برون‌سپاری فناوری اطلاعات و مدیریت امنیت

ترجمه و تألیف: صابر شعری*
مسعود غلام‌زاده لداری**

چکیده

برون‌سپاری فناوری اطلاعات زمانی اتفاق می‌افتد که یک سازمان برای انجـــام کارهای فناوری اطلاعات خود با یک ارائه‌کننده‌ی خدمات فناوری اطلاعات، قراردادی را منعقد کند. برون‌ســـپاری پدیده‌ی جدیدی نیست، اما مقیاس و دامنه‌ی انجام آن در دهه‌ی گذشـــته به‌طور قابل ملاحظه‌ای افزایش یافته است.

برون‌ســـپاری چیزی فراتر از تصمیم‌گیری ســـاده‌ی خریـــد بر مبنای معیارهای مالی و اقتصادی است. برون‌سپاری یک تصمیم راهبردی است که شـــامل واگذاری خدماتی خاص به شـــخص ثالث و ایجاد یک رابطه‌ی بلندمدت اســـت که می‌تواند منابع با ارزش جدیدی را برای یک سازمان فراهم کند.

کلید درک برون‌ســـپاری این است که به‌رغم واگذاری اجرای خدمات، مســـئولیت‌های مربوط واگذار نخواهد شـــد. علاوه بر این، انجام خدمات برون‌ســـپاری شـــده باید برای اســـتفاده‌کنندگان از خدمات و مشتریان سازمان نیز شفاف باشد.

در این مقاله، نظریه‌های برون‌ســـپاری، مزایا و چالش‌های آن، مســـائل مرتبط بـــا امنیت اطلاعات و مدیریت امنیت فنـــاوری اطلاعات در زمان برون‌سپاری بحث خواهد شد.

بخش ۱- نظریه‌های برون‌سپاری فناوری اطلاعات

نظریه‌های متعددی در رابطه با مطالعات برون‌ســـپاری خدمات فناوری اطلاعات وجود دارد که مهم‌ترین آنها در ادامه آمده‌اند.

۱-۱- نظریه‌ی قابلیت‌های محوری: فعالیت‌های ســـازمان را می‌توان به دو طبقه‌ی فعالیت‌های اصلی و فعالیت‌های کم‌اهمیت‌تر تقسیم‌بندی کرد. این فعالیت‌ها ممکن است از طریق برون‌سپاری، در داخل یا خارج سازمان، به انجام برسند. به عقیده‌ی بسیاری از نویسندگان، فعالیت‌ها و خدمات مربوط به فناوری اطلاعات جزء فعالیت‌های اصلی یک سازمان هستند که می‌توانند به‌صورت کلی یا بخشـــی برون‌سپاری شـــوند که این امر به سطح محرمانه بودن اطلاعات و سامانه‌ی اطلاعاتی شرکت بستگی دارد.

۱-۲- نظریه‌ی مبتنی بر منبع: برون‌ســـپاری خدمات فناوری اطلاعات یک تصمیم راهبردی اســـت که می‌تواند منجر به بهبود منابع اطلاعاتی شرکت شود.

۱-۳- نظریـــه‌ی هزینه‌ی معاملات : نبود یک قـــرارداد کامل بین طرفین موجب بروز هزینه‌ی معاملات می‌شـــود، زیرا این شرایط می‌تواند منجر به مذاکـــرات متعدد و افزایش مخارج در طول قرارداد شـــود. هر چه هزینه‌ی معاملات برون‌ســـپاری افزایش یابد، کارایی کل فرآیند برون‌سپاری کاهش می‌یابد.

۴-۱- نظریه‌ی قراردادی: قرارداد برون‌سپاری خدمات فناوری اطلاعات، شامل چارچوب نهادی و قانونی برای حقوق و تعهدات طرفین است. قرارداد برون‌سپاری باید از مخاطرات و فرصت‌طلبی‌ها پیش‌گیری کند.

۵-۱- نظریه‌ی اقتصاد نوکلاسیک: شرکت‌ها برای کاهش هزینه از طریق صرفه‌جویی در حفظ و نگهداری خدمات فناوری اطلاعات، به برون‌سپاری این خدمات تمایل دارند. آنها در صورتی واحد فناوری اطلاعات خود و کارکردهای آن را تأمین مالی می‌کنند که مخارج مربوط به آن کم‌تر از مخارجی باشد که در صورت برون‌سپاری تحمل می‌شود.

بخش ۲- مزایا و چالش‌های برون‌سپاری

۱-۲- مزایای برون‌سپاری

مدیریت می‌تواند به‌دلایل مختلف اقدام به برون‌سپاری فناوری اطلاعات کند. مهم‌ترین دلایل چنین تصمیمی به‌تفکیک منافع عملیاتی، مزایای فناوری و مسائل مالی در ادامه آمده است.

الف- منافع عملیاتی

مزایای عملیاتی برون‌سپاری عبارتند از: ۱) با حداقل کردن منابع اختصاص یافته به فعالیت‌های فرعی و در نتیجه تمرکز بیشتر بر توانمندی‌های محوری، سازمان قادر به بهبود عملکرد خود از طریق تجدید ساختار یا بازمهندسی فرآیندهای کسب و کار خواهد بود. ۲) برون‌سپاری می‌تواند باعث کاهش زمان ورود به بازار شود. کوچک‌سازی تأسیسات و امکانات یکی دیگر از مزایای بالقوه‌ی برون‌سپاری است.

ب- مزیت‌های فناورانه

دست‌یابی به کارایی فناوری اطلاعات ممکن است مهم‌ترین انتظار سازمان از انجام برون‌سپاری باشد. یک سازمان می‌تواند با انجام برون‌سپاری به فناوری، افراد و فرآیندهایی دسترسی داشته باشد که دسترسی به آنها از طریق دیگر صرفه‌ی اقتصادی نداشته باشد. اغلب برون‌سپاری امکان دسترسی به فناوری‌های پیشرفته را فراهم می‌کند. این کار می‌تواند راهی برای استفاده از فناوری روز، دسترسی به کارشناسان فناوری اطلاعات و در نتیجه بهبود کیفیت ارائه خدمات مربوط به سازمان و مشتریان شود.

ج- مزیت‌های مالی

یکی از مهم‌ترین مزایای برون‌سپاری فناوری اطلاعات از نقطه‌نظر مدیریت، نتایج مالی آن است. برون‌سپاری امکان تحت کنترل درآوردن مخارج مربوط به فناوری اطلاعات را از طریق اثربخشی انجام فعالیت توسط ارائه‌کننده‌ی خدمات یا تسهیم هزینه‌های مشترک میان آنها فراهم می‌کند. برون‌سپاری از طریق استاندارد کردن نرم‌افزارهای مورد استفاده‌ی کاربران، خرید سخت‌افزار به قیمت عمده‌فروشی، تقسیم هزینه‌های توسعه و نگهداری سامانه‌ها بین پروژه‌ها و اجرای عملیات سامانه در حجم وسیع‌تر می‌تواند صرفه‌جویی قابل ملاحظه‌ای در هزینه‌ها ایجاد کند. شرکت‌هایی که سرمایه‌گذاری‌های هنگفتی در فناوری اطلاعات کرده‌اند می‌توانند با فروش دارایی‌ها، هزینه‌های سالانه‌ی خود را کاهش دهند و وضعیت نقدشوندگی را بهبود بخشند.

