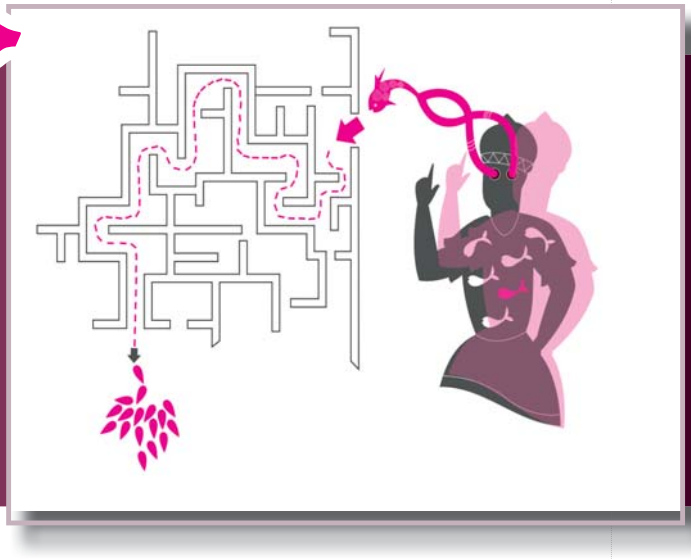
حسابرسی مبتنی بر ریسک با استفاده از کوبیت



ترجمه: محمد میکائیلی
R. Johannessen

در این مقاله، تجاربی که در نتیجه اســتفاده از جعبه ابزار کوبیت (هدفهای کنترلی برای اطلاعات و فناوری مرتبط) به‌دست آمده، بیان می‌شود. هدف مقاله پیش از آن‌که ارائه الگویی برای استقرار حسابرسی مبتنی‌بر ریسک باشد، پیشنهادی تجربی درباره روشی برای حسابرسی است.

هم‌اکنون بیشــتر ســازمانهای خصوصی و عمومی از الگوی کوبیت استفاده می‌کنند. سازمانهایی که از این ابزار استفاده کرده‌اند، تأیید می‌کنند که این الگو، بسیار جامع و به‌طور کامل زمان‌بر است. در وضعیت روزمره فعلی، محدودیت زمانی برای انجام وظایف محول‌شده، با زمان‌بر بودن در تناقض کامل اســت. از اینرو، انتخاب صحیح مهمترین عرصه‌ها و فرایندها که در معرض بالاترین ریســک هستند، اهمیت دارد تا بتوان بیشترین ارزش افزوده را برای صاحبکار ایجاد کرد.

کوبیت، رهنمودی شــفاف برای چگونگی ارزیابی ریســک حسابرسی در ســطح بالا را فراهم نمی‌کند؛ به عبارت دیگر، چگونگی انتخاب مهمترین عرصه‌ها و یا فرایندها برای حسابرسی. از اینرو، در این مقاله الگویی عمومی برای انجام عملیات حسابرسی طراحی شده است. این مدل که بر مبنای ارزیابی کیفی است و انعطاف‌پذیری درخور توجهی در ارتباط با صاحبکار حسابرسی دارد، در **شکل ۱** نشان داده شده است.

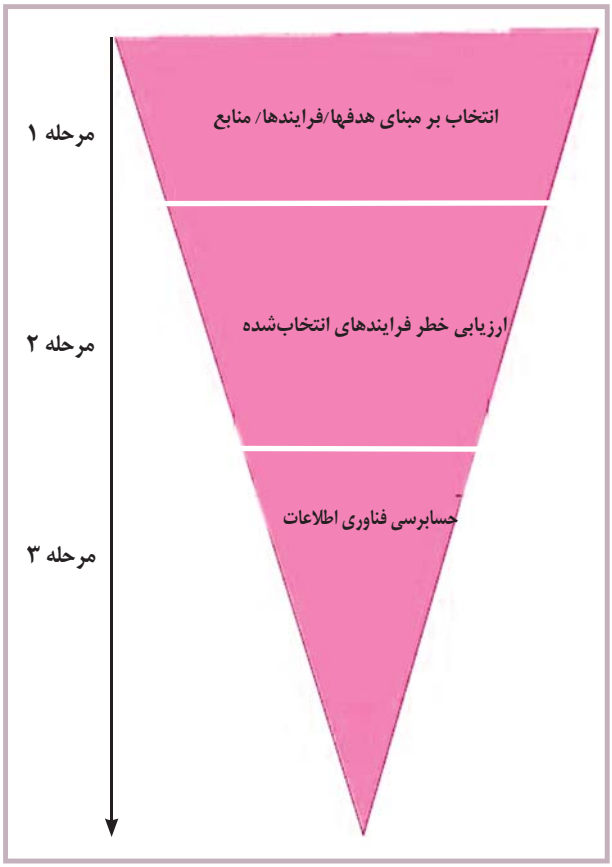
مرحله اول: انتخاب بر مبنای هدفها/فرایندها/منابع

