Journal of
Professional Auditing Research
Spring 2024, V.4, No 14 pp 158-184

COSO in the Cyber Age and Auditing cyber risks

Javad Shekarkhah[1], seyed hamid mousavibasir[2]

Received: 2023/08/29
Approved: 2023/12/09

Review Paper

Abstract:

The more information organizations have about the cyber threats most likely to affect substruction, the better they can reduction cyber risk. The purpose of this research is to review how the COSO (2013) helps risk management and cyber risk controls. It also shows the role of Internal auditing in cyber risk management control for organizations. Based on the library research method, previous researches have been studied and their results have been analyzed and examined. The results of this study indicate that organizations should invest in cyber risk management and prioritize cyber risk control, strategic goals and future plans depending on their positions. As the cyber environment evolves, risk management and internal auditing will need to keep pace. . Indeed, By focusing on the implementation of the 2013 framework, companies will identify their cyber risks and at the best opportunity, they will show their readiness to react appropriately to face the risks caused by the cyber world. Finally, creating a culture based on cyber security, continuous evaluation of all technologies used, continuous evaluation of vulnerable systems, comprehensive analysis of examples of cyber attacks carried out in organizations, continuous cyber risk management activities and cyber security training, These are the most important things that organizations should consider.

Key Words: COSO and cyber risks, cyber security, cyber age, Auditing cyber risks

10.22034/JPAR.2023.2010425.1211

1. Associate Professor. Department of Accounting, Faculty of Management and Accounting, Allameh Tabatabai University, Tehran, Iran. (Corresponding Author) shekarkhah@atu.ac.ir
2. MSc of Management Accounting ,Allameh Tabatabai University, Tehran, Iran. s.h.musavibasir@gmail.com
http://article.iacpa.ir

فصلنامه‌ی پژوهش‌های حسابرسی حرفه‌ای
JPAR Journal of Professional Auditing Research
سال چهارم، شماره چهاردهم، بهار ۱۴۰۳، صص ۱۵۸-۱۸۴

چارچوب کنترل داخلی یکپارچه در عصر سایبری و حسابرسی ریسک سایبری

جواد شکرخواه[1]✉، سیدحمید موسوی بصیر[2]

مقاله‌ی ترویجی

تاریخ دریافت: ۱۴۰۲/۰۶/۰۷
تاریخ پذیرش: ۱۴۰۲/۰۹/۱۸

چکیده:

هرچقدر سازمان‌ها اطلاعات بیشتری در مورد تهدیدات سایبری که به احتمال زیاد بر زیرساخت‌ها تأثیر می‌گذارند داشته باشند ، بهتر می‌توانند ریسک سایبری را کاهش دهند. هدف از این تحقیق بررسی این موضوع است که چگونه چارچوب کنترل داخلی یکپارچه (۲۰۱۳) به مدیریت ریسک وکنترل‌های ریسک سایبری کمک می‌کند. و همچنین نقش حسابرسی داخلی در کنترل مدیریت ریسک سایبری، برای سازمان‌ها را نشان می‌دهد. با اتکا به روش پژوهش کتابخانه‌ی، تحقیقات پیشین مورد مطالعه و نتایج آنها مورد تجزیه و تحلیل و بررسی قرار گرفته است. نتایج حاصل از این پژوهش بیانگیر این مطلب می‌باشد که سازمان‌ها باید در زمینه مدیریت ریسک سایبری سرمایه‌گذاری کنند و بسته به جایگاه‌های که درآن قرار دارند کنترل ریسک سایبری را در اولویت، اهداف استراتژیک و برنامه‌های آتی قرار دهند. همانطور که محیط سایبری تکامل می‌یابد، مدیریت ریسک و حسابرسی داخلی باید سرعت خود را حفظ کنند و در مرحله برنامه ریزی برنامه حسابرسی، باید چشم‌انداز تهدید سایبری گسترده را در نظر بگیرد. درحقیقت، سازمان‌ها با تمرکز روی اجرای چارچوب ۲۰۱۳ ریسک‌های سایبری خود را شناسایی و در بهترین فرصت آمادگی عکس العمل مناسب جهت مقابله با خطرات ناشی از دنیای سایبری محور را، از خود نشان خواهد داد. در نهایت، ایجاد فرهنگی برمبنای امنیت سایبری، ارزیابی مستمر تمامی تکنولوژی‌هایی مورد استفاده، ارزیابی مستمر سیستم‌های آسیب‌پذیری، تحلیلی جامع در مورد نمونه حمله‌های سایبری انجام شده در سازمان‌ها، انجام فعالیت‌های مدیریت ریسک سایبری بصورت مستمر و آموزش امنیت سایبری، مهمترین مواردی هستند که باید مد نظر سازمان‌ها قرار گیرند.

واژه‌های کلیدی: کوزو و ریسک‌های سایبری، ایمنی و عصر سایبری،عصر سایبری، حسابرسی ریسک سایبری

10.22034/JPAR.2023.2010425.1211

۱. دانشیار،گروه حسابداری، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی، تهران، ایران. (نویسنده مسئول) shekarkhah@atu.ac.ir
۲. کارشناسی ارشدحسابداری مدیریت، دانشگاه علامه طباطبایی، تهران، ایران. s.h.musavibasir@gmail.com

http://article.iacpa.ir

۱- مقدمه

در سال ۱۹۹۲، زمانی که چارچوب یکپارچه کنترل داخلی (COSO)[۱] (چارچوب ۱۹۹۲) منتشر شد، اداره کسب‌وکارها بسیار متفاوت بود. در طول دو دهه گذشته، فناوری اطلاعات (IT)[۲] به‌طور چشمگیری راه و روش اداره کردن کسب‌وکار را در دنیای تجارت به جهان سایبری-محور[۳] تبدیل کرده است. سفارشات مشتریان در حال حاضر، به وسیله مبادلات الکترونیکی داده‌ها در اینترنت و بدون دخالت انسان و یا با دخالت خیلی کم انسان پردازش داده می‌شود. فرآیند کسب‌وکار ارائه‌دهندگان خدمات توسط شبکه‌های متصل به هم برون سپاری شده است. اکثرا پرسنل شرکت کار خود را از راه دور و یا درخانه، و با نیاز بسیارکمی به دفتر کار انجام می‌دهند. فهرست موجودی در انبار از طریق استفاده از فرکانس رادیوای (RFID) برچسپ‌ها[۴] دنبال می‌شود. صرفا بانک‌های انلاین وجود دارند و تقریبا همه بانک‌ها خدمات اینترنتی به مشتریان پیشنهاد می‌کنند.کسب‌وکار و تکنولوژی بنابر چارچوب ۲۰۱۳ تکامل پیدا کردند. یکی از مبانی بنیادی به روزرسانی و انتشار چارچوب در سال ۲۰۱۳ نیاز به چگونه آشنایی سازمان‌ها در استفاده و تکیه بر تکنولوژی درحال تکامل برای اهداف داخلی بوده است. در چارچوب کنترل داخلی ۲۰۱۳ روش‌های جهت اینکه سازمان‌ها باید به نوآوری در مدیریت فناوری اطلاعات متمرکز شوند، افزایش یافت. از جمله موارد نوآوری در مدیریت فناوری اطلاعات می‌توان به موارد زیر اشاره کرد: جهانی شدن بازارها و عملیات، پیچیدگی بیشتر فرآیندهای کسب‌وکار، خواسته‌ها و پیچیدگی‌ها در قوانین و مقررات، آیین نامه‌ها و استانداردها، استفاده وتکیه برفناوری درحال تکامل؛ ودرنهایت انتظارات مربوط به پیشگیری و کشف تقلب (مری[۵]، ۲۰۱۵).

از زمانی که چارچوب اصلی در سال ۱۹۹۲ منتشر شد، نوآوری در کسب‌وکار، ساختار پیچیده غنی از به‌هم‌پیوستگی در اینترنت به وجود آورده است. بنابراین، اینترنت در درجه اول برای به اشتراک گذاری اطلاعات طراحی شده و نه محافظت از اطلاعات. هر روز، گزارش‌های متعددی از رسانه‌ها در مورد حوادث قابل توجه سایبری وجود دارد. وقتی که حملات سایبری در یک سازمان اتفاق می‌افتد و در اخبار و رسانه‌ها پوشش داده می‌شود، همه سازمان‌ها در معرض خطر حملات سایبری قرار می‌گیرند. اطلاعات، سیستم‌ها و دارایی‌های که دارای ارزش افزوده هستند، درهرنقطه خاص در هر زمان که باشند عامل تحریک‌کننده برای حملات سایبری هستند. تا زمانی که حوادث سایبری ادامه داشته باشد بر روی وضعیت مالی شرکت تاثیر منفی دارد. تا زمانی که وقایع سایبری ادامه یابد به طور چشم‌گیری اثر منفی بر رفاه مالی شرکت‌های قربانی دارد و نیاز به بررسی قانونی دقیق و اضافی را می‌طلبد، حملات سایبری تا رویدادهای سطح بالایی که میزان فشار بالایی را به دنبال دارد ادامه خواهد یافت. برای رسیدن به این افزایش دیجیتال باید توجه ویژه به داده‌ها، به خصوص داده‌های که توسط شرکت‌ها یا احزاب خارجی مانند ارائه‌دهندگان خدمات برونسپاری که اطلاعات شرکت را به اشتراک دارند و لایه‌ای از پیچیدگی، نوسانات و وابستگی به زیر ساخت‌های که به طور کامل در کنترل این سازمان نیست، را داشته باشیم. گرچه در محل بین شرکت و طرف‌های خارجی[۶] (به عنوان مثال، ارائه‌دهندگان خدمات، فروشندگان،

و مشـــتریان) برای اداره کردن عملیات کسب‌وکار روابط اعتماد و کنترل ممکن است برقرار شود، ولی این خود باعث می‌شود که اطلاعات و ارتباطات الکترونیکی را به اشتراک بگذارند. دیجیتالی شدن سریع اقتصاد و روابط اجتماعی دلیل اصلی اهمیت یافتن مسایل ریسک سایبری، تهدیدات ســـایبری و امنیت سایبری اســـت (مری، ۲۰۱۵). علیرغم افزایش تعداد مقالات تحقیقاتی در این زمینه‌ها، مقالات علمی که ریســـک ســـایبری را تعریف می کنند نسبتاً کمیاب هستند. علاوه بر این، تعریف یکنواخت پذیرفته شـــده از ریسک سایبری هنوز به تصویب نرسیده است که احتمالاً به دلیل ماهیت بین رشـــته ای این مفهوم و پویایی تغییر آن اســـت. این تحقیق به ادبیات مربوط به ریســـک سایبری، امنیت سایبری و مدیریت ریسک سایبری کمک می‌کند، همچنین این مقاله به بررســـی اجزای کنترل داخلی پرداخته اســـت و در ادامه نشـــان خواهد داد که چگونه هر یک از اجزا با ســـایر اجزا مرتبط هســـتند و چگونه فرآیند ارزیابی ریسک سایبری نیاز دارد که پویا و مستمر باشـــد. محیط کنترلی و فعالیت‌های کنترلی شرکت برای بررسی ریسک کنترلی بنیادی هستند. به عبارت دیگر سازمان‌ها برای رسیدن به امنیت، مراقبت و بهبود، ترکیب کنترل داخلی باید بروز باشـــد. در غیر این صورت این احتمال وجود دارد که یک ســـازمان به اندازه کافی قادر به درک ریســـک ســـایبری، گســـترش تاثیر طراحی فعالیت‌های کنترل داخلی و پاسخگویی‌های متناســـب به ریســـک ســـایبری به طور کارا نباشـــد. و همچنین تمرکز اصلی این مقاله بر روی، مدیریت ریسک سایبری، تعریف ریسک ســـایبری، نقش فناوری اطلاعات در سازمان‌ها، سیستم اطلاعاتی بر اســـاس چارچوب۲۰۱۳ کوزو، ارزیابی ریسک ســـایبری بر اساس کوزو ، فعالیت‌های نظارتی و مدیریت ریسک سایبری، تکامل ریسک سایبری، ملاحظات کلیدی امنیت سایبری برای سال۲۰۲۲، تکنیک‌های پیشگیری از خطر تهدیدات سایبری، تکنیک‌های کاهش ریسک سایبری، چشم‌انداز و آینده ریسک سایبری واقع شده است، در نهایت به مقوله نقش حسابرسی داخلی در حسابرســـی ریسک‌های سایبری و رویکرهای موجود در این زمینه که حسن ختام این مقاله است بحث خواهد شد.

