دستورالعمل حسابرسی فناوری اطلاعات

(IT AM)

نویسنده:

سازمان آفریقایی دیوان‌های محاسبات انگلیسی زبان

برگردان: عباس ارباب سلیمانی

بهاره حقیقی طلب

رامین جهانگیری

مرکز آموزش و تحقیقات حسابداران رسمی

جامعه حسابداران رسمی ایران

فروردین ۱۴۰۲

عنوان و نام پدیدآور:	دستورالعمل حسابرسی فناوری اطلاعات (IT AM)/ نویسنده: سازمان آفریقایی دیوان‌های محاسبات انگلیسی زبان؛ برگردان: عباس ارباب سلیمانی، بهاره حقیقی طلب و رامین جهانگیری.
مشخصات نشـر:	تهران جامعه حسابداران رسمی ایران، ۱۴۰۲.
مشخصات ظاهری:	۳۱۲ ص ۲۲×۲۹ س م.
شابک:	978-622-94504-9-9
وضعیت فهرست‌نویسی:	فیپا
یادداشت:	عنوان اصلی ۲۰۱۷، IT AM ; IT audit manual (IT AM) .
موضوع:	تکنولوژی اطلاعات -- حسابرسی-- دستنامه‌ها
	Information technology -- Auditing -- Handbooks, manuals, etc
	تکنولوژی اطلاعات -- حسابرسی -- استانداردها
	Information technology -- Auditing -- Standards
شناسه افزوده:	ارباب سلیمانی، عباس، ۱۳۲۳
شناسه افزوده:	حقیقی طلب، بهاره، ۱۳۶۵- مترجم
شناسه افزوده:	جهانگیری، رامین، ۱۳۴۴- مترجم
شناسه افزوده:	سازمان آفریقایی دیوان‌های محاسبات انگلیسی زبان
شناسه افزوده:	African Organisation of English-speaking Supreme Audit Institutions
شناسه افزوده:	جامعه حسابداران رسمی ایران
رده‌بندی کنگره:	T۵۸/۵
رده‌بندی دیویی:	۶۵۷/۴۵۰۲۸۵
شماره کتاب‌شناسی ملی:	۹۱۸۶۰۴۵
اطلاعات رکورد کتابشناسی	فیپا

نام کتاب:	دستورالعمل حسابرسی فناوری اطلاعات (IT AM)
برگردان:	عباس ارباب سلیمانی، بهاره حقیقی طلب و رامین جهانگیری.
ناشـر:	جامعه حسابداران رسمی ایران، مرکز آموزش و تحقیقات حسابداران رسمی
شمارگان:	۲۰۰۰
نوبت چاپ:	اول، فروردین ۱۴۰۲.
قیمت:	۱ر۵۰۰ر۰۰۰ ریال
شابک:	978-622-94504-9-9

نشانی: تهران- خیابان سپهبد قرنی- نرسیده به پل کریم‌خان زند- خیابان شهید امانی- شماره ۴

کدپستی ۱۵۹۸۸۶۶۴۱۶- صندوق پستی: تهران ۷۵۴۳-۱۵۸۷۵

تلفن: ۴۲۹۲۵ نمابر: ۸۸۸۰۱۹۱۰

www.iacpa.ir info@iacpa.ir

چاپ شده در آفریقای جنوبی

چاپ اول، ۲۰۱۷

شابک ۹۷۸-۰-۶۳۹۹۹۴۳-۲-۱

AFROSAI-E

www.afrosai-e.org.za

فهرست مطالب	شماره صفحه

فهرست مطالب	شماره صفحه

فهرست مطالب	شماره صفحه

فهرست مطالب	شماره صفحه

فهرست مطالب	شماره صفحه

فهرست مطالب	شماره صفحه

فهرست مطالب	شماره صفحه

فهرست مطالب	شماره صفحه

به‌نام یزدان پاک

پیشگفتار

جامعه حسابداران رسمی ایران در راستای ایفای رسالت اجتماعی و وظایف قانونی و حرفه‌ای خود و همچنین، به‌منظور بالا بردن دانش تخصصی حسابداران رسمی از طریق گسترش و بهبود آموزش، انجام تحقیقات و انتشار نشریه‌های تخصصی و حرفه‌ای در سال‌های گذشته اقدام به برگزاری کلاس‌های آموزشی حرفه‌ای، برگزاری کارگاه‌های آموزشی و انتشار نشریه‌هایی در حوزه حسابداری، حسابرسی و قوانین کرده است و در آینده نیز چنین خواهد کرد.

بنگاه‌های اقتصادی به‌طور فزاینده‌ای فناوری‌های اطلاعات و ارتباطات را برای ایفای وظایف خود و ارائه خدمات مختلف به کار گرفته‌اند. گسترش مداوم فناوری اطلاعات، امکان دریافت، ذخیره، پردازش و ارائه اطلاعات را به صورت الکترونیکی ممکن ساخته است. این گذار به پردازش الکترونیکی، تغییرات چشمگیر در محیط فعالیت حسابرسی را ضروری ساخته است. حسابرسان برای نتیجه‌گیری مناسب حسابرسی ملزم به کسب اطمینان از سیستم‌های کامپیوتری هستند. حسابرسی فناوری اطلاعات، فرایند کسب اطمینان از این است که تدوین و توسعه، پیاده‌سازی، پشتیبانی و نگهداری از سیستم‌های اطلاعاتی در راستای دستیابی به هدف‌های بنگاه اقتصادی، حفاظت از دارایی‌های اطلاعاتی و حفظ یکپارچگی داده‌ها انجام می‌شود. به بیان دیگر، حسابرسی فناوری اطلاعات، اطمینان یافتن از پیاده‌سازی سیستم‌ها و کنترل‌های فناوری اطلاعات مطابق با نیازهای سازمان و بدون آسیب رساندن به امنیت، حریم خصوصی، بهای تمام شده و سایر عناصر مهم تجاری است.

هدف از حسابرسی فناوری اطلاعات، کسب اطمینان از آن است که منابع فناوری اطلاعات، دستیابی اثربخش به هدف‌های سازمانی و استفاده بهینه از منابع را میسر می‌سازند. حسابرسی فناوری اطلاعات، می‌تواند تحقق برنامه‌های کاربردی فناوری اطلاعات، عملیات فناوری اطلاعات، راهبری واحد فناوری اطلاعات، سیستم‌های برنامه‌ریزی منابع سازمانی، امنیت سیستم‌های اطلاعاتی، یافتن راه‌حل‌های تجاری، تدوین و توسعه سیستم و تداوم کسب و کار را امکان‌پذیر سازد. همه این‌ها، زمینه‌های خاصی از پیاده‌سازی سیستم‌های اطلاعاتی یا ناظر بر ارزشی هستند که سیستم‌های اطلاعاتی می‌تواند ارائه نماید. نمونه‌هایی از هدف‌های حسابرسی فناوری اطلاعات عبارتند از:

- بررسی کنترل‌های سیستم‌های فناوری اطلاعات برای اطمینان یافتن از کفایت و اثربخشی آن‌ها.
- ارزیابی فرایندهای مربوط به عملیات یک زمینه چون سیستم حقوق و دستمزد یا سیستم حسابداری مالی.
- ارزیابی عملکرد یک سیستم و امنیت آن، چون سیستم خرید بلیت قطار.
- بررسی فرایند تدوین و توسعه سیستم‌ها و رویه‌ها.

ایجاد نظم و هماهنگی در روش‌های اجرای حسابرسی، از ابتدا مورد توجه و تأکید جامعه حسابداران رسمی ایران بوده است. از آنجا که پیشرفت و توسعه فناوری اطلاعات با سرعت هرچه تمام‌تر در ابعاد مختلف زندگی امروزی تأثیر می‌گذارد، کارگروه فناوری اطلاعات جامعه حسابداران رسمی ایران (آقایان سعید براتی، حمیدرضا بنی‌اسدی، رامین جهانگیری، امیرحسین نریمانی و با مدیریت آقای مهدی بیرانوند و در ادامه، همکاری خانم بهاره حقیقی‌طلب و مدیریت آقای محمدهادی افشاری) بر آن شد تا به‌منظور ارائه مرجع مناسبی برای نشر دانش حسابرسی فناوری اطلاعات و استفاده کاربردی توسط اهالی حرفه حسابرسی و همچنین، ایجاد نظم و یکپارچگی در روش‌های حسابرسی فناوری اطلاعات، کتاب حاضر از انتشارات Afrosai (نسخه سال ۲۰۱۷) را به دلیل پوشش مطالب گسترده (ازجمله کنترل‌های عمومی فناوری اطلاعات) برای برگردان برگزیند.

اهم مطالب پوشش داده شده به شرح زیر است:

- ❖ آشنایی با حسابرسی فناوری اطلاعات؛
- ❖ استانداردها و چارچوب‌ها؛
- ❖ برآورد ریسک حسابرسی با نگرش مدیریت ریسک؛
- ❖ شناخت کنترل‌های فناوری اطلاعات؛
- ❖ مروری کلی بر برنامه‌ریزی؛
- ❖ راهبری فناوری اطلاعات؛
- ❖ حسابرسی خرید، تدوین و توسعه و نگهداری سیستم‌های اطلاعاتی؛
- ❖ عملیات فناوری اطلاعات و شاخص‌های کلیدی عملکرد آن؛
- ❖ امنیت فناوری اطلاعات؛
- ❖ مدیریت تغییر؛
- ❖ حسابرسی تداوم کسب و کار و بازیابی فاجعه؛
- ❖ برون‌سپاری فناوری اطلاعات؛
- ❖ حسابرسی سیستم‌های برنامه‌ریزی منابع سازمانی و
- ❖ گزارشگری.

توجه به این نکته ضروری است که ناشر اصلی، دستورالعمل حاضر را برای اجرای حسابرسی فناوری اطلاعات توسط دیوان محاسبات عمومی منتشر کرده است، اما، رویه‌های پیشنهادی عمدتاً با استناد به استانداردهای بین‌المللی انجمن حسابرسان سیستم‌های اطلاعاتی(ISACA) و استانداردهای سازمان بین‌المللی استانداردها (ISO) ارائه شده‌اند که از عمومیت برخوردار هستند و از این‌رو، می‌توانند برای حسابرسی فناوری اطلاعات توسط مؤسسات حسابرسی نیز مورد استفاده قرار گیرند. همچنین، مفاهیمی از استانداردهای بین‌المللی حسابرسی دیوان محاسبات عمومی که در این کتاب مورد ارجاع قرار گرفته‌اند تا حدود زیادی مشابه استانداردهای بین‌المللی حسابرسی هستند.

اهالی حرفه حسابرسی و استادان دانشگاه همواره از ظرفیت حرفه حسابرسی در جهان، برای اجرای انواع حسابرسی آگاه بوده‌اند. آنچه در این نشریه به آن پرداخته می‌شود، رویه‌های اجرایی و کاربردی برای انجام حسابرسی فناوری اطلاعات است که با توجه به پیشرفت تکنولوژی، مورد نیاز بازار حرفه امروز ایران می‌باشد و امید است نظم بخشیدن به رویه‌های عمل در این دستورالعمل، گامی بلند در راستای آگاهی‌رسانی به صاحبکاران برای استفاده از ظرفیت موجود در مؤسسات حسابرسی برای انجام حسابرسی فناوری اطلاعات باشد. همچنین، نگارندگان تلاش کرده‌اند تا با گردآوری و ارائه واژگان و اصطلاحات تخصصی در حوزه فناوری اطلاعات، امکان دسترسی به سایر مرجع‌های بین‌المللی و نیز هماهنگی در زمینه بکارگیری از این اصطلاحات را برای مخاطبان ایجاد نمایند. از سوی دیگر، پیوست نشریه حاضر دربرگیرنده کاربرگ‌ها و نمونه‌هایی کاربردی برای اجرای کار حسابرسی فناوری اطلاعات می‌باشد که امید است کارگشا باشد.

این کتاب، **دستورالعمل حسابرسی فناوری اطلاعات**، حاصل کار آقای عباس ارباب‌سلیمانی، خانم بهاره حقیقی‌طلب و آقای رامین جهانگیری است. صفحه‌آرایی این نشریه توسط خانم فاطمه دستمزد انجام گردیده است و همکاران مرکز آموزش و تحقیقات حسابداران رسمی، امکان چاپ و نشر آن را فراهم کرده‌اند.

در پایان امیدواریم از راهنمایی‌های همکاران حرفه‌ای، پژوهشگران و استادان برخوردار شویم و کاستی‌ها را، در صورت وجود، جبران کنیم.

مرکز آموزش و تحقیقات حسابداران رسمی

جامعه حسابداران رسمی ایران

به نام ایزد یکتا

پیشگفتار برگردانندگان

حسابرسی یک حرفه پویا است که به‌طور مداوم و فزاینده در معرض تحولات محیط پیرامونی خود قرار می‌گیرد. این تحولات گسترده، زمینه‌ساز بازنگری در رویه‌های اجرای کار و نیز زیربنای لزوم به‌روزآوری رویه‌ها و البته نگرش‌هاست. اهالی حرفه حسابرسی به‌طور مداوم با این بازنگری‌ها و بازبینی‌ها مواجه هستند و در این راستا نیازهای جدید و گوناگونی را احساس می‌کنند. یکی از اساسی‌ترین موضوع‌های روز حرفه حسابرسی، چگونگی کسب شناخت از سیستم‌های اطلاعاتی مورد استفاده سازمان مورد رسیدگی، نحوه اتکا بر آنها و چگونگی بکارگیری آنها در راستای دست‌یابی به هدف‌های حسابرسی است.

آنچه ضرورت دارد که به آن بیندیشیم، لزوم به‌روزآوری و نظام بخشی به برداشت از عبارت **"حسابرسی فناوری اطلاعات"** است. با طرح این عبارت در ایران، دو موضوع به ذهن متبادر می‌شود. نخست، حسابرسی با استفاده از فناوری اطلاعات که تا تاریخ برگردان این کتاب، استفاده از نوعی نرم‌افزار حسابرسی مدون و یکپارچه، در ایران پیاده‌سازی نشده است و دوم، استفاده از فناوری اطلاعات یا رایانه در حسابرسی. این کتاب هیچ‌یک از این دو را به تفصیل بیان نمی‌کند اما، می‌تواند حسابرسان را در اجرای هر دو گونه حسابرسی یاد شده در بالا یاری رساند. در واقع دستورالعمل حاضر، رویه‌های عمل کاربردی برای حسابرسانی را فراهم می‌آورد که هدف آنها، ارائه نظر درباره سیستم‌های اطلاعاتی صاحبکار است، خدمتی جدید و ارزشمند که حسابرسان با بکارگیری این دستورالعمل در همکاری با افراد حرفه‌ای فناوری اطلاعات، قادر به ارائه آن می‌باشند.

ناگفته پیداست حسابرسانی که قادر و مجهز به انجام حسابرسی فناوری اطلاعات به مفهوم اخیر آن باشند، هنگام انجام حسابرسی مالی و سایر انواع حسابرسی، برای کسب شناخت از سیستم‌های اطلاعاتی مورد استفاده سازمان مورد رسیدگی، تعیین میزان قابلیت اتکا بر آنها و بکارگیری مؤثر آنها در راستای دست‌یابی به هدف‌های حسابرسی مالی نیز توانمند خواهند بود. تأخیر در مطالعه، یادگیری و آموزش و بازنشر مفاهیم این کتاب، تأخیر در پذیرش حقیقت پیش روی حسابداران رسمی می‌باشد و امید است بکارگیری آن بتواند در بهبود اثربخشی و کارایی انواع خدمات حسابرسی و اطمینان‌بخشی مؤثر افتد.

برگردان اولیه این کتاب توسط اعضای کارگروه فناوری اطلاعات جامعه حسابداران رسمی ایران (آقایان سعید براتی، حمیدرضا بنی‌اسدی، رامین جهانگیری، امیرحسین نریمانی و با مدیریت آقای مهدی بیرانوند) انجام شده است. با شروع همکاری آقای محمدهادی افشاری با این کارگروه، بازنگری در این برگردان به‌عهده خانم بهاره حقیقی‌طلب گذارده شد- با پیشنهاد کارگروه، آقای عباس ارباب‌سلیمانی نیز به خانم حقیقی‌طلب پیوست. در این راه، از نظرها، پیشنهادها و همفکری آقای رضا باقرزادگان، آقای آرین مرادپور، خانم مائده‌سادات معصومی و خانم شیوا بزرگی‌زاده بهره‌مند شده‌ایم.

در پایان، مسئولیت هرگونه کاستی برعهده برگردانندگان است و امیدواریم استادان حرفه و دانشگاه، حسابرسان، دانش‌پژوهان و دانشجویان، کاستی‌ها را، در صورت وجود، بر ما ببخشایند و ما را از نظرها و پیشنهادهای بهبودبخش خویش، محروم نفرمایند.

عباس ارباب سلیمانی
بهاره حقیقی طلب
رامین جهانگیری
فروردین ۱۴۰۲

کلمات اختصاری

CAATs	*Computer Assisted Audit Techniques*	**تکنیک‌های حسابرسی به کمک رایانه**
CIA	*Confidentiality, Integrity and Availability*	**محرمانگی، کامل بودن و در دسترس بودن**
CISA	*Certified Information Systems Auditor*	**حسابدار رسمی سیستم‌های اطلاعاتی**
COBiT	*Control Objectives for Information and related Technology*	**هدف‌های کنترلی برای اطلاعات و فناوری‌های مرتبط**
COSO	*Committee of Sponsoring Organisations (of the Treadway Commission)*	**کمیته سازمان‌های حمایت‌کننده (تِرِدوی)**
ERP	*Enterprise Resource Planning*	**برنامه‌ریزی منابع سازمانی**
ICT	*Information and Communication Technologies*	**فناوری‌های اطلاعات و ارتباطات**
IS	*Information Systems*	**سیستم‌های اطلاعاتی**
ISACA	*Information System Audit & Control Association*	**انجمن حسابرسان سیستم‌های اطلاعاتی**
ISO	*International Standards Organisation*	**سازمان بین‌المللی استانداردها**
IT	*Information Technology*	**فناوری اطلاعات**
ITAF	*Information Technology Assurance Framework*	**چارچوب اطمینان‌بخش فناوری اطلاعات**
ITIL	*Information Technology Infrastructure Library*	**کتابخانه زیربنایی فناوری اطلاعات**
KPI	*Key Performance Indicators*	**شاخص‌های کلیدی عملکرد**
SAI	*Supreme Audit Institution*	**دیوان محاسبات عمومی**
TOGAF	*The Open Group Architecture Framework*	**چارچوب معماری اُوپِن گروپ**

فصل ۱

آشنایی با حسابرسی فناوری اطلاعات

۱. کلیات

نهادهای دولتی به‌طور فزاینده‌ای فناوری‌های اطلاعات و ارتباطات (ICT) را برای ایفای وظایف خود و ارائه خدمات مختلف به‌کار گرفته‌اند. گسترش مداوم فناوری‌های اطلاعات و ارتباطات امکان دریافت، ذخیره، پردازش و ارائه اطلاعات به صورت الکترونیکی را ممکن ساخته است. این گذار به پردازش الکترونیکی، تغییرات چشمگیر در محیط فعالیت دیوان محاسبات عمومی (SAI) را ضروری ساخته است. برای نتیجه‌گیری مناسب حسابرسی، حسابرسان ملزم به کسب اطمینان از این سیستم‌های رایانه‌ای هستند. به سیستم‌های فناوری اطلاعات (IT)، به‌طور معمول، سیستم‌های اطلاعاتی (IS) نیز گفته می‌شود.

۲. حسابرسی فناوری اطلاعات چیست؟

حسابرسی فناوری اطلاعات، فرایند کسب اطمینان از این است که توسعه، پیاده‌سازی، پشتیبانی و نگهداری از سیستم‌های اطلاعاتی در راستای دستیابی به هدف‌های سازمان، حفاظت از دارایی‌های اطلاعاتی و حفظ یکپارچگی داده‌ها می‌باشد. به بیان دیگر، حسابرسی فناوری اطلاعات، اطمینان یافتن از پیاده‌سازی سیستم‌ها و کنترل‌های فناوری اطلاعات مطابق با نیازهای سازمان و بدون آسیب رساندن به امنیت، حریم خصوصی، بهای تمام شده و سایر عناصر مهم تجاری است.

۳. هدف‌های حسابرسی فناوری اطلاعات

هدف از حسابرسی فناوری اطلاعات، کسب اطمینان از آن است که منابع فناوری اطلاعات، دستیابی اثربخش به هدف‌های سازمانی و استفاده بهینه از منابع را میسر می‌سازند. حسابرسی فناوری اطلاعات، می‌تواند تحقق برنامه‌های کاربردی فناوری اطلاعات، عملیات فناوری اطلاعات، راهبری واحد فناوری اطلاعات، سیستم‌های برنامه‌ریزی منابع سازمانی، امنیت سیستم‌های اطلاعاتی، یافتن راه‌حل‌های تجاری، تدوین و توسعه سیستم و تداوم کسب‌وکار را امکان‌پذیر سازد. همه این‌ها، زمینه‌های خاصی از پیاده‌سازی سیستم‌های اطلاعاتی یا ناظر بر ارزشی هستند که سیستم‌های اطلاعاتی می‌توانند ارائه نمایند.

نمونه‌هایی از هدف‌های حسابرسی فناوری اطلاعات عبارتند از:

- بررسی کنترل‌های سیستم‌های فناوری اطلاعات برای اطمینان یافتن از کفایت و اثربخشی آن‌ها.
- ارزیابی فرایندهای مربوط به عملیات یک زمینه، چون سیستم حقوق و دستمزد یا سیستم حسابداری مالی.
- ارزیابی عملکرد یک سیستم و امنیت آن، چون سیستم خرید بلیت قطار.
- بررسی فرایند تدوین و توسعه سیستم‌ها و رویه‌ها.

۴. الزام برای حسابرسی فناوری اطلاعات

مأموریت دیوان محاسبات برای حسابرسی فناوری اطلاعات، از مأموریت کلی این دیوان‌ها برای انجام حسابرسی ناشی می‌شود. همچنین، در برخی از دیوان‌های محاسبات ممکن است الزام خاصی برای اجرای حسابرسی فناوری اطلاعات یا حسابرسی سیستم‌های اطلاعاتی وجود داشته باشد.

برای بسیاری از دیوان‌های محاسبات، انجام حسابرسی مالی، عملکرد و رعایت، الزامی است کافی برای انجام حسابرسی فناوری اطلاعات. این بدان دلیل است که سیستم‌های فناوری اطلاعات از عملیات اصلی یک سازمان، که ممکن است شامل سیستم‌های مالی باشد، پشتیبانی می‌کنند. بدینسان، حسابرسی فناوری اطلاعات ممکن است دیگر به الزام جداگانه نیاز نداشته باشد.

یک الزام خاص، در صورت وجود باید زمینه‌ی حسابرسی[1] را برای حسابرسی سیستم‌های فناوری اطلاعات، که برای تحقق هدف‌های عملکردی سازمان استفاده می‌شوند، به‌روشنی بیان کند. همچنین باید دسترسی به‌موقع، بدون محدودیت، مستقیم و رایگان را به کلیه اسناد و اطلاعات لازم از توابع یا قسمت‌های درون یا برون‌سپاری شده سازمان، به‌صورت دستی و الکترونیکی، فراهم کند.

۵. انواع و دامنه حسابرسی‌های فناوری اطلاعات

حسابرسی‌های فناوری اطلاعات ممکن است به‌صورت بررسی جداگانه از سیستم‌های اطلاعاتی یا همراه با حسابرسی صورت‌های مالی، بررسی کنترل‌های داخلی و/ یا به‌عنوان حسابرسی‌های عملکرد سیستم‌های فناوری اطلاعات یا برنامه‌های کاربردی فناوری اطلاعات انجام شود. دامنه حسابرسی‌های فناوری اطلاعات، شامل حسابرسی ویژه[2]، حسابرسی دادگاهی[3] و پروژه‌های تدوین سیستم‌های اطلاعاتی[4] نیز می‌باشد.

1. Jurisdiction of Audit
2. Specialised Audit
3. Forensic Audit
4. Information Systems (IS) Development Projects

دامنه هر حسابرسی در زیر آمده است:

- **حسابرسی سیستم‌های اطلاعاتی**

حسابرسی سیستم‌های اطلاعاتی[1]، فرایند گردآوری و ارزیابی شواهدی است تا مشخص شود آیا سیستم‌های اطلاعاتی و منابع مرتبط، به‌اندازه کافی از دارایی‌ها حفاظت می‌کنند؟ آیا یکپارچگی و در دسترس بودن سیستم و داده‌ها را حفظ می‌کنند؟ آیا اطلاعات مربوط و قابل اتکا ارائه می‌دهند؟ آیا به صورت اثربخش، به هدف‌های سازمانی دست می‌یابند؟ آیا منابع را به‌گونه‌ای کارآمد مصرف می‌کنند و کنترل‌های داخلی مؤثری برای کسب اطمینان معقول از دستیابی به هدف‌های تجاری، عملیاتی و کنترلی را برقرار می‌کنند؟ آیا از رویدادهای نامطلوب، پیشگیری یا آن‌ها را به‌موقع، کشف و اصلاح می‌کنند؟

- **حسابرسی مالی**

حسابرسی مالی[2] به دنبال ارزیابی درستی صورت‌های مالی یک سازمان است. حسابرسی فناوری اطلاعات برای ارزیابی کفایت حفاظت از یکپارچگی داده‌ها توسط سیستم‌های اطلاعاتی و منابع مرتبط (شامل اطلاعات)، در حسابرسی مالی انجام می‌شود.

- **حسابرسی رعایت**

حسابرسی رعایت[3] شامل آزمون کنترل‌های مشخص برای بررسی مطابقت با مقررات و استانداردهای خاص است. این حسابرسی‌ها اغلب با حسابرسی‌های سنتی فناوری اطلاعات، همپوشانی دارند اما ممکن است بر سیستم‌ها یا داده‌های خاصی تمرکز کنند.

- **حسابرسی عملکرد**

حسابرسی عملکرد[4]، بررسی مستقل، واقع‌بینانه و قابل اتکا برای این است که انطباق عملکرد اقدامات، سیستم‌ها، عملیات، برنامه‌ها، فعالیت‌ها یا سازمان‌های دولتی با اصول صرفه اقتصادی، کارایی و اثربخشی و همچنین، وجود امکان پیشرفت را مشخص کند. حسابرسان فناوری اطلاعات، سیستم‌های فناوری اطلاعات را که با توجه به معیارهای صرفه اقتصادی، کارایی، اثربخشی و ارزش‌آفرینی برای شهروند پیاده‌سازی می‌شوند، بررسی می‌کنند (استاندارد بین‌المللی دیوان‌های محاسبات[5]، بخش ۵۳۰۰).

1. Information System Audit
2. Financial Audit
3. Compliance Audit
4. Performance Audit
5. International Standards of Supreme Audit Institutions 5300 (ISSAI-5300)

حسابرسی فناوری اطلاعات می‌تواند سایر بررسی‌های تخصصی درباره زمینه‌های خاص را، مانند برون‌سپاری یا هدف‌های خاص چون دادگاه‌های دیجیتال، پوشش دهد.

صرف‌نظر از نوع حسابرسی، حسابرس فناوری اطلاعات موظف است سیاست‌ها و رویه‌های هدایت‌کننده محیط کلی فناوری اطلاعات سازمان مورد حسابرسی را ارزیابی کند تا از برقراری کنترل‌های مربوط و مکانیسم‌های اجرایی اطمینان یابد.

حسابرس فناوری اطلاعات باید از میان هدف‌های تعیین‌شده برای حسابرسی فناوری اطلاعات، درباره دامنه حسابرسی تصمیم بگیرد. تعیین دامنه حسابرسی فناوری اطلاعات عبارت است از: تصمیم‌گیری در مورد ژرفای رسیدگی‌ها[1]، پوشش سیستم‌های فناوری اطلاعات و ویژگی‌های آن‌ها، فرآیندهای فناوری اطلاعات که باید حسابرسی شوند، محل استقرار سیستم‌های فناوری اطلاعات زیرِ پوشش و دوره پوشش. این امر در واقع، تنظیم یا ترسیم مرزهای حسابرسی خواهد بود.

۶. مرور کلی فرآیند حسابرسی فناوری اطلاعات

حسابرسی فناوری اطلاعات مراحلی مشابه با حسابرسی قانونی[2] را دنبال می‌کند. با این‌حال، روش‌ها و ابزارهای مورد استفاده برای گردآوری شواهد حسابرسی ممکن است متفاوت باشند. این مراحل را می‌توان به‌طور کلی به شرح زیر طبقه‌بندی کرد:

فعالیت‌های پیش از بستن قرارداد- دربرگیرنده ارزیابی واقع‌بینی[3]، صلاحیت و توان تخصصی کارکنان حسابرسی و تعیین بودجه زمانی حسابرسی است. همچنین، دستیابی به شناخت و انتظاراتی مشترک برای انعقاد قرارداد را دربر می‌گیرد.

شناخت سازمان

- **برآورد ریسک**- برآورد ریسک که طی آن، حسابرسان از جوّ سازمان مورد حسابرسی شناخت بدست می‌آورند، ریسک‌ها و سطح اهمیت را در سطح سازمانی شناسایی و ارزیابی می‌کنند. این فرایند همچنین، از مورد توجه قرار دادن همه عوامل پیرامونی محیط فعالیت سازمان مورد رسیدگی اطمینان می‌دهد. طرح کلی حسابرسی در این مرحله با سازمان مورد حسابرسی مطرح می‌شود.

1. Audit Scrutiny
2. Regularity Audit
3. Objectivity

- **اجرای حسابرسی**- در این مرحله از حسابرس انتظار می‌رود که فرآیندهای تفصیلی مربوط به هر مرحله حسابرسی را درک کرده باشد، برنامه‌های حسابرسی را طراحی نموده باشد و اجرای برنامه‌ها را با تکمیل الگوهای ارائه شده، مستندسازی کند.
- **گزارشگری حسابرسی**- آخرین نامه مدیریتی که از فرآیند حسابرسی حاصل می‌شود.

هنگام اجرای حسابرسی فناوری اطلاعات برای شناسایی اولویت باید از رویکرد حسابرسی با نگرش مدیریت ریسک استفاده شود؛ که شامل شناسایی عوامل ریسک موجود در سازمان مورد ارزیابی، همراه با تعیین امتیازات موزون ریسک بر اساس معیارهای خاص ارزیابی است. این امتیاز موزون ریسک، می‌تواند حسابرس را با تعیین اثر و احتمال رخداد یک اثر نامطلوب درگیر کند. حسابرس با رعایت یک معیار مناسب می‌تواند ریسک‌ها را به‌صورت بالا، متوسط و پایین طبقه‌بندی نماید.