این مرحله متشکل از تصمیم‌گیری در سطح کلی است؛ بر چه چیزی تأکید شود، چه چیزی ممکن است نمونه‌ای از قلمروها، فرایندها، منابع فناوری اطلاعات و یا نمونه‌ای از معیارهای اطلاعات باشــد. حسابرس، بر مبنای اولویتهای انتخاب‌شده، فهرستی از فرایندهایی راکه ممکن اســت برای آزمون عمیقتر مرتبط باشــد، اســتخراج می‌کند. در مثال زیر (**شکل ۲**)، برای نشان دادن مدل یادشده، دامنه «موارد تحصیل و پیاده‌سازی‌شــده» انتخاب شــده و «مدیریت تغییر» و «تحصیل و نگهداشت نرم‌افزار» به‌عنوان بااهمیت‌ترین فرایندها برای صاحبکار حسابرسی شناسایی و از اینرو برای حسابرسی انتخاب شده‌اند.

مرحله دوم: ارزیابی ریسک فرایندهای انتخاب‌شده

در نتیجه انتخاب انجام‌شده در مرحله اول، حسابرس هم‌اکنون نمونه‌ای از فرایندها در اختیار دارد که به‌عنوان اولویت در نظر گرفته شده اند. در این مثال (**شــکل ۲**)، فرایندهای A12 و A16 در قلمرو «تحصیل و پیاده‌سازی» مربوط شناخته می‌شوند. در نتیجه محدودیت زمانی و منابع، اغلب لازم اســت که میزان کار بیشتر کاهش یابد. حسابرس در مرحله ۲، دوباره اولویتهای مربوط به فرایندهایی که در مرحله ۱ تعیین

شکل ۱- مدل انجام عملیات حسابرسی ریسک



شده‌اند را توصیف و سپس پرخطرترین آنها را انتخاب می‌کند. در مثال زیر (**شکل ۳**)، سعی شده است موارد یادشده که در آن حسابرس فرم **شکل ۳** را برای هر یک از فرایندهای انتخاب‌شده در مرحله ۱ کامل می‌کند (در این مثال برای A16)، نشان داده شود.

شکل ۳ مجموعه‌ای از پرسشهای کنترلی مرتبط با هر فرایند را فهرست می‌کند- که از نمره‌های فهرست‌شده زیر عنوان «و مورد توجه قرار می‌گیرد» در صفحه اول هر فرایند، استخراج می‌شود. حسابرس، بر مبنای نمونه انتخابی، برای «حس کردن» روال کارها، مستندها و فرایندهای مورد استفاده در این زمینه را تدوین می‌کند. اطلاعات مورد نیاز برای پاسخ به پرسشهای نمونه، ممکن است از طریق مصاحبه یا مشاهده روال مورد استفاده، جمع‌آوری شود. در این مرحله، حسابرس هیچ‌گونه ارزیابی جامعی از محتوا و کیفیت اطلاعات در دسترس انجام نمی‌دهد.

ستون مربوط به روالهای کنترلی باید با عنوانهای «مستند»، «غیرمستند» یا «نامعلوم» علامت‌گذاری شود. معیارهای **جدول ۱** ممکن است برای پاسخ به پرسشها استفاده شود.

شکل ۲

فرایند فناوری اطلاعات		اهمیت			
		نامعلوم	نه خیلی مهم	مهم	خیلی مهم
تحصیل و استقرار فناوری اطلاعات					
شناسایی راه‌حلها	A۱۱		X		
تحصیل و نگهداری نرم‌افزار	A۱۲				X
تحصیل و نگهداری زیرساختهای فناوری	A۱۳		X		
ایجاد و نگهداری دستورعملها و روال فناوری اطلاعات	A۱۴		X		
نصب و تأیید سیستمها	A۱۵		X		
مدیریت تغییر	A۱۶				X

گام بعدی شامل ارزیابی کلی احتمال وجود خطا، نقطه‌ضعف و راه گریز در فرایند است. نقطه شروع این ارزیابی، بررسی مقدماتی فرایند و هر زمان مناسب باشد، اظهارنظر خود حسابرس است. حسابرس باید عوامل داخلی و خارجی که ممکن است تأثیر منفی بر فرایند داشته باشند را در نظر بگیرد. نتایج این ارزیابی در **جدول ۲** نشان داده شده است.