۲- مبانی نظری پژوهش

ریســـک سایبری به دلیل تأثیرات فاجعه بار بالقوه آن بر سیستم های اطلاعاتی سازمانی، خطر اعتبار و از دست دادن بالقوه اعتماد مصرف کننده و ذینفعان، تهدیدی رو به رشد برای مؤسسات دولتی و خصوصی اســـت. با ظهور اینترنت و گســـترش فناوری اطلاعات، شـــرکت‌ها، موسسات غیرانتفاعی و دولتی عموماً برای شناسایی و مقابله با این خطر آمادگی نداشتند، اما این تهدید به مرور زمان و شدت آن افزایش یافته است. حملات نیز تغییر کرده است. در بسیاری از موارد اولیه، عاملان حملات سایبری و کمپین‌های اختلال در اطلاعات، عملیات تجاری را صرفاً برای سرگرمی خود قطع می‌کردند، یا نفوذ به زیرســـاخت فناوری اطلاعات شـــرکت را یک چالش می‌دانستند. آنها وب‌ســـایت‌ها را تخریب می‌کنند یا ســـرورها را به منظور تشـــدید یا به چالش کشیدن دیگر متخصصان ســـایبری به منظور اثبات اینکه می‌توانند این کار را انجام دهند، نه برای ســـود بردن،

از بین می‌برند(هالام باکر،۲۰۰۸). با این حال، با رشـــد اینترنت و شکوفا شدن تجارت الکترونیک، دسترســـی کارکنان به داده‌های شرکت افزایش یافته است، و دسترسی از راه دور به سیستم‌های کامپیوتری داخلی رایج شده است، مهاجمان سایبری تکامل یافته و پیچیده‌تر شده‌اند و اثرات آنها ویران‌کننده‌تر (رحمانن، ۲۰۱۱). تهدیدها و مهاجمان ســـایبری کنونی به طور فزاینده ای بر سود بردن از پیامدهای اقدامات حمله خود متمرکز شـــده اند و یا از داده‌هایی که به طور غیرقانونی به دســـت می‌آورند برای منافع شخصی، برای بازیابی خدمات می‌باشد (مایلارت و همکاران، ۲۰۱۰). اثر موجی که حملات سایبری می‌تواند ایجاد کند می‌تواند بر تامین‌کنندگان، کاربران نهایی و خود ســـازمان تأثیر بگذارد و حتی می‌تواند این پتانسیل را داشته باشد که بخش‌های بزرگی از اقتصاد را بی‌ثبات کند، اگر هدف حملات ســـایبری از نظر سیستمی مهم باشد (مانند یک سیستم مالی مهم، مؤسسات، اپراتورهای آب و برق، تأسیسات تصفیه آب، شبکه حمل و نقل و غیره). علاوه بر این، تکنیک‌های جاسوســـی سایبری به سرعت در حال توسعه هستند و اسرار تجاری سازمانی را نیز در برابر سرقت رقبا آسیب‌پذیر می‌کنند (پاتریک و همکاران، ۲۰۱۲). جهانی شدن، دیجیتالی شـــدن و فناوری‌های هوشـــمند، گرایش و شدت جرایم سایبری را تشـــدید کرده است. در حالی که این یک زمینه تحقیقاتی و صنعتی در حال ظهور اســـت، اهمیت سیســـتم‌های دفاعی امنیت سایبری قوی در سطوح شرکتی، ملی و فراملی برجسته شده است. تأثیرات امنیت سایبری ناکافی برآورد می‌شود که در سال ۲۰۲۰ مبلغ ۹۴۵ میلیارد دلار برای اقتصاد جهانی هزینه داشته باشد (مالکس و همکاران، ۲۰۲۰). آســـیب‌پذیری‌های سایبری آسیب‌های قابل توجهی را برای شرکت ایجاد می‌کنند، از جمله وقفه در کســـب‌وکار، نقض حریم خصوصی و زیان‌های مالی (شـــیحان و همکاران، ۲۰۱۹). علیرغم ارتباط روزافزون برای اقتصاد بین‌المللی، در دســـترس بودن داده‌ها در مورد خطرات سایبری محدود است. دلایل این بسیار زیاد است. اولاً، این یک خطر در حال ظهور و در حال تکامل اســـت. بنابراین، منابع داده‌های تاریخی محدود هستند (بینر، ۲۰۱۵). همچنین می تواند به این دلیل باشـــد که به طور کلی، مؤسساتی که هک شده‌اند، رویدادها را منتشر نمی کنند(ایلانگ و همکاران، ۲۰۱۶) . فقدان داده‌ها، چالش‌هایی را برای بســـیاری از زمینه‌ها، مانند تحقیق، مدیریت ریســـک و امنیت ســـایبری ایجاد می‌کند (فالکو، ۲۰۱۹) . اهمیت این موضوع با اعلام شـــورای اروپا در آوریل ۲۰۲۱ نشـــان می‌دهد که مرکز عالی امنیت ســـایبری برای تجمیع ســـرمایه‌گذاری‌ها در تحقیق، فناوری و توسعه صنعتی، ایجاد شده است. هدف این مرکز افزایش امنیت اینترنت و ســـایر شبکه‌های حیاتی و سیستم‌های اطلاعاتی اســـت (شورای اروپا ۲۰۲۱). تخمین زده می‌شـــود که جرایم ســـایبری در ســـال ۲۰۲۰ کمتر از ۱ تریلیون دلار برای اقتصاد جهانی هزینه داشـــته باشد که نشـــان دهنده افزایش بیش از ۵۰ درصدی از سال ۲۰۱۸ است. با افزایش میانگین خسارت بیمه سایبری از ۴۵۰۰۰ دلار در سال ۲۰۱۹ به ۳۵۹۰۰۰ دلار در سال ۲۰۲۰، روند رو به رشـــدی وجود دارد. که ضرورت منابع اطلاعاتی سایبری بهتر، پایگاه‌های داده استاندارد، گزارش اجباری و آگاهی عمومی را نشان می‌دهد (مارتین و همکاران،۲۰۲۱). براساس گزارش[۷] Cybersecurity Ventures پیش‌بینی می‌شـــود که جرایم ســـایبری در سال ۲۰۲۳،

مبلغ ۸ تریلیون دلار برای جهان هزینه داشـــته باشـــد. طبق بررسی‌های متعدد مشخص شده که بزرگی بازار جرایم ســـایبری این حوزه را به ســـومین اقتصاد بزرگ دنیا تبدیل کرده است. ارزش بازار جرایم سایبری در حالی تا ۸ تریلیون دلار برآورد شده که حجم تولید ناخالص داخلی آمریکا بیش از ۲۳ تریلیون دلار اســـت و در رتبه نخست جهان قرار می‌گیرد. در رتبه دوم، چین با تولید ناخالـــص داخلی با ارزش بیـــش از ۱۷ تریلیون دلار قرار گرفته و اقتصاد بزرگ بعدی، بازار جرایم سایبری است.

مدیریت ریسک سایبری

مدیریت ریســـک سیستم را قادر می سازد تا با اثرات عدم قطعیت بر فعالیت تجاری کنار بیاید. بر اســـاس اســـتانداردهای بین المللی (ISO ۲۰۱۸ [۸])، هدف مدیریت ریسک، ایجاد و حفاظت از ارزش است. برای این منظور، عملکرد سازمان را افزایش می دهد، نوآوری را تشویق می کند و از دستیابی به اهداف تعیین شده حمایت می کند. برای اینکه فرآیند مدیریت ریسک موثر و کارآمد باشد، باید اصول اساسی در نظر گرفته شود. وظایف مدیریت ریسک باید متناسب با سطح ریسکی که یک ســـازمان با آن مقابله می‌کند، در راستای ســـایر فعالیت‌های سازمان باشد و باید جامع و درون سازمان باشد. در نهایت، آنها باید در برابر خطرات آتی و در حال تغییر فعال و واکنش نشان دهند. (لوبوریک ۲۰۱۹).

در میـــان ریســـک‌هایی که در فعالیت‌های تجاری با آن مواجه اســـت، ریســـک‌های عملیاتی، ریســـک‌هایی هســـتند که ناشـــی از رویدادهای بیرونی یا سیســـتم‌ها، افراد و فرآیندهای داخلی بد و بی‌ثمر، هســـتند. ریسک‌های سایبری به دسته ریســـک‌های عملیاتی تعلق دارند، حتی اگر ویژگی‌های عجیب و غریبی را نشـــان دهند. در این راستا، به خوبی شناخته شده است که محیط خطرات ســـایبری به دلیل فناوری‌های جدید و توسعه سریع سیستم‌های اطلاعات رایانه‌ای، دائماً در حال تغییر اســـت. تکنیک های حمله به طور مداوم تغییر می‌کنند و می‌توانند به روشی آسان و ارزان انجام شوند (آلبینا ارلاندو، ۲۰۲۱).

در بارومتر ریســـک آلیانز[۹] ۲۰۲۰ ، بیش از ۲۷۰۰ کارشـــناس مدیریت ریســـک از ۱۰۲ کشور و منطقه به ما می‌گویند که حوادث ســـایبری مهم‌ترین ریســـک تجاری در نظر گرفته می‌شـــود. خطرات ســـایبری همچنان در حال تکامل هستند و کسب‌وکارها با تعداد فزاینده‌ای از چالش‌های جدید مقابله می‌کنند، که شـــامل نقض داده‌های بزرگتر و گرانتر، افزایش باج افزار حوادث ایمیل تجاری (جعل) و همچنین امکان طرح دعوی قضایی پس از یک رویداد اســـت. در نتیجه، بسیاری از شـــرکت‌ها می‌دانند که ریسک سایبری جزء کلیدی مدیریت ریسک سازمانی (ERM[۱۰]) است و هدف اصلی آنها تقویت انعطاف پذیری ســـایبری اســـت. یعنی «توانایی سیستم‌ها و سازمان‌ها بـــرای مقاومت در برابر رویدادهای ســـایبری، که با ترکیب میانگین زمان تا شکســـت و میانگین زمان بازیابی اندازه‌گیری می‌شـــود». مدیریت ریسک امنیتی شـــامل شناسایی، ارزیابی و درمان ریســـک‌های مرتبط با یکپارچگی، در دسترس بودن و محرمانه بودن دارایی‌های سازمان است، با آگاهی کامل از اینکه ریســـک باقیمانده باید پذیرفته شود. در واقع، اتخاذ بهترین رویه‌های امنیت

ســـایبری و تنظیم اقدامات متقابل مختلف، اجتناب از حوادث سایبری را، صرف‌نظر از هزینه‌های قابل‌توجه، تضمین نمی‌کند. پذیرش ریســـک باقیمانده بخشـــی از امنیت سایبری همراه با تلاش برای مدیریت ریسک سایبری است(مارتینال و همکاران، ۲۰۱۸).

تعریف ریسک سایبری

ریســـک ســـایبری به عنوان ریســـک مرتبط با یک رویداد الکترونیکی مخرب که باعث اختلال در کســـب‌وکار و ضرر مالی می‌شـــود، تعریف می شود. ریسک ســـایبری تمام خطرات مربوط به فعالیت آنلاین، مانند ذخیره داده‌های شخصی در اینترنت یا انجام تراکنش‌های آنلاین که ممکن اســـت منجر به آسیب به شـــهرت، ضرر مالی، اختلال در زندگی یا تجارت شود را پوشش می‌دهد (NAIC[۱۱] , ۲۰۱۸) ریســـک سایبری با این موارد مشخص می‌شـــود: علت دیجیتالی، آسیب به دارایی‌های دیجیتال، علت دیجیتالی، آســـیب به دارایی‌های فیزیکی یا علت فیزیکی آســـیب به دارایی‌های دیجیتال (آهمی و همکاران، ۲۰۱۸).

ریســـک سایبری شامل هرگونه خطر ناشی از استفاده از فناوری اطلاعات و ارتباطات (ICT[۱۲]) اســـت که محرمانه بودن، در دسترس بودن یا یکپارچگی داده‌ها یا خدمات را به خطر می اندازد. اختلال در فناوری عملیاتی(OT[۱۳]) در نهایت منجر به اختلال در کســـب و کار، خرابی (بســـیار حیاتی) زیرســـاخت و آســـیب فیزیکی به انسان‌ها و دارایی‌ها می‌شـــود. خطر سایبری یا ناشی از بلایای طبیعی است یا توسط انسان ساخته شده است، جایی که ممکن است بلایای سایبری ناشی از شکســـت انسانی باشد. شـــامل جنایت (مانند اخاذی، کلاهبرداری)، جنگ سایبری یا تروریسم سایبری است (ایلینگ و همکاران، ۲۰۱۶).