گفتنی است، به دلیل تغییرات سریع فناوری، شرکت‌ها باید منابع زیادی را صرف تجهیز سامانه‌های اطلاعاتی خود به آخرین پیشرفت‌های مربوطه کنند. علاوه بر این، برون‌سپاری می‌تواند ریسک سرمایه‌گذاری در فناوری نادرست را کاهش دهد، میزان سرمایه‌ی مورد نیاز را به‌طور قابل ملاحظه‌ای محدود کند و منابع مالی را برای انجام فعالیت‌های راهبردی آزاد کند.

۲-۲- چالش‌های برون‌سپاری

اگر چه غالباً برون‌سپاری جذاب به‌نظر می‌رسد، اما چالش‌هایی را نیز به‌دنبال دارد. در ادامه به برخی از این چالش‌ها اشاره می‌شود.

الف- چالش‌های عملیاتی

تهدیدهای دسترسی، یکپارچگی سامانه‌ها و منابع، محرمانه بودن اطلاعات و رعایت مقررات: ناتوانی سامانه‌ها، فقدان یکپارچگی داده‌ها یا دسترسی غیرمجاز به داده‌ها می‌تواند توانایی سازمان را در اتخاذ تصمیمات تجاری صحیح با استفاده از اطلاعات تولید شده توسط سامانه‌های اتکاءپذیر با مخاطراتی مواجه سازد و هدایت عملیات آن در راستای اجرای مقررات را دشوار سازد. این شرایط می‌تواند منجر به از دست رفتن مزایای رقابتی و حسن شهرت سازمان شود و زیان‌های مالی (مانند مخارج انجام دعاوی حقوقی و پرداخت جرایم) را برای سازمان به‌دنبال داشته باشد.

از دست رفتن کنترل: شـــرکتی که بخش عمده‌ای از فناوری اطلاعات خود را به‌صورت برون‌ســـپاری اداره می‌کند، خطر از دســـت رفتن کنترل ســـامانه و داده‌هایش افزایش می‌یابد. عـــلاوه بر این، هنگامی که پردازش داده‌های فعالیت‌های شـــرکتی توسط یک مؤسسه‌ی خدماتی دیگر انجام می‌شود، امکان سوء اســـتفاده (مانند افشای اطلاعات محرمانه‌ی شرکت) وجود دارد.

از دســـت دادن افراد شایســـته و کاهش مزایای رقابتی: در بسیاری از برون‌ســـپاری‌ها، دارایی‌هـــا و کارمندان مربوط به فنـــاوری اطلاعات به ارائه‌کننـــده‌ی خدمات واگذار می‌شـــوند. این کار منجر بـــه مأمور کردن کارکنان با مهارتی می‌شود که سرمایه‌ی فکری سازمان محسوب می‌شدند. بنابراین ریسک از دست دادن افراد شایسته و با دانش در زمینه‌ی سامانه‌ها و عملیات مربوطه در حالت برون‌ســـپاری متصور اســـت. این امر توانایی سازمان برای انجام عملیات و مدیریت کارآمد را تحت تأثیر قرار می‌دهد. از طرف دیگر نمی‌توان انتظار داشت که ارائه‌کننده‌ی خدمات برون‌سازمانی خود برای شناخت نیازهای اساسی سامانه‌های اطلاعاتی، چگونگی تأمین این نیازها و تحقق مزیت‌های رقابتی یک صنعت خاص تلاش زیادی انجام دهد. در حالی که انتظار انجام این کار توســـط کارکنان لایق سازمان قبل از برون‌سپاری متصور بود.

ب- چالش در ارائه‌ی خدمات

برآورده نشـــدن انتظارات یا نیازهای سازمان: ممکن است سازمان با استاندارد خاص و سبک مشـــخصی از عملکرد خو گرفته باشد که توسط بخش فناوری اطلاعات درون‌ســـازمانی قبل از برون‌سپاری انجام می‌شد. ممکن اســـت ارائه‌کننده‌ی خدمات جدید قادر به ادامه‌ی همان استاندارد و سبک نباشـــد. میزان تفاوت، دســـت کم در کوتاه‌مدت، می‌تواند مورد توجه باشـــد تا این‌که دو طرف عادات خـــود را به محیط عملیاتی جدید رشد دهند.

مشـــکل احتمالی دیگر این است که ممکن است ارائه‌کننده‌ی خدمات قادر به درک کامل اولویت‌های عملیاتی ســـازمان یا سایر انتظارات اصلی نباشد. این مشـــکل نیز ممکن است کوتاه‌مدت باشد و با تکامل تدریجی محیط جدید حل شـــود. از طرف دیگر ممکن اســـت این چالش حاکی از فقدان شـــفافیت مدیریت یا راهبری باشـــد، مشکلی که حل آن بسیار دشوارتر است.

ج- چالش‌های مربوط به مخارج

مخارج پیش‌بینی نشده در قراردادهای برون‌سپاری: وقتی برون‌سپاری بـــه اندازه‌ی کافی برنامه‌ریزی نشـــود، ممکن اســـت مخـــارج پیش‌بینی نشـــده‌ای در رابطه با واگذاری و مدیریت بر ســـازمان تحمیل شود و در نتیجه سودآوری تصمیم برون‌سپاری را تحت تأثیر قرار دهد. اغلب درک سازمان و ارائه کننده‌ی خدمات از خدمات موضوع قرارداد، خدمات خارج از قرارداد می‌باشـــند و نحوه‌ی قیمت‌گذاری این خدمات، متفاوت است. ممکن است ارائه‌کنندگان خدمات بابت ارائه خدماتی به سازمان، مبلغی به حساب آن منظور کنند اما سازمان انجام آن خدمات و در نتیجه مبلغ آن را در همـــان مبلغ اولیه فرض کند (نه پرداخت مبلغ اضافی بابت آن).

مانند آموزش یا پشـــتیبانی از رایانه‌های شـــخصی. افزون بر این، ممکن اســـت نحوه‌ی قیمت‌گذاری در قرارداد بر اســـاس معیارهای کیفی باشد (مانند عملکرد و درجه‌ی دشواری) که تعیین مخارج را دشوار می‌کند.

مخارج خاتمه‌ی یک قرارداد، بازگشـــت به انجام خدمات به‌صورت داخلی یا جســـتجوی ارائه‌کننده‌ی جدید خدمات: گاهی اوقات شرایط غیرمنتظره‌ای سازمان را در وضعیتی قرار می‌دهد که مجبور به خاتمه‌ی قرارداد می‌شود. خاتمه‌ی یک قرارداد مخارج زیادی را در پی دارد. تغییر ارائه‌کننده‌ی خدمات یا بازگشـــت به انجام خدمات به‌صورت داخلی نیز هزینه‌های بالایی را موجب می‌شـــود. این وضع وقتی وخیم‌تر خواهد شد که تعداد اندکی از دیگر ارائه‌کننده‌ی خدمات برای انجام این خدمات به رقابت بپردازند.

مخارج مرتبط بـــا اختلافات و دعاوی حقوقی: قرارداد ضعیف یا روابط نامناسب بین ســـازمان و ارائه‌کننده‌ی خدمات، ریسک بروز اختلافات و دعـــاوی حقوقی را افزایش می‌دهد. این امر می‌تواند تمرکز مدیریت را از فعالیت‌های اصلی منحرف و مخارج زیادی را به سازمان تحمیل کند.

د- چالش‌های مربوط به امنیت فناوری اطلاعاتی

حفـــظ امنیت فنـــاوری اطلاعات در زمان برون‌ســـپاری آن، فرآیندی پیچیده اســـت. برخی از چالش‌های امنیتی فناوری اطلاعات که سازمان باید در زمان برون‌سپاری بدان توجه داشته باشد در ادامه آمده است.