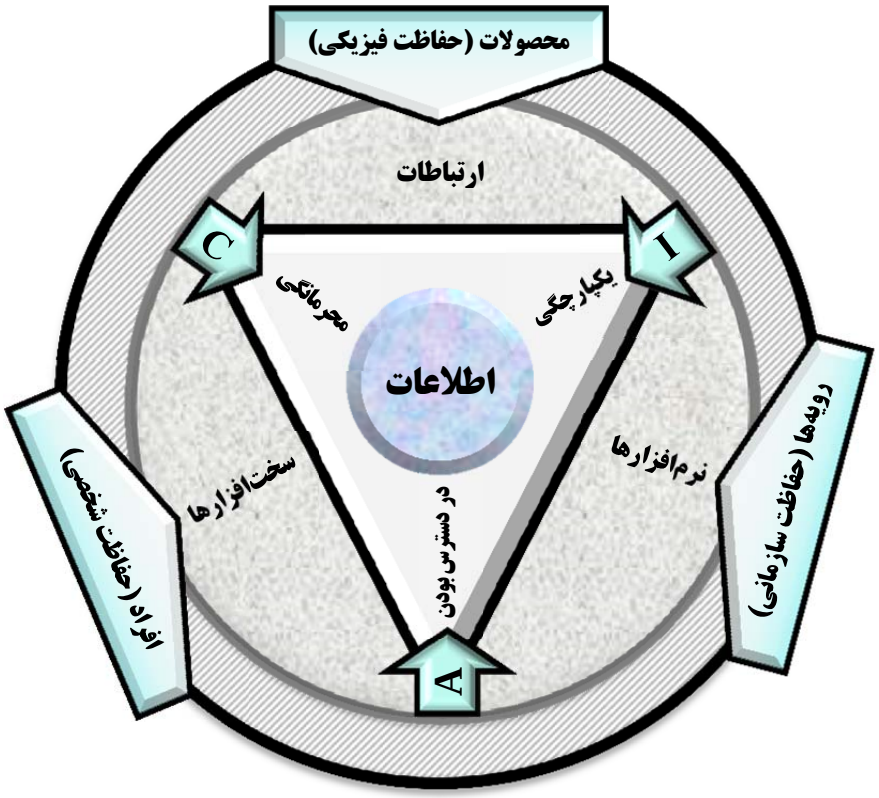
استاندارد بین‌المللی دیوان‌های محاسبات بخش ۵۳۰۰، حسابرس را به تهیه مستندات حسابرسی به‌اندازه کافی و تفصیلی ملزم می‌کند که یک درک کلی نسبت به حسابرسی را فراهم کند. بررسی این مستندات باید هر حسابرس فناوری اطلاعات دیگری را قادر به دستیابی به نتیجه‌گیری مشابه نماید. هیچ روش استانداردی برای مستندسازی حسابرسی فناوری اطلاعات در استاندارد بین‌المللی دیوان‌های محاسبات تعریف نشده است. افزون بر این، ممکن است رویه‌ها از یک دیوان به دیوان دیگر فرق کند. سطحی از استانداردسازی در قالب چک‌لیست‌ها، کاربرگ‌ها، نمونه نامه‌ها و غیره می‌تواند در هر دیوان وجود داشته باشد.

در طول فرآیند حسابرسی، برای اطمینان یافتن از دستیابی به هدف‌های حسابرسی باید کنترل کیفیت وجود داشته باشد.

۷. پیوندهای حسابرسی مالی و حسابرسی فناوری اطلاعات

استاندارد بین‌المللی دیوان‌های محاسبات شماره ۱۳۱۵، مسئولیت حسابرس را برای شناسایی و ارزیابی ریسک‌های تحریف با اهمیت از طریق شناخت سازمان و محیط آن، مشخص می‌کند. از این‌رو، در یک محیط رایانه‌ای، شناخت اینکه چگونه کنترل‌ها می‌توانند بر صورت‌های مالی مؤثر باشند، مهم است. حسابرس باید درک درستی از سیستم اطلاعاتی، ازجمله فرآیندهای تجاری مرتبط با گزارشگری مالی بدست آورد.

همان‌گونه که در نمودار زیر مشخص شده است، تمرکز کنترل‌های حسابرسی فناوری اطلاعات بر ارزیابی **محرمانگی**[1]، **یکپارچگی**[2] و **در دسترس بودن**[3] **(CIA)** منابع سیستم اطلاعاتی است.



از سوی دیگر، حسابرسی مالی **به ارائه مطلوب صورت‌های مالی** مربوط است. حسابرس باید رعایت شدن یا نشدن گزاره‌هایی (ادعاهایی) مانند رخداد، کامل بودن، درستی، انقطاع زمانی، طبقه‌بندی، وجود و ارزشیابی را ارزیابی کند تا بتواند نظر مناسبی ارائه دهد.

پیوند بین آن دو در این است که هدف‌های کنترلی فناوری اطلاعات (محرمانگی، یکپارچگی و در دسترس بودن) ممکن است در گزاره‌های مالی تأثیر داشته باشند. ارزیابی این کنترل‌های فناوری اطلاعات به حسابرس کمک می‌کند تا از ارائه منصفانه صورت‌های مالی تهیه شده با استفاده از سیستم‌های اطلاعاتی و فرآیندهای آن، اطمینان حاصل کند.

1. Confidentiality
2. Integrity
3. Availability

۸. نقش حسابرس فناوری اطلاعات در حسابرسی مالی چیست؟

با توجه به استاندارد بین‌المللی دیوان‌های محاسبات، کاملاً مشخص است که حسابرس باید در طول حسابرسی مالی، کنترل‌های داخلی را بررسی کند. نقش حسابرس فناوری اطلاعات در فرآیند حسابرسی مالی، کمک به حسابرس مالی در تعیین این است که آیا می‌توان به کنترل‌هایی که سازمان ایجاد کرده است و اثربخشی محیط کنترلی فناوری اطلاعات و همچنین، محیط کاربرد آن اطمینان کرد؟ نتایج حاصل از کار حسابرس فناوری اطلاعات، رویکردی را تعیین می‌کند که حسابرس مالی در اجرای حسابرسی پیش خواهد گرفت.

برنامه‌ریزی حسابرسی کنترل‌های عمومی نیز باید در مرحله برنامه‌ریزی حسابرسی مالی و همچنین، آزمون کنترل‌ها انجام شود. نتایج حاصل از حسابرسی کنترل های عمومی به تعیین طرح کلی حسابرسی توسط حسابرس کمک خواهد کرد. در صورت نیاز به حسابرسی کاربردها، اجرای آن در مرحله اجرای حسابرسی مالی انجام می‌شود. در صورت وجود یافته‌های با اهمیت، حسابرس پس از در نظر گرفتن و آزمون هرگونه کنترل جبرانی مربوط به ضعف خاص در کنترل‌ها باید آن یافته‌ها را در مرحله گزارشگری حسابرسی مالی به مدیریت گزارش کند.

با وجود این‌که ارزیابی کنترل‌های فناوری اطلاعات بر روی محرمانگی، یکپارچگی و در دسترس بودن منابع سیستم اطلاعاتی تمرکز دارد، چگونگی امکان ارتباط دادن یافته‌های حسابرسی فناوری اطلاعات به گزاره‌های حسابرسی مالی نیز در صورت امکان، مهم است. در بسیاری از موارد، حسابرس مالی اطمینان ندارد که استقرار نیافتن کنترل‌های عمومی چگونه می‌تواند بر صورت‌های مالی اثر بگذارد. نبود کنترل‌های فناوری اطلاعات، اثر غیرمستقیم بر صورت‌های مالی دارد و گاه این ریسک‌ها می‌تواند به‌صورت مبالغ کمی درآید؛ برای مثال، استفاده از تکنیک‌های حسابرسی به کمک رایانه (CAAT)[1] برای تعیین ایام مرخصی کارکنان و زمان تصویب معاملات.

در پایان هر روز کاری، حسابرس مالی باید کار انجام شده توسط حسابرس فناوری اطلاعات را مطابق با الزامات استانداردهای بین‌المللی دیوان‌های محاسبات تأیید کند و همان‌گونه که پیشتر آمد باید در گزارش حسابرسی سالانه رییس دیوان محاسبات[2] بیاید.

1. Computer Assissted Audti Techniques (CAATs)
2. Auditor General

اصطلاحاتی که در فصل ۱ بر آن تأکید شده است:

- **انواع و دامنه حسابرسی‌های فناوری اطلاعات (Types and Scope of IT Audits)**: حسابرسی‌های فناوری اطلاعات ممکن است به‌صورت رسیدگی ویژه به سیستم‌های اطلاعاتی یا همراه با حسابرسی صورت‌های مالی، بررسی کنترل‌های داخلی و/ یا به‌عنوان حسابرسی‌های عملکرد سیستم‌های فناوری اطلاعات یا برنامه‌های کاربردی فناوری اطلاعات انجام شود. دامنه حسابرسی‌های فناوری اطلاعات، حسابرسی ویژه، حسابرسی دادگاهی و پروژه‌های توسعه سیستم‌های اطلاعاتی را دربر می‌گیرد.
- **هدف از حسابرسی فناوری اطلاعات (IT Audit Objective)**: اطمینان یافتن از آن‌که منابع فناوری اطلاعات، دستیابی اثربخش به هدف‌های سازمانی و استفاده بهینه از منابع را میسر می‌سازند.

فصل ۲

استانداردها و چارچوب‌ها

۱. کلیات

چارچوب‌ها، استانداردها، دستورالعمل‌ها و ابزارهای بسیاری وجود دارند که حسابرس را در انجام حسابرسی سیستم‌های اطلاعاتی راهنمایی می‌کنند. حسابرس باید هنگام حسابرسی فناوری اطلاعات از اطلاعات موجود آگاه باشد و بتواند از آن‌ها به‌عنوان ابزارهای مرجع استفاده کند.

۲. استانداردها

استانداردها، مجموعه‌ای از معیارهای عملیاتی یا فنی، روش‌ها یا رویه‌های عمل هستند. استانداردها، اطلاعات تفصیلی‌تر را درباره چگونگی انجام جنبه‌های خاصی از وظایف مدیران و متخصصان، ارائه می‌دهد. حسابرس هنگام حسابرسی باید به این استانداردها پایبند باشد.

۲-۱. استانداردهای بین‌المللی دیوان‌های محاسبات

مجموعه استانداردهای بخش ۵۳۰۰ تا ۵۳۹۹ در چارچوب استانداردهای بین‌المللی دیوان‌های محاسبات به ارائه دستورالعمل‌های حسابرسی فناوری اطلاعات اختصاص داده شده است. استاندارد بخش ۵۳۰۰ دربر دارنده اصول کلی این استانداردها درباره مبانی اساسی حسابرسی فناوری اطلاعات است که چارچوب دستورالعمل‌های تفصیلی‌تر را فراهم می‌آورد.

برخی از این استانداردهای خاص مربوط به حسابرسی سیستم‌های اطلاعاتی به شرح زیر است:

- دستورالعمل استاندارد بین‌المللی دیوان‌های محاسبات شماره ۵۳۰۰ برای راهنمایی متخصصان حسابرسی فناوری اطلاعات در اجرای حسابرسی فناوری اطلاعات.
- استاندارد بین‌المللی دیوان‌های محاسبات شماره ۵۳۱۰ درباره روش بررسی امنیت سیستم‌های اطلاعاتی.
- استاندارد بین‌المللی دیوان‌های محاسبات شماره ۵۴۵۰ درباره سیستم اطلاعاتی دیون بخش عمومی.

۲-۲. استانداردهای انجمن حسابرسان سیستم‌های اطلاعاتی

انجمن حسابرسان سیستم‌های اطلاعاتی (ISACA)[1]، یک انجمن جهانی است که در زمینه توسعه، پذیرش و بکارگیری جهانی دانش پیشرو در صنعت و رویه‌های مرتبط با سیستم‌های اطلاعاتی فعالیت می‌کند. استانداردهای حسابرسی و اطمینان‌بخشی سیستم‌های اطلاعاتی، الزامات لازم‌الاجرا برای حسابرسی و گزارشگری سیستم‌های اطلاعاتی را تعریف و مقرر می‌کند که:

- ❖ افراد حرفه‌ای حسابرسی و اطمینان‌بخشی سیستم‌های اطلاعاتی، زمانی به سطح عملکرد قابل قبول الزامی دست می‌یابند که دستِ‌کم مسئولیت‌های حرفه‌ای یاد شده در آیین رفتار حرفه‌ای انجمن[2] را رعایت کنند.
- ❖ دارندگان مدرک حسابرس خبره سیستم‌های اطلاعاتی (CISA)[3] در صورت احراز شرایط.

رعایت نکردن این استانداردها ممکن است به تحقیق در مورد دارنده مدرک حسابرس خبره توسط هیأت مدیره انجمن یا کمیته مربوط منجر و در نهایت، سبب اقدامات انضباطی شود (برای مطالعه بیشتر، به چارچوب اطمینان‌بخش فناوری اطلاعات (ITAF)[4] مراجعه کنید).

۲-۳. مقررات و استانداردهای ملی

استانداردهای ملی را می‌توان استانداردهای مقرر توسط نهادهای دولتی گفت. هر سازمان باید الزامات دولتی و برون‌سازمانی مربوط به سیستم‌های اطلاعاتی را رعایت کند. حسابرس باید به استانداردهای ملی مؤثر بر سیستم‌های اطلاعاتی مورد حسابرسی خود توجه نماید. این استانداردها زیربنایی برای ارزیابی سیستم اطلاعاتی یک سازمان را تشکیل می‌دهند. اگرچه، در صورت نبود استانداردهای ملی، حسابرس باید از بهترین رویه‌های عمل موجود راهنمایی بگیرد.

۲-۴. استانداردهای فناوری اطلاعات سازمان بین‌المللی استاندارد

سازمان بین‌المللی استاندارد (ISO)[5] بزرگترین استاندارد گذار جهانی در زمینه وضع استانداردهای بین‌المللی برای پذیرش داوطلبانه است. استانداردهای بین‌المللی، جدیدترین ویژگی‌ها برای محصولات، خدمات و رویه‌های مناسب را برای کارایی و اثربخشی هرچه بیشتر صنعت ارائه می‌دهند. همچنین، از طریق اجماع جهانی، به کاهش موانع تجارت بین‌المللی کمک می‌کند.

1. Information Systems Audit and Control Association (ISACA)
2. ISACA Code of Professional Ethics
3. Certified Information System Auditor (CISA)
4. IT Assurance Framework (ITAF)
5. International Organization for Standardization (ISO)

برخی از استانداردهای قابل اجرا برای حسابرسی فناوری اطلاعات به شرح زیر است:

- **ایزو ۲۰۰۰۰ (عملیات فناوری اطلاعات)**

ایزو ۲۰۰۰۰، اولین استاندارد در مدیریت خدمات فناوری اطلاعات و شامل طراحی، انتقال، تحویل و بهبود الزامات خدمات و ارائه ارزش برای هر دو طرف، یعنی سازمان و ارائه‌دهنده خدمات است.

- **ایزو ۲۷۰۰۰ (امنیت فناوری اطلاعات)**

این استاندارد، دستورالعمل‌ها و اصول کلی را برای تدوین، پیاده سازی، نگهداری و بهبود مدیریت امنیت اطلاعات[1] در یک سازمان ارائه می‌دهد.

- **ایزو ۳۱۰۰۰ (ریسک)**

این استاندارد، سازمان‌ها را در مدیریت مؤثر ریسک در محیطی سرشار از عدم اطمینان، یاری می‌رساند تا سازمان‌ها بتوانند به‌طور فزاینده‌ای به هدف‌های خود دست یابند، شناسایی فرصت‌ها و تهدیدها را بهبود بخشند و منابع را به‌گونه مؤثری برای مقابله با ریسک تخصیص دهند و استفاده نمایند.

- **ایزو ۳۸۵۰۰ (راهبری)**

این استاندارد، چارچوبی را برای راهبری[2] مؤثر فناوری اطلاعات برای مدیریت ارشد، فراهم می‌نماید تا تعهدات حقوقی، قانونی و اخلاقی خود را برای استفاده سازمان از فناوری اطلاعات درک و رعایت کنند. این استاندارد، شش اصل را برای راهبری خوب فناوری اطلاعات به شرح زیر، تعیین کرده است:

- مسئولیت،
- راهبرد (استراتژی)،
- تحصیل،
- عملکرد،
- سازگاری، و
- رفتار انسانی.

1. Security
2. Governance

۳. چارچوب‌ها

چارچوب، بیانیه‌ای رسمی است که محتوا و رهنمودهای لازم را برای هیأت مدیره با نگرش به موضوع یا انواع سیاست‌های اداره سازمان فراهم می‌کند. همچنین، ساختار لازم برای پشتیبانی از درک راهبردی آن سیاست‌های خاص و دیگر ابزارها را فراهم می‌آورد و چرایی تعیین سیاست سازمان را در زمینه خاص، مثلاً موارد زیر، تشریح می‌کند:

۳-۱. چارچوب اطمینان‌بخش فناوری اطلاعات (ITAF)

چارچوب اطمینان‌بخش فناوری اطلاعات (ITAF) تهیه شده توسط انجمن حسابرسان سیستم‌های اطلاعاتی، الگویی جامع و مدلی خوب از رویه‌های عمل است که:

- در مورد طراحی، اجرا و گزارشگری حسابرسی فناوری اطلاعات و وظایف اطمینان‌بخشی، راهنمایی لازم را فراهم می‌کند.
- اصطلاحات و مفاهیم خاص اطمینان بخشی فناوری اطلاعات را تعریف می‌کند.

این چارچوب، استانداردهایی وضع می‌کند که به نقش‌ها و مسئولیت‌های حرفه‌ای، دانش و مهارت‌ها، دقت نظر، الزامات اجرا و گزارشگری حسابرس فناوری اطلاعات می‌پردازد. این چارچوب، مرجعی یگانه را برای حسابرسان سیستم‌های اطلاعاتی فراهم می‌نماید تا بتوانند از طریق آن، راهنمایی‌ها، سیاست‌ها و رویه‌های پژوهشی، برنامه‌های حسابرسی و اطمینان‌بخشی و ارائه گزارش‌های مؤثر را دریافت کنند.

۳-۲. هدف‌های کنترلی فناوری اطلاعات (COBIT)

هدف‌های کنترلی اطلاعات و فناوری‌های مرتبط (COBiT)[1] یک چارچوب کنترلی برای راهبری فناوری اطلاعات است که دلایل نیاز به راهبری فناوری اطلاعات، ذینفعان آن و آنچه را که برای تحقق آن لازم است، تعریف می‌کند. این هدف‌ها، یک نقشه راه برای راهبری خوب فناوری اطلاعات است. COBiT، بهترین رویه‌های عمل را در دامنه و چارچوب فرآیند ارائه می‌دهد و فعالیت‌هایی را در یک ساختار قابل کنترل و منطقی ارائه می‌دهد. این هدف‌ها بیشتر بر کنترل تمرکز دارند تا بر اجرا. این رویه‌ها، به بهینه‌سازی سرمایه‌گذاری‌های مبتنی بر فناوری اطلاعات

1. Control Objectives for Information and related Technology (COBiT)

کمک می‌کند، از ارائه خدمات، اطمینان می‌دهد و معیارهایی را برای قضاوت هنگام نادرست بودن امور ارائه می‌دهد. تمرکز COBiT بر مورد زیر:

> **COBiT**، کسب‌وکار را به تعریف الزامات عملیاتی و کنترلی و استفاده از خدمات خودکار متعهد می داند، حال آنکه فناوری اطلاعات، وظیفه خودکارسازی و پیاده‌سازی الزامات عملیاتی و کنترل تعیین شده توسط کسب وکار و ایجاد کنترل‌هایی برای حفظ یکپارچگی کنترل‌های کاربردی را بر عهده دارد.

۴. کتابخانه زیربنایی فناوری اطلاعات (ITIL)

کتابخانه زیربنایی فناوری اطلاعات (ITIL)[1] مجموعه‌ای است از رویه‌ها که بر همگرایی فناوری اطلاعات با هدف‌های تجاری تمرکز دارد. این مجموعه، مبنایی را برای سازمان برای برنامه‌ریزی، پیاده‌سازی و اندازه‌گیری خدمات مورد ارائه فراهم می‌کند. نشر سوم این کتابخانه دارای پنج بخش زیر است:

- راهبرد خدمات کتابخانه،
- طراحی خدمات کتابخانه،
- انتقال/ ارائه خدمات کتابخانه،
- عملیات خدمات کتابخانه، و
- بهبود مستمر خدمات کتابخانه.

۵. ارزش‌آفرینی فناوری اطلاعات (Val IT)

ارزش‌آفرینی فناوری اطلاعات یک چارچوب سازماندهی جامع و عملگرا است که می‌تواند از سرمایه‌گذاری‌های مبتنی بر فناوری اطلاعات، ارزش تجاری ایجاد کند. این ارزش‌آفرینی همگرا و مکمل با COBiT طراحی شده است و مجموعه‌ای از اصول راهبری عملی و اثبات شده، فرایندها، رویه‌ها و دستورالعمل‌های پشتیبانی را در اختیار قرار می‌دهد که اعضای هیأت مدیره، گروه‌های مدیریت اجرایی و سایر رهبران سازمانی را در شناخت و درک ارزش سرمایه‌گذاری در فناوری اطلاعات یاری می‌کند.

1. IT Infrastructure Library (ITIL)

۶. سایر استانداردها و چارچوب‌هایی که حسابرس فناوری اطلاعات باید بداند

۶-۱. کمیته سازمان‌های حمایت‌کننده (تِرِدوی) (COSO)

کوزو[1] سازمانی مستقل است که در ابعاد مهم راهبری سازمانی، اخلاق کسب‌وکار و مدل کنترل داخلی، امکان رهبری را برای مدیریت اجرایی و نهادهای راهبری فراهم می‌آورد و بر مبنای آن، شرکت‌ها و سازمان‌ها می‌توانند سیستم‌های کنترلی خود را ارزیابی کنند. کوزو، توسط پنج سازمان پشتیبانی می‌شود که عبارتند از: انجمن حسابداران مدیریت (IMA)[2]، انجمن حسابداری آمریکا (AAA)[3]، انجمن حسابداران رسمی آمریکا (AICPA)[4]، انجمن حسابرسان داخلی (IIA)[5] و مدیران مالی بین‌المللی (FEI)[6].

۶-۲. ریسک فناوری اطلاعات

مجموعه‌ای است از اصول راهنما و نخستین چارچوب برای کمک به شرکت‌ها در شناسایی، اداره و مدیریت مؤثر ریسک فناوری اطلاعات.

۶-۳. چارچوب معماری اُوپِن گروپ

چارچوبی است برای معماری سازمانی که رویکردی را برای طراحی، برنامه‌ریزی، پیاده‌سازی و راهبری معماری فناوری اطلاعات سازمان ارائه می‌دهد. این چارچوب (TOGAF)[7] از سال ۲۰۱۱ تاکنون یک برند تجاری ثبت شده از اُوپِن گروپ در ایالات متحده و سایر کشورها است.

این چارچوب، یک رویکرد والارتبه برای طراحی است که معمولاً در چهار سطح زیر مدل‌سازی می‌شود:

- کسب وکار،
- برنامه کاربردی،
- داده‌ها، و
- فناوری.

این امر به شدت به مدل‌سازی، استانداردسازی و فناوری‌ها و محصولات ثبت شده موجود اتکا دارد.

1. Committee of Sponsoring Organisations of the Treadway Commission (COSO)
2. Institute of Management Accountants (IMA)
3. American Accounting Association (AAA)
4. American Institute of Certified Public Accountants (AICPA)
5. Institute of Internal Auditors (IIA)
6. Financial Executives International (FEI)
7. The Open Group Architecture Framework (TOGAF)

۶-۴. استانداردهای فنی انجمن و بهترین رویه‌های عمل

سازمان‌ها و انجمن‌های گوناگونی وجود دارند که استانداردها و بهترین رویه‌های عمل را برای راهنمایی اعضای خود ایجاد کرده‌اند. برخی از آن‌ها به شرح زیر است:

- **انجمن صنعت ارتباطات از راه دور**

مجموعه‌ای از استانداردهای ارتباط از راه دور توسط انجمن صنعت ارتباطات از راه دور (TIA)[1] ایجاد شده است که برقراری ارتباطات تجاری برای محصولات و خدمات ارتباطات از راه دور را مد نظر قرار داده است. یکی از استانداردهای خاص این انجمن که حسابرس فناوری اطلاعات می‌تواند از آن استفاده کند، استاندارد شماره ۹۴۲ با نام مراکز داده[2] است.

- **مرکز امنیت اینترنت**

مرکز امنیت اینترنت (CIS)[3] سازمانی است که برای ارتقای آمادگی و برخورد با امنیت سایبری در بین نهادهای دولتی و بخش خصوصی تشکیل شده است.

- **انجمن ملی استاندارد و فناوری (NIST)**

انجمن ملی استاندارد و فناوری (NIST)[4] بخشی از وزارت بازرگانی ایالات متحده است که اصول و روش‌های پذیرفته شده برای امنیت سیستم‌های فناوری اطلاعات و مجموعه‌ای از اصول و شیوه‌ها را برای ایجاد و حفظ امنیت سیستم، منتشر می‌کند.

۶-۵. استانداردهای ارائه‌کنندگان/ فروشندگان و بهترین رویه عمل خاص

فروشندگان مختلف (برای مثال مایکروسافت، اوراکل، SAP) در مورد بهترین رویه‌های عمل و چگونگی حفاظت از محصولات خود، توصیه‌هایی را ارائه می‌دهند.

۷. دستورالعمل‌ها

دستورالعمل‌ها، راهنمایی‌هایی را برای بکارگیری استانداردهای حسابرسی سیستم‌های اطلاعاتی ارائه می‌دهند. حسابرس سیستم‌های اطلاعاتی باید این دستورالعمل‌ها را در تعیین چگونگی استقرار آنها و استفاده از قضاوت حرفه‌ای در بکارگیری آن‌ها در نظر بگیرد و بتواند هرگونه انحراف از آن‌ها را توجیه کند. هدف دستورالعمل‌های حسابرسی سیستم‌های اطلاعاتی، فراهم آوردن اطلاعات بیشتر در مورد چگونگی رعایت استانداردهای حسابرسی سیستم‌های اطلاعاتی است.

1. Telecommunication Industry Association (TIA)
2. Data Centres
3. Centre for Internet Security (CIS)
4. National Institute of Standards and Technology (NIST)

اصطلاحاتی که در فصل ۲ بر آن تأکید شده است:

- **استانداردها (Standards):** استانداردها، مجموعه‌ای از معیارهای عملیاتی یا فنی، روش‌ها یا رویه عمل‌ها است که اطلاعات تفصیلی‌تر درباره چگونگی انجام جنبه‌های خاصی از وظایف مدیران و متخصصان را ارائه می‌دهد. حسابرس هنگام انجام حسابرسی باید به این استانداردها پایبند باشد.

- **چارچوب‌ها (Frameworks):** بیانیه‌هایی رسمی هستند که محتوا و رهنمودهای لازم را برای هیأت مدیره با نگرش به موضوع یا انواع سیاست‌های اداره سازمان فراهم می‌کند. همچنین، ساختار لازم برای پشتیبانی از درک راهبردی آن سیاست‌های خاص و دیگر ابزارها را فراهم و چرایی تعیین سیاست سازمان را در زمینه خاص، تعیین می‌کنند. برای مثال، این که چرا سازمان، سیاستی را در مورد موضوعی تعیین می‌کند، توضیح می‌دهد.

- **دستورالعمل‌ها (Guidelines):** دستورالعمل‌ها، راهنمایی‌هایی را برای بکارگیری استانداردهای حسابرسی سیستم‌های اطلاعاتی ارائه می‌دهند. حسابرس سیستم‌های اطلاعاتی باید این دستورالعمل‌ها را در تعیین چگونگی استقرار آنها و استفاده از قضاوت حرفه‌ای در بکارگیری آن‌ها در نظر بگیرد و بتواند هرگونه انحراف از آنها را توجیه کند. هدف دستورالعمل‌های حسابرسی سیستم‌های اطلاعاتی، فراهم آوردن اطلاعات بیشتر در مورد چگونگی رعایت استانداردهای حسابرسی سیستم‌های اطلاعاتی است.

فصل ۳

برآورد ریسک فناوری اطلاعات و حسابرسی با نگرش مدیریت ریسک

۱. استانداردهای برآورد ریسک فناوری اطلاعات و حسابرسی‌های با نگرش مدیریت ریسک

استانداردهای بین‌المللی دیوان‌های محاسبات بخش ۳۱۵، حسابرس را به کسب شناخت از سازمان درباره وجود فرآیندهایی برای موارد زیر ملزم می‌کند:

- شناسایی ریسک‌های تجاری مربوط به هدف‌های گزارشگری مالی؛
- برآورد اهمیت ریسک‌ها؛
- ارزیابی احتمال رخداد؛ و
- تصمیم‌گیری برای مدیریت این ریسک‌ها.

استانداردهای انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۳-۱-S۱۲۰۲ مقرر می‌کند که برای تهیه طرح کلی حسابرسی سیستم‌های اطلاعاتی و تعیین اولویت‌ها برای تخصیص مؤثر منابع در اجرای حسابرسی و اطمینان‌بخشی سیستم‌های اطلاعاتی باید از یک روش مناسب ارزیابی ریسک و روش‌های پشتیبان استفاده گردد. متخصصان حسابرسی و اطمینان‌بخشی سیستم‌های اطلاعاتی هنگام برنامه‌ریزی برای هر یک از کارهای حسابرسی باید نسبت به شناسایی و ارزیابی ریسک‌های مربوط به موضوع مورد بررسی، اقدام کنند و ریسک کسب وکار، ریسک حسابرسی و سایر ریسک‌هایی را مورد توجه قرار دهند که سازمان در معرض آن‌ها قرار دارد.

استانداردهای بین‌المللی دیوان‌های محاسبات بخش ۵۳۰۰، انجام حسابرسی‌های فناوری اطلاعات با رویکرد نگرش مدیریت ریسک را مقرر کرده است. رویکرد حسابرسی با نگرش مدیریت ریسک، شامل شناسایی عناصر ریسک در سازمان مورد رسیدگی همراه با شناسایی تأثیر بالقوه آن‌ها و درنتیجه شناسایی زمینه‌های دارای اولویت برای انجام حسابرسی است.

۲. اصول ریسک فناوری اطلاعات

چارچوب ریسک فناوری اطلاعات، مربوط به ریسک‌های فناوری اطلاعات است. اصول مبنای این چارچوب، ارتباط روشنی با کسب‌وکار دارد. برای مثال، راهبری و مدیریت مؤثر ریسک فناوری اطلاعات:

- همیشه با هدف‌های سازمان ارتباط دارد.
- در صورت همگرایی ریسک کسب‌وکار مربوط به فناوری اطلاعات با مدیریت ریسک کلی سازمان، مدیریت را تسهیل می‌کند.
- هزینه‌ها و منافع مدیریت ریسک را موازنه می‌کند.
- ارتباط منصفانه و روشن با ریسک فناوری اطلاعات را ارتقا می‌بخشد.
- با تعریف و الزام به مسئولیت‌پذیری شخصی برای عملکرد در سطحی پذیرفتنی و به‌خوبی تعریف شده، فضای مناسبی را از طرف سطوح ارشد سازمان ایجاد می‌کند.
- یک فرآیند مداوم و بخشی از فعالیت‌های روزانه است.

ریسک فناوری اطلاعات، اصول راهنمای متعددی را برای مدیریت مؤثر ریسک فناوری اطلاعات تعریف می‌کند که بر اصول پذیرفته شده مدیریت ریسک سازمان در زمینه فناوری اطلاعات مبتنی است. مدل فرایند ریسک فناوری اطلاعات به‌گونه‌ای طراحی و ساخته شده است که سازمان‌ها را قادر می‌سازد تا اصول را در عمل به‌کار گیرند و عملکرد خود را بسنجند.

۳. تعریف ریسک فناوری اطلاعات

ریسک، احتمال آن است که رویدادی با بهره گرفتن از آسیب‌پذیری‌های یک دارایی یا گروهی از دارایی‌ها به سازمان آسیب برساند.

ریسک فناوری اطلاعات یک ریسک تجاری است که به استفاده، مالکیت، عملیات، مشارکت، تأثیر و پذیرش فناوری اطلاعات در یک سازمان مربوط است. ریسک فناوری اطلاعات شامل آن‌دسته از رویدادهای مرتبط با فناوری اطلاعات است که می‌تواند به‌طور بالقوه، بر کسب‌وکار تأثیر بگذارد. ریسک فناوری اطلاعات شامل نااطمینانی از میزان تکرار و اندازه است که چالش‌هایی را در دستیابی به هدف‌های راهبردی و همچنین، نااطمینانی در پیگیری فرصت‌ها ایجاد می‌کند. ریسک‌های فناوری اطلاعات را می‌توان به روش‌های گوناگون زیر، طبقه‌بندی کرد:

- ریسک ارائه خدمات فناوری اطلاعات، مربوط به عملکرد و در دسترس بودن خدمات فناوری اطلاعات است، و می‌تواند تخریب یا کاهش ارزش را برای شرکت به دنبال داشته باشد.