فناوری اطلاعات در سازمان‌ها

با پیدایش کامپیوتر، دنیا به ســـرعت در حال تغییر بوده و عملیات‌های کسب‌وکار نیز به واسطه بهبـــود مداوم فناوری با ســـرعت فراوانی در حال تغییر هســـتند.گزارش‌هایی در خصوص دزدی اطلاعات، کلاهبرداران کامپیوتری، ســـوء اســـتفاده از اطلاعات و سایر دغدغه‌های کنترل فناوری اطلاعات به کرات در اطراف جهان شـــنیده می‌شوند. سازمان‌ها به لحاظ اطلاعاتی هشیارتر بوده، افراد به دلیل تمرکززدایی پراکنده شده و کامپیوترها در کلیه حوزه‌های تجاری به طور گسترده‌ای اســـتفاده می‌شوند. به دلیل گســـتردگی ســـریع فناوری‌های کامپیوتری و آسان بودن دسترسی به اطلاعات، حسابرســـان داخلی آموزش دیده و ماهر در کار لازم اســـت تا اطمینان حاصل شود کـــه کنترل‌های موثری برای حفظ یکپارچگی داده‌ها و مدیریت دسترســـی به اطلاعات قرار داده می‌شـــوند. همچنین آنها باید با محیط عملیاتی برای ارزیابی اثر بخشـــی کنترل‌های داخلی آشنا شده و شناخت لازم را از آن بدست آورند (فلامرزی و همکاران،۱۳۹۵).

فناوری اطلاعات در سازمان‌ها تاثیر بسزایی دارد. این فناوری افراد و گروه‌های مورد نیاز را دور هم جمع می‌کند؛ مانند تیم‌های مجازی جوامع مجازی، تجارت مجازی و تجارت اشتراکی. مبادله اطلاعات، دسترسی آسان به داده‌ها از راه دور، کارکنان یک سازمان را قادر می‌سازد تا واحد کاری خـــود را به طور پویا در موقعیت‌های جغرافیایی و ابعـــاد زمانی متفاوت ایجاد کنند. بنابراین، یک

سازمان می‌تواند شانش بهتری در تبدیل شدن به کلاس جهانی به واسطه انعطاف‌پذیر بودن و مجازی بودن داشته باشد (میرقان[۱۴]، ۲۰۰۶).

سیستم اطلاعاتی بر اساس چارچوب یکپارچه ۲۰۱۳

سیستم اطلاعاتی مجموعه‌ای ازفعالیت‌ها، شامل افراد، فرآیندها، داده‌ها تعریف شده است، که سازمان‌ها را در جهت دستیابی به سطح بهینه تولید و برقرای ارتباط معاملات برای پاسخگویی، اندازه‌گیری و بررسی عملکرد واحد تجاری به منظور پیشبرد دستاوردها و اهداف سازمان سوق می‌دهد. در حالی که بنگاه‌ها هنگام به اشتراک‌گذاری اطلاعات درمورد فناوری خود خیلی محتاط عمل می‌کنند، هر دو اطلاعات داخلی و خارجی برای محافظت از عملیات کسب‌وکار در مقابل طیف عاملان سایبری قرار می‌گیرند. آنها به اشتراک‌گذاری اطلاعات را، بدون اعلام روز، با کمی ترس از عواقب قانونی، و اغلب با مقدار زیادی از گمنامی فاش می‌کنند. حمله‌کنندگان سایبری، برای حمله به داده‌های مورد هدف خود به صورت اهرمی از تکنولوژی استفاده می‌کنند. واقعیت این است که ریسک سایبری چیزی است غیر قبل اجتناب، و به جای برطرف کردن این ریسک، باید آن را اداره و مدیریت کرد (مری، ۲۰۱۵).

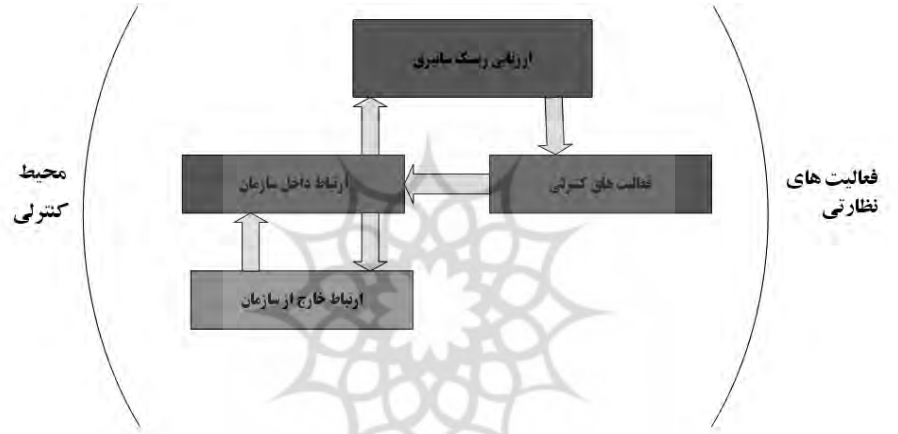
به رغم این که مراتب رسیدن به تهدید سایبری روشن است، اما محافظت از تمام داده‌ها امکان پذیر نمی‌باشد، به همین دلیل برای حمایت از عملیات سازمان نحوه اهداف، فرآیندها و فناوری سازمان متحول خواهد شود. هر سیر تکامل، فرصت آسیب پذیری را ایجاد می‌کند درحالی‌که این سیر تکاملی می تواند برای به حداقل رساندن فرصت‌های آسیب پذیری به دقت مورد استفاده قرار گیرد، اطمینان صد درصدی در عمل غیر ممکن است. علاوه براین، تحول حملات سایبری، برای یافتن راه‌های جدید برای بهره‌برداری از نقاط ضعف ادامه پیدا می‌کنند. درنتیجه واقعیت این است که ریسک سایبری چیزی است غیر قابل اجتناب و به جای برطرف کردن کامل ریسک، باید آن را اداره و مدیریت کنیم. استفاده ازچشم‌انداز برای داده‌ها در سازمان خیلی مهم است. مدیریت باید در هزینه کنترل امنیتی برای حفاظت از مهمترین دارایی‌های خود، سرمایه‌گذاری کند. به منظورمدیریت ریسک‌های سایبری در وضعیت منعطف، هوشیار و ایمن، سازمان‌ها می‌تواند نمودار سایبری خود را از طریق اجزای کنترل داخلی بررسی کنند. برای مثال:

- محیط کنترلی- آیا هیات مدیره نمودار ریسک سازمان را درک کرده است؟
- ارزیابی ریسک- آیا سازمان‌ها در عملیات خودارزیابی، بحران، گزارش‌ها، انطباق اهداف و جمع آوری اطلاعات، چگونگی تاثیر ریسک سایبری بر این اهداف را درک می‌کنند؟
- فعالیت‌های کنترلی- آیا فعالیت کنترل توسعه، شامل فعالیت‌های کنترل عمومی بر فناوری که سازمان را قادر به مدیریت ریسک در سطح تحمل قابل قبول نگاه می‌دارد، در سازمان وجود دارد؟
- اطلاعات و ارتباطات- آیا سازمان اطلاعات مورد نیاز و مدیریت کنترل داخلی بر ریسک سایبری را شناخته است؟
- نظارت بر فعالیت- چگونه سازمان، انجام ارزیابی برای تعیین طراحی و عامل اثر بخش

کنترل‌های داخلی که نشانه‌هایی از ریسک‌های سایبری هستند را انتخاب می‌کند؟

وقتی یک شرکت ریسک سایبری را از طریق چشم‌انداز کوزو مدیریت می کند، هیئت مدیره و مدیران ارشد را قادر به برقراری ارتباط بهتر با اهداف کسب‌وکار ، تعریف سیستم‌های اطلاعاتی بحرانی و سطح مرتبط با تحمل ریسک می‌کند. این عمل دیگران را در داخل سازمان (از جمله پرسنل فناوری اطلاعات) را قادر می‌سازد که برای انجام دقیق یک تجزیه و تحلیل ریسک سایبری به وسیله سیستم اطلاعاتی که به احتمال زیاد توسط حمله‌کنندگان مورد هجوم قرار می‌گیرند، و روش‌های احتمال حمله و نقاط استثمار را در نظر بگیرند (کوزو،۲۰۱۳).

در ادامه فرآیندهای از مدل چارچوب کنترل داخلی یکپارچه در عصر سایبری که در این پژوهش مورد ارزیابی قرار گرفتند، بیان شده است:



شکل۱، مدل چارچوب کنترل داخلی یکپارچه در عصر سایبری

ارزیابی ریسک سایبری بر اساس کوزو

هر سازمان برای منابع داخلی و خارجی خود بر روی انواع گوناگونی از ریسک سایبری تمرکز می‌کند. ریسک سایبری عبارت است از ارزیابی در مقابله با رویدادهایی که ممکن است در آینده اتفاق بیافتد و اثر معکوس بر اهداف سازمان در راه رسیدن به آن‌ها داشته باشد. بازیگران بداندیش، بویژه افرادی که فقط انگیزه مالی دارند،گرایش به یک مبنای هزینه/پاداش دارند. کسانی که حملات سایبری انجام می‌دهند و انگیزه‌های پشت حملات خود دارند، به طورکلی عبارت‌اند از، دولت‌های ملی و جاسوسان[۱۵]، جنایتکاران سازمان یافته[۱۶]، تروریست‌ها[۱۷]، هکتیویست‌ها[۱۸]، کارمندان داخلی[۱۹]. یک سازمان منابع محدودی دارد و تصمیماتش برای سرمایه‌گذاری در فعالیت‌های کنترلی باید بر اساس اطلاعات مربوط و با کیفیتی که یافته‌ها را با سیستم‌های اطلاعاتی که در شرکت مهمترین هستند اولویت‌بندی می‌کند. ارزیابی ریسک سایبری یک سازمان برای اولین بار باید به وسیله درک آنچه که سیستم‌ها یا اطلاعاتی که در سازمان ارزشمند

هســـتند، شروع شـــود. ارزش باید در برابر اثرات بالقوه به اهداف شرکت، اندازه‌گیری شود (مری، ۲۰۱۵).

ساختارهای شـــناختی- ادراکی ناســـازگارانه میتوانند در مجرمان سایبری وجود داشته باشند که حتی بیمارگونه نباشـــد اما بر ارتکاب جرم مؤثر باشـــد و منجر به رفتار مجرمانه شود یا آن را گســـترش دهد. مجرمان نوع خاصی از تفکر را دارند که به‌وسیله آن رویدادها و برداشت‌های خود را از محیط تفسیر کرده و به آنها معنی می‌دهند. لذا پس از بررسی ساختارهای شناختی- ادراکی مجرمان سایبری مشاهده گردید این ساختارها افکار، احساسات، ارزش‌ها، باورها، بینش مجرمان ســـایبری را در برمی‌گیرد که منجر به شـــکل گیری نوع خاصی از اختلالات روانی، سبک هویت، سبک‌های مقابله‌ای ناکارآمد، قضاوت اخلاقی، اعتقادات مذهبی و طرح‌های ناسازگار اولیه در افراد می‌شود که فرد را به ارتکاب جرم سوق می‌دهد (هادی خامنه و همکاران، ۱۴۰۰).

اصل ششـــم چارچـــوب ۲۰۱۳، در مورد چگونگـــی ارزیابی اهداف خود به شـــیوه‌ای که بتواند ارزیابی ریسک ســـایبری را تحت تاثیر قرار دهد، چشم انداز به سازمان‌ها ارائه می‌کند. این نقطه تمرکز تحت مقوله‌های زیرتعریف می‌شود: اهداف عملیات، اهداف گزارشگری مالی برون سازمانی، اهداف غیرمالی گزارشگری برون سازمانی، اهداف گزارشگری داخلی و برآوردن اهداف. بسیاری از سازمان‌ها وقت کافی صرف بدست آوردن درک اینکه چه سیستم‌های اطلاعاتی برای سازمان واقعا بحرانی اســـت را ندارند؛ همچنین آنها ممکن است درک مشکلی از این که اطلاعات کجا و چگونه ذخیره شـــوند را نداشته باشند و این می‌تواند منجربه کوشـــش‌هایی برای محافظت از هر چیزی شـــود، این امر منجر به محافظت بیش از حد از سیستم‌های اطلاعاتی معین و سایر سیستم‌های تحت محافظت می‌شود. برای این که سیستم‌های اطلاعاتی ارزش پیدا کند، مستلزم درجه بالایی از همکاری بین بنگاه‌ها و ســـهامداران فناوری اطاعات (ذینفعان) است. به دلیل این که سازمان‌ها قادر به پرداختن به همه ریســـک‌ها به دلیل محدودیت زمان بودجه و منابع در دسترس نیستند، مدیریت باید ســـطح قابل قبولی از ریســـک را بپذیرد و روی آن تمرکز کند. اصل هفتم چارچوب ۲۰۱۳، سازمان‌ها بایستی خطرات دستیابی به اهداف خود را در سراسر سازمان شناسایی و تجزیه وتحلیل این ریسک‌ها را مورد توجه قرار دهد. (کوزو،۲۰۱۳).