وقتی سازمان:

- از ریسک‌های امنیتی و تعهدات قانونی مربوطه آگاهی ندارد.
- ارائه‌کنندگان خدمات را از ریسک‌های امنیتی و تعهدات قانونی مرتبط با حوزه‌های کسب و کار آگاه نسازد.
- فـــرض می‌کند که ارائه‌کنندگان خدمات بهترین رویه‌ی امنیتی را اجرا خواهند نمود، درحالی‌که ممکن است تنها مواردی را اجرا کنند که بابت آن قرارداد امضاء کرده‌اند یا وجوه دریافت نموده‌اند.
- فـــرض می‌کند که امنیت فناوری اطلاعات به‌عنوان بخشـــی از الزامات کارآمد و سودمند استنباط شده اســـت، درحالی‌که الزامات امنیتی باید صریحاً شناسایی شود.
- سیاســـت‌های مبهم یا ناســـازگار شناســـایی می‌کند یا استانداردهای امنیتی و مجموعه رویه‌هایی استخراج می‌گردد که انحراف قابل ملاحظه در تفسیر را مجاز می‌شمارد.
- نســـبت به تغییرات در ریسک یا چشم‌انداز مقرراتی مرتبط با تغییرات مستمر در محیط امنیتی الکترونیکی آگاهی ندارد.
- بـــه مدیریت در ســـطح خرد و الزامـــات امنیتی مرتبط بـــا آن تمرکز دارد، فرصت ارائه‌کننده‌ی خدمات برای نـــوآوری و انعطاف‌پذیری کم‌تر می‌شود.
- مدیریت امنیت فناوری اطلاعات را در ســـطح تفصیلی ادامه می‌دهد، به‌رغم وجـــود برون‌ســـپاری تلاش‌ها مضاعـــف و پاســـخگویی‌ها مبهم می‌شوند.
- در انجام نظارت مستمر شبکه‌های اطلاعاتی برای فعالیت‌های غیرمجاز و مشکوک ناتوان است، طرح‌های پاسخ تصادفی را مستقر می‌کند یا قادر به انجام آزمون مناسب نیست.

وقتی مدیریت سازمان:

- به‌طـــور ضمنی کاهـــش امنیت فناوری اطلاعات و ســـطح کارآمدی یا خدمـــات را مجاز می‌داند و این زمانی اتفـــاق می‌افتد که مدیران ارزیابی نمی‌شوند یا مسئولیت پاسخگویی ندارند.
- نسبت به ریسک‌های جرایم احتمالی یا مسئولیت مدنی آگاهی ندارند، و
- پـــس از برون‌ســـپاری فناوری اطلاعات، دیگر احســـاس مســـئولیتی نمی‌کند.

وقتی قرارداد برون‌سپاری سازمان:

- قصد ساده‌ســـازی بیش از حد الزامات امنیتی فنـــاوری اطلاعات را در مفاد قرارداد دارد،
- انعطاف‌پذیری لازم برای مطابقت با تغییرات محیط مخاطره‌آمیز تجاری را نداشته باشد، و
- نتواند الزامات امنیتی را به‌طور دقیق تعریف کند.

وقتی ارائه‌کننده‌ی خدمات:

- خود را نسبت به امنیت فناوری اطلاعات پاسخگو نداند.
- در زمینه‌ی تخصیص منابع به مدیریت امنیت، با تجربه و واجد شـــرایط لازم نباشد.
- فرآیندهای امنیتی را که در قرارداد صریحاً تشـــریح نشـــده‌اند با هدف کاهش هزینه یا افزایش حاشیه‌ی سود خود، کاهش دهد.
- درصدد فرصت‌هایی برای کاهش مخارج و افزایش حاشـــیه ســـود خود باشـــد، شامل انجام کار توسط پیمانکاران دست دوم بیشتر در صورتی که قرارداد مانع از انجام این کار باشد.
- مانـــع تلاش‌های ســـازمان در جهت کســـب عینیت و ملموس شـــدن فرآیندهـــای امنیتی فنـــاوری اطلاعاتی یا بررســـی‌های اطمینان‌دهی یا حسابرسی امنیت شود.
- تضمین‌هایی که الزامات سازمان را فراهم می‌سازد، برآورده می‌کند.

بخش ۳- امنیت اطلاعات در برون‌سپاری

ســـازمان در انجام هرگونه برون‌ســـپاری فناوری اطلاعات، نســـبت به امنیت فناوری اطلاعات خود مســـئول است. در یک سازمان بدون داشتن چارچوب راهبری امنیتی اثربخش و منســـجم نمی‌توان به‌نحو مؤثری به اهداف امنیت فناوری اطلاعات دست یافت.

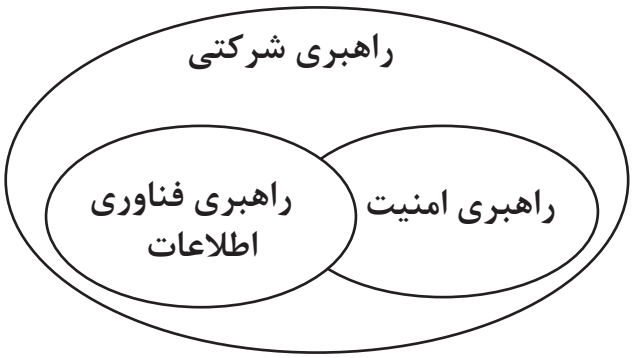
۳-۱- راهبری امنیت فناوری اطلاعات و برون‌سپاری

برون‌ســـپاری یک راهبرد تجاری است که ســـازمان برای دست‌یابی به اهداف راهبردی خود آن را دنبال می‌کند. اگر به امنیت فناوری اطلاعات

به‌طور دقیق توجه نشـــود، محرک‌های اصلی برون‌سپاری (کاهش هزینه، افزایش انعطاف‌پذیری تجاری، استفاده از فناوری‌های جدید و دسترسی به تخصص بیشـــتر) اهمیت خود را از دست خواهند داد. یک حادثه در انجام کار فناوری اطلاعات به دلایل خطای انسانی، نقص‌های سیستمی یا حتی برنامه‌هـــای خرابکارانه می‌تواند کل منافع حاصل از برون‌ســـپاری را خنثی کند.

سازمان‌ها باید راهبری امنیت فناوری اطلاعات را به‌عنوان یکی از اجزای اصلی یک مدل کلی برون‌ســـپاری در نظر بگیرند. در حال حاضر اطلاعات و ســـامانه‌های فناوری اطلاعات در قلب عملیات یک ســـازمان ایفای نقش می‌کننـــد و راهبری امنیت فناوری اطلاعات یکی از عناصر کلیدی راهبری شرکتی مطلوب می‌باشد.

نمایه‌ی ۱- روابط بین راهبری شرکتی، فناوری اطلاعات و امنیت



مراحلی که باید به‌منظور اطمینان از امنیت اطلاعات در برون‌ســـپاری‌ها رعایت شود، به‌شرح زیر است:

۱. اطمینان از استقرار سامانه‌ی مدیریت امنیت اطلاعات داخلی مناسب
۲. شناسایی و ارزیابی ریسک‌ها
۳. برداشتن گام‌های امنیتی
۴. نقش‌ها و مسئولیت‌ها
۵. انعقاد قرارداد برای امنیت اطلاعات
۶. آرایش امنیتی دوران واگذاری
۷. اطمینان‌بخشی و هماهنگی
۸. مدیریت مستمر امنیت (شامل مدیریت تغییر)
۹. مدیریت حوادث و اتفاقات و گزارشگری و
۱۰. خاتمه و انتقال

خط‌مشـــی‌های راهبری داخلی و برون‌سازمانی امنیت فناوری اطلاعات ســـازمان، باید مبتنی بر درک تهدیدهای احتمالـــی از جمله، تهدیدهای مرتبط با برون‌ســـپاری باشد، تعهدات مربوط به قوانین و مقررات را رعایت کند و متکی بر ارزیابی ریســـک، راهبردهای مدیریت استثنائات و آزمون‌ها باشد.