- ریسک ارائه راه‌حل/ تحقق منافع فناوری اطلاعات، مربوط به سهم فناوری اطلاعات در راه‌حل‌های تجاری جدید یا بهبود یافته کسب‌وکار، معمولاً در قالب پروژه‌ها و برنامه‌ها، است.
- ریسک تحقق منافع فناوری اطلاعات، مربوط به فرصت‌هایی است برای استفاده از فناوری برای بهبود کارایی یا اثربخشی فرآیندهای تجاری یا استفاده از فناوری به‌عنوان توانمندساز نوآوری‌های جدید تجاری.
- ریسک فناوری اطلاعات همیشه وجود دارد، حتی اگر توسط سازمان کشف یا شناسایی نشده باشد، بازهم باید مدیریت شود.

۴. ریسک حسابرسی و اهمیت

ریسک حسابرسی را می‌توان احتمال این ریسک تعریف کرد که اطلاعات، ممکن است حاوی خطای با اهمیتی باشد که در طول حسابرسی کشف نشده باقی بماند. حسابرس سیستم اطلاعاتی باید به دیگر عوامل کاربردی مرتبط با سازمان، ازجمله داده‌های سازمان، محرمانگی، در دسترس بودن خدمات ارائه شده و همچنین، حُسن شهرت عمومی سازمان، نهادهای عمومی یا مؤسسات توجه نماید.

ریسک حسابرسی به شرح زیر طبقه‌بندی می‌شود:

- **ریسک ذاتی**- احتمال وجود اشتباهی است که می‌تواند همراه با سایر اشتباه‌های مشاهده شده حین حسابرسی، با اهمیت یا اساسی باشد با فرض اینکه هیچ‌گونه کنترل جایگزینی برای آن وجود ندارد. امکان وجود تحریف‌های با اهمیت، در صورت نبود کنترل‌های مربوط (ریسک ذاتی) است. ریسک ذاتی به‌دلیل ماهیت کسب‌وکار می‌تواند اتفاق بیفتد.
- **ریسک کنترل**- احتمال وجود یک خطای با اهمیت که به‌موقع توسط سیستم کنترل داخلی از رخداد آن پیشگیری یا شناسایی نشود. برای مثال، ریسک‌های کنترلی مرتبط با بررسی دستی تراکنش‌های رایانه‌ای، بالا است؛ زیرا، به دلیل حجم بالای معاملات وارد شده، فعالیت‌های مستلزم بررسی، اغلب به‌راحتی از قلم می‌افتند.
- **ریسک عدم کشف**- اینکه حسابرس سیستم‌های اطلاعاتی از آزمون‌های ناکافی استفاده کند و علیرغم وجود اشتباه‌های با اهمیت، نتیجه بگیرد که اشتباه‌های با اهمیتی وجود ندارد.
- **ریسک کلی حسابرسی**- مجموع ریسک‌های جداگانه‌ی ارزیابی‌شده برای هر هدف کنترلی. هدف از تدوین رویه حسابرسی، محدود کردن ریسک حسابرسی زمینه مورد رسیدگی است به‌گونه‌ای که پس از تکمیل فرآیند حسابرسی، ریسک حسابرسی در سطح پایین قرار گیرد.

بین ریسک و اهمیت، رابطه معکوس وجود دارد. هرچه آستانه اهمیت پایین‌تر باشد، انتظارات از حسابرسی، دقیق‌تر و ریسک حسابرسی، بیشتر می‌شود. بنابراین، برای به‌دست آوردن اطمینان بیشتر در مواردی که ریسک حسابرسی بالاست یا آستانه اهمیت پایین است، حسابرس سیستم‌های اطلاعاتی باید برای جبران (کاهش) این ریسک، نسبت به افزایش حدود و ماهیت آزمون‌های حسابرسی (افزایش آزمون کنترل‌ها) یا افزایش و بسط آزمون‌های محتوا اقدام نماید.

۵. مدیریت ریسک سازمان

از نظر انجمن حسابرسان سیستم‌های اطلاعاتی، مدیریت ریسک عبارت است از: فرآیند شناسایی آسیب‌پذیری‌ها و تهدیدهای مربوط به منابع اطلاعاتی مورد استفاده یک سازمان برای دستیابی به هدف‌های تجاری و تصمیم‌گیری در مورد اقدامات متقابل احتمالی برای کاهش ریسک تا سطحی پذیرفتنی، متناسب با ارزش منابع اطلاعاتی برای سازمان.

برای ایجاد درک درستی از ریسک حسابرسی، حسابرس سیستم‌های اطلاعاتی باید از چگونگی مدیریت ریسک توسط سازمان مورد رسیدگی، شناخت کسب کند.

برآورد ریسک باید هم‌راستا با معیارهای پذیرش ریسک و هدف‌های مرتبط با سازمان، ریسک‌ها را شناسایی، کمّی و اولویت‌بندی کند. نتایج باید اقدامات مدیریتی مناسب، اولویت‌های مدیریت ریسک، امنیت اطلاعات و اولویت‌های پیاده‌سازی کنترل‌ها را برای مقابله با ریسک مشخص کند.

برآورد ریسک باید به صورت دوره‌ای انجام شود تا تغییرات در محیط، در الزامات امنیتی و شرایط ریسک را درباره دارایی‌ها، تهدیدها، آسیب‌پذیری‌ها و آثار آن، مورد پوشش قرار دهد.

در مورد ریسک‌هایی که تصمیم سازمان، مقابله با آن‌ها از طریق اعمال کنترل‌ها است، کنترل‌ها باید به‌گونه‌ای انتخاب شوند که از کاهش آن ریسک به سطحی پذیرفتنی، اطمینان بدست آید.

۶. برآورد ریسک توسط حسابرس

برآورد ریسک، فرآیندی است برای شناسایی و ارزیابی ریسک‌ها و آثار بالقوه آن‌ها؛ شامل بررسی منظم موارد زیر:

- آسیب‌های تجاری که ممکن است از وجود نقصی در امنیت ناشی شود، همراه با در نظر گرفتن پیامدهای بالقوه از دست رفتن محرمانگی، یکپارچگی و در دسترس بودن دارایی‌های اطلاعاتی.
- احتمال واقعی رخداد چنین نقصی در پرتو تهدیدهای غالب، آسیب‌پذیری‌ها و کنترل‌های فعلی در حال اجرا.

استاندارد شماره ۱۲۰۲ انجمن حسابرسان سیستم‌های اطلاعاتی، برآورد ریسک در دو سطح را هنگام برنامه‌ریزی حسابرسی سیستم‌های اطلاعاتی الزامی می‌دارد:

(۱) برآورد ریسک برای تدوین یک طرح کلی حسابرسی سیستم‌های اطلاعاتی و تعیین اولویت‌ها برای تخصیص مؤثر منابع حسابرسی سیستم‌های اطلاعاتی.

(۲) برآورد ریسک جداگانه هر کار حسابرسی.

۳-۶-۱. برآورد ریسک برای تدوین طرح کلی حسابرسی سیستم‌های اطلاعاتی

برای آسانی تدوین طرح کلی حسابرسی سیستم‌های اطلاعاتی، برآورد مناسب ریسک باید دستِ‌کم هرسال یک‌بار انجام و مستندسازی شود. حسابرسان سیستم‌های اطلاعاتی هنگام تدوین طرح باید عناصر زیر را در نظر بگیرند:

الف) پوشش کامل همه زمینه‌ها در دامنه حسابرسی سیستم‌های اطلاعاتی، که حدود همه فعالیت‌های ممکن حسابرسی را نشان می‌دهد.

ب) قابلیت اتکا و مناسب بودن برآورد ریسک ارائه شده توسط مدیریت.

پ) فرآیندهای اتخاذ شده توسط مدیریت برای نظارت، آزمون و گزارش ریسک‌های محتمل یا مشکلات.

ت) پوشش ریسک‌های مرتبط با فعالیت‌های مورد رسیدگی.

دامنه حسابرسی سیستم‌های اطلاعاتی اغلب دیوان‌های محاسبات، از تعداد زیادی سیستم‌های اطلاعاتی تشکیل شده است که نمی‌توانند به‌طور جامع، در چرخه‌ای یک ساله مورد حسابرسی قرار گیرند. این امر ممکن است ناشی از محدود بودن منابع باشد. حتی در صورت کافی بودن منابع، ممکن است حسابرسی سالانه برخی از سیستم‌های اطلاعاتی، توجیه‌پذیر نباشد. افزون‌بر این، برخی از برنامه‌ها ممکن است برنامه‌های حساس کاربردی باشند که وقفه در آن‌ها، عواقب بسیار گسترده‌ای پدید می‌آورد (برای مثال، سیستم اطلاعاتی یکپارچه مدیریت مالی[1]) و ممکن است به توجه بیشتری نیاز داشته باشند. بنابراین، مدیریت حسابرسی سیستم‌های اطلاعاتی باید از یک روش برآورد ریسک استفاده کند که به اولویت بندی و برنامه ریزی کار حسابرسی سیستم‌های اطلاعاتی و اطمینان‌بخشی کمک کند. برای کاهش ذهنیت‌گرایی در تعیین ماهیت، زمان‌بندی،

1. Integrated Financial Management and Information System (IFMIS)

و حـدود حسابرسی سیستـم‌های اطلاعاتی و منابـع اختصـاص یافتـه برای انجـام کار حسابرسـی، عوامل ریسک زیر (که کاربردشان ضروری است) باید در نظر گرفته شود:

۱) انواع سیستم‌ها (خریداری شده به صورت آماده یا تدوین درون سازمانی).

۲) موارد ارتباط سیستم با عملیات حیاتی کسب‌وکار.

۳) تعداد کاربران سیستم‌ها.

۴) تعداد رابط‌های سیستم[1].

۵) نحوه اتصال به شبکه (شبکه داخلی، شبکه خارجی یا شبکه مبتنی بر وب/ دامنه عمومی).

۶) تعداد سال‌های استفاده از (عملیاتی شدن) سیستم.

۷) حجم داده‌ها در سیستم.

۸) روش پیاده‌سازی سیستم[2].

۹) بودجه یا وجوه پردازش شده در سیستم.

۱۰) منافع ذینفعان[3].

۱۱) حسابرسی سال پیش.

وزن اختصاص داده شده به این عوامل، تأثیر و احتمال رخداد آن‌ها ممکن است بـرای یـک دیـوان محاسبات نسبت به دیوان محاسبات دیگر متفاوت باشد. این برآورد ریسک سیستم‌هـای اطلاعـاتی می‌تواند با برآورد ریسک کلی انجام شده برای همه سازمان‌های مورد حسابرسی، ادغام شود.

۲-۶. برآورد ریسک هر کار حسابرسی

برآورد ریسک یک کار حسابرسی، با کسب شناخت کامل گروه حسابرسـی از فعالیـت‌هـای لازم در دامنه حسابرسی، آغاز می‌شود. در طول برآورد ریسک، افـراد حرفـه‌ای بایـد مـوارد زیـر را در نظـر بگیرند:

- نتایج کار حسابرسی قبلی، بررسی‌ها و یافته‌ها، شامل هرگونه اقدامات اصلاحی،
- فرایند اساسی برآورد ریسک سازمان،
- احتمال رخداد یک ریسک خاص، و
- تأثیر یک ریسک خاص در صورت رخداد (در قالب پول یا سایر معیارهای ارزش).

1. Interface to the System
2. System Implementation Method
3. Stakeholders Interest

افزون بر این، حسابرس سیستم‌های اطلاعاتی باید اعمال غیرقانونی احتمالی را در نظر بگیرد که می‌توانند تغییر در ماهیت، زمان‌بندی یا میزان اجرای رویه‌های موجود را ضروری سازند.

هدف از برآورد ریسک کار حسابرسی، کاهش ریسک حسابرسی به یک سطح پذیرفتنی است. ریسک حسابرسی، یعنی احتمال آنکه حسابرس، نادانسته نظر خود را درباره صورت‌های مالی حاوی تحریف‌های با اهمیت، به‌طور مناسبی تعدیل نکند. ریسک حسابرسی تحت تأثیر ریسک‌های زیر است:

- ریسک ذاتی
- ریسک کنترل
- ریسک عدم کشف

۱-۲-۶. ریسک ذاتی

احتمال رخ دادن یک تحریف با اهمیت در یک حساب و با فرض این که برای آن، کنترل داخلی وجود نداشته باشد. ریسک ذاتی، مستقل از حسابرسی وجود دارد و می‌تواند به دلیل ماهیت کسب وکار رخ دهد. برای مثال، تمام دارایی‌های اطلاعاتی برخط در معرض ریسک هک شدن (نفوذ) هستند. فارغ از فناوری کنترل‌های بازدارنده‌ی مورد استفاده برای کاهش احتمال رخداد ریسک، این ریسک همیشه وجود خواهد داشت.

ریسک ذاتی در بیشتر زمینه‌های حسابرسی سیستم‌های اطلاعاتی بالا است؛ زیرا، آثار بالقوه اشتباه‌ها به صورت معمول، در اغلب کسب‌وکارها و برای بسیاری از کاربران به وجود می‌آید.

۲-۲-۶. ریسک کنترل

کنترل‌ها برای کاهش احتمال رخداد تهدیدی طراحی شده است که با بهره‌گیری از آسیب‌پذیری‌ها، خسارت‌هایی را تحمیل می‌کند. ریسک کنترل، عبارت است از احتمال رخ دادن یک تحریف با اهمیت در یک حساب و کشف نشدن به‌موقع آن توسط سیستم کنترل داخلی. برای مثال، ریسک کنترل مرتبط با بررسی دستی تراکنش‌های رایانه‌ای به دلیل حجم زیاد اطلاعات وارد شده، می‌تواند بالا باشد.

افراد حرفه‌ای باید ریسک کنترل را بالا ارزیابی کنند مگر در شرایطی که کنترل‌های داخلی مربوط:

- شناسایی شده باشد؛
- به‌عنوان کنترل‌هایی مؤثر، ارزیابی شده باشد؛ و
- آزمون شده و عملکرد مناسب آن‌ها مورد تأیید باشد.

گروه حسابرسی ممکن است برای شناسایی یک ریسک فراگیر و اطمینان از برخورد مناسب با آن، نشستی برگزار کند.

ریسک‌های فراگیر، ریسک‌هایی هستند که به همه محیط سیستم‌های اطلاعاتی مربوط می‌شوند و در نتیجه، بر همه اجزای سیستم اطلاعاتی تأثیر می‌گذارند. برای مثال، ارزیابی نشدن ریسک توسط مدیریت، زیرپا گذاری کنترل‌ها توسط مدیریت، نداشتن صلاحیت عمومی مدیریت، درستکار نبودن مدیریت یا قابل اتکا نبودن سوابق سازمان. ریسک‌های فراگیر بر قابلیت اتکای کنترل‌های کاربردی و کنترل‌های تفصیلی سیستم‌های اطلاعاتی تأثیر می‌گذارد، در نتیجه ریسک این که کنترل‌های طراحی شده در سطح یک گزاره غیر مؤثر باشند، بالا است.

حسابرس سیستم‌های اطلاعاتی باید از آزمون شناخت سیستم[1] استفاده کند تا قابلیت اتکای سیستم کنترل داخلی سازمان مورد حسابرسی را تعیین کند. هدف اصلی، پاسخ دادن به این پرسش است که آیا کنترل‌های داخلی برای برخورد با ریسک، پیاده‌سازی شده‌اند؟ به بیان دیگر، آیا باید از آزمون کنترل‌ها[2] استفاده شود یا رویکرد آزمون محتوا[3] به‌طور کامل استفاده گردد.

- **آزمون کنترل‌ها باید زمانی انجام شود که:**
  - کنترل‌های داخلی، مؤثر و قابل اتکا هستند.
  - آزمون‌های محتوا به‌تنهایی نمی‌توانند شواهد حسابرسی کافی و مناسب را فراهم آورند. برای مثال، هنگامی که تعداد معاملات بسیار زیاد است.

- **آزمون‌های محتوا باید زمانی انجام شود که:**
  - کنترل‌های داخلی برقرار نشده باشد یا مؤثر نیستند.
  - حجم معاملات مورد حسابرسی، به نسبت کم است. آزمون کنترل‌ها در این مورد، کارایی ندارد.

1. System Walk-Through Test
2. Test of Controls
3. Substantive Testing

▣ **آزمون رعایت کنترل‌ها**

- ❖ آزمون رعایت کنترل‌ها[1]، عبارت است از گردآوری شواهد برای آزمون رعایت شدن (یا نشدن) رویه‌های کنترلی یک سازمان.
- ❖ هدف کلی آزمون رعایت، فراهم آوردن اطمینان معقول برای حسابرسان سیستم‌های اطلاعاتی است که کنترل‌های خاصی که قصد دارند بر آن‌ها اتکا کنند، به همان‌گونه‌ای عمل می‌کنند که در ارزیابی مقدماتی، از آن‌ها شناخت کسب کرده‌اند.
- ❖ حسابرس سیستم‌های اطلاعاتی پس از آزمون کنترل‌ها ممکن است نتیجه بگیرد که اتکا بر کنترل‌ها مناسب نیست، که در این صورت باید قابلیت اتکای کنترل‌ها را پایین برآورد نماید. این امر، اجرای آزمون‌های محتوای بیشتری را الزامی می‌سازد.

۳-۲-۶. آزمون محتوا

آزمون محتوا، یکپارچگی پردازش واقعی را اثبات می‌کند. آزمون محتوا عبارت است از گردآوری شواهد حسابرسی درباره کامل بودن، درستی یا وجود فعالیت‌ها یا معاملات در دوره مورد حسابرسی.

افراد حرفه‌ای باید در تعیین میزان آزمون‌های محتوای مورد نیاز، موارد زیر را در نظر بگیرند:

- ❖ برآورد ریسک ذاتی.
- ❖ نتیجه‌گیری درباره ریسک کنترل پس از آزمون رعایت کنترل‌ها.

هرچه برآورد ریسک‌های ذاتی و کنترل بیشتر باشد، حسابرسان باید شواهد حسابرسی بیشتری را از طریق اجرای آزمون‌های محتوا گردآوری کنند.

۷. حسابرسی با نگرش مدیریت ریسک

کنترل‌های ویژه برخورد با ریسک‌های خاص حسابرسی، در حسابرسی با نگرش مدیریت ریسک، شناسایی و آزمون می‌شوند. این فرآیند به‌طور معمول با شناسایی آنچه که می‌تواند به خطا منجر شود یا بیانیه ریسک‌هایی که می‌تواند مانع دستیابی به هدف‌های حسابرسی مورد نظر شوند، آغاز می‌شود و در ادامه، به فهرست کردن هدف‌های کنترلی و سرانجام تهیه یک برنامه کاری برای آزمون کنترل‌هایی می‌پردازد که با این ریسک‌ها، برخورد می‌کنند.

1. Compliance Test of Controls

اســاس رویکرد نگرش مدیریت ریسک در حسابرسی فناوری اطلاعات همانند سایر انواع حسابرسی اســت و به‌طور معمول، مستلزم انجام موارد زیر توسط حسابرسان است:

- **گردآوری اطلاعات و برنامه‌ریزی:**
  - شناخت کسب و کار و صنعت.
  - نتایج حسابرسی سال پیش.
  - آخرین اطلاعات مالی (صورت‌های مالی).
  - سیستم‌های اطلاعاتی و پروژه‌های در دست اجرا.
  - وضعیت نظارتی.
  - برآورد ریسک ذاتی.

- **شناخت ریسک‌های فناوری اطلاعات و کنترل‌های داخلی:**
  - محیط کنترلی فناوری اطلاعات.
  - رویه‌های کنترلی.
  - برآورد ریسک عدم کشف.
  - برآورد ریسک.
  - رتبه‌بندی و طبقه‌بندی ریسک‌ها.

- **اجرای آزمون‌های رعایت:**
  - شناسایی کنترل‌هایی که باید آزمون شوند.
  - انجام آزمون‌هایی در مورد قابلیت اتکا، پیشگیری از ریسک، میزان رعایت و سیاست‌هــا و رویه‌های سازمانی.

- **انجام آزمون‌های محتوا:**
  - بررسی‌های تحلیلی.
  - آزمون جزئیات مانده حساب‌ها.
  - سایر روش‌های آزمون محتوا.

- **نتیجه‌گیری در حسابرسی:**
  - تهیه و تدوین پیشنهادها.
  - نوشتن گزارش حسابرس.

از دیدگاه کارگروه حسابرسی فناوری اطلاعات[1]، موارد زیر گام‌های رویکرد نگرش مدیریت ریسک برای حسابرسی فناوری اطلاعات است:

۱) شناسایی دامنه حسابرسی شامل فهرستی از همه سازمان‌های قابل حسابرسی یا واحدهای زیرِ پوشش یک حوزه دیوان محاسبات.

۲) تهیه فهرست سیستم‌های اطلاعاتی مورد استفاده در سازمان/ واحدهای قابل حسابرسی.

۳) شناسایی عوامل مؤثر بر لزوم وجود سیستم در سازمان برای آن که بتواند وظایف خود را انجام و خدمات را ارائه دهد.

۴) تخصیص وزن به عوامل مهم. این می‌تواند با مشورت سازمان مورد حسابرسی انجام شود.

۵) گردآوری اطلاعات برای کلیه سیستم‌ها در همه سازمان‌ها و اولویت‌بندی انجام حسابرسی سیستم‌ها/ سازمان‌ها بر اساس امتیازات تجمیعی.

۶) تهیه برنامه حسابرسی سالانه که اولویت‌ها، رویکرد و برنامه حسابرسی‌های فناوری اطلاعات را روشن کند. این امر می‌تواند با تناوب سالانه انجام شود و بنابر این، می‌تواند برنامه‌ای تکرار شونده باشد.

۸. چرا حسابرسی با نگرش مدیریت ریسک؟

رویکرد حسابرسی با نگرش مدیریت ریسک، حسابرس را در تصمیم‌گیری برای انجام آزمون رعایت یا آزمون محتوا یاری می‌کند. این رویکرد در تعیین ماهیت و میزان آزمون‌هایی که باید در جریان حسابرسی انجام شود، به حسابرس کمک می‌کند.

۹. مستندسازی برآورد ریسک

حسابرس هنگام تعیین دامنه حسابرسی باید ریسک‌ها را ارزیابی و زمینه‌های با ریسک بالایی را مشخص کند که باید مورد حسابرسی قرار گیرند. روش‌های فراوانی برای ارزیابی ریسک وجود دارد؛ از طبقه‌بندی ساده ریسک‌ها به ترتیب بالا، متوسط و پایین برمبنای قضاوت حسابرس سیستم‌های اطلاعاتی گرفته تا محاسبات علمی برای رتبه‌بندی عددی ریسک‌ها. مثال زیر نشان می‌دهد که چگونه حسابرس می‌تواند ریسک را با استفاده از فهرست ریسک‌ها ارزیابی کند.

صورت‌ریز ریسک‌ها، مجموعه‌ای از ویژگی‌های اصلی مشکلات بالقوه و شناخته‌شده فناوری اطلاعات است. این ویژگی‌ها، نام، توضیحات، مالک، میزان تکرار احتمالی/ واقعی، بزرگی احتمالی/ واقعی، تأثیر احتمالی/ واقعی بر کسب و کار و وضع ریسک‌ها را در بر می‌گیرد.

1. Working Group on IT Audit (WGITA)

حسابرس پس از شناسایی و برآورد ریسک باید آن را ارزیابی کند. حسابرس در طول فرآیند شناسایی ریسک، به شناسایی دارایی‌ها، تهدیدها، کنترل‌های موجود، آسیب‌پذیری‌ها و پیامدها می‌پردازد. فرایند برآورد ریسک به شرح زیر است:

- برآورد پیامدها،
- برآورد احتمال رخداد، و
- برآورد کمی/ کیفی ریسک.

صورت ریز ریسک‌ها می‌تواند ساده یا پیچیده باشد اما در بیشتر موارد، شامل موضوع‌های زیر می‌شود:

بیانیه ریسک[1]

تشریح شرایط فعلی که ممکن است به زیان منجر شود و توضیحی در مورد آن زیان (منبع: انجمن مهندسی نرم‌افزار[2]). برای شناخت ریسک باید ریسک را به‌روشنی بیان نمود. چنین بیانیه‌ای باید شرایط فعلی که ممکن است به زیان منجر شود و شرحی از آن زیان را شامل شود. نمونه‌ای از بیانیه ریسک به شرح زیر است:

از آنجا که تغییرات اضطراری، مستندسازی یا تأیید نشده اند، این ریسک وجود دارد که تغییرات غیرمجاز می‌تواند در محیط تولید سیستم ایجاد شود.

احتمال

احتمال رخداد یک رویداد. احتمال رخداد را می‌توان زیاد، متوسط یا پایین طبقه‌بندی کرد.

رتبه‌بندی تأثیر

رتبه‌بندی[3] ریسک به‌صورت بالا، متوسط یا پایین برمبنای برآورد اثر ریسک بر یک زمینه خاص.

کنترل‌های جبرانی

کنترل‌های جبرانی[4] شامل اقداماتی است برای کاهش تکرار رخداد یا تأثیر یک ریسک.

ریسک باقی‌مانده

ریسک باقی‌مانده[5] پس از برخورد مدیریت با ریسک‌ها. هنگامی‌که کنترل‌های جبرانی کافی برقرار باشد، حسب شرایط، ریسک باقیمانده می‌تواند متوسط یا پایین برآورد شود.

1. Risk Statement
2. Software Engineering Institute (SEI)
3. Impact Rating
4. Mitigating Controls
5. Residual Risk

تمرکز حسابرسی در رویکرد نگرش مدیریت ریسک، بر پوشش زمینه‌های با ریسک بالاتر است. نمونه‌ای از صورت‌ریز ریسک به شرح زیر است:

ریسک	احتمال رخداد	اثر	کنترل‌های جبرانی	ریسک باقیمانده
کنترل‌های دسترسی منطقی[1] ریسک ایجاد تغییرات غیرمجاز به دلیل ضعف کنترل‌های دسترسی	**متوسط**	**بالا**	**رضایت‌بخش**	**پایین**

۱۰. خلاصه

مضمون اصلی استانداردهای حسابرسی با نگرش مدیریت ریسک، برنامه‌ریزی مکرر است. یکی از عناصر اصلی حسابرسی‌های با نگرش مدیریت ریسک، دستاورد برآورد ریسک فناوری اطلاعات قابل ارائه است که توسط گروه حسابرسی هنگام تعیین رویه‌های حسابرسی اضافی لازم برای کاهش ریسک حسابرسی به سطحی پذیرفتنی، در نظر گرفته می‌شود. استانداردهای حسابرسی با نگرش مدیریت ریسک، به‌روشنی بر برنامه ریزی مستمر با نگرش به اطلاعات جدید بدست آمده در طول حسابرسی تأکید می‌کند. فعالیت‌های مرحله برآورد ریسک و گزارش آن، ایستا هستند. برآورد ریسک فناوری اطلاعات می‌تواند کنترل‌هایی را شناسایی کند که در صورت تشخیص مؤثر بودن عملکرد آن‌ها از طریق آزمون، می‌توانند ریسک حسابرسی را برای یک یا چند گزاره و همچنین، در سطح صورت‌های مالی کاهش دهند. در طول این مرحله، گزارش برآورد ریسک حسابرس فناوری اطلاعات باید یک عنصر اصلی در برنامه‌ریزی حسابرسی باشد. هدف، تعیین مورد نیاز بودن یا نبودن روش‌های حسابرسی بیشتر، با نگرش به فناوری اطلاعات و ریسک‌های تحریف با اهمیت است.

اصطلاحاتی که در فصل ۳ بر آن تأکید شده است:

- **حسابرسی با نگرش مدیریت ریسک (Risk Based Auditing)**: در حسابرسی با نگرش مدیریت ریسک، کنترل‌هایی که با ریسک‌های خاص حسابرسی برخورد می‌کنند، شناسایی و آزمون می‌شوند. این فرآیند به‌طور معمول، با شناسایی آنچه که می‌تواند به اشتباه منجر شود یا بیانیه ریسک‌هایی که می‌توانند مانع دستیابی به هدف‌های حسابرسی مورد نظر شوند، آغاز می‌شود و به فهرست کردن هدف‌های کنترلی و سرانجام، تهیه یک برنامه کاری برای آزمون کنترل‌های مقابله‌کننده با این ریسک‌ها، ادامه می‌یابد.

1. Logical Access Control

- **ریسک حسابرسی (Audit Risk)**: احتمال آنکه حسابرس، نادانسته نظر خود را درباره صورت‌های مالی حاوی تحریف‌های با اهمیت، به طور مناسبی تعدیل نکند. حسابرس سیستم‌های اطلاعاتی باید به دیگر عوامل کاربردی مرتبط با سازمان از جمله داده‌های سازمان، محرمانگی، در دسترس بودن خدمات ارائه شده و همچنین، حسن شهرت سازمان، نهادهای عمومی یا مؤسسات توجه نماید.
- **ریسک فناوری اطلاعات (IT Risk)**: ریسک، یک تهدید بالقوه خاص است که با بهره گرفتن از آسیب‌پذیری‌های یک دارایی یا گروهی از دارایی‌ها، به سازمان آسیب می‌رساند.
- **مدیریت ریسک سازمان (Entity's Risk Management)**: از نظر انجمن حسابرسان سیستم‌های اطلاعاتی، مدیریت ریسک عبارت است از: فرآیند شناسایی آسیب‌پذیری‌ها و تهدیدهای مربوط به منابع اطلاعاتی مورد استفاده یک سازمان برای دستیابی به هدف‌های تجاری و تصمیم‌گیری در مورد اقدامات متقابل احتمالی برای کاهش ریسک تا سطحی پذیرفتنی، متناسب با ارزش منابع اطلاعاتی برای سازمان.

فصل ۴

شناخت کنترل‌های فناوری اطلاعات

۱. کنترل‌ها چه هستند؟

حسابرس فناوری اطلاعات باید کنترل‌های فناوری اطلاعات که جزئی جدایی‌ناپذیر از محیط کنترلی فناوری اطلاعات سازمان است را ارزیابی و نظارت کند. حسابرسان باید با ارائه مشاوره در مورد طراحی، پیاده‌سازی، اجرا و بهبود کنترل‌های فناوری اطلاعات، به مدیریت کمک کنند.

کنترل‌ها، همه روش‌ها، سیاست‌ها و رویه‌هایی هستند که از حفاظت دارایی‌های سازمان، درستی و قابلیت اطمینان اسناد و مدارک آن و پایبندی عملیاتی به استانداردهای مدیریت، اطمینان می‌دهند.

حسابرس باید بین کنترل‌های عمومی[1] و کنترل‌های کاربردی[2] تمایز قایل شود. کنترل‌های عمومی، محیطی را ایجاد می‌کنند که در آن، سیستم‌های فناوری اطلاعات در قالب تعداد اندکی رویه‌های کنترلی، تدوین، اجرا، مدیریت و نگهداری می‌شوند. نمونه‌هایی از کنترل‌های عمومی، تدوین و پیاده‌سازی راهبرد سیستم اطلاعاتی و سیاست امنیتی سیستم اطلاعاتی، سازماندهی کارکنان سیستم اطلاعاتی برای تفکیک وظایف متضاد و برنامه‌ریزی برای پیشگیری و بازیابی حوادث را شامل می‌شود.

کنترل‌های کاربردی، کنترل‌هایی خاص و منحصر به یک برنامه رایانه‌ای است. این کنترل‌ها در مورد بخش‌های برنامه به کار می‌رود و به تراکنش‌ها و داده‌های ایستا[3] (کم تغییر) مربوط می‌شوند. برنامه‌های کاربردی شامل اعتبارسنجی داده‌های ورودی، رمزگذاری داده‌های انتقالی و غیره است. برای مثال، در یک برنامه پرداخت برخط، یک شرط داده ورودی می‌تواند این باشد که تاریخ انقضای کارت اعتباری باید پس از تاریخ تراکنش باشد و جزئیات وارد شده باید رمزگذاری شوند.