به عنوان خروجی اهدافی که در نتیجه به کار گیری اصل ششـــم شناســـایی شـــده است، یک ســـازمان باید درک روشنی از سیستم‌های اطلاعاتی که جهت دســـتیابی به اهداف حیاتی است، داشته باشد. ســـپس با به‌کارگیری اصل هفتم به طور عمیق‌تر به ارزیابی ریسک می‌پردازد و این امر منجر می‌شود که سازمان‌ها شدت و احتمال اثرات ریسک سایبری را ارزیابی کنند. برای اینکه فرآیند ارزیابی خطر موثر باشـــد، افرادی که درگیر هســـتند باید درک درستی از ریسک سایبری سازمان داشته باشند. این درک‌ها شـــامل اینکه چه سیستم‌هایی برای عاملان سایبری ارزشمند هستند و درک اینکه چگونه این حملات به احتمال زیاد رخ خواهند داد می‌باشد. گرانترین حملات مربوط به آنهایی اســـت که به دلایل خاص یک ســـازمان را مورد هدف قرار داده‌اند. مثلا صنعت نفت‌وگاز که ممکن اســـت توسط دولت‌های ملی با انگیزه ســـرقت اطلاعات استراتژیک در مورد

سایت‌های نفتی آینده مورد هدف قرار گیرند. شرکت‌های مواد شیمیای ممکن است خودشان را به سبب مسائل محیطی درک شده پیرامون محصول‌شان مورد هدف هکتیویست‌ها بیابند. علیرغم انگیزه‌های حمله‌کنندگان سایبری، آنها بی رحم، خبره، و شکیبا هستند. آنها حملات را در طول زمان با جمع آوری اطلاعات که نقاط ضعف در سیستم‌های اطلاعاتی سازمان‌ها و کنترل‌های داخلی است را در معرض حمله قرار می‌دهند. حمله‌کنندگان از طریق ارزیابی دقیق انگیزه‌ها و روش‌های حمله و به احتمال زیاد از تکنیک‌ها، ابزارها و فرآیندهای(TTPs)[۲۰] استفاده می‌کنند، یک سازمان می‌تواند برای پیش‌بینی بهتر این حملات یک موقعیت خوب از کنترل داخلی را طراحی کرده و این طراحی برای به حداقل رساندن احتمال حمله سایبری و حفظ دارایی ایمن و با ارزش موثر هستند (مری،۲۰۱۵).

اصل نهم چارچوب ۲۰۱۳، سازمان، تغییراتی که تاثیر قابل توجهی می‌توانند بر سیستم کنترل داخلی داشته باشند را شناسایی و ارزیابی می‌کند. تغییر خاصی که در هر سازمان وجود دارد باید در عملکرد ارزیابی ریسک سایبری پیش‌بینی شود. چشم‌انداز سایبری شامل عاملان جدید حملات سایبری، همراه با روش‌های جدید بهره‌برداری است. کسب‌وکار، فن‌آوری از سوی سازمان تلاش برای رشد، نوآوری و بهینه‌سازی هزینه را به تصویب می‌رساند. با این حال، خلاقیت و نوآوری نیز در معرض خطرات جدید ایجاد شده قرار می‌گیرد. برای مثال، تصویب و یا قبول کار با وب، تلفن همراه و فن‌آوری رسانه اجتماعی این فرصت را برای بهره‌برداری توسط عاملان سایبری افزایش می‌دهد. به طورمشابه، برون سپاری که خارج از کنترل سازمان است در معرض آسیب پذیری‌های بالقوه سایبری قرار می‌گیرند. ارزیابی ریسک سایبری باید به طور مستمر به‌روز شود تا تغییراتی که می‌تواند منجر به توسعه کنترل سایبری یک سازمان برای حفاظت مهمترین سیستم‌های اطلاعات شود، تحت تاثیر قرار گیرد (کوزو،۲۰۱۳)

شناخت و اجرای فعالیت‌های کنترلی ریسک سایبری

فعالیت‌های کنترل داخلی اقدامات انجام شده توسط افراد درون سازمانی برای کمک به حصول اطمینان از دستورات مدیریت به منظور کاهش ریسک برای رسیدن به اهداف را دنبال می‌کند. ازجمله فعالیت‌های کنترل مستندسازی سیاست‌ها و کمک به اطمینان از فعالیت‌های کنترلی که خارج از سازمان به طور مداوم انجام می شود می‌توان اشاره کرد. ساختارهای کنترلی باید در یک رویکرد طبقه لایه‌ای آرایش یابند تا بعد از اینکه لایه‌های آغازین دفاعی به خطر افتاده از پرسه‌زدن آزادانه مزاحمان به سیستم های اطلاعاتی ممانعت به عمل آورد. به دلیل این که ریسک سایبری از نقاط مختلف داخلی و خارجی وارد سازمان می‌شود، باید یک برنامه کنترل پیشگیرانه و کاراگاهانه برای کاهش خطرات ریسک سایبری انجام داد. کنترل پیشگرانه اگر به خوبی طراحی شود می‌تواند به وسیله نگه داشتن مزاحمان خارج از محیط فناوری اطلاعات داخلی و نگاه داری سیستم‌های امنیتی اطلاعاتی، حملات مزاحمان را متوقف کند. کنترل پیشگیرانه نیز ممکن است در محیط داخلی فناوری اطلاعات به عنوان موانع سرعت مزاحمان مستقر شود و عمل کند. حتی زمانی که سوء استفاده رخ می‌دهد، کنترل می‌تواند با یک تشخیص به موقع از نقض سازمان،

مدیریت را قادر می‌سازد که اقدامات اصلاحی و آسیب‌های احتمالی برای ارزیابی را در اسرع وقت انجام دهد. پس از آنکه اقدامات اصلاحی انجام شـــد، بســـیار مهم است که مدیریت ریشه علت به وجود آمدن این مشـــکل را به منظور بهبود کنترل برای جلوگیری از ســـوء استفاده و یا تشخیص مشـــابه که ممکن است در آینده رخ دهد را ارزیابی کند. یک چارچوب نظری حسابرسی فناوری اطلاعات داخلی، سیســـتم‌های اطلاعاتی اســـت که داده‌ها را توســـط منابع مختلف جمع‌آوری و توسعه می‌دهد. و فرایندهای نظیر حسابرسان فن‌آوری اطلاعات، مدیران سیستم-های اطلاعاتی و حسابرسان را شامل می‌شود(داگلاس هاوکا[۲۱]، ۲۰۱۳)، همچنین اهمیت حسابرسی پایگاه داده‌ها، امنیت داده‌ها و نیاز به توســـعه روش‌های جدید حسابرسی فنی با توسعه سریع فن‌آوری اطلاعات همراه می‌باشـــد (ایان روس[۲۲]، ۲۰۱۵). به طور کلی، در تحقیقات راجع به موضوع امنیت سایبری تنها به برخی از شـــاخص‌ها توجه می‌شود. بنابراین، برای گسترش سیاست‌های محافظت از بخش خصوصی و زیرســـاخت‌های حفاظت از جامعه عمومی، باید به دامنه گســـترده‌تری، گسترش یابد (کتابچی و همکاران ،۱۴۰۰).

کنترل سایبری پیشگیرانه و گارگاهانه (پلیسی)

کنترل کاراگاهانه تهدیدها را شناسایی و این شناسایی کاهش تهدیدها در سیستم‌های اطلاعاتی را در پی خواهد داشـــت. کنترل پیشـــگیرانه برای جلوگیری از خطـــر مرتبط با ضعف‌های آینده وجود دارد. علاوه برکنترل‌های پیشـــگیرانه وکاراگاهی، فعالیت‌های کنترل مســـتقر برای کاهش خطرات سایبری باید شامل ترکیبی از فن آوری اطلاعات عمومی (GITC)[۲۳] همراه با کنترل‌های دیگرکسب وکار باشد. GITCs کنترل‌های احتمالی هستند که برای جلوگیری و یا نقض سایبری زمانی که در ســـفارش ســـازمان به صورت ارتجاعـــی رخ می‌دهد، به کار مـــی‌رود. اصول و نقاط چارچوب ۲۰۱۳ به طور مســـتقیم روی ســـازمانی که به سمت فعالیت‌های کنترلی خوب طراحی شده‌اند تمرکز می‌کند. هر سازمانی توسط افراد مختلف با مهارت و تجربه‌های خاص که به سمت قضاوت‌های حرفه‌ای حرکت می‌کند، اعمال مدیریت را تحت تاثیر قرار می‌دهد. وقتی که طراحی ارزیابی ســـازمان، به طور مناســـب کنترل واجرایی شود، باعث کاهش ریسک سایبری در سازمان می‌شـــود، و این امر به مقایسه فعالیت‌های کنترلی با استانداردها و چارچوب که با مدیریت ریسک سایبری هم‌ترازند، کمک می‌کند. COBIT[۲۴]، ISO۲۷۰۰۰[۲۵] و NIST[۲۶] رفرنس و پیش‌زمینه‌ی بر استانداردها و چارچوب‌های سایبری‌محور هستند که می‌تواند ابزارکمک کننده برای سازمان‌ها در مسیر ارزیابی کارایی کنترل‌ها باشند (مری,۲۰۱۵).

تجارب الکترونیک فرصت‌های بســـیاری برای شـــرکت‌ها به ارمغان آورده است. اجرای تجارب الکترونیـــک ابزارها و شـــیوه‌هایی جدید در خصـــوص کاهش هزینه‌ها، روابـــط موثرتر، افزایش و بهبود کارایی واثر بخشـــی عملیات به ســـازمان‌ها ارائه نموده است. چنین روابطی شرکت‌ها را به یکپارچه سازسی شبکه‌ی جهانی قادر ساخته است. به هر حال به منظور حرکت همگام با تحولات الکترونیک در تجارت، حسابرس داخلی بایستی در راستای کسب آگاهی از فناوری‌های نوین گام بردارند. در این راستا کنترل‌های داخلی باید به گونه‌ای طراحی شود که دستیابی به اهداف تجارت

الکترونیک سازمان به گونه‌ای کنترل شده، تسهیل گردد(پریس[۲۷]، ۲۰۰۱).

تولید و ارائه اطلاعات مربوط و با کیفیت برای مدیریت ریسک‌های سایبری

اجزای اطلاعات و ارتباطات دارای سه اصل است که بر تلاش‌های سازمان تمرکزدارد، (۱) شناسایی اطلاعات مربوط و با کیفیت (۲) تعریف اینکه چگونه اطلاعات باید در داخل ارتباط برقرار کنند و (۳) تعریف این که چگونه سازمان باید با طرف‌های خارجی ارتباط برقرارکند. همه اجزای کنترل داخلی به هم دیگر وابسته و مرتبط اند، اطلاعات با کیفیت از طریق ترکیب اطلاعات‌وارتباطات حمایت می‌شوند.کنترل‌ها در مکان درون سازمان نیازهای اطلاعاتی سازمان را دیکته می‌کند. این اطلاعات می تواند در قالب گزارش، داده‌های مورد استفاده درتجزیه وتحلیل کنترل، یا نمودارکلی دریک سطح بالاتری از ساختار کسب‌وکار سازمان باشند. شناسایی اطلاعات مورد نیاز بحرانی با کنترل داخلی و تجزیه و تحلیل ریسک سایبری مرتبط با روند ارزیابی ریسک به هم آمیخته هستند. برای رسیدن به این نتیجه نهایی، کسب وکار و سایرگروه‌های ذینفع فناوری اطلاعات باید در ابتدا یک درک مشترک از بالاترین سطح از ساختار کسب‌وکار، از جمله ارائه دهندگان خدمات برون سپاری، و اهداف کسب‌وکار مرتبط و اهداف فرعی سازمان را داشته باشند (مری، ۲۰۱۵).