گام بعدی، ارزیابی پیامدهای یک واقعه منفی است. افزون‌بر هر گونه زیان پولی، عواملی مانند شهرت و محیط کاری باید مورد توجه قرار گیرد. به **جدول ۳** توجه کنید.

به این ترتیب، هر فرایند تابع ارزیابی ریسک از طریق بررسی همزمان احتمال وقوع و پیامدهای ریسک است. بر مبنای ارتباط فرایند با نوع ریسک (بالا، متوسط، پایین)، یک نمونه برای استفاده در مرحله حسابرسی فناوری اطلاعات، انتخاب می‌شود.

مرحله سوم: حسابرسی فناوری اطلاعات

با استفاده از «رهنمود حسابرسی» کوبیت، حسابرسی فناوری اطلاعات روی فرایندهای دارای بالاترین خطرهای

شکل۳

عطف	ریسک				روالهای کنترلی			فرایند فناوری اطلاعات	
	پایین	متوسط	بالا	پیامد	احتمال	نامعلوم	غیرمستند	مستند	
									مدیریت تغییر A16
									۱- آیا تمام درخواستهای مربوط به تغییر و نگهداری سیستم مستند است و تابع رویه‌های رسمی و سازمند تغییر است؟
									۲- آیا تمام درخواستهای تغییر طبق معیارهای روشن دسته‌بندی و اولویت‌بندی شده است؟
									۳- آیا روال سازمان برای مدیریت تغییر، اطمینان ایجاد می‌کند که پیامدهای ناشی از یک تغییر معین، پیش از تأیید شناسایی و ارزیابی شده است؟
									۴- آیا رویه‌هایی ایجاد شده که اطمینان دهد نظارت بر سیستمها در مورد مدیریت تغییر و سیستم کنترل پیکربندی سازمان، وجود دارد؟
									سایر

جدول ۱

مقیاس	روالهای کنترلی
مستند	واحد حسابرسی‌شده، روال یا فرایند یا مستندی برای برخورد با موضوع دارد.
غیرمستند	واحد حسابرسی‌شده، روال یا فرایند یا مستندی برای برخورد با موضوع ندارد.

جدول ۲

مقیاس	احتمال
بالا	احتمال تأثیرپذیری منفی فرایند از رویدادهای داخلی و خارجی بالا است.
متوسط	احتمال تأثیرپذیری منفی فرایند از رویدادهای داخلی و خارجی وجود دارد.
پایین	احتمال تأثیرپذیری منفی فرایند از رویدادهای داخلی و خارجی پایین است.

جدول ۳

مقیاس	نتایج
بالا	انتظار می‌رود وقایع داخلی یا خارجی منفی، پیامد عمده‌ای بر فرایند داشته باشد.
متوسط	انتظار می‌رود وقایع داخلی یا خارجی منفی، پیامد متوسطی بر فرایند داشته باشد.
پایین	انتظار می‌رود وقایع داخلی یا خارجی منفی، پیامد ضعیفی بر فرایند داشته باشد.

شناسایی‌شده، انجام می‌شود (**جدول ۴**).

این مشاهده‌ها و پیشنهادها ممکن است در بسط و توسعه یک رویکرد تجربی در مورد چگونگی انجام حسابرسی مبتنی‌بر ریسک با استفاده از کوبیت، کمک کند.

کوبیت

کوبیت که به‌وسیله **انجمن کنترل و حسابرسی سیستمهای اطلاعاتی** (ISACA) تهیه شده است، شامل استانداردهای پذیرفته‌شده برای امنیت فناوری اطلاعات و فعالیتهای

جدول ۴

	فرایند فناوری اطلاعات و پرسشهای حسابرسی	نتایج ارزیابی و آزمون	توصیه	عطف
A16	**تغییر مدیریت**			
	آیا روشی برای اولویت‌بندی تغییرهای توصیه‌شده از جانب کاربران، وجود دارد؟ اگر بلی، از آن استفاده می‌شود؟ آیا رویه‌های مدون برای تغییرها ناگهانی وجود دارد؟ اگر بلی، مورد استفاده قرار می‌گیرند؟ آیا رویه رسمی برای نظارت بر تغییرها وجود دارد؟ اگر بلی، مورد استفاده قرار می‌گیرد؟ آیا تغییرها به‌گونه‌ای در سیستم ثبت می‌شوند که نشان دهند به‌نحو رضایتبخش انجام شده‌اند؟ سایر موارد.	**مشاهده:** - روش تغییرها ... - هیچ رویه‌ای برای تغییرها ناگهانی وجود ندارد ... سایرموارد **ارزیابی:**- روش‌شناسی مورد نظر، از نظر تغییرها ناگهانی کامل نیست ... **نتیجه‌گیری:** - روش‌شناسی ناکافی است ...	توصیه می‌شود...	