نمایه‌ی ۲- چک‌لیست مسائل مربوط به امنیت اطلاعات

الزامات مربوط به امنیت اطلاعات

- اســـتانداردهای امنیـــت ســـامانه‌ها و تبـــادل اطلاعاتی که باید توســـط سامانه‌های ارائه‌کننده‌ی خدمات و سازمان تأمین شود.
- محافظت از اطلاعات محرمانه و دارایی‌های فکری‌سازمان
- محافظـــت از اطلاعـــات شـــخصی و داده‌هـــای مربوط به مشـــتریان و ارباب‌رجوع‌های سازمان
- رعایت اطلاعات، امنیت و سیاست‌های خصوصی، قوانین و مقررات
- برداشت اطلاعات از سامانه‌های فرعی و هرگونه سامانه‌ی اجاره شده

ملاحظات مربوط به کارکنان داخلی و بیرونی

- استخدام کارکنان و مدیران امنیت اطلاعات واجد شرایط و باتجربه
- جزئیات نظارت بر کارکنان و پیمانکاران
- تأیید صلاحیت، بررسی کارکنان و ناظران به‌نحو صحیح
- توافق نسبت به کنترل‌ها و میزان دسترسی از راه دور توسط ارائه‌دهنده‌ی خدمات، کارکنان و پیمانکاران
- سرپرســـتی، نظارت، تأیید صلاحیت و کنترل پیمانکاران دســـت دوم و مسئولیت‌های پاسخگویی آنها
- شرایط جبران خسارات توسط ارائه‌کننده‌ی خدمات و پیمانکاران آن

ملاحظات پاسخگویی، گزارشگری و رعایت

- الزامات و توافقات در رابطه با امنیت سامانه‌ها
- بررسی سامانه‌ها و حسابرسی امنیت
- گزارشگری موارد نقض امنیت
- پوشـــش خسارات، موافقت در مورد نگهداری اســـناد و مدارک و رویه‌ی گزارشگری
- طرح‌های تداوم کسب و کار برای سازمان و برای ارائه‌کننده‌ی خدمات
- حوادث امنیتی و مدیریت ریسک و تعهدات گزارشگری

انتقال/ خاتمه‌ی قرارداد

- آرایش قراردادی شفاف برای فرآیند انتقال یا خاتمه
- درک روشن سازمان و ارائه‌کننده‌ی خدمات از فرآیند خاتمه

۲-۳- مسائل مربوط به امنیت اطلاعات که باید قبل از سازمان‌دهی برون‌سپاری در نظر گرفت:

ســـازمان قبل از ورود به عرصه‌ی برون‌ســـپاری فناوری اطلاعات، باید نســـبت به معنادار بودن هرگونه سیاست‌های درون‌سازمانی، استانداردها و الزامات مربوطه و نیز بررســـی آنها به‌لحاظ قانونی اطمینان حاصل کند. در غیر این‌صورت، انتظار می‌رود اختلالات و مشکلاتی در زمینه‌ی امنیت

فناوری اطلاعات برون‌سپاری به‌وجود آید.

در حین مراحل اولیه‌ی برنامه‌ریزی قرارداد برون‌سپاری، سازمان باید مشخص کند که آیا توانایی داخلی برای مدیریت اثربخش امنیت فناوری اطلاعات خود را دارا است یا بهتر است مدیریت امنیت فناوری اطلاعات را به شخص ثالث واجد شرایط برون‌سپاری نماید.

قبل از آن‌که سازمان فرآیند برون‌سپاری را آغاز کند پیشنهاد می‌شود چک‌لیستی از مسائل مربوط به امنیت اطلاعاتی تکمیل شود تا نسبت به کفایت امنیت، ساز و کارهای پرسنلی و گزارشگری مربوط به خط‌مشی‌ها و راهبری‌های امنیت فناوری اطلاعات اطمینان حاصل شود. در نمایه‌ی ۲ چک‌لیستی شامل برخی از این مسائل ارائه شده است.

بخش ۴- مدیریت امنیت فناوری اطلاعات در زمان برون‌سپاری

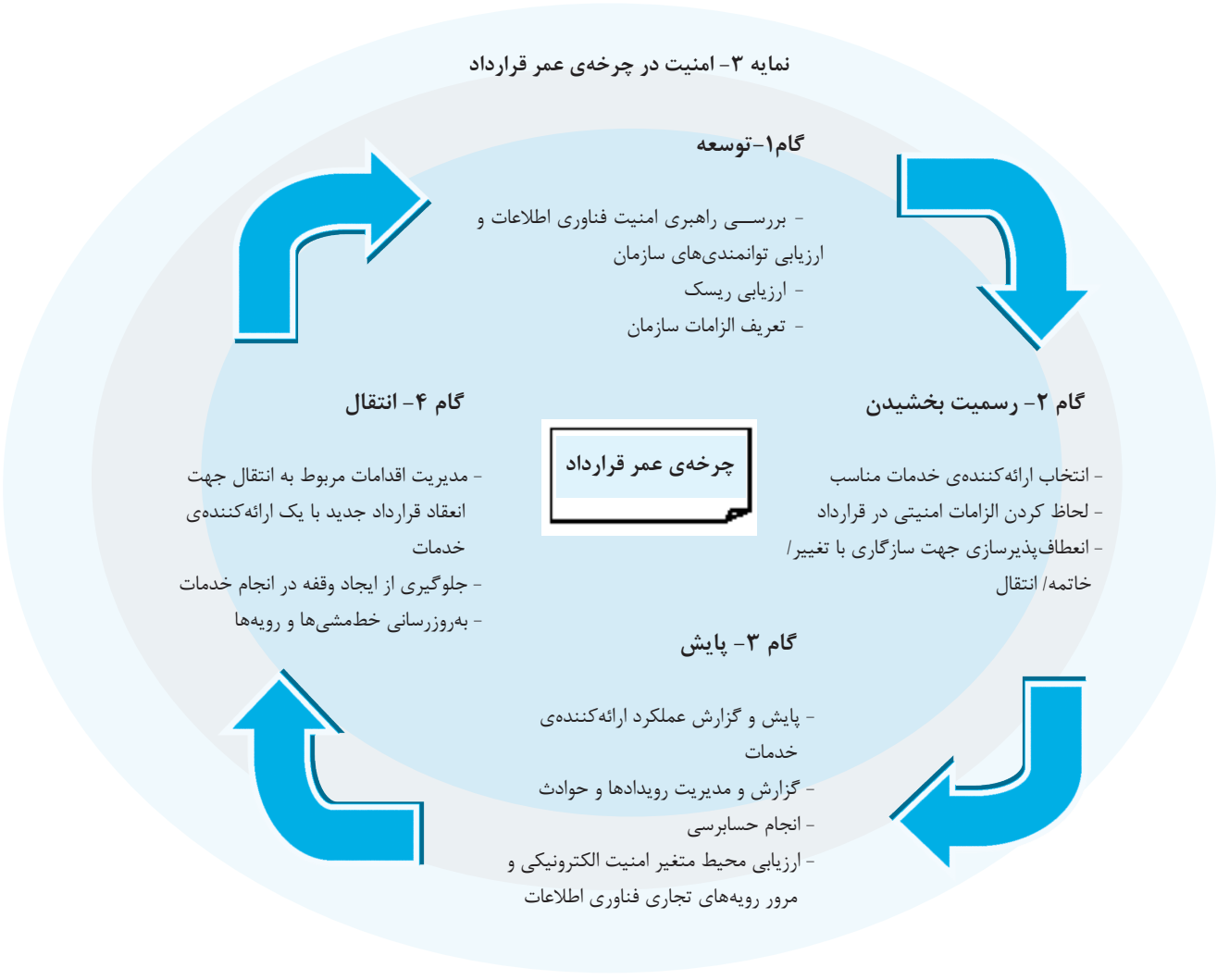
هر رویکردی که در رابطه با ریسک امنیت اطلاعات اتخاذ می‌شود باید براساس طرح راهبردی جامع سازمان باشد. بنابراین طرح راهبردی کلی باید آگاهی‌هایی در زمینه‌ی مدیریت امنیت فناوری اطلاعات در هر برون‌سپاری فراهم آورد. نمایه‌ی ۳ مسائل با اهمیت مرتبط با امنیت فناوری اطلاعات را نشان می‌دهد که در مراحل مختلف چرخه‌ی قرارداد و طی مراحل برنامه‌ریزی و اجرای برون‌سپاری باید به آنها توجه شود.