برقراری ارتباط اطلاعات کنترل داخلی

پرسنل، امنیت، مراقبت و انعطاف‌پذیربودن، یک مسئولیت‌پذیری سازمانی است که در آن هر فرد نقشی را در محافظت از سیستم‌های اطلاعاتی بازی می‌کند. در مورد خطرات سایبری و کنترل به منظور بالا بردن آگاهی پرسنل سازمان یک برنامه گسترش ارتباط سازمان باید توسعه و اجرا شود. چنین ارتباطی می‌تواند آنچه را که اغلب ضعیف‌ترین لینک کنترل داخلی (افراد) به سبب طبیعت انسان باشد را تقویت کند. در مورد انشعابات کنجکاوری انسان‌ها موارد ذیل را می‌توان اشاره کرد: افراد زمانی که ایمیلی را که تصور می‌شود از طرف همکار، مشتری، فروشنده، یا سایر شرکای تجاری مورد اعتماد فرستاده شده باشند، چکار می‌کنند؟ افراد اگر یک درایور USB[۲۸] که روی محدوده زمین افتاده باشند را ببینند چه واکنشی نشان می‌دهند؟ (مری، ۲۰۱۵).

ویژگی‌های رفتاری طبیعی انسان، مانند کنجکاوی بشر و اعتماد به دیگران یک نقطه ضعف شکستن ساختار کنترل داخلی یک سازمانو یک فرصت برای مهاجمان برای حمله‌کردن است. برقرای ارتباط در تمام سطوح سازمان، به طور منظم افزایش آگاهی از امنیت سایبری احتمال سو استفاده پرسنل را در مورد موفقیت خود در سازمان را کاهش می دهد. برنامه‌های ارتباطی ممکن است ترکیبی از استراتژی‌های مختلف تفویض برای به حداکثر رساندن آگاهی کارکنان از خطر سایبری و مسئولیت پذیری باشد (مری، ۲۰۱۵).

مسئولیت مدیریت و نظارت بر ریسک سایبری و کنترل‌ها

همانطور که در جزء فعالیت های کنترلی قبلا اشاره شد، مدیریت برای حفاظت از سیستم‌های اطلاعاتی باید استقرار سیستم‌های کنترل داخلی را طراحی و توسعه دهد. اطلاعات کنترل داخلی برای کمک به مدیریت و پرسنل سازمان در انجام مسئولیت‌های کنترل سایبری در

سراسر سازمان از طریق کانال‌های داخلی باید به اشتراک گذاشته شود. به خاطر پیچیده‌گی‌های چشـــم‌انداز سایبری که درون کالبد سازمان یافته شده اســـت، بسیار مهم است که مستندسازی رسمی در ارتباط با کنترل‌های سایبری را نگاه داریم. بدون اسناد رسمی برای حمایت از انتظارات کنترل داخلی، توانایی سازمان برای مدیریت ریسک سایبری به طور چشم گیری کاهش می یابد (مری، ۲۰۱۵).

هیئت مدیره، امروزه بیش از هر زمان دیگری نیاز به نشان دادن درک خود از روند سایبری دارد که می‌تواند در توانایی ســـازمان در رسیدن به اهدافش، تاثیرگذارباشد. هیئت مدیره نقش بنیادی در امنیت، مراقبت و انعطافپذیری در مورد درک ریسک سایبری دارد، هیات مدیره نقش بنیادی در ایمن، مراقبت و منعطف بودن از طریق درک ریســـک‌های ســـایبری انجام می‌دهد و همینطور کنترل‌های کشـــف‌کننده و پیش‌گیرانه‌ای که در آن چنین ریسک‌هایی در سطح مطلوبی از دامنه تحمل ریســـک هســـتند را تایید می‌کند و انتظاراتی که رویه‌ها و فرآیندهای پاسخ‌گویی مناسب توســـط مدیریت محقق شده‌اند را تعریف می‌کند. (مری ، ۲۰۱۵). همچنین توانایی و پاسخگویی مدیریت در کاهش ریســـک تداوم فعالیت شـــرکت‌ها از طریق بکارگیری مفهوم اشتهای ریسک، از اهمیت بســـیار بالایی برخوردار اســـت. مدیران توانا با طراحی مناســـب سطح اشتهای ریسک و بکارگیری اســـناد اشتهای ریسک در فعالیت‌های شـــرکت، میزان قابل توجهی از ریسک تداوم فعالیت شرکت را کاهش می‌دهند (یاری و همکارن، ۱۴۰۰).

فعالیت‌های نظارتی و مدیریت ریسک سایبری

برای اینکه سازمان مدیریت ریسک سایبری درستی داشته باشد، محیط کنترلی و فعالیت‌های نظارتـــی اجزای کنترل داخلی، اصول بنیادی هســـتند. همان طوری که در چارچوب ۲۰۱۳ بیان شـــده اســـت، محیط کنترلی مجموعه‌ای از استانداردها فرآیندها و ســـاختارهایی است که پایه و اســـاس انجام کنترل‌های داخلی در سراسر سازمان را ارائه می کند. هیئت‌مدیره و مدیریت ارشد سیستم‌هایی را در خصوص اهمیت کنترل داخلی و استانداردهای مورد نظر رفتاری برقرار می‌کنند. مدیریت و هیئت‌مدیره قدرت و اختیار مجموعه‌ای از مســـئولیت‌های شرکت را دارا می‌باشند. اگر امنیت، مراقبت و منعطف بودن، به عنوان یک اولویت در درون سازمان تعریف و ابلاغ نشود، امید خیلی کمی وجود دارد که سازمان بتواند منابع کافی برای استقرار و حافظت از سیستم اطلاعاتی برای پاسخ به رویدادهای سایبری مناسب را داشته باشد (مری، ۲۰۱۵).

پیچیدگی‌های ریســـک سایبری می‌تواند یک چالش نگران کننده برای مدیریت و هیئت مدیره باشد. برای به انجام رساندن مســـئولیت‌ها، موضوع خطرسایبری تکنولوژی اطلاعات باید در برابر اهداف سازمان و اولویت‌های کســـب‌وکار تفسیرشود. درحالی که برخی از سازمان‌ها ممکن است متخصصان داخلی داشـــته باشند که فرآیندها و اهداف یک ســـازمان را تفسیر و تحت تاثیر قرار دهند، بســـیاری از ســـازمان‌های دیگر هم وجـــود دارد، که به کمک کارشناســـان خارجی واجد شـــرایط برای کمک تصمیم گیری استراتژی حرکت آن‌ها برای تبدیل شدن به امنیت، مراقبت و انعطاف‌پذیر بودن نیاز دارند. کمک از متخصصان واجد شـــرایط ریسک سایبری حیاتی است تا به

طور موثری گسترش منابع علیه ریسک‌های سایبری را اولویت‌بندی کند . مدیریت و هیئت مدیره باید از ارزش اطلاعات سیستم که با اهداف واحد تجاری هم تراز هستند آگاه و مطلع باشند. با این اطلاعات آن‌ها می‌توانند سطح خود از تحمل ریسک، تعریف و کمک به اطمینان از حاصل شدن مبالغ سرمایه گذاری و محافظت از اطلاعات برای دستیابی به اهداف مهم سازمان را بدانند. (مری، ۲۰۱۵).

تکامل ریسک سایبری

تکامل ریسک سایبری عموماً انباشته است، یعنی محرک‌ها و فرصت‌ها در یک دوره جایگزین فرصت‌های دوران قبل نمی‌شوند، بلکه افق را گسترش می‌دهند. (گوردون آرچیبالد[۲۹]، ۲۰۲۲).

سال‌های ۲۰۰۵ -۲۰۱۲، دوران انطباق: در پی انقلاب اینترنت، سازمان‌ها بر روی استانداردهای جدید برای امنیت اطلاعات تمرکز کردند. بحران مالی همچنین تمرکز بر رعایت مقررات در حوزه ریسک اطلاعات و فناوری را تشدید کرد.

سال‌های بین ۲۰۱۳ -۲۰۲۱، دوران ریسک: حملات سایبری با مشخصات بالا در صنایع مختلف توجه رسانه‌ها، مردم، هیئت‌های مدیره و مدیریت اجرایی را برانگیخت و بسیاری از سازمان‌ها را ترغیب کرد که فراتر از انطباق، ریسک‌های تجاری اساسی سایبری را بررسی کنند.

سال‌های ۲۰۲۲ و پس از آن، دوران بلوغ و فراگیری: بلوغ رو به رشد در سراسر قابلیت‌ها و راه‌حل‌های ۱۵ سال گذشته، بسیاری از سازمان‌ها را به دنبال کارایی هزینه بهتر سوق می‌دهد. در عین حال، اتصال فراگیر محصولات و زیرساخت‌ها تمرکز بر مدیریت ریسک در اینترنت را تشدید می‌کند (گوردون آرچیبالد، ۲۰۲۲).

ملاحظات کلیدی امنیت سایبری برای سال۲۰۲۲

۱-گسترش مکالمه امنیتی استراتژیک؛ مکالمه را از هزینه و سرعت به امنیت موثر تغییر دهید تا به ارائه ارزش تجاری و تجربه کاربری افزایش یافته، کمک کند.

۲- دستیابی به فاکتور استعدادها و مهارت‌های حیاتی؛ تغییر وضعیت فعلی رئیس امنیت اطلاعات، کارکنان و تیم‌های آنها از مجریان امنیت سایبری گرفته تا کسانی که به نوعی تاثیرگزار هستند.

۳- تطبیق امنیت برای توده‌های ابری؛ افزایش امنیت ابر از طریق اتوماسیون - از استقرار و نظارت تا اصلاح.

۴- قرار دادن هویت در قلب اعتماد صفر؛ مدیریت هویت و دسترسی و اعتماد صفر را در محل کار بیش از حد متصل امروزی قرار دهد.

۵- بهره‌برداری از اتوماسیون امنیتی؛ از استقرار هوشمند اتوماسیون امنیتی برای کمک به درک ارزش تجاری استفاده کنید.

۶- حفاظت از مرزهای حریم خصوصی؛ به سمت یک رویکرد چند رشته‌ای برای مدیریت ریسک حریم خصوصی حرکت کنید که حریم خصوصی و امنیت را با طراحی تعبیه کند.

۷- امنیت فراتر از مرزها؛ تغییر رویکردهای امنیتی زنجیره تامین - از دستی و زمان بر به خودکار و مشارکتی.

۸- قالب بندی مجدد گفتگوی تاب‌آوری سایبری؛ گسترش توانایی حفظ عملیات، بهبود سریع و کاهش عواقب هنگام وقوع یک حمله سایبری. (اندرو موریسون[۳۰]، ۲۰۲۲).

تکنیک‌های پیشگیری از خطر تهدیدات سایبری

یک ضرب المثلی وجود دارد که اشـــاره می‌کند «یک اونس پیشـــگیری ارزش یک پوند درمان را دارد» به ویژه در برخورد با تهدیدات ســـایبری صادق اســـت. برای مثال، اگر تراکنش مالی یک شـــرکت از طریق اینترنت ربوده شود و وجوه یا اطلاعات به سرقت رفته باشد، ممکن است مدتی طول بکشد اطلاعات بازیافت شود، بعلاوه این احتمال وجود دارد که عواید آن هرگز بازیابی نشود و سارقان نیز دستگیر نشوند. خیلی بهتر است در وهله اول از سرقت یا جرایم سایبری جلوگیری شـــود (کلارک[۳۱]، ۲۰۰۸). نرم افزارهای امنیتی شامل، ضد جاسوس، شناسایی ابزارهای تبلیغاتی مزاحم، بدافزارها و محافظت آنتی ویروس که از یک فروشـــنده معتبر تهیه شده است. یک ویژگی به‌روزرسانی خودکار همراه با اسکن روتین خودکار سیستم نیز ضروری است و وصله‌های نرم‌افزاری باید در صورت وجود نصب شود. همچنین مشاوره گرفتن از مشاوران - بیمه‌گران ریسک سایبری، وکلا، حسابداران و مدیران ریسک، تمرین تجاری خوبی است. (مجله بیمه، ۲۰۱۱).

تکنیک‌های کاهش ریسک سایبری

در حالیکـــه نمی‌توان از همه خطرات جلوگیری کـــرد، اما اثرات مخرب آن را می توان با برنامه ریزی عاقلانه کاهش داد. به طور معمول، شـــرکت‌هایی که به دنبال مقابله با ریسک سایبری خود هستند، از چارچوب‌های مدیریت ریســـک و تکنیک‌هایی استفاده می‌کنند که آسیب‌پذیری‌های امنیت اطلاعات را شناسایی می‌کند. اولین گام، ممیزی امنیتی است که توسط شرکت (یا شخص ثالث) انجام می‌شود که خطرات و آسیب‌پذیری‌ها را در سیستم‌های شرکت شناسایی می‌کند. این مرحله معمولاً شامل بازرسی محیط محاسبات فیزیکی برای تهدیدات ریسک خارجی و همچنین بررسی شـــبکه‌های الکترونیکی (از جمله دسترسی خارج از ســـایت توسط کارکنان و مشتریان) اســـت. علاوه بر این، شـــرکت‌ها با مصاحبه با مدیران فناوری اطلاعات و تعیین هزینه‌های مالی فرآیند مدیریت ریسک، اطلاعاتی را در مورد مشخصات ریسک فعلی جمع‌آوری می‌کنند. (سیگل و همکاران، ۲۰۰۲).