---

1. General Controls
2. Application Controls
3. Standing Data

برنامه‌های کاربردی[1]، نرم‌افزارهای خاصی هستند که می‌تواند رویه‌های دستی و رایانه‌ای برای پیدایش تراکنش[2]، پردازش داده‌ها، نگهداری پیشینه و تهیه گزارش را شامل باشد. یک برنامه کاربردی را می‌توان به بخش‌های ورودی داده‌ها (پیدایش و ورود داده‌ها)؛ ارتباطات داده‌ها؛ پردازش؛ ذخیره داده‌ها (شامل داده‌های اصلی) ؛ خروجی و توزیع نتایج تقسیم کرد.

سیستم‌های بی‌درنگ[3] برنامه‌هایی کاربردی هستند که پردازش و به‌روزرسانی بانک‌های اطلاعاتی در آنها بی‌درنگ با ورود داده‌ها اتفاق می‌افتد. برای مثال، کاربران می‌توانند تراکنش‌ها را در یک مرکز کاری[4] وارد و تأثیر فوری آن را روی حساب مشاهده کنند؛ یعنی، هر زمان که کاربر یک تراکنش را وارد می‌کند، حساب‌ها به‌روز می‌شوند. سیستم‌های بی‌درنگ به کاربران این امکان را می‌دهند تا به‌موقع بودن[5] اطلاعات مدیریت را بهبود بخشند. با این حال، این سیستم‌ها شامل کنترل‌های سنتی مانند جمع دسته‌ها[6] نیستند.

مجاز بودن[7] اقدامی است که نخست، تراکنش پیشنهادی را با برنامه‌ها، شرایط، محدودیت‌ها یا دانش عمومی در مورد اینکه دارایی چیست، مقایسه می‌کند و سپس، درباره معتبر و مطابق بودن آن با هدف‌های مدیریت، تصمیم می‌گیرد.

اعتبارسنجی[8] اقدامی است که درستی یا مربوط بودن یک مبلغ یا واقعیت را از طریق اجرای دوباره، سندرسی، دریافت تأییدیه یا تطبیق اثبات می‌کند. رویه‌ها یا روش‌های تعبیه شده در برنامه‌های رایانه‌ای، می‌توانند داده‌ها را به‌محض وارد کردن، اعتبارسنجی کنند.

۲. کنترل‌های عمومی و کنترل‌های کاربردی

کنترل‌های عمومی، پایه و اساس ساختار کنترل فناوری اطلاعات است؛ این کنترل‌ها از قابلیت اتکای داده‌های تولید شده توسط سیستم‌های فناوری اطلاعات اطمینان می‌دهد، از این گزاره حمایت می‌کند که سیستم‌ها به همان شکل مورد نظر (برنامه‌ریزی شده) عمل می‌کنند و خروجی‌ها قابل اطمینان هستند. سازمان آفریقایی دیوان‌های محاسبات انگلیسی زبان (AFROSAI-E)، یک چک‌لیست کنترل‌های عمومی تهیه کرده است که زمینه‌های زیر را دربر می‌گیرد:

- ❖ راهبری فناوری اطلاعات.
- ❖ مدیریت امنیت (ایمنی).

1. Applications
2. Transaction Origination
3. Real-Time Systems
4. Work Station
5. Timeliness
6. Batch Totals
7. Authorisation
8. Validation

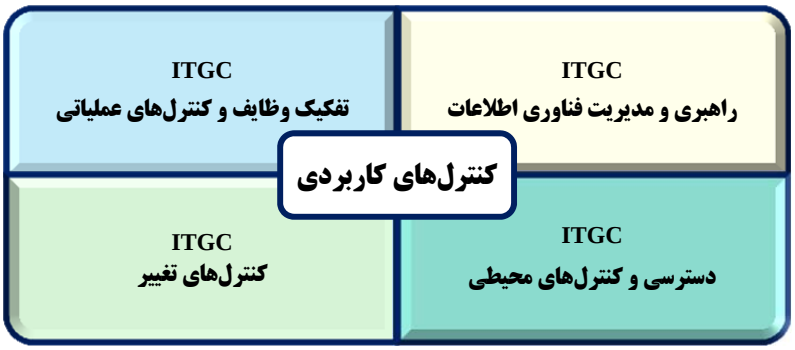
- مدیریت تغییر برنامه‌ی کنترل دسترسی فیزیکی.
- کنترل‌های محیطی.
- تداوم خدمات فناوری اطلاعات.
- کنترل‌های دسترسی منطقی.

کنترل‌های کاربردی، کنترل‌های کاملاً خودکار هستند که برای اطمینان از کامل و دقیق بودن پردازش داده‌ها از ورود تا خروج، طراحی شده‌اند. کنترل‌های کاربردی شامل موارد زیر است:

- کنترل‌های کامل بودن.
- کنترل‌های اعتبار.
- شناسایی.
- احراز هویت.
- مجاز بودن.
- کنترل‌های ورودی.
- کنترل‌های خروجی.

۳. ارتباط کنترل‌های عمومی فناوری اطلاعات و کنترل‌های کاربردی

کنترل‌های فناوری اطلاعات به دو دسته کنترل‌های عمومی و کنترل‌های کاربردی تقسیم می‌شوند. دسته‌بندی‌ها به گستره اثر کنترل‌ها و میزان ارتباط آن‌ها با هرنوع برنامه‌ی خاص، بستگی دارد.

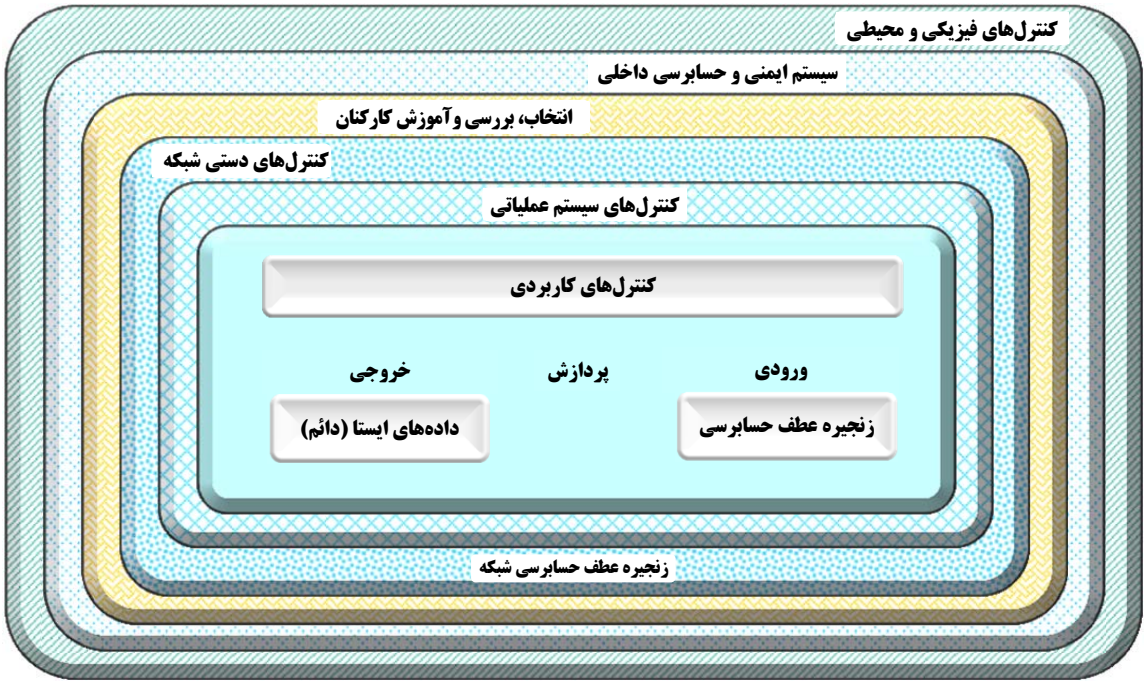


کنترل‌های عمومی فناوری اطلاعات (ITGC) شامل راهبری فناوری اطلاعات، تفکیک وظایف، قوانین دسترسی و رویه‌های تغییر، مرز برونی چارچوبی را برای کنترل کلی فعالیت‌های فناوری اطلاعات ایجاد می‌کنند. این کنترل‌ها، پی‌ریزی لازم را برای افزودن هر نوع کنترل کاربردی خاص فراهم می‌آورد.

در سطح هر کنترل کاربردی خاص، کنترل‌های اجازه و اعتبارسنجی پیدایش تراکنش (کنترل‌های ورودی)، اطمینان از پردازش دقیق و کامل (کنترل پردازش) و تولید خروجی‌های معتبر (کنترل‌های خروجی) وجود دارد که با هم، کنترل‌های کاربردی را تشکیل می‌دهند. این روش‌ها در سیستم‌های مالی، کنترل‌هایی خاص در برنامه‌های حسابداری هستند و از اینکه همه معاملات، مجاز و ثبت شده‌اند، به‌طور کامل، دقیق و به‌موقع پردازش می‌شوند، اطمینان می‌دهند. کنترل‌های کاربردی می‌تواند شامل رویه‌های دستی که توسط کاربران اجرا می‌شوند (کنترل‌های کاربر) و رویه‌های خودکاری باشد که توسط نرم‌افزار رایانه‌ای انجام می‌شوند.

طراحی و پیاده‌سازی کنترل‌های عمومی فناوری اطلاعات می‌تواند اثر چشم‌گیری در اثربخشی کنترل‌های کاربردی داشته باشد. کنترل‌های عمومی، به گونه‌ای، منابع مورد نیاز برنامه‌های کاربردی را فراهم می‌کند و از نبود امکان ایجاد تغییرات غیرمجاز در برنامه‌ها (یعنی پیشگیری از برنامه‌ریزی دوباره) یا بانک‌های اطلاعاتی اصلی (مجموعه بزرگ داده‌های تراکنش‌ها) اطمینان می‌دهد. در همین حال، کنترل‌های کاربردی بر روی تک‌تک تراکنش‌ها اعمال می‌شود و از درستی ورود، پردازش و خروج داده‌ها اطمینان ایجاد می‌کند.

چارچوب کنترل‌های فناوری اطلاعات



می‌توانیم به لایه‌های کنترل به صورت هم مرکز (شبیه یک پیاز) فکر کنیم که در آن، راه خود را از وسط پیاز با صورت‌های مالی شروع می‌کنیم و از طریق لایه‌های کنترل پی در پی، راه را ادامه می‌دهیم. این لایه‌ها در کنار هم باید ریسک اینکه صورت‌های مالی به دلیل ریسک کنترل فناوری اطلاعات، حاوی اشتباه‌های با اهمیت باشد را کاهش دهد.

۴. کنترل‌های عمومی فناوری اطلاعات

کنترل‌های عمومی پایه و اساس ساختار کنترل فناوری اطلاعات می‌باشند. این کنترل‌ها بر محیط کلی تدوین و عملکرد، مدیریت و سیستم‌های فناوری اطلاعات متمرکز است. کنترل‌های عمومی فناوری اطلاعات، چارچوبی را برای کنترل کلی فعالیت‌های فناوری اطلاعات ایجاد می‌کند و درباره دستیابی به هدف‌های کلی کنترلی تا حدودی اطمینان می‌دهند. همچنین، کنترل‌های عمومی شامل کنترل‌های فراگیر هستند. این‌گونه کنترل‌ها برای مدیریت و نظارت بر محیط فناوری اطلاعات طراحی شده‌اند و بنابراین، بر همه فعالیت‌های مرتبط با فناوری اطلاعات اثر می‌گذارند.

کنترل‌های عمومی فناوری اطلاعات به زیرساخت‌های فناوری اطلاعات سازمان مورد رسیدگی مربوط است، از جمله هرگونه سیاست، رویه و روش کار مربوط به فناوری اطلاعات. روش‌های کنترلی معمولاً تفکیک وظایف، استفاده از دارایی‌های فناوری اطلاعات، تحصیل و نگهداری برنامه‌های کاربردی فناوری اطلاعات، کنترل‌های دسترسی و عملیات مرکز داده را راهبری می‌کند.

کنترل‌های عمومی، به جریان‌های جداگانه‌ای از تراکنش‌ها یا بسته‌های خاص حسابداری یا برنامه‌های خاص کاربردی مالی اختصاص ندارند.

نقش اصلی حسابرس، اطمینان دادن نسبت به کنترل‌های داخلی برقرار در سازمان مورد رسیدگی است. چنانچه سازمان مورد رسیدگی در محیط فناوری اطلاعات فعالیت داشته باشد، حسابرس باید طراحی، پیاده‌سازی و انطباق با چارچوب کنترل فناوری اطلاعات را ارزیابی کند. هر زمینه کنترلی، بر مجموعه‌ای از هدف‌های کنترلی برای کاهش ریسک کنترل مبتنی است و حسابرس باید کافی بودن یا نبودن کنترل‌های استقرار یافته را برای تحقق هدف‌ها، ارزیابی کند. حسابرس در مورد کنترل‌های عمومی باید گروه‌های عمده و میزان کنترل‌های عمومی استقراریافته را شناسایی کند، توجه مدیریت و آگاهی کارکنان سازمان را در این باره ارزیابی کند و میزان مؤثر (کارآمد) بودن این کنترل‌ها را برای مقاصد اطمینان‌بخشی ارزیابی کند. اگر کنترل‌های عمومی ضعیف باشند، از قابلیت اطمینان کنترل‌های مرتبط با هر برنامه کاربردی فناوری اطلاعات، به‌طور جدی کاسته خواهد شد.

۴-۱. طبقه‌های اصلی کنترل‌های عمومی

طبقه‌های اصلی کنترل‌های عمومی در شکل زیر نشان داده شده است:

۱-۱-۴. راهبری و مدیریت فناوری اطلاعات

راهبری و مدیریت فناوری اطلاعات[1]، یک بخش جدایی‌ناپذیر از مدیریت سازمان است و شامل رهبری و ساختارها و فرآیندهای سازمانی است که از حفظ هدف‌ها و راهبردهای کسب و کار توسط سیستم فناوری اطلاعات اطمینان می‌دهد. کنترل‌های عمومی در کل، جریانی از بالا به پایین[2] است که با راهبری و مدیریت فناوری اطلاعات هدایت می‌شود. این جریان، محیط کنترلی را به وجود می‌آورد و زیربنای شیوه‌های کنترل داخلی درست و مناسب و گزارش‌دهی در سطوح عملیاتی را برای نظارت و بازنگری‌های مدیریت بنیاد می‌کند.

کنترل‌های سطح بالاتر که از طریق سیاست‌های تعریف شده مدیریت برقرار می‌شوند، جوّ رأس سازمان[3] را مورد توجه قرار می‌دهند. حسابرسان برای تعیین اینکه آیا تصمیمات، مسیرهای هدایتی، منابع، مدیریت و نظارت فناوری اطلاعات، پشتیبان راهبردها و هدف‌های سازمان است باید مؤلفه‌های مختلف ساختار راهبری فناوری اطلاعات را شناسایی و ارزیابی کنند.

حسابرس برای انجام برآورد باید اجزای اصلی راهبری و مدیریت فناوری اطلاعات را بداند. حسابرس باید از ریسک‌های ناشی از کافی نبودن هر یک از مؤلفه‌ها در سازمان مورد رسیدگی، آگاه باشد.

دو مؤلفه نخست، یعنی ساختار سازمانی و راهبرد فناوری اطلاعات، به ساختار راهبری مربوط هستند و زیربنایی را برای طراحی و همگرایی راهبرد فناوری اطلاعات و فرآیندها با هدف‌های کسب و کار فراهم می‌کنند.

1. Governance and Management of IT
2. A Top Down Flow
3. Tone at the Top

هدف‌های کنترلی[1]- برای اطمینان یافتن این که در برنامه‌ریزی، پیاده‌سازی و نگهداری از زیرساخت‌های فناوری اطلاعات، سطوح مدیریت ارشد به‌گونه‌ای مشارکت دارند که فناوری اطلاعات، شناخت مناسب، توجه یا منابعی را که برای دستیابی به هدف‌های کسب و کار نیاز دارد، دریافت می‌نماید.

ریسک کنترلی- در صورت مشارکت نکردن مناسب مدیریت ارشد در تدوین راهبرد فناوری اطلاعات، تخصیص منابع از طریق رویه‌های کمیته راهبری ساختار یافته[2]، یک ریسک ذاتی به وجود می‌آید که عملکرد فناوری اطلاعات، نتواند نیازهای کسب و کار را برآورده کند. این امر می‌تواند سیستم‌های مالی را با مشکل ناتوانی در رفع نیازهای گزارشگری جدید مواجه سازد (که ممکن است به دلیل تغییری در استانداردهای حسابداری ملی یا در الزامات دولتی رخ دهد).

ساختارهای گزارشگری ضعیف، با سرانجام تصمیم‌گیری ناکافی، می‌تواند توانایی سازمان را برای ارائه خدمات و تداوم فعالیت در آینده، تحت تأثیر قرار دهد (یکی از اصول اساسی حسابداری).

برنامه‌ریزی نامناسب یا بدون برنامه بودن فناوری اطلاعات، به محدود شدن رشد کسب و کار به دلیل کمبود منابع فناوری اطلاعات منجر می‌شود.

رویه‌های منابع انسانی

میزان پشتیبانی سیستم‌های اطلاعاتی از هدف‌های تجاری سازمان، به منابع انسانی که سبب کار کردن سیستم می‌شوند، بستگی دارد.

هدف کنترلی- اطمینان یافتن از اینکه سازمان، رویه‌های استخدامی و آموزش مناسبی برقرار کرده است که از ریسک اشتباه‌ها، از قلم افتادگی‌ها و دیگر موارد تخطی کارکنان، می‌کاهد.

این امر با استقرار موارد زیر حاصل می‌شود:

- نمودارهای سازمانی[3] که شرح شغل[4] همه کارکنان از جمله کارکنان فناوری اطلاعات را به‌روشنی تعیین می‌کند. این نمودارها باید خطوط گزارشگری و مدیریت را به‌روشنی ترسیم کنند. نمودارها، به همه کارکنان این امکان را می‌دهد که بدانند در کجای آن جای دارند

1. Control Objectives
2. Structured Steering Committee
3. Organisational Charts
4. Jobs Role

و هنگام بروز مشکلات باید به چه کسی اطلاع بدهند. رویه‌های برنامه‌ریزی نیروی انسانی به‌گونه‌ای ایجاد شده‌اند که از وجود تعداد کافی کارکنان ماهر برای اجرای برنامه‌ها/ ماژول‌های مختلف در سیستم‌های فعلی و همچنین، برآورده کردن نیازهای استخدامی آتی، اطمینان دهد.

- رویه‌های جذب کارکنان به صورت دائمی، موقت، پیمانکاران و مشاوران. این رویه‌ها شامل بررسی پیشینه، تفاهم‌نامه حفظ محرمانگی و رفتار حرفه‌ای است. کارکنان جدید باید از نقش و مسئولیت‌های خود در رابطه با مسأله‌های امنیتی آگاه شوند.
- رویه‌های آموزش مبتنی بر نقش‌های تعیین شده و تغییرهای اتفاقی/ برنامه‌ریزی شده در زیرساخت‌های فناوری اطلاعات. آموزش فناوری اطلاعات، اغلب پرهزینه است و باید با برنامه‌های آموزشی و بودجه، کنترل شود.
- شرایط قرارداد شامل رفتار حرفه‌ای، چرخش شغلی، کنترل‌های ویژه و رویه‌های مرخصی. در مواردی که واحد فناوری اطلاعات از متخصصان، پیمانکاران و مشاوران برای انجام کارهایی که تنها یک‌بار انجام می‌شود[1]، دعوت به کار می‌کند، قراردادهای ویژه‌ای بسته می‌شود. رویه‌هایی باید وجود داشته باشد که افراد این قراردادهای ویژه نیز به سیاست‌ها و رویه‌های تعیین شده، پایبند باشند.
- رویه‌های ارزیابی کارکنان[2] برای تشویق، ترفیع، تنزل رتبه[3] مبتنی بر معیارهای قابل اندازه‌گیری از پیش تعریف شده. روش‌های ارزیابی باید منصفانه و عادلانه و برای همه کارکنان، قابل درک باشد.
- رویه‌های پایان همکاری[4] که مراحلی را برای مواردی تعریف می‌کند که دیگر به خدمات کارمند نیاز نیست. این موارد باید خاتمه داوطلبانه/ غیر داوطلبانه/ خاتمه فوری و معیارهای امنیتی را شامل شود.
- اطلاع‌رسانی به سایر کارکنان: روال‌های پرداخت نهایی را به‌گونه‌ای ترتیب می‌دهد که از حذف وی از لیست حقوق و دستمزد، برگشت اموال سازمان مانند رایانه‌های شخصی، لپ‌تاپ، دستگاه پیجر و غیره اطمینان حاصل شود.

1. Once off Jobs
2. Staff Assessment Policies
3. Demotions
4. Termination Policies

ریسک کنترلی- در صورت نبود یک سیاست و رویه منابع انسانی به‌خوبی طراحی شده، ممکن است موارد مکرر از بین رفتن داده‌ها، تکرار زیاد خطا در داده‌ها، داده‌ها و اصلاحات غیرمجاز برنامه، عدم امکان دسترسی به سیستم و عدم تداوم کسب و کار ناشی از خطا و حذف‌هایی به‌دلیل درک ناقص از شرح شغل، تقلب، نقص سخت‌افزار/ نرم‌افزار و فرسایش بالای کارکنان ایجاد شود.

مستندسازی و رویه‌های نگهداری مستندات

مستندسازی سیستم‌های اطلاعاتی، برنامه‌های کاربردی، وظایف شغلی، سیستم‌های گزارشگری و تناوب آن، نقطه عطفی است برای همگرا کردن عملیات فناوری اطلاعات با هدف‌های سازمانی.

رویه‌های مناسب نگهداری مستندات، ردیابی و مدیریت تغییرات مکرر در ساختار اطلاعات سازمان را امکان‌پذیر می‌سازد.

هدف کنترلی- مستندسازی مناسب ساختار اطلاعاتی و وظایف شغلی با این هدف انجام می‌شود که از پیروی از شیوه‌های استاندارد شده کار مربوط به هر وظیفه شغلی، مدیریت بدون اختلال در فرآیندهای کسب و کار، رخدادها/ نگهداری و تغییرات مکرر در ساختار اطلاعاتی، اطمینان به‌دست آید.

سازمان باید برای مستندسازی سیستم‌ها، فرآیندها و وظایف شغلی، سیاستی را برگزیند که بر به‌روز رسانی کنترل، نسخه نشر، پشتیبان‌گیری و نگهداری تأکید داشته باشد. سازمان‌های دارای گواهینامه‌های کیفیت، ممکن است رویه‌هایی در زمینه ایجاد، تأیید و صدور اسناد و همچنین، رویه‌هایی برای کنترل تغییرات در مستندات موجود، داشته باشند.

افزون بر الزام به نگهداری مستندات که زنجیره عطف حسابرسی[1] را برای اطمینان‌بخشی مستقل درباره کنترل‌های داخلی و گزارشگری مالی فراهم می‌کند، ممکن است الزامات دیگری غیر از حسابرسی نیز وجود داشته باشد که سازمان را ملزم به حفظ مستندات معامله می‌کند؛ برای مثال، مقررات گمرکی، قوانین مالیاتی و الزامات مقرراتی ثبت شرکت‌ها.

ریسک کنترلی- ریسک‌های مرتبط با رویه‌های مستندسازی ناکافی، انجام اقدامات غیرمجاز توسط کارکنان فناوری اطلاعات، افزایش تعداد اشتباه‌های ایجاد شده توسط کارکنان عملیاتی و صرف زمان بیشتر برای برطرف کردن اختلالات را شامل می‌شود. برای مثال، اگر شبکه سازمان به‌اندازه کافی مستندسازی نشده باشد و مشکلی در سیم‌کشی شبکه ایجاد شود، افراد مسئول انجام تعمیرات، ممکن است در پیدا کردن محل رخداد خرابی با دشواری رو به‌رو شوند.

1. Audit Trail

رویه برون سپاری

برون سپاری[1] فناوری اطلاعات این امکان را به مدیریت سازمان می‌دهد که تلاش خود را بر فعالیت‌های اصلی کسب وکار متمرکز کند. دلیل برون سپاری ممکن است از نیاز به کاهش هزینه‌های جاری ناشی شود.

هدف کنترلی- چنانچه سازمان فعالیت‌های فناوری اطلاعات خود را برون سپاری کند یا قصد داشته باشد آن را برون سپاری کند باید از همگرایی این فعالیت‌ها با هدف‌های کسب وکار، حفاظت از امنیت، محرمانگی و در دسترس بودن داده‌ها و همچنین، پدید نیامدن هرگونه اختلالی در فرآیندهای تجاری، اطمینان حاصل کند.

این هدف با گنجاندن قابلیت دسترسی، یکپارچگی، محرمانگی و امنیت داده‌های سازمان به همراه مالکیت انحصاری سازمان بر داده‌ها در قرارداد برون سپاری، برآورده می‌شود. هنگامی که سازمان از یک مدل برون‌سپاری استفاده می‌کند که در آن، مسئولیت برخی عملیات تجاری به شریک برون‌سپاری واگذار شده است، مسئولیت نهایی برای اثربخشی امور برون سپاری شده، استقرار و اجرای کنترل‌ها و فرایندهای درون سازمانی مناسب، همچنان بر عهده مدیریت باقی می‌ماند.

ریسک کنترلی- در صورت نبود سیاست‌ها و رویه‌های مناسب برای برون سپاری، سازمان با ریسک در دسترس نبودن داده‌های عملیاتی/ مالی، نا امنی داده‌ها و نبود یکپارچگی داده‌ها، نقض محرمانگی، اختلال در تداوم کسب و کار و از بین رفتن سرقفلی رو به‌رو می‌شود.

حسابرسی داخلی

مسئولیت نهایی اطمینان یافتن از کفایت سیستم کنترل داخلی بر عهده مدیریت است.

هدف کنترلی- مدیریت باید هرچند گاه یک‌بار (به‌صورت دوره‌ای) از این اطمینان یابد که کنترل‌های گوناگون مربوط به فرآیندهای کسب وکار در محیط فناوری اطلاعات، استقرار یافته است؛ در سطوح عملیاتی مربوط رعایت می‌شود؛ و برای پوشش ناهمگرایی عملیات فناوری اطلاعات با هدف‌های تجاری کافی است.

مدیریت بدین منظور، سیاست‌ها و روش‌هایی را برقرار و برای اطمینان یافتن از کفایت آن‌ها، بر رسیدگی‌های حسابرسان داخلی، اتکا می‌کند.

حسابرس مستقل می‌تواند عملکرد حسابرسی داخلی سازمان را به عنوان بخشی از ساختار کلی کنترلی بررسی کند (چون که آن‌ها از بروز نقاط ضعف کنترل‌ها و اشتباه‌ها پیشگیری، یا آنها را کشف و اصلاح می‌کنند). حسابرس مستقل می‌تواند با انجام یک ارزیابی (از کار حسابرسان داخلی) نسبت به اتکا کردن یا نکردن بر کار حسابرسان داخلی، تصمیم‌گیری کند.

1. Outsourcing Policy

ریسک کنترلی- در صورت ناکافی بودن خدمات حسابرسی داخلی، مدیریت ممکن است نتواند اطلاعات دوره‌ای به‌موقع و قابل اتکا را درباره کفایت چارچوب کنترلی مستقر در سازمان و میزان رعایت آن، به‌دست آورد.

سیاست امنیت فناوری اطلاعات

برای حفاظت از دارایی‌های اطلاعاتی که موقعیت سازمان را به‌روشنی بیان می‌کنند، استقرار سیاستی برای امنیت فناوری اطلاعات توسط سازمان از اهمیت زیادی برخوردار است.

هدف کنترلی- مدیریت ارشد سازمان باید یک چارچوب امنیت تعریف کند تا کنترل‌های دسترسی فیزیکی و منطقی[1] دقیقی را برای گروه‌های مختلف دارایی‌های اطلاعاتی، به‌صورتی یکنواخت برقرار سازد.

سیاست‌های امنیتی فناوری اطلاعات معمولاً به صورت شرح نوشته‌ای مختصر، یعنی در چند صفحه، بیان می‌شوند. این سیاست برای اعتبار داشتن، به تأیید مدیریت ارشد نیاز دارد و سرانجام باید توسط هیأت مدیره یا معادل آن تصویب شود. این خط مشی باید در دسترس همه کارکنان مسئول امنیت اطلاعات باشد. در مواردی که سازمان دارای کارکنان عملیاتی با دسترسی به سیستم‌های فناوری اطلاعات می‌باشد، این سیاست باید اجزای زیر را تعیین کند:

اجزای یک سیاست امنیت فناوری اطلاعات
❖ **تعریف امنیت اطلاعات (هدف‌ها و دامنه، شامل رعایت محرمانگی داده‌ها).**
❖ **الزامات اصول امنیتی، استانداردها و رعایت/ انطباق.**
❖ **کارکنان بخش فناوری اطلاعات نباید مسئولیت‌های عملیاتی یا حسابداری داشته باشند.**
❖ **تعریف مسئولیت‌های عمومی و خاص برای همه جنبه‌های امنیت اطلاعات.**
❖ **استفاده از دارایی‌های اطلاعاتی و دسترسی به ایمیل، اینترنت.**
❖ **نحوه و رویه‌های دسترسی به فرآیندهای پشتیبان‌گیری.**
❖ **رویه‌های برخورد با بدافزارها/ برنامه‌های مخرب[2].**
❖ **آموزش و پرورش عناصر امنیت.**
❖ **فرآیند گزارشگری وقایع امنیتی مشکوک در برنامه‌های تداوم کسب و کار.**
❖ **روش‌های آگاهی‌رسانی خط‌مشی و رویه‌های مصوب امنیت سیستم‌های اطلاعاتی به کارکنان.**

1. Physical and Logical Access Controls
2. Malicious Software / Programs

مسئولیت امنیت فناوری اطلاعات معمولاً بر عهده واحد/ مدیریت امنیت قرار می‌گیرد. در مورد سازمان‌های کوچکتر، این وظیفه ممکن است به صورت پاره‌وقت باشد که توسط یکی از کارکنان به نام مأمور امنیت فناوری اطلاعات [1] انجام شود. انتظار می‌رود سازمان‌های بزرگتر، کارکنان اختصاصی برای امنیت فناوری اطلاعات داشته باشند.

انطباق قانونی و مقرراتی

الزامات قانونی و مقرراتی می‌تواند شامل موارد زیر باشد:

- ❖ قانون حفاظت از داده‌ها و حریم خصوصی برای محافظت از اطلاعات شخصی افراد،
- ❖ قانون سوء استفاده از رایانه که نفوذ و دسترسی غیرمجاز به رایانه را به‌عنوان یک جرم جنایی [2] جرم انگاری می‌کند،
- ❖ مقررات بانکی و مالی، جایی که بانک‌ها برای ادامه فعالیت باید بررسی‌های دوره‌ای را بپذیرند، و
- ❖ قوانین کپی‌رایت برای پیشگیری از سرقت نرم‌افزارهای رایانه‌ای.

سازمان باید از مقررات قانونی محل(های) فعالیت خود آگاه باشد و اقدامات لازم را برای اطمینان از انطباق با آن‌ها، انجام دهد.

ریسک کنترلی- رعایت نکردن (کنترل‌ها) ممکن است به اقدامات متفاوتی از دریافت یک اخطار [3] تا پیگرد قانونی [4] یا حتی تعطیلی کسب و کار بیانجامد.

۲-۱-۴. تفکیک وظایف و کنترل‌های عملیاتی

سازمان باید شرح شغل‌ها را به‌گونه‌ای تعریف کند که تفکیک وظایف [5] و مسئولیت‌ها را برای سطوح/ وظایف مختلف کارکنان به‌روشنی مشخص کند.