سازمان باید توانمندی داخلی خود را برای مدیریت اثربخش امنیت در فرآیند برون‌سپاری مدنظر قرار دهد. اگر سازمانی نسبت به توانایی خود در این زمینه مطمئن نباشد باید با یک شخص ثالث برون‌سازمانی واجد شرایط قراردادی منعقد کند. برای یک سازمان آگاهی از مسئولیت خود در مورد اطمینان از اجرا و کنترل فرآیندهای امنیتی اثربخش حائز اهمیت است.

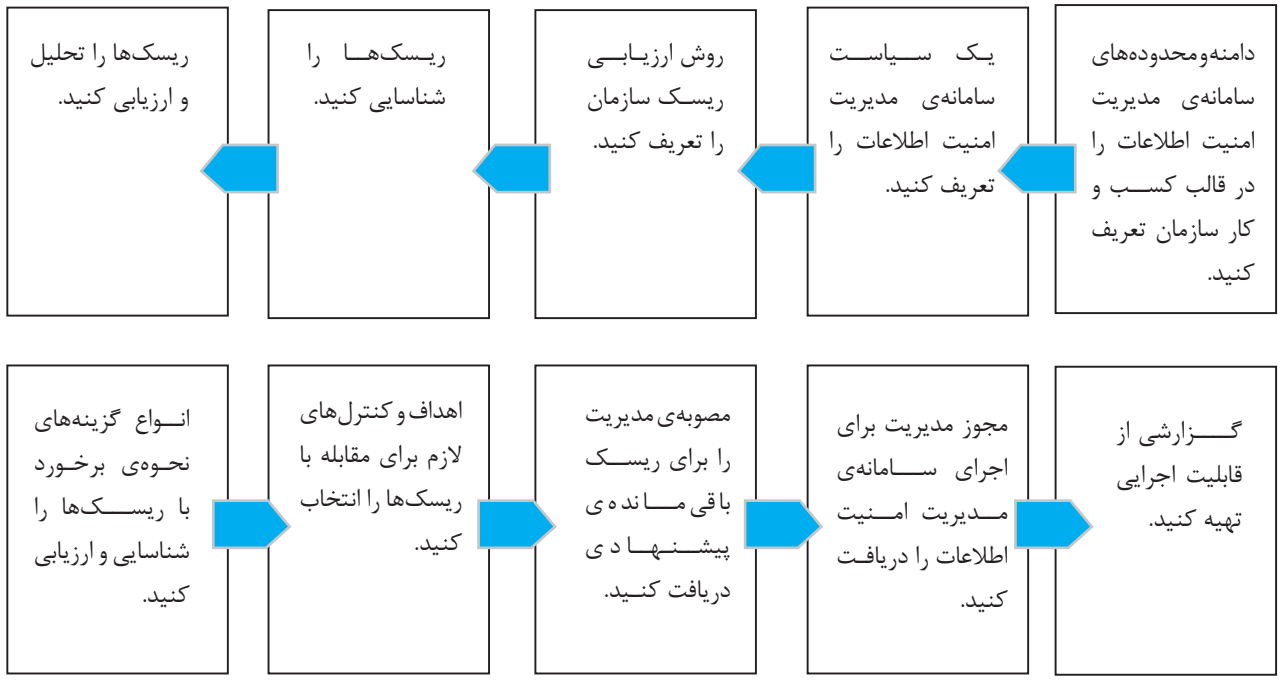
بنابراین قبل از وارد شدن به برون‌سپاری، باید یک راهبرد امنیت فناوری اطلاعات سازمانی مناسب اتخاذ گردد و به‌طور یکنواخت و با ثبات رویه در هر یک از قراردادهای برون‌سپاری اجرا شود. این امر:

- یکنواختی بین قرادادهای برون‌سپاری و راهبردهای گسترده‌ی شرکت را افزایش می‌دهد،

نمایه ۳- امنیت در چرخه‌ی عمر قرارداد

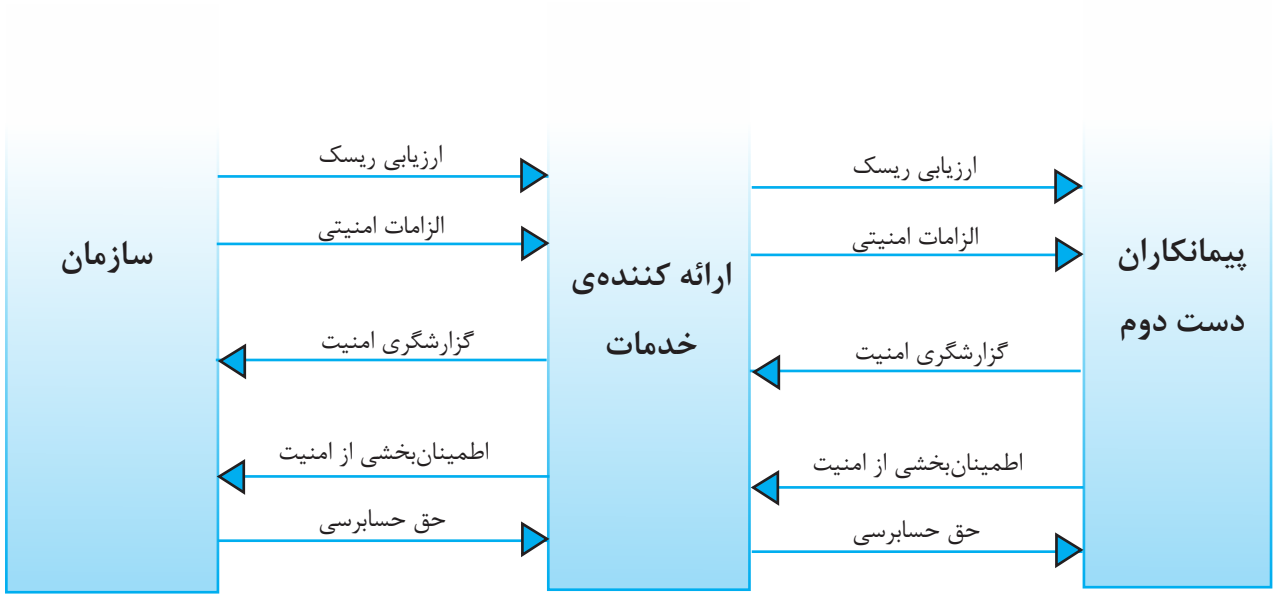


نمایه ۴ – مدل سامانه‌ی مدیریت امنیت اطلاعات



فرآیند مدیریت امنیت اطلاعات تشریح شده در نمایه‌ی ۵، توسعه‌ی روابط بین سازمان و ارائه‌کننده‌ی خدمات و نیز نحوه‌ی مدیریت جریان اطلاعات مرتبط با ارزیابی ریسک، الزامات امنیتی، گزارشگری، اطمینان‌بخشی در مورد امنیت و حسابرسی را نشان می‌دهد.

