و به‌صورت گسترده‌ای فعالیت داشته و ضمن ارایه خدمات در عرصه علمی و حرفه‌ای با هماهنگی دانشگاه‌ها اقدام به تشکیل دوره‌های تخصصی این رشته در مقاطع کارشناسی ارشد و دکترا کرده‌اند. در همین راستا، «انجمن علمی حسابرسی فناوری اطلاعات ایران» با کسب مجوز رسمی از وزارت علوم، تحقیقات و فناوری و با مشارکت تنی چند از اساتید برجسته و متخصصین فعال در حوزه فناوری اطلاعات، حسابداری، و حسابرسی کشور در اسفند ۱۳۸۸ تشکیل و فعالیت خود را به منظور حصول به اهداف زیر آغاز کرد:

- تشکیل کارگروه‌های علمی و تخصصی حسابرسی فناوری اطلاعات
- ارایه خدمات آموزشی، پژوهشی و تخصصی
- برگزاری همایش‌های ملی و بین‌المللی
- ترغیب و تشویق متخصصین، پژوهشگران و تجلیل از محققان و استادان ممتاز، و
- انتشار نشریات و کتب تخصصی

هیئت موسس انجمن عبارت است از:

- دکتر مهدی خدمتی (لیسانس کامپیوتر، فوق‌لیسانس حسابرسی کامپیوتر، دکترای مالی از دانشگاه موناش استرالیا، و حسابرس رسمی داخلی از انجمن حسابرسان داخلی آمریکا، حسابرس

▼ بقیه در صفحهٔ ۴۰

انجمن حسابرسان داخلی ایران

درباره انجمن

انجمن حسابرسان داخلی ایران به منظور ساماندهی لازم برای تبیین مناسب تر نقش حسابرسی داخلی با هدف ارزش آفرینی و افزایش قابلیت اتکا و اعتماد به گزارش‌های مالی و غیرمالی (عملکرد) در بنگاه‌های انتفاعی و غیرانتفاعی در بخش‌های دولتی و خصوصی و نهادهای عمومی دولتی و غیردولتی و به‌منظور شفافیت هر چه بیشتر اطلاعات مالی و غیر مالی و ترویج فرهنگ پاسخگویی در سطح کشور، در سال ۱۳۹۱ تشکیل شده است.

اهداف انجمن

هدف از تشکیل انجمن عبارت است از تنظیم امور و اعتلای حرفه حسابرسی داخلی در کشور و نظارت حرفه‌ای بر کار حسابرسان داخلی از طریق:

الف – تشکل حسابرسان داخلی کشور و برقراری ارتباط مستمر فنی و حرفه‌ای بین آنان

ب – گسترش کیفی و کمی خدمات حرفه‌ای حسابرسی داخلی در کشور

پ – تهیه و تدوین استانداردهای حسابرسی داخلی و ارایه به مراجع ذیصلاح کشور برای تصویب

ت – ارتقای دانش تخصصی و حرفه‌ای اعضا از طریق انتشار کتب و نشریات تخصصی به صورت کاغذی یا الکترونیکی

ث – حمایت از حقوق حرفه‌ای اعضا

ج – تعامل با تشکل‌های حرفه‌ای منطقه‌ای و بین‌المللی و در صورت لزوم عضویت در آن‌ها مطابق با ضوابط و قوانین کشور

چ – همکاری با دستگاه‌های ذیربط در تدوین قوانین و مقررات مربوط

کمیته‌ها

۱- کمیته تعیین صلاحیت، آزمون و پذیرش
۲- کمیته اعضای حقوقی
۳- کمیته آیین رفتار حرفه‌ای
۴- کمیته فنی و تدوین استانداردهای حسابرسی داخلی
۵- کمیته آموزش و تحقیقات
۶- کمیته کنترل کیفیت
۷- کمیته حسابرسی فناوری اطلاعات (Audit IT)
۸- کمیته قوانین و مقررات
۹- کمیته شرکت‌های پذیرفته شده در بورس اوراق بهادار
۱۰- کمیته برگزاری همایش‌ها و سمینارها

علاوه بر شرایط ذکر شده در اساسنامه انجمن برای پذیرش اعضای حقیقی، فارغ التحصیلان رشته مهندسی کامپیوتر (سخت‌افزار، نرم‌افزار و فناوری اطلاعات)، که خدمات برجسته‌ای را به حرفه حسابرسی داخلی در کشور عرضه نموده‌اند و یا سابقه مدیریت واحد حسابرسی فناوری اطلاعات داشته یا دست کم سه سال سابقه کار در واحدهای حسابرسی داخلی، عملیاتی یا حسابرسی فناوری اطلاعات داشته باشند، می‌توانند به عضویت انجمن پذیرفته شوند.

کمیته حسابرسی فناوری اطلاعات (IT Audit)

کمیته حسابرسی فناوری اطلاعات در انجمن حسابرسان داخلی ایران برای تامین اهداف در حوزه‌های زیر تشکیل گردیده است:

۱- حسابرسی فناوری اطلاعات (Information Technology Audit)

با عنایت به اهمیت روزافزون سامانه‌های عملیاتی مبتنی بر فناوری اطلاعات در سازمان‌ها و افزایش درجه اتکاء سازمان‌ها به ویژه سازمان‌های بزرگ به چنین سامانه‌هایی، اهمیت بررسی و حصول اطمینان از میزان کارایی و قابلیت اتکاء عملیاتی سامانه‌های مبتنی بر فناوری اطلاعات و اعمال نظام‌های کنترلی مدیریتی در چنین سامانه‌هایی، اهداف و برنامه‌های زیر در برنامه کمیته فناوری اطلاعات انجمن در نظر گرفته شده است:

۱-۱. انتخاب استانداردهای قابل به‌کارگیری در حوزه حسابرسی فناوری اطلاعات در کشور

۱-۲. ترجمه و کمک به بومی‌سازی و اختصاصی کردن استانداردهای حسابرسی فناوری اطلاعات

۱-۳. تدوین مراحل استقرار استانداردهای حسابرسی فناوری اطلاعات

۲- حسابرسی به کمک کامپیوتر و بهره گیری از فناوری اطلاعات (Computer Assisted Audit) :

ضرورت استفاده از ابزارهای کامپیوتری و فناوری اطلاعات در اجرای برنامه‌های حسابرسی و حسابرسی داخلی هم اکنون سال‌ها است که مورد توجه قرار داشته و عملاً درکشورهای مختلف دنیا به صورت عملی در این حرفه‌ها مورد استفاده است. در این چارچوب کمیته فناوری اطلاعات انجمن، اهداف و برنامه‌های زیر را دنبال خواهد نمود:

۲-۱. مطالعه تطبیقی و استخراج کاربردهای متصور فناوری اطلاعات در اجرای فرآیند حسابرسی

۲-۲. انتخاب استانداردها و رویه‌های قابل به‌کارگیری در حوزه حسابرسی به کمک کامپیوتر در کشور

۲-۳. بررسی و اظهار نظر در رابطه با نرم‌افزارهای حسابرسی کامپیوتری

۲-۴. ترجمه و کمک به بومی‌سازی و اختصاصی کردن دستورالعمل‌ها، رویه‌ها و سامانه‌های حسابرسی کامپیوتری

۲-۵. تدوین مراحل به‌کارگیری فناوری اطلاعات در فرآیند حسابرسی

۳- ارتباطات با جوامع حرفه‌ای و آموزشی:

۳-۱. همکاری در تدوین برنامه دوره‌های آموزشی و آزمون‌های ارزیابی حرفه‌ای شاغلین در حوزه حسابرسی فناوری اطلاعات و همکاری در برگزاری دوره‌های آموزشی در این حوزه

۳-۲. همکاری با شورای عالی انفورماتیک و سازمان نظام صنفی رایانه‌ای کشور در حوزه حسابرسی فناوری اطلاعات و حسابرسی کامپیوتری

▼ ادامه از صفحهٔ ۴۰

رسمی سیستم‌های اطلاعاتی از انجمن حسابرسی و کنترل سیستم اطلاعاتی آمریکا و مدرس دانشگاه موناش استرالیا)،

- دکتر حمیدرضا ربیعی (دانشیار دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف)
- دکتر کامبیز بدیع (دانشیار و عضو هیئت‌علمی پژوهشگاه ارتباطات و فناوری اطلاعات ایران)
- دکتر احمد شربت‌اوغلی (استادیار دانشکده اقتصاد و مدیریت دانشگاه صنعتی شریف)
- دکتر مسعود اسدپور (استادیار دانشکده مهندسی برق و کامپیوتر دانشگاه تهران)
- دکتر علی ثقفی (دانشیار دانشکده حسابداری و مدیریت دانشگاه علامه طباطبایی)
- دکتر ویدا مجتهدزاده (دانشیار دانشکده حسابداری دانشگاه الزهرا)
- دکتر سید حسین سجادی (دانشیار دانشکده حسابداری دانشگاه شهید چمران اهواز)
- دکتر امید پورحیدری (دانشیار دانشکده حسابداری دانشگاه شهید باهنر کرمان)
- مهندس حمید علی‌حسینی (مدیر عامل شرکت داده‌ورزی سامانه و فوق لیسانس کامپیوتر و دانشجوی دکترای حسابداری)

این انجمن از همکاری کلیه سازمان‌ها و نهادهای دولتی و غیردولتی و نیز اساتید، دانشجویان و متخصصین علاقمند رشد و ارتقاء حرفه حسابرسی فناوری اطلاعات در کشور استقبال می‌کند.

Interview
مصاحبه

رصد اطلاعات شهری در رصدخانه شهرداری تهران

مصاحبه با آقای مهندسی حسن علیشیری
کارشناس رصدخانه شهرداری تهران
(زیرمجموعه سازمان فناوری اطلاعات و ارتباطات شهرداری تهران)

بی‌گمان با شنیدن کلمه رصدخانه شهر تهران، اولین چیزی که به ذهن خطور می‌کند اتاقی است با تلسکوپ‌های بزرگ و پیچیده و کمتر کسی قبل از بازدید از رصدخانه یا مطالعه اطلاعات در مورد آن باور می‌کند که رصدخانه شهر تهران با موضوع ممیزی اطلاعات رابطه تنگاتنگی داشته باشد. پس از بازدید اولیه از رصدخانه برآن شدیم تا با آقای مهندس علی‌شیری، در مورد رصدخانه‌های شهری، کاربردها و مزایای آن به صحبت بنشینیم. در لابه لای صحبتمان ایشان به دغدغه بسیار مهم «خطر پرداختن غیر منطقی به تجهیزات ارایه به‌جای تمرکز بر ایجاد پایگاه یکپارچه اطلاعات شهری» اشاره کردند، که به نظر می‌رسد یکی از مخاطرات اصلی همه‌گیر شدن این رصدخانه‌ها در سطح کشور است. آنچه در ادامه می‌خوانید حاصل گفتگو دوستانه ما با این مهندس جوان است.

■ پرسش: اگر مدیریت را به سه گروه مدیریت در شرایط عادی، مدیریت در شرایط اضطراری و مدیریت در بحران تقسیم کنیم به نظر می‌رسد رصدخانه در نوع سوم مدیریت نقش ایفا می‌کند آیا برداشت من از رسالت رصدخانه درست است؟

در مدیریت بحران هم می‌تواند کاربرد داشته باشد اما نکته کلیدی آن است که برخلاف مراکز مدیریت بحران یا بهتر بگویم مفهوم مدیریت بحران که مبتنی بر پایش لحظه به لحظه شهر است، رصدخانه هدفش پایش بطنی شهر است بدین معنا که اگر بارندگی شدیدی در شهر رخ دهد که گرفتگی معابر را در پی داشته باشد، رصدخانه در لحظه در آن مداخله نمی‌کند بلکه این واقعه را تنها به عنوان یک رویداد ثبت می‌کند تا بتوان با ارایه این موضوع که در ده سال گذشته تعداد آب‌گرفتگی‌ها چند مورد بوده، این موارد بیشتر در کدام مناطق واقع شده و اطلاعاتی از این دست در اتخاذ تصمیمات مناسب به مدیران و ایجاد سازوکارهای لازم برای پیشگیری از این موارد کمک کننده باشد. بنابراین در بحران ما مستقیما مداخله نمی‌کنیم ممکن است اطلاعات ما برای شناخت بهتر شهر در زمان بحران نیزمورد استفاده قرار گیرد اما هدف اصلی رصدخانه مدیریت بحران نیست. موضوع رصدخانه پایش و نمایش اطلاعات شهری است که معمولاً در هیاهوی مدیریت شهر در لحظه و در روند سیر تحولات گم می‌شود. مدیران شهری به خاطر مشغله‌های زیادی که دارند و خدمت‌رسانی

مستقیمی که باید به مردم انجام دهند کمتر می‌تواند روی تغییرات رفتار شهروندی و عناصر شهری در دراز مدت تمرکز کنند. به گمان بنده در سلسله مراتب مدیران حاکمیتی، مدیران شهری بیش از همه با مردم به طور مستقیم سر و کار دارند از ارتباطات روزانه مستقیم. مثل جمع آوری زباله و نظافت خیابان‌ها گرفته تا ارایه خدمات کلان حمل و نقل شهری و غیره. مدیران شهری به دلیل دغدغه‌های این چنینی به شدت درگیر روزمرگی هستند و بخش‌های پژوهشی در شهر هم تمرکزشان بر راهکارهایی برای ارتقاء بهبود کیفیت خدمت شهری است، یک حلقه مفقوده وجود دارد که آن بررسی تحولات

شـــهر دربازه‌های زمانی بلند است. در رصدخانه به دنبال پرکردن این شکاف و ایجاد این حلقه مفقوده هستیم، البته رصدخانه اهداف متعدد دیگری هم دارد. اما از آنجا که برای تمامی مهمان‌های رصدخانه که ما برای آن‌ها امکانات رصدخانه را ارایه کردیم این برداشت اشتباه ایجاد شـد که هدف نهایی از رصدخانه مدیریت بحران است می‌خواستم در ابتدا تاکید کنم که هدف اصلی رصدخانه این مورد نیست.

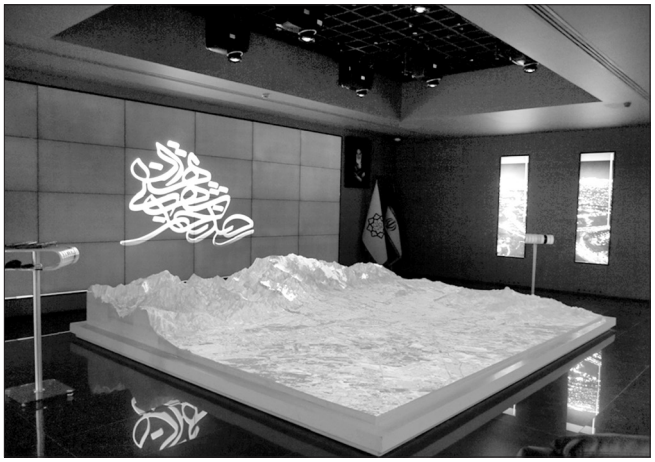
هدف از رصدخانه ایجاد یک شاهراه اطلاعاتی است که کلیه اطلاعات شـهری از کلیـه نهادهـای مرتبط از طریق سـنجش شـاخص‌های مشـترک، جمع آوری، یکپارچه شـده، از طریـق کانال‌های مختلف ارتباطی در اختیار کلیه مخاطبین از شهروندان گرفته تا مورد استفاده پژوهشگران و مدیران شهری برای اتخاذ تصمیمات مناسب قرار گیرد.

■ پرسش: رصدخانه شهری چیست؟

رصدخانه اطلاعات شهری ترجمه اصطلاح Urban observatory است که ما برای observe واژه فارسـی «رصد» را به عنوان معادل انتخاب کردیم. شاید اگر آن را به «مرکز پایش اطلاعات شهری» ترجمه می‌کردیم با رصد سـتارگان و بحث‌های نجوم اشتباه نمی‌شد. به هر صورت رصدخانه‌های شـهری، مرکز پایش اطلاعات و آمار شهرها در جهان هستند. در تهران هم در این زمینه از سال‌ها پیش، نیاز وجود مرکزی فعال که وظیفه اصلی آن جمع‌آوری و یکپارچه‌سازی اطلاعات شهری باشد وجود داشته است که با احداث این رصدخانه به این نیاز پاسخ داده شد.

رصدخانه شـهر تهران، در ابتدای تاسیس به دلیل سابقه چندین ساله سازمان فناوری اطلاعات شهرداری تهران در بحث جمع‌آوری و تجمیع اطلاعـات با یـک مجموعه غنـی از اطلاعات کار خود را شـروع کرد، برعکس بسیاری از شهرهای مهم دنیا که عدم وجود چنین سازمانی در آن‌ها باعث شده فرآیند ممیزی و جمع آوری اطلاعات به صورت کامل در رصدخانه انجام شـود. لذا در گام نخسـت، تمرکز ما بیشتر بر روی نمایش و بصری سـازی اطلاعات بوده، به ویژه که در این رصدخانه ما امکانات مناسـبی به‌منظور ارایه و انتقال اطلاعات تجهیز شده است. از یک ماکت در مقیاس ۱/۱۰۰۰۰ که بر اسـاس عوارض توپوگرافی شهر تهران سـاخته شده و به وسیله ۶ ویدئو پروژکتور با تفکیک‌پذیری بالا اطلاعات بر روی ماکت نمایش داده می‌شـود بهره برده‌ایم. با اسـتفاده از این امکانات سـخت‌افزاری امکان ایجاد تصور زنده‌ای از شـهر تهران مهیا شـده است. در سـالنی که به منظورِ ارایه، مجهز شده است علاوه بر امکانات عنوان شده، نمایش تصاویر دوبعدی و سه‌بعدی با ویدیو نیز امکان‌پذیر است. هم‌چنین تلاش شـده معماری و فضای صوتی سالن نمایش به گونه‌ای باشـد که بتوان تمرکز مخاطب را در نهایت بر روی اطلاعات بالا برد و بالاترین حد تاثیرگذاری را داشت.

اما آنچه در رصدخانه شهر تهران فعلا اتفاق افتاده است با تحقق کامل Urban observatory فاصله دارد. به دلیل آن که در رصدخانه شهر تهران برای اولین بار اقدام به ارایه اطلاعات خاص از رصد شهری به این صورت شده است. اما بقیه رصدخانه‌های دنیا به اندازه ما نیاز به ارایه ندارند. هر

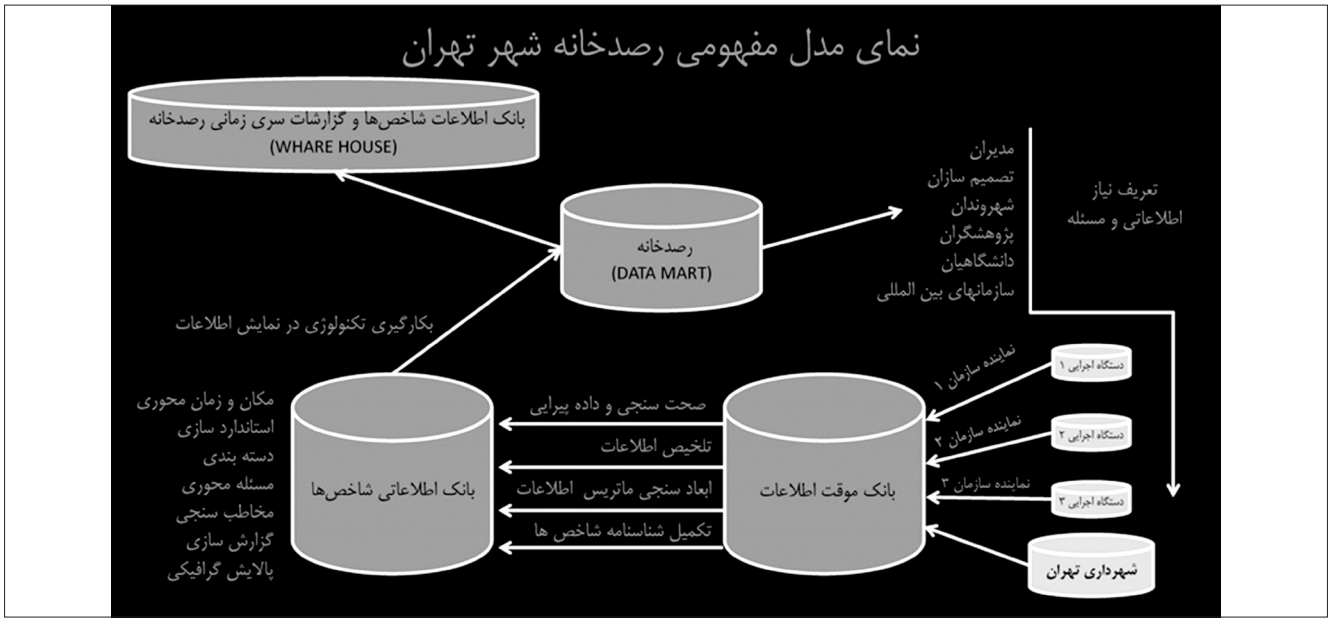


چند کار ما تنها ارایه (Presentation) نیست بلکه کار ما Presentation و Demonstration به معنای انواع ارایه با اهداف متفاوت اسـت. اما همین موضوع هم در دنیا به عنوان هدف کلیدی ایجاد رصدخانه نمی‌باشـد، بلکه ایجاد همان شـاهراه اطلاعاتی که به آن اشاره کردم حایز اهمیت اسـت. در واقع، نمایش، تنها بخش کوچکی از این کوه بزرگ یخ است کـه از آب بیرون آمده در حالی که اصل کوه یخ از جمع‌آوری گرفته تا تجمیع و سپس استانداردسازی و مقایسه با سایر شهرها، اقداماتی است که در برنامه کاری رصدخانه در آینده قرار دارد.

نکته که پس از ارایه‌ها برای افراد مختلف برای ما مشـخص شـد آن است که ارایه اطلاعات در رصدخانه شهری و با استفاده از امکانات که ذکر کردم مخاطب را نسبت به اطلاعات و صحت آن حساس می‌کند و همین باعث می‌شـود در مجموعه خود اقداماتی را در جهت تکمیل اطلاعات ما یا ارایه خدمات بهتر انجام دهد. حضور شهرداران مناطق در رصدخانه باعث شـده که آن‌ها با دقت بیشتری اطلاعات را بررسی کننـد در صورتـی که این اطلاعـات قبلاً از طریـق کتابچه‌هایی که سـازمان فناوری اطلاعات هر ساله چاپ می‌کند در اختیار آن‌ها قرار گرفته بوده است. در واقع ما با تمرکز بر مشکلات و بزرگ‌نمایی آن‌ها از طریق امکانات رصدخانه و به رخ‌کشـیدن اطلاعات باعث می‌شویم سـازمان‌ها متوجه مشکلات موجود در مجموعه خود شده برای بهبود آن راه‌کارهای اصلاحی طراحی و اجرا کنند.

■ پرسش: بر اساس توضیحاتی که فرمودید به نظر می‌رسد که شما نقش مهمی در ممیزی صحت اطلاعات دارید و بازخوردهایی که براساس نتایج این ممیزی به سازمان‌ها ارایه می‌کنید ورودی مناسب برای انجام اقدامات اصلاحی در این سازمان‌ها است.

کاملاً درسـت اسـت. بدین علت که ما خروجی حاصـل از ممیزی و هم‌چنین جمع آوری اطلاعات شـهری را در معـرضِ دید مخاطبین مختلـف قرار می‌دهیـم. و این مخاطبین وقتـی در فضای رصدخانه قـرار می‌گیرند تمرکز بیشـتری بر روی اطلاعات دارند و نسـبت به آن موضـع می‌گیرند و ایـن موضع‌گیری باعث می شـود هم صحت اطلاعات جمع‌آوری شـده در رصدخانه ممیزی شود و هم در زمینه



شکل ۱

رفع معضلاتی که در ارایه در رصدخانه بزرگنمایی شده است اقدامات اصلاحی در سازمان مخاطب صورت گیرد. به عنوان مثال بارها پیش آمده معاونین و شهردار یک منطقه برای بازدید، مهمان رصدخانه بوده‌اند و نسبت به صحت اطلاعات ارایه نشده نکاتی را عنوان کرده‌اند و این باعث شده در سنجش بعدی اطلاعات دقیق‌تری از آن منطقه ارایه شود. مثلا در بخش شاخص‌های اجتماعی که بخشی پر چالش است وقتی نتایج این ارزیابی‌ها به مخاطبان که ممکن است نهادهای خارج از مجموعه شهرداری باشند ارایه می‌شود نسبت به آن واکنش نشان می‌دهند و گاهی این واکنش به همکاری دوجانبه نهادها برای دستیابی به اطلاعات صحیح‌تر می‌انجامد.

راهکار دیگر ما برای ارایه بازخورد مناسب به ارگان‌های شهری و هم‌چنین طرح‌ریزی اقدامات اصلاحی ایجاد ۶ کارگروه در رصدخانه است که ۴ کارگروه شهرسازی، اجتماعی- فرهنگی، حمل و نقل و ترافیک و محیط زیست هم‌اکنون فعالیت خود را شروع کرده و ۲ کارگروه دیگر مدیریت هوشمند شهری و مدیریت بحران در آینده تشکیل خواهند شد. اعضای این کارگروه‌ها از نمایندگان سازمان‌های مختلف هستند. طراحی این کارگروه‌ها در جهت بالابردن کمیت و کیفیت اطلاعات شاهراه اطلاعاتی است که به آن اشاره کردم، بدین طریق ما وظیفه تامین اطلاعات این شاهراه اطلاعاتی را نیز انجام می‌دهیم. سازمان فناوری اطلاعات، اطلاعات حوزه شهرداری را جمع‌آوری می‌کند و ما در رصدخانه طرح ایجاد پایگاه جامع اطلاعات شهری را بر عهده داریم.

با استقرار کارگروه‌ها موضوع ممیزی صحت اطلاعات پیش از ارایه اطلاعات نیز تحقق می‌یابد. به عنوان مثال در نظر بگیرید در زمینه یک بحران اجتماعی مانند اعتیاد معاونت فنی اجتماعی شهرداری، اطلاعاتی براساس طرح سنجش عدالت و به روش نمونه‌برداری جمع‌آوری کرده است. این اطلاعات قبل از آن که در معرض بازدید عموم قرار گیرد و در سالن نمایش ارایه شود در کارگروه مربوطه با حضور نمایندگانی از تمامی نهادهای مرتبط مانند نماینده نیروی انتظامی، نماینده قوه قضاییه، نماینده بهزیستی، بررسی می‌شوند. اطلاعات ممیزی و صحت آن‌ها تضمین می‌شوند سپس در معرض نمایش عموم قرار می‌گیرند.

هدف نهایی ما تحقق کامل ممیزی صحت اطلاعات و یکپارچه‌سازی اطلاعات از طریق کارگروه‌هاست. هم اکنون در رصدخانه در کارگروه شهرسازی تا حد بسیار زیادی این موضوع محقق شده است. ولی در سایر کارگروه‌ها در حال مکاتبه و طی کردن مراحل رسمی به منظور ایجاد ارتباطات با تمامی نهادها و سازمان‌هایی هستیم که در حوزه شهری دارای مسئولیت بوده و ثبت کننده اطلاعات و یا درخواست دهنده آن هستند.

■ پرسش: در مورد مدل مفهومی جمع‌آوری اطلاعاتتان بیشتر توضیح می‌دهید؟

مدل مفهومی که ما در پی پیاده‌سازی کامل آن هستیم در شکل ۱ مشخص است.