هدف کنترلی- زیربنای تفکیک وظایف این است که هیچ کارمند یا گروهی از کارکنان نباید در موقعیتی باشند که بتوانند در روال عادی انجام وظایف خود، اشتباه یا تقلب‌هایی مرتکب شوند و آن را پنهان دارند. تفکیک وظایف، یک روش اثبات شده برای اطمینان یافتن از این است که تراکنش‌ها به‌گونه مناسبی مجاز و ثبت شده‌اند و از دارایی‌ها محافظت می‌شود. تفکیک وظایف زمانی تحقق پیدا می‌کند که یک فرد، فعالیت‌های فرد دیگر را بررسی می‌کند.

1. IT Security Officer
2. Criminal Offence
3. Warning letter
4. Prosecution
5. Segregation of Duties (SoD)

۴-۱-۳. کنترل دسترسی

کنترل دسترسی[1] یک تکنیک امنیتی است برای تعیین اینکه چه کسی یا چه چیزی مجاز به مشاهده یا استفاده از منابع موجود در یک محیط رایانه‌ای است. این کنترل دوگونه‌ی عمده دارد: کنترل‌های دسترسی فیزیکی و کنترل‌های دسترسی منطقی. کنترل دسترسی فیزیکی، دسترسی به ساختمان یا ساختمان‌ها، اتاق‌ها یا سیستم فناوری اطلاعات مبتنی بر رایانه را محدود می‌کند. دسترسی منطقی، اتصال به شبکه‌های رایانه‌ای، پرونده‌های سیستم و داده ها را محدود می‌کند.

کنترل دسترسی در یک محیط دولتی اهمیت زیادی دارد؛ زیرا، بسیاری از سازمان‌های دولتی، داده‌های حساس[2] را پردازش می‌کنند و ملاحظات مربوط به حفظ محرمانگی، افرادی که باید بخش‌های مختلف اطلاعات را مشاهده کنند، محدود می‌سازد. کنترل دسترسی، از این که تنها کاربران مجاز، به داده‌های حساس دسترسی می‌یابند، اطمینان می‌دهد.

۴-۱-۴. کنترل‌های تغییر

کنترل تغییر، رویکردی منظم برای مدیریت همه تغییراتی است که در یک محصول یا سیستم رخ می‌دهد. هدف، اطمینان یافتن از این است که هیچ‌گونه تغییر غیرضروری ایجاد نمی‌شود، همه تغییرات مستندسازی می‌شود، ارائه خدمات به‌جز در مواقع ضروری، مختل نمی‌شود و از منابع، به‌صورت کارآمد استفاده می‌گردد.

۴-۲. اثر کنترل‌های فراگیر بر حسابرسی

حسابرس در طول حسابرسی خود باید اثر کنترل‌های فراگیر را نیز در نظر بگیرد. کنترل‌های فراگیر را می‌توان به‌عنوان آن دسته از کنترل‌هایی تعریف کرد که برای مدیریت و نظارت بر محیط سیستم‌های اطلاعاتی طراحی شده‌اند و بنابراین، بر همه زمینه‌های مرتبط به آن اثر می‌گذارند.

رهنمودهای حسابرسی انجمن حسابرسان سیستم‌های اطلاعاتی مقرر می‌دارد که حسابرسان باید از کنترل‌های حاکم بر عملیاتی که حسابرسی خواهند کرد، برآوردی اولیه به‌عمل آورند. این برآورد اولیه باید شناسایی و ارزیابی اثر کنترل‌های فراگیر را شامل باشد. حسابرس در طول برنامه‌ریزی حسابرسی باید همه کنترل‌های فراگیری را شناسایی کند که برای هدف‌های مختلف حسابرسی کاربرد دارد و همچنین، از وجود روش‌های کافی برای برخورد با همه کنترل‌های فراگیر، اطمینان یابد.

1. Access Control
2. Sensitive Data

اگر کنترل‌های فراگیر، تأثیر با اهمیتی بر هدف حسابرسی داشته باشند، برنامه حسابرسی حسابرسان نمی‌تواند تنها بر کنترل‌های تفصیلی متمرکز شود، بلکه باید کنترل‌های فراگیر را نیز مورد توجه قرار دهد. حسابرسان در مواردی که آزمون کنترل‌های فراگیر ناممکن (یا غیرعملی) باشد باید محدودیت در دامنه حسابرسی را گزارش دهند.

چنانچه حسابرس به این نتیجه برسد که کنترل‌های فراگیر، رضایت‌بخش هستند، می‌تواند میزان آزمون کنترل‌های تفصیلی را کاهش دهد؛ زیرا، کنترل‌های فراگیر قوی، همان اطمینانی را برای حسابرس به وجود می‌آورند که وی با آزمون کنترل‌های تفصیلی به‌دست می‌آورد. اما، در صورت رضایت‌بخش نبودن کنترل‌های فراگیر، حسابرسان برای کسب شواهد کافی درباره اثربخشی اجرای کنترل‌های تفصیلی باید تعداد آزمون کنترل‌های تفصیلی را افزایش دهند.

حسابرسان هنگام گزارش یافته‌های حسابرسی به مدیریت سازمان مورد رسیدگی باید نقاط ضعف یافت شده در کنترل‌های فراگیر را حتی اگر آن کنترل‌ها جزئی از دامنه اولیه حسابرسی نبوده باشند، نیز گزارش کنند.

در مواردی که کنترل‌های فراگیر نسبت به کنترل‌های تفصیلی از اهمیت برخوردار است؛ اما، کنترل‌های فراگیر توسط حسابرسان مورد آزمون قرار نگرفته است، حسابرسان باید این موضوع را همراه با بیان اثر بالقوه آن بر یافته‌های حسابرسی، نتیجه‌گیری‌ها و پیشنهادها، به اطلاع مدیریت برسانند.

برای مثال، اگر حسابرسان به حسابرسی تحصیل یا تدوین و توسعه یک بسته نرم‌افزاری جدید می‌پردازند و سند راهبردی فناوری اطلاعات [1] آن را پیدا نمی‌کنند باید نبود سند راهبردی فناوری اطلاعات یا ارائه نشدن آن را برای رسیدگی، به مدیریت گزارش کنند. اثر نبود راهبرد فناوری اطلاعات می‌تواند به این معنا باشد که سرمایه‌گذاری‌ها در زمینه فناوری اطلاعات با هدف‌های سازمان همراستا نیست. با وجود این باید توجه داشت که در موارد نبود راهبرد یا سیاست، حسابرس باید شیوه‌های مدیریت فناوری اطلاعات و ارتباطات و تخصیص منابع را برای ارزیابی مطابقت با هدف‌های کسب و کار، بررسی و مستند کند.

۳-۴. شناخت مستندات اصلی مفید برای تکمیل بررسی کنترل‌های عمومی رایانه‌ای

مستندات گوناگونی وجود دارد که حسابرس برای کسب شناخت از سازمان و محیط فناوری اطلاعات آن، می‌تواند از سازمان بخواهد.

1. IT Strategy Document

سند راهبردی فناوری اطلاعات- چگونگی یاری رساندن واحد فناوری اطلاعات به سازمان در دستیابی به هدف‌های خود و جزئی جدایی‌ناپذیر[1] بودن از راهبرد کسب و کار را توصیف می‌کند. سند راهبردی فناوری اطلاعات به رهبری (هدایت) بلندمدتی مربوط می‌شود که سازمان بخواهد از اهرم فناوری اطلاعات برای بهبود فرآیندهای کسب و کار استفاده کند.

بودجه فناوری اطلاعات- بودجه فعلی باید برای کنترل کفایت و رعایت اولویت‌های فعالیت فناوری اطلاعات بررسی شود.

ساختار راهبری فناوری اطلاعات[2]- شامل آخرین نمودار سازمانی و شرح شغل سِمَت‌های کلیدی فناوری اطلاعات است. سِمَت‌های کلیدی فناوری اطلاعات شامل موارد زیر است:

- مدیر سیستم[3].
- مدیر امنیت[4].
- مدیر بانک اطلاعاتی[5].
- تحلیلگر سیستم[6].
- برنامه نویسان کاربردی[7].
- برنامه نویسان سیستم[8].

برای ارزیابی عملکرد سیستم فناوری اطلاعات، حسابرس فناوری اطلاعات لازم است اطلاعات اولیه‌ای را بدست آورد. کاربرگ‌های مربوط به شناخت سازمان، دربرگیرنده بخشی از اطلاعات اولیه‌ای است که حسابرس فناوری اطلاعات می‌تواند به دست آورد.

۵. کنترل‌های کاربردی فناوری اطلاعات

کنترل‌های تعبیه شده در برنامه‌های فرآیند کسب و کار معمولاً به‌عنوان کنترل‌های کاربردی نامیده می‌شوند.

1. Integral Part
2. IT Governance Structure
3. System Administrator
4. Security Administrator
5. Database Administrator
6. Systems Analyst
7. Application Programmers
8. System Programmers

کنترل‌های کاربردی به کنترل‌های مربوط به پردازش معاملات و داده ها در یک سیستم کاربردی اشاره دارند و بنابراین، مختص همان برنامه هستند. در حالی‌که کنترل‌های عمومی فناوری اطلاعات سازمان، فضای حاکم بر محیط کنترلی کلی سیستم‌های اطلاعاتی را تنظیم می‌کنند، کنترل‌های کاربردی برای اطمینان و محافظت از کامل بودن، درستی، اعتبار، یکپارچگی، قابلیت اتکا و محرمانگی اطلاعات در برنامه‌های خاص برقرار می‌شوند. بنابراین، هدف کنترل‌های کاربردی به‌طور کلی شامل اطمینان یافتن از موارد زیر است:

- داده‌های تهیه شده برای سازمان/ داده‌های ورودی،کامل، معتبر و قابل اتکا هستند؛
- داده‌ها به شکلی خودکار تبدیل شده و با دقت، به طور کامل و به‌موقع وارد شده‌اند؛
- داده‌ها به طور کامل، به‌موقع و مطابق با الزامات تعیین‌شده توسط برنامه پردازش می‌شوند؛
- خروجی‌ها از تغییر غیر مجاز[1] یا آسیب، محافظت و طبق سیاست‌های تعیین‌شده، توزیع می‌شود.

۱-۵. کنترل‌های کاربردی شامل چه مواردی هستند

کنترل‌های کاربردی دربرگیرنده رویه‌های دستی همراه یک برنامه کاربردی هستند. این کنترل‌ها نه‌تنها در برنامه‌های خاص تعبیه می‌شوند، بلکه در فرایندهای تجاری همجوار نیز لحاظ می‌گردند. برای مثال، مسئول ورود داده‌ها ممکن است پیش از ورود داده‌ها به سیستم به یک فرم ورودی نیاز داشته باشد که امضا (تأیید) شده است. ترکیب کنترل‌های دستی و خودکار انتخاب شده، اغلب نتیجه‌ی ملاحظات مربوط به هزینه و کنترل، در مرحله طراحی برنامه کاربردی است.

۲-۵. اهمیت کنترل‌های کاربردی

کنترل‌های کاربردی برای اطمینان یافتن از محرمانگی، یکپارچگی و در دسترس بودن اطلاعات، نقش مهمی در محیط پردازش اطلاعات دارند. در یک سازمان که محیط کنترل‌های عمومی آن به‌گونه معقولی تنظیم شده باشد، حسابرس باید از درستی آغاز، مجاز بودن، پردازش و ثبت معاملات اطمینان یابد. از آنجا که کنترل‌های کاربردی با هریک از معاملات ارتباط نزدیکی دارد، به‌سادگی می‌توان درک کرد که چرا آزمون این کنترل‌ها، درباره درستی مانده یک حساب خاص به حسابرس اطمینان می‌دهد. حسابرس ممکن است لازم بداند که به‌درستی کامل شدن یا نشدن فعالیت‌های دستی لازم برای تکمیل و پشتیبانی از فعالیت‌های خودکار را ارزیابی کند.

برای مثال، آزمون کنترل‌های برنامه حقوق و دستمزد، در مورد مبلغ حقوق و دستمزد در صورت‌های مالی سازمان اطمینان فراهم می‌کند. بدیهی است که آزمون کنترل‌های عمومی

1. Unauthorised Modification

فناوری اطلاعات سازمان (برای مثال روش‌های کنترل تغییر) سطح اطمینان مشابهی را برای همان مانده حساب فراهم نمی‌کند.

۴-۵. هدف‌های کنترل‌های کاربردی

کنترل‌های کاربردی برای اطمینان دادن از دستیابی به هدف‌های تجاری مدیریت در ارتباط با یک برنامه معین هستند. این کار، با اطمینان از تهیه و ورود داده‌ها به صورت مجاز، کامل، معتبر و قابل اتکا انجام می‌شود؛ یکپارچگی داده‌ها در طول پردازش حفظ می‌گردد؛ خروجی‌ها در برابر تغییر غیرمجاز محافظت می‌شود و توزیع آن طبق سیاست‌های مقرر انجام می‌گیرد.

۴-۵. طبقه‌بندی برنامه کاربردی

راهکارهای اجرایی خودکار[1]، معمولاً به یکی از شکل‌های زیر هستند:

- **سیستم‌های اطلاعاتی مدیریت**[2]- این راهکارها برای خودکارسازی گردآوری و پردازش اطلاعات مربوط به اجرا و جنبه‌های مالی فعالیت‌های اصلی سازمان طراحی شده‌اند، اما به گردآوری و پردازش اطلاعات مربوط به فرآیندهای سازمان، منابع و مشتریان نیز مربوط می‌شوند. نمونه‌های معمول عبارتند از: سیستم‌های یکپارچه برنامه‌ریزی منابع سازمانی (ERP)[3] که گردآوری و پردازش اطلاعات مالی، انباره داده‌ها یا سیستم‌های اطلاعاتی اجرایی (EIS) مشابه و سیستم‌های مورد استفاده در پشتیبانی از تصمیم‌گیری‌های تجاری (DSS)[4] را خودکار می‌سازد.
- **سیستم خودکارسازی فرآیند**- این راهکار برای خودکارسازی فعالیت‌های مشخص یک فرایند، طراحی شده است. نمونه‌ای از سیستم خودکار فرایند، یک سیستم روباتیک است که در صنعت خودروسازی مورد استفاده قرار می‌گیرد.

درک طبقه‌بندی برنامه از نظر رویه‌های پردازش از این جهت برای حسابرسان اهمیت دارد که بتوانند کنترل‌های کاربردی خاص هر طبقه را شناسایی و ارزیابی کنند. دو طبقه اصلی شامل سیستم‌های پردازش دسته‌ای[5] و سیستم‌های بی‌درنگ هستند. اولی معمولاً به سیستم‌های مالی قدیمی مربوط است. معاملات معمولاً توسط کاربران به یک بخش مرکزی فناوری اطلاعات یا بخش ورود داده‌های مالی منتقل می‌شوند، در آنجا معاملات دسته‌بندی و به صورت دسته‌ای وارد رایانه می‌شوند. در سیستم‌های بی‌درنگ، کاربران می‌توانند تراکنش‌ها را در یک مرکز کاری وارد و تأثیر فوری آن را

1. Automated Solutions Implemented
2. Management Information Systems
3. Enterprise Resource Planning (ERP)
4. Decision Support Systems
5. Batch Data Entry Systems

روی حساب مشاهده کنند، یعنی هر زمان که کاربر یک تراکنش را وارد می‌کند، حساب‌ها به‌روز می‌شوند. سیستم‌های بی‌درنگ به کاربران این امکان را می‌دهند تا فوراً اشتباه‌ها را اصلاح کنند و به‌موقع بودن اطلاعات مدیریت را بهبود بخشند. با این حال، این سیستم‌ها شامل کنترل‌های سنتی مانند جمع دسته نیستند.

۵-۵. انواع کنترل‌های کاربردی

کنترل‌های کاربردی امنیتی	❖ **کنترل دسترسی منطقی (اختصاص سطوح دسترسی ویژه گوناگون و منوها به هریک از کاربران).** ❖ **مدیریت پیشینه فعالیت‌های خودکار و زنجیره عطف حسابرسی.**
کنترل‌های ورودی	❖ **ورود داده/ اعتبارسنجی فیلد[1] (مانند اعتبارسنجی شماره کارت اعتباری وارد شده).** ❖ **مقررات گردش کار (مانند ردیابی و امضای درخواست خرید).** ❖ **ورودی‌های فیلد، تکمیل شده بر اساس مقادیر از پیش تعریف‌شده (مانند فهرست قیمت‌ها).**
کنترل‌های پردازش	❖ **مقررات تجاری مدیریت محاسبات خودکار و زنجیره عطف حسابرسی.**
کنترل‌های خروجی	❖ **مغایرت‌گیری، بررسی و پیگیری گزارش‌های استثنای تولید شده توسط برنامه.**
کنترل‌های پرونده‌های اصلی و داده‌های ایستا (ثابت)	❖ **مراحل توسعه (SoDs)[2] اعمال شده در برنامه‌های کاربردی.**

1. Field فیلد ناحیه‌ای است در یک مکان ثابت یا شناخته شده در یک واحد داده مانند رکورد، سرصفحه پیام یا دستورالعمل رایانه که دارای هدف و معمولاً اندازه ثابت است. یک فیلد را می‌توان به فیلدهای کوچک‌تر تقسیم کرد. در اینجا چند نمونه آورده شده است:

   ۱) در یک جدول بانک اطلاعاتی، یک فیلد یک ساختار داده برای یک تکه از داده است. فیلدها در رکوردهایی سازماندهی می‌شوند که شامل تمام اطلاعات موجود در جدول مربوط به یک موجودیت خاص است. برای مثال، در جدولی به نام اطلاعات تماس سازمان، شماره تلفن احتمالاً فیلدی در یک ستون است و فیلدهای دیگری مانند نشانی، شامل خیابان و شهر نیز وجود دارند. رکوردها ردیف‌های جدول و فیلدها ستون‌ها را تشکیل می‌دهند (م).

   ۲) در فرمی که در یک وب سایت تکمیل می‌کنید، هر کادری که از شما اطلاعات می‌خواهد یک فیلد ورودی متن است (برگرفته از سایت https://searchoracle.techtarget.com/)- (م).

2. Stage of Development (SOD)

۱-۵-۵. کنترل‌های ورود داده

صرف‌نظر از اینکه سیستم مالی، دستی یا مبتنی بر رایانه باشد، بهترین تضمین برای اعتبار ورودی داده‌ها، وجود نوعی از مجوز است.

هدف‌های کنترلی

اعتباربخشی و تأیید اقدامات تهیه داده‌های منبع، مجوز و ورود داده‌ها به‌گونه‌ای که داده‌های دقیق، قابل اتکا و کامل توسط برنامه کاربردی به صورت به‌موقع پذیرفته شود، از جمله هدف‌های کنترل‌های ورود داده‌هاست.

بخش قابل توجهی از این اقدامات در مرحله تدوین و توسعه[1] یک برنامه کاربردی، در طول مراحل مختلف تدوین و توسعه سیستم پس از تعیین قوانین کسب و کار بر اساس تعریف الزامات، طراحی می‌شوند. در حالی که ورود داده‌ها می‌تواند دستی، یا توسط رابط کاربری سیستم انجام شود، از طریق طراحی خوب فرم ورود داده‌ها، کافی بودن تفکیک وظایف مربوط به پیدایش/ ایجاد و تأیید اسناد ورود داده‌ها و کنترل اصالت[2]، درستی و کامل بودن آن‌ها، می‌توان اشتباه‌ها و از قلم افتادگی‌ها را به حداقل رساند (با گزینه‌های منو یا پیام تعاملی).

اجزای کنترل‌های ورودی

مجوز ورود	**رویه دستی/ مجوز سطح نظارت بر داده‌ها در فرم ورود داده‌ها. برای مثال: تأیید جزئیات مدرک ورود داده به‌منظور پردازش در برنامه‌های گمرک.**
کامل بودن داده‌های ورودی	**بررسی کامل بودن برای اطمینان از اینکه پیش از نقل تراکنش به حساب‌ها، همه اطلاعات کلیدی تراکنش وارد شده است. برای مثال: در برنامه صدور بلیت برخط، تاریخ سفر/ نوع بلیت/ نام مسافر/ شماره شناسایی مسافر، فیلدهایی کلیدی هستند که بدون آن‌ها، تراکنش توسط سیستم پذیرفته نخواهد شد.**
اعتبارسنجی داده‌های ورودی[3]	**کنترل‌های اعتبارسنجی خودکار بر داده‌های ورودی سیستم. برای مثال، قرار گرفتن داده‌های سفر، خارج از دوره اعتبار بلیت.**
بررسی اقلام تکراری و مطابقت	**مقایسه تراکنش‌های جدید با تراکنش‌های انتقالی به همان حساب در گذشته. برای مثال، بررسی فاکتورهای تکراری.**
رویه مطابقت برای برخورد با ورودی‌های رد شده	**اقدامات اصلاحی بعدی/ که ورود دوباره را امکان‌پذیر می‌سازد. برای مثال، تصفیه اقلام معلق**[4]**.**

1. Development stage
2. Authenticity
3. Data Input Validation
4. Clearance of Suspense Items

ریسک کنترل‌های ورودی

در صورت نبود کنترل‌های ورودی مناسب، ریسک پردازش نادرست یا متقلبانه به وجود می‌آید و در نتیجه، این برنامه نمی‌تواند هدف‌های کسب و کار سازمان را برآورده کند.

در سیستم‌های پردازش پیوسته، برخی از اقدامات کنترلی مانند تطبیق جمع ورودی و خروجی دسته‌ها برای اطمینان از کامل بودن ورودی، حفظ مستندات ایجاد/ پیدایش داده‌ها برای زنجیره عطف حسابرسی در دسترس نیست. با این وجود، در سیستم‌های برخط، کنترل‌های جبران‌کننده[1] دیگری چون کامل‌بودن تعاملی داده‌ها/ درخواست‌های اعتبار سنجی، ثبت سوابق تلاش‌های دسترسی و غیره تعبیه شده است.

۲-۵-۵. کنترل‌های پردازش

هدف‌های کنترلی

معیارهایی برای حفظ یکپارچگی، اعتبار و قابلیت اتکای داده‌ها و محافظت آن در برابر اشتباه‌های پردازشی در طول چرخه پردازش تراکنش- از دریافت داده‌ها از زیر سیستم ورودی تا فرستادن داده‌ها به بانک اطلاعاتی، ارتباطات یا زیرسیستم خروجی. این معیارها از اینکه داده‌های ورودی معتبر، تنها یک‌بار پردازش می‌شوند و کشف تراکنش‌های اشتباه، باعث اختلال در پردازش تراکنش‌های معتبر نمی‌شود، اطمینان می‌دهد. این معیارها همچنین، برای افزایش قابلیت اتکای برنامه‌هایی است که دستورهای لازم را برای برآورده کردن نیازهای خاص کاربر، اجرا می‌کند.

روش‌های کنترل شامل ایجاد و پیاده‌سازی مکانیسم‌هایی برای صدور مجوز آغاز پردازش تراکنش و تأکید بر این موضوع است که تنها از برنامه‌ها و ابزارهای مناسب و مجاز استفاده شده است. این روش‌ها، اجرای پردازش به صورت کامل و دقیق را حسب مورد، به‌طور خودکار بازبینی می‌کند. انواع این کنترل‌ها می‌تواند شامل بررسی اشتباه‌های توالی و تکرار، شمارش تراکنش/ رکورد، کنترل‌های یکپارچگی مرجع، جمع کنترلی و جمع در هم، کنترل دامنه و سرریز حافظه موقت[2] باشد.

در سیستم‌های پیوسته، برخی از کنترل‌های جبرانی ممکن است شامل بررسی یک‌به‌یک، گزارش گذشته‌نگر استثناها[3] و گزارشگری حساب معلق باشد.

1. Compensating controls
2. Buffer overflow
3. Retrospective batching exception

ریسک کنترل

اشتباه‌های پردازش ممکن است به دلیل نگاشت نادرست از قواعد کسب‌وکار، ناکافی بودن آزمون کد برنامه یا کنترل ناکافی بر نسخه‌های مختلف برنامه‌ها پس از برقراری دوباره یکپارچگی پردازش پس از بروز یک مشکل، ایجاد شود. در نبود فعالیت‌های کنترلی لازم برای پردازش، تراکنش‌های تکراری اشتباه می‌تواند رخ دهد که بر هدف‌های تجاری و سرقفلی تأثیر می‌گذارد.

۳-۵-۵. کنترل‌های خروجی

هدف‌های کنترلی

کنترل‌های خروجی، معیارهایی تعبیه شده در برنامه هستند که داده‌های پردازش شده توسط یک برنامه را در برابر تغییر و توزیع غیرمجاز، محافظت می‌کند.

فرآیندهای کنترل، شامل تعریف مناسب از خروجی‌ها، گزارش‌های مورد نظر در مرحله طراحی و توسعه سیستم، مستندسازی مناسب از منطق گزارش‌گیری، کنترل‌های محدودکننده دسترسی به داده‌های پردازش شده، بررسی خروجی‌ها، مغایرت‌گیری و بررسی است.

ریسک کنترل

در نبود اقدامات کنترلی کافی برای خروجی‌ها، ریسک اصلاح یا حذف غیرمجاز داده‌ها، ایجاد گزارش‌های مدیریتی سفارشی اشتباه و نقض محرمانگی داده‌ها وجود دارد.

۴-۵-۵. کنترل پرونده‌های اصلی/ داده‌های ایستا (ثابت)

پرونده‌های اصلی، پرونده‌های داده‌ای است شامل داده‌های نیمه دائمی مالی یا مرجع، که ممکن است توسط چندین برنامه کاربردی پردازش شوند. داده‌های ذخیره شده در پرونده اصلی، به‌عنوان داده‌های ایستا شناخته می‌شوند. برنامه‌های کاربردی برای پردازش تراکنش‌های خود از داده‌های مرجع موجود در پرونده‌های اصلی فراخوانی می‌کنند.

برای مثال، یک پرونده اصلی ممکن است شامل داده‌های ایستا در مورد قیمت‌های فروش کالاها باشد. هنگامی که فروشی انجام می‌شود، برنامه از کاربر می‌خواهد که داده‌های متغیر معامله مانند مقدار کالای فروخته شده را وارد کند. سپس، برنامه کاربردی، قیمت را از داده‌های ایستا در پرونده اصلی فرا می‌خواند و برای به‌دست آوردن قیمت کل فروش، قیمت واحد را با مقدار کالای فروخته شده ترکیب می‌کند.

داده‌های ایستا (ثابت) ممکن است نرخ پرداخت برای هر رده از کارکنان، مشخصات ارائه‌کننده (شماره ارجاع، نشانی، شماره تلفن و شرایط اعتباری)؛ مشخصات سازمان؛ شماره‌حساب بانکی کارکنان؛ نرخ تورم و شاخص‌ها؛ نرخ سربار و داده‌های مدیریت سیستم را شامل شود.

۵-۵-۵. استفاده از داده‌های ایستا

داده‌های ایستا به دلیل ماهیتی که دارند، برای پردازش بسیاری از معاملات استفاده می‌شود. برای مثال، داده‌های مالیات بر ارزش‌افزوده ممکن است برای تعیین بدهی‌های مالیاتی صدها یا هزاران تراکنش سازمان استفاده شود. سازمان باید کنترل‌هایی را برای اطمینان یافتن از مجاز بودن اصلاحات در داده‌های ایستا، پاسخگو بودن کاربران برای هرگونه تغییر، به‌روز و دقیق بودن و حفظ یکپارچگی پرونده‌های اصلی برقرار کند.

از آنجا که وجود اشتباه در داده‌های ثابت، اثری گسترده دارد، بدیهی است که کنترل بر روی این داده‌ها باید قوی‌تر از کنترل در معاملات جداگانه باشد.

۶-۵-۵. فرآیندهای کنترل پرونده اصلی

انواع کنترل‌هایی که سازمان می‌تواند برای محافظت از داده‌های ثابت از آن استفاده کند، مانند کنترل‌های دسترسی فیزیکی و منطقی، پیشتر در این مجموعه توضیح داده شده است. این کنترل‌ها باید از این موضوع اطمینان ایجاد کنند که تنها کاربران مجاز، قادر به دستیابی، ایجاد، اصلاح یا حذف داده‌های ثابت هستند.

این کنترل‌ها می‌توانند هم در سطح برنامه و هم در سطح نصب برقرار شوند. تک‌تک تراکنش‌ها باید مجوز داشته باشند و برای هرگونه تغییر در داده‌های پرونده اصلی نیز باید اصول مشابهی اعمال شود. از این‌رو، سازمان باید رویه‌ها و کنترل‌هایی را برای انجام اصلاحات در داده‌های پرونده اصلی داشته باشد. این موارد ممکن است شامل تهیه اصلاحات لازم در داده‌ها و اعمال آن توسط کاربر دیگری با مجوزهای خودکار باشد.

سوابق حسابرسی[1] از این دید سودمند است که می‌توانند تک‌تک کاربرانی را شناسایی کنند که اصلاحات غیرمجاز انجام می‌دهند. در بهترین حالت، سوابق حسابرسی باید مشخص کند که کدام سوابق و زمینه‌ها اصلاح شده‌اند، چه زمانی اصلاح شده‌اند، از چه چیزی به چه چیزی تغییر یافته‌اند، و چه کسی این اصلاح را انجام داده است.

1. Audit Logs

۶-۵. طبقه‌بندی کاربران و کنترل‌های امنیت برنامه

حسابرس برای تعیین فرآیند کنترل امنیت برنامه باید نقش مسئولانی را شناسایی کند که با یک برنامه کاربردی سروکار دارند. سه بازیگر اصلی عبارتند از: صاحب برنامه (با داشتن مسئولیت کلی برای سودمندی راهبردی، برای دستیابی به هدف‌های کسب‌وکار مانند، مدیر مالی برای یک برنامه حسابداری)، مدیر برنامه (مسئول دسترسی، پشتیبانی و کارکردهای امنیتی و گزارش به صاحب برنامه) و کاربر سیستم (با داشتن دسترسی محدود به ماژول‌ها/ روش‌های خاص). کنترل‌های امنیتی برنامه، با محدود کردن دسترسی برای گروه‌های مختلف کاربر، تراکنش‌ها و سوابق فعالیت را برای زنجیره عطف حسابرسی ایجاد می‌کند.

حسابرس باید از روش‌های پردازش داده‌های ورودی (ورود دسته‌ای/ برخط)، گردش تراکنش‌ها و خروجی‌ها، معاملات عمده انجام‌شده و پرونده‌های داده نگهداری شده و حجم تراکنش‌ها شناخت مناسبی بدست آورد. حسابرس برای ارزیابی کنترل‌های کاربردی باید از قضاوت حرفه‌ای استفاده کند و هنگام ارائه پیشنهادهایی برای بهبود باید ملاحظات لازم را در نظر بگیرد. جزئیات بیش از حد (اضافه) برای ثبت تراکنش‌ها می‌تواند هزینه‌های سربار سازمان را افزایش دهد و ممکن است زنجیره عطف موردنظر را ایجاد نکند. در شرایطی که سازمان از سیستم‌های مالی آماده[1] با مکانیسم‌های کنترل دسترسی استاندارد استفاده می‌کند، حسابرس باید وجود کنترل‌های دسترسی و درستی این کنترل‌ها را همگام با مراحل توسعه تعریف شده، تعیین کند.

مکانیسم‌های مؤثر شناسایی و احراز هویت را پیاده‌سازی کنید.