نمایه ۵- جریان اطلاعات مدیریت ریسک در برون‌سپاری



• امور اجرایی را کارآتر می‌سازد،
• احتمال رعایت آنها را به‌طور کلی افزایش می‌دهد، و
• امکان کشف آسان‌تر مسائل سامانمند و سازمانی را فراهم می‌سازد.

AS/NZS ISO/IEC ۲۷۰۰۱ یک استاندارد استرالیایی است که برای تشخیص الزامات مربوط به مدل سیستم مدیریت امنیت اطلاعات اثربخش استفاده می‌شود. براساس AS/ISO۲۷۰۰۱:۲۰۰۶، یک سیستم مدیریت امنیت اطلاعات باید از مدل تشریح شده در نمایه‌ی ۴ پیروی کند.

در صورتی‌که ارائه‌کننده‌ی خدمات با پیمانکار دست دوم فعالیت کند، باید فرآیند مدیریت امنیت اطلاعات برون‌سپاری با هر پیمانکار دست دوم توسط ارائه‌کننده خدمات تکرار شود، به‌نحوی که سامانه‌ی مدیریت امنیت اطلاعات کلیه‌ی اطلاعات و سامانه‌های برون‌سپاری شده توسط سازمان را پوشش دهد. این امر باید از طریق یک قرارداد برون‌سپاری داخلی مدیریت شود.

باید قبل از تصمیم‌گیری در خصوص ورود به عرصه‌ی برون‌سپاری یک ارزیابی از ریسک‌های امنیتی انجام شود. برخی از گام‌های کلی ارزیابی ریسک در چک لیست زیر ارائه شده است.

بخش ۵- راهبردهای کاهش ریسک‌های برون‌سپاری فناوری اطلاعات

۵-۱- تدوین یک راهبرد برون‌سپاری فناوری اطلاعات

گام نخست در برون‌سپاری فناوری اطلاعات درک صحیح و مستندسازی اهداف تجاری و نحوه‌ی دست‌یابی به این اهداف از طریق فناوری‌های پشتیبان است. این کار به مدیریت اجازه می‌دهد تا انتظارات واقعی را شکل دهد، نیازهای سازمان را به‌نحوی کارآمد به ارائه‌کنندگان خدمات اطلاع‌رسانی کند، معیارهای اندازه‌گیری عملکرد معناداری را برای مقایسه منافع و مخارج برون‌سپاری تدوین کند، و پیشنهادهای ارائه شده را به‌صورت عینی با استفاده از معیارهای تدوین شده ارزیابی کند.

یک سازمان بدون درک اهداف برون‌سپاری، ممکن است کاهش هزینه را تنها معیار خود قرار دهد که در این صورت برآورده نشدن انتظارات محتمل خواهد بود، زیرا امکان دارد سایر ارزش‌های راهبردی و فناورانه اهمیت بیشتری داشته باشند.

۵-۲- حفظ متخصصین فناوری اطلاعات داخلی

سازمان به تعداد کافی از متخصصین داخلی فناوری اطلاعات نیاز دارد تا به‌گونه‌ای کارشناسانه طرح راهبردی فناوری اطلاعات را ترسیم، پیشرفت آن را کنترل و دائماً تغییر نیازها و فناوری‌های جدید را پایش کنند. هم‌چنین در زمان برون‌سپاری باید یک تیم مذاکره‌کننده متشکل از متخصصین فناوری اطلاعات تشکیل شود که نسبت به الزامات سازمان آگاهی داشته باشند. همچنین یک مشاور حقوقی مشارکت فعال داشته باشد تا مفاد قانونی قرارداد بهینه باشد.

۵-۳- تأیید درک ارائه‌کننده‌ی خدمات از نیازهای سازمان

درک متقابل از فرآیندها و سامانه‌های کسب و کار سازمان و اهداف و انتظارات فناوری اطلاعات آن، اساس یک تجربه‌ی رضایت‌بخش از برون‌سپاری را تشکیل می‌دهد. سازمان باید اطمینان حاصل کنند که ارائه‌کننده‌ی خدمات نیازهای سازمان را به‌نحو صحیحی درک نموده و پیشنهادات ارائه شده مبتنی بر مفروضات مناسب است.

۵-۴- ارزیابی وضعیت مالی و عملیاتی ارائه‌کننده‌ی خدمات

توانایی‌های مالی و عملیاتی ارائه‌کننده‌ی خدمات جهت برآورده ساختن نیازها و اهداف سازمان باید بررسی شود. این اقدام می‌تواند شامل بررسی صورت‌های مالی حسابرسی شده، گزارش‌های کنترل داخلی حسابرسی شده، پوشش بیمه‌ای (آتش‌سوزی، بدهی، از بین رفتن داده‌ها و غیره) و تشکیل جلسات با مدیریت و مشاهده عینی در محل فعالیت باشد.

۵-۵- ارزیابی تجربه، تخصص و کفایت منابع ارائه‌کننده‌ی خدمات

سازمان باید در جهت ارزیابی تجربه‌ی ارائه‌کننده‌ی خدمات، توانایی آن در محیط عملیاتی پیش‌بینی شده، کار کردن با انواع سامانه‌ها و برنامه‌های رایانه‌ای مورد استفاده، آشنایی با فرآیندهای تجاری صنعت مربوطه، توانایی نگهداشت سامانه‌ها در حالت عملیات و واکنش نسبت به توقف خدمات تلاش کافی را به‌عمل آورد. تشکیل جلسه با کارکنان ارائه‌کننده‌ی خدمات و سایر ارباب رجوع‌ها می‌تواند به ارزیابی صلاحیت و تجربیات آن کمک کند. مشاهده‌ی عینی از محل کار ارائه‌کننده‌ی خدمات نیز می‌تواند در ارزیابی نحوه‌ی عملکرد ارائه‌کننده‌ی خدمات و حمایت او از ارباب رجوع‌ها یاری‌رسان باشد.

۵-۶- ارزیابی کفایت کنترل‌های داخلی ارائه‌کننده‌ی خدمات

مسئولیت حفاظت، درستی و کیفیت داده‌های شرکت و فرآیندهای فناوری اطلاعات همچنان بر عهده‌ی مدیریت است. بنابراین رسیدگی و ارزیابی چارچوب کنترل‌های داخلی ارائه‌کننده‌ی خدمات در محیط برون‌سپاری (به‌ویژه سیاست‌ها و رویه‌های آن در زمینه‌ی حفاظت و نگهداری از سامانه‌ها، داده‌ها و نرم‌افزارها و کنترل‌های موجود بر امنیت، تداوم فعالیت و بازیافت فناوری اطلاعات، توسعه‌ی سامانه‌ها و حفظ و نگهداشت آنها)، ضرورت دارد. ارائه‌کننده‌ی خدمات باید آگاهی کافی خود از قوانین و مقررات مربوط به خدمات را، به‌ویژه موارد مختص صنعتی که سازمان در آن فعالیت می‌کند، اثبات کند. مرور گزارش حسابرس درخصوص سامانه‌ی کنترل داخلی ارائه‌کننده‌ی خدمات (اگر در دسترس باشد) می‌تواند در جهت اطمینان سازمان از طراحی، استقرار و عملکرد اثربخش کنترل‌های داخلی یاری‌رسان باشد.