بر اساس این مدل نقطه شروع، نیازهای اطلاعاتی است که توسط مدیران، تصویرسازان، شهروندان، پژوهشگران وسازمان‌های بین‌المللی اعلام می‌شوند. دستگاه‌های اجرایی برای تامین این نیاز، اطلاعاتشان را در یک بانک موقت اطلاعات جمع‌آوری می‌کنند. بر روی اطلاعات، فرآیند صحت‌سنجی، تلخیص اطلاعات، ابعادسنجی ماتریس اطلاعات، تکمیل شناسنامه شاخص‌ها انجام شده، اطلاعات تغییر یافته وارد بانک اطلاعاتی شاخص‌ها می‌شوند. سپس مکان و زمان محوری، استانداردسازی، دسته‌بندی مساله محوری، مخاطب‌سنجی، گزارش‌گیری و پالایش گرافیکی بر روی آن‌ها انجام می‌شود و در

نهایت اطلاعات در Data martهای رصدخانه شهری تهران ذخیره می‌شوند و با استفاده از امکانات سخت‌افزاری که به آن اشاره شد به مخاطبین نمایش داده می‌شوند. Data martها بخشی از انبارداده‌های بزرگ شهر تهران خواهند بود که می‌تواند جوابگوی نیازها، مسایل و مشکلات جدید نیز باشند.

■ پرسش: در واقع شما با رویکردتان در رصدخانه به دنبال ایجاد مدیریت یکپارچه شهری هستید؟

این هدف نهایی ماست. اگر بخواهیم برای رصدخانه یک ماموریت اصلی تعریف کنیم. آن ماموریت «دستیابی به مدیریت یکپارچه شهری» است. این مورد در تهران که نهادها و ارگان‌های مختلف مسوول ارایه خدمات شهری هستند و یک نهاد یگانه، مسئولیت نظارت بر فعالیت آن‌ها را ندارد بسیار حیاتی‌تر از جایی مانند نیویورک است که شهردار بر همه نهادهای خدمات شهری نظارت مستقیم دارد. در بحث تجمیع اطلاعات شهری مشکل ما ایجاد زیرساخت‌های فناوری و راه‌کارهای مکانیزه تجمیع اطلاعات نیست، مشکل ما تعامل بین سازمان‌ها و تصویب و توافق یک استاندارد واحد در زمینه تعریف شاخص‌ها و جمع‌آوری اطلاعات است. عدم وجود چنین استانداردی که مورد توافق تمامی نهادهای خدمات شهری باشد، باعث شده شاخص‌های مشترک در جمع‌آوری اطلاعات وجود نداشته باشد و همین موضوع سبب اجرای اقدامات موازی در نهادهای در زمینه جمع‌آوری اطلاعات شده است. در نهایت هم نمی‌توان این اطلاعات را به علت تفاوت در نوع جمع‌آوری یکپارچه کرد. همان‌طور که گفتم در کارگروه‌ها ما به دنبال دستیابی به استاندارد واحد و موضوع یکسان‌سازی برداشت‌ها هستیم. در واقع ما می‌خواهیم نهادهای مختلف شهری مرتبط با هر کارگروه در کارگروه مربوطه حضور فعال داشته باشند و علاوه بر ارایه اطلاعات خودشان به ما صحت اطلاعات ما را نیز ممیزی کنند. باز هم تاکید می‌کنم رصدخانه شهری تهران خیلی نوپاست و فعالیت‌های خود را در این راستا تازه شروع کرده است. به ویژه که بحث رصد اطلاعات شهری ذاتاً کار جدیدی است که در کشور برای اولین بار انجام شده است. و حتی در بخش دانشگاهی و آکادمیک هم شناخت دقیقی از آن وجود ندارد. بنابراین تجربه و دانش داخلی در این زمینه بسیار کم است. اما در مواردی که بخش عمده اطلاعات در اختیار شهرداری بود، مانند شهرسازی پیشرفت‌های خوبی داشته‌ایم.

هم‌اکنون ما با ۹ سازمان به منظور تبادل اطلاعات تفاهم‌نامه امضاء کرده‌ایم. با برخی از سازمان‌ها مانند سازمان آب منطقه‌ای تبادل اطلاعات هم صورت گرفته ولی با برخی دیگر فعلاً در حال نامه‌نگاری و طی مراحل قانونی هستیم.

بخشی که بسیار برای ما اهمیت دارد این است که به عنوان یک رصدخانه در UN habitant که بخش اصلاح سازمان بین‌الملل است و وظیفه ساماندهی رصدخانه شهری را بر عهده دارد ثبت شویم. UN habitant ایده Global Urban Observatory را دنبال می‌کند که به معنای رصدخانه شهری جهانی است. بر اساس این ایده رصدخانه‌ها در سه سطح محلی (Local)، منطقه‌ای (Regional) و ملی (National) تعریف شده‌اند که ما در رده محلی هستیم و در تلاش هستیم که بر اساس شاخص‌ها UN habitant به یک استاندارد ملی در زمینه تدوین شاخص‌ها و جمع‌آوری اطلاعات شهری با تمام سازمان‌های جمع‌آوری کننده اطلاعات شهری در شهر تهران برسیم. جمع‌آوری، یکپارچه‌سازی اطلاعات بر اساس شاخص‌های استاندارد و ارایه خروجی بر این اساس، باعث شناخت بهتر شهر تهران در عرصه بین‌المللی خواهد شد.

یکی از اهداف جانبی رصدخانه‌های شهری مقایسه شهرهاست. چیزی که در مورد شهرهای ایران هم‌اکنون امکان‌پذیر نیست. علت اصلی عدم امکان مقایسه شهرها، عدم وجود یک تعریف واحد از شاخص‌های ارزیابی است. به عنوان مثال تعریف شاخص بیکاری در اصفهان با تعریف این شاخص در تهران لزوماً یکسان نیست. لذا مقایسه نتایج عملاً بی‌معناست. علاوه بر تعریف نامشابه شاخص‌ها مشکل دیگر یکپارچه‌سازی اطلاعات، دامنه جمع‌آوری آن‌ها است. مثلاً ما اطلاعاتی در زمینه معضلات اجتماعی داریم که بر اساس طرح سنجش عدالت، به تفکیک هر محله و به صورت مکان محور جمع‌آوری شده است. اما بقیه نهادهای شهری اطلاعات را به صورت کلی جمع‌آوری می‌کنند. مکان محور بودن اطلاعات و مزایای آن در شهرداری امری بدیهی است اما در سایر ارگان‌ها توجیه لزوم آن نیاز به صرف انرژی و زمان دارد. مثلاً سازمان بهزیستی آمار کل معلولین شهر تهران را به تفکیک مناطق مختلف ندارد ولی اگر همین اطلاعات بر اساس محله‌ها و به صورت مکان محور جمع‌آوری شده بود بهزیستی می‌توانست در وهله نخست مناطقی که بیشترین معلولین را دارد شناسایی کرده و سپس در آن مناطق بودجه لازم برای بهسازی معابر را صرف کند. شاید صرف هزینه برای مناسب سازی کلیه معابر شهر تهران برای استفاده راحت‌تر معلولین غیرممکن باشد ولی قطعاً برای چند منطقه امکان‌پذیر است.

■ پرسش: با توجه به محدودیت بودجه، با این روش که شما توضیح دادید صرف بودجه هم هدفمندتر شده و تصمیمات درست‌تری هم می‌توان اتخاذ کرد؟

صد در صد همین‌طور است که اشاره کردید. به نفع نهادهای مخاطب هم هست در این زمینه ما فعلاً در مرحله ایجاد نیاز در بقیه سازمان‌ها هستیم در واقع هدف دیگری که با ارایه اطلاعات دنبال می‌کنیم این است که احساس نیاز را در نهادها ایجاد کنیم. قطعاً تا زمانی که نیازی ایجاد نشود اقدامی هم برای آن صورت نمی‌گیرد. به عنوان مثال اگر سازمان نظام صنفی بداند با ثبت آدرس شرکت‌ها به عنوان یک نقطه مکان محور چه خدماتی را فقط به اعضای خود می‌تواند ارایه کند قطعاً در این زمینه اقدام می‌کند.

■ پرسش: به نظر می‌رسد عدم جمع‌آوری اطلاعات به صورت مکان محور بیشتر از ناآگاهی نهادهای خارج از شهرداری نسبت

به مزایای این نوع جمع‌آوری است. و در صورتی که تحلیل‌های قابل حصول پس از ثبت اطلاعات مکان محور به سازمان‌ها ارایه شود، سازمان‌ها و ارگان‌ها به جمع‌آوری اطلاعات مکان محور تمایل بیشتری خواهند داشت؟

دقیقاً همین طور است. در واقع آن‌چه که از آن به عنوان «جریان آزاد اطلاعات» نام برده می‌شود در صورتی می‌تواند محقق شود که اطلاعات دقیق و درست وجود داشته باشد و در اختیار عموم مردم قرار گیرد. برگردم به مثال قبلی در مورد نظام صنفی، فرض کنید با مکان محور شدن این اطلاعات می‌توان به شرکت‌ها گزارش داد که تجمع شرکت‌های نرم‌افزاری در کدام منطقه تهران است؟ تجمع افراد متخصص در حوزه نرم‌افزار در کدام منطقه است؟ نحوه زیرساخت اطلاعاتی این مناطق چگونه است و تحلیل‌های نظیر این که با تجمیع اطلاعات به راحتی به‌دست می‌آیند. با این تجمیع صرف هزینه‌های شهری نیز به شدت پایین می‌آید حتماً به یاد دارید زمانی را که بسیاری از سازمان‌ها برای حفاری معابر اطلاع درستی از یکدیگر نداشتند و به محض پایان یافتن کار یک سازمان و ترمیم آسفالت، سازمان بعدی اقدام به حفاری در همان نقطه می‌کرد. اما هم اکنون ما در شهر تهران یک سیستم جامع حفاری داریم که هر نهادی که می‌خواهد در شهر حفاری کند ابتدا باید نقطه مدنظر خود را در آن سامانه ثبت کند. بدین طریق این اطلاعات از طریق زیرساخت فیبر نوری در اختیار همه نهادهای خدمت شهری قرار می‌گیرد. اما جالب است بدانید هم این نکته در شهری مانند نیویورک به گزارش یکی از مشاوران آن جزو معضلات است. یا هم اکنون هر فردی که با تلفن ثابت با آتش‌نشانی تماس می‌گیرد نشانی وی شناسایی شده و از طریق GPS به ماشین‌های آتش‌نشانی و آمبولانس اعلام می‌شود. با این که ارایه این خدمات از نظر تکنولوژی مسئله ساده‌ای است اما تعامل سازمان‌ها و نحوه ارایه یک خدمت یکپارچه بسیار تاثیرگذار است. بخشی از کار ما هم به رخ کشیدن کارهای انجام شده است تا شهروندان از امکانات تحقق یافته مطلع شوند.

■ پرسش: در تعریف شاخص‌ها چقدر از تجارب سایر کشورها و نهادهای استانداردگذار استفاده کرده‌اید و در چه زمینه فکر می‌کنید در یکسان‌سازی شاخص‌ها موفق‌تر بوده‌اید؟

درزمینه استفاده از تجارب سایر کشورها حتی قبل از احداث رصدخانه برنامه‌ریزی‌هایی صورت گرفته است. اما هم‌اکنون این ارتباطات به سمت همکاری پیش رفته است. اما واقعیت آن است که به علت تفاوت در ماهیت فعالیت‌ها لازم است تجارب آن‌ها حتما بومی شده و مورد استفاده قرار گیرد. در برخی از کشورها موضوع اصلی رصدخانه تجمیع و یکپارچگی اطلاعات است که در کار ما بخش اعظم آن به عهده سازمان فناوری اطلاعات شهرداری است. در برخی دیگر لزوم به ارایه با این ابعاد و به شکل زنده وجود ندارد و حتی در برخی از کشورها رصدخانه‌های شهری صرفاً یک سازمان مجازی است که گزارش‌هایشان را صرفاً از طریق درگاه شهری منتشر می‌کنند. اما ما در رصدخانه بر اساس نیازهای محلی نیاز به یک مکان زنده ارایه داشتیم.

کلام آخر: هیچ دیکته نانوشته‌ای غلط ندارد، ایجاد رصدخانه هم برای اولین بار در ایران اتفاق افتاده، با وجود استقبال مخاطبان، قطعاً اشکالاتی در کار ما وجود دارد مخصوصاً در حوزه ایجاد پایگاه اطلاعات شهر تهران که با تعامل با سایر نهادهای شهری حل خواهد شد. اما در بحث رصدخانه‌های شهری آن‌چه همیشه نگرانی بنده و دغدغه شخصی من است، اهمیت دادن به بخش نمایشی و خرید تجهیزات با کیفیت بالا و غافل شدن از بحث صحت اطلاعات، تعریف شاخص‌های استاندارد و جمع‌آوری اطلاعات یکپارچه مکان محور است. یادمان باشد که ما با رصدخانه‌های شهری هدفمان به رخ کشیدن اطلاعات و بزرگ‌نمایی مشکلات است، نه به رخ کشیدن خودمان و ارایه دستاوردهایمان و محو کردن شکایات. در اقداماتی که در سطح کشور بر اساس الگو رصدخانه شهری تهران در سایر شهرها در حال انجام است نگرانی عدم وجود محتوی و اطلاعات مناسب برای نمایش وجود دارد و بیم این که در صورت نبود اطلاعات سازمان‌ها به ساخت و جعل اطلاعات روی بیاورند. خوشبختانه ما این مشکل را در تهران اصلاً نداشتیم زیرا متولی اطلاعات حوزه شهرداری، سازمان فناوری اطلاعات شهرداری است که بر اساس پایش‌های دوره‌ای، مجموعه غنی از اطلاعات را در اختیار دارد و ما در گام نخست ارایه همان اطلاعات را برعهده گرفتیم. در برخی از کشورهای دنیا متولی رصدخانه نهادهای مرم‌نهاد هستند تا سازمان‌های مخاطب به علت منافع خود نتوانند دخل و تصرفی در اطلاعات داشته باشند.

هم اکنون تمام اطلاعات نمایش داده شده در رصدخانه مستقیماً از پایگاه‌های اطلاعات شهری که نتایج جمع‌آوری اطلاعات به روش نمونه‌برداری از سراهای محله تحت عنوان «طرح سنجش عدالت» بوده است استخراج می‌شود. نمایندگان پژوهشگران محله که در این طرح شرکت داشتند منطقه به منطقه به رصدخانه آمده‌اند تا نتایج خروجی کارشان را از نزدیک مشاهده کنند. این طرح که بر اساس طرح Urban HEART سازمان جهانی بهداشت که مخفف Urban Health Equity Assessment and Response Tool است، در کل کشورهای در حال توسعه انجام در تهران در دو نوبت در سال‌های ۸۷ و ۹۰ انجام شد. اجرای این طرح باعث ایجاد ذهنیت بسیار خوبی در مورد شهر تهران در سازمان جهانی بهداشت شد. نکته کلیدی طرح این بود که پس از سنجش اطلاعات، نتایج در اختیار سراهای محله قرار گرفت تا بسته به معضلات شناسایی شده در محله خود مداخله کنند مثلاً برای محله یوسف آباد یک کیف که حاوی کتابچه‌های مختلف اطلاعاتی بود تهیه شد. هر کتابچه مربوط به یک موضوع بود در این کتابچه‌ها هشدارهای لازم به سایر نهادها مثلاً خانه‌های بهداشت داده شد تا با مداخله در موضوعات مختلف وضعیت سلامت سرای محله خود را بهبود دهند. امسال هم قرار است با ۹۵۰/۰۰۰ نمونه این طرح دوباره انجام شود.

ممیزی فناوری اطلاعات با استفاده ازچارچوب COBIT5

الهه نجفی
شرکت مهندسی پدیدپرداز، کمیسیون استاندارد و تدوین مقررات سازمان نظام صنفی رایانه‌ای استان تهران
پست الکترونیکی: elahe.najafi@pdpsoft.com

۱- مقدمه

با آن‌که بحث ممیزی فناوری اطلاعات یا IT Audit که برخی ترجمه فارسی حسابرسی فناوری اطلاعات را برای آن برگزیده‌اند از حوزه حسابرسی‌های مالی و با نگرش بازخواست و رسیدگی متولد شد اما این واژه در طول عمر حدود ۱۴ ساله خود یک تکامل مفهومی داشته است که به نظر هنوز هم فرآیند بلوغ آن ادامه دارد. در سال ۲۰۱۳ ایساکا مستندی با عنوان COBIT5 for assurance را منتشر کرد که در این مستند فرایند تضمین فناوری اطلاعات بر اساس مفاهیم چارچوب COBIT 5 و توانمندسازهای تعریف شده در این چارچوب تشریح شد. پس از ان ایساکا مستندات جداگانه‌ای برای ممیزی و تضمین هر یک از فرایندهای تعریف شده در COBIT5 منتشر کرد. آنچه در این مستندات حائز اهمیت است استفاده از دو واژه ممیزی و تضمین در بسیاری از موارد به صورت یک زوج کلمه ممیزی/تضمین و در برخی موارد به جای یکدیگر است.

ممیزی و تضمین را شاید بتوان دو روی یک سکه دانست. در واقع با ممیزی ارایه خدمات و محصولات منطبق با تجربیات برتر و استانداردها، با کیفیت توافق شده و در چارچوب قوانین، مقررات و الزامات بالادستی تضمین می‌شود. تضمین با پایش و سنجش نحوه اجرای تعهدات در سازمان ارایه کننده خدمات و محصولات به مخاطبین این اطمینان را می‌دهد که ارایه‌کنندگان نسبت به وظایف خود به ایشان متعهد و پاسخگو هستند.

این مستند به بیان مدل عمومی فرآیند تضمین/ممیزی فناوری اطلاعات بر اساس چارچوب COBIT5 اختصاص دارد. در ادامه در بخش ۲ به مزایای استفاده از چارچوب COBIT5 برای ممیزی فناوری اطلاعات می‌پردازیم. بخش سه به بیان مولفه‌های ممیزی از نگاه ایساکا اختصاص دارد. فرآیند ممیزی/تضمین فناوری اطلاعات موضوع بخش چهار است و در نهایت مراجع در بخش ۵ ارایه شده است.

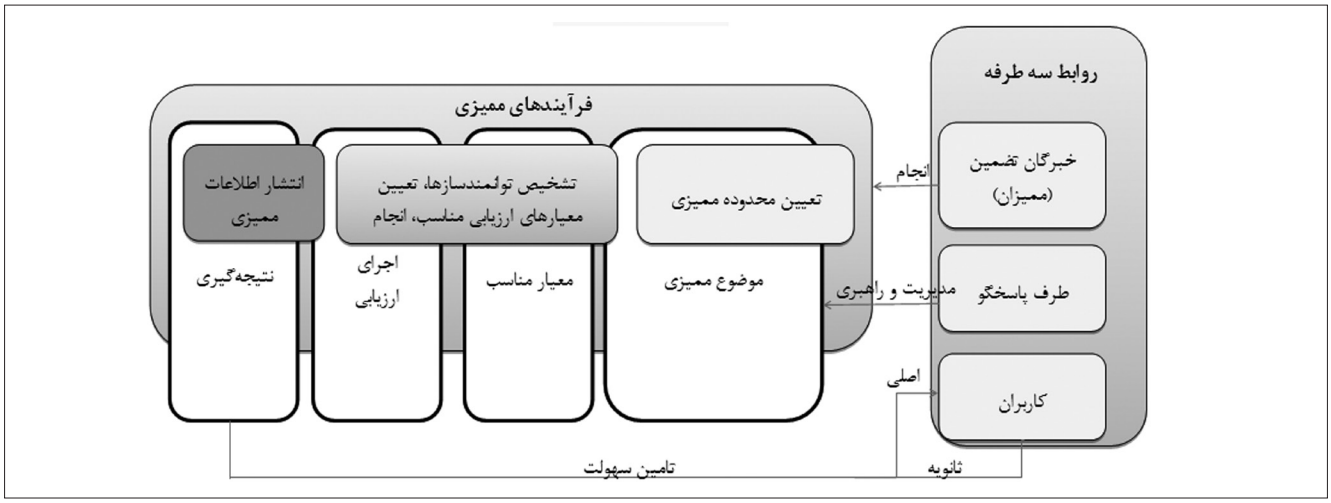
۲- مزایای استفاده از COBIT5 به منظور چارچوبی برای ممیزی/تضمین

تاکنون چارچوب‌های و استانداردهای متعددی به منظور ممیزی فناوری اطلاعات مانندITAF [۱] ارایه و مورد استفاده قرار گرفته است. آنچه به عنوان مزایای COBIT5 به عنوان چارچوب پایه ممیزی فناوری اطلاعات می‌توان برشمرد موارد ذیل است[۲]:

۱) در COBIT 5 بر اساس یک رویکرد کل‌نگر ۷ توانمندساز برای سازمان‌ها تعریف و ارایه شده است، که این توانمندسازها تمامی دارایی‌های سازمانی مرتبط با ممیزی فناوری اطلاعات را شامل می‌شوند، لذا استفاده از این چارچوب باعث شده که کلیه توانمندسازها، نقش و تاثیر آن‌ها در فرآیند ممیزی تعریف و مشخص شود. و ممیزی فناوری اطلاعات تنها معطوف به فرآیندها یا سیستم‌های اطلاعاتی نشود.

۲) یکی از مزایای استفاده از پیروی از این چارچوب به‌منظور تعیین اهداف ممیزی، استفاده از مدل آبشار اهداف است. بر این اساس اهداف ممیزی بر اساس اهداف سازمانی، اهداف فناوری اطلاعات و توانمندسازها تعریف شده و همچنین ارتباط بین اهداف و مخاطرات سازمانی برقرار می‌شود این ارتباط در انتهای ممیزی امکان شناسایی و ردیابی اهداف متاثر از مشکلات یافت شده را مشخص می‌کند.

۳) استفاده از چارچوب COBIT5 تحقق «کامل بودن فرآیند ممیزی» در حین« انعطاف‌پذیری» آن‌را باعث می‌شود. کامل بودن از آن جهت



شکل ۱: مولفه‌های ممیزی/تضمین فناوری اطلاعات[۲]

کــه کلیه توانمندســازها همانطور که در مورد یک عنوان شــد مد نظر قــرار می‌گیرند و مــوردی از قلم نمی افتد و انعطاف پذیری از آن جهت که محــدوده ممیزی که در مرحله نخســت فرایند ممیزی مشــخص می‌شود تعیین کننده سطح جزییات و موضوعات ممیزی مرتبط است. بدین معنا که لازم نیســت حتما فرایند ممیزی با محدوده کل سازمان و کل توانمندســازها آغاز شــود بلکه بر اســاس تصمیم اتخاذ شده در مرحله اول فرایند ممیزی محدوده توانمندســازها و نوع مواردی که در محدوده ممیزی وجود دارد مشــخص می‌شــود اما لحاظ نشدن برخی توانمندســازها در محدوده ممیزی بر اساس یک طرح مشخص و نه به علت از قلم افتادن موضوعات ممیزی و عدم وجود نگاه جامع و یکپارچه به ممیزی اتفاق می‌افتد.

۴) ایســاکا پــس از ارایه مســتندات مربــوط به توصیــف فرآیندهای COBIT5 [۳]و پیاده‌ســازی آن [۴]، مراحــل ممیزی هــر فرآیند را بر اســاس مدل عمومی که در ادامه به آن می‌پردازیم به صورت مستندات جداگانه ارایه کرده اســت [۵-۲۷]. در این مســتندات با شرح جزییات کلیه فعالیت‌ها , وظایف مربوط به ممیزی هر فرآیند COBIT5 مشخص و توصیف شده است.

۳- مولفه‌های ممیزی فناوری اطلاعات

ممیزی شــامل ۶ مولفــه اصلی روابط ســه طرفه[۱]، موضــوع ممیزی[۲]، معیارهای مناسب[۳]، اجرای ممیزی، نتیجه‌گیری و فرآیند ممیزی است. نحوه ارتباط این مولفه‌ها با یکدیگر و با مراحل فرآیند ممیزی در شکل شماره ۱ مشخص شده است[۲].

۳-۱- موضوع ممیزی

اطلاعات مشخص، تجارب و کنترل‌هایی است که موضوع فرآیند ممیزی و تضمیــن بازبینی‌ها، ســنجش و گزارش‌دهی اســت. موضوع ممیزی می‌تواند شــامل طراحی یا عملیاتی‌ســازی تجــارب فرآیندی و تجارب مدیریتی بر روی هر جنبه ســازمانی یا مطابقت با استانداردها، قوانین و مقررات خاص باشد

لازم به‌ذکر است در COBIT5 واژه «تجارب فرآیندی» جایگزین «اهداف کنترلی» و واژه «فعالیت‌های فرآیندی» جایگزین «فعالیت‌های کنترلی» و کنترل‌ها شده است[۲].

۳-۲- معیارهای مناسب

معیارهای ممیزی، استانداردها و محک‌هایی هستند که برای سنجش و ارزیابی موضوعات ممیزی مورد استفاده قرار می‌گیرند. این معیارها لازم است هدفمند[۴]، قابل ارزیابی[۵]، قابل فهم[۶]، کامل[۷] و مرتبط[۸] باشند[۲].

هدفمند: به‌دور از تعصب قابل تعریف و اتخاذ باشند.

قابــل اندازه‌گیــری: بتوان بر اســاس روش‌های کمّی یا کیفــی آن‌ها را سنجش نمود.

قابل فهم: به صورت شــفاف تعریف شــده، و توسط مخاطبین مختلف تفسیر آن‌ها خالی از ابهام باشد.

کامل: تمام مواردی که ممکن اســت نادیده‌گرفتن آن‌ها در معیارهای ســنجش، نتیجه‌گیری درباره موضوع ممیزی را تحت تاثیر قرار دهد و باعث عدم صحت نتیجه نهایی شود باید مد نظر قرار گیرند

مرتبط: تمام معیارها به موضوع ممیزی مرتبط باشند.

پــس از تعیین معیارهــای ممیزی، خبرگان تضمین (ممیــزان) باید از پوشــش کامل محدوده ممیزی توســط معیارهای تعریف شده مطمئن شوند.