کنترلی است که فراهم‌کننده یک چارچوب مرجع برای مدیریت، استفاده‌کنندگان، حسابرسان سیستمهای اطلاعاتی و متخصصان امنیت و کنترل می‌باشد.

کوبیت شامل محصولات اصلی زیر است:

چارچوب مفهومی: یک سازمان موفق روی چارچوب مفهومی مستحکم از اطلاعات و داده‌ها ساخته می‌شود. چارچوب مفهومی، فرایندهای فناوری اطلاعات در انتقال اطلاعاتی که واحد تجاری در دستیابی به اهدافش به آن نیاز دارد را تشریح می‌کند.

این انتقال با ۳۴ هدف کنترلی سطح بالا (هر کدام برای یک فرایند فناوری اطلاعات) و در ۴ قلمرو، کنترل می‌شود. این چارچوب مفهومی مشخص می‌کند کدامیک از هفت معیار اطلاعات (اثربخشی، کارایی، محرمانگی، درستی، دسترس‌پذیری، رعایت و اتکاپذیری)، و همچنین کدام منابع فناوری اطلاعات (افراد، برنامه‌های کاربردی، فناوری، تسهیلات و تجهیزات و داده‌ها) برای فرایندهای فناوری اطلاعات اهمیت دارند تا از هدفهای کسب‌وکار به‌طور کامل پشتیبانی کنند.

رهنمود مدیریت: برای حصول اطمینان از موفق بودن واحد تجاری، باید پیوند سیستمهای اطلاعاتی و فرایندهای تجاری به‌طور مؤثر مدیریت شود. رهنمود مدیریت جدید متشکل از الگوهای بلوغ، عوامل اصلی موفقیت، شاخصهای اصلی هدف و شاخصهای اصلی عملکرد است. رهنمود مدیریت، در پاسخدهی به نگرانیهای فوری تمام افرادی که در موفقیت بنگاه سهم دارند، کمک خواهد کرد.

اهداف کنترلی تفصیلی: کلید حفظ سودآوری در محیط با تغییرهای فناوری، بستگی به حفظ کنترل دارد. هدفهای کنترلی کوبیت، بینش بااهمیتی را فراهم می‌کند که برای ترسیم یک سیاست شفاف و عملکرد خوب برای کنترلهای فناوری اطلاعات، مورد نیاز است. این موارد شامل بیانیه نتایج مورد انتظار یا هدفهایی است که باید با پیاده‌سازی ۳۱۸ هدف کنترلی مشخص و تفصیلی از میان ۳۴ هدف کنترلی سطح بالا، به‌دست آیند.

رهنمودهای حسابرسی: تجزیه‌وتحلیل، ارزیابی، تفسیر، واکنش و پیاده‌سازی. برای به‌دست آوردن هدفهای مورد انتظار، رویه‌های مورد استفاده باید به‌طور مداوم و یکنواخت حسابرسی شوند. رهنمودهای حسابرسی، فعالیتهای واقعی متناظر با هر یک از ۳۴ هدف کنترلی فناوری اطلاعات را پیشنهاد داده و مشخص می‌کند و در همان حال، ریسک هدفهای کنترلی پاسخ‌داده‌نشده را آشکار می‌سازد.

مجموعه ابزار پیاده‌سازی: مجموعه ابزار پیاده‌سازی، شامل آگاهی مدیریت و امکانات عیب‌شناسی فناوری اطلاعات، راهنمای پیاده‌سازی، پرسشهای متداول، بررسی موارد خاص از سازمانهایی که به‌تازگی از کوبیت استفاده کرده‌اند و فیلمهای آموزشی که می‌تواند در معرفی کوبیت به دیگر سازمانها مفید باشند، است. این مجموعه ابزار برای تسهیل پیاده‌سازی کوبیت،طراحی شده و مطالب آموخته‌شده از سازمانهایی که با سرعت و موفقیت کوبیت را در محیط کار اجرایی کرده‌اند را منتقل و در انتخاب گزینه‌های پیاده‌سازی به مدیریت کمک می‌کند.

منبع:

Johannessen R., Risk-based Sampling Using COBIT, Into IT INTOSAI IT, 2004