۵-۷- درنظر گرفتن استفاده از اشخاص ثالث

مشارکت اشخاص ثالث با ارائه‌کنندگان خدمات جهت کمک به اجرای خدمات به سایر ارباب رجوع‌ها امری غیرمعمول نیست. سازمان باید

سطح مشـــارکت اشخاص ثالث جهت حمایت از ارائه‌کننده‌ی خدمات و اثر آن بر اجرای خدمات برون‌سپاری شده، کنترل‌ها و الزامات مقرراتی را شناسایی کند.

۸-۵- تعیین دوره‌ی انتقال مورد انتظار

مدیران بایـــد دوره‌ی انتقال مـــورد انتظار را برآورد کنند، دوره‌ای که به‌گونه‌ی اثربخش برای ســـازمان و ارائه‌کننده‌ی خدمات دوره‌ی آموزش محســـوب می‌شود. گاهی اوقات این دوره تا قبل از منظور کردن تغییرات فرهنگی توسط سازمان و نیز قبل از تســـلط کامل ارائه‌کننده‌ی خدمات بر ســـامانه‌ها و فرآیندهای کسب و کار سازمان طول می‌کشد. اســـتفاده‌کنندگان باید از دوره‌ی انتقـــال و ناهماهنگی‌های احتمالی آگاهی کافی داشته باشند.

۹-۵- تدویـــن و پیگیـــری معیارهـــای اندازه‌گیری عملکرد

تدویـــن معیارهای اندازه‌گیری عملکرد به لحاظ ارزیابی مقایسه‌ای عملکرد ارائه‌کننده‌ی خدمات و بررسی کیفیت خدمات انجام شده حائز اهمیت اســـت. این معیارها ســـازمان را از حداقل سطح انجام خدمات مطمئن می‌کنـــد و باید به‌عنوان بخشی از قرارداد مورد توافق طرفین قرار گیرد.

۱۰-۵- استقرار یک تیم مدیریت قرارداد و روابط

اطلاع‌رسانی مناسب بین طرفین، درک متقابل از نیازها و حل به‌موقع مشکلات برای اطمینـــان از کیفیت خدمات ضروری است. برای برآورده ساختن این الزامات، ســـازمان به یک تیم مدیریت روابط شامل افراد و فرآیندها نیازمند اســـت، تا قرارداد برون‌سپاری و روابط کلـــی با ارائه‌کننـــده‌ی خدمات خود را مدیریت کند. انـــدازه و ترکیب این تیم با توجه به نوع خدمات فناوری اطلاعات برون‌سپاری شده و میزان اهمیت آن برای سازمان می‌تواند متنوع باشـــد. وظایف این تیم می‌تواند شامل نظارت بر کیفیت خدمـــات و ارزیابی عملکرد ارائه‌کننده‌ی خدمات، نظارت بر کفایـــت کنترل‌های داخلی، مطابقـــت با قوانیـــن و مقـــررات مربوطه و حل مشکلات به‌وجود آمده در زمینه‌ی ارائه‌ی خدمات و عملکرد باشد.

۱۱-۵- تدوین یک طرح تداوم کسب و کار

ســـازمان بایـــد اطمینان حاصل کنـــد که در صورت توقف فعالیـــت ارائه‌دهنده‌ی خدمات، یا عدم توانایی ارائه‌ی خدمات توســـط وی، امکان دســـترســـی به کلیه‌ی امکانات مورد نیاز خود را خواهد داشت.

۱۲-۵- تهیه‌ی نســـخه‌ی نهایی توافق بین طرفین

یک قرارداد جامع باید مســـتند باشد. سازمان باید درصدد اســـتفاده از خدمات مشاور حقوقی متخصص در زمینه‌ی چنین قراردادهایی باشـــد. برخی از مســـائل با اهمیتی که ســـازمان باید در توافقنامه‌ی برون‌سپاری مورد توجه قرار دهد در ادامه تشریح می‌شود.

دامنه‌ی خدمـــات: دامنه‌ی خدمـــات، مدت آن، دوره‌ی تمدید و حقوق و مســـئولیت‌های دو طرف قرارداد باید به‌وضوح تشریح شده باشـــد. در صورت لزوم، با پیوست و جداول همه‌ی معـــیارهای اندازه‌گـــیری عملکرد، حـــق‌الزحمه و مسئولیت‌های انجام خدمات تعریـــف شـــوند. همچنین توافق باید فرآیندهایی را کـــه بـــدان‌وسیله می‌توان تغییراتی را در خدمات فعلی ایجاد کرد یا خدمات جدیدی اضافه کرد، تعریف نماید.

حق‌الزحمه: قرارداد باید به حق‌الزحمه‌ای که بابت انجام خدمات به حســـاب سازمان منظور می‌شود اشـــاره کند (بر اســـاس حجم یا سایر متغیرهـــا) و نحوه‌ی محاســـبه‌ی حق‌الزحمه‌ی انجام خدمـــات اضافی، نحـــوه‌ی منظور کردن مخارج خرید و نگهداری نرم‌افزار و ســـخت‌افزار، توسعه و تبدیل سامانه‌ها و مواردی از این دست را مشـــخص کند. مدت قرارداد، دوره‌ی تمدید، حق دســـت‌یابی به حق‌الزحمه و محدودیت‌های افزایش حق‌الزحمه نیز باید روشن شود. مسائلی از قبیل فاکتور کـــردن و پرداخت، بازپرداخت و انجام خدمات به‌صـــورت اعتباری، مخارج مورد اختلاف، تســـهیم ســـودها یا زیان غیرمنتظره و هرگونه محرک‌هـــای کاهش هزینه باید تصریح شود.

معیارهـــای اندازه‌گیری عملکـــرد: تعیین معیارهای اندازه‌گیری عملکرد (مانند معیارهایی بـــرای امنیت ســـامانه‌ها، دسترســـی، رازداری، درستی پردازش و زمان) موجب حصول اطمینان از برآورده شدن الزامات سازمان خواهد شد.

مالکیت ســـرمایه‌های فکری: دو طرف باید حقوق و مزایای مرتبط با مالکیت یا حق استفاده از دارایی‌های فکـــری را صراحتاً در قرارداد ذکر کنند. توســـعه‌ی نرم‌افـــزار و طراحـــی تارنماها نمونه‌هایی از آنها است.

کنترل‌ها و حسابرســـی: قرارداد باید مسئولیت ارائه‌کننـــده‌ی خدمات بـــه اســـتقرار و اجرای کنترل‌های داخلـــی کافی مطابق الزامات قانونی از قبیل قوانین خصوصی، قانون ساربنز - آکسلی و الزامات کمیسیون بورس اوراق بهادار آمریکا را به صراحت مشخص کند.

قرارداد باید مســـئولیت طرفیـــن را در مورد اســـتقرار، حفـــظ و اجرای کنترل‌هـــای داخلی تعریف کند. قرارداد باید تعیین کند چه چیز قرار است محافظت شـــود، کدام طرف دارای قدرت تغییر رویه‌ها و الزامات کنترلی است، کدام طرف بابت زیان ناشی از نقض کنترل‌ها مسئول خواهد بود و در صورت نقض کنترل، الزمات هشداردهی چیســـت؟ قرارداد باید ثبت‌ها و رســـیدگی‌های لازم، حق ســـازمان در دسترسی به این ثبت‌ها و مســـئولیت ارائه‌کننده‌ی خدمات جهت ایجاد

اطمینان از دسترسی و حفاظت را تعریف کند.