۳-۳- روابط سه طرفه

این روابط نحــوه ارتباط کلیه نقش‌های درگیر در فرآیند ممیزی را مشــخص می‌کند. قبل از توصیف سه طرف شرکت‌کننده در فرایند

1-Three-partyRelationship
2-Subject Matter
3-Suitable Criteria
4-Objectivity
5-Measurability
6-Understandability
7-Completeness
8-Relevance

ممیزی ابتدا به توصیف نقش‌ها بر اساس COBIT5 می‌پردازیم.
در تحقق اهداف فناوری اطلاعات سازمان، فرآیندهای مختلفی تعریف و اجرا می‌شود و افراد متفاوتی در هر فرآیند درگیر بوده مسئولیت‌های متفاوتی را برعهده دارند. این مسئولیت‌ها در COBIT5 براساس نمودار[۹] RACI تعریف شده، شامل چهار نقش مسئول[۱۰]، پاسخگو[۱۱]، مشاور[۱۲] و مطلع شونده[۱۳]است.
مسئول: به فردی اطلاق می‌شود که وظیفه انجام فعالیت را به‌عهده داشته و بیشترین سهم را در اجرای ان دارد.
پاسخگو: در زمینه هر فرآیند یا هر دارایی فناوری و یا به اصطلاح عامتر هر موضوع فناوری، تنها یک فرد یا یک کمیته پاسخگو باشد. پاسخگو بودن به معنای آن است که مسئولیت نهایی انجام درست کارها مطابق با تعریف اولیه بر عهده آن فرد یا کمیته است. و در نهایت اوست که در زمینه موضوع ممیزی در صورت انجام نادرست بازخواست خواهد شد.
مطلع شونده[۱۴]: به افرادی اطلاق می‌شود که اطلاعات را دریافت می‌کنند ولازم است پیشرفت فعالیت‌ها به ان‌ها اطلاع داده شود. افراد پاسخگو نیز لازم است به منظور پایش وضعیت فعالیت‌ها و مواردی که نسبت به آن پاسخگو است در جریان اطلاعات و روند پیشرفت فعالیت‌ها قرار گیرد.
مشاور: به افرادی گفته می‌شود که اطلاعات ورودی را فراهم می‌کنند. اتخاذ اطلاعات مورد نیاز هر فعالیت از افراد مختلف وظیفه افراد مسئول و پاسخگو است و ممکن است این اطلاعات از افراد مختلف حتی اعضای کمیته راهبری، مدیرعامل و ... اتخاذ شود. اما مشاور فردی است که اطلاعات کلیدی نسبت به فرآیند در اختیار دارد.
در این فرآیند سه نقش اصلی وجود دارد خبرگان تضمین(ممیزان)، طرف پاسخگو و کاربران[۲].
پاسخگو: در فرآیند ممیزی، یک از سه طرف مشارکت کننده در فرآیند ممیزی، فرد پاسخگو در زمینه موضوع ممیزی است. پاسخگو فردی است که در زمینه موضوع ممیزی، محدوده و یا فرآیند ممیزی پاسخگو است. فرآیند ممیزی بر اساس تعهد پاسخگو به کاربر شرکت می‌گیرد و در واقع تضمین کننده این موضوع است که فرد یا کمیته پاسخگو به تعهدات خود به کاربر عمل کرده است. معمولا نقش پاسخگو بر عهده مدیران است.
کاربر: کاربران ممیزی بسته به موضوع ممیزی طیف وسیعی از ذی‌نفعان مختلف شامل سهامداران، مشتریان، اعضای هیات مدیره، اعضای کمیته ممیزی، قانون گذاران و تنظیم کنندگان مقررات را دربرمی‌گیرند.
خبرگان ضمانت (ممیزان) افرادی هستند که مسئولیت کارایی ممیزی و تضمین انتشار گزارش‌های مرتبط بر روی موضوعات ممیزی را بر عهده دارند. در انجام فرآیند ممیزی/تضمین وظیفه ممیز اطمینان از عملکرد ممیز شونده در قبال مسئولیت‌هایی است که در قبال کاربران دارد. شاید این جمله در ابتدا واضح به نظر برسد که ممیزی تضمین آن است که مسئولین در قبال موضوعات ممیزی و تعهدات خود به کاربران پاسخگو هستند. اما اهمیت این جمله وقتی مشخص می‌شود که در برخی از مواقع در سازمان‌ها، ممیزی بر اساس موضوعات ممیزی انجام می‌شود که پاسخگو مشخصی برای ان در نظر گرفته نشده است. در واقع پیش‌نیاز فرآیند ممیزی تعریف نقش پاسخگو برای هر یک از موضوعات ممیزی اعم از فرآیندها، فعالیت‌ها، سیستم‌های اطلاعاتی و غیره است.

۳-۴- اجرای ارزیابی

فرآیند ممیزی شامل ارزیابی موضوعات ممیزی بر اساس شاخص‌های استخراج شده از معیارهای ممیزی است. ارزیابی، اجرای کلیه فعالیت‌ها و وظایف مربوط به سنجش تا حصول نتیجه را شامل می‌شود[۲].

۳-۵- نتیجه‌گیری

فرآیند تحلیل نتایج ممیزی یا تضمین پس از تایید نتایج ارزیابی تا دستیابی به نتایج و توصیه‌ها فرآیندی پیچیده است. آنچه این فرآیند را پیچیده می‌کند شناسایی مشکلات اصلی و ریشه بروز آن‌ها بر اساس یافته‌های ممیزی است. لازم به‌ذکر است آنچه در نگاه اول بر اساس یافته‌های ممیزی به عنوان فهرست مشکلات استخراج می‌شود ممکن است مشکل واقعی نبوده بلکه اثرات یک مشکل باشد. ریشه‌یابی مشکلات استخراج شده از فعالیت‌های پیچیده ولی بسیار با اهمیت و تاثیرگذار است. در این راستا لازم است فرآیند نتیجه‌گیری از تایید یافته‌های ممیزی با اشخاص کلیدی در حوزه ممیزی تا تشخیص علل بروز مشکلات توسط ممیزان پیگیری شود. در نهایت یافته‌های ممیزی به عنوان موارد ذیل در زمینه نتیجه حاصل از تحلیل ارایه می‌شوند:

- توسعه سناریوهای مختلف که منجر به توصیه‌ها در زمینه اقدامات اصلاحی شود.
- انتخاب توصیه مناسب که قابل دستیابی و قابل اجرا باشد.
- تشخیص مراحلی که لازم است به منظور رضایت ذی‌نفعان طی شود.

ممیزان باید به فهم مناسب از موضوعات ممیزی و محیط کسب‌وکار دست یابند. لازم است آن‌ها تصاویر بزرگتر را ببینند، تاثیرات ناشی از یافته‌های ممیزی را با اهداف سازمان مرتبط ساخته جنبه‌های پنهان آن را کشف و آشکار نمایند. مدیران عامل علاقمند به دانستن جزییات مشاهده‌ها نیستند بلکه آنچه آن‌ها نیاز دارند عصاره یافته‌ها و بینشی است که از تحلیل آن‌ها به‌دست می‌آید[۲].

۳-۶- ذینفعان

ذی‌نفعان ممیزی طیف وسیعی از مخاطبان داخلی و خارجی را تشکیل می‌دهند. ذی‌نفعان داخلی را می‌توان در پنج گروه ذیل دسته‌بندی کرد.

- اعضای هیئت مدیره
- کمیته ممیزی،
- گروه‌ها/بخش‌های مدیریت ریسک، ممیزی و تطابق پذیری

۹- نموداری است که مسئولیت‌های مختلف مربوط به فعالیت‌ها را مشخص می‌کنند. کلمه RACI سرنامی برای چهار کلمه Responsible، Consultant،Accountable و Informed است.

10-Responsible
11-Accountable
12- Consultant
13-Informed

۱۴- با وجود اینکه ترجمه متعارف Informed واژه مطلع است، اما به نظر نگارنده واژه مطلع شونده مفهوم Informed را در چارت RACI بهتر منتقل می‌کند.

- مدیریت عامل
- مدیران کسب‌وکار

ذی‌نفعان خارجی در واقع افراد یا گروه‌هایی هستند که نسبت به نتایج فرآیند ممیزی علاقه داشته و یا در انجام آن مسئولیتی متوجه آن‌هاست این نوع ذی‌نفعان شامل موارد زیر است:

- سرمایه‌گذاران و سهامداران
- ممیزان خارجی
- قانونون گذاران و وضع‌کنندگان مقررات
- شرکای تجاری
- مشتریان و کاربران

نیازمندی‌های هریک از این ذی‌نفعان از فرآیند ممیزی و تضمین یکسان نیست. به همین دلیل است که باید بین انواع مختلف ممیزی تفاوت قائل شد[۲].

۳-۷- انواع ممیزی

انواع ممیزی را می‌توان در سه گروه اصلی خود ارزیابی[15]، ممیزی داخلی[16] و ممیزی خارجی[17] دسته‌بندی نمود[۲].

خود ارزیابی: در این حالت ممیزی توسط واحد کسب‌وکاری که مالک توانمندسازهاست هدایت می‌شود. مراحل این فرآیند همان مراحل عمومی فرآیند ممیزی است که در بخش ۴ ارایه خواهد شد. تنها تفاوت در آن است که در بحث ارزیابی لازم است با ارایه راهنماهایی برای ارزیابان، نحوه انجام سنجش به صورت شفاف مشخص شود، در این زمینه لازم است با استفاده از ابزارها و استانداردهای داخلی راه و روش ممیزان برای ارزیابی، هدایت و اعتبارسنجی شود. همچنین پس از مشخص شدن نتایج ارزیابی، پیگیری[18] انجام اقدامات اصلاحی در زمینه رفع نقاط ضعف اعلام شده تا حصول نتیجه‌نهایی در دستورکار قرار گیرد تا ارزش افزوده‌ای، از ممیزی برای سازمان حاصل شود. در این نوع از ممیزی نیازی به استقلال ممیزان وجود ندارد تنها لازم است مسئولیت‌ها و نحوه انجام فرآیند ممیزی و پیگیری آن به‌درستی طراحی و استقرار یابد.

ممیزی داخلی/ بازبینی تطابق‌ها:

در این حالت ممیزی توسط شخص ثالثی انجام می‌شود. این شخص دخالتی در عملکرد توانمندسازها نداشته، اما توسط مالک توانمندسازها برای ممیزی استخدام شده است. در سازمان‌های متوسط و بزرگ معیارهای ارزیابی توسط ممیزان داخلی تعریف و بازبینی می‌شوند. در این نوع ممیزی استقلال بیشتری نسبت به نوع «خود ارزیابی» وجود دارد. تدوین تجارب موفق و راهنماهای سازگار لازمه بهینه‌سازی ارزش افزوده از این نوع ممیزی است.

ممیزی خارجی:

این نوع از ممیزی بسیار شبیه ممیزی داخلی است با این تفاوت که تیم ممیزی توسط مالکین کسب‌وکار به کار گماشته نشده و خارج ازمحدوده سازمان متقاضی هستند. در این حالت این ممیزان استقلال بیشتری داشته و فرآیند ممیزی توسط ذی‌نفعان خارجی هدف‌گذاری می‌شوند. قالب گزارش‌ها و نیازمندی‌ها تا حد زیادی استاندارد شده و لازم است نتایج بر اساس قالب استاندارد ارایه شود.

۴- فرآیند تضمین/ممیزی

مراحل فرآیند تضمین مطابق شکل شماره ۲ شامل سه مرحله اصلی ۱) تعیین محدوده آغازین ممیزی، ۲) تشخیص توانمندسازها، تعیین معیارهای ارزیابی مناسب، انجام ارزیابی و ۳) انتشار اطلاعات ممیزی است[۲].

۴-۱- تعیین محدوده آغازین ممیزی/تضمین

فعالیت‌های اصلی این مرحله شامل تعیین ذی‌نفعان و سهم آن‌ها در فرایند ممیزی، تبیین اهداف ممیزی و تعیین توانمندسازهاست.

۴-۱-۱- تعیین ذی‌نفعان

در این فعالیت ذی‌نفعان مختلف شامل مخاطبین و استفاده‌کنندگان گزارش تضمین، مشارکت‌کنندگان در فرآیند تضمین و افراد پاسخگو و مسئول در مورد موضوعات ممیزی مشخص شده و سهم هریک در فرآیند ممیزی مشخص می‌شود.

۴-۲-۲- تعیین اهداف ممیزی

در تعریف اهداف ممیزی می‌توان از ساختار آبشار اهداف COBIT5 کمک گرفت. بر اساس این ساختار اهداف ممیزی در ابتدا بر اساس یک توصیف ساده بیان می‌شوند اما این توصیف ساده باید به مجموعه‌ای از اهداف کمّی قابل اندازه‌گیری و قابل مدیریت منتهی شود تا هم بتوان فرآیند ممیزی را بر اساس آن طراحی و اجرا نمود و هم نحوه حصول اهداف کلان قابل ردیابی و مدیریت باشد.

آبشار اهداف همانطور که در شکل شماره ۳ مشخص است با ایجاد یک ساختار سلسله مراتبی از اهداف قابلیت ردیابی آن‌ها را آسان می‌سازد استفاده از این نقشه اجازه تعیین اولویت‌های پیاده‌سازی، بهبود و تضمین را بر اساس اهداف ممیزی و مخاطرات سازمانی فراهم می‌کند[۳].

COBIT5 اهداف را در سطوح سازمانی، فناوری اطلاعات و در نهایت اهداف هر یک از توانمندسازها تعریف کرده و بر اساس ارایه جداول نگاشتی ارتباط آن‌ها را مشخص می‌کند. هر چند اهداف نهایی ممیزی سازمان بر اساس کسب‌وکار، راهبردها و فرهنگ هر سازمانی تعریف و نهایی می‌شود اما مطالعه این جداول نگاشت به عنوان راهنما در ایجاد یک نگاه کل نگر و کم‌رنگ شدن احتمال جا افتادن موارد با اهمیت بسیار کمک کننده است.

با وجود آن‌که یکی از منابع تعریف اهداف ممیزی آبشار اهداف است اما توجه به این مطلب حائز اهمیت است که اهداف سازمان و اهداف فناوری اطلاعات تنها منبع تعریف اهداف ممیزی نیستند.

15-Self-Assessment
16-Internal audit/compliance review
17-External Audit
18-Follow-up

شکل ۲: فرآیند ممیزی فناوری اطلاعات[۲]

اهداف ممیزی بر پایه اهداف سازمانی و فناوری اطلاعات هر سازمان، ارزیابی محیط داخل و خارج هر کسب‌وکار و فرصت‌های پیش‌رو که در اهداف سازمانی تحقق نیافته است و مخاطراتی که تهدیدکننده اهداف کسب‌وکاری است تدوین می‌شوند. یکی از منابع تعیین کننده اهداف ممیزی، مخاطرات و چالش‌هایی است که تهدید کننده اهداف سازمانی است، با ممیزی این فرصت فراهم می‌شود که این مخاطرات تحت کنترل قرار گیرد. بنابراین برای تعیین اهداف ممیزی لازم است راهبردها، اولویت‌ها، محیط داخلی و زمینه‌های کسب‌وکار خارجی مدنظر قرار گیرد. اهداف ممیزی اهداف قابل سنجشی هستند که از فرصت‌ها، مخاطرات، سلسله مراتب اهداف سازمانی (اهداف کلان راهبردی، اهداف کیفی، اهداف فناوری) تعیین می‌شوند.

۴-۱-۳- تعیین توانمندسازهای مرتبط

در این مرحله توانمندسازها که در محدوده تعریف شده ممیزی قراردارند مشخص شده و سطح جزئیاتی که در مورد هریک باید مد نظر قرارگیرد تعیین می‌شود. به‌طور کلی توانمندسازها، فاکتورهایی هستند که بر کارکرد راهبری و مدیریت سازمان تاثیر می‌گذارند. پیشران این هفت گروه توانمند ساز، آبشار اهداف است. این هفت توانمندساز کلیه دارایی‌های سازمانی که نیازمند مدیریت و راهبری هستند را در برمی‌گیرند. این توانمندسازها بر اساس COBIT5 مطابق شکل شماره ۴ شامل هفت گروه ذیل می‌باشند[۳].

اصول، خط مشی‌ها و چارچوب‌ها: راهنماهای عملی حاوی دستورالعمل، آیین‌نامه‌ها، مستندات تشریح کننده نحوه انجام و اصول فعالیت‌های گام به گام روزانه

فرآیندها: مجموعه سازمان‌دهی شده از تجارب و فعالیت‌ها به منظور دستیابی به اهداف واقعی و تولید مجموعه‌ای از خروجی‌ها به منظور دستیابی به اهداف سازمان

ساختار سازمانی: ساختاری که نحوه ارتباط نقش‌ها، مسئولیت‌ها و پست‌های سازمانی را مشخص می‌کند. مولفه‌های این ساختار در تحقق فعالیت‌ها و تجارب فرآیندی نقش‌های مختلفی ایفا می‌کنند.

فرهنگ، اخلاق، رفتار :عادات، منش‌ها و فضای رفتاری سازمان که نقش کلیدی در پیشبرد اهداف داشته و معمولا بدون پیروی از یک سازوکار زمینه سینه به سینه منتقل می‌شود.

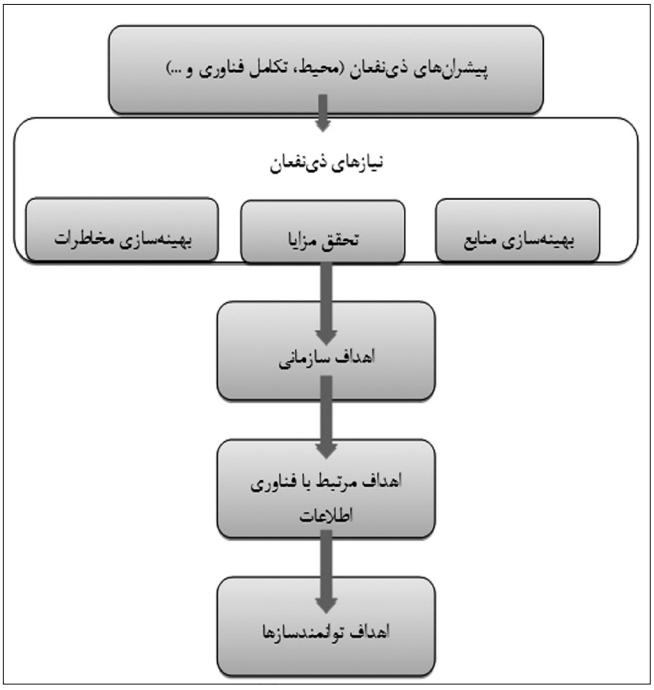
اطلاعات: در برگیرنده کلیه داده‌ها و اطلاعات تولید شده در هر یک از فعالیت‌ها و یا وظایف سازمانی بوده به عنوان یک دارایی کلیدی سازمان راهبری و هدایت سازمان را ممکن می‌سازد.

خدمت، زیرساخت و برنامه‌های کاربردی: محصولات، خدمات و امکانات فناوری اطلاعات که که بستر فناوری اطلاعات لازم به منظور استقرار و نهادینه سازی فرآیندهای سازمانی و تحقق اهداف را ایجاد می‌کنند.

افراد. مهارت‌ها و شایستگی‌ها: نیروی انسانی مورد نیاز به‌منظور انجام موفق فعالیت‌ها، اتخاذ تصمیمات مناسب و اجرای اقدامات اصلاحی.

حسن مدل توصیه شده COBIT 5 تضمین توجه متعادل به تمامی توانمندسازهای سازمانی است، که در مستندات مربوط به توصیف چارچوب COBIT 5 از آن به عنوان «تحقق رویکرد جامع سازمانی» نام‌برده می‌شود. هر چند توانمندسازها با یکدیگر ارتباطات تنگاتنگ داشته و با تمرکز بر یکی سایر جنبه‌ها نیز شناسایی و مورد توجه قرار می‌گیرند اما توجه اختصاصی به هر یک مخاطره از قلم افتادن موضوعات کلیدی در فرایند ممیزی را از بین می‌برد.

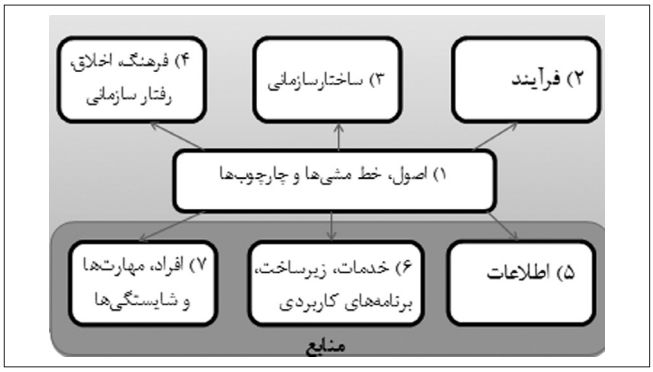
شکل شماره ۴علاوه بر ارایه فهرست توانمندسازهای سازمان، الگوی



شکل ۳: آبشار اهداف[۳]

فکری سیستماتیک را به منظور دستیابی به اهداف کلیدی سازمان مشخص می‌کند. این الگو در ابتدا بر توجه متعادل بر کلیه توانمندسازها تمرکز داشته و سپس مشخص می‌سازد توانمندسازها با یکدیگر ارتباطات تنگاتنگ داشته و با تمرکز بر یکی سایر جنبه‌ها نیز شناسایی و مورد توجه قرار می‌گیرند.

به عنوان مثال اگر هدف سازمانی ارایه خدمات بهتر به کاربران باشد. تمرکز در ابتدا بر خدمات فناوری اطلاعات مورد نیاز کاربران است و به دنبال آن بستر زیرساختی و برنامه‌ها یا مولفه‌های کاربردی که توسعه و استقرار آن‌ها در نهایت منجر به ارایه خدمات مذکور می‌باشد مورد توجه قرار می‌گیرد. توسعه، عملیاتی سازی ونگهداشت این مولفه‌های فناوری نیاز به ساختار سازمانی و تعیین سلسله مراتب پاسخگویی و گزارش‌دهی دارد این ساختار تشکیل شده از افرادی است که بر حسب پست سازمانی اتخاذ کرده مهارت‌ها و شایستگی‌های متفاوتی دارند. و در نهایت آنچه که نادیده گرفتنش قطعا تحقق هدف اولیه ارایه خدمات بهتر به کاربران را با چالش جدی مواجه می‌کند فرآیندهای سازمانی است که در حوزه‌های مختلف از تولید سیستم‌اطلاعاتی تا عملیاتی کردن خدمات و سایر موارد را در بر می‌گیرد. فرآیندهای مجموعه‌ای از فعالیت‌ها و وظایفی بوده که توسط افراد سازمان انجام می‌گیرند به‌علاوه اطلاعاتی را به عنوان ورودی دریافت و به عنوان خروجی ایجاد می‌کنند که یکپارچگی و تجمیع آن دانش سازمانی مورد نیاز اتخاذ تصمیمات صحیح را فراهم می‌کند. از سوی دیگر انجام این فعالیت‌ها در خلأ صورت نگرفته و اصول ارزشی سازمان، فرهنگ و اخلاق سازمان در نحوه انجام آن تاثیرگذار بوده و تدوین دستورالعمل‌های سازمانی و ارایه آیین‌نامه‌های گام به گام پیشبرد این فعالیت‌ها را ممکن می‌سازد. اتخاذ تصمیمات درست سازمانی بدون به‌کارگیری این الگوی



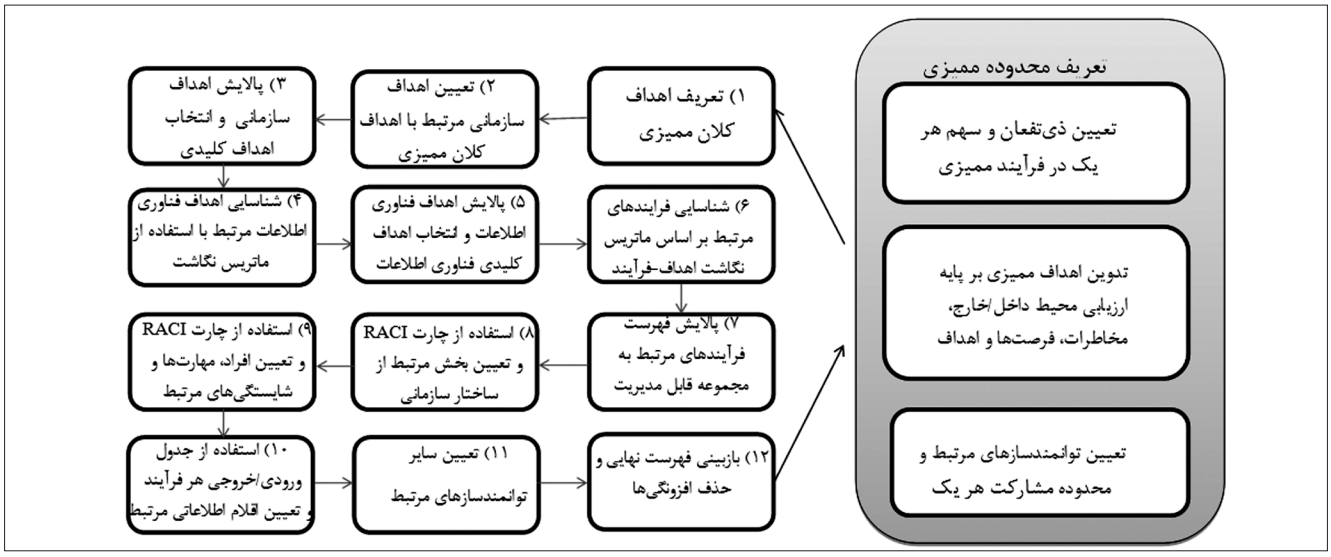
شکل ۴: توانمندسازها در چارچوب COBIT5 **[۳]**

سیستماتیک غیرقابل انجام است. لذا در تعامل با ذی‌نفعان لازم است توانمندسازهای مرتبط مورد تحلیل و بررسی قرار گرفته و حد پرداختن به هر یک مشخص شود.

پس از تعیین فهرست کلیه توانمندسازها لازم است افزونگی‌های احتمالی حذف شود. از آنجا که در مدل ممیزی فناوری اطلاعات بر اساس COBIT5 معیارها برای توانمندسازها تعریف شده و با توجه به ارتباط توانمندسازها، احتمال وقوع افزونگی در اطلاعات وجود دارد. به عنوان مثال ممکن است یک قلم اطلاعاتی هم به صورت مستقل به عنوان موضوع ممیزی مد نظر قرار گیرد و هم در پالایش فرآیندها به عنوان ورودی یا خروجی یک فرآیند. یا یک نقش سازمانی هم به صورت مستقل و به عنوان بخشی از ساختار سازمانی و هم به عنوان پاسخگو نسبت به یک فعالیت در فرآیندی از سازمان. در نتیجه لازم است فهرست نهایی توانمندسازها بازبینی شده موارد افزونده از آن حذف شود. به‌طور کلی فعالیت‌های مرحله یک فرآیند ممیزی فناوری اطلاعات و تقدم و تاخر آن‌ها در شکل شماره ۵ مشخص شده است.

۴-۲- مرحله دوم: تشخیص توانمندسازها، تعیین معیارهای ارزیابی مناسب، اجرای ارزیابی

مرحله دوم از فرآیند ممیزی مربوط به تعریف معیارهای سنجش، طراحی‌شاخص‌ها و ارزیابی موضوعات ممیزی بر اساس شاخص‌های تعریف شده و توافق شده است. یک اشتباه مصطلح در زمینه ممیزی این است که شاخص‌ها و سنجه‌ها توسط ممیزان تعریف شده و توافقی در زمینه آن‌ها با افراد مشارکت‌کننده در فرآیند ممیزی و افراد مخاطب نتایج ممیزی صورت نمی‌گیرد. مخاطبین معمولا در بمباران سوالات مختلفی قرار می‌گیرند که نه فلسفه وجودی آن‌ها را می‌دانند و نه معنا و مفهوم دقیق آن‌ها را. بنابراین ممیزی بدون مشارکت فعالانه ذی‌نفعانی که مسئولیت و مالکیت موضوع ممیزی را داراهستند صورت می‌پذیرد. سردرگمی مخاطبان ممیزی در سنجش، سردرگمی آن‌ها در اجرای اقدامات اصلاحی را نیز به‌دنبال خواهد داشت. جالب توجه آن‌که در عبارت انگلیسی انجام ممیزی و یا تضمین از فعل engagement به معنای مشارکت داشتن استفاده شده و از افعالی مانند اجرا یا انجام پرهیز شده است. هر چند اجرای فرآیند ممیزی بدون توافق ذی‌نفعان بر روی موضوعات ممیزی و معیارهای سنجش هر یک ممکن است تا انتها و



شکل ۵: فعالیت‌های مرحله نخست فرآیند ممیزی فناوری اطلاعات[۲]

با موفقیت دنبال شـود ولی قطعا اثربخشی لازم را نخواهد داشت. و در مرحلـه نهایی این فرآیند که انتشـار نتایج و پیگیری ممیزی اسـت با چالش‌های جدی روبرو خواهیم شد.