یک تکنیک کاهش خطر، بســـیار مهم برای پیاده سازی شرکت‌ها، استفاده از رمزگذاری داده‌ها است، که اساساً هر سند را به گونه‌ای کدگذاری می‌کند که حتی در صورت سرقت یا ربوده شدن در انتقـــال تلفن همراه، قابل خواندن نباشـــد. رمزگذاری انتقال و/یا اســـناد، هک مؤثر پایگاه‌های داده یا دســـتگاه‌های تلفن همراه را برای اشـــخاص ثالث تقریباً غیرممکن می‌کند. راه‌های زیادی برای اســـتفاده از رمزگذاری وجود دارد. فایل‌های منفرد را می‌توان رمزگذاری کرد یا کل آرشیوها را می‌توان رمزگذاری کـــرد. انواع مختلفی از رمزگذاری وجود دارد. این دو انواع اصلی رمزگذاری رمزنـــگاری کلید خصوصی و رمزنگاری کلید عمومی اســـت. رمزگذاری کلید خصوصی دارای یک کلید واحد اســـت که برای رمزگذاری و رمزگشایی استفاده می شـــود. با توجه به «الگوریتم‌های کلید خصوصی به طور کلی بسیار سریع و به راحتی در سخت افزار پیاده سازی می‌شوند، بنابراین

آنها معمولا برای رمزگذاری داده‌های انبوه اســـتفاده می شوند.» رمزگذاری کلید خصوصی عمدتاً برای رمزگذاری فایل، دایرکتوری و پارتیشـــن اســـتفاده می‌شـــود که فقط توسط صاحب داده‌ها شـــناخته شده است. دو دسته کلی از الگوریتم‌های کلید خصوصی وجود دارد: رمزهای جریانی و رمزهـــای بلوکی. یک رمز جریان بـــه صورت جداگانه هر بایت داده را رمزگذاری می‌کند و معمولاً برای ارتباطات بی‌ســـیم استفاده می‌شود. از طرف دیگر، رمزهای بلوکی یک بلوک از داده‌ها را در یک زمان رمزگذاری می‌کنند و عمدتاً برای رمزگذاری داده‌ها اســـتفاده می‌شوند. رمزنگاری کلید عمومی شامل استفاده از دو کلید متمایز اما مرتبط است: یک کلید عمومی و یک کلید خصوصی. کلید عمومی را می‌توان با هر کســـی به اشتراک گذاشت و برای رمزگذاری داده‌های دارنده کلید خصوصی اســـتفاده می‌شود. کلید خصوصی را نمی‌توان به اشتراک گذاشت و برای رمزگشایی هر داده‌ای که توسط کلید عمومی رمزگذاری شده است استفاده می‌شود. رمزنگاری کلید عمومی در درجه اول برای پیام‌های ایمیل، پیوســـت‌های فایل، امضای دیجیتال و سایر فرآیندهای مربوط به تراکنش استفاده می‌شود. نظارت و شناسایی نیز گامی حیاتی در جلوگیری از خطر سایبری است (اُلحُرست[۳۲]، ۲۰۱۰) .

چشم‌انداز و آینده ریسک سایبری

مقررات و کنترل‌ها در فناوری سایبری با سرعت بسیار کمتری نسبت به رشد و پیشرفت واقعی در خود فناوری توســـعه یافته‌اند و در نتیجه باعث ایجاد تاخیر در اجرا و عدالت شده‌اند. بسیاری از تهدیدات خطر ســـایبری از کشورهایی متفاوت از کشـــور میزبان سرچشمه می‌گیرند و تنظیم یا اجرای قوانین علیه چنین مجرمان فرامرزی می‌تواند دشـــوار یا حتی غیرممکن باشـــد. دولت‌ها و نهادهـــای نظارتی بین المللی، مانند ســـازمان ملل متحد، اکنون در تلاش هســـتند تا مقررات سخت‌گیرانه‌تری. به منظور جلوگیری از این نوع فعالیت‌های غیرقانونی خطر سایبری متقابل ملی ایجاد کنند. با این حال، تا زمانی که توافق گسترده‌ای در مورد اجرا و مجازات وجود نداشته باشد، شـــرکت‌ها مجبور خواهند بود به تنهایی با این خطرات مقابله کنند. هر مدیر ریسکی که به آینده نـــگاه می کند بایـــد بتواند برای این تهدیدات منحصر به فرد و پیچیدگـــی روزافزون آن‌ها برنامه ریزی کنید. از آنجایی که اینترنت امکان دسترســـی بالقوه را از هرجایی فراهم می‌کند، شرکت‌ها و شـــرکت‌های دولتی باید برای مقابله با تهدیدات خطر ســـایبری داخلی و خارجی آماده باشند (اُلحُرست، ۲۰۱۰) .

حسابرسی ریسک‌های سایبری

حسابرسان داخلی باید اطمینان حاصل کنند که دانش مناسبی در مورد ریسک سایبری دارند.

یکی از مؤلفه‌های حیاتی حاکمیت ریسک، کسب اطمینان از طریق حسابرسی داخلی است که فرآیندهای مدیریت ریســـک موجود به درستی کار می‌کنند و منابع به طور مؤثر به کار می‌روند. همانطور که محیط سایبری تکامل می‌یابد، مدیریت ریسک و حسابرسی داخلی باید سرعت خود را حفظ کنند. ریســـک‌های سایبری، در معنای وسیع آن‌ها، باید پس از ارزیابی مبتنی بر ریسک، در برنامه‌ریزی و اجرای حسابرسی داخلی منعکس شوند. حسابرسان داخلی باید اطمینان حاصل

کنند که دانش مناسبی در مورد ریسک سایبری دارند و حسابرسی داخلی و مدیریت ریسک و مدیریت عملیاتی باید برای به اشتراک گذاشتن اطلاعات و اعتبارسنجی پاسخ‌های کنترلی با یکدیگر همکاری نزدیک داشته باشند. (دیوید کانهام[۳۳]، ۲۰۱۴) و همچنین در خصوص نبود دانش و تجربه کافی در زمینه حسابرسی فناوری اطلاعات می‌توان گفت که بهبود دانش حسابرسان در خصوص فناوری اطلاعات به عنوان یک عامل مهم در خصوص اجرای این نوع حسابرسی محسوب می‌شود (پرندین، ۱۴۰۲). در ادامه به برخی از ملاحظات کلیدی برای حسابرسی داخلی در حوزه مدیریت ریسک سایبری خواهیم پرداخت.

اصول حسابرسی داخلی

مؤسسه جهانی حسابرسان داخلی[۳۴] (IIA) حسابرسی داخلی را اینگونه تعریف می‌کند: «... یک فعالیت تضمینی و مشاوره مستقل و عینی که برای افزودن ارزش و بهبود عملیات سازمان طراحی شده است. این به سازمان کمک می‌کند تا با ارائه یک رویکرد منظم، برای ارزیابی و بهبود اثربخشی فرآیندهای مدیریت ریسک، کنترل و حاکمیت، به اهداف خود دست یابد. (دیوید کانهام، ۲۰۱۴). و همچنین ضمن مشارکت حسابرسان داخلی با مدیریت ریسک درفرآیند ارزیابی ریسک، تنظیم برنامه‌ی حسابرسی داخلی با نگرش مبتنی بر ریسک برای شناسایی اولویت‌های فعالیت حسابرسان داخلی، زمینهی اثربخشی مؤثرتر حسابرسی داخلی فراهم می‌نماید (برخوردار، ۱۴۰۰). عملکرد حسابرسی داخلی به تیم‌های مدیریتی، مدیران غیر اجرایی وکمیته‌های حسابرسی در مورد سلامت محیط کنترل اطمینان می‌دهد، در مواردی که مسائل کشف می‌شوند گزارش می‌دهند و مکان‌هایی را که اقدامات اضافی مورد نیاز است شناسایی می‌کند. مدل سه خط حسابرسی دفاعی (تأیید شده در بریتانیا) توسط IIA و موسسه مدیران) چارچوب ساده‌ای را برای درک سطوح مختلف کنترل و اطمینان ارائه می‌کند: این مدل، از نشریه IIA «آنچه هر مدیر باید درباره حسابرسی داخلی بداند» گرفته شده است، به صورت نموداری در شکل ذیل نشان داده شده است (دیوید کانهام، ۲۰۱۴).

شکل ۲، مدل سه خط حسابرسی دفاعی

خـــط ۱ - کنترل‌های مدیریت عملیاتی که به‌عنوان بخشـــی از مدیریت کســـب‌وکار به‌صورت مدیریت خط روزانه به کار گرفته می‌شوند. به عنوان مثال، در زمینه ریسک سایبری ممکن است تیمی از آزمایش‌کنندگان کنترل در بخش مدیر ارشـــد اطلاعات وجود داشـــته باشد که تضمین می‌دهد، هم به حاکمیت عملیاتی و هم در برنامه حسابرسی سازمان کمک می‌کند.

خط ۲ - نظارت و تسهیل مدیریت عملیاتی توسط تیم مدیریت ریسک یا سایرین مانند اتحادیه انطباق. خط ۲ مشاوره، آموزش، چالش و نظارت بر فعالیت‌های خط اول را ارائه می‌دهد. به عنوان بخشـــی از این نقش خـــط دوم، تیم‌های اطمینان با خط اول برای ارزیابی نقاط ضعف و آســـیب پذیری در محیط کنترل و انطباق با چارچوب‌های قانونی و نظارتی، با اســـتفاده از محیط نظارتی سازمان و ثبت ریسک ذاتی برای هدایت فعالیت‌ها کار می‌کنند.

خط ۳ - عملکرد حسابرســـی داخلی، با انجام بررســـی‌های مســـتقل بر اساس ریسک، از نحوه عملکرد خط اول و دوم دفاعی اطمینان می‌دهد.

در ادامه رویکرد ســـنتی حسابرسی را بررسی می‌کند و نشان می‌دهد که چگونه در یک محیط «سایبری» نقش حسابرس داخلی ممکن است متفاوت باشد.

رویکرد حسابرسی سنتی

تعدادی از تغییرات در رویکرد حسابرســـی داخلی وجود دارد به شش مرحله به شرح ذیل بیان می‌شود

مرحل اول - برنامه‌ریزی سطح بالا؛ در تنظیم برنامه حسابرسی باید از تعدادی از منابع استفاده شود تا از جامع ترین طرح ممکن اطمینان حاصل شود. این منابع شامل موارد ذیل می‌باشد؛ (لازم به ذکر است، در برخی موارد ممکن است فقط محدود به موارد ذیل نباشد)

۱- پروفایل ریســـک ذاتی ۲- محدوده ریســـک فعلی شـــرکت۳- اســـتانداردهای سازمانی ۳- حسابرسی‌های قبلی ۴- منابع خارجی، ۴- ملاحظات قانونی ۵- راهنمایی‌های کمیته حسابرسی و مدیریت سازمان و ۶- برنامه‌های تضمین خط یک و دو

در ســـازمان مدرن، شـــبکه‌ای از طرف‌های داخلی و خارجی وجود خواهد داشت که بر برنامه حسابرســـی تأثیر می‌گذارد. برای مثال ممکن اســـت شـــرایط قرارداد خاصی مورد نیاز باشـــد تا به ســـازمان اجازه دهد فرآیندهای مربوط به تامین‌کنندگان و برون ســـپاری‌ها را بررســـی کند، تیم‌های حسابرسی داخلی که به‌طور ســـنتی حول یک برنامه سالانه استوار است، اکنون رویکرد انعطاف‌پذیرتری را بر اساس برنامه‌های متحرک بر اساس «سه به علاوه نه» یا «شش بعلاوه شش» اتخاذ می‌کنند.[۳۵] (دیوید کانهام، ۲۰۱۴).

مرحلـــه دوم - برنامه‌ریزی وظایف: هنگامی که طرح ایجاد شـــد، می‌توان وظایف حسابرســـی جداگانه را انجام داد. شرایط مرجع باید در ارتباط با مدیریت خط مقدم تهیه شود و دامنه فعالیت حسابرســـی داخلی را مشـــخص کند از جمله ذینفعان کلیدی که باید درگیر شوند، تخمین زمان مورد نیاز و ارزیابی خطرات را باید در نظر داشت.