یکی از الزامات رایج در بسیاری از قراردادهای برون‌سپاری این است که ارائه‌کننده‌ی خدمات، گزارش حسابرس مستقل در خصوص صورت‌های مالی یا وجود و اثربخشی کنترل‌های داخلی خود را به سازمان ارائه کند. در مواردی که امنیت اطلاعات یکی از موضوعات پر ریسک است، مانند عملیات تجارت الکترونیک، ممکن است سازمان آزمون دوره‌ای امنیت را الزامی کند. آزمون نفوذپذیری ، آزمون تشخیص نفوذ ، پویش شبکه یا دیواره‌های آتش یا آزمون طرح بازیابی پس از بحران نمونه‌هایی از این آزمون‌ها هستند. دامنه‌ی حسابرسی، زمان‌بندی و تناوب آن، حق دسترسی به نتایج حسابرسی و آزمون‌ها، تعهد به رفع نواقص گزارش شده و تحمل مخارج باید در قرارداد شرح داده شود.

مسئولیت‌های ارائه‌کننده‌ی اولیه خدمات: قرارداد باید ارائه‌کننده‌ی خدمات را نسبت به خدمات مورد توافق مسئول تلقی کند، چه این خدمات مستقیماً توسط او اجرا شود چه با استفاده از یک پیمانکار دست دوم. الزامات هشداردهنده و اعطای مجوز استفاده از پیمانکار دست دوم توسط ارائه‌کننده‌ی خدمات باید در قرارداد ذکر شوند.

فرآیند حل اختلافات: برخی از مهم‌ترین مواردی که باید در بخش مذکور تعریف شوند عبارت‌اند از: چه چیزی اختلاف را تشکیل می‌دهد، فرآیند حل اختلافات احتمالی، رویه‌های تعدیل و ابزارهای حل اختلاف. مفاد مذکور در حل به‌موقع اختلافات کمک‌کننده بوده و اطمینان می‌دهد طی دوره‌ی حل اختلاف، وقفه‌ای در ارائه خدمات اتفاق نخواهد افتاد.

پوشش بیمه‌ای: ارائه‌کننده‌ی خدمات باید ملزم به هشدار دادن به سازمان در خصوص تغییرات با اهمیت در پوشش بیمه‌ای باشد و مفاد عمومی و شرایط پوشش بیمه‌ای خود را افشا کند.

محدودیت بدهی: بدهی یکی از مسائل اساسی در توافقات برون‌سپاری به‌حساب می‌آید. بدهی نسبی بابت زیان‌ها یا آسیب‌های هر طرف باید به روشنی تعریف شود.

خاتمه: شرایطی که تحت آن طرفین قادر به خاتمه‌ی قرارداد می‌باشند، در مفاد اساسی قرارداد پیش‌بینی شود. حق خاتمه، دوره و شرایط خاتمه (برای مثال چارچوب زمانی اطلاع‌رسانی به طرف دیگر، شرایط جرایم و غیره) مندرج در قرارداد می‌تواند تعیین‌کننده‌ی گزینه‌ی قابل پذیرش در زمان بروز مشکل باشد.

بخش ۶- نتیجه‌گیری

برون‌سپاری فناوری اطلاعات برای بسیاری از سازمان‌ها جذابیت دارد. برون‌سپاری فناوری اطلاعات باید بخش تفکیک‌ناپذیری از راهبرد تجاری یک سازمان به‌حساب آید. منطق برون‌سپاری عبارت است از کسب منافع راهبردی، مالی و فناورانه. ممکن است مشکلاتی در رابطه با کیفیت خدمات، مخارج انجام خدمات یا اثرات کلی آن بر عملیات واحد تجاری به‌وجود آید. در گام نخست، یک ارزیابی ریسک کامل از عوامل شکل‌گیری این مشکلات احتمالی ابزار مناسبی برای اجتناب از آنها است. اگرچه نسخه‌ی کاملی برای حذف ریسک برون‌سپاری فناوری اطلاعات وجود ندارد، برخی از راهکارهای تشریح شده در این مقاله می‌توانند باعث کاهش این ریسک‌ها شوند. مطالعه و درک صحیح از راهبرد فناوری اطلاعات، دقت در انتخاب ارائه‌کننده‌ی خدمات، دقت در تنظیم نسخه‌ی نهایی قرارداد و نظارت مناسب خدمات انجام شده تحت قرارداد برون‌سپاری فناوری اطلاعات از جمله راهکارهایی هستند که به سازمان در جهت دست‌یابی به منافع مورد انتظار کمک خواهند کرد.

در پایان به چند نکته‌ی کلیدی دیگر که با مطالعه‌ی این مقاله باید به آنها پی برده باشیم، اشاره می‌شود:

• بازار برون‌سپاری خدمات فناوری اطلاعات در سال‌های اخیر به‌گونه‌ای چشمگیر در حال رشد بوده است و به‌نظر می‌رسد چنین روند افزایشی در آینده، دست کم درکوتاه‌مدت، نیز استمرار داشته باشد.

• فرآیند برون‌سپاری امکان تمرکز مدیریت بر روی جنبه‌های اصلی فعالیت سازمان را فراهم می‌کند.

• کلید درک برون‌سپاری این است که به‌رغم انتقال اجرای خدمات، مسئولیت‌های ذی‌ربط منتقل نخواهد شد. علاوه بر این، انجام خدمات برون‌سپاری شده باید برای استفاده‌کنندگان خدمات و مشتریان سازمان شفاف باشد.

• اجرای دقیق و کامل برون‌سپاری بدون داشتن یک راهبرد جامع فناوری اطلاعات و یکپارچگی کامل با اهداف و راهبردهای عمومی سازمان امکان‌پذیر نیست.

• سازمان باید قبل از ارزیابی برون‌سپاری دانش کافی از اجزای تشکیل‌دهنده‌ی کارکردهای فناوری اطلاعات خود داشته باشد، تا بتواند تعریف دقیقی از نیازها و الزامات خود در فرآیند مذاکره با ارائه‌کننده‌ی خدمات ارائه دهد.

منابع و مآخذ:

1. Boldea, I & C. Brandas, 2007, "Some considerations about IT outsourcing process".
2. Australian Government, DepartmentofCommunications, InformationTechnologyandthe Arts,2007,"ManagingITSecurity WhenOutsourcingtoanITService Provider: Guide for Owners and OperatorsofCriticalInfrastructure".
3. Chandiramani, S.R, 2007, "Information Technology and Corporate Governance".
4.Caonjur,P&C.Bokhoree,2006, "RiskofInsiderThreatsinInformation Technology Outsourcing: Can deceptivetechniquesbeapplied?".
5.Tho,I,2005,"Managingtherisksof outsourcing".
6. The Canadian Institute of CharteredAccountants,Information TechnologyAdvisoryCommittee, 2003, "Information Technology Outsourcing".

۷. مارشال بی. رامنی، پال جان استین بارت، "سیستم‌های اطلاعاتی حسابداری"، ترجمه‌ی سید حسین سجادی و سید محسن طباطبایی‌نژاد، دانشگاه شهید چمران اهواز، ۱۳۸۵.

* عضو هیأت علمی دانشگاه علامه طباطبایی

** دانشجوی دکتری حسابداری دانشگاه علامه طباطبایی