در مـدل ارایه شـده ممیزی/تضمین بـر اسـاس COBIT5 معیارهای ارزیابی بر اسـاس هر یک از توانمندسـازها تعریف می‌شـود. به منظور طراحی سـنجه‌ها و انجام فرایند ارزیابی برای هر سنجه اهداف مرتبط، دستاوردهای قابل حصول و مراحل ارزیابی به طور تفصیلی تعریف شده و در زمینه آن توافقات ذی‌نفعان کسب می‌شود.

به عنوان نمونه سـنجه‌های مربوط به دو هدف «پاسخ چابک به فضای متغییر کسـب وکار» و «همسـویی راهبردهای کسـب‌وکار و فناوری اطلاعات» در جدول ۱ ارایه شده است.

انجـام فرایند ارزیابی می‌تواند به هریـک از روش‌های تحقق و تایید[19]، بازرسی[20]، مشاهده[21]، انجام یا محاسبه دوباره[22] و بازبینی مجموعه‌ای از شـواهد[23] اجرا شـود. در ادامه نمونه‌هایی از هر یک از این روش‌ها ارایه می‌شود[۲].

تحقیق و تایید

- کشف استثنائات/ انحرافات و آزمایش آن‌ها
- بررسی رویدادها و تراکنش‌های غیرمعمول
- مصاحبه با کارمندان و ارزیابی سطح دانش، آگاهی و رفتار آن‌ها
- پرسش سوالات مدیریتی و دستیابی به پاسخ‌ها به منظور تایید یافته‌ها

بازرسی

- بازبینی اهداف، سیاست‌ها و فرآیندها
- جستجو در نتایج ممیزی و سوابق مشکلات

19-Enquire and confirm
20- Inspect
21- Observe
22- Reperform and/or recalculate
23- Review automated evidence collection

- مقایسه آنچه به‌دست آمده با مقدار مورد انتظار
- برنامه‌ریزی و استقرار در حین کار

مشاهده

- مشاهده و توصیف فرآیندها
- مشاهده و توصیف افراد، مهارت‌های آن‌ها

مقایسه رفتار واقعی با رفتار مورد انتظار

- جمع‌آوری نمونه‌ها
- استخراج استثنائات و تراکنش‌های کلیدی
- استفاده از ممیزی تعبیه شده

۴-۳- مرحله سه: نتیجه‌گیری و انتشار اطلاعات ممیزی

مرحله نهایی ارایه نتایج ممیزی و مشـاهده‌ها به ذی‌نفعان اسـت. لازم به‌ذکر اسـت برخی می‌پندارند با پایان ارزیابی ممیزی، فرآیندِ ممیزی خاتمه یافته است؛ غافل از این‌که یک از مهمترین مراحل ممیزی انتشار اطلاعـات و ارایه نتایج ممیزی به صـورت کارا و اثربخش به مخاطبین اسـت. در این مرحله یکی از فعالیت‌های مهم تعریف یک نقشـه راه به منظور آغاز فرآیند اصلاح و رفع مشکلات گزارش‌شده است. فعالیت‌های این مرحله شامل دو فعالیت اصلی مستندسازی استثنائات و فاصله‌ها و ارایه کارا و اثربخش نتایج کشف‌شده است.

۴-۳-۱- مستندسازی استثنائات و فاصله‌ها:

در این فعالیت هدف آن است که در ابتدا بر اساس یافته‌ها ریشه مشکلات و علل وقوع آن‌ها شناسـایی شده و سپس یافته‌های مرتبط با هر علت ارایه شود. این فعالیت وظایف ذیل را در برمی‌گیرد

بیان تاثیر خطاهای توانمندسازها و نقاط ضعف آن‌ها با اعداد و سناریو خطاهای رخ داده، مصادیقی از استفاده نامناسب و ناکارآمدی

شفاف‌سازی نقاط آسـیب‌پذیر، تهدیدها و فرصت‌های از دست‌رفته که احتمال وقوع آن‌ها در صورت کارانبودن توانمندسازها وجود دارد.

جدول ۱: مثالی از جدول سنجه‌ها بر اساس COBIT5 [۵]

هدف سازمانی	سنجه‌ها	دستاوردهای قابل حصول	گام های ارزیابی
پاسخ چابک به فضای متغیر کسب‌وکار	سطح رضایتمندی هیئت عامل از میزان پاسخگو بودن سازمان به نیازهای جدید. تعداد محصولات کلیدی و خدمات حمایت شده توسط فرآیندهای کسب‌وکار بروز. زمان متوسط برای تبدیل اهداف راهبردی به ابتکارهای عملی توافق و تصویب شده.	توافق بر روی مقادیر مورد انتظار برای سنجه‌های تعریف شده.	سنجه‌های مرتبط با هدف بازبینی و ارزیابی شده تا مشخص شود آیا به معیارهای تعریف شده دست‌یافته‌ایم.
همسویی راهبردهای کسب‌وکار و فناوری اطلاعات	درصد اهداف و نیازمندی‌های راهبردی سازمانی که به‌وسیله اهداف راهبردی فناوری اطلاعات حمایت می‌شوند. سطح رضایتمندی ذی‌نفعان نسبت به محدوده پرتفولیو برنامه‌ها و خدمات برنامه‌ریزی شده. درصد پیشران‌های با ارزش فناوری اطلاعات که به پیشران‌های با ارزش کسب‌وکار نگاشت شده‌اند.	توافق بر روی ارزش مورد انتظار از سنجه‌های اهداف مرتبط با فناوری اطلاعات.	سنجه‌های مرتبط با هدف بازبینی و ارزیابی شده تا مشخص شود آیا به معیارهای تعریف شده دست‌یافته‌ایم.

تشخیص و مستندسازی نقاط ضعف و تاثیرات آن‌ها بر اهداف سازمانی: لازم به‌ذکر است این مورد با استفاده از آبشار اهداف و روابط سلسله مراتبی که در مرحله اول ایجاد شد امکان‌پذیر است.

۴-۳-۲- ارایه کارا و اثربخش نتایج کشف‌شده

پس از کشف ریشه مشکلات و دسته‌بندی یافته‌ها بر اساس آن‌ها لازم است که نتایج ممیزی به صورت کارا و اثربخش به مخاطبین ارایه شود. در این زمینه وجود ارتباط مستمر بین ممیزان و ذی‌نفعان بسیار حائز اهمیت است.

یافته‌های ممیزی بر حسب میزان علاقه ذی‌نفعان‌ها با جزییات متفاوت به آن‌ها ارایه می‌شود. گزارش‌های ممیزی اطلاعات خام حاصل از ارزیابی نیست بلکه ارایه تحلیل‌هایی است که بر اساس اطلاعات حاصل از ارزیابی به‌دست آمده است. نمونه‌ای از این گزارش‌ها می‌تواند موارد ذیل باشد:

- اندازه‌گیری و مستندسازی میزان دوباره‌کاری در زمینه هریک از توانمندسازها
- استفاده از روش‌های محک‌زنی و مقایسه به منظور ارایه وضعیت سازمان نسبت به دیگران
- استفاده از نمودارها و داشبوردها برای توصیف بهتر مشکلات
- ارایه نتایج حاصل از ممیزی به مسئول مربوطه به منظور اجرای اقدامات اصلاحی

در انتهای ممیزی لازم است گزارشی که حاوی فهرست اقدامات اساسی و با اولویت است منتشرشود. ساختار این گزارش باید به گونه‌ای باشد که ذی‌نفعان با علایق مختلف بتوانند از آن استفاده لازم را نموده و ارایه جزییات به صورت پراکنده و نامنظم باعث سردرگمی آن‌ها نسبت به اقدامات اصلاحی مورد نیاز نشود.

مراجع

مراجعی که در تدوین این مقاله از آن‌ها استفاده شده، به شرح زیر است:

[1] ITAF™: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition, ISACA, 2014

[2] COBIT5 for Assurance, ISACA, 2013

[3] COBIT5 A Business Framework for the Governance and Management of Enterprise IT, ISACA, 2012

[4] COBIT5 Implementation, ISACA, 2012

[5] BAI01 Manage Programs and Projects Audit/Assurance Program, ISACA, 2014

[6] BAI02 Manage Requirements Definition Audit/Assurance Program, ISACA, 2014

[7] BAI03 Manage Solutions Identification and Build Audit/Assurance Program, ISACA, 2014

[8] BAI04 Manage Availability and Capacity Audit/Assurance Program, ISACA, 2014

[9] BAI05 Manage Organizational Change Enablement Audit/Assurance Program, ISACA, 2014

[10] BAI06 Manage Changes Audit/Assurance Program BAI06 Manage Changes Audit/Assurance Program, ISACA, 2014

[11] BAI07 Manage Change Acceptance and Transitioning Audit/Assurance Program, ISACA, 2014

[12] BAI08 Manage Knowledge Audit/Assurance Program, ISACA, 2014

[13] BAI09 Manage Assets Audit/Assurance Program, ISACA, 2014

[14] BAI10 Manage Configuration Audit/Assurance Program, ISACA, 2014

[15] APO01 Manage the IT Management Framework Audit/Assurance Program, ISACA, 2014

[16] APO02 Manage Strategy Audit/Assurance Program, ISACA, 2014

[17] APO03 Manage Enterprise Architecture Audit/Assurance Program, ISACA, 2014

[18] APO04 Manage Innovation Audit/Assurance Program, ISACA, 2014

[19] APO05 Manage Portfolio Audit/Assurance Program, ISACA, 2014

[20] APO06 Manage Budget and Costs Audit/Assurance Program, ISACA, 2014

[21] APO07 Manage Human Resources Audit/Assurance Program, ISACA, 2014

[22] APO08 Manage Relationships Audit/Assurance Program, ISACA, 2014

[23] APO09 Manage Service Agreements Audit/Assurance Program, ISACA, 2014

[24] APO10 Manage Suppliers Audit/Assurance Program, ISACA, 2014

[25] APO11 Manage Quality Audit/Assurance Program, ISACA, 2014

[26] APO12 Manage Risk Audit/Assurance Program, ISACA, 2014

[27] APO13 Manage Security Audit/Assurance Program, ISACA, 2014

تبیین رویکرد ممیزی خدمات فناوری اطلاعات بر اساس بهروش ITIL: مطالعه موردی شرکت توسن

ایمان برادری
شرکت دانش‌آفرینان نیک‌اندیش (دانا)
پست الکترونیکی: imanbaradari@gmail.com

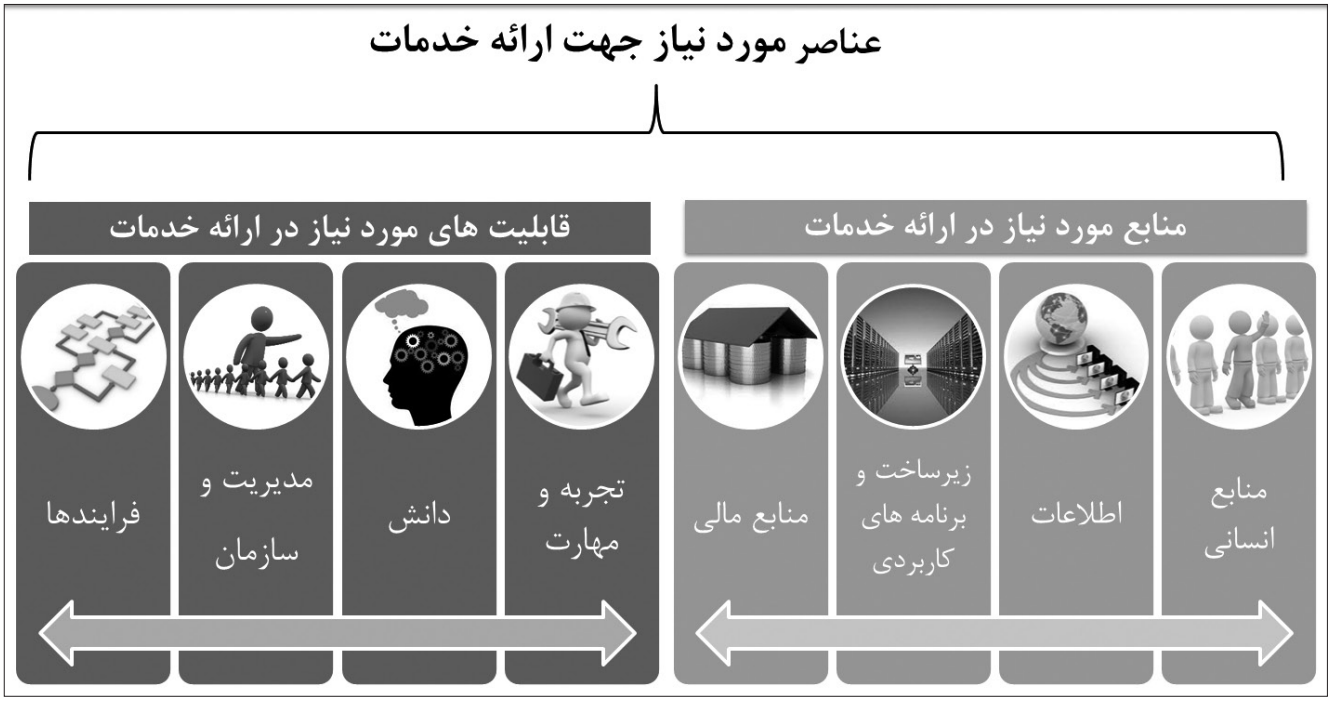
خلاصه
در این مقاله به بررسی نحوه ممیزی خدمات فناوری اطلاعات بر اساس بهروش ITIL پرداخته می‌شود. با توجه به این‌که رویکرد ITIL کاملا خدمت‌محور است، روش ممیزی این بهروش نیز کاملاً بر پایه خدمات استوار است. برای بررسی کامل رویکرد ممیزی خدمات فناوری اطلاعات بر این اساس، شرکت توسعه سامانه‌های نرم افزار نگین (توسن) به عنوان نمونه کاربردی در نظر گرفته شده است.
در این مقاله پس از بررسی تاریخچه و متدولوژی پیاده‌سازی ITIL در شرکت توسن، مفهوم ممیزی خدمات فناوری اطلاعات تشریح شده و نهایتاً نمونه واقعی و پیاده‌سازی شده مفاهیم مذکور ارایه می‌شود.
واژه‌های کلیدی: مدیریت خدمات فناوری اطلاعات، ممیزی فناوری اطلاعات، مدیریت سطوح خدمات، شاخص‌های ارزیابی

هدف

هدف از این مقاله تشریح ساختار و فرایند ممیزی خدمات فناوری اطلاعات و فواید حاصل از آن بر اساس بهروش ITIL است.

ممیزی خدمات فناوری اطلاعات بر اساس ITIL

از دیدگاه بهروش ITIL، خدمت امری نامحسوس است، و تا زمانی که نامحسوس است امکان برنامه‌ریزی، کنترل و هدایت ندارد. این بهروش بیان می‌کند که هر چند خدمات نامحسوس است، اما از طریق دارایی‌هایی ارایه می‌شود که اکثر آن‌ها قابل اندازه‌گیری است. شکل شماره ۱، فهرست دارایی‌های خدمت (Service Asset) را که به دو بخش منابع (Resource) و قابلیت (Capability) طبقه‌بندی شده، نمایش می‌دهد. به بیان دیگر، برای ارایه یک خدمت با کیفیت مطلوب باید دارایی‌های ذیل به شکل مناسب به‌کار گرفته شود. بنابراین ممیزی خدمات باید بر ممیزی دارایی‌هایی که خدمات فناوری اطلاعات از طریق آن‌ها ارایه می‌شود، متمرکز باشد.
با توجه به این‌که ارزیابی کلیه دارایی‌های خدمات بسیار مشکل است، ITIL پیشنهاد می‌دهد که ممیزی خدمات می‌تواند با تمرکز بر ممیزی فرآیندهای ارایه دهنده خدمات فناوری اطلاعات، عملیاتی شود. به‌طور مثال در فرآیند مدیریت استقرار، ممکن است میانگین زمان ارایه نسخ جدید بیش از حد طولانی شود. این مشکل از طریق ممیزی فرآیند مدیریت استقرار شناسایی می‌شود. حال با بررسی



شکل ۱: دارایی‌های مورد نیاز برای ارایه خدمت

فرآیند مدیریت اســتقرار می‌توان به این نتیجه رسید که کدامیک از دارایی‌های خدمت دچار مشــکل بوده که ســبب بروز مشکل اعلامی شده است؛ آیا مشکل از دانش تیم توسعه نرم‌افزار است و یا ابزارهای توسعه نرم‌افزار دچار مساله است.

بنابراین هرچند از دیدگاه ITIL، فرآیندها و شــاخص‌های موجود در آن‌ها در حال ممیزی اســت، امّا درصورت شناسایی هرگونه مشکلی می‌توان اقدام به تحلیل و بررســی، ونهایتاً دارایی مرتبط با مشکل را تعیین کرد. بنابراین از دیدگاه ITIL، فرآیندها و شــاخص‌هایی که در هریــک از آن‌ها وجــود دارد باید به‌صورت مداوم مــورد ممیزی قرار گیرد.

مطالعه موردی- شرکت توسن

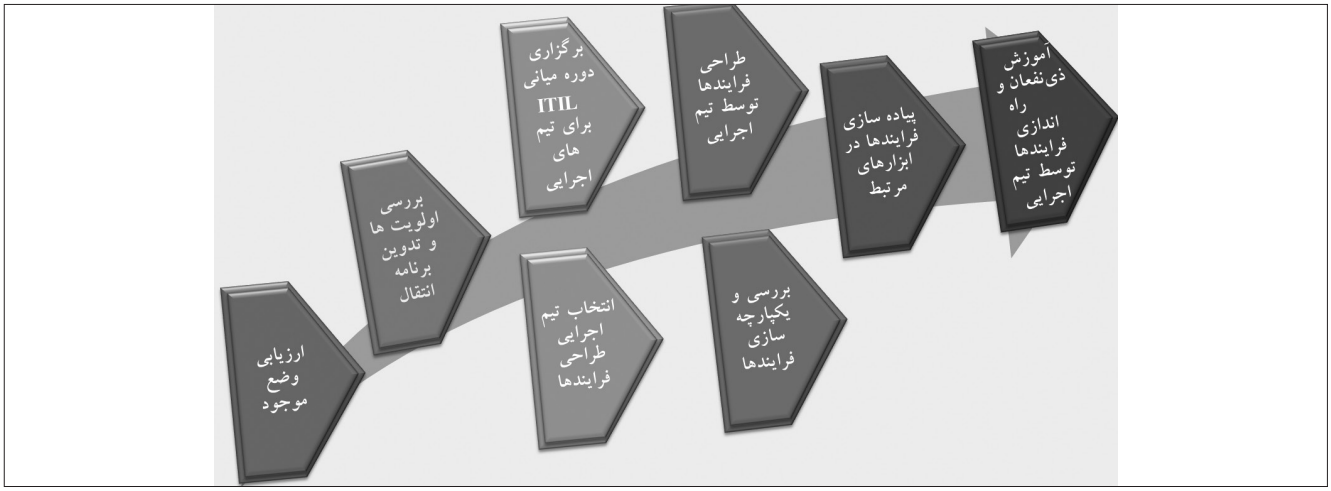
شرکت توسن در سال ۱۳۷۸ با هدف ایجاد بستری مستقل و بومی برای طراحی و تولید محصولات و راه‌حل‌های نوین فناوری اطلاعات در حوزه‌هــای بانکی وخدمات مالی تاســیس شــد. رویکرد اصلی و عامل محرک این شــرکت همواره اســتفاده از توان‌مندی‌های افراد متخصص ایرانی و طراحی نرم‌افزارهای جامع بانکی در داخل کشور بوده اســت. هم اکنون محصولات این شرکت در بیش از ۹۰ درصد بانک‌هــای خصوصی و برخی بانک‌های دولتی و موسســات مالی و اعتباری کشــور در حال اســتفاده است. توســن یک شرکت کاملاً خصوصی اســت که با بیش از ۷۰۰ نیروی متخصص و ۱۳ شــرکت زیرمجموعــه، خدمات خود را به بیش از نیمی از بانک‌های کشــور ارایه می‌دهد. شــرکت توسن خدمات متنوعی را در حوزه بانکداری الکترونیکــی اعم از خدمات حوزه بانکداری خرد، بانکداری مدرن و خدمات حوزه کارت و پرداخت به مشتریان خود ارایه می‌کند.

تاریخچه پیاده‌سازی ITIL در شرکت توسن

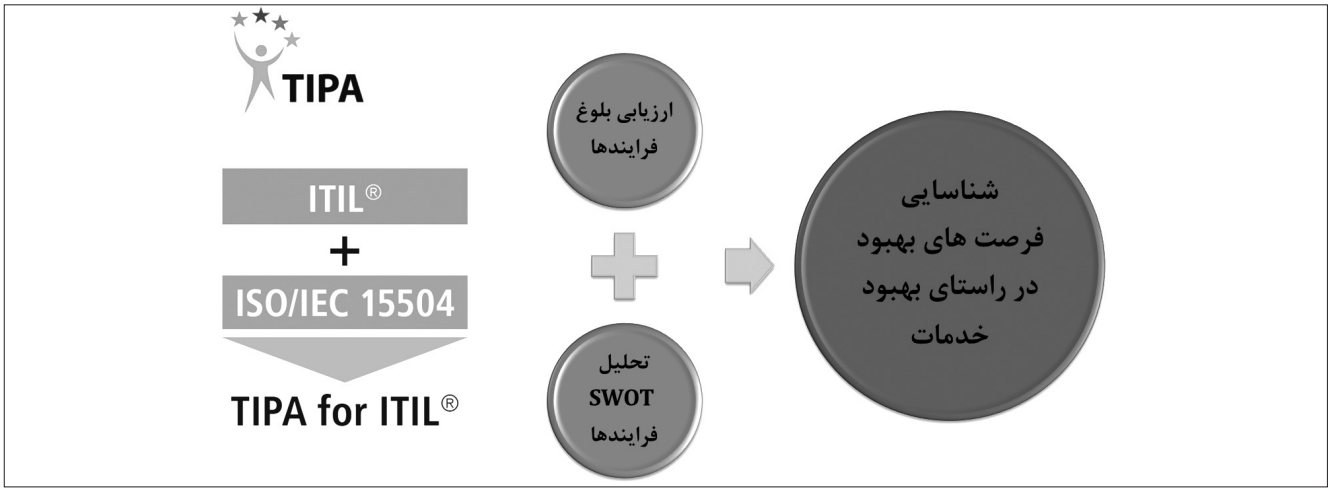
اهمیت خدمات فناوری اطلاعات در صنعت بانکداری بر هیچ کســی پوشــیده نیســت. در همین راستا، بر اســاس نیاز مشتریان و اهمیت خدمات ارایه شــده توســط شــرکت توســن، از بدو تاسیس شرکت، مدیریت عامل و هیئت‌مدیره تمرکز زیادی بر اســتفاده از بهروش‌ها و استانداردهای مطرح دنیا در این حوزه داشته‌اند.

در همیــن راســتا و از ســال ۱۳۸۵، پیاده‌ســازی ITIL بــا برخی از فرآیندهــای کلیدی از جمله «مدیریت تغییــرات» آغاز، و در انتهای ســال ۱۳۹۱ فرآیندهای «مدیریت خرابی» (Incident Management) و «مدیریت درخواســت» نیز به‌صورت کامل پیاده‌سازی شد. در این مدت، حدود ۳۰۰ نفر از مدیران و کارشناسان شرکت توسن در دوره آموزشی مقدماتی ITIL نیز شــرکت کرده، و دانش مدیریت خدمات فناوری اطلاعات به‌صورت گسترده در این سازمان نهادینه شد.

از انتهای ســال ۱۳۹۱ و بر اســاس مدیران ارشــد، شــرکت اقدام به پیاده‌ســازی همه فرآیندهای ITIL و اخذ استاندارد بین المللی /ISO IEC 20000 کرد. در همین راستا، برنامه زمان‌بندی تدوین، و مقرر شد در مدت ۱۸ ماه کلیه فرآیندها پیاده‌ســازی شــده و استاندارد مذکور اخذ شــود. با این حال، با توجه به گســتردگی پروژه مقرر شــد ابتدا خدمــات حوزه بانکداری مدرن در دامنه پروژه قرار گرفته و در ادامه، سایر خدمات به مجموعه اضافه شود.



شکل ۲: متدولوژی پیاده‌سازی ITIL شرکت توسن



شکل ۳: ساختار کلان مدل TIPA

متدولوژی پیاده سازی ITIL در شرکت توسن

با توجه به گستردگی فعالیت‌های مورد نیاز و تنوع ذی‌نفعان، یک متدولوژی جامع توسط تیم مشاور به‌منظور طراحی، پیاده‌سازی و راه‌اندازی فرآیندها پیشنهاد شد (شکل شماره ۲).

گام‌های اصلی متدولوژی فوق به شرح ذیل است:

گام اول، با ارزیابی وضعیت موجود فرآیندهای مدیریت خدمات فناوری اطلاعات در شرکت توسن آغاز شد. برای ارزیابی وضع موجود، مدل TIPA که یکی از روش‌های مطرح در ارزیابی بلوغ فرآیندها بر مبنای ITIL است،استفاده شد. شکل شماره ۳، نمای مفهومی از مدل TIPA را نشان می‌دهد.