سازمان‌ها باید سیاست‌ها و رویه‌های امنیتی را برای شناسایی و احراز هویت[2] کاربر برنامه برقرار کنند. مدیریت باید محیطی را ایجاد کند که در آن، همه کاربران، شناسه و گذرواژه منحصر به فرد خود یا مکانیسم‌های دیگری مانند توکن‌ها و بیومتریک‌ها را برای دسترسی به هر بخش از سیستم اطلاعاتی و برنامه‌های کاربردی داشته باشند که به آنان اجازه دهد تا وظایف عملیاتی خود را مطابق با شرح شغلی خود انجام دهند. افزون بر این، شناخت مکانیسم‌های مورد استفاده برای اختصاص حق تقدم دسترسی به برنامه‌های مورد ارزیابی، حائز اهمیت است. ارزیابی کنترل‌های شناسایی و احراز هویت شامل بررسی عوامل زیر است:

- ❖ چگونه کاربران به برنامه کاربردی دسترسی پیدا می‌کنند؟
- ❖ آیا کاربران برای ورود به هر برنامه، موظف به وارد کردن نام کاربر/ شناسه و گذرواژه هستند؟

1. Off the Shelf Financial Packages
2. Identification and Authentication Mechanisms

- ❖ آیا همه کاربران دارای یک شناسه جداگانه و منحصر به فرد هستند تا ثبت و بررسی فعالیت‌های کاربر امکان‌پذیر شود؟
- ❖ ویژگی‌های بنیادی گذرواژه (یعنی الزامات تعداد کاراکترها و غیره) چیست؟
- ❖ برنامه کاربردی هرچند وقت یک‌بار کاربر را ملزم به تغییر گذرواژه می‌کند؟
- ❖ آیا مواردی وجود دارد که کاربران، شناسه و گذرواژه چندگانه داشته باشند؟
- ❖ آیا مواردی وجود دارد که کاربران، شناسه یا گذرواژه خود را به اشتراک بگذارند؟
- ❖ شناسه‌ها و گذرواژه‌های دیگری که کاربر باید پیش از دسترسی به صفحه ورود به سیستم برای برنامه وارد کند، چیست؟
- ❖ آیا کاربر، یک شناسه و گذرواژه شبکه‌ای وارد می‌کند؟
- ❖ آیا مدیریت، فهرستی به‌روز از کاربران مجاز را نگهداری و بررسی می‌کند؟
- ❖ آیا مدیریت به‌صورت دوره‌ای، فهرست کاربران را به‌منظور اطمینان یافتن از این‌که تنها افراد مجاز حق دسترسی دارند و دسترسی فراهم شده برای هر کاربر، مناسب است، مورد بررسی قرار می‌دهد؟
- ❖ آیا دسترسی عمومی (اشخاص برون‌سازمانی) به برنامه مجاز است؟
- ❖ آیا دسترسی از طریق اینترنت مجاز است؟ در این صورت، این دسترسی چگونه کنترل می‌شود؟

حسابرس با شناخت طراحی و عملکرد امنیت برنامه کاربردی، می‌تواند اثربخشی کنترل‌های امنیتی را بر سایر سطوح احراز هویت ارزیابی کند، به‌ویژه هنگامی‌که نقاط ضعفی در لایه امنیتی برنامه شناسایی می‌شود و ممکن است این ضعف‌ها توسط کنترل‌های قوی‌تر در سایر سطوح، جبران شود.

۷-۵. زنجیره عطف حسابرسی

زنجیره عطف حسابرسی سابقه‌ای از فعالیت‌های کاربر را به ترتیب تاریخ[1] فراهم می‌کند. این می‌تواند برای مستندسازی زمان ورود کاربر به سیستم، مدتی که وی به فعالیت‌های مختلف پرداخته و اینکه چه‌کارهایی انجام داده است، مورد استفاده قرار گیرد. مدیریت باید درباره فعالیت‌هایی که باید

1. Chronological Record

ثبت شود، تصمیم بگیرد؛ زیرا، نگهداری سابقه از هر فعالیت می‌تواند منابع رایانه ای را مصرف کند. حسابرس از جمله باید از موارد زیر اطمینان حاصل کند:

- ❖ نوع فعالیت‌هایی که در سیستم ثبت شده‌اند.
- ❖ آیا فهرست ورودهای امنیتی ایجاد و بررسی می‌شود؟
- ❖ آیا فهرست تراکنش‌ها / ورودها توسط مدیریت ارشد کسب‌وکار بررسی می‌شود؟
- ❖ آیا مدیریت، دسترسی درون برنامه کاربردی را کنترل می‌کند (یعنی تلاش‌های دسترسی غیرمجاز، فعالیت غیرمعمول و غیره)؟
- ❖ آیا برنامه کاربردی، گزارش‌هایی را برای شناسایی تلاش‌های دسترسی غیرمجاز، ایجاد می‌کند؟

۸-۵. اختیار و مسئولیت مدیر سیستم

مدیر سیستم، شخصی است که مسئولیت استفاده از سیستم رایانه‌ای چند کاربره، سیستم ارتباطی یا هر دو را بر عهده دارد.

از آنجا که سیستم‌های مدیریت داده توسط یک یا چند سیستم عامل[1] پشتیبانی می‌شوند، حسابرس باید از نقش مدیران سیستم‌های مدیریت داده شناخت کسب کند. تفکیک وظایف مشخصی بین مدیر سیستم مدیریت داده[2] و مدیر سیستم عامل[3] باید وجود داشته باشد. مدیر سیستم عامل ممکن است نیاز به دسترسی به سیستم مدیریت داده داشته باشد، اما این دسترسی باید محدود باشد. به همین ترتیب، مدیر سیستم مدیریت داده ممکن است به دسترسی به سیستم عامل زیربنایی نیاز داشته باشد، اما باید فقط دسترسی لازم برای مدیریت عملکرد سیستم مدیریت داده را داشته باشد.

حسابرس باید میزان تفکیک وظایف بین مدیر سیستم مدیریت داده و کارکنان مسئول سوابق حسابرسی و تراکنش‌ها را نیز ارزیابی کند.

مدیر سیستم مدیریت داده‌ها نباید به سوابق حسابرسی موجود در سیستم مدیریت داده دسترسی داشته باشد. این سوابق باید توسط یک مدیر امنیتی بررسی شود.

جدایی بین جنبه‌های عملکردی محیط‌های سیستم مدیریت داده نیز باید وجود داشته باشد. دسترسی به سیستم مدیریت داده باید با تفکیک عملکردی وظایف در محیط برنامه سازگار باشد.

1. Operating Systems
2. Data Management System Administrator
3. Operating System Administrator

کاربرانی که توسعه‌دهنده هستند تنها باید به محیط توسعه دسترسی داشته باشند و به تبع آن، تنها به سیستم مدیریت توسعه داده. کاربرانی که به دسترسی به تولید نیاز دارند، تنها باید به سیستم مدیریت تولید داده دسترسی داشته باشند.

اصطلاحاتی که در فصل ۴ بر آن تأکید شده است:

انواع کنترل‌های کاربردی (***Categories of Application Controls***): انواع کنترل‌های کاربردی عبارتند از کنترل‌های کاربردی امنیتی، کنترل‌های ورودی، کنترل‌های پردازش، کنترل‌های خروجی، کنترل‌های پرونده‌های اصلی/ داده‌های ایستا (ثابت).

طبقه‌های اصلی کنترل‌های عمومی (***Major Categories of General Controls***): طبقه‌های اصلی کنترل‌های عمومی عبارتند از تفکیک وظایف و کنترل‌های عملیاتی، کنترل‌های دسترسی، کنترل‌های تغییر.

کنترل‌ها (***Controls***): کلیه روش‌ها، سیاست‌ها و رویه‌هایی هستند که از حفاظت از دارایی‌های سازمان، درستی و قابلیت اطمینان از سوابق آن و پایبندی عملیاتی به استانداردهای مدیریت، اطمینان ایجاد می‌کنند.

کنترل‌های عمومی فناوری اطلاعات (***IT General Controls***): کنترل‌های عمومی، پایه و اساس ساختار کنترل فناوری اطلاعات می‌باشد. این کنترل‌ها بر محیط کلی تدوین و عملکرد، مدیریت و سیستم‌های فناوری اطلاعات متمرکز است. کنترل‌های عمومی فناوری اطلاعات، چارچوبی را برای کنترل کلی فعالیت‌های فناوری اطلاعات ایجاد می‌کند و درباره دستیابی به هدف‌های کلی کنترلی، تا حدودی اطمینان می‌دهد. همچنین، کنترل‌های عمومی شامل کنترل‌های فراگیر هستند. این گونه کنترل‌ها برای مدیریت و نظارت بر محیط فناوری اطلاعات طراحی شده‌اند؛ بنابراین، بر همه فعالیت‌های مرتبط با فناوری اطلاعات اثر می‌گذارند.

کنترل‌های کاربردی فناوری اطلاعات (***IT Application Controls***): کنترل‌های تعبیه شده در برنامه‌های فرآیند کسب‌وکار معمولاً با نام کنترل‌های کاربردی مورد اشاره قرار می‌گیرند. کنترل‌های کاربردی به کنترل‌های مربوط به پردازش معاملات و داده‌ها در یک سیستم کاربردی اشاره دارند و بنابراین، مختص هر برنامه هستند.

فصل ۵

مروری کلی بر برنامه‌ریزی

امروزه، حسابرسی فناوری اطلاعات در بیشتر حسابرسی‌های مالی، نقشی اساسی دارد. کنترل‌های فناوری اطلاعات در بیشتر سازمان‌ها از اهمیت ویژه‌ای برخوردار است و حسابرس فناوری اطلاعات باید در مرحله برنامه‌ریزی حسابرسی مشارکت کند تا کنترل‌های فناوری اطلاعات را ارزیابی و مشخص کند که آیا می‌توان از رویکرد حسابرسی اتکا بر کنترل‌ها، استفاده کرد.

حسابرس در طول حسابرسی فناوری اطلاعات، محیط کنترل‌های عمومی و کاربردی را ارزیابی و تعیین می‌کند که آیا می‌توان بر کنترل‌ها اتکا کرد یا به انجام آزمون‌های اضافی نیاز است. نتیجه این ارزیابی باید به‌گونه‌ای کافی و مناسب به حسابرس مالی (یا سایرین) انتقال داده شود تا حسابرس سیستم‌های مالی، این یافته‌ها را در رویکرد حسابرسی خود مورد توجه قرار دهد. همان‌گونه که پیشتر در مورد ریسک آمد، برای برآورد ریسک و کمک به حسابرس در تصمیم‌گیری در مورد بهره‌گیری از رویکرد آزمون رعایت یا آزمون محتوا، از رویکرد حسابرسی با نگرش مدیریت ریسک استفاده می‌شود.

حسابرس فناوری اطلاعات باید هدف کلی حسابرسی را درک کند چون نوع و ماهیت، زمان‌بندی و میزان روش‌های حسابرسی فناوری اطلاعات بسته به هدف حسابرسی، فرق می‌کند. همان‌گونه که در فصل ۱ آمد، انواع مختلف حسابرسی‌های فناوری اطلاعات، هدف‌های کلی متفاوتی دارند. اگر حسابرسی برای پشتیبانی از حسابرسی مالی یا حسابرسی دیگری باشد، حسابرس فناوری اطلاعات باید از هدف‌های آن حسابرسی شناخت داشته باشد.

نخستین گام در رویکرد با نگرش مدیریت ریسک که در فصل ۳ آمد، گردآوری اطلاعات و برنامه‌ریزی است. حسابرس باید از عملیات اصلی و فرایندهای تجاری اصلی[1] سازمان شناخت بدست آورد. حسابرس برای برنامه‌ریزی حسابرسی، شناختی کلی از زیرساخت سیستم اطلاعاتی سازمان[2] کسب می‌کند، که بررسی مستندات اصلی سازمانی به شرح زیر را شامل می‌شود:

- مستندات راهبرد و رویه فناوری اطلاعات.
- ساختار سازمانی واحد فناوری اطلاعات.
- بودجه فناوری اطلاعات و برنامه‌های عملیاتی.
- مدارک تحصیلی و شایستگی کارکنان کلیدی فناوری اطلاعات.
- طراحی سیستم‌های فناوری اطلاعات، نقشه‌ها، راهنماهای کاربرها و رویه‌های فرآیند کسب‌وکار.

بررسی این مستندات، حسابرس را در شناخت تفصیلی کسب‌وکار، جریان معاملات و تعاملات برنامه کاربردی کمک می‌کند. حسابرس بر اساس شناخت خود از این سیستم‌ها، نقاط کلیدی کنترل‌های اصلی[3] را در طراحی سیستم‌های اطلاعاتی سازمان، مشخص می‌کند.

۱. کدام استانداردهای حسابرسی به ارزیابی کنترل‌های داخلی توسط حسابرس مربوط است

استاندارد بین‌المللی دیوان‌های محاسبات بخش ۱۳۰۰، به مسئولیت حسابرس در برنامه‌ریزی حسابرسی صورت‌های مالی می‌پردازد. این استاندارد، حسابرس را به انجام فعالیت‌های مقدماتی حسابرسی برای شناخت سازمان (استاندارد بین‌المللی دیوان‌های محاسبات بخش ۱۲۱۰)، مدیریت مؤثر ارتباط با سازمان مورد رسیدگی[4] و ارزیابی میزان رعایت الزامات اخلاقی[5] (استاندارد بین‌المللی دیوان‌های محاسبات بخش ۱۲۲۰)، ملزم می‌کند. افزون بر این، این استاندارد حسابرس را به تدوین یک طرح کلی حسابرسی[6] و یک برنامه حسابرسی[7] موظف می‌کند. برنامه حسابرسی در یکی از فصل‌های آتی بحث می‌شود.

استاندارد بین‌المللی دیوان‌های محاسبات بخش ۱۳۱۵، با مسئولیت حسابرس در شناسایی و ارزیابی ریسک‌های تحریف با اهمیت در صورت‌های مالی، از طریق کسب شناخت از سازمان و محیط آن،

1. Key Business Processes
2. Entity's IS Infrastructure
3. Key Critical Control Points
4. Auditee
5. Ethical Requirements
6. Overall Audit Strategy
7. Audit Plan

از جمله کنترل داخلی، سروکار دارد. این استاندارد، حسابرس را به کسب شناخت از کنترل‌های داخلی مرتبط با حسابرسی ملزم می‌کند. اگرچه بیشتر کنترل‌های مربوط به حسابرسی احتمالاً به گزارشگری مالی مربوط می‌شوند، اما همه کنترل‌های مربوط به گزارشگری مالی، مربوط به حسابرسی نیستند (بندهای الف ۴۲ تا الف ۶۵). افزون بر این، این استاندارد حسابرس را به کسب شناخت از سیستم‌های اطلاعاتی، از جمله فرایندهای تجاری مرتبط با گزارشگری مالی نیز ملزم می‌کند (بندهای الف ۸۱ تا الف ۸۵).

۲. گردش فرآیند حسابرسی

حسابرسان فناوری اطلاعات در انجام بررسی عملکرد سیستم، به احتمال زیاد با دو سناریو به شرح زیر رو به‌رو می‌شوند:

- ❖ حسابرسان فناوری اطلاعات صرفاً بررسی سیستم فناوری اطلاعات را انجام می‌دهند. برای مثال، حسابرسی توسعه سیستم یا بررسی امنیت شبکه[1].
- ❖ حسابرسان فناوری اطلاعات به صورت یکپارچه با حسابرسان قانونی، عملکرد یا رعایت، حسابرسی را انجام می‌دهند.

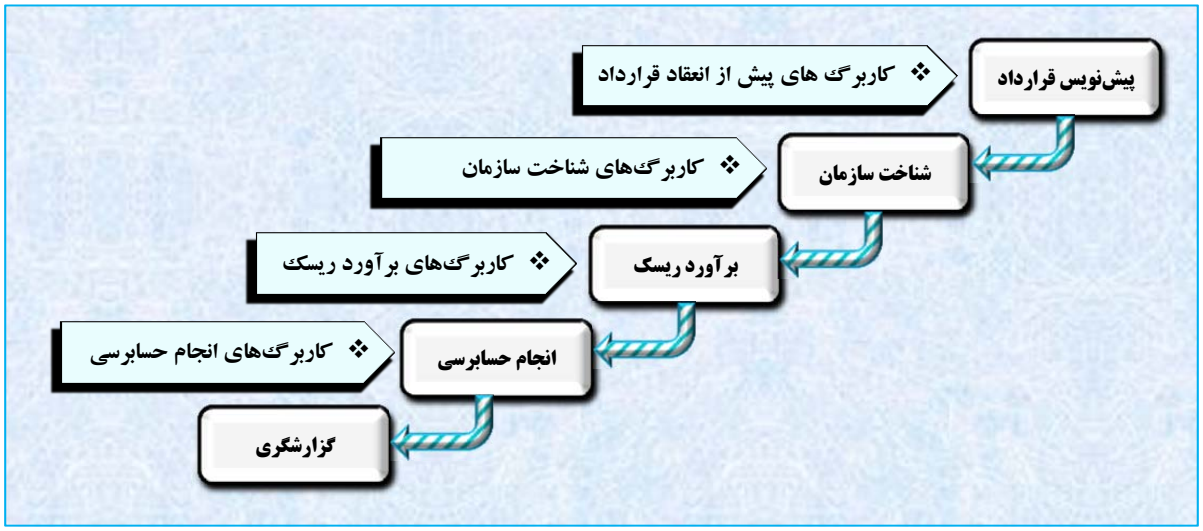
جریان فرآیند حسابرسی که توسط حسابرسان سیستم‌های اطلاعاتی در هر دو سناریو دنبال می‌شود، معمولاً مراحل یکسانی با فرآیند حسابرسی مالی یا دیگر انواع حسابرسی دارد.

نمونه کاربرگ‌هایی[2] برای گنجاندن موضوع‌های مرتبط با فناوری اطلاعات تهیه شده که پیشتر در سایر کاربرگ‌ها نیامده است. هدف این کاربرگ‌های نمونه، تلاشی است برای اطمینان یافتن از اینکه کنترل‌های فناوری اطلاعات و غیر فناوری اطلاعات و ریسک ناشی از آن‌ها در همه مراحل حسابرسی، به‌اندازه کافی ارزیابی می‌شوند.

چنانچه این کاربرگ‌ها (ی نمونه) به‌طور کامل تکمیل شوند، از مطابقت کامل با الزامات استانداردهای بین‌المللی دیوان‌های محاسبات و سایر استانداردهای پذیرفته شده بین‌المللی[3] اطمینان می‌دهند.

1. Network Security Review
2. Template Working Papers
3. Internationally Accepted Standards

مراحل و نمونه کاربرگ‌های آن‌ها به شرح زیر است:



۳. اهمیت

مفاهیم کلیدی زیر بر اساس استانداردهای انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۱۲۰۴، در مورد اهمیت آورده شده است:

- حسابرسان سیستم‌های اطلاعاتی و دیگر اطمینان‌بخشان حرفه‌ای باید ضعف یا نبود احتمالی کنترل‌ها را هنگام برنامه‌ریزی یک کار حسابرسی و این که چنین ضعف یا نبود کنترل‌ها می‌تواند به نقص یا ضعف با اهمیت منجر شود یا خیر را مورد توجه قرار دهند.
- حسابرسان و دیگر اطمینان‌بخشان حرفه‌ای سیستم‌های اطلاعاتی باید اهمیت و ارتباط آن را با ریسک حسابرسی برای تعیین نوع و ماهیت، زمان‌بندی اجرا و میزان روش‌های حسابرسی در نظر بگیرند.
- حسابرسان و دیگر اطمینان‌بخشان حرفه‌ای سیستم‌های اطلاعاتی باید اثر انباشته نارسایی‌ها یا ضعف‌های کنترلی جزئی و اینکه آیا نبود کنترل‌ها به نارسایی یا ضعف با اهمیتی منجر می‌شود را در نظر بگیرند.

حسابرسان و دیگر اطمینان‌بخشان حرفه‌ای سیستم‌های اطلاعاتی باید موارد زیر را در گزارش خود افشا کنند:

- نبود کنترل‌ها یا وجود کنترل‌های غیر اثربخش.
- اهمیت ضعف‌های کنترلی.
- احتمال این که چنین ضعف‌هایی به نارسایی یا ضعف با اهمیت منجر شود.

حسابرسان فناوری اطلاعات در یک حسابرسی یکپارچه باید در چارچوب کلی اهمیتی فعالیت کنند که توسط حسابرسان قانونی برای همه مسأله‌های مالی تعیین شده است. با این حال، این امر حسابرسان فناوری اطلاعات را از توجه به اهمیت در حسابرسی موضوع های فناوری اطلاعات مستثنی نمی‌سازد. استانداردهای بین‌المللی دیوان‌های محاسبات بخش ۵۳۰۰، مقرر می‌دارد که حسابرسان فناوری اطلاعات در طول فرآیند حسابرسی فناوری اطلاعات، اهمیت را در نظر بگیرند.

با این‌حال، اهمیت یک موضوع حسابرسی فناوری اطلاعات باید در چارچوب کلی اهمیت در هر دیوان محاسبات (SAI) تعیین شود. چشم‌انداز اهمیت، بسته به نوع و ماهیت هر حسابرسی فناوری اطلاعات، فرق می‌کند. اهمیت در حسابرسی مالی، عملکرد و رعایت بخش عمومی، که حسابرس فناوری اطلاعات نیز بخشی از آن است، در استانداردهای بین‌المللی دیوان‌های محاسبات بخش‌های ۲۰۰، ۳۰۰ و ۴۰۰ مورد بحث قرار گرفته است (استانداردهای بین‌المللی دیوان‌های محاسبات بخش ۵۳۰۰).

۴. اولویت‌بندی سیستم اطلاعاتی

حسابرسان فناوری اطلاعات پس از شناخت سیستم فناوری اطلاعات در سطح راهبردی از طریق مستندسازی سیستم و چک‌لیست زیرساخت‌های فناوری اطلاعات باید تصمیم بگیرند که کدام سیستم را حسابرسی کنند و در مورد آن گزارش بدهند.

این تعیین اولویت به اثر مالی، اثر سیستم بر عملکردها یا دارایی‌های اساسی، موجودی‌ها، مشتریان، تصمیم‌گیری و میزان برخط بودن عملیات آن‌ها، نگرانی‌های ذینفعان، منافع عمومی، الزامات نظارتی و پیامدهای آن برای جامعه بستگی دارد.

اثر مالی در یک حسابرسی یکپارچه، عاملی است کلیدی برای تعیین اولویت سیستم‌های مورد حسابرسی. جدول صفحه آتی می‌تواند برای کمک به اولویت‌بندی سیستم‌ها مورد استفاده قرار گیرد؛ زیرا، حسابرسان باید سیستمی را حسابرسی کنند که اقلام با اهمیت را پردازش می‌کند.

شناخت سیستم اطلاعاتی مربوط به گزارشگری مالی– طبق ISSAI ۱۳۱۵ بخش ۱۸				
نام برنامه کاربردی	گروه‌های معاملات/ مانده حساب‌ها (به جدول راهنمای حسابرسان نظارتی مراجعه کنید)		شرح و هدف برنامه کاربردی	آیـا سیستم به حسابرسی مربوط است؟ ارزیابی مختصری از اهمیت، تنوع و پیچیدگی عملیات سازمان و پیچیدگی سیستم‌ها ارائه دهید.
	گروه‌های معاملات	مبلغ		
برای مثال: سیستم‌های اطلاعاتی مدیریت مالی یکپارچه[1]	اقلام تدارکاتی	۳۰٫۰۰۰	این یک سیستم مدیریت مالی یکپارچه است که ۹۰ درصد هزینه‌های دولت را مدیریت می‌کند.	مبلغ، مقدار و سیستم، ۹۰ درصد هزینه‌های دولت را پوشش می‌دهد.

۵. برنامه‌های حسابرسی

۵–۱. برنامه حسابرسی چیست؟

برنامه حسابرسی[2] مجموعه‌ای از مراحل یا رویه‌هایی است که برای دستیابی به هدف حسابرسی اجرا می‌شود.

۵–۲. چرا حسابرس فناوری اطلاعات باید برنامه حسابرسی تهیه/ تدوین کند؟

استانداردهای بین‌المللی دیوان‌های محاسبات بخش ۱۲۳۰، در بخش رهنمودهای حسابرسی مالی، به مسئولیت حسابرس در تهیه مستندات حسابرسی در حسابرسی صورت‌های مالی می‌پردازد. حسابرس باید جنبه‌های مختلف حسابرسی را در یک سند با عطف متقابل به کاربرگ‌های پشتیبان، ثبت کند.

استاندارد انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۱۲۰۱ با نام **"برنامه‌ریزی کار حسابرسی"** مقرر می‌دارد که حسابرس سیستم‌های اطلاعاتی باید برای هر کار حسابرسی و اطمینان بخشی سیستم‌های اطلاعاتی یک برنامه رسیدگی[3] تهیه و مستندسازی کند.

1. Integrated Financial Management Information Systems (IFMIS)
2. Audit Programme
3. Project plan

طرح حسابرسی به حسابرسان در تهیه برنامه حسابرسی فناوری اطلاعات کمک می‌کند. پیش‌نیاز تهیه برنامه حسابرسی، داشتن شناختی کافی از سازمان مورد حسابرسی و سیستم‌های اطلاعاتی آن است (دستورالعمل IDI[1]).

افزون بر این، حسابرسان باید یک برنامه حسابرسی و/ یا طرحی تفصیلی از نوع و ماهیت، زمان‌بندی اجرا و میزان روش‌های حسابرسی مورد نیاز برای تکمیل حسابرسی را تهیه و مستندسازی کنند.

این روش‌های حسابرسی باید به‌گونه‌ای مستندسازی شوند که حسابرس فناوری اطلاعات بتواند روش‌های تکمیل شده را ثبت و کارهای باقی‌مانده برای اجرا را شناسایی کند. حسابرس فناوری اطلاعات باید با پیشرفت کار و بر اساس اطلاعات گردآوری شده در طول حسابرسی، کفایت برنامه را ارزیابی کند. چنانچه حسابرس فناوری اطلاعات تشخیص دهد که روش‌های برنامه‌ریزی شده، کافی نیستند باید برنامه را به‌گونه‌ای مناسب اصلاح کند.

برنامه حسابرسی، مبتنی بر دامنه و هدف‌های حسابرسی فناوری اطلاعات و شامل روش‌هایی است برای بدست آوردن شواهد کافی، مربوط و قابل اعتماد برای پشتیبانی از نتیجه‌گیری‌ها و اظهارنظرهای حسابرس.

حسابرس پس از تکمیل ماتریس برنامه‌ریزی حسابرسی فناوری اطلاعات که در قسمت پیش آمد باید برنامه حسابرسی تفصیلی را تدوین کند. این برنامه حسابرسی شامل روش‌های حسابرسی تفصیلی مورد نیاز برای تکمیل حسابرسی خواهد بود.

۵-۳. محتوای یک برنامه حسابرسی

بهترین رویه عمل‌ها مقرر می‌دارد که برنامه حسابرسی شامل موارد زیر باشد:

- توصیف زمینه حسابرسی.
- هدف‌های حسابرسی.
- معیارها و منابع هر مرحله حسابرسی.
- عطف‌گذاری کاربرگ‌ها[2].

1. INTOSAI Development Initiative (IDI)
2. Working Paper (W/p) Reference

- ❖ نام حسابرس رسیدگی‌کننده.
- ❖ تاریخ رسیدگی.
- ❖ پیشنهادها (برای مثال، اگر مورد ندارد، چرا).
- ❖ نتیجه‌گیری.
- ❖ زمان‌بندی اجرا و میزان آزمون‌ها.

توصیف زمینه حسابرسی

برای مثال، طرح تداوم کسب‌وکار (BCP) [1]- مجموعه گسترده‌ای از فرایندها و دستورالعمل‌های کل سازمان برای اطمینان یافتن از تداوم فرایندهای کسب‌وکار- شامل، اما نه محدود به فناوری اطلاعات- در صورت پدید آمدن وقفه است. این طرح، برنامه‌هایی را برای بازیابی پس از رخداد حوادث جزئی تا اختلالات (قطعی) عمده عملیات برای سازمان فراهم می‌کند. این طرح معمولاً، به قسمت‌های سازمان و مدیریت بحران یا اداره پیشگیری از ریسک تعلق دارد و توسط آن‌ها مدیریت می‌شود. برنامه‌های عملکردی تداوم، زیرمجموعه‌هایی از برنامه‌ریزی تداوم فعالیت سازمان هستند و از ارائه خدمات اساسی کسب‌وکار، پشتیبانی می‌کنند.

هدف حسابرسی

برای مثال، حسابرسی برنامه‌ریزی تداوم فعالیت شامل موارد زیر است:

- ❖ یک ارزیابی از میزان آمادگی سازمان در صورت رخداد اختلال عمده در کسب‌وکار به مدیریت ارائه دهید. مسأله‌های محدودکننده را پردازش و بازیابی طی دوره را شناسایی کنید.
- ❖ یک ارزیابی مستقل از میزان اثربخشی برنامه تداوم فعالیت سازمان و همسویی آن با برنامه‌های تداوم زیرمجموعه آن را برای مدیریت فراهم کنید.

دامنه حسابرسی

برای مثال، این بررسی بر برنامه تداوم فعالیت کسب‌وکار سازمان، سیاست‌ها، استانداردها، دستورالعمل‌ها، رویه‌ها و قوانین و مقرراتی تمرکز می‌کند که به حفظ خدمات مستمر کسب‌وکار می‌پردازد و شامل موارد زیر خواهد بود:

- ❖ تدوین، نگهداری و آزمون برنامه تداوم فعالیت سازمان.
- ❖ توانایی ارائه خدمات تجاری طی دوره و بازسازی مؤثر و به‌موقع آن.
- ❖ مدیریت ریسک و هزینه‌های مربوط به برنامه تداوم فعالیت سازمان.

1. Business Continuity Plan (BCP)

معیارها و منابع لازم برای هر مرحله حسابرسی

حسابرسان فناوری اطلاعات باید معیارهایی را انتخاب کنند که بر اساس آن‌ها اطلاعات موضوع، مورد ارزیابی قرار خواهد گرفت. حرفه‌ای‌ها هنگام انتخاب معیارها باید مناسب بودن، مقبولیت و منبع معیارها را کاملاً مورد توجه قرار دهند (استاندارد حسابرسی و اطمینان بخشی ۱۰۰۸ ISACA- معیارها).

حسابرس در این بخش، اطلاعات لازم را برای رسیدن به هدف و منبع دریافت آن اطلاعات، تعیین می‌کند. برای مثال. حسابرس باید برنامه تداوم فناوری اطلاعات، برنامه آزمون، برنامه پیاده‌سازی، کاستی‌ها و چگونگی رفع کاستی‌ها را به دست آورد.

عطف‌گذاری کاربرگ رسیدگی

بهترین نحوه عمل‌ها، حسابرس را به ایجاد یک کاربرگ برای هر زمینه حسابرسی ملزم می‌کند. کار انجام شده، مسأله‌های شناسایی شده و نتیجه‌گیری‌ها، در این کاربرگ می‌آید. از عطف‌گذاری باید برای عطف متقابل مراحل حسابرسی به کاربرگ‌های رسیدگی پشتیبانی‌کننده، استفاده شود.

پیشنهادها

از ستون پیشنهادها/ نظرات می‌توان برای نشان دادن علت چشم‌پوشی از یک مرحله یا روش مربوط به مرحله انجام شده، استفاده کرد نه به‌عنوان کاربرگی جایگزین تشریح کار انجام شده.

۶. شواهد و مدارک

استاندارد سیستم‌های اطلاعاتی شماره ۱۲۰۴ انجمن حسابرسان سیستم‌های اطلاعاتی با نام **شواهد** شامل مفاد زیر است:

- حسابرسان سیستم‌های اطلاعاتی و دیگر اطمینان‌بخشان باید شواهد کافی و مناسب را برای نتیجه‌گیری معقول بدست آورند تا نتایج کار را بر اساس آن بنا کنند
- حسابرسان سیستم‌های اطلاعاتی و دیگر اطمینان‌بخشان باید کافی بودن شواهد گردآوری شده را برای پشتیبانی از نتیجه‌گیری‌ها و دستیابی به هدف‌های کار، ارزیابی کنند.

شواهد حسابرسی عبارت است از گردآوری داده‌ها، اسناد و مدارک و اطلاعات توسط حسابرسان فناوری اطلاعات برای اثبات یافته‌های خود به ذینفعان ذی‌ربط، در بازه زمانی مربوط (در زمان حسابرسی یا پس از آن) و به‌گونه‌ای کافی، قابل اتکا و مناسب (استانداردهای بین‌المللی دیوان‌های محاسبات بخش ۵۳۰۰).