مرحله ســـوم - تجزیه و تحلیل کسب‌وکار: با شروع بررسی و ورود حسابرسان داخلی به محل،

اولین فعالیت انجام شده تجزیه و تحلیل تجاری است. این فرآیند برای ایجاد یک دیدگاه مشترک از محیط فرآیندی که باید بررسی شود، مهم است. این می‌تواند به شکل بازنگری دستورالعمل‌های فرآیند، ایجاد نمودارهای جریان فرآیند و/یا روایتی باشـــد که نحوه عملکرد و بررسی فرآیندهای مشمول حسابرسی را توصیف می‌کند. علاوه بر این، یک ثبت کنترلی از نقاط کنترل‌های کلیدی باید ایجاد شـــود، اولاً به عنوان بخشـــی از فرآیند شناســـایی و ثانیاً برای امـــکان آزمایش مؤثر و همسویی با خطرات در حال بررسی.

مرحله چهارم - تجزیه و تحلیل ریسک و کنترل: مرحله چهارم فرآیند موقعیت، تجزیه و تحلیل ثبت ریسک سازمانی است. این امر کنترل‌های شناسایی شده در مرحله تجزیه و تحلیل کسب‌وکار را به ثبت ریسک مرتبط می‌کند و همچنین مناطقی را که شکاف‌هایی در ثبت ریسک وجود دارد شناســـایی می‌کند. حســـابرس داخلی معمولاً یک ماتریس ریسک و کنترل از این اطلاعات ایجاد می‌کند که به بررســـی کمک می‌کند و به فرمول‌بنـــدی یافته‌هایی کمک می‌کند که این اقدام با پیشرفت بررسی ثبت می‌شوند و نهایتا به اطلاع‌رسانی گزارش نهایی کمک می‌کنند.

مرحله پنجم - اثربخشـــی آزمون: هنگامی که ماتریس ریسک و کنترل درست شد و فرآیندها ترســـیم و درک شـــدند، بررسی می‌تواند با اســـتفاده از ترکیبی از مصاحبه‌ها، بررسی‌های فنی از طریق اشـــخاص ثالث انجام شود. یافته‌های این فرآیند و مسائل شناسایی شده در نهایت منجر به گزارش حسابرسی نهایی می‌شود.

مرحله ششـــم - گزارش و اظهار نظر: مرحله نهایی تهیه گزارش حسابرســـی اســـت. یافته‌ها بر اســـاس یک سلسله مراتب اهمیت ریسک سازمانی درجه‌بندی می‌شوند. معمولاً این انتظار وجود دارد که این رتبه‌بندی توسط مدیریت اصلاح شود. رتبه بالاتر معمولاً نیاز به یک طرح حل سریعتر را به ســـازمان دیکته می‌کند. گزارش جمع‌آوری شـــده از همه حسابرسی‌ها در یک حوزه کنترلی خاص، یک «نظر حسابرســـی» را تشـــکیل می‌دهد که به طور دوره‌ای بـــه هیئت مدیره، کمیته حسابرسی و در صورت لزوم به اشخاص ذینفع خارجی گزارش می‌شود.

پیـــروی از یک الگوی تعیین شـــده بـــرای اطمینان از کیفیت و یکپارچگی برنامه حسابرســـی سازمانی منطقی اســـت، اما فرآیند سنتی زمان می برد و در کنار محیط کنترلی سازمان مربوطه تنظیم می‌شـــود. با یک محیط سایبری سریع، یک رویکرد ســـنتی ممکن است برای کنترل‌های امنیت داده‌ها کافی باشـــد، اما برای تهدیدات ســـایبری در حال تحول ممکن اســـت به شیوه‌ای متفاوت از تفکر نیاز باشد. (دیوید کانهام، ۲۰۱۴).

به‌کارگیری رویکرد حسابرسی در محیط سایبری

در هنگام اعمال رویکرد حسابرســـی در محیط سایبری، ملاحظاتی وجود دارد که شامل موارد ذیل است ولی محدود به رویکرد سنتی نمی‌باشد؛

۱- برنامه‌ریزی سطح بالا

محدوده مرحله برنامه ریزی برنامه حسابرســـی باید چشـــم‌انداز تهدید سایبری گسترده را در نظر بگیرد. به طور سنتی برنامه‌های حسابرسی حول نقشه فرآیند سازمانی و ثبت ریسک ساخته

شده‌اند، اما در یک محیط «سایبری» باید عوامل خارجی بیشتری در نظر گرفته شوند، برای مثال:

• شبکه‌ای از تامین کنندگان، اشخاص ثالث و مشاوران در سراسر سازمان وجود خواهد داشت. روش‌های مختلفی برای اطمینان از انطباق و کنترل از طریق استانداردهای معتبر وجود دارد، اما حسابرس داخلی باید تصمیم بگیرد که آیا این میزان اطمینانی را که سازمان مادر برای برآورده کردن تحمل ریسک خود به آن نیاز دارد، برآورده می‌کند یا خیر.

• سازمان‌ها باید مکانیسم‌های نظارتی کافی برای هشدار فعالانه در مورد نفوذ سایبری داشته باشند. کنترل‌های سنتی پیرامون امنیت مانند خط‌مشی‌ها، رویه‌ها، فایروال‌ها و غیره تحت بررسی حسابرسی داخلی هستند، اما به طور فزاینده‌ای، حسابرس داخلی باید نیاز گسترده‌تری را برای نظارت و اسکن فعال‌تر و در سطح سازمانی در نظر بگیرد. به عنوان مثال آیا سازمان دارای یک مرکز عملیات امنیتی است؟

• هوش خارجی در برنامه ریزی و ارزیابی خطرات درون یک سازمان اهمیت فزاینده ای دارد. با عدم تمایل به گزارش و به اشتراک گذاری اطلاعات در مورد تخلفات در بخش خصوصی به ویژه، بررسی اطلاعات در دسترس عموم در برنامه‌ریزی، استفاده از پیوندهای غیررسمی بین شرکت‌ها و بررسی پایگاه‌های اطلاعاتی صنعت مانند ORIC (در بخش بیمه) می تواند به توسعه جامع برنامه حسابرسی سازمانی کمک کند. (دیوید کانهام، ۲۰۱۴).

۲- کنترل و اصلاح

از دیدگاه حسابرسی، چشم انداز تهدید گسترده است، از داخلی به خارجی، مالی به حق امتیاز، جنایی تا مخرب. اساساً هنگام ایجاد بررسی طرح‌ها و ماتریس ریسک و کنترل، حسابرس داخلی باید نه تنها کنترل‌های موجود، بلکه ترکیبی از کنترل‌ها را در نظر بگیرد. در سطح بالا، حسابرس داخلی باید انواع کنترل‌های زیر را در نظر بگیرد: پیشگیرانه، کارگاه و اصلاح (دیوید کانهام، ۲۰۱۴).

۳- قدم یا گام حسابرس

با یک چشم‌انداز تهدید سریع که محیط «سایبری» را احاطه کرده است، رویکرد سنتی حسابرسی باید مورد سؤال قرار گیرد و همچنین در نظر گرفتن اینکه حسابرسی داخلی چه نقشی در بررسی یک حادثه ایفا می‌کند نیز وجود دارد. سازمان‌ها فرآیندهایی را برای مقابله با عواقب فوری یک «رویداد سایبری» ایجاد کرده‌اند، اما بررسی و کنترل‌ها در مورد ضعف‌های منتهی به رویداد و تأثیرات آن می‌تواند از نظارت مستقل توسط حسابرس داخلی بهره‌مند شود (دیوید کانهام، ۲۰۱۴).

۳- بحث و نتیجه‌گیری

هدف این پژوهش، بررسی چگونگی کمک چارچوب کنترل داخلی یکپارچه (۲۰۱۳) به مدیریت ریسک و کنترل‌های سایبری است و همچنین نقش حسابرسی داخلی در کنترل مدیریت ریسک سیابری، برای سازمان‌ها را نشان می‌دهد. مدیریت ریسک در حوزه امنیت یک مفهومی کلیدی است که هدف اصلی آن استفاده از مکانیزم‌های مختلف امنیتی برای حافظت بیشتر از

دارایی‌های حیاتی سازمان می‌باشد، مدیریت ریسک در امنیت سایبری علاوه بر استفاده ازابزارهای امنیت فیزیکی مانند درب‌ها، قفل‌های امنیتی و گاوصندوق‌ها، شامل کلیه اقدامات مربوط به استفاده از راهکارهای ترکیبی، شامل استراتژی‌ها، تکنولوژی‌های امنیتی وحتی آموزش کاربران برای حفاظت از اطلاعات سازمان در برابر حملات نیز می‌شود. در حال حاضر هر نوع حمله‌ای می‌تواند سیستم‌های اطلاعاتی سازمان را به خطر بیاندازد و باعث به سرقت رفتن اطلاعات ارزشمند سازمان و آسیب به شهرت سازمانی شود. با توجه به افزایش میزان حملات سایبری نیاز به استفاده از راهکارهای مدیریت ریسک در حوزه سایبری افزایش چشمگیری داشته است. در پی‌توجه به ریسک سایبری از طریق لنز COSO، بسیاری از سازمان‌ها می‌توانند درتغییراتی که کنترل‌ها را بهبود می‌بخشد، تجدید نظر کنند. اگر امنیت، مراقبت و انعطاف‌پذیر بودن برای سازمان‌هادر اولویت نباشد، در نهایت در اولویت قرار خواهد گرفت. اگر ریسک سایبری توسط مدیریت منعکس نشده باشد، آسیب از یک حمله سایبری به طور بالقوه می‌تواند آنقدر شدید باشد که عملیات سازمان را منقطع ویا حیات سازمان را به خطر بیندازد. ریسک سایبری ادامه خواهد داشت تا کار مدیریت زمان و توسعه فناوری دشوارتر شود و هکرها پیچیده‌تر شوند. با این حال با توجه به مدل چارچوب کنترل داخلی یکپارچه در عصر سایبری شرکت‌ها باید در این زمینه سرمایه‌گذاری، مدیریت ریسک سایبری را در اولویت و اهداف استراتژیک سازمان را مورد توجه قراردهند. هر سازمان بسته به جایگاه‌ای که در آن قرار دارد کنترل ریسک سایبری را مورد توجه و در برنامه‌های آتی قرار می‌دهد. راهنمای چارچوب ۲۰۱۳ در جهت تلاش‌ها و قدم‌های که یک سازمان برای طراحی، ارزیابی و نگه‌داری یک محیط ایمن ، هوشیار و منعطف بر می‌دارد، می‌تواند مورد استفاده قرار گیرد.

و همچنین با توجه به دوره تکامل ریسک سایبری و دوره حاضر، ملاحظات کلیدی امنیت سایبری برای سال۲۰۲۲ که در این پژوهش معرفی شدن باید مورد توجه سازمان های مختلف قرارد گیرد. لازم به ذکر است همانطور که محیط «سایبری» تکامل می‌یابد، نیاز به مدیریت ریسک و حسابرسی داخلی برای همگام شدن با آن افزایش می یابد.

به طور خلاصه و با توجه به اهمیت موضوع امنیت سایبری انجام اقدامات به شرح ذیل به مدیریت ریسک سایبری و اسیب پذیری کمتر سازمان کمک می‌کند: ایجاد فرهنگی برمبنای امنیت، ارزیابی مستمر تمامی تکنولوژی‌هایی که در سازمان استفاده می‌شود، ارزیابی مستمرآسیب‌پذیری سیستم‌های سازمان که احتمالا توسط کارمندان و پروتکل‌ها بوجود می‌آید، تحلیلی جامع در مورد نمونه حمله‌های سایبری انجام شده در سازمان‌های مشابه صورت پذیرد، فعالیت‌های مدیریت ریسک سایبری بصورت مستمر انجام پذیرد و همچنین سازمان‌ها باید برروی آموزش امنیت سایبری تمرکز کنند. با توجه به پژوهش‌های انجام شده در این مورد، فلامرزی در سال ۱۳۹۵ به بررسی حسابرسی فناوری و ریسک عملیاتی پرداخته‌اند که نتایج حاصل از پژوهش نشان می‌دهد که حسابرسان آموزش دیده و ماهر به عنوان بخشی از نظام راهبری فناوری اطاعات باید در معرفی فناوری جدید درگیر شوند، و همچنین در پژوهشی که توسط علیوردی نیا در سال

۱۳۹۴ صورت پذیرفته اســت که نشان می‌دهد بهترین روش اجرای مقابله با خطرات سایبری به افراد، فرهنگ، مهارت و آموزش‌های لازم بســتگی دارد. که در مقایسه با نتایج این دو پژوهش با پژوهش جاری و با توجه به یافته‌های فوق، آموزش و مهارت برای مقابله با ریسک سیابری، ایجاد فرهنگ امنیت ســایبری با نتایج گذشــته همسو می‌باشــد. و در نهایت با توجه به اینکه بهترین راهکار برای مدیریت ریســک باید شــامل تکنولوژی، فرایندها و افراد متخصص باشد. اعضای تیم باید در آموزش منظم و مداوم امنیت سایبری شرکت کنند. مدیریت ریسک سایبری به سازمان‌ها کمک می‌کند که شکاف‌های عملکرد و پوشش‌های ناقص را شناسایی کنند.