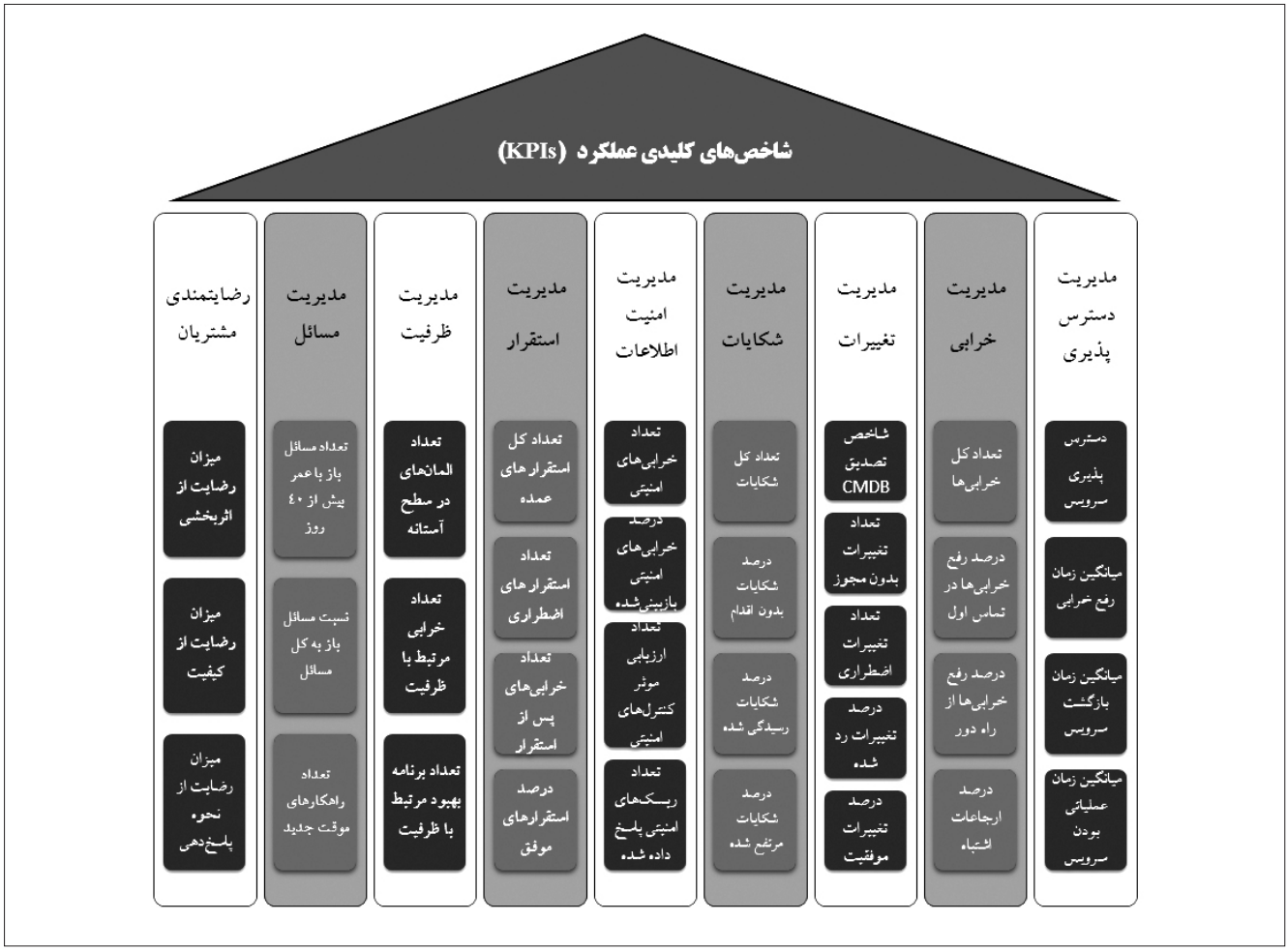
همان‌طور که در مدل مفهومی نیز مشخص شده، مدل TIPA بر اساس تلفیقی از ITIL و استاندارد ISO/IEC 15504 ایجاد شده است. این مدل به‌صورت جامع، همه ابعاد فرآیندهای مدیریت خدمات را مورد بررسی و تحلیل قرار داده، و به‌صورت دقیق تعیین می‌کند که برای بهبود فرآیندها چه اقداماتی باید صورت پذیرد.

در گام دوم، با توجه به خروجی‌های گام ابتدایی TIPA، فهرست دقیقی از بهبودهایی که باید در فرآیندهایی شرکت ایجاد شود، شکل گرفت.

در گام سوم، تیم‌های اجرایی مورد نیاز بررسی، و به ازاء هر فرآیند یک کمیته تخصصی از مدیران و کارشناسان شرکت تشکیل شد. در این پروژه، دیدگاه مدیران ارشد شرکت این بود که از ابتدای مرحله طراحی، نیروهای داخلی شرکت در کنار تیم مشاور، به‌صورت فعال در طراحی و پیاده‌سازی ایفای نقش کنند. برای افزایش اثربخشی تیم‌های داخلی، برای اعضاء کمیته‌ها، دوره‌های میانی ITIL برگزار و دانش این تیم‌ها به شکل قابل توجهی افزایش یافت.

در گام چهارم، کمیته‌های متشکل از کارشناسان شرکت با هدایت تیم مشاور اقدام به طراحی فرآیندهای مدیریت خدمات فناوری اطلاعات کردند. تیم مشاور نیز در این میان وظیفه کنترل طراحی‌های صورت گرفته و یکپارچه‌سازی میان فرآیندها را بر عهده داشت.

در گام پنجم، فرآیندهای طراحی شده در ابزارهای مورد نیاز پیاده‌سازی شد. در این پروژه دو تیم متفاوت وظیفه پیاده‌سازی ابزار را بر عهده داشت. در انتها نیز پس از پیاده‌سازی فرآیندها در ابزارهای



شکل۴: ساختار درختی شاخص‌های ارزیابی عملکرد

مرتبط، آموزش نهایی به ذی نفعان ارایه، و فرآیندهای جدید به‌صورت مکانیزه عملیاتی شد.

پیاده‌سازی کلیه فرآیندها و تشکیل سامانه مدیریت خدمات در فروردین ماه سال ۱۳۹۳ به اتمام رسید. پس از اتمام پیاده‌سازی، ۳ ماه فرآیندها برای بررسی اثربخشی، کارآیی و منطبق بودن با الزامات استاندارد تحت نظارت کامل قرار داشت، و ممیزی داخلی توسط تیم مشاور در تیرماه سال ۱۳۹۳ به انجام رسید.

نهایتاً در اواخر مردادماه سال ۱۳۹۳، ممیزی خارجی توسط ممیزی از کشور استرالیا انجام، و شرکت توسن بدون هیچ‌گونه عدم تطابقی موفق به اخذ استاندارد ISO/IEC 20000 شد، و عنوان اولین شرکت خصوصی دارنده این گواهینامه بین‌المللی در ایران را از آن خود کرد.

عوامل کلیدی موفقیت شرکت توسن در اخذ استاندارد ISO/IEC 20000

عوامل متفاوتی توسط ITIL به عنوان عوامل کلیدی موفقیت در پیاده‌سازی ITIL نام برده می‌شود، امّا اصلی‌ترین علل در شرکت توسن به شرح ذیل است:

حمایت صریح و قاطع مدیریت ارشد

یکپارچه شدن تیم مشاور و تیم‌های اجرایی شرکت توسن

عدم محدودیت در حوزه ابزار

فرهنگ سازی گسترده مفاهیم مدیریت خدمات در میان کلیه مدیران و کارشناسان شرکت توسن

اصلاح ساختار سازمانی به رویکردی خدمت‌گرا و مبتنی بر ITIL

روال ممیزی خدمات فناوری اطلاعات در شرکت توسن

همان‌طور که در بخش ممیزی خدمات بر اساس ITIL نیز تشریح شد، مسئولیت اصلی ممیزی خدمات فناوری اطلاعات بر عهده فرآیند مدیریت سطوح خدمات است. در شرکت توسن نیز بر اساس ITIL فرآیند مشخصی برای ممیزی خدمات فناوری اطلاعات وجود دارد.

گام ابتدایی در ممیزی خدمات فناوری اطلاعات، تعیین شاخص‌هایی قابل دستیابی، قابل اندازه‌گیری و توافق شده با مشتری بر روی ویژگی‌های خدمت قابل قبول و با کیفیت است. در ITIL، پیش از ارایه خدمات، همواره طی فرآیندی مشخص و با تعامل میان مشتری و ارایه‌دهنده خدمات این ویژگی‌ها تبیین و در توافقنامه سطح خدمت (SLA) ثبت می‌شود.

جدول ۱: نحوه امتیازدهی شاخص‌ها

حوزه شاخص	شاخص	امتیاز حوزه	وزن شاخص	هدف مورد نظر	مقدار بدست آمده	ارزش
مدیریت استقرار	تعداد کل استقرار های عمده	25	٪10	1	1	2.5
	تعداد استقرارهای اضطراری		٪20	1	2	0
	تعداد خرابی‌های پس از استقرار		٪30	5	2	7.5
	درصد استقرارهای موفق		٪40	٪50	94.45	10
	مجموع ارزش به‌دست آمده در حوزه مدیریت استقرار					20

جدول ۲: ساختار محاسبه ارزش نهایی خدمت

TOSAN NEGIN SOFTWARE DEVELOPMENT CO. — گزارش ماهانه بازنگری خدمت — ITIL — ISO/IEC 20000

حوزه ارزیابی	کل وزن حوزه	امتیاز کسب شده
شاخص های حوزه مدیریت رضایت مندی مشتریان	۵	۴
شاخص های حوزه مدیریت مسائل	۵	۲
شاخص های حوزه مدیریت ظرفیت	۵	۵
شاخص های حوزه مدیریت استقرار	۲۵	۲۰
شاخص های حوزه مدیریت امنیت اطلاعات	۱۰	۹
شاخص های حوزه مدیریت شکایات	۵	۴
شاخص های حوزه مدیریت تغییرات	۱۰	۸
شاخص های حوزه مدیریت خرابی	۱۰	۷
شاخص های حوزه مدیریت دسترس پذیری	۲۵	۲۳.۵
مجموع ارزش خدمت		۸۲.۵

شکل شماره ۴، نمونه‌ای از شاخص‌های مرتبط با یک مشتری را نمایش می‌دهد. شایان ذکراست از یک مشتری به مشتری دیگر و هم‌چنین از یک خدمت به خدمت دیگر، این امکان وجود دارد که اولاً فهرست شاخص‌ها و ثانیا سطح پذیرش آن‌ها متفاوت باشد.

علاوه بر این، هر یک از حوزه‌های ارزیابی برای خود وزن مشخصی داشته، و شاخص‌های اندازه‌گیری در هر حوزه نیز دارای یک وزن مشخص است. اهمیت وزن‌دهی در این روش به این دلیل است که بتوان در نهایت ارزش خدمت ارایه شده به مشتری را محاسبه کرد. به‌طور مثال، جدول شماره ۱، نشان می‌دهد که حوزه فرآیند مدیریت استقرار ۲۵% از اهمیت و ارزش خدمت را برای مشتری در خود دارد. هم‌چنین، هر شاخصی از وزن مشخصی برخوردار است. این گزارش نشان می‌دهد که در بازه زمانی تدوین گزارش، خدمت ارایه شده در حوزه دسترس‌پذیری به یکی از اهداف خود دست نیافته، و بنابراین از ۲۵ امتیاز ممکن تنها ۲۰ امتیاز را کسب کرده است.

این گزارش برای کلیه حوزه‌ها تدوین شده، و بر اساس آن، در نهایت عددی تولید شده که به آن ارزش خدمت (Service Value) گفته می‌شود. این عدد که بیانگر مجموع عملکرد کلیه فرایندها است، نشان می‌دهد که چه میزان فرآیندها، ساختار و سازمان ارایه‌دهنده خدمات فناوری اطلاعات اثربخش و کارآ است. جدول شماره ۲ نشان می‌دهد که خدمت ارایه شده در یک ماه مشخص از ۱۰۰ امتیاز ممکن، ۸۲,۵ امتیاز را کسب کرده است. علاوه بر آن، کاملاً مشخص شده که در کدامیک از فرآیندها و به چه میزان، امتیاز از دست رفته است.

در شرکت توسن، مطابق با بهروش ITIL، پس از انعقاد SLA و قرارداد با مشتریان که در آن کلیه شاخص‌ها به همراه وزن آن‌ها نهایی شده، به‌صورت ماهانه ممیزی کیفیت خدمات ارایه شده به مشتریان، مطابق با شکل شماره ۵، در ۴ گام به انجام می‌رسد.

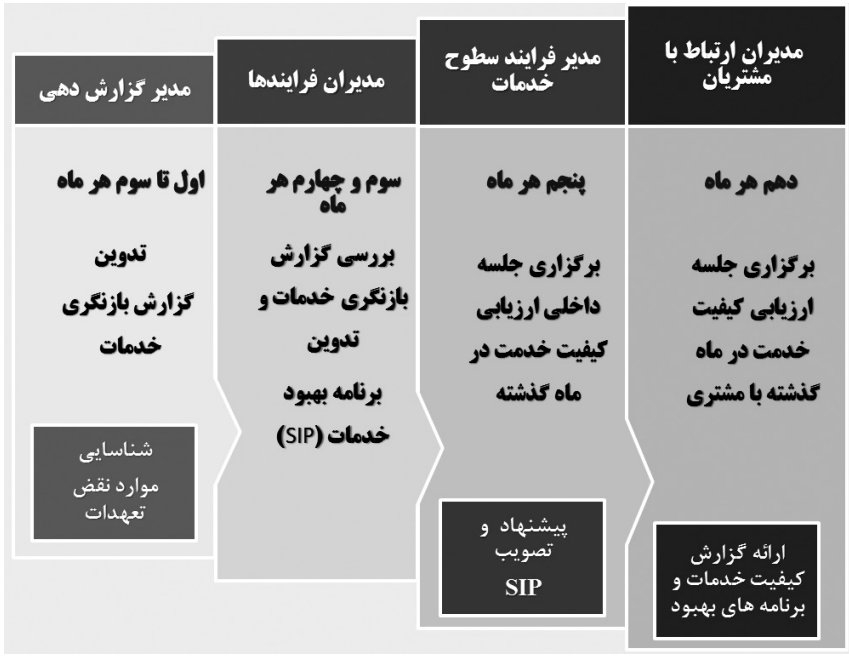
گام اول: در این گام با توجه به این مسئله که فرآیندها از طریق ابزارهای مختلفی عملیاتی شده، مدیر فرآیند گزارش‌دهی خدمات، اقدام به جمع‌آوری و یکپارچه‌سازی گزارش‌ها و تدوین گزارش بازنگری خدمات (Service Review Report) می‌کند. این گزارش تعیین می‌کند که در کدامیک از شاخص‌ها شرکت نتوانسته به تعهدات خود نسبت به مشتری عمل کند.

گام دوم: با توجه به این‌که هر یک از شاخص‌ها مرتبط با یکی از مدیران فرآیندها است، مدیران فرآیندهایی که شاخص مرتبط با آن‌ها دچار نقض تعهد (Breach) شده، باید پس از دریافت گزارش، اقدام به بررسی، ریشه‌یابی و شناسایی نحوه رفع مشکل به‌منظور عدم وقوع مجدد آن‌ها در آینده کند. پیشنهادهای بهبود هریک از مدیران فرآیندها، در مستندی به نام برنامه بهبود خدمت (Service improvement plan-SIP) ثبت می‌گردد. پیشنهاد بهبود می‌تواند به هر یک از ۸ عامل موثر در ارایه خدمت مرتبط باشد.

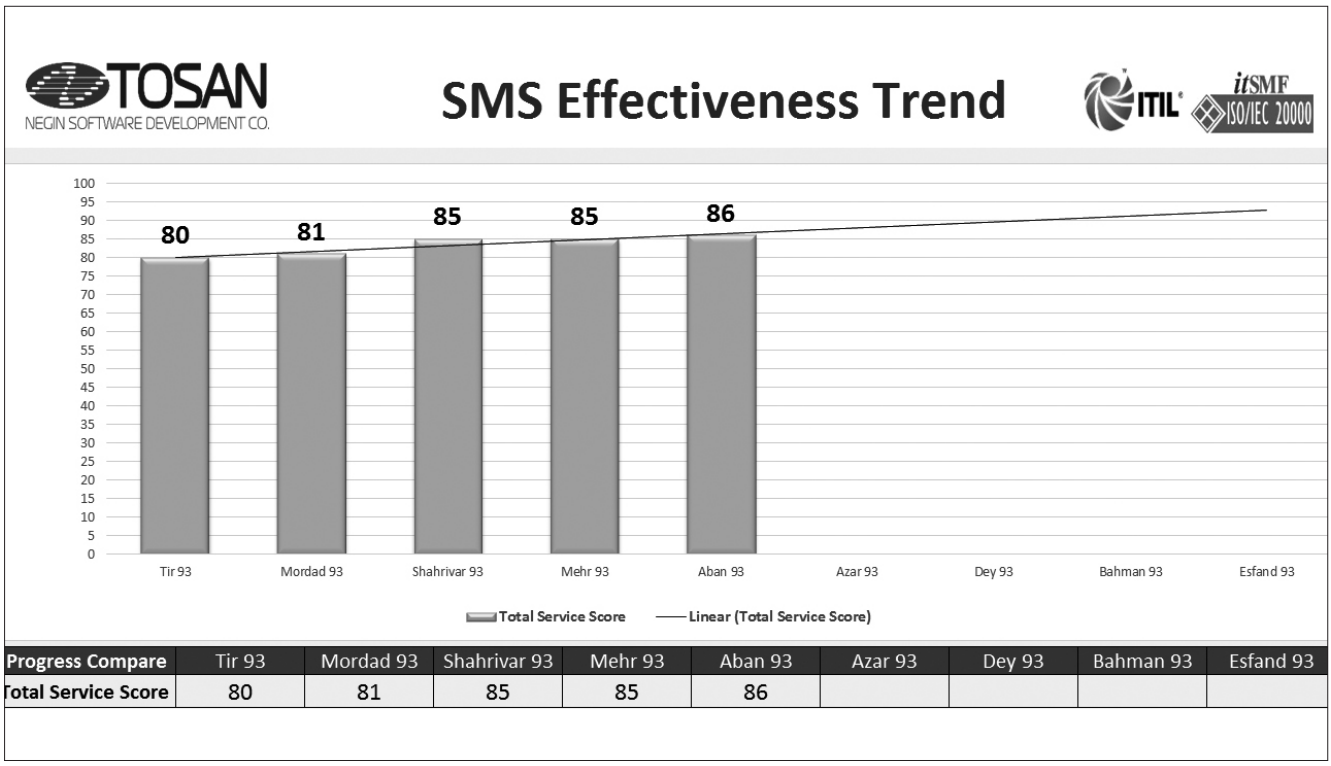
گام سوم: در تاریخ پنجم هر ماه، جلسه بازنگری خدمات به ازای مشتریان مختلف برگزار شده و مدیران فرآیندهایی که دارای شاخص‌های نقض شده، اقدام به توضیح برنامه بهبود مرتبط می‌کند. با توجه به این‌که مدیران اصلی فرآیندها و هم‌چنین مدیران خدمات در جلسه حضور دارند، برنامه‌های بهبود در همان جلسه بررسی و به تصویب می‌رسد و یا مدیر فرآیند موظف می‌شود برنامه دیگری را پیشنهاد کند.

گام چهارم: در آخرین گام، و در دهم هر ماه، مدیر ارتباط با مشتری، مدیر سطح خدمت و مدیران فرآیندهای مرتبط جلسه‌ای را با مشتری برگزار کرده، و وضعیت ارایه خدمت در ماه گذشته را که شامل مرور شاخص‌ها است ارایه می‌کند. هم‌چنین فهرست برنامه‌های بهبود را که به‌صورت هدف‌مند تدوین تا در آینده تقض تعهدی در ارایه خدمات صورت نگیرد، به مشتری ارایه می‌دهد.

این روال ممیزی، فرآیندی ساخت‌یافته، هدف‌مند و کارآ در شناسایی نقاط ممیزی، مرور مداوم شاخص‌ها، ارتباط موثر با کلیه ذی نفعان، شناسایی برنامه‌های بهبود و اجرایی کردن آن‌ها است. شایان ذکر است، علاوه بر این‌که در فرآیند ممیزی یک نگاه جزءنگر به عملکرد تک تک فرآیندها وجود دارد، یک نگاه جامع نیز به کلیت عملکرد و یا اثربخشی کل سامانه وجود دارد. این ارزیابی از طریق بررسی روند ارزش کلان خدمات ارایه شده در طول زمان به انجام می‌رسد.



شکل ۵: فرآیند ممیزی خدمات فناوری اطلاعات



Progress Compare	Tir 93	Mordad 93	Shahrivar 93	Mehr 93	Aban 93	Azar 93	Dey 93	Bahman 93	Esfand 93
Total Service Score	80	81	85	85	86				

شکل ۶: روند ارزش ارایه شده توسط خدمات

به‌طـور مثال نمودار شـکل ۶، روند اثربخشـی سـامانه مدیریت خدمات فناوری اطلاعات را به مشـتریان نشـان می‌دهد. در این نمودار، ارزش خدمات ارایه شده به مشتری در طول زمان با شیب ملایمی در حال بهبود بوده، و بنابراین نیاز به تغییرات اساسی در فرآیندها، سـاختار و ابزارهای مدیریـت خدمات فناوری اطلاعات وجود ندارد.

Interview
مصاحبه

مصاحبه با آقای دکتر شاهپری؛ رییس امور سیستم‌ها و دولت الکترونیکی معاونت توسعهٔ مدیریت و سرمایهٔ انسانی رئیس جمهور

در یک روز پاییزی به معاونت توسعه مدیریت و سرمایه انسانی رییس جمهور قدم گذاشتیم تا با آقای دکتر شاهپری در مورد جشنواره شهید رجایی از منظر ممیزی فناوری اطلاعات و تاثیر برگزاری آن در بهبود خدمات فناوری اطلاعات و استقرار دولت الکترونیکی در کشور صحبت کنیم. آن‌چه می‌خوانید حاصل این صحبت دوستانه است:

پرسش:در ابتدا لطفاً جشنواره شهید رجایی را معرفی نمایید؟

پاسخ: هر ساله توسط معاونت توسعه و سرمایه انسانی رییس‌جمهوری، در تمامی حوزه‌ها ارزیابی عملکرد دستگاه‌های دولتی انجام می‌شود. پیش‌نیاز انجام این ارزیابی، طراحی «بسته ارزیابی» است. این بسته شامل توصیف حوزه‌های ارزیابی، شاخص‌های هر حوزه، امتیاز هر شاخص، سازوکار ارزیابی و تشریح نحوه ثبت اطلاعات توسط دستگاه‌ها در همه حوزه‌ها است. براساس شاخص‌های تعریف شده ذیل هر حوزه، کلیه دستگاه‌های اجرایی که فهرست آن‌ها در جدول‌الف آمده است مورد سنجش قرار می‌گیرند. نمونه‌ای از این بسته ارزیابی برای دو شاخص در پیوست ارایه شده است. فرآیند ارزیابی بدین گونه است که هر سازمانی از طریق سامانه ارزیابی الکترونیکی دولت با شناسه کاربری و رمز عبور خود وارد سامانه شده، اطلاعات را در سامانه وارد می‌کند. اطلاعات به صورت خوداظهاری است. به این معنا که هر دستگاه شواهد مربوط به انجام هر شاخص را در مجموعه خود از طریق سامانه ثبت کرده و مستندات مربوطه را پیوست می‌کند.

براساس سنجش انجام شده، دستگاه‌های برتر مشخص، و در جشنواره سالانه شهید رجایی معرفی شده و از آن‌ها تقدیر به عمل می‌آید. در این جشنواره علاوه بر دستگاه‌های برتر، کارکنان برتر نیز معرفی می‌شوند. هدف از این ارزیابی و جشنواره، بهبود مستمر خدمات دولت است.

پرسش:با توضیحات شما به نظر می‌رسد این ارزیابی به منظور ممیزی دستگاه‌ها به طور کلی و به‌طور خاص ممیزی فناوری اطلاعات طراحی و اجرا می‌شود.

پاسخ:بله کاملا درست است. در حوزه فناوری اطلاعات دو زیر حوزه ۱- مهندسی مجدد فرآیندها و اصلاح سیستم‌ها و ۲- الکترونیکی کردن خدمات دستگاه‌های اجرایی، فعلاً محدوده ممیزی است. دستگاه‌های اجرایی بر اساس شاخص‌های تعریف شده در این دو حوزه از نظر فناوری اطلاعات ارزیابی می‌شوند، و امتیازهای کسب شده توسط هر دستگاه به آن‌ها ابلاغ می‌شود.

پرسش:منظورتان از دستگاه‌های اجرایی چیست؟

پاسخ:همه دستگاه‌هایی که از دولت بودجه دریافت می‌کنند، وزارتخانه‌ها، استانداری‌ها و..... که در دو سطح ملی و استانی ارزیابی می‌شوند. در سطح ملی، ارزیابی برعهده معاونت توسعه، و در سطح استانی بر عهده استانداری ها است.

پرسش: یک نگاه به موضوع ممیزی فناوری اطلاعات آن است که هدف از ممیزی فناوری اطلاعات برخوردهای قهری و تنبیهی است و حتی برخی افراد عنوان می‌کنند این کار باید توسط واحدهای غیر از فناوری اطلاعات انجام شود چون متخصصین فناوری، اطلاعات ممیزی مربوط به حوزه خود را به درستی منتشر نمی‌کنند و نگاه دیگر لزوم پرداختن به این موضوع به عنوان یک فرآیند مستمر و لازمه بهبود مستمر است، که شما به آن اشاره فرمودید. در فرآیند ارزیابی چه اقداماتی را برای ترویج نگاه دوم و حذف شائبه به اصطلاح عامیانه مچ‌گیری، انجام داده‌اید؟

پاسخ:هدف ما از ممیزی، ایجاد بهبود در دستگاه‌ها و ترغیب آن‌ها به افزایش و بهبود خدمات الکترونیکی و اصلاح فرآیندها است. لذا به منظور تحقق این هدف در ابتدا سعی می‌کنیم دستگاه‌ها به درستی شاخص‌های تعریف شده را متوجه شده و تعریف شاخص و نحوه سنجش آن به صورت شفاف ارایه شود. در هر یک از شاخص‌ها امتیاز حداکثر ذکر شده است. پس از ثبت اطلاعات در سامانه و ذکر شواهد مربوط به هر شاخص توسط دستگاه به صورت خوداظهاری، اطلاعات دستگاه‌ها یک به یک توسط کارشناسان معاونت ارزیابی، و نظرات کارشناسان از طریق توضیحات در فرم خوداظهاری اعلام می‌شود.

به عنوان مثال مطابق با ماده ۳۶ قانون مدیریت خدمات کشوری دستگاه‌ها موظف به اجرای اقداماتی در حوزه اصلاح فرآیندها هستند. در این راستا، از آن‌ها خواسته شده فهرست اقدامات خود را در خصوص مستندسازی فرآیندها و اصلاح فرآیندها با ذکر شواهد و مستندات ارایه نمایند. هم‌چنین در حوزه دولت الکترونیکی، از سازمان‌ها خواسته شده فهرست خدمات الکترونیکی خود را با مستند ارایه کرده، و وضعیت هر خدمات خدمت از نظر این‌که کاملا الکترونیکی شده و یا نیمه الکترونیکی است را مشخص کنند. در واقع به دنبال آن بودیم که هر سازمانی کاتالوگ خدمات خود را مستند نماید تا در ابتدا بداند چه خدماتی را عرضه می‌کند و بر اساس شرح وظایف مصوب موظف به ارایه چه خدماتی است. سپس خدمات ارایه شده توسط سازمان مستندسازی شده و در نهایت الکترونیکی شود و یا از طریق کانال‌های متفاوت در عرضه استفاده عموم قرار گیرد. این کانال‌ها می‌تواند وبگاه، موبایل و یا دفاتر پیشخوان باشد. و بدین صورت بهبود مستمر در دستگاه‌ها اتفاق بیفتد.

مثلاً دستگاه اعلام کرده در بحث مستندسازی فرآیندی امتیاز من ۲۵ از ۲۵ است، ولی بر اساس نظر کارشناس امتیاز وی ۱۸ از ۲۵ برآورد می‌شود. علت این کاهش برای هر شاخص توسط کارشناس اعلام می‌شود. حسن این روش آن است چون هر شاخص در تمامی دستگاه‌ها توسط کارشناسان واحد بررسی می‌شود، در بحث ارزیابی سازگاری وجود دارد. پس از اظهار نظر کارشناس دستگاه می‌تواند نظرات کارشناسان ارزیابی را از طریق همان سامانه مشاهده و در مورد آن‌ها در صورت نیاز اعتراض کند و مستندات بیشتری ارایه کند که تاییدی بر امتیاز خوداظهاری خودش باشد. پس از سنجش در ابتدا نتایج که از طریق سامانه در اختیار دستگاه‌ها قرار گرفته، آن‌ها می‌توانند به نتایج اعتراض کنند. به منظور بررسی اعتراضات و تشریح بیشتر شاخص‌ها و هم‌چنین ارایه راه‌کارهای اصلاحی، در برخی موارد هم با دستگاه‌ها به منظور شفافیت بیشتر و اهتمام ما به بهبود خدمات جلساتی حضوری برگزار شده تا به اعتراض‌ها در جلسات حضوری و بر اساس تعامل متقابل رسیدگی می‌شود. در این جلسات با مقایسه دستگاه با سایر دستگاه‌ها امتیازهای وی توجیه می‌شود، تا هم ابهامات دستگاه برطرف شود و هم در روند بهبود با نمونه‌های برتر آشنا شود. در نهایت ارزیابی نقاط قوت و ضعف دستگاه به آن‌ها اطلاع‌رسانی می‌شود. و فهرست اقدامات مورد نیاز برای بهبود شاخص‌ها عنوان می‌شود.