شواهد حسابرسی‌های فناوری اطلاعات باید به‌گونه‌ای مناسب نام‌گذاری و ذخیره شوند تا بدون هیچ‌گونه تغییری در طول زمان و برای استفاده دوباره در دسترس باشند. حسابرسان فناوری اطلاعات در صورت وجود یک سیستم معاملات پیوسته[1] باید از مشخص بودن دوره مرور زمان[2] شواهد بدست آمده برای به‌روزرسانی یا تغییرات احتمالی، اطمینان یابند (استانداردهای بین‌المللی دیوان‌های محاسبات بخش ۵۳۰۰).

روش‌های مورد استفاده برای گردآوری شواهد، بسته به ویژگی‌های سیستم اطلاعاتی مورد رسیدگی، زمان‌بندی حسابرسی، دامنه و هدف‌های حسابرسی و قضاوت حرفه‌ای حسابرس فرق می‌کند. شواهد را می‌توان با استفاده از روش‌های حسابرسی دستی، تکنیک‌های حسابرسی به کمک رایانه (CAATs) یا ترکیبی از هر دو گردآوری کرد. متخصصان باید مناسب‌ترین روش را در ارتباط با هدف حسابرسی سیستم‌های اطلاعاتی انتخاب کنند (دستورالعمل حسابرسی و اطمینان بخشی ISACA 2205- شواهد[3]).

۷. ابزارهای حسابرسی فناوری اطلاعات

دیوان محاسبات باید ابزارهای حسابرسی فناوری اطلاعات مقتضی و متناسب با برآورد ریسک کار حسابرسی، ظرفیت و منابع در دسترس را به‌گونه‌ای مؤثر به‌کار گیرد.

حسابرس می‌تواند از نرم‌افزارهای عمومی حسابرسی یا تکنیک‌های حسابرسی به کمک رایانه برای تجزیه‌وتحلیل اطلاعات استفاده کند. ابزارهایی مانندExcel، Access، IDEA، ACL و غیره نمونه‌هایی از نرم‌افزارهای عمومی حسابرسی هستند که امکان واردکردن و همچنین، تجزیه‌وتحلیل داده‌ها را فراهم می‌کنند (دستورالعمل IDI).

استفاده از تکنیک‌های حسابرسی به کمک رایانه بسیار سودمند است، از جمله، تجزیه‌وتحلیل ورود کاربران[4]، گزارش استثناها[5]، جمع زدن، مقایسه پرونده، طبقه‌بندی، نمونه‌گیری[6]، بررسی دوباره[7]، تشخیص شکاف‌ها[8]، تجزیه سنی[9]، محاسبات فیلدهای مجازی[10] و غیره (استانداردهای بین‌المللی دیوان‌های محاسبات بخش ۵۳۰۰).

1. Continuous Transacting System
2. Timestamps
3. ISACA IS Audit and Assurance Guideline 2205-Evidence
4. User Log Analysis
5. Exception Reporting
6. Sampling
7. Duplicate Checks
8. Gap Detection
9. Ageing
10. Virtual Field Calculations

اصطلاحاتی که در فصل ۵ بر آن تأکید شده است

برنامه حسابرسی (Audit Programme): مجموعه‌ای از مراحل یا رویه‌هایی است که برای دستیابی به هدف حسابرسی اجرا می‌شود.

گردش فرآیند حسابرسی (The Audit Process Flow)- حسابرسان فناوری اطلاعات در انجام بررسی عملکرد سیستم، به‌احتمال زیاد با دو سناریو رو به‌رو می‌شوند: (۱) حسابرسان فناوری اطلاعات صرفاً بررسی سیستم فناوری اطلاعات را انجام می‌دهند، برای مثال، حسابرسی تدوین و توسعه سیستم یا بررسی امنیت شبکه و (۲) حسابرسان فناوری اطلاعات به صورت یکپارچه با حسابرسان قانونی، عملکرد یا رعایت، حسابرسی را انجام می‌دهند.

فصل ۶

راهبری فناوری اطلاعات

۱. راهبری فناوری اطلاعات چیست؟

مسئولیت راهبری فناوری اطلاعات با هیأت مدیره و مدیریت ارشد است. راهبری فناوری اطلاعات بخشی جدایی‌ناپذیر از راهبری سازمانی و شامل رهبری، ساختارها و فرایندهای سازمانی است که از حفظ و گسترش راهبرد و هدف‌های سازمان توسط فناوری اطلاعات اطمینان می‌دهد.

هدف از راهبری فناوری اطلاعات، هدایت منابع فناوری اطلاعات است تا از برآورده شدن هدف‌های زیر توسط عملکرد فناوری اطلاعات، اطمینان بدست آید:

- همسویی فناوری اطلاعات با سازمان و تحقق منافع مورد انتظار؛
- استفاده از فناوری اطلاعات برای توانمندسازی سازمان با استفاده از فرصت‌ها و حداکثرسازی منافع؛
- استفاده مسئولانه از منابع مرتبط با فناوری اطلاعات؛ و
- مدیریت مناسب ریسک‌های فناوری اطلاعات.

راهبری فناوری اطلاعات اساساً به دو چیز مربوط می‌شود:

- ارزش افزایی فناوری اطلاعات برای سازمان و کاهش ریسک‌های فناوری اطلاعات. ارزش افزایی عمدتاً از طریق همسویی راهبردی فناوری اطلاعات با کسب‌وکار انجام می‌شود، درحالی‌که کاهش ریسک‌های فناوری اطلاعات با ایجاد مسئولیت‌پذیری (پاسخگویی) در سازمان محقق می‌گردد.
- راهبری فناوری اطلاعات فرآیندی مستمر است که در ابتدا با تدوین یک راهبرد و همسویی آن در سرتاسر سازمان آغاز می‌شود و با پیاده‌سازی ادامه می‌یابد و باید به‌طور منظم مورد نظارت قرار گیرد.

حسابرس باید از نقش‌ها و مسئولیت‌های کارکنان و کمیته‌های کلیدی مدیریت فناوری اطلاعات، شناخت داشته باشد. با این‌حال، پذیرش این که این سِمَت‌ها احتمالاً در همه سازمان‌ها وجود دارد، اما با عنوان‌های متفاوت یا یک نفر که چندین نقش را (به شرح زیر) ایفا می‌کند از اهمیت برخوردار است:

- **هیأت مدیره (مجلس)**- بلندپایه‌ترین مدیران اجرایی و/ یا غیر اجرایی سازمان که مسئول راهبری سازمان هستند و کنترل کلی بر منابع آن دارند.
- **مدیرعامل** که مدیریت کل سازمان را بر عهده دارد.
- **کمیته مدیریت ارشد**- گروهی از مدیران ارشد که از طرف هیأت مدیره برای مدیریت عملیات روزمره سازمان منصوب شده‌اند.
- **کمیته راهبری فناوری اطلاعات**[1]- شامل ذینفعان کلیدی از مدیران ارشد، مدیران اجرایی و فناوری اطلاعات برای اولویت‌بندی برنامه‌های سرمایه‌گذاری فعال فناوری اطلاعات مطابق با راهبرد تجاری و اولویت‌های سازمان؛ پیگیری وضعیت پروژه‌ها؛ برطرف کردن تضاد منافع؛ نظارت بر سطح خدمات و بهبود خدمات.
- **مدیر ارشد اطلاعات (CIO)**[2]- ارشدترین مقام سازمان که مسئول واحد فناوری اطلاعات؛ همسویی فناوری اطلاعات و راهبرد تجاری؛ برنامه‌ریزی، تأمین منابع و مدیریت ارائه خدمات فناوری اطلاعات؛ و بکارگیری منابع انسانی مرتبط است. مدیر ارشد اطلاعات به‌طور معمول، ریاست شورای راهبری مدیریت پرتفو را برعهده دارد.
- **مدیر/ معاون مالی (CFO)**[3]- ارشدترین مقام سازمان که مسئول برنامه‌ریزی مالی، امور مالی و ریسک‌های مالی است. مالکان فرایندهای کسب‌وکار- افرادی که مسئولیت شناسایی نیازهای فرآیند، تأیید طراحی فرایند و مدیریت عملکرد فرایند را به عهده دارند. به طور کلی، مالک فرآیند کسب‌وکار باید در سطح بالایی در سازمان باشد و اختیارات لازم را برای تخصیص منابع به فعالیت‌های **"رویکرد نگرش مدیریت ریسک"** خاص فرایند داشته باشد.
- **حسابرس مستقل**[4]- تنها، مسئولیت اظهارنظر حسابرسی و تعیین نوع و ماهیت، زمان‌بندی اجرا و میزان روش‌های حسابرسی را دارد. حسابرس داخلی- به معنای فعالیت ارزیابی ایجاد شده در درون سازمان برای ارائه خدمات به سازمان است. از جمله وظایف آن، نظارت بر کفایت و اثربخشی کنترل‌های داخلی است.

1. IT Steering Committee
2. Chief Information Officer (CIO)
3. Chief Financial Officer (CFO)
4. External Auditor

۲. چرا شناخت راهبری فناوری اطلاعات برای حسابرس فناوری اطلاعات اهمیت دارد؟

راهبری فناوری اطلاعات برای اطمینان یافتن از ارزش‌آفرینی سرمایه‌گذاری‌های جدید و موجود در فناوری اطلاعات، کاهش ریسک‌های مربوط به فناوری اطلاعات و پرهیز از شکست، ضروری است.

فناوری اطلاعات، رمز موفقیت سازمان در ارائه خدمات و کالا به‌طور مؤثر و کارآمد است؛ به‌ویژه، هنگامی‌که فناوری اطلاعات برای ایجاد تغییر در سازمان طراحی شده باشد. این روند تغییر، که معمولاً **"تحول کسب‌وکار"** نامیده می‌شود، در حال حاضر عامل اصلی ایجاد مدل‌های تجاری جدید هم در بخش خصوصی و هم در بخش عمومی است. تحول کسب‌وکار، منافع زیادی دارد، هرچند که احتمال پدید آمدن ریسک‌های زیادی را هم دارد که می‌تواند عملیات را مختل کند و پیامدهای ناخواسته‌ای داشته باشد. برقراری تعادل بین ریسک و ارزشِ افزوده هنگام استفاده از فناوری اطلاعات برای ایجاد تغییرات سازمانی، وضعیت دشواری است.

علیرغم تلاش‌های صنعت نرم‌افزاری برای شناسایی و بکارگیری بهترین شیوه‌های عمل در تدوین پروژه‌های فناوری اطلاعات، هنوز هم میزان بالایی از شکست و دست نیافتن به هدف‌ها وجود دارد. بیشتر پروژه‌های فناوری اطلاعات، هدف‌های سازمان را برآورده نمی‌کنند.

۳. محدودیت‌های راهبری فناوری اطلاعات می‌تواند به نظر مشروط حسابرس منجر شود

سازمان‌هایی که برای پیاده‌سازی ساختار مؤثر راهبری تلاش می‌کنند، به‌ویژه هنگامی‌که سرمایه‌گذاری‌های با اهمیتی در فناوری اطلاعات دارند، با محدودیت‌های گوناگونی مواجه می‌شوند. بدون وجود راهبری مؤثر برای برخورد با این محدودیت‌ها، پروژه‌های فناوری اطلاعات از ریسک شکست بالاتری برخوردارند.

هر سازمانی با چالش‌های منحصر به‌فرد خود روبه‌رو است؛ زیرا، مسأله‌های محیطی، سیاسی، جغرافیایی، اقتصادی و اجتماعی خاص خود را دارد. هر یک از این مسأله‌ها می‌تواند مانعی برای فراهم کردن راهبری مؤثر باشد. این حسابرس فناوری اطلاعات است که باید این‌گونه مسأله‌ها را با مدیران ارشد و در مواردی با هیأت مدیره مطرح کند.

همه عوامل بازدارنده‌ی راهبری فناوری اطلاعات را هرگز نمی‌توان فهرست کرد، اما موارد زیر در بیشتر سازمان‌ها رایج است:

- **مشارکت نداشتن مدیریت ارشد در فناوری اطلاعات:** مسأله مهمی که مانع موفقیت پروژه‌های فناوری اطلاعات می‌شود این است که مدیریت ارشد به مشارکت دادن فناوری اطلاعات در فرایند تصمیم‌گیری تمایلی ندارد. مدیریت هنگام برنامه‌ریزی برای سرمایه‌گذاری‌های عمده در فناوری اطلاعات باید با بخش فناوری اطلاعات خود همکاری تنگاتنگ داشته باشد تا مطمئن شود که دانش و بازخورد لازم برای تصمیم‌گیری‌های مناسب، در اختیار آن قرار گرفته است.

- **همسویی ضعیف راهبردی:** از سرمایه‌گذاری‌های عمده فناوری اطلاعات که به‌گونه‌ای راهبردی با هدف‌ها و منابع سازمان هماهنگ نیست، ممکن است ارزش سازمانی صفر یا اندک به دست آید. چنین همسویی ضعیف راهبردی بدین معناست که فناوری اطلاعات ممکن است به‌طور کارآمد و اثربخش در دستیابی به هدف‌های سازمان سهیم نباشد.

- **نپذیرفتن مالکیت پروژه:** بسیاری از پروژه‌های فناوری اطلاعات در گذشته تنها در اختیار بخش فناوری اطلاعات بود و مدیریت ارشد کوشش می‌کرد مالکیت چنین پروژه‌هایی را به عهده نگیرد. نبود رهبری روشن از سوی مدیران ارشد، پروژه فناوری اطلاعات را در ادغام هدف‌های خود با هدف‌های کلی سازمان، با ریسک عدم موفقیت رو به‌رو می‌سازد. مدیریت در بیشتر موارد، **"مسئولیت"** را به بخش فناوری اطلاعات منتقل می‌کند که به عدم یکپارچگی و همسویی فناوری اطلاعات با هدف‌های کلی سازمان منجر می‌شود. این موضوع، ناکارآمدی‌های زیادی را پدید می‌آورد که مدیران فناوری اطلاعات معمولاً به خاطر آن سرزنش می‌شوند.

- **مدیریت ضعیف ریسک:** برای موفقیت بیشتر پروژه‌های فناوری اطلاعات، مدیریت ضعیف ریسک یک محدودیت عمده است. **"رویکرد نگرش مدیریت ریسک"** با ارزیابی و کاهش همه تهدیدهای احتمالی پروژه سروکار دارد. چنانچه با این مسأله‌ها در شروع و ادامه پروژه برخورد نشود، به احتمال بسیار زیاد، شکست به وجود می‌آید. اغلب، آسیب‌رسان‌ترین ریسک‌های فناوری اطلاعات، آنهایی هستند که توسط مدیران ارشد به‌خوبی درک نشده‌اند.

- **مدیریت ناکارآمد منابع:** یک سازمان برای دستیابی به نتایج مطلوب با کمترین هزینه باید منابع فناوری اطلاعات خود را به‌گونه‌ای اثربخش و کارآمد مدیریت کند. کلید دستیابی به ارزش سرمایه‌گذاری در فناوری اطلاعات، اطمینان یافتن از وجود منابع کافی فنی، سخت‌افزاری، نرم‌افزاری و مهم‌تر از همه، انسانی برای ارائه خدمات فناوری اطلاعات است.

۴. برخی از بهترین نحوه عمل‌های کلیدی هنگام ارزیابی اثربخشی راهبری فناوری اطلاعات در یک سازمان توسط حسابرس سیستم‌های اطلاعاتی

پیاده‌سازی ساختار سازمانی، شامل چارچوب راهبری مؤثر، با وظیفه و مسئولیت‌های به‌خوبی تعریف شده برای ذینفعان فناوری اطلاعات، از جمله حسابرسان سیستم‌های اطلاعاتی، بهترین نحوه عمل کلیدی است. چنین چارچوبی از هم‌راستایی سرمایه‌گذاری‌های فناوری اطلاعات با هدف‌ها و راهبردهای سازمان و ارائه

خدمات مورد نظر، اطمینان می‌دهد. اگرچه بسیاری از سازمان‌ها اهمیت راهبری فناوری اطلاعات را در نظر نمی‌گیرند، اما بدون این چارچوب، پروژه‌های فناوری اطلاعات بیشتر در معرض شکست هستند. چنین سازمان‌هایی بدون درک کامل از الزامات سازمانی پروژه و چگونگی ارتباط آن با هدف‌های سازمان، پروژه‌های فناوری اطلاعات را اجرا می‌کنند.

یکی دیگر از بهترین نحوه عمل‌های کلیدی برای مدیریت فناوری اطلاعات، شناسایی هدف‌های سازمانی برای فناوری اطلاعات است. در گذشته، مدیران ارشد، پروژه‌های فناوری اطلاعات را با دید محدود هدف‌های ورودی و خروجی نگاه می‌کردند. این دیدگاه ناکارآمد و غیر اثربخش مستقیماً ناشی از نداشتن تجربه فنی این مدیران برای برخورد با پیچیدگی چنین پروژه‌هایی بود. افزون بر این، به دلیل ناکارآمدی زیاد ناشی از عدم موفقیت سازمان در یکپارچه‌سازی هدف‌های پروژه‌های فناوری اطلاعات با هدف‌های کلی سازمان، این مدیران به ناحق مقصر شناخته می‌شدند.

یک سازمان برای موفقیت باید همه عوامل زیر را که به بهترین نحوه عمل‌ها منجر می‌شود، در نظر بگیرد: چارچوب سطح بالا، اطمینان بخشی مستقل، گزارشگری عملکرد مدیریت، مدیریت منابع، **"رویکرد نگرش مدیریت ریسک"**، همسویی راهبردی و ارزش افزایی:

چارچوب سطح بالا: شامل تعریف رهبری و هدایت، فرآیندها، وظیفه‌ها و مسئولیت‌ها، الزامات اطلاعاتی و ساختارهای سازمانی- از هم‌راستایی سرمایه‌گذاری فناوری اطلاعات با راهبردهای کلی سازمان و حداکثرسازی استفاده از فرصت‌های فناوری اطلاعات موجود اطمینان می‌دهد.

اطمینان بخشی مستقل: حسابرسی مستقل و داخلی می‌تواند بازخورد به‌موقع در مورد انطباق فناوری اطلاعات با سیاست‌ها، استانداردها، رویه‌ها و هدف‌های کلی سازمان را تأمین کند. این رسیدگی‌ها باید به‌صورت بی‌طرفانه و واقعی انجام شوند، به‌گونه‌ای که ارزیابی منصفانه‌ای از پروژه فناوری اطلاعات مورد رسیدگی به مدیران ارائه شود.

مدیریت منابع: از طریق ارزیابی‌های منظم، از برخورداری فناوری اطلاعات از منابع کافی، شایسته و کارآمد برای برآوردن نیازهای سازمان اطمینان می‌دهد.

رویکرد نگرش مدیریت ریسک: "رویکرد نگرش مدیریت ریسک" در مسئولیت‌های مدیریت سازمان و ارزیابی‌های منظم و گزارش ریسک‌ها و آثار سازمانی مربوط به فناوری اطلاعات، گنجانده شده است. هر مشکلی که پیش آید، پیگیری می‌شود و به هرگونه اثر منفی احتمالی بر هدف‌های کلی سازمان، توجه ویژه‌ای می‌شود.

همسویی راهبردی: درک مشترک بین مدیریت سازمان و بخش فناوری اطلاعات، هیأت مدیره و مدیریت ارشد را به درک مسأله‌های راهبردی فناوری اطلاعات قادر می‌سازد. راهبرد فناوری اطلاعات، بینش‌ها و قابلیت‌های فناوری سازمان را نشان می‌دهد و از هم‌راستایی سرمایه‌گذاری فناوری اطلاعات با راهبردهای کلی سازمان و استفاده بهینه از فرصت‌های فناوری اطلاعات موجود، اطمینان می‌دهد.

ارزش‌آفرینی: مزایایی را که می‌توان از سرمایه‌گذاری در فناوری اطلاعات بدست آورد نشان می‌دهد. این سرمایه‌گذاری باید همیشه برای سازمان ارزش‌آفرین و بر اساس نیازهای سازمان سرمایه‌گذار باشد.

۵. مدیریت عملکرد

معیارهای عملکرد، اساس ساختار راهبردی فناوری اطلاعات است. برای اینکه سازمان از راهبری خوبی برخوردار باشد باید بداند که ارزش‌آفرینی واقعی سرمایه‌گذاری‌های فناوری اطلاعات در کجاست. وجود مجموعه‌ای دقیق از معیارهای عملکرد، ابزارهایی را برای اندازه‌گیری موفقیت در اختیار مدیران قرار می‌دهد و زمینه‌های نیازمند تمرکز برای بهبود اثربخشی و کارایی سرمایه‌گذاری‌های فناوری را تعیین می‌کند.

معیارهای عملکرد، شامل شاخص‌های کلیدی عملکرد، سازمان را در درک تناسب عملکرد با آرمان‌ها و هدف‌های راهبردی یاری می‌رساند.

حسابرس فناوری اطلاعات از همین معیارها برای اطمینان یافتن از کافی و مناسب بودن اقدامات مدیریت در برخورد با مشکلات استفاده می‌کند. بدون وجود معیارهای عملکردی، ارزیابی میزان پیشرفت در دستیابی به هدف‌های فناوری اطلاعات دشوار خواهد بود.

نمونه‌هایی از معیارهای راهبری مورد استفاده سازمان‌ها به شرح زیر است:

تعداد کارکنان فناوری اطلاعات: سازمان چگونه ارزشِ افزوده هر فعالیت را در مقایسه با میزان منابع به‌کار گرفته شده اندازه‌گیری می‌کند.

نسبت‌های برون‌سپاری: سازمان چگونه اثربخشی کارکنان خود را تعیین می‌کند و به آنان اجازه می‌دهد تا میزان وابستگی خود را به منابع برون‌سازمانی بسنجند.

در دسترس بودن سیستم: در مقایسه با ساعات استاندارد هفتگی، سیستم چند ساعت در هفته در دسترس است.

میانگین زمانی بین شکست‌ها[1]: میانگین زمانی بین شکست‌ها چقدر است؟

میانگین زمان تعمیر: معیار اصلی قابلیت استفاده قطعات تعمیری چیست (می‌تواند نشان‌دهنده متوسط (میانگین) زمان مورد نیاز برای تعمیر قطعه یا دستگاه خراب باشد).

۶. پرسش‌های کلیدی که حسابرس فناوری اطلاعات باید هنگام حسابرسی راهبری فناوری اطلاعات به آنها پاسخ دهد، کدامند؟

پرسش کلی: آیا ساختارها و فرآیندهای رهبری و سازمانی لازم برای دستیابی به هدف‌های شرکت و پشتیبانی از راهبرد سازمان وجود دارد؟ (منبع: WGITA)

رهبری و سازمان: آیا ساختار سازمانی فناوری اطلاعات و مدیریت منابع انسانی آن از راهبردها و هدف‌های سازمان پشتیبانی می‌کند؟

راهبرد فناوری اطلاعات: آیا راهبرد فناوری اطلاعات، از جمله سمت‌وسوی فناوری اطلاعات و فرآیندهای تدوین راهبرد، تصویب، اجرا و نگهداری راهبرد، با راهبردها و هدف‌های سازمان هماهنگ است؟

سیاست‌ها و رویه‌ها: آیا سیاست‌ها، استانداردها و رویه‌های فناوری اطلاعات و فرایندهای تدوین، تأیید، اجرا، نگهداری و نظارت بر آنها برای پشتیبانی از راهبرد فناوری اطلاعات و رعایت الزامات قانونی و مقرراتی وجود دارد؟

سیستم مدیریت کیفیت: آیا سیستم مدیریت کیفیت فناوری اطلاعات برای پشتیبانی از راهبردها و هدف‌های سازمان وجود دارد؟

کنترل‌های فناوری اطلاعات: آیا مدیریت فناوری اطلاعات، بر کنترل‌ها (برای مثال نظارت مستمر، اطمینان بخشی) برای پشتیبانی از سیاست‌ها، استانداردها و رویه‌های سازمان نظارت کافی وجود دارد؟

برنامه‌ریزی سرمایه‌گذاری: آیا منابع سرمایه‌گذاری، استفاده و تخصیص منابع فناوری اطلاعات، شامل معیارهای تعیین اولویت هماهنگ با راهبردها و هدف‌های سازمان، وجود دارد؟

انعقاد قرارداد: آیا راهبردها و خط‌مشی‌های انعقاد قرارداد فناوری اطلاعات و شیوه‌های مدیریت قرارداد برای پشتیبانی از راهبردها و هدف‌های سازمان وجود دارد؟

1. Mean Time Between Failures (MTBF)

رویکرد نگرش مدیریت ریسک: آیا شیوه‌های رویکرد نگرش مدیریت ریسک برای اطمینان یافتن از مدیریت درست ریسک‌های مربوط به فناوری اطلاعات سازمان، وجود دارد؟

نظارت و گزارشگری: آیا شیوه‌های نظارتی لازم برای ارائه اطمینان بخشی کافی و به‌موقع اطلاعات درباره عملکرد فناوری اطلاعات به هیأت مدیره و مدیریت اجرایی، وجود دارد؟

برنامه‌ریزی تداوم کسب‌وکار: آیا برنامه تداوم کسب‌وکار برای پشتیبانی از بازیابی منظم عملیات اصلی کسب‌وکار در دوره پدید آمدن اختلال در فناوری اطلاعات، وجود دارد؟

حسابرس باید در صورت پاسخ نامطلوب به هر یک از پرسش‌های بالا، کفایت کنترل‌های جبرانی را بررسی کند. در مواردی که کنترل‌های جبرانی وجود ندارد یا غیرمؤثر است باید نظر مشروط ارائه شود.

اصطلاحاتی که در فصل ۶ بر آن تأکید شده است:

راهبری فناوری اطلاعات (IT Governance)- بخشی جدایی‌ناپذیر از راهبری سازمان و شامل رهبری، ساختارها و فرایندهای سازمانی است که از حفظ و گسترش راهبردها و هدف‌های سازمان توسط فناوری اطلاعات، اطمینان می‌دهد.

عوامل بازدارنده‌ی راهبری فناوری اطلاعات (IT Governance Constraints): رایج‌ترین این عوامل در اکثر سازمان‌ها عبارتند از: مشارکت نداشتن مدیریت ارشد در فناوری اطلاعات، همسویی ضعیف راهبردی، نپذیرفتن مالکیت پروژه، مدیریت ضعیف ریسک، مدیریت ناکارآمد منابع.

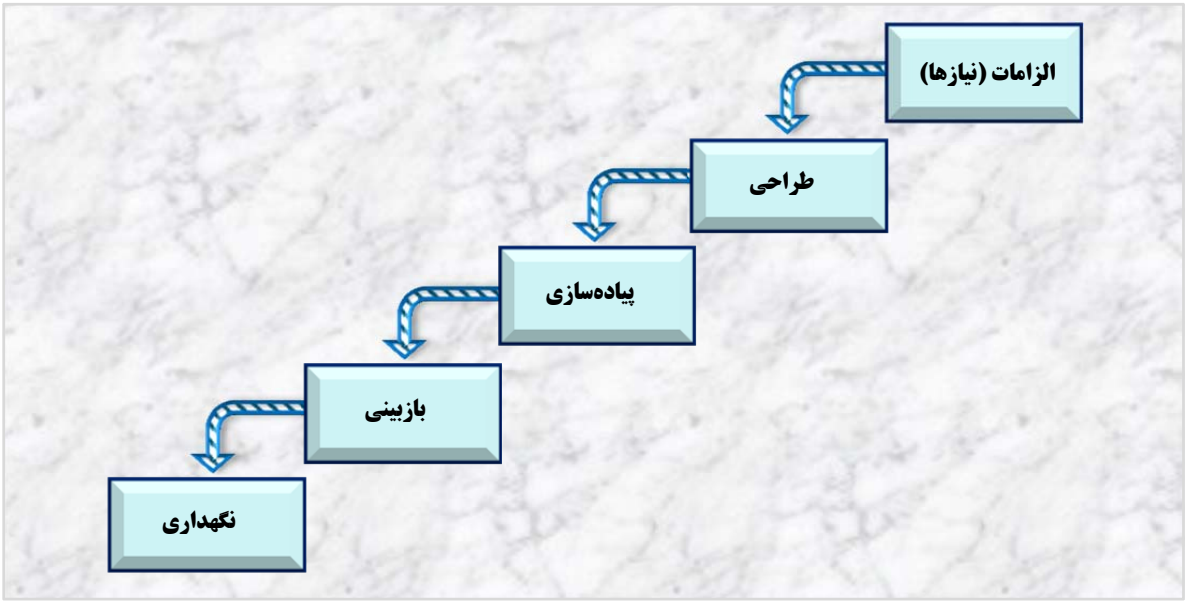
فصل ۷

حسابرسی خرید، تدوین و توسعه و نگهداری سیستم اطلاعاتی

چرخه عمر تدوین و توسعه سیستم[1] عبارت‌است از فرآیند مدیریت چرخه عمر توسعه یک سیستم تازه تدوین شده یا پیاده‌سازی سیستمی که به صورت آماده خریداری شده و با توجه به نیازهای سازمان، متناسب‌سازی شده است.

چرخه عمر تدوین و توسعه سیستم- یک متدولوژی یا یک روش تدوین سیستم است که در آن، سیستم به صورت گام به گام توسعه می‌یابد. بدینسان، مدیریت پروژه بر مدیریت گروه در استفاده از چرخه عمر تدوین و توسعه سیستم و دیگر ابزارها برای ایجاد محصول متمرکز است.

۱. گام‌های تدوین و توسعه سیستم



حسابرس فناوری اطلاعات باید توجه داشته باشد که این گام‌های مختلف می‌تواند به گام‌ها و طبقات جزئی‌تری نیز تقسیم یا در هم ادغام شوند.

1. System Development Life Cycle (SDLC)

۲. چرا حسابرسان فناوری اطلاعات باید درباره مراحل چرخه عمر تدوین و توسعه سیستم، آگاهی داشته باشند؟

حسابرس فناوری اطلاعات می‌تواند با بررسی فرایند تدوین و توسعه سیستم، از رعایت راهبردها و استانداردهای سازمانی در سیستم تدوین شده، اطمینان دهد. شناخت نقایص نرم‌افزارهای گوناگون، نشان داده است که تدوین و توسعه گام به گام نرم‌افزارها نسبت به تدوین یک مرحله‌ای آن‌ها اولویت دارد. هر مرحله، هدف‌های خاصی دارد و حسابرس فناوری اطلاعات باید از دستیابی مدیر پروژه به هدف‌های هر مرحله اطمینان بدست آورد. در غیر این صورت، به احتمال زیاد یک محصول نرم‌افزاری را تولید می‌کنند که نیاز کاربران را برآورده نمی‌کند یا حاوی اشتباه‌های بسیار است.

۳. محتوای هر مرحله از چرخه عمر تدوین و توسعه سیستم چیست؟

مراحل مختلف چرخه عمر تدوین و توسعه سیستم به شرح زیر است:

۳-۱. تعریف نیازهای کاربر

هدف‌های این مرحله عبارتند از: گردآوری و اولویت‌بندی نیازهای اولیه کاربر از دیدگاه ضعف (یا ضعف‌های) کسب‌وکار، تحلیل مقدماتی، ارزیابی و پیشنهاد راه‌حل‌های جایگزین، تشریح هزینه‌ها و منافع و ارائه یک برنامه اولیه برای رفع نیازهای نرم‌افزاری، سخت‌افزاری و سایر اقلام (مانند تغییر فرآیند).

حسابرسان در صورت رسیدگی به یک سیستم در جریان تدوین و توسعه باید این مرحله را (با دستاوردهای مورد انتظار و مستندات نیازمندی‌ها) به‌دقت بررسی کنند تا مطمئن شوند که سازمان، سیستم و نیازمندی‌ها را به‌خوبی درک کرده است.