پیشنهادهای پژوهش

توصیه‌های این پژوهش به شرح ذیل می‌باشد؛

۱- ریسک‌های سایبری، به معنای وسیع آن‌ها و به‌عنوان مثال، ریسک‌های رسانه‌های اجتماعی، احتمالاً یک حوزه خطر قابل توجه در آینده برای اکثر سازمان‌ها هستند و این باید پس از ارزیابی مبتنی بر ریسک، در برنامه‌ریزی و اجرای حسابرسی داخلی منعکس شود.

۲- توجه ویژه باید به خطرات مرتبط با تعامل و تبادل داده با تامین کنندگان (از جمله خدمات ابری) و سایر اشخاص ثالث در شرکت توسعه یافته شود.

۳- همچنیــن باید به جنبه‌های رفتاری ریســک ســایبری - اقدامــات و انگیزه‌های افراد - و همچنین جنبه‌های فنی و فرآیندی امنیت اطلاعات توجه دقیق شود.

۴- حسابرسان داخلی باید دانش خود را در مورد خطرات سایبری به روز نگه دارند تا بتوانند از مدیریت خود اطمینان حاصل کنند. این باید هر دو کنترل فعال و واکنشی و استفاده از اطلاعات خارجی را پوشش دهد.

۵- حسابرســی داخلی، مدیریت ریســک و مدیریت عملیاتی باید برای به اشــتراک گذاشتن اطلاعات در مورد خطرات ســایبری با یکدیگر همکاری نزدیک داشــته باشند. حسابرس داخلی نباید به‌عنوان «مدیر تعیین تکلیف» در نظر گرفته شــود، بلکه باید به‌عنوان بخشــی یکپارچه از فرآیند مدیریت ریســک که با عملکردهای تضمینی خط اول و دوم برای اشتراک‌گذاری اطلاعات و اعتبارسنجی پاسخ‌های کنترلی کار می‌کند، در نظر گرفته شود.

۶- اســتقلال حاصل از حسابرسی داخلی باید بخش ارزشــمندی از فرآیند تحقیق پس از یک حادثه یا به عنوان پاسخی به الگوهای غیرمعمول فعالیت‌هایی باشد که در نظارت انتخاب شده‌اند.

منابع

برخوردار، کتایون؛ ناظمی و همکاران(۱۴۰۰). «بررســی عوامل مؤثر بر اثربخشــی حسابرسی داخلی و ارزیابی‌نقش حسابرسی داخلی در مدیریت ریسک و کنترل‌های داخلی بانک کشاورزی» پژوهش‌های حسابرسی حرفه‌ای، شماره دوم، بهار ۱۴۰۰، صص۸-۳۵.

پرندین، کاوه؛ دوست جباریان و همکاران(۱۴۰۲). «موانع اجرای حسابرسی فناوری اطلاعات در

ایران» پژوهش‌های حسابرسی حرفه‌ای، شماره دوازدهم، پاییز ۱۴۰۲، صص ۸۸-۱۰۵.

فلامرزی، حامد و مجیدی، ملیجه(۱۳۹۵). «حسابرسی فناوری و ریسک عملیاتی»،پژوهش‌های نوین در مدیریت، اقتصاد و حسابداری، پنجمین کنفرانس بین‌المللی، مرداد ۱۳۹۵.

کتابچی، الناز و پور قهرمانی(۱۴۰۰) «چالش‌های امنیت سایبری در کشورهای «آ سه آن»»، فصلنامه مطالعات بین‌المللی، صحفات ۱۳۹-۱۵۶- شماره ۶۹ تابستان ۱۴۰۰.

هادی‌خامنه، اعظم و خدیجه ابوالمعالی (۱۴۰۰). «ارائه مدل مفهومی ساختارهای شناختی-ادراکی جرم‌زا در مجرمان سایبری براساس تحلیل روایت زندگی آنان» مجله طب انتظامی، دوره ۱۰ ، شماره ۳، تابستان ۱۴۰۰، ص ۲۰۷-۱۹۸.

یاری، فاطمه و مهر آذین و همکارن (۱۴۰۰)، «اشتهای ریسک، ریسک تداوم فعالیت، توانایی و پاسخگویی مدیریت» حسابداری و منافع اجتماعی، تابستان ۱۴۰۰ ص ۲۰-۱.

Andrew Morrison, cyber security landscape 2022, Deloitte, February 2022.

Albina Orlando, Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk, Risks • October 2021.

Barkhordar, Katayoun, and Nazemi et al. " Investigating Factors Influencing the Internal Audit Effectiveness and Evaluating Internal Audit Role in Risk Management and Internal Controls of Keshavarzi Bank".Professional Auditing Research, Spring 2021, V.1, No2, pp 8-35. (In Persian).

B¨ohme, R., Laube, S., Riek, M., 2018. A fundamental approach to cyber risk analysis. Variance 12 (2), 161–185.

Biener, C., M. Eling, and J.H. Wirfs. 2015. Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance—Issues and Practice 40 (1): 131–158. https:// doi. org/ 10. 1057/ gpp. 2014. 19.

Clarke, R. (June 15-18, 2008). A Risk Assessment Framework for Mobile Payments, 21st Bled eConference e Collaboration: Overcoming Boundaries through Multi-Channel Interaction Bled, Slovenia, April 29, 2011, Available from http://domino.fov.unimb.

Committee of Sponsoring Organizations of the TreadwayCommission(COSO) 2013. Internal Control: Integrated Framework. May 2013. Available at:www.coso.org.

David Canham, Cyber Risk Resources for Practitioners)،2014, Chapter 17: Auditing cyber risks.

Douglas Haveka, Jeffrey W. Merhout.(2013)."Internal information technology audit process quality:Theory development using structured group processes". International Journal of Accounting Information systems14(2013) 165-192.

Eling, M., and W. Schnell. 2016. What do we know about cyber risk and cyber risk insurance? Journal of Risk Finance 17 (5): 474–491. https:// doi. org/ 10. 1108/ jrf- 09- 2016- 0122.

Eling, M., Schnell, W., 2016. Ten key questions on cyber risk and cyber risk insurance. Technical Report 2016. The Geneva Association, Zurich.

European Council. 2021. Cybersecurity: how the EU tackles cyber threats. https:// www. consi lium. europa. eu/ en/ polic ies/ cyber secur ity/. Accessed 10 May 2021.

Falco, G. et al. 2019. Cyber risk research impeded by disciplinary barriers. Science (American Association for the Advancement of Science) 366 (6469): 1066–1069.

Flamarzi, Hamed and Majidi, Malijeh (2015). "Technology Audit and Operational Risk",

Modern Researches in Management, Economics and Accounting, Fifth International Conference, August 2015. (In Persian).

Gordon Archibald, Cyber security considerations 2022 Trust through security KPMG Australia, Janurary 2022. KPMG.com.au.

Hallam-Baker, P. (February 21, 2008). Famous for Fifteen Minutes: A History of Hacking Culture, In: CSO Online-Security and Risk, September, 11 2011.

Hadi-Khameneh, Azam and Khadijah Abul-Maali (2021). "Presentation of the conceptual model of criminal cognitive-perceptual structures in cybercriminals based on the analysis of their life narratives" Journal of Law Enforcement Medicine, Volume 10, Number 3, 2021, pp. 198-207. (In Persian).

Identity Theft Resource Center. (2011). Identity Theft Resource Center A Nonprofit Organization, March 21, 011, Available from http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_L ist.shtml.

Ioan Rus(2015). "Technologies And Methods For Auditing Databases" .Procedia Economice and Finance 26.2015.991-999.

Ketabchi, Elnaz and Pour Garhami (2021) "Challenges of cyber security in ASEAN countries", International Studies Quarterly, pages 139-156- number 69, 2021. (In Persian).

Maleks Smith, Z., E. Lostri, and J.A. Lewis. 2020. The hidden costs of cybercrime. https:// www. mcafee. com/ enter prise/ en- us/ assets/ repor ts/ rp- hidden- costs- of- cyber crime. pdf. Accessed 16 May 2021.

Martin Mullins1 • Finbarr Murphy1 • Stefan Materne2 Cyber risk and cybersecurity: a systematic review of data Availability. Received: 15 June 2021 / Accepted: 20 January 2022 The Geneva Papers on Risk and Insurance - Issues and Practice

Mary E. Galligan and Kelly Rau, (January 2015), COSO in the Cyber Age, Deloitte.

Mohemed, mirghan & Michael Stankosky and Arthur Murray(2006) .konwledge management and information technology:can they work in perfect harmony? Journal of knowledge management.vol.10.no.30.

Maillart, T., Sornette, D. (2010). Heavy-tailed distribution of cyber-risks, European Physical Journal B, Vol. 75, No. 3 (June 2010), pp. 357–364, Available from http://www.springerlink.com/content/866j4814v275r582/fulltext.pdf

NAIC, 2018. Cybersecurity Risk Management, National Association of Insurance Commissioners (NAIC), National Association of Insurance Commissioners (NAIC). (accessed 21 October 2019).AIC (2018).

Ohlhorst, F. (February 10, 2010). Three encryption apps to keep your data safe – data encryption - PC World Business, In: PC World Australia, April 12, 2011, Available from.

Patrick L. Brockett, Linda L. Golden and Whitley Wolman University of Texas at Austin USA, Enterprise Cyber Risk.

Parandin, Kaveh and Doustjabbarian et al ."Obstacles to the implementation of information technology audit in Iran". Professional Auditing Research, Fall 2023, V.3, No 12 pp 88-105. (In Persian).

Price J.(2001) "Auditing E-Business Applications". Internal Auditor.58(4).pp.21-23.

Management, Chapter 14 (pages 319-340)in Risk Management for the Future – Theory and Cases, (2012),Jan Emblemsvag (Ed.)

Rhemann, M. (2011). “Cyber Trends” In: Trends Digest, September 11, 2011.

Sheehan, B., F. Murphy, M. Mullins, and C. Ryan. 2019. Connected and autonomous vehicles:

A cyberrisk classification framework. Transportation Research Part a: Policy and Practice 124: 523–536. https:// doi. org/ 10. 1016/j. tra. 2018. 06. 033.

Siegel, C., Sagalow, T., & Serritella, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security, CRC Press, (March 4, 2002), Available from http://www.eprivacy.com/lectures/cyber-risk.pdf.

Yari, Fatemeh and Mehr Azin et al., "Risk Appetite, Business Continuity Risk, Management Ability and Accountability", Accounting and Social Interests, 2021, pages 1-20. .(In Persian).

پی‌نویس:

1. Committee of Sponsoring Organizations of the Treadway Commission.
2. Information Technology.
3. Cyber-driven world.
4. Radio-frequency identification.
5. Mary
6. External parties.

۷. Cybersecurity Ventures، محقق و ناشر پیشرو در جهان است که اقتصاد سایبری جهانی را پوشش می‌دهد و یک منبع قابل اعتماد برای حقایق، ارقام و آمار امنیت سایبری است.

8. international Organization for Standardization
9. Allianz Global Corporate & Specialty 2020
10. Enterprise Risk Management
11. National Association of Insurance Commissioners
12. Information Communications Technology
13. Operational Technology
14. Mirghan
15. Nation-states and spies.
16. Organized criminals
17. Terrorists.
18. Hacktivists.
19. Insiders.
20. Techniques, tools, and processes
21. Douglas Haveka
22. Ioan Rus
23. General information technology controls.
24. Control Objectives for Information and Related Technology (COBIT).
25. International Organization for Standardization (ISO).
26. National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity
27. Price
28. Universal Serial Bus
29. Gordon Archibald
30. Andrew Morrison
31. Clarke
32. Ohlhorst
33. David Canham
34. Institute of Internal Auditors

۳۵. راهنمایی دقیق در مورد برنامه‌ریزی حسابرسی مبتنی بر ریسک را می‌توان در وب سایت موسسه حسابرسان داخلی www.iia.org.uk بر اساس مدل‌هایی مانند مدل چهار مرحله‌ای برای خدمات مالی نشان داده شده است، یافت.