در این فرآیند، تاکید ما در وهله نخست آن است که دستگاه وظیفه‌اش را به درستی شناخته، سپس مفهوم شاخص‌ها به درستی درک شود و در نهایت مشخص شود که آیا در دستگاه برنامه مشخصی برای تحقق این شاخص‌ها وجود دارد یا خیر، در ضمن زیرساخت‌های لازم برای اجرای این برنامه در دستگاه فراهم شده باشد. بنابراین برخوردهای حذفی و تنبیهی و یا در اصطلاح عامیانه مچ‌گیری تا حد زیادی با این رویکرد از بین می‌رود. از نظر بنده ارزیابی شروع کار است نه پایان کار. در واقع آن‌چه ما به دنبال آن هستیم پس از ارزیابی و مشاهده نتایج توسط دستگاه‌های ذیربط آغاز می‌شود. از آن‌جا که در فرآیند ارزیابی بخش‌های متفاوتی از سازمان درگیر می‌شوند در واقع شاخص‌ها مربوط به حوزه‌های کاری متفاوتی در دستگاه‌ها است که اطلاعات خود را به واحد ارزیابی عملکرد ارایه کرده و در نهایت اطلاعات آن‌ها توسط واحدهای ارزیابی عملکرد جمع‌آوری شده و به صورت نتایج شاخص‌ها به ما اعلام می‌شود. پس از ارزیابی، افراد مختلف از دستگاه‌های مختلف رجوع می‌کنند که در فرآیند بهبود آن‌ها را کمک کنیم. هدف ما از کل این فرآیند، در این مواقع، محقق می‌شود. ایجاد این حساسیت‌ها در دستگاه پیش‌نیاز بهبود مستمری است که شما از آن یاد کردید.

پرسش:با توجه به این‌که بحث ارزیابی یکی از سه مجموعه فرآیند چارچوب‌های حاکمیتی است و با توجه به نقش معاونت توسعه در حوزه حاکمیت دولت الکترونیکی اگر ممکن است به نحوه انجام کلیه فرآیندهای حاکمیتی در معاونت توسعه اشاره فرمایید.

پاسخ: در چارچوب‌های حاکمیتی سه حوزه فرآیندی اصلی هدایت، پایش و ارزیابی تعریف شده است. در حوزه دولت و حوزه کاری ما بحث هدایت از طریق تصویب و ابلاغ آئین‌نامه‌ها و بخشنامه ها،و قوانین بالادستی مانند قانون برنامه پنجم و قانون مدیریت خدمات کشوری و سایر قوانین صورت می‌پذیرد. در زمینه سنجش همان‌طور که گفته شد شاخص‌هایی تعریف می‌شود که مبنای آن‌ها همان قوانین بوده، و در فرم‌های ارزیابی به قوانین و مقررات مرتبط به صورت شفاف اشاره شده است.

پرسش: در زمینه به اشتراک‌گذاری تجارب دستگاه‌ها چه تمهیداتی اندیشیده‌اید؟

پاسخ: به نکته بسیار خوبی اشاره کردید. در این زمینه اقدامات ما تا این زمان معرفی دستگاه‌های برتر در جشنواره شهید رجایی و اعلام عمومی دلایل برتری آن‌ها است.

علاوه بر آن هم‌اکنون نشست‌هایی داریم که ۱۰۰ نفر از مدیران فناوری اطلاعات کشور در آن‌ها شرکت می‌کنند. در این نشست‌ها که تاکنون ۳ مورد آن برگزار شده، به دنبال ارایه تجارب برتر هستیم. در واقع هم اشتراک دانش در زمینه اجرای شاخص‌ها و هم ارزیابی و بازبینی شاخص‌ها با وجود افراد متخصص.

با این حال، برنامه‌ریزی آتی معاونت ایجاد درگاهی به منظور اطلاع‌رسانی در زمینه تجارب برتر است، ضمن برگزاری نشست‌هایی که در آن‌ها سازمان‌های برتر تجربیات خود را عرضه نمایند. علاوه بر آن، به دنبال ایجاد یک سامانه ملی برای ثبت پروژه‌های انجام شده در زمینه ارایه

خدمات الکترونیکی و مهندسی مجدد فرآیندها هستیم تا تجربیات دستگاه‌ها در این زمینه به اشتراک گذاشته شود و تمام دستگاه‌ها از پروژه‌های موفق و ناموفق این حوزه خبردار شوند. در این زمینه، ابلاغیه‌ای در حوزه مهندسی مجدد فرآیندها تصویب شده که احتمالاً در دی ماه سال ۱۳۹۳ ابلاغ می‌شود.

حوزه مورد تمرکز اولیه ما در زمینه سامانه ملی در زمینه مهندسی مجدد فرآیندها است در این زمینه تفکر شبکه اجتماعی، بهره‌مندی از نظرات خبرگان و جذب افراد علاقمند می‌تواند مفید و تاثیرگذار باشد.

پرسش: در فرآیند و ارزیابی که به آن اشاره فرمودید مهم‌ترین چالش‌ها را چه می‌دانید؟

پاسخ: مهمترین چالش‌ها را می‌توان سه مورد دانست.

چالش نخست آن‌که برخی از دستگاه‌ها، که البته تعدادشان زیاد نیست، صرفاً به دنبال نمره ارزیابی هستند. در صورتی که هدف اصلی ارزیابی در ابتدا شناسایی نقاط قوت و ضعف و در نهایت بهبود نقاط ضعف است. نگاه ما به ارزیابی یک فرآیند بی‌پایان است که به عنوان بخشی از چرخه PDCA بهبود را مدنظر قرار می‌دهد. بنابراین صرف رتبه‌بندی ایجادکننده ارزشی نخواهد بود.

چالش دوم آن است که با تمام تلاشی که می‌شود بعضاً برخی شاخص‌ها برای دستگاه‌ها نامفهوم بوده، و برداشت مشترک و تفاهمی در این مورد وجود ندارد. در صورتی که لازم است در فرآیند ارزیابی، بین ارزیاب و ممیزشونده درک مشترکی در مورد شاخص‌ها وجود داشته باشد که این چالش لزوم جلسات توجیهی و تشریحی شاخص‌ها را به صورت شفاف مشخص می‌کند.

چالش سوم آن است که ارتباط ما با دستگاه بعضاً ارتباطی گسسته است. بدان معنا که از یک ارزیابی تا ارزیابی بعدی ارتباط ما قطع می‌شود. با برگزاری نشست‌های تخصصی و ارایه تجربیات برتر و هم‌چنین نشست‌های ارزیابی خود شاخص‌ها به دنبال ایجاد ارتباطی مستمر هستیم.

پرسش: در صحبت‌های قبلی به بهبود مستمر اشاره کردید. بهبود مستمر را در دو حوزه داریم: ۱- در حوزه اجرا و دستگاه‌ها که به نظر می‌رسدارزیابی‌های مستمر و مداوم شما موتور محرکی برای خودارزیابی در حوزه دستگاه‌ها بوده است و ۲- در حوزه حاکمیت، بدین معنا که آیا ارزیابی آیین‌نامه‌ها و قوانین ابلاغی و به دنبال آن فرآیند اصلاحی در حوزه وضع قوانین و بخشنامه‌هاو آیین‌نامه‌ها، وجود دارد؟ و آیا بازخورد حاصل از بدنه اجرایی در تصحیح قوانین و مقررات تاثیری دارد؟

پاسخ: بله، در این زمینه اقداماتی انجام می‌دهیم: ۱- در نشست‌هایی که برگزار می‌کنیم با حضور نمایندگان دستگاه‌های اجرایی و خبرگان به تبادل نظر در مورد فرآیند ارزیابی، بخش‌نامه‌ها، آیین‌نامه‌ها و قوانین ابلاغی می‌پردازیم. دومین اقدام بازبینی نتایج ارزیابی است. بر این اساس در صورتی که در شاخصی نمره همه ارگان‌ها پایین باشد نمایانگر سه موضوع است: یا بستر لازم برای اجرای قانون وجود ندارد؛ یا بخش‌نامه، قانون، آیین‌نامه متناظر به درستی تدوین نشده؛ و یا توضیح شاخص مرتبط به درستی انجام نشده است. تمام این سه مورد با جزئیات مورد بررسی و کنکاش قرار گرفته و در صورتی که مطمئن شویم اشکال از آئین‌نامه‌ها، بخش‌نامه‌ها و قوانین است، اصلاح آن‌ها در دستور کار قرار می‌گیرد. در بعضی موارد ابلاغیه های جدید اصلاحی تدوین می‌شود.

پرسش: در برخی موارد پیوند نتایج ارزیابی با میزان بودجه‌ای که دستگاه دریافت می‌کند، می‌تواند تاثیرگذارتر باشد. آیا این موضوع در ارزیابی‌های شما هم لحاظ می‌شود؟

پاسخ: دستگاه‌ها بر اساس دو گروه شاخص ارزیابی می‌شوند: شاخص‌های اختصاصی و عمومی. «شاخص‌های عمومی» توسط معاونت توسعه طراحی و ابلاغ می‌شود و شاخص‌های اختصاصی توسط معاونت برنامه‌ریزی و نظارت راهبردی رییس جمهور با همکاری دستگاه‌ها تهیه می‌شود. به عنوان مثال در وزارت راه، وضعیت فناوری اطلاعات خدمات الکترونیکی، ساختار و پرسنل وزارت از طریق سنجش «شاخص‌های عمومی» مشخص می‌شود و وضعیت خدمات راه‌سازی، پل‌سازی، جاده‌سازی از طریق «شاخص‌های اختصاصی» تعیین می‌شود. لذا نتایج سنجش در اختصاص بودجه در سال‌های بعد تاثیرگذار است. اما موردی که به آن اشاره کردید، پیوند بین ممیزی و تعیین بودجه، هنوز کامل نیست. حلقه‌های مفقوده‌ای در این زمینه وجود دارد. به عنوان مثال، پایش میزان استفاده صحیح ازبودجه توسط دستگاه‌ها هنوز انجام نمی‌شود. در برنامه آتی ما معرفی دستگاه‌های برتر در زمینه استفاده از بودجه و هم‌چنین دستگاه‌هایی که بودجه را به درستی استفاده نکرده و آن را هدر داده‌اند قرار دارد.

پرسش: در بحث رتبه ایران در شاخص‌های جهان مثل سازمان ملل و ITU در زمینه شاخص‌های فناوری اطلاعات، معمولاً رتبه ایران رتبه نامناسب و گاهی غیرباور است. در برخی از این گزارش‌ها اشاره شده که به دلیل عدم دسترسی به اطلاعات مناسب و بر اساس شواهد قابل وصول این رتبه محاسبه شده است. نقش انجام فرآیند مستمر خودتان را جمع‌آوری آمار ملی تا چه حد مفید می‌دانید.

پاسخ: نکته بسیار مهم در زمینه ملی آن است که اطلاعات به صورت سیستماتیک و از کانال‌های رسمی منتقل نمی‌شود. اطلاعات اعلام شده گاهی اوقات بر اساس حدس و گمان و یا ذوق و سلیقه افراد اعلام می‌شود. در برخی موارد هم به علت نبود ترجمه درست اطلاعات به انگلیسی، تصور نهادهای بین‌المللی آن است که چنین اطلاعاتی وجود ندارد. در این فرآیند بخشی از وظایف به عهده معاونت توسعه است که در حوزه وظایف معاونت توسعه، برنامه‌ریزی شده که اسناد با زبان انگلیسی در دسترس مخاطبان قرار گیرد. اما لازم است که یک تلاش ملی در زمینه تجمیع اطلاعات، ایجاد کانال‌های رسمی اطلاع‌رسانی و ترجمه اسناد ملی به‌وجود آید.

پرسش: با توجه به این‌که مخاطب خدمات دولت طیف وسیعی از ذی‌نفعان هستند چگونه نظرات این طیف وسیع در ارزیابی‌های شما لحاظ می‌شود؟

پاسخ: وظیفه اصلی دولت ارایه خدمات بهتر به شهروندان است. لذا در فرآیند سنجش یکی از گروه‌هایی که به صورت خاص مورد نظر قرار

می‌گیرد، مردم هستند. در این زمینه پرسش‌نامه‌هایی تدوین می‌شود و از شهروندان پرسیده می‌شوند. به عنوان مثال در دور آخر ارزیابی که شهریور سال جاری انجام شد، نظر ۳۰۰ هزار نفر از شهروندان در مورد شاخص‌های مختلف دستگاه‌های متفاوت کسب شد. این ارزیابی‌ها استانی بود و تاثیر به‌سزایی در انتخاب دستگاه برتر داشت. حوزه دیگری که غیر از افراد و بخش‌های داخلی هر دستگاه و شهروندان در بحث ارزیابی پوشش داده می‌شود تعاملات دستگاه با دستگاه‌های دیگر است.

در خصوص تعامل یک دستگاه با دستگاه‌های دیگر، موضوع به صورت دوگانه کنترل می‌شود. به این معنا که اگر دستگاه «الف» در فهرست خدمات الکترونیکی خود، ارایه خدمتی خاص به دستگاه «ب» را اعلام نماید، حتماً در اطلاعات ارزیابی دستگاه «ب» موضوع کنترل می‌شود که آیا از دستگاه «الف» خدمتی را دریافت می کند یا خیر.

کلام آخر

کلام آخر همان تاکید قبلی است، که ارزیابی لازمه انجام یک کار درست است. برخی اوقات تصور دستگاه‌های اجرایی آن است که خدمات خود را به خوبی ارایه می‌کنند. امّا وقتی این موضوع توسط ذی‌نفعان مختلف ارزیابی می‌شود، نتیجه متفاوت از تصور دستگاه خواهد بود. اگر به ممیزی فناوری به عنوان یک فرآیند مستمر نگاه کنیم هم بهبود در سطح دستگاه‌های اجرایی را خواهیم داشت و هم اصلاح آیین‌نامه‌ها و بخشنامه‌ها، به نحوی که قابل اجرا و تسهیل‌کننده باشد نه بازدارنده.

پیوست:

شاخص اول	احصا و اولویت‌بندی خدمات قابل ارایه از طریق الکترونیکی

مستندات شاخص: آیین‌نامه توسعه خدمات الکترونیکی دستگاه‌های اجرایی (مصوبه شماره ۷۷۴۰/۹۳/۲۰۶ تاریخ ۱۰/۶/۱۳۹۳ شورای‌عالی اداری)

جدول فهرست استاندارد از خدمات دستگاه

ردیف	عنوان دستگاه/سازمان وابسته	عنوان خدمت	الکترونیکی /غیر الکترونیکی

توجه: شامل فهرستی از کلیه خدمات الکترونیکی و غیرالکترونیکی چه استانی و چه ملی است که عناوین و تعداد آنها به تأیید بالاترین مقام دستگاه رسیده باشد. عناوین خدمات اعلام شده به منزله عناوین استاندارد خدمات بوده و کدبندی خواهند شد و پس از این ملاک عمل ارزیابی ها، قرار خواهند گرفت.

شاخص دوم، سوم و چهارم	اطلاع‌رسانی الکترونیکی در خصوص شیوه ارایه خدمات ارایه فرم‌های مورد نیاز جهت انجام خدمات از طریق الکترونیکی(تعاملی) ارایه خدمات به صورت الکترونیکی(تراکنشی)

مستندات شاخص: ماده ۳۷ و ۴۰ قانون مدیریت خدمات کشوری، آیین‌نامه اجرایی ماده (۴۰) قانون مدیریت خدمات کشوری(تصویب‌نامه شماره ۸۱۸۳۹/ ت۴۴۲۹۴ک تاریخ ۱۹/۴/۱۳۹۰) و مصوبه شماره ۷۲۲/۱۳.ط تاریخ ۲۲/۴/۱۳۸۱ شورای‌عالی اداری

جدول الف) فهرست اطلاعات عمومی دستگاه

ردیف	عنوان دستگاه/ سازمان وابسته	معرفی تشکیلات و ساختار دستگاه(۲امتیاز)		مجموعه قوانین و مقررات فعالیتهای دستگاه به تفکیک موضوع(۲امتیاز)		آگهی های مناقصه و مزایده(۲امتیاز)		به روزرسانی اطلاعات تماس با دستگاه(ادرس، تلفن، نمابر، پست الکترونیک) (۲امتیاز)		اسامی مدیران واحدها بر اساس ساختار و نحوه ارتباط با آنان(۲امتیاز)		شمارشگر مراجعان به صورت کلی و برحسب موضوع(۱ امتیاز)		دریافت سوال وارسال پاسخ به مردم از طریق کانال های ارتباطی مختلف (پست الکترونیک، پیامک، تلفن و...) (۲امتیاز)		پرسش های متداول(۲امتیاز)		پیوند به جایگاه های اینترنتی مرتبط با فعالیت های دستگاه(۲امتیاز)		پیوند به جایگاههای اینترنتی دفتر مقام معظم رهبری، ریاست محترم جمهوری، در محل مناسبی در صفحه اول جایگاه(۲امتیاز)		وجود موتور جستجوی جایگاه اینترنتی(۲امتیاز)		نظرسنجی(۲امتیاز)		درج فهرست و مشخصات دفاتر پیشخوان ارائه کننده خدمات در سایت دستگاه مطابق جدول ب(۲امتیاز)	
		بلی	خیر	بلی	خیر	بلی	خیر	بلی	خیر	بلی	خیر	بلی	خیر	بلی	خیر	بلی	خیر	بلی	خیر	بلی	خیر	بلی	خیر	بلی	خیر	بلی	خیر	بلی	خیر

جدول ب)درج فهرست و مشخصات دفاتر دریافت کننده خدمات در سایت دستگاه

ردیف	عنوان دستگاه/سازمان وابسته	عنوان خدمت	کد دفتر ارائه کننده خدمت	نام مسئول دفتر	آدرس و تلفن دفتر

جدول ج) فهرست کلیه خدمات تخصصی دستگاه در پرتال یا سایت(اطلاع‌رسانی، تعاملی و تراکنشی)

ردیف	عنوان دستگاه/ سازمان وابسته	عنوان خدمت	ارائه اطلاعات مربوط به خدمت* (بلی/ خیر)	قابل دسترس بودن فرم‌های مورد نیاز برای انجام خدمت از طریق جایگاه اینترنتی(۱۰ امتیاز)		امکان تکمیل و ارسال فرم‌های مرتبط با خدمت از طریق جایگاه اینترنتی دستگاه(۱۰ امتیاز)		امکان اخذ خدمت به صورت کاملاً الکترونیکی(e-service) از طریق جایگاه اینترنتی دستگاه(۳۰ امتیاز)	
				بلی/خیر	آدرس URL	بلی/خیر	آدرس URL	بلی/خیر	آدرس URL

* از قبیل شرح خدمت، قوانین و مقررات مربوطه، مدارک مورد نیاز برای انجام خدمت ،روش‌های انجام خدمات به شهروندان(همراه با زمان‌بندی انجام آن‌ها)

Article
مقاله

نظارت بر شبکه پرداخت الکترونیکی

سیامک آزادی‌ابد
مدیر امنیت و نظارت شرکت شاپرک
پست الکتریکی: s.azadi@shaparak.com

محمدرضا عباسی
کارشناس ارشد امنیت اطلاعات شرکت شاپرک
پست الکتریکی: m.abasy@shaparak.com

آمنه ملقب به نگین فیروزه
کارشناس ارشد نظارت بر عملکرد شرکت شاپرک
پست الکتریکی: n.firuzehi@shaparak.com

پیش از ایجاد شاپرک، پرداخت الکترونیکی در کشور ایران، دارای مشکلات و معضلاتی بود که در سال ۱۳۹۰، چاره آن در ایجاد یک بازوی نظارتی و کنترلی برای بانک مرکزی ج.ا.ا. با نام شاپرک دیده شد. بدین منظور، در شرکت شاپرک، مدیریت امنیت و نظارت تشکیل شد که به تدوین الزامات فنی و امنیت اطلاعات پرداخته و به اجرای آن‌ها توسط شرکت‌های پرداخت الکترونیکی، نظارت کند. لذا، ابتدا وضعیت موجود شبکه پرداخت الکترونیکی کشور مورد بررسی و مطالعه قرار گرفت و هم‌چنین مطالعه‌ای تطبیقی با نمونه‌های موفق جهانی (مانند ویزا و مسترکارت) انجام شد. در نقشه‌راهی که از این طریق به دست آمد، پرداختن به تدوین الزامات و مقررات، و نیز ابلاغ و نظارت بر اجرای آن‌ها، مهم‌ترین فعالیت امنیتی و نظارتی شبکه پرداخت الکترونیکی کشور بیان شده است. بدین منظور، اقداماتی در زمینه‌های سیاست‌گذاری فنی و امنیت اطلاعات و هم‌چنین نظارت بر اجرا و نگهداری این چارچوب‌های الزامی در طی حدود دو سال گذشته در شاپرک صورت گرفت. نتایج کلی حاصل از این اقدامات، فارغ از بومی‌سازی و نهادینه کردن استانداردهای حوزه پرداخت در کشور، ارتقاء سطح انطباق شرکت‌ها با استانداردها از میزان متوسط ۳۹,۱ %به میزان ۹۶,۵ % را نشان می‌دهد.
در این مقاله، تجربه موفق دوساله شاپرک در حوزه سیاست‌گذاری، راهبری، و نظارت بر شبکه پرداخت الکترونیکی کشور بیان شده و علاوه بر ترسیم مسیر طی شده، به نتایج کیفی و کمی حاصله پرداخته می‌شود.

واژه‌های کلیدی: سیاست‌گذاری، نظارت، الزامات، انطباق

اهداف

به صورت کلی می‌توان اهداف کلان امنیتی و نظارتی شاپرک در بازار پرداخت الکترونیکی کارت را در موارد زیر خلاصه نمود:

- کاهش احتمال وقوع حوادث کلان امنیت اطلاعات (مانند پایداری سرویس یا محرمانگی اطلاعات)
- ارتقاء سطح امنیت اطلاعات
- ایجاد مرکزی واحد برای هماهنگی امنیت اطلاعات
- سامان‌دهی کیفیت خدمت از نگاه مشتری نهایی و افزایش رضایت‌مندی
- ارتقاء کارآیی و بهره‌وری خدمات شرکت‌های پرداخت (PSP)
- ایجاد یکپارچگی و وحدت رویه در عملیات و خدمات شرکت‌های پرداخت
- بهره‌وری مطلوب و حداکثری از منابع و سرمایه‌های کشور

اقدامات امنیتی و نظارتی صورت گرفته

در ابتدای تاسیس شاپرک، با بهره‌گیری از تجارب نخبگان حوزه پرداخت و بررسی شبکه‌های پرداخت بین‌المللی مانند ویزا، نقشه راهی به منظور نظارت بر شبکه پرداخت در شاپرک ترسیم شد که دو فعالیت اصلی آن، همانند آن‌چه در شبکه ویزا انجام می‌شود، ابلاغ الزامات و استانداردهای لازم و نظارت بر اجرای دقیق آن‌ها است. در این بخش، مراحل طی شده در این نقشه راه، تشریح خواهد شد.

مطالعه وضعیت موجود

به‌منظور تهیه الزامات فنی و امنیت اطلاعات و برنامه‌ریزی برای رفع مشکلات، در ابتدا باید مشکلات و نقاط آسیب‌پذیر و ضعف شبکه پرداخت الکترونیکی کارت در سطح کشور شناسایی می‌شد. در این خصوص، طی بررسی‌های صورت گرفته از شرکت‌های پرداخت و اخذ نظر صاحب‌نظران این حوزه، مسایل و مشکلات کلان ذیل، مشاهده شد:

- ضعف امنیت اطلاعات در سطح شبکه شرکت‌های پرداخت
- ضعف امنیت اطلاعات در حفاظت از داده‌های شرکت‌های پرداخت
- ضعف امنیتی سیستم‌ها و نرم‌افزارهای مرتبط با پرداخت کارت در شرکت‌های پرداخت
- ضعف ساختار و نیروی انسانی در زمینه‌های فنی و امنیت اطلاعات شرکت‌های پرداخت
- ضعف آموزش و آگاهی‌رسانی نیروی انسانی در زمینه‌های فنی و امنیت اطلاعات در شرکت‌های پرداخت
- ضعف مستندسازی و شفافیت فرآیندهای کلان شرکت‌های پرداخت
- عدم وجود برنامه مناسب در به‌کارگیری ابزارها و پایانه‌های فروش در شرکت‌های پرداخت و نیاز به سامان‌دهی
- فقدان تحلیل و آمار دقیق و صحیح از تراکنش‌های پرداخت
- عدم پیروی یکپارچه از استاندارد واحد در زمینه‌های فنی و امنیت اطلاعات در بازار پرداخت
- ضعف وحدت رویه در خصوص رعایت حداقل‌های مسایل حقوقی در قراردادها و تعاملات شرکت‌های پرداخت با بانک‌ها، شرکت‌های ثالث، پذیرندگان و مشتریان
- عدم شفافیت در رویه‌های تصدیق هویت و اهلیت نمایندگان شرکت‌های پرداخت و پذیرندگان خدمات مختلف آن‌ها

تدوین الزامات و مستندات

با توجه به مشاهدات انجام شده، شرکت شاپرک، حداقل‌های الزامات امنیت اطلاعات و فنی شبکه پرداخت را تدوین کرد. در این راستا، ابتدا قوانین و مقررات ابلاغی بانک مرکزی ج.ا.ا. مرتبط در نظام پرداخت مطالعه، و سپس استانداردهای مرتبط جهانی و تجارب دیگر کشورها مورد بررسی قرار گرفت. در نهایت، با بهره‌گیری از تجارب صاحب‌نظران و بررسی فنی وضعیت موجود و کارشناسی موضوعات تخصصی در کارگروه‌های تخصصی، چندین سند از جمله «الزامات امنیت اطلاعات شاپرک»، «الزامات فنی شاپرک»، «الزامات پذیرندگان»، «قوانین و مقررات رسید پایانه‌های فروش»، «قوانین و مقررات یکسان‌سازی منوی پایانه‌های فروش» و «قوانین و مقررات استفاده از نام و نشان تجاری شاپرک» تهیه شد تا کمینه چارچوب‌های امنیتی، فنی و اجرایی لازم که مبنایی برای انجام مسوولیت‌های شرکت‌های پرداخت است، فراهم شود.

در هر کدام از اسناد فوق، موضوعات مرتبط به تفصیل بیان شده است. به عنوان مثال، در سند «الزامات امنیت اطلاعات شاپرک»، الزامات برقراری و معیارهای سنجش امنیت اطلاعات در حوزه‌های مختلف فناوری اطلاعات در محدوده سازمان‌های فعال در زمینه خدمات الکترونیکی کارت در کشور ایران، ارایه شده است. امنیت اطلاعات در این سند، به برقراری سه عامل محرمانگی، صحت، و دسترسی‌پذیری سیستم‌ها و اطلاعات اشاره دارد و حوزه‌های مختلف فناوری اطلاعات تحت پوشش این سند، شبکه و ارتباطات، سامانه‌های عامل، پایگاه‌های‌داده‌ها، نرم‌افزارها (مانند سوییچ پرداخت)، داده‌ها و اطلاعات، حفاظت فیزیکی، کارکنان (منابع انسانی)، و فرآیندها است. الزامات و کنترل‌های ارایه شده در این سند، از منظر امنیتی با دو رویکرد فرآیندی و فنی تدوین شده است. در این سند، ابتدا با نگاه فرآیندی، چگونگی ایجاد و نگه‌داری سازمان و چرخه امنیت اطلاعات بیان شده و سپس کنترل‌های فنی برای رسیدن به اهداف این سند، تشریح شده است.

در سند «الزامات فنی شاپرک» و دیگر اسناد عنوان شده نیز، به صورت کلان، الزامات مرتبط با حوزه‌های زیرساختی، کیفیت ارایه خدمات، مشتری-مداری، استفاده بهینه از منابع، و مواردی از این دست، تدوین شده که رئوس کلی زمینه‌های آن عبات است از: مرکز داده، سوییچ و Back office، پایانه‌های فروش فیزیکی و مجازی، شبکه‌های ارتباطاتی، منابع انسانی، الزامات قراردادی، مرکز تماس و الزامات پذیرندگان.

وضعیت عمومی شرکت‌های پرداخت در ابتدای شاپرک

در انتهای سال ۱۳۹۱ و ابتدای سال ۱۳۹۲، یک مرحله ارزیابی کلی و بازرسی از شرکت ها بر مبنای الزامات تدوین شده صورت پذیرفت که در آن زمان به صورت متوسط، میزان انطباق شرکت‌ها با الزامات و مقررات، برابر ۳۹,۱ % ارزیابی شد. هم‌چنین میزان کمینه درصد انطباق در بین شرکت‌ها، برابر ۱۳,۳ % و مقدار بیشینه، برابر ۶۰,۷ %تعیین شد.

برگزاری جلسات و آموزش

پس از تدوین نسخ اسناد ذکر شده در شرکت شاپرک و پیش از ابلاغ به شرکت‌های پرداخت، ابتدا مفاد الزامات در طی جلساتی برای شرکت‌ها ارایه شده و در خصوص کاربردپذیری و امکان پیاده‌سازی آن‌ها، نظرات ایشان اخذ و در تدوین نسخ لازم‌الاجرا لحاظ شد. سپس این مستندات به تایید مقام مسئول در بانک مرکزی ج.ا.ا. (به‌طور مشخص: اداره نظام‌های پرداخت) رسید.

پیش از ابلاغ الزامات به شرکت‌ها، جلساتی در محل شرکت شاپرک و با حضور نمایندگان شرکت‌های پرداخت و بانک مرکزی، به منظور آموزش و رفع ابهامات در اجرای الزامات برگزار شد. الزامات فنی نیز، به‌همین روش، در قالب جلساتی برای شرکت‌ها تشریح، و نحوه اجرا و پیاده‌سازی آن‌ها به نحو مقتضی، ارایه شد.

ابلاغ و نظارت بر اجرای الزامات و مقررات

الزامات گفته شده از نیمه دوم سال ۱۳۹۱ به تدریج به شرکت ها ابلاغ، و پیاده‌سازی آن‌ها در شرکت‌های پرداخت از زمان ابلاغ آغاز شد. در این راستا با توجه به این که شرکت‌های پرداخت الکترونیکی کارت، دارای مجوزهای فعالیت دایمی از جانب بانک مرکزی ج.ا.ا. نیستند، پس از انجام مطالعات و شناخت اولیه از وضعیت موجود و مشاهده مشکلات متعدد ذکر شده در این شرکت‌ها، با نظر بانک مرکزی ج.ا.ا.، برنامه‌ای گام‌به‌گام برای انطباق شرکت‌ها با الزامات شاپرک تهیه و در اختیار شرکت‌ها قرار گرفت تا متناسب با آن به شرکت‌ها در چند مرحله مجوز موقت فعالیت ارایه شده، و در هر مرحله، برای اخذ مجوز بعدی، شرکت موظف به انطباق با بخشی از الزامات ابلاغ شده باشد. بدین ترتیب پس از ابلاغ الزامات، ابتدا بازه زمان سه ماهه برای اجرای بخشی از الزامات به شرکت‌ها داده شد تا در اردیبهشت ۱۳۹۲، اولین بازرسی جامع از شرکت‌ها صورت پذیرد. در این مرحله از بازرسی، شرکت‌ها بر حسب میزان انطباق خود با الزامات، توانستند مجوز فعالیت سه یا شش ماهه کسب کنند. پس از آن، هر سه ماه شرکت‌ها مورد ارزیابی جامع قرار گرفته و با کسب امتیاز در اجرای حداقل‌های لازم ابلاغی، هر شرکت توانست مجوز سه ماهه بعدی را نیز کسب کند.

دوره دوم این ارزیابی، آبان ماه سال ۱۳۹۲ بوده و در انتهای سال جاری نیز، ارزیابی جامعی از کلیه الزامات صورت خواهد گرفت و شرکت‌های دارای امتیاز بیش از ۹۵ (از ۱۰۰ امتیاز)، برای تمدید مجوز بلند مدت به بانک مرکزی پیشنهاد خواهند شد. البته پس از آن، کماکان تمامی بازرسی‌ها و ارزیابی‌ها به صورت مداوم صورت گرفته و در صورت عدم انطباق شرکتی با الزامات در این بازه زمانی سه ساله، امکان کاهش رتبه شرکت مذبور و احیاناً لغو مجوز آن وجود خواهد داشت.

به منظور تعیین رتبه شرکت‌ها و مقایسه آن‌ها با وضعیت مطلوب، شاخصهای کلی ذیل برای ارزیابی در نظر گرفته شد:

- کارکرد عملیاتی
  - کارآیی پایانه‌های فروش
  - کیفیت خدمات و میزان موفقیت تراکنش‌ها
  - دسترسی‌پذیری سرور
- الزامات فنی و امنیت
  - الزامات مرکز تماس
  - الزامات زیرساخت مرکز داده
  - الزامات پایش عملکرد سامانه‌ها
  - الزامات سوییچ پرداخت
  - الزامات فرآیندها و روال‌های عملیاتی
  - الزامات قراردادی
  - الزامات پایانه‌های فروش
  - الزامات امنیت اطلاعات (شامل شبکه، داده، سیستم‌ها، کنترل دسترسی، امنیت فیزیکی، و فرآیندهای امنیتی)
- برنامه‌های اجرایی
  - پالایش و تدقیق اطلاعات پذیرندگان
  - الزامات رسیدگی و نگهداری پایانه‌های فروش

البته به منظور بازرسی و صحت‌سنجی این موارد، لیست‌های کنترلی با حدود ۶۰۰ قلم قابل بررسی در شاپرک، تهیه و به تیمی مجرب برای این ارزیابی‌ها آموزش داده شده است.

نتایج، جمع‌بندی، و فعالیت‌های آتی

نتایج کیفی بهبود وضعیت

در خصوص نتایج فعالیت‌های نظارتی و امنیتی شاپرک به صورت کلی، می‌توان گفت در زمینه‌های زیر در هر یک از شرکت‌های پرداخت، بهبودهای قابل ملاحظه‌ای ایجاد شده است:

- امنیت شبکه، شامل امنیت کانال‌های ارتباطاتی، تشخیص نفوذ، پیگیری جرم، و امنیت ارتباطات راه دور
- امنیت داده و سیستم، شامل امنیت اطلاعات کارت، امنیت سیستم‌های عامل، امنیت نرم‌افزارها، کنترل دسترسی، و حساب‌های کاربری
- مدیریت کلید کلیدهای رمزنگاری و رعایت محرمانگی اطلاعات کارت و حساب مشتریان
- مرکز تماس، که موجب افزایش رضایت‌مندی مشتریان، ارتقاء سطح اعتماد عمومی به شبکه پرداخت، و افزایش سرعت در انجام پیگیری مطالبات و ارایه خدمات به تماس مشتریان شده است
- سوییچ پرداخت، که موجب افزایش بهره‌وری، کارایی، امنیت و سطح کیفی خدمات شده است
- ابزارهای پذیرش پذیرش
- نیروی انسانی شرکت‌ها، در راستای افزایش ضریب تخصصی و عملکرد پرسنل شرکت‌ها و آموزش‌های امنیتی
- مرکز داده، که موجب افزایش بهره‌وری، کارایی، امنیت و سطح کیفی خدمات شده
- پایش، به‌منظور پایش مستمر، برای بهبود خدمات پرداخت کشور و کمک به افزایش سطح کیفی خدمات شبکه پرداخت
- قراردادها، در راستای اعمال قوانین و مقررات بانک مرکزی بر قراردادها
- فرآیندهای حوزه‌های عملیاتی

نتایج کمّی بهبود وضعیت

در زمان نگارش این مقاله بر اساس بازرسی صورت گرفته از شرکت‌ها بر مبنای الزامات تدوین شده، به صورت متوسط، میزان انطباق شرکت‌ها با الزامات و مقررات، برابر ۹۶,۵ % است. هم‌چنین میزان کمینه درصد انطباق بین شرکت‌ها، برابر ۹۲,۲ % و مقدار بیشینه آن، برابر ۹۹,۲ % است.

از اینکه با بخش پشتیبانی فنی تماس گرفته‌اید متشکرم، صحبت‌های شما برای اینکه بعداً پیش همکاران پخش کنیم و بخندیم ضبط خواهد شد.

معرفی استاندارد ۳۸۵۰۰: راهبری سازمانی فناوری اطلاعات

سیدعلی آذرکار
شرکت مهندسی پدیدپرداز
کمیسیون استاندارد و تدوین مقررات، سازمان نظام صنفی رایانه‌ای استان تهران
پست الکترونیکی: ali.azarkar@pdpsoft.com

۱- مقدمه

امروزه فناوری اطلاعات تمامی زیرساخت‌های کسب‌وکاری سازمان‌ها را دستخوش تحولات و تغییرات بنیادین کرده است. پیچیدگی‌های کسب‌وکارهای جدید و نیاز به دقت و سرعت در انجام و ارایه خدمات و محصولات، استفاده از این فناوری را اجتناب‌ناپذیر کرده است. از سوی دیگر، تجربه چند دهه اخیر نشان داده که به‌کارگیری این فناوری، مفاهیم پایه‌ای مانند آموزش، خدمت، محصول و امثالهم را نیز مشمول بازنگری و بازتعریف کرده است.

سازمان‌ها در سال‌های اخیر، برای بهره‌گیری از قابلیت‌های فناوری اطلاعات، برای توسعه کسب‌وکار خود، سرمایه‌گذاری‌های گسترده و زیادی انجام داده و در نیل به اهداف خود هم موفق بوده‌اند. امّا معمولاً این سرمایه‌گذاری‌ها به صورت موردی یا حوزه‌ای بوده و نوعاً سازمان‌ها را در بلند مدت با طیف گسترده‌ای از سامانه‌ها و زیرساخت‌های فناوری اطلاعات مواجه کرده که گاه با یکدیگر در تعارض بوده‌اند. به‌علاوه، سرمایه‌گذاری هم توسط سازمان‌ها در زمینه توسعه به‌کارگیری فناوری اطلاعات انجام شده که به دلایلی مانند عدم هم‌سویی با کسب‌وکار و یا عدم تحقق سود و فایده‌ی پیش‌بینی شده، موفقیتی را از آن خود نکرده است.

هنگامی که توسعه فناوری اطلاعات، اگر چه با موفقیت همراه باشد، نتواند سرمایه‌گذاری‌های انجام شده را در حصول فواید کسب‌وکاری پیش‌بینی شده عینیت بخشد، موضوع در سطح دیگری از سازمان، یعنی هدایت‌کنندگان آن (مدیر عامل، هیئت‌مدیره، مدیران ارشد، سهام‌داران، ذی‌نفعان و غیره)، مطرح می‌شود. سوال مشخص آن‌ها این است که اصولاً در چه حوزه‌هایی از کسب‌وکار سازمان باید از فناوری اطلاعات استفاده کرد؟ چه عواملی متضمن سودآوری و بهبود سازمان، در صورت استفاده از فناوری اطلاعات است؟ چه میزان باید در توسعه فناوری اطلاعات سرمایه‌گذاری کرد؟ سرمایه‌گذاری‌های قبلی، چه اثری بر کسب‌وکار سازمان گذاشته است؟ چگونه باید فناوری‌های نوین اطلاعاتی و ارتباطی را در مسیر تعالی و پیشرفت سازمان به‌کار گرفت؟

پاسخ سوالاتی از این دست، شکل‌گیری موضوعی تحت عنوان «حاکمیت» (Governance) یا «راهبری» فناوری اطلاعات در سازمان را شکل داده است. سطح طرح و بررسی این موضوع به‌طور کلی، مدیریت ارشد و تصمیم‌ساز سازمان بوده و فراتر از موضوعات «فنی»، مانند مدیریت و اجرای یک پروژه خاص فناوری اطلاعات است.

با توجه به مقدمه کوتاه فوق، و هم‌چنین موضوع کلی مقالات این شماره که مرتبط با «ممیزی فناوری اطلاعات» (که خود در حوزه مفاهیم راهبری فناوری اطلاعات جای دارد) است، در ادامه استاندارد بین‌المللی ISO/IEC 38500:2008 (با عنوان «راهبری سازمانی فناوری اطلاعات» (اختصاراً: «استاندارد») معرفی، و به اجمال بررسی خواهد شد.

این استاندارد، یک استاندارد سطح بالا (مدیریتی)، مشاوره‌ای، و مبتنی بر اصول است که علاوه بر این‌که راهنماهایی در خصوص نقش بدنه راهبری به مدیریت سازمان ارایه می‌دهد، توجه آن‌ها را به به‌کارگیری استانداردهای مناسب و ویژه راهبری فناوری اطلاعات جلب می‌کند.

این اولین استانداردی است که توسط سازمان ایزو در خصوص مقوله راهبری فناوری اطلاعات تدوین شده است. مانند سایر استانداردهای

بررسی شده در قبل، توسعه و نگهداری این استاندارد بر عهده JTC1 است. این استانداردتلاش دارد که موضوعات مهم این حوزه را مورد اشاره قرار داده و بستری را برای توسعه‌های آتی و تبیین دقیق‌تر موضوع فراهم کند. از زمان انتشار نسخه اولیه این استاندارد در سال ۲۰۰۸، JTC1 تلاش‌های زیادی را برای استانداردسازی بیشتر این موضوع انجام داده، که بازنگری این استاندارد و توسعه دو استاندارد مرتبط، از جمله این فعالیت‌ها است.

۲- مشخصات

مشخصات این استاندارد در جدول شماره ۱ نشان داده شده است.

جدول ۱: مشخصات استاندارد

شماره:	۳۸۵۰۰
قسمت:	-
نوع سند:	استاندارد بین‌المللی
عنوان لاتین:	Corporate governance of information technology
عنوان فارسی:	راهبری سازمانی فناوری اطلاعات
تعداد صفحات:	۱۵
سال چاپ:	۲۰۰۸
زبان:	تک زبانه، انگلیسی
شماره ویرایش:	ندارد
متمم و اصلاحیه:	ندارد
استاندارد(های) جایگزین شده:	ندارد
کد رده‌بندی استانداردی (ICS):	۳۵،۰۸۰
نهاد استانداردگذار:	ایزو
شماره استاندارد معادل فارسی:	۱۲۰۴۷ (عنوان: راهبری سازمانی فناوری اطلاعات)
ناشر استاندارد فارسی:	سازمان ملی استاندارد ایران
سال چاپ:	۱۳۸۸
شماره ویرایش:	۱
تعداد صفحات:	۱۹

۳- ساختار

این استاندارد دارای بخش‌های زیر است:

- بند ۱: محدوده، کاربرد، و اهداف
- بند ۲: چارچوبی برای راهبری خوب فناوری اطلاعات
- بند ۳: راهنمایی برای راهبری فناوری اطلاعات

۴- سیر تکامل استاندارد

شالوده این استاندارد، مبتنی بر استاندارد AS8015 بوده که در سال ۲۰۰۵ توسط نهاد ملی استانداردگذار استرالیا، تدوین شد. این استاندارد در سال ۲۰۰۸ و پس از اقتباس توسط ایزو (مشخصاً JTC1)، با شماره ۳۸۵۰۰ منتشر شد. این استاندارد هم‌اکنون در دست بازنگری است.

۵- موضوع و هدف

هدف این استاندارد ارایه چارچوبی از استانداردها برای مدیریت ارشد برای استفاده در هنگام ارزیابی، هدایت، و پایش استفاده از فناوری اطلاعات در سازمان آن‌ها است. سرمایه‌گذاری در فناوری اطلاعات می‌تواند نشان‌گر بخش مهمی از سرمایه‌گذاری سازمان در حوزه‌های مالی و منابع انسانی باشد. به‌هرحال، بازگشت این سرمایه گاهی به‌درستی محقق نشده و تاثیرات آن می‌تواند قابل توجه باشد.

به‌طور کلی، هدف این استاندارد، ارتقای اثربخش، کارا، و قابل پذیرش استفاده از فناوری اطلاعات در تمامی سازمان‌ها، از طرق زیر، است:

- حصول اطمینان به ذی‌نفعان (مشتریان، سهام‌داران، و کارکنان) از این‌که می‌توانند به راهبری فناوری اطلاعات در سازمان اعتماد داشته باشند،
- اطلاع‌رسانی و راهنمایی مدیریت ارشد در خصوص راهبری استفاده از فناوری اطلاعات در سازمان آن‌ها، و
- ارایه مأخذی برای ارزیابی عینی راهبری سازمانی فناوری اطلاعات

این استاندارد چارچوبی را برای راهبری «اثربخش» فناوری اطلاعات، با هدف کمک به مدیریت ارشد در زمینه درک و تحقق تعهدات مقرراتی، اهلاقی، و حقوقی آن‌ها نسبت به استفاده سازمان متبوع از فناوری اطلاعات ارایه می‌دهد. چارچوبی که توسط این استاندارد پیشنهاد و ارایه شده، مشتمل بر تعاریف، اصول، و یک مدل است. نکته دیگر این‌که، این استاندارد راهنمایی را برای افرادی که به مدیران مشاوره داده و یا به آن‌ها اطلاع‌رسانی می‌کنند نیز فراهم می‌کند. این افراد می‌توانند شامل موارد زیر باشد:

- مدیریت ارشد
- افرادی که منابع سازمانی را پایش می‌کنند
- متخصصین خارجی کسب‌وکار یا فنی
- ارایه‌دهندگان سخت‌افزار، نرم‌افزار، و سایر محصولات فناوری اطلاعات
- ارایه‌دهندگان داخلی و خارجی خدمات (مانند مشاورین)
- ممیزین فناوری اطلاعات

این استاندارد تاکید می‌کند که راهبری مناسب سازمانی فناوری اطلاعات به مدیریت ارشد کمک خواهد کرد تا اطمینان حاصل کند فناوری اطلاعات به شکل مثبت و سازنده‌ای در ارتقای کارایی سازمان، از طریق روش‌های زیر، مشارکت دارد:

- پیاده‌سازی و عملیات مناسب سرمایه‌های فناوری اطلاعات
- ایجاد شفافیت در مسئولیت و پاسخ‌گویی، هم برای به‌کارگیری و هم برای پیش‌بینی نقش فناوری اطلاعات در تحقق اهداف سازمان

- استمرار و پایداری کسب‌وکار
- هم‌سویی فناوری اطلاعات با نیازهای کسب‌وکاری
- تخصیص اثربخش منابع
- توآوری در خدمات، بازارها، و کسب‌وکار
- تجارب برتر در ارتباط و تعامل با ذی‌نفعان
- کاهش هزینه‌های سازمان
- تحقق واقعی فواید اثبات شده از هر سرمایه‌گذاری فناوری اطلاعات

۶- چارچوب راهبری خوب سازمانی فناوری اطلاعات

این استاندارد ۶ اصل را برای راهبری خوب سازمانی فناوری اطلاعات، که قابل استفاده توسط تمامی سازمان‌ها است، ارایه می‌کند. این اصول، رفتار «برتر» برای هدایت تصمیم‌گیری را تصریح و تاکید می‌کند. مانند هر استاندارد دیگری، این اصول آن‌چه را که باید رخ دهد تبیین کرده، ولی به نحوه و چگونگی پیاده‌سازی آن‌ها اشاره‌ای نمی‌کند. باید توجه داشت که این اصول با یک‌دیگر در ارتباط بوده و به همین دلیل پیاده‌سازی هر کدام باید با درک تبعات آن بر سایر اصول، مورد توجه قرار گیرد.

۶-۱- مسئولیت

افراد و گروه‌ها در سازمان مسئولیت خود را در قبال هم تامین و هم درخواست فناوری اطلاعات درک کرده و پذیرفته‌اند. افرادی که مسئولیت اجرایی دارند، دارای صلاحیت لازم برای اقدامات پیش‌بینی شده هستند.

۶-۲- راهبرد

راهبرد کسب‌وکار سازمان، قابلیت‌های فعلی و آتی فناوری اطلاعات را مد نظر قرار می‌دهد. طرح‌های راهبردی فناوری اطلاعات، نیازهای فعل و آینده راهبرد کسب‌وکار سازمان را محقق می‌کند.

۶-۳- اکتساب

اکتساب(ها) یا خریدهای فناوری اطلاعات برای دلایل معتبر، بر مبنای تحلیل‌های مناسب و جاری و طی یک فرآیند روشن و شفاف تصمیم‌گیری، انجام می‌شود. تعادل مناسبی بین فواید، فرصت‌ها، هزینه‌ها، و مخاطرات، هم در کوتاه مدت و هم در بلند مدت، وجود دارد.

۶-۴- کارایی

فناوری اطلاعات با هدف پشتیبانی سازمان، ارایه خدمات، سطوح خدمات، و کیفیت خدمات مورد نیاز، برای تحقق نیازمندی‌های حال حاضر و آینده کسب‌وکاری مناسب‌سازی شده است.

۶-۵- سازگاری

فناوری اطلاعات به همه قوانین و مقررات اجباری منطبق و سازگار است. سیاست‌ها و تجارب به روشنی تعریف، پیاده‌سازی، و الزام می‌شود.

۶-۶- رفتار انسانی

سیاست‌ها، تجارب، و تصمیم‌گیری‌ها، حاکی از احترام به رفتار انسانی، شامل نیارهای جاری و در حال تکوین همه افراد درگیر در فرآیند، است.

۷- مدل پیشنهادی

مدیریت ارشد می‌تواند فناوری اطلاعات را از طریق سه فعالیت اصلی زیر «راهبری» کند:

- «ارزیابی» استفاده فعلی و آتی فناوری اطلاعات
- «هدایت» آماده‌سازی و پیاده‌سازی طرح‌ها و سیاست‌ها، با هدف حصول اطمینان از این‌که به‌کارگیری فناوری اطلاعات اهداف کسب‌وکار را محقق و برآورده می‌سازد.
- «پایش» سازگاری سیاست‌ها و کارایی در مقایسه با طرح‌ها

این مدل و تعامل آن با سایر عوامل سازمانی، در شکل ۱ نشان داده شده است.

۷-۱- ارزیابی

موضوعات مهمی که باید در حوزه «ارزیابی» مورد توجه قرار گیرد، عبارت است از:

- الزام مدیریت به بررسی و قضاوت در خصوص استفاده‌های جاری و آتی از فناوری اطلاعات (شامل راهبردها و پیشنهادها)، و تامین تدارکات لازم (چه داخلی و چه خارجی)
- لحاظ کردن فشارهای داخلی و خارجی بر روی کسب‌وکار (مانند تغییرات فناوری، شرایط اقتصادی، روندهای اجتماعی، تاثیرات سیاسی)، در زمان ارزیابی به‌کارگیری فناوری اطلاعات
- تعهد مدیریت به ارزیابی مستمر، هم‌زمان با تغییر فشارها
- لحاظ کردن نیارهای فعلی و آینده کسب‌وکاری، اهداف جاری و آتی سازمانی، توسط مدیریت ارشد

۷-۲- هدایت

موضوعات مهمی که باید در حوزه «هدایت» مورد توجه قرار گیرد، عبارت است از:

- تفویض مسئولیت‌ها و هدایت آماده‌سازی و پیاده‌سازی طرح‌ها و سیاست‌ها
- حصول اطمینان مدیریت ارشد از گذار طرح‌ریزی شده و برنامه‌ریزی شده پروژه‌ها به وضعیت عملیاتی، با لحاظ کردن اثرات آن بر کسب‌وکار، تجارب عملیاتی، و زیرساخت و سامانه‌های موجود فناوری اطلاعات
- تشویق یک فرهنگ خوب راهبری سازمانی فناوری اطلاعات در

سازمان، توسط مدیریت ارشد، از طریق درخواست از مدیران برای ارایه اطلاعات به‌موقع، و هم‌چنین سازگاری و هم‌سویی با اصول ۶ گانه راهبری خوب
- هدایت پذیرش پیشنهادها برای تصویب، با هدف رفع نیازهای شناسایی شده

۷-۳- پایش

موضوعات مهمی که باید در حوزه «پایش» مورد توجه قرار گیرد، عبارت است از:
- پایش کارایی فناوری اطلاعات، از طریق سامانه‌های مناسب اندازه‌گیری
- حصول اطمینان از سازگاری کارایی با طرح‌ها، به‌ویژه نسبت به اهداف کسب‌وکاری
- حصول اطمینان از سازگاری فناوری اطلاعات با تعهدات خارجی (قوانین عمومی، قراردادها، مقررات، و امثالهم) و هم‌چنین تجارب کاری داخلی

۸- فعالیت‌های مربوط به اصول ۶ گانه

این استاندارد، برای تشریح دقیق‌تر چارچوب پیشنهادی، تلاش کرده تا فعالیت‌هایی جزیی را که در قالب فعالیت‌های کلی ۳ گانه (ارزیابی، هدایت، و پایش)، باید برای هر یک از اصول ۶ گانه (مسئولیت، راهبرد، اکتساب، کارایی، سازگاری، و رفتار انسانی) انجام شود را بیان می‌کند. این‌ها در واقع وظایفی که در حوزه‌های مختلف بر عهده مدیریت ارشد گذاشته شده است.

۸-۱- فعالیت‌های مربوط به اصل «مسئولیت»

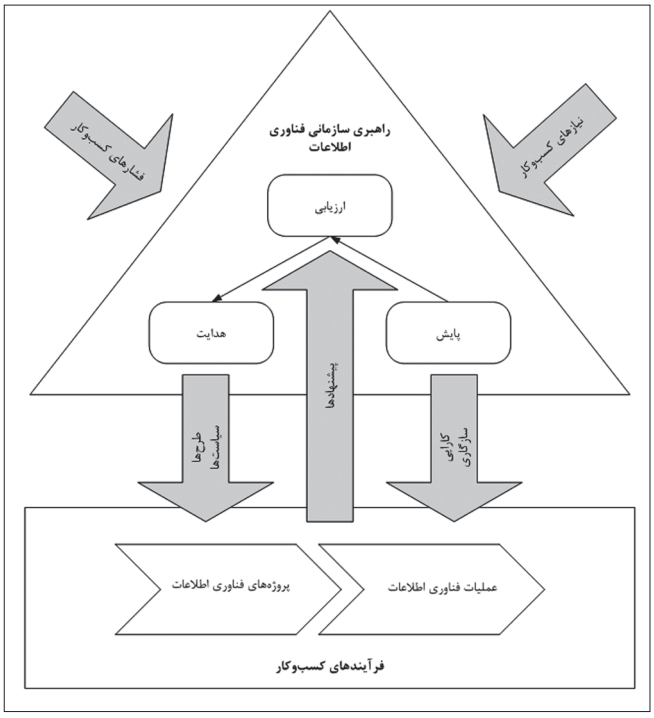
فعالیت‌هایی که باید در زمینه «ارزیابی» انجام شود، به شرح زیر است:
- ارزیابی انتخاب‌ها برای تفویض مسئولیت‌ها
- ارزیابی صلاحیت افرادی که به آن‌ها مسئولیت تصمیم‌گیری در حوزه فناوری اطلاعات داده شده

فعالیت‌هایی که باید در زمینه «هدایت» انجام شود، به شرح زیر است:
- هدایت انجام طرح‌های، طبق مسئولیت‌های اختصاص داده شده در فناوری اطلاعات
- هدایت دریافت اطلاعات مورد نیاز برای مسئولیت‌ها و پاسخ‌گویی‌ها

فعالیت‌هایی که باید در زمینه «پایش» انجام شود، به شرح زیر است:
- پایش ایجاد سازوکارهای مناسب راهبری فناوری اطلاعات
- پایش درک درست از مسئولیت‌های واگذار شده
- پایش کارایی افرادی که به آن‌ها در حوزه فناوری اطلاعاتی مسئولیتی داده شده

۸-۲- فعالیت‌های مربوط به اصل «راهبرد»

فعالیت‌هایی که باید در زمینه «ارزیابی» انجام شود، به شرح زیر است:



شکل ۱: مدل راهبری خوب فناوری اطلاعات

- ارزیابی توسعه در فناوری اطلاعات و فرآیندهای کسب‌وکاری، با هدف حصول اطمینان از پشتیبانی نیازهای آتی کسب‌وکاری توسط فناوری اطلاعات
- حصول اطمینان از کاربرد فناوری اطلاعات، همراه با ارزیابی مخاطرات وابسته

فعالیت‌هایی که باید در زمینه «هدایت» انجام شود، به شرح زیر است:
- هدایت آماده‌سازی و استفاده از طرح‌ها و سیاست‌هایی که اطمینان می‌دهد سازمان از توسعه‌های فناوری اطلاعات بهره‌مند خواهد شد.
- تشویق ارسال پیشنهادها برای استفاده نوآوران از فناوری اطلاعات، با هدف توان‌مندسازی سازمان در پاسخ به فرصت‌های جدید کسب‌وکار
- فعالیت‌هایی که باید در زمینه «پایش» انجام شود، به شرح زیر است:
- پایش پیشرفت پیشنهادهای مصوب فناوری اطلاعات، برای حصول اطمینان از تحقق اهداف در طرف زمانی مورد نیاز و منابع اختصاص یافته
- پایش به‌کارگیری فناوری اطلاعات، با هدف حصول اطمینان از تحقق فواید مورد نظر

۸-۳- فعالیت‌های مربوط به اصل «اکتساب»

فعالیت‌هایی که باید در زمینه «ارزیابی» انجام شود، به شرح زیر است:
- ارزیابی انتخاب‌ها برای تدارک فناوری اطلاعات با هدف تحقق پیشنهادهای مطلوب

فعالیت‌هایی که باید در زمینه «هدایت» انجام شود، به شرح زیر است:
- هدایت اکتساب سرمایه‌های فناوری اطلاعات در مسیر و روش مناسب
- هدایت تامین تدارکات لازم به منظور پشتیبانی نیازهای کسب‌وکاری سازمان

فعالیت‌هایی که باید در زمینه «پایش» انجام شود، به شرح زیر است:
- پایش سرمایه‌گذاری‌های فناوری اطلاعات، با هدف اطمینان از تدارک قابلیت‌های مورد نیاز
- پایش گستره درک مشترک سازمان و تامین‌کنندگان از قصد سازمان در به‌کارگیری هر اکتساب فناوری اطلاعات

۸-۴- فعالیت‌های مربوط به اصل «کارایی»

فعالیت‌هایی که باید در زمینه «ارزیابی» انجام شود، به شرح زیر است:
- ارزیابی ابزارهای پیشنهادی مدیران برای حصول اطمینان از پشتیبانی توانایی‌ها و ظرفیت‌های مورد نیاز توسط فناوری اطلاعات
- ارزیابی مخاطرات یکپارچگی اطلاعات و حفاظت سرمایه‌های فناوری اطلاعات(شامل سرمایه‌های معنوی)
- ارزیابی انتخاب‌ها برای اطمینان از تصمیم‌های اثربخش و بموقع، درباره به‌کارگیری فناوری اطلاعات در پشتیبانی از اهداف کسب‌وکار
- ارزیابی مستمر اثربخشی و کارایی سامانه سازمان برای راهبری فناوری اطلاعات

فعالیت‌هایی که باید در زمینه «هدایت» انجام شود، به شرح زیر است:
- حصول اطمینان از اختصاص منابع لازم برای تحقق نیازهای سازمان توسط فناوری اطلاعات، طبق اولویت‌ها و محدودیت‌های بودجه‌ای
- ارزیابی افراد مسئول، به‌منظور حصول اطمینان از پشتیبانی کسب‌وکار توسط فناوری اطلاعات

فعالیت‌هایی که باید در زمینه «پایش» انجام شود، به شرح زیر است:
- پایش گستره‌ای که فناوری اطلاعات می‌تواند کسب‌وکار را پشتیبانی کند.
- پایش گستره‌ای که منابع اختصاص یافته و بودجه‌ها، طبق اهداف کسب‌وکاری اولویت‌بندی شده است.
- پایش گستره‌ای که سیاست‌ها به‌درستی دنبال و تبعیت می‌شود.

۸-۵- فعالیت‌های مربوط به اصل «سازگاری»

فعالیت‌هایی که باید در زمینه «ارزیابی» انجام شود، به شرح زیر است:
- ارزیابی مستمر گستره‌ای که فناوری اطلاعات تعهدات (حقوقی، قراردادی، مقرراتی، و ...) سیاست‌های داخلی، استانداردها، و راهنماهای داخلی را محقق می‌کند.
- ارزیابی مستمر انطباق داخلی سازمان با سامانه راهبری فناوری اطلاعات آن

فعالیت‌هایی که باید در زمینه «هدایت» انجام شود، به شرح زیر است:
هدایت افراد مسئول برای ایجاد سازوکارهای مرتب و منظم به‌منظور حصول اطمینان از انطباق فناوری اطلاعات با تعهدات (حقوقی، قراردادی، مقرراتی، و ...) سیاست‌های داخلی، استانداردها، و راهنماهای داخلی
- هدایت ایجاد و الزام سیاست‌ها به‌منظور توان‌مندسازی سازمان برای تحقق تعهدات در به‌کارگیری فناوری اطلاعات
- هدایت افراد فناوری اطلاعات به‌منظور تبعیت از راهنماها برای رفتار حرفه‌ای و توسعه‌های تخصصی
- هدایت اقدامات مرتبط با فناوری اطلاعات، به نحوی که اخلاق‌مدارانه باشد.

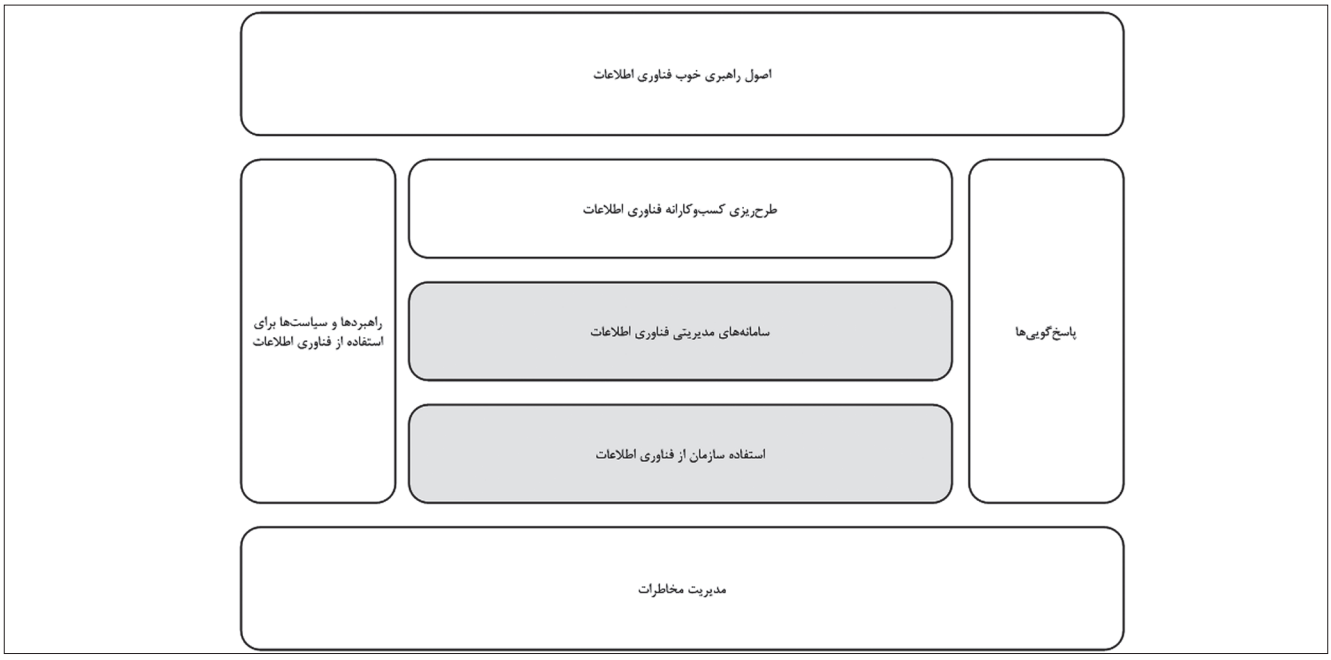
فعالیت‌هایی که باید در زمینه «پایش» انجام شود، به شرح زیر است:
- پایش سازگاری و انطباق فناوری اطلاعات، از طریق فعالیت‌های ممیزی و گزارش‌گیری
- پایش فعالیت‌های فناوری اطلاعات

۸-۶- فعالیت‌های مربوط به اصل «رفتار انسانی»

فعالیت‌هایی که باید در زمینه «ارزیابی» انجام شود، به شرح زیر است:
- ارزیابی فعالیت‌های فناوری اطلاعات، با هدف حصول اطمینان از این‌که رفتارهای انسانی شناسایی، و به‌درستی لحاظ شده است.
- فعالیت‌هایی که باید در زمینه «هدایت» انجام شود، به شرح زیر است:
- هدایت فعالیت‌های فناوری اطلاعات به نحوی که سازگار با رفتارهای شناسایی شده انسانی باشد.
- هدایت مخاطرات، فرصت‌ها، موضوعات، و نگرانی‌ها، به‌نحوی که شناسایی شده و به فرد در هر زمانی گزارش شود.
- فعالیت‌هایی که باید در زمینه «پایش» انجام شود، به شرح زیر است:
- پایش فعالیت‌های فناوری اطلاعات با هدف حصول اطمینان از این‌که رفتارهای شناسایی شده انسانی به شکل مرتبطی باقی‌مانده، و توجه لازم به آن‌ها شده است.
- پایش تجارب کاری، با هدف حصول اطمینان از سازگاری آن‌ها با استفاده مناسب از فناوری اطلاعات

۹- سایر استانداردهای مرتبط

همان‌گونه که در ابتدا اشاره شد، این استاندارد فقط کلیاتی را از موضوع راهبری سازمانی فناوری اطلاعات بیان کرده است. اهمیت موضوع، تلاش بیشتری را می‌طلبید و به همین دلیل ایزو (JTC1) فعالیت‌های گسترده‌تری را در این خصوص شروع کرده و در دست انجام دارد. در



شکل ۲: اجزای کلیدی یک چارچوب راهبری برای فناوری اطلاعات

ادامه سعی شده کلیات این فعالیت‌ها به اجمال ارایه شود.

۱- از ابتـدای سـال گذشـته میلادی، و بـا توجه بـه اهمیت یافتن موضوعات حوزه راهبری فناوری اطلاعات و هم‌چنین مدیریت خدمات فناوری اطلاعات، فعالیت‌های مرتبط با این موضوعات در کمیته فرعی جدیدالتاسیس ۴۰ (در ساختار JTC1) شکل گرفت. دبیری این کمیته فرعی بر عهده کشـور استرالیا اسـت که دارای سوابق موفقی در این حوزه (مانند تدوین استاندارد AS8015) است.

۲- اسـتاندارد ۳۸۵۰۰ که به اجمال بررسی شـد، از سال ۲۰۱۲ در فرآیند بازنگری قرار گرفته اسـت. نسخ موقت این استاندارد حاکی از آن است که موضوع جدید و شاخصی به آن اضافه نشده است. انتظار می‌رود نسخه جدید این استاندارد در سال ۲۰۱۵ ارایه شود.

۳- در گـزارش فنـی ISO/IEC TR 38502:2014 (بـا عنوان: «فناوری اطلاعات-راهبـری فناوری اطلاعات-چارچوب و مدل»)، تلاش بر این است که مدل ارایه شده در استاندارد ۳۸۵۰۰ با تفصیل بیشتری ارایه شـود. در این گزارش فنی، اجزای کلیدی یک چارچوب راهبری برای فناوری اطلاعات (آن‌گونه که در شـکل ۲ نمایش داده شـده)، تبیین شود. این گزارش فنی در ژانویه سال ۲۰۱۴ رسماً منتشر شد.

۴- مشـخصه فنـی ISO/IEC 38501 (با عنوان: «فنـاوری اطلاعات-راهنمای پیاده‌سـازی راهبری فناوری اطلاعات») نیز توسط JTC1 در دسـت تهیه است. این سـند می‌تواند مکمل دو سند قبلی باشد. این سـند مراحل توسعه خود را می‌گذراند و پیش‌بینی می‌شود در ژانویه سال ۲۰۱۶ منتشر شود.

۱۰- راهبری فناوری اطلاعات در سطح ملی

ذکر این نکته پایانی مهم اسـت که موضوع راهبری فناوری اطلاعات مختص سـازمان‌ها نیست، بلکه در سـطح ملی و کشوری هم مطرح است. واضح است که طرح موضوع در سطح ملی پیچیدگی‌های بسیار بیشـتری داشـته و گسـتردگی آن قابل قیاس با «سـطح سازمانی» نیسـت؛ اگر چه مواردی که در این اسـتاندارد به آن اشاره شده قطعاً با دامنه گسـترده‌ای برای یک کشـور هم می‌تواند صادق باشـد. در خصوص راهبری ملی فناوری اطلاعات استانداردی منتشر نشده (چرا که در حوزه فعالیت‌های ایزو نیست) و کشورها هر کدام حسب شرایط و نیازهـای خود، طرح‌ها و برنامه‌هایی را برای پیاده‌سـازی آن ایجاد کرده‌اند.

۱۱- جمع‌بندی

در این شماره، به بررسـی اجمالی استاندارد ISO/IEC 38500:2008 (با عنـوان: «راهبری سـازمانی فناوری اطلاعات») پرداخته شـد. فلسـفه و موضوع این استاندارد، نحوه و شرایط به‌کارگیری فناوری اطلاعات در سـطح سـازمان‌ها، با هدف دستیبانی سـریع‌تر آن به اهداف کسـب‌وکاری است. مخاطب این اسـتاندارد مدیران ارشد و تصمیم‌ساز (و نه مدیران فنی) سـازمان است. این استاندارد حالت مشـاوره‌ای و راهنمایی داشـته و تلاش دارد بسـتری را (بر مبنای اصول، و فعالیت‌های مرتبط) برای ایجاد ساختاری با هدف استفاده اثربخش از فناوری اطلاعات در سازمان تبیین کند.

ایـن اسـتاندارد هنوز در مراحـل اولیه خود از حیث شـکل‌گیری محتوایی اسـت و به همین دلیل سازمان ایزو پس از ارایه و انتشار نسـخه اولیه آن در سـال ۲۰۰۸، اقدام به توسـعه اسـناد مکمل (گزارش فنی/مشـخصه فنی) برای تدقیق و کاوش بیشـتر موضوع کرده است.

قابل توجه اعضای حقوقی انجمن انفورماتیک ایران

گـروه تخصصـی "راهبری و مدیریت خدمـات فناوری اطلاعات" انجمـن انفورماتیک ایران آمادگی برگـزاری دوره‌های زیر را برای کارشناسان سازمان‌ها دارد.

۱- کارگاه نیم روزه تدوین توافقنامه‌های سطح خدمات
۲- کارگاه یک روزه طراحی و استقرار پیشخوان خدمات
۳- کارگاه نیم روزه طراحی کاتالوگ خدمات
۴- کارگاه یک روزه ابزارهای مدیریت خدمات فناوری اطلاعات
۵- کارگاه نیم روزه برون سپاری خدمات و محصولات فناوری اطلاعات
۶- کارگاه نیم روزه همسوسازی IT با کسب وکار (IT Alignment) از طریق COBIT5
۸- کارگاه یک روزه راهبری فناوری اطلاعات (IT Governance) از طریق COBIT5
۹- کارگاه یک روزه راهبری فناوری اطلاعات (IT Governance)
۱۰- کارگاه نیم روزه مدیریت تداوم کسب و کار ISO2012:22301
۱۱- کارگاه نیم روزه راهبری فناوری اطلاعات و ITBSC
۱۲- کارگاه نیم روزه تدوین استراتژی خدمات فناوری اطلاعات
۱۳-کارگاه یک روزه مدیریت خدمات فناوری اطلاعات
۱۴- کارگاه سه روزه ITIL V3 Foundation 2011
۱۵- کارگاه یک روزه مدیریت مخاطرات فناوری اطلاعات
۱۶- کارگاه سه روزه دوره جامع COBIT5
۱۷-کارگاه نیم روزه توسعه نیازمندی‌ها مبتنی بر چارچوب CCMI-ACQ و استاندارد ISO/IEC29148:2011

ویژگی‌های این کارگاه‌ها عبارتند از :

- مشارکت گروهی، بحث و انجام سناریو، حل نمونه آزمون‌های امتحانی
- استفاده از مثال‌های مرتبط با حوزه فعالیت هر کسب وکار
- برگزاری دوره حداقل توسط دو مدرس دارای مدرک بین‌المللی
- برگزاری دوره در محل سازمان متقاضی
- ارائه مدرک شرکت در دوره از سوی انجمن انفورماتیک ایران
- ارائه مستندات آموزشی

در صورت تمایل به دریافت اطلاعات بیشتر می توانید با دفتر انجمن انفورماتیک ایران(۳-۸۸۸۶۱۴۲۱) و یا نشانی پست الکترونیکی member@isi.org.ir تماس بگیرید.

کمیته آموزش انجمن انفورماتیک ایران

لیست اعضای حقوقی

انجمن انفورماتیک ایران

اعضای حقوقی فعال در حوزه راه‌حل‌های برنامه‌ریزی منابع سازمان و نرم‌افزارهای پیشرفته سازمانی

- آینده کاوان کهکشان نرم‌افزار
- ایریسا (بین‌المللی مهندسی سیستم‌ها و اتوماسیون)
- بهکو (بهینه کوشان سپهر)
- برگ سیستم پویا
- پارس رویال نفیس
- پارس تصمیم
- پردازش موازی سامان
- تدبیرگران نوآوری رایسان
- تدوین فرآیند
- چارگون
- چرخه داده‌های سبز
- درگاه ارتباطات جدید
- رایاوران توسعه
- سامانه پرداز اریس
- پایه‌ریزان راه‌کارهای فراگیر
- سامه آرا پردازشگر
- سبز داده افزار
- سیستم‌های اطلاعات مدیریت شرق رایا
- سند پرداز
- شماران سیستم
- شرکت سامانه آسه
- کرانه (سامانه برنامه‌ریزی منابع کرانه)
- گروه نرم‌افزاری پیوست
- نوید ایرانیان (گسترش فضای مجازی)
- مانیر (مشاورین انفورماتیک نیرو)
- مجتمع داده‌ها و سیستم‌ها (MDS)
- مهندسی بهینه ایران
- ماموت مدیریت سیستم‌ها
- مدار گسترش فناوری اطلاعات
- مهندسی نرم‌افزاری رایورز
- مهندسی نرم افزار فرارای (سهامی خاص)
- نوین فن‌آوران اضداد
- نماد ایران
- پیشگامان آسیا
- گروه مشاورین ورانگر نوین
- رایان دژ سپاهان
- مشاوران یام آذر

اعضای حقوقی فعال در حوزه نرم‌افزارهای کاربردی

- اطلاع‌رسانی پیوند داده‌ها
- اختر رایانه پارس
- ایران رایانه
- آریانا پرداز آینده (آرپا)
- آرادین پرداز هزاره سوم
- آناهیتا فن پارس
- پندار کوشک ایمن
- پردازش اطلاعات و ارتباطات هاماوران آسیا
- پیشتازان اندیشه پویا
- توسعه ارتباطات رایانه‌ای آبانگان
- تیم تعمیرات ونگهداری خطوط لوله خاورمیانه
- داده پردازان احداث

لیست اعضای حقوقی

انجمن انفورماتیک ایران

داده‌پردازان آبشار

داده‌پردازی حرفه‌ای‌ها

دی کاو ماندگار

طرفه نگار

رایانه خدمات امید

راهبر نیروی خراسان(رانیر)

سارینا سیستم پرداز

سافت سیستم کیش

سنجه حساب

سبزافزار آریا

شایگان سیستم

مشاوران اندیشمند رادنگر

مهندسی تکرو سیستم

Keyanafze

مدیران سیستم پاسارگاد

مهندسی نرم‌افزار ایده‌گستر پوریا

همراهان سیستم گوهر

همکاران سیستم

نرم‌افزاری امن پرداز

تحلیل‌گران اطلاعات و نوآوران داتیس

فنی مهندسی اندیشه پرداز کیهان

اعضای حقوقی فعال در حوزه بانکی و بانکداری الکترونیکی

الماس هوشمند ایرانیان

بهسازان ملت

بانک اقتصاد نوین

بانک آینده

به‌پرداخت ملت

پدیسار انفورماتیک

پویا

بانک سرمایه

توسعه‌فن‌افزارتوسن

ثامن ارتباط عصر

شرکت کسب و کارهای نوپای خاورزمین

ماتریس تحلیلگران سیستم‌های پیچیده

خدمات انفورماتیک

توسعه سامانه‌های نرم‌افزاری نگین (توسن)

خدمات ماشین‌های اداری امیم رایانه

سفیر آبی آرام

سامانه یکپارچه سیمرغ تجارت

شرکت رایان صنعت اقتصاد نوین

شرکت توسعه فن‌افزار توسن

داده‌پردازی ایران

زرین کیش

داده‌ورزی فرادیس البرز

شرکت شبکه الکترونیکی پرداخت کارت شاپرک

سامانه تبادل الکترونیک دفاتر پیشخوان دولت

فناوری اطلاعات و ارتباطات پاسارگاد آریان (فناپ)

مشاورین بهبود روش‌ها و سامانه‌های مبنا

فناوری اطلاعات ناواکو

گرایش تازه کیش

گسترش فناوری‌های نوین کشاورز

توسعه فناوری اطلاعات خوارزمی

لیست اعضای حقوقی

انجمن انفورماتیک ایران

بانک سینا

اعضای حقوقی فعال در حوزه اینترنت و پورتال‌ها

آزاد نت رسانه

ارتباطات فن‌آوا

ارتباطات مبین نت

افرانت

ایمان نت

پارس لین

پیشگامان دامنه فناوری

تندیس تلاش و تفکر

تدبیر (ایران سون استار)

داده پردازی پویای شریف

برتر سامانه شرق گیلان

ره پویان علم

رایان هوشمند نویان

فناوری اطلاعات و ارتباطات پارس پردازش سدید

فن‌آوری اطلاعات پارسیان میزبان

فناوری رادین پاسارگاد

کیانا پارسیان کیش

کلیدگستر آینده (نت بینا)

گروه شرکت‌های فن‌آوا

مؤسسه گسترش اطلاعات و ارتباطات و فرهنگی ندا رایانه

هاست ایران

اعضای حقوقی فعال در حوزه شبکه و سخت‌افزار

آداک فناوری مانیا

آریا همراه سامانه (سهامی خاص)

آرین وب ایرانیان

اروند رایان گستر

برد پرداز رایانه

بانی‌نو

پردیس فن‌آوری افق

پرتو بیتا جاوید

پارس آوان رایان

تحلیلگران شبکه گستر پارسه

تحلیلگران اطلاعات نگاره

توسعه سرمایه گذاری گروه آروند

تلکام آوا

توسعه دهندگان فن‌آوری گستر طبرستان رایان

توسعه داده‌پردازی بنیس

دانشگاه آزاد علوم تحقیقات خوزستان

رایان مهر الکتریک

رهنمون فناوری اطلاعات

خدمات کامپیوتری خانه سیستم

چرخه ارتباط سبز

سرو رایانه

سیمرغ سامانه تهران

مهندسی پیمان عمران نیرو

مبین تجارت اطلس

شایان توسعه البرز

شبکه پایدار فناوری اطلاعات

شبکه هوشمند پدیده آپادانا

سامانه گستر رشد

صبا کاربردلتا

شبکه گستر نسل جدید

لیست اعضای حقوقی
انجمن انفورماتیک ایران


فن‌آوری اطلاعات و ارتباطات آرمان تندیس ایرانیان (فن آرا)


کارنما رایانه


کهکشان رایانه الوند


کیسان صنعت ایرانیان


کیسون


گروه مهندسین فرایند


مهندسی رایان توان افزار


مهندسی شبکه گستر


مرکز مهندسی کامپیوتری زحل


مهندسی پارتیان ابتکار پایدار


مهندسی افق داده ایرانیان


میزان گستر رایانه


نوین ارتباط نوآوا


شرکت توانش


اندیشه‌پرداز دوران


مهندسین مشاور آمارپردازان فراز

اعضای حقوقی فعال در حوزه مدیریت پروژه


فناوران اطلاعات بهاران

اعضای حقوقی مشتریان بهره‌بردار از راه‌حل‌های نرم‌افزارهای پیشرفته سازمانی و بهره‌بردار از فناوری اطلاعات


انرشیمی


ارتباط پردازان تجارت ایرسا


پارسین تجارت پایا کیش


پردازش هوشمند البرز


نفت ایرانول


خدمات مشاور خرد پیروز


زورق آرامش


مهندسی و ساخت بویلر مپنا


گروه کارخانجات چینی مقصود


گسترش فناوری اطلاعات ستاره ویدا


مهندسی آریا تدبیر ایلیا


مرکز گسترش فناوری اطلاعات (مگفا)

اعضای حقوقی فعال در حوزهٔ آموزش و پژوهش


آماج فناوری اطلاعات وارتباطات ایرانیان


آموزشکده فنی و حرفه‌ای سما


پردیس بین‌المللی رشد وتوسعه فناوری خوزستان


آموزشکده فنی و حرفه‌ای سما واحد نیشابور


آموزشکده دخترانه سما- واحد کرج


دانشگاه بین‌المللی مصطفی


سماتک


فناوری اطلاعات بین‌الملل


مؤسسه عالی مدیریت دانش


مرکز تخصصی پردازش هوشمند

اعضای حقوقی فعال در حوزهٔ مشاوره


آریا ایمن تدبیر

دانش آفرینان نیک اندیش

الهه کوچک نرم افزار

مشاوره مدیریت رایزن سامانه گستر

موسسه حقوقی واقتصادی آرمان ایرانیان

طرح و توسعه الکترونیک افق