۳-۲. تجزیه‌وتحلیل سیستم‌ها و تعریف پیش‌نیازهای سیستم

هدف از این مرحله عبارت است از: تفکیک بخش‌های سخت‌افزاری و نرم‌افزاری به اجزای قابل مدیریت، تعریف تفصیلی پیش‌نیازهای هر یک، تعیین رابط‌های برون و درون‌سازمانی سیستم، شناسایی ذینفعان مربوط، مهارت‌ها و ابزارهای مورد نیاز برای تدوین سیستم، طراحی برنامه زمانی، از جمله شناسایی ریسک‌های برنامه. یک نشست **"بررسی نیازمندی‌ها"** را برای اطمینان یافتن از اینکه ذینفعان و کاربران، نیازمندی‌ها را درک می‌کنند، برگزار کنید و در پایان آن، مجموعه الزاماتی که سیستم پیاده‌سازی خواهد کرد را به تصویب برسانید.

حسابرسان همچنین باید خروجی نهایی این مرحله را از دید این‌که ذینفعان، در تدوین الزامات و روند تأیید آنها مشارکت دارند، به‌دقت بررسی کنند.

۳-۳. طراحی سیستم

هدف از این مرحله، در نظر گرفتن اجزای مختلف سیستم و طراحی راه‌حل‌های تفصیلی، شامل طرح صفحه نمایش، قواعد کسب‌وکار، نمودار فرآیندها، کدهای ساختگی و سایر مستندات است. طراحی سیستم را بررسی و یک نشست بررسی اولیه و تفصیلی طراحی را برای کسب مشارکت و موافقت ذینفعان با آن، برگزار کنید.

۳-۴. پیاده‌سازی (توسعه)

در این مرحله، توسعه‌دهنده (تدوین‌کننده) سیستم، بخش‌های مختلف را کدنویسی می‌کند، بررسی دوباره را انجام می‌دهد و کدهای هر قسمت را، شامل آزمون رگرسیون در صورت استفاده تکراری از برخی کدها توسط منابع دیگر، می‌آزماید.

حسابرسان سیستم‌های اطلاعاتی ممکن است در این مرحله به‌طور مستقیم ورود نکنند اما، می‌توانند نتایج آزمون‌های بخش و رگرسیون را بازبینی کنند. از نظر اخلاقی حسابرسان نمی‌توانند سیستمی را که خودشان ایجاد کرده‌اند، حسابرسی نمایند.

۳-۵. بازبینی و اعتبار سنجی (آزمون)

یکپارچه‌سازی و آزمون: در این مرحله همه بخش‌های مختلف سیستم (نرم‌افزار، سخت‌افزار، ابزار آزمون و غیره) مورد آزمایش قرار می‌گیرند تا از برآورده شدن الزامات اطمینان حاصل شود.

حسابرس سیستم‌های اطلاعاتی در این مرحله باید نتایج آزمون‌ها یا خروجی‌ها را بازبینی کند.

۳-۶. پذیرش، استقرار، گسترش

در این مرحله است که نرم‌افزار در محیط تولید آزمایشی قرار می‌گیرد و توسط کاربران، آزمون می‌شود و پس از قبولی در آزمون پذیرش بر اساس معیارهای سازمانی، نرم‌افزار به‌کار گرفته می‌شود.

حسابرس باید مستندسازی آزمون پذیرش کاربر را بررسی کند. چنانچه از محیط آزمایشی و نه یک محیط تولیدی برای آزمون استفاده شده باشد، حسابرس می‌تواند مستندسازی را بازبینی کند.

۳-۷. نگهداری

این مرحله معمولاً آخرین مرحله است و به‌طور کلی شامل به‌روزرسانی‌ها و رفع مشکلات دوره‌ای نرم‌افزار یا سیستم است تا اطمینان حاصل شود که سیستم، هدف‌های تجاری سازمان را برآورده می‌سازد. گروه تدوین‌کننده سیستم برای مرحله نگهداری نیز از همان مدلی استفاده می‌کنند که برای تدوین و توسعه اولیه استفاده کرده‌اند. با این وجود، اگر تعداد تغییرات به نسبت اندک یا به منابع

زیادی احتیاج نداشته باشد، گروه اجرایی ممکن است مجموعه‌ای از مراحل فشرده‌تر را برای نگهداری انتخاب کند. یکی از نگرانی‌های اصلی در این مرحله این است که سازمان متوجه شود که مستندات کافی از اشتباه‌های ثابت نرم‌افزار در محصول وجود ندارد.

یادآوری می‌شود که یک سازمان می‌تواند یک سیستم آماده را انتخاب کند و بخرد که در این صورت، ممکن است به نسخه‌های جدیدتر همان سیستم که در دست توسعه است دسترسی پیدا نکند.

به‌هرحال، حسابرس سیستم‌های اطلاعاتی باید فرآیند خرید را بررسی کند تا از برآورده شدن الزامات و نیازهای سازمان، مالکان سیستم و نیازهای کاربران اطمینان یابد و همچنین، به‌روز بودن نسخه مورد استفاده را بازبینی کند.

اطلاعات بیشتر در مورد عملیات فناوری اطلاعات، شامل نگهداری سیستم‌های فناوری اطلاعات، در فصل آتی آورده شده است.

۴. مروری بر مدل‌های چرخه عمر تدوین و توسعه سیستم

دو مدل چرخه عمر تدوین توسعه سیستم که بسیار مورد استفاده قرار می‌گیرند عبارتند از:

- مدل آبشاری[1]، و
- مدل اسپیرال[2].

بیشتر سازمان‌ها از دو مدل بالا برای تدوین سیستم‌های خود استفاده می‌کنند. با این‌حال، برای پروژه‌های مبتنی بر وب یا پروژه‌هایی که به زمان گردش سریع‌تری نیاز دارند، مدل تدوین چابک استفاده می‌شود. زیرا محصول کار را زودتر از دو مدل بالا در اختیار کاربران قرار می‌دهد.

۴-۱. مدل آبشاری

مدل آبشاری برای تدوین و توسعه نرم‌افزار یا سیستم‌ها یک فرایند تکرارشونده از الزامات، نمونه‌های اولیه و بهبود آن‌ها است. در این مدل، فرض بر این است که تدوین و توسعه هر مرحله، پیش از انتقال به مرحله بعدی، تکمیل می‌شود و شروع فاز بعدی تنها در صورت تکمیل فاز پیش از آن امکان‌پذیر است. این فرض در دنیای واقعی چندان واقع‌بینانه نیست و در عمل، مواردی کشف شده که لازم است به‌طور مرتب بخش‌هایی از نرم‌افزار، دوباره توسعه یابد[3].

1. Waterfall Model
2. Spiral Model
۳. مشکل بزرگ این روش این است که اگر از یک مرحله توسعه رد شویم و اشتباهی مربوط به آن مرحله را کشف کنیم نمی‌توانیم به مرحله پیش بازگردیم و باید تا آخر کار ادامه دهیم به امید آنکه در به‌روز رسانی آتی نرم‌افزار، آن اشتباه برطرف گردد.

۴-۲. مدل اسپیرال

درحالی‌که مدل آبشاری، مسیر تدوین و توسعه را به صورت خطی و از ابتدا تا پایان از طریق طی مراحل تعریف شده (تعریف الزامات سیستم تا آزمون آن) در نظر می‌گیرد، ازسرگیری یک مرحله یا بخشی از آن، تصحیح و اصلاح آن همزمان با تدوین مرحله را مدل اسپیرال امکان‌پذیر می‌کند. هر نسخه از نرم‌افزار در این مدل، چرخه نسخه پیشین را همزمان با افزودن قابلیت‌های بیشتر و بهبود مواد قبلی، تکرار می‌کند. کاربران و ذینفعان این مدل می‌توانند سیستم کاربردی را خیلی زودتر از مدل آبشاری مشاهده کنند اما ممکن است عملکرد سیستم هنوز کامل نشده و محدود باشد.[۱]

۴-۳. مدل چابک

تدوین مدل‌های آبشاری و اسپیرال بسیار وقت‌گیر می‌باشد و بسته به‌اندازه سیستم، کاربران مجبورند ماه‌ها یا حتی بیشتر صبر کنند تا محصول کار را ببینند. اما در مدل چابک، نرم‌افزار کاری در زمانی به کوتاهی سی روز در اختیار کاربران قرار می‌گیرد. به هرحال، نرم‌افزار اولیه تحویل شده، معمولاً در سی روز، امکان افزودن الزامات (نیازمندی‌های) جدید یا درخواست انجام تغییرات در نسخه تحویلی را برای کاربران فراهم می‌کند.

روش تدوین و توسعه نرم‌افزار چابک، بیشتر بر تحویل نرم‌افزارهای کاری (کاربردی) تأکید دارد تا مستندسازی جامع و کامل. در مدل چابک، گروه تدوین‌کننده، مراحل طراحی، پیاده‌سازی و بازبینی تدوین سیستم را در بازه زمانی سی‌روزه ترکیب می‌کند [۲]و در پایان این دوره، محصول را تحویل می‌دهد.

۴-۳-۱. اصطلاحات مورد استفاده در سیستم چابک

اسکرام[۳] روشی است که مدل چابک را پیاده‌سازی می‌کند. روش اسکرام همه مراحل معمول تدوین و توسعه نرم‌افزار (نیازها، طراحی، توسعه و آزمون) را در یک دوره سی‌روزه، فشرده می‌کند. در اسکرام، بازه زمانی، مراحل انجام هر کار و فازهای کاری تعریف می‌شود و به تیم تدوین‌کننده، مجموعه‌ای از نیازهای سازمان که به زبان فنی بیان شده است داده می‌شود که در سی روز آینده انجام دهند.

---

۱. کسب و کارهایی که در مورد الزامات خود مطمئن نیستند یا انتظار تغییرات اساسی در طول پروژه‌های پر ریسک خود را دارند، می‌توانند از مقیاس‌پذیری این روش استفاده کنند.

2. Sprint: Sprint معمولاً یک دوره دو تا چهار هفته‌ای است (طول دوره را گروه تدوین‌کننده مشخص می‌کند) اعضا، یک محصول بالقوه قابل ارائه و قابل استفاده را تدریجاً تولید می‌کنند (م).

3. Scrum.

نام‌های سنتی	نام‌ها در اسکرام
الزامات (نیازها)	Product Backlog[1], Sprint Backlog[2]
برنامه‌ریزی	Sprint Planing
مرحله تدوین و توسعه	Sprint
نشست‌ها	Daily Scrum[3]
ردیابی پروژه	Burn Down[4]
تحویل نرم‌افزار	Build /Release/ Increment[5]

۲-۳-۴. شرایط اسکرام

الزامات و نیازهای سازمان

لیستی از الزامات و نیازهای مربوط به محصول است که توسط سازمان براساس موضوع‌هایی مانند ریسک، ارزش کسب‌وکار، وابستگی‌ها و تاریخ مورد نیاز سازمان، تعیین یا اولویت‌بندی شده است.

نشست‌های برنامه‌ریزی

در ابتدای هر اسپرینت، یک نشست برنامه‌ریزی برگزار می‌شود تا نسبت به انتقال نیازهای سازمان به اسپرینت، تصمیم‌گیری شود.

الزامات و نیازهای سازمان در اسپرینت

لیست کارهایی است که گروه تدوین‌کننده باید در اسپرینت انجام دهد. به بیان دیگر، نیازهای سازمان به زبان فنی مورد فهم اعضای گروه تبدیل می‌شود. گروه تدوین‌کننده در طول سی روز کاری اسپرینت با کاربران سیستم تعامل برقرار می‌کند تا از برآورده شدن نیازهای آنان توسط محصول نهایی، اطمینان بدست آید. در درون گروه، وظایف بین اعضا تقسیم می‌شوند. معمولاً هر گروه مسئول، از یک اسپرینت به اسپرینت بعدی می‌رود.

---

۱. اصطلاح Product Backlog نامی است که به بانک اطلاعاتی نیازهای عملیاتی و غیرعملیاتی کل یک پروژه گفته می‌شود و در حقیقت، مجموعه‌ی اولویت‌بندی شده از نیازمندی‌های سطح بالای سیستمی است که سرانجام باید تحویل داده شود (م).

۲. Sprint Backlog : مواردی از Product Backlog که قرار است در یک Sprint انجام شود را اصطلاحاً Sprint Backlog می‌نامند. مفاد Sprint Backlog در واقع توافقی است بین اعضای تیم و سازمان که بعد از تصویب شدن مفاد یک sprint، هیچ‌کس نمی‌تواند آن را در طول sprint تغییر دهد. در طول دوره، نیازمندی‌های لحاظ شده در Sprint Backlog از Product Backlog حذف می‌شوند. اما امکان دارد به دلایلی، این نیازمندی‌ها دوباره به Product Backlog برگردند (م).

۳. نشست گروهی برای مشورت درباره مراحل کار.

۴. ردیابی پیشرفت کار و پیش‌بینی زمان پایان پروژه.

۵. اجرا، تحویل و افزایش.

اسکرام روزانه (نشست)

نشست روزانه اعضای گروه برای بحث درباره مسأله‌های مربوط به کار را اسکرام روزانه[1] می‌گویند. همه می‌توانند در این نشست حضور داشته باشند، اما تنها گروه اصلی، اجازه صحبت دارد. این نشست به‌طور کلی حدود پانزده‌دقیقه طول می‌کشد و به آنچه‌در روز گذشته انجام شده است، آنچه امروز انجام خواهد شد و مسأله‌هایی که باید برطرف شود، می‌پردازد.

اسپرینت سی‌روزه[2] (تدوین)

اسپرینت، واحد اساسی تدوین و توسعه در اسکرام است. اسپرینت‌ها می‌توانند بین یک هفته تا یک ماه باشند اما به‌طور معمول، سی روز طول می‌کشند. آنها برنامه زمانی بسته[3] هستند که مدت زمان آن‌ها به‌طور معمول تمدید نمی‌شود و اسپرینت، حداکثر در پایان سی روز به پایان می‌رسد.

نظارت بر پروژه

نمودار بررسی پیشرفت کار اسپرینت، نموداری است که کارهای باقی‌مانده تعریف شده را به ما نشان می‌دهد. این نمودار به صورت روزانه، به‌روز می‌شود و دیدی ساده (روشن) از میزان پیشرفت اسپرینت می‌دهد که منبع خوبی برای بررسی سریع وضعیت پیشرفت اسپرینت نیز می‌باشد.

تدوین، تحویل، افزودنی‌ها

افزودنی‌ها عبارت است از جمع همه اقلام کامل شده در طول اسپرینت و اسپرینت‌های پیشین. در پایان یک اسپرینت، افزودنی‌ها باید طبق تعریف گروه اسکرام از انجام کار باشد (این باید تعریف شود اما عموماً شامل کد (هایی) است که فعال، آزمون شده و بدون اشتباه است).

۵. چرا حسابرسان باید از مدل‌های چرخه عمر تدوین و توسعه سیستم آگاهی داشته باشند؟

تا اینجا، مراحل چرخه عمر تدوین و توسعه سیستم را بحث کرده‌ایم. اما، یک حسابرس فناوری اطلاعات باید بداند که مدل‌های توسعه سیستم، راهی برای پیاده‌سازی مراحل مختلف چرخه عمر تدوین و توسعه سیستم است. مدل‌ها، ریسک‌های خاصی دارند که مدیر برنامه (ناظر بر فرایند چرخه عمر تدوین و توسعه) باید با آن‌ها برخورد کند. حسابرس با استفاده از پرسش‌های مربوط به حسابرسی می‌خواهد اطمینان حاصل کند که مدیر برنامه، این ریسک‌ها را به‌گونه‌ای مؤثر مدیریت می‌کند.

1. Daily Scrum
2. 30 Day Sprint
3. Timeboxed

۶. نکاتی برای حسابرسان فناوری اطلاعات

حسابرسان باید روش‌های متداول تدوین و توسعه سیستم رایج را بشناسند تا بتوانند یک سیستم اطلاعاتی در دست تدوین را حسابرسی کنند. مراحل تدوین و توسعه سیستم و ریسک‌های هر یک به همراه پرسش‌های مربوط به حسابرسی (رویکرد نگرش مدیریت ریسک توسعه سیستم) در جدول زیر آورده شده است:

مرحله توسعه سیستم	شرح ریسک	پرسش‌های مربوط به حسابرسی
الزامات و نیازهای کاربر	❖ **توصیف، بررسی و تحلیل نشدن الزامات به‌اندازه کافی.**	❖ آیا الزامات شما برای این پروژه، مستند شده است؟ ❖ چه کسی مجموعه الزامات را بررسی می‌کند؟ ❖ چه کسی مجموعه الزامات را تأیید کرده است؟ ❖ فرایند شما برای مدیریت تغییرات در الزامات پایه چیست؟
	❖ **برای تبیین نیازها، از کاربران سیستم مشورت گرفته نمی‌شود.**	❖ چگونه اطمینان حاصل می‌کنید که نیازهای کاربران در الزامات یک سیستم گنجانده شده است؟
طراحی	❖ **طراحی نامشخص، بررسی نشدن طراحی.**	❖ اگر طرح، به دلیل الزامات مبهم، انجام نشدنی باشد، فرایند شما برای اصلاح الزامات چیست؟ ❖ چه کسی خارج از گروه نرم افزاری، طراحی سیستم را بررسی می‌کند؟ ❖ چگونه طراحی سیستم برای کاربران و سایر ذینفعان توضیح داده شده است؟
پیاده‌سازی	❖ **اشتباه ایجاد شده توسط برنامه‌نویسان، توابع نادیده گرفته شده، مطابق نبودن با استانداردهای تعیین شده.**	❖ روند شما برای یافتن اشتباه‌های کدنویسی در هنگام توسعه نرم‌افزار، چیست؟ ❖ چگونه از پیاده‌سازی توابع مورد نیاز تعیین شده توسط مدیر برنامه توسط برنامه نویسان، اطمینان می‌یابید؟ ❖ رابط‌های سخت‌افزاری و نرم‌افزاری خود را در کجا مستند می‌کنید (برای ورودی‌ها، خروجی‌ها، انتقال داده‌ها و غیره).

مرحله توسعه سیستم	شرح ریسک	پرسش‌های مربوط به حسابرسی
بازبینی و اعتبارسنجی (آزمایش کردن)	❖ عملکرد از دست رفته، ❖ آزمایش کردن‌های ناکافی، ❖ نبود معیار موفقیت.	❖ چگونه از ردیابی الزامات تأیید شده در طراحی و آزمایش سیستم اطمینان می‌یابید؟ ❖ چه کسی برنامه آزمون شما را تأیید می‌کند؟ ❖ آیا کاربران نیز در مرحله آزمون شما شرکت دارند؟ ❖ چه شاخصی مثبت یا منفی بودن یک آزمون را تعیین می‌کند؟
نگهداری	❖ نبود مستندات کافی.	❖ مستندات پروژه را در کجا نگهداری می‌کنید؟ ❖ چگونه از کافی بودن مستندات و انعکاس کارکرد نرم‌افزار، اطمینان می‌یابید؟
	❖ نبود مهارت برای حفظ و نگهداری.	❖ آیا گروه شما مهارت لازم برای حفظ و نگهداری نرم‌افزار را دارد؟
	❖ محصول، بیش از اندازه. ❖ تغییرات در محصول.	❖ چگونه تغییراتی که در این نرم‌افزار ایجاد خواهید کرد را اولویت‌بندی می‌کنید؟
مدل چابک	❖ مستندات.	❖ چگونه از مطابقت مستندات شما با محصول تحویل داده شده اطمینان می‌یابید؟
	❖ آزمایش کردن.	❖ چگونه از آزمایش کافی نرم‌افزار، توسط گروه خود اطمینان می‌یابید؟
	❖ تکمیل پروژه.	❖ از کجا می‌دانید محصول در چه زمانی کامل می‌شود؟ ❖ الزامات سیستم در کجا مستندسازی شده است؟
	❖ فروشنده، نرم‌افزار را تحویل نمی‌دهد.	❖ چه اتفاقی رخ می‌دهد اگر گروه پیاده‌کننده مدل توسعه نتوانند در زمان مقرر (سی یا چهل‌روزه) و مطابق با چارچوب زمانی سیستم، محصول را تحویل دهند؟

۷. نقشی که حسابرس فناوری اطلاعات می‌تواند در پیاده‌سازی سیستم‌ها داشته باشد

ازآنجا که دولت به‌گونه‌ای روزافزون از سیستم‌های اطلاعاتی استفاده می‌کند، منابع مصرف شده برای این سیستم‌ها بسیار هنگفت است. تعداد بسیاری از ضعف‌ها و شکست‌های سیستم، نتیجه‌ی شیوه‌های بد پیاده‌سازی آن است و نقش داشتن حسابرسان فناوری اطلاعات در طول پیاده‌سازی سیستم‌های اطلاعاتی از اهمیت برخوردار است. با این وجود، حسابرسان باید مراقب باشند نقشی را ایفا نکنند که توانایی حسابرسی آن سیستم خاص را از خود سلب کنند؛ برای مثال، نقش داشتن در طراحی و کنترل.

برخی از نقش‌هایی که حسابرس می‌تواند برای اطمینان از تکمیل و پیاده‌سازی موفقیت‌آمیز هر سیستم جدید ایفا کند، عبارت است از:

- **شناسایی آسیب‌پذیری‌های احتمالی و نقاط نیازمند کنترل:**
  - در زمینه تدوین چرخه عمر برنامه کسب‌وکار
  - این کار، تلاش برای اطمینان یافتن از طراحی و پیاده‌سازی کنترل‌های مناسب در سیستم جدید را آسان می‌کند.
- **نقش حسابرس در مشاوره دادن به گروه پروژه درباره نارسایی‌های کنترل‌ها، فعالیت‌های مربوط به کنترل‌ها یا فرآیندهای مناسب برای پیاده‌سازی و پیگیری.**

این نقش‌ها می‌توانند به‌صورت زیر انجام شوند:

- حسابرس فناوری اطلاعات می‌تواند همه زمینه‌ها و مراحل تدوین و توسعه سیستم را بررسی و گزارش خود را درباره انطباق با هدف‌های برنامه‌ریزی شده و رویه‌های شرکت به طور مستقل به مدیریت ارائه کند.
- حسابرس فناوری اطلاعات می‌تواند بخش‌هایی خاص از سیستم را شناسایی و براساس مهارت و توانایی‌های شخصی خود، درگیر جنبه‌های فنی آن شود.
- حسابرس فناوری اطلاعات می‌تواند روش‌ها و فنون به‌کار رفته در تدوین و توسعه را ارزیابی کند.

حسابرسان می‌توانند از رهنمود کارگروه حسابرسی فناوری سیستم‌های اطلاعاتی[1] دیوان برای حسابرسی پیاده‌سازی سیستم‌ها استفاده کنند.

اصطلاحاتی که در فصل ۷ بر آن تأکید شده است

چرخه عمر تدوین و توسعه سیستم (*The System Development Life Cycle*) - یک متدولوژی یا یک روش تدوین و توسعه سیستم است که در آن، سیستم به‌صورت گام‌به‌گام تدوین می‌شود. بدینسان، مدیریت پروژه بر مدیریت گروه در استفاده از چرخه عمر تدوین و توسعه سیستم و دیگر ابزارها برای ایجاد محصول متمرکز است.

گام‌های تدوین و توسعه سیستم (*System Development Phases*) - گام‌های تدوین و توسعه سیستم، عبارتند از شناخت نیازها (الزامات)، طراحی، پیاده‌سازی، بازبینی و نگهداری که در این فصل تشریح شده‌اند. حسابرس فناوری اطلاعات باید توجه داشته باشد که این گام‌های مختلف می‌توانند به گام‌ها و طبقات جزئی‌تری نیز تقسیم یا در هم ادغام شوند.

1. WGITA: Working Group on Information Technology Audit

فصل ۸

عملیات فناوری اطلاعات و شاخص‌های کلیدی عملکرد آن

۱. عملیات فناوری اطلاعات کدامند؟

منظور از عملیات فناوری اطلاعات، فعالیت‌های روزانه سیستم‌های فناوری اطلاعات است که از فرآیندهای تجاری یک سازمان پشتیبانی می‌کنند.

این عملیات می‌تواند شامل موارد زیر، ولی نه محدود به این‌ها باشد:

- خرید یا تدوین سیستم‌های فناوری اطلاعات؛
- نگهداری، به‌روز رسانی و امنیت سیستم‌های فناوری اطلاعات (بانک‌های اطلاعاتی، برنامه‌ها و غیره) که به صورت درون‌سازمانی مدیریت یا برون‌سپاری می‌شوند؛
- بررسی و مستندسازی سیستم‌ها؛
- خط‌مشی‌ها، آموزش و پشتیبانی کاربر.

۲. شاخص کلیدی عملکرد چیست؟

شاخص‌های کلیدی عملکرد[1]، معیارهایی برای سنجش عملکرد فرآیند سازمان در دستیابی به هدف‌های تعیین شده است. این شاخص‌ها نشانه اصلی آن است که دستیابی به یک هدف، احتمالاً ممکن خواهد شد یا نه و معیار خوبی برای ارزیابی توانمندی‌ها، روش‌ها و مهارت‌ها نیستند. این شاخص‌ها، فعالیت‌ها و هدف‌هایی را اندازه‌گیری می‌کنند که صاحبان فرآیندها باید برای دستیابی به عملکرد کارآمد، اتخاذ نمایند.

برای تعریف معیارهای مربوط به شاخص‌های کلیدی عملکرد معناداری که با هدف‌های سازمان همسو باشد، پرسش‌های زیر باید پرسیده شود:

- معیارها یا الزامات تجاری و سازمانی کدامند؟
- این معیارها یا الزامات چگونه به معیارهای خدمات سیستم‌های اطلاعاتی تبدیل می‌شوند؟

---

1. Key Performance Indicators

- یک فرایند، چگونه از معیارهای خدمات فناوری اطلاعات پشتیبانی می‌کند؟
- چگونه می‌توان این موارد را گردآوری، تحلیل و اندازه‌گیری کرد؟

نمونه‌هایی از معیارهای شاخص کلیدی عملکرد و تعاریف و هدف‌های مربوط در زیر می‌آید:

فرآیند	هدف (عامل اصلی موفقیت)	شاخص کلیدی عملکرد	روش اندازه‌گیری
موافقت‌نامه سطح خدمات[1]	بهبود توانایی ردیابی و انجام سطوح خدمات توافق شده با مشتریان	درصد افزایش یا کاهش و تحقق هدف‌ها در سطح خدمات	پیگیری از طریق مدیریت بحران و گزارشگری ماهانه.
مدیریت تغییر (می‌تواند شامل مدیریت پَچ[2] نیز باشد)	کاهش وقایع ناشی از تغییرات غیرمجاز	درصد کاهش در تعداد وقایع ناشی از دسترسی غیرمجاز	پیگیری از طریق مدیریت بحران، مدیریت تغییر و گزارشگری ماهانه

توجه:

مدیریت پَچ ممکن است زیر نظر مدیریت تغییر قرار بگیرد؛ زیرا، این فرآیند شامل ایجاد تغییراتی (مانند اضافه‌کردن ویژگی‌ها) در یک سیستم است. از این‌رو، حسابرس فناوری اطلاعات باید تعریف شده، مناسب و پیاده‌سازی شده بودن سیاست‌ها، استانداردها و رویه‌های مدیریت پَچ را تعیین کند.

شاخص‌های کلیدی عملکرد باید بینش موارد زیر را ایجاد کنند:

- **کیفیت**- روند کار چقدر خوب است؟ آیا حرکت به سمت هدف‌هایی است که برای این فرآیند تعیین شده‌اند؟
- **کارایی**- آیا توان آمایش[3] فرآیند کافی است؟
- **سازگاری**- آیا این فرآیند پیگیری می‌شود؟
- **ارزش**- آیا آنچه که باید، انجام می‌شود؟

1. Service Level Agreement (SLA)

۲. Patch management : مدیریت پَچ، فرآیند توزیع و اعمال به‌روز رسانی برای نرم‌افزار است. پَچ‌ها (همانند وصله‌کاری) بیشتر برای تصحیح اشتباه‌ها در نرم‌افزار ضروری هستند (م).

3. Throughput

۳. چرا شاخص‌های کلیدی عملکرد برای حسابرس سیستم‌های اطلاعاتی مهم هستند و چگونه می‌توانند در حسابرسی فناوری اطلاعات استفاده شوند؟

با وجود اینکه شاخص‌های کلیدی عملکرد در زمینه مسئولیت مدیریت عملیات سیستم‌های اطلاعاتی هستند، درک این مسأله که حسابرس چگونه می‌تواند از این شاخص‌های کلیدی عملکرد در طول حسابرسی استفاده کند، مهم است. شاخص‌های کلیدی عملکرد می‌تواند در موارد پرسش درباره عملکرد عملیات سیستم‌های اطلاعاتی و شناسایی زمینه‌های بالقوه با اهمیت، مانند تعداد حوادث فناوری اطلاعات در هرماه که می‌تواند نشانه‌ای از بروز مشکلات در سیستم‌ها باشد، به حسابرس یاری رساند.

بررسی شاخص‌های کلیدی عملکرد حسابرس را در طرح پرسش مربوط به موارد زیر یاری می‌رساند:

- ❖ آیا سیستم‌ها به‌طور مؤثر و کارآمد عمل می‌کنند؟
- ❖ آیا مکانیسم‌هایی برای شناسایی ضعف در عملکرد، برخورد با ضعف‌های شناسایی شده و پیگیری انجام اقدامات اصلاحی حاصل از ارزیابی عملکرد سازمان، وجود دارد.
- ❖ عملکرد سازمان چگونه با سایر سازمان‌ها مقایسه می‌شود؟
- ❖ شناسایی مسأله‌های کنترلی در سازمان مورد حسابرسی و بدین ترتیب، کمک به تعیین نوع و ماهیت، زمان‌بندی اجرا و میزان آزمون‌ها.

۴. موافقت‌نامه‌های سطح خدمات درون‌سازمانی

۴-۱. توافق سطح خدمات درون‌سازمانی چیست؟

موافقت‌نامه‌ای است بین واحد فناوری اطلاعات و مالکان سازمان. پایبند نبودن به این توافق، بر دستیابی به نیازهای کاربران تأثیر می‌گذارد. عملیات سیستم‌های اطلاعاتی و صاحبان سازمان باید دستِ‌کم در مورد ارائه خدمات فناوری اطلاعات زیر توافق کنند:

- ❖ مدیریت ظرفیت
- ❖ مدیریت مالی فناوری اطلاعات
- ❖ مدیریت دسترسی

مدیریت ظرفیت با برنامه‌ریزی و نظارت بر محاسبات و منابع شبکه سروکار دارد تا از منابع موجود، به‌گونه‌ای مؤثر و کارآمد استفاده شود. این امر مستلزم آن است که افزایش یا کاهش منابع به‌موازات رشد یا کاهش کلی کسب‌وکار صورت گیرد.

مدیریت مالی فناوری اطلاعات با اطمینان یافتن از این سروکار دارد که سیستم‌های مالی، می‌توانند گزارش‌های مالی دقیق و به‌موقع را تولید کنند. سیستم باید طی دوره اوج کار در دسترس باشد و بتواند حجم زیادی از تراکنش‌ها را بدون ایجاد اختلال، پردازش کند. در دسترس نبودن سیستم ممکن است به از دست رفتن کسب‌وکار یا دست نیافتن به نتایج مورد انتظار شرکت منجر شود.

عملیات سیستم‌های اطلاعاتی و صاحبان سازمان نیز باید در مورد در دسترس بودن سیستم در طول دوره‌های مورد نیاز به توافق برسند؛ زیرا، در دسترس نبودن سیستم در موارد لزوم ممکن است بر کسب‌وکار، پردازش اطلاعات و گزارش تراکنش‌های مالی تأثیر مستقیم داشته باشد. بنابراین، زمان خرابی سیستم باید به حداقل برسد زیرا بر پردازش و گزارش تراکنش‌های مالی تأثیر می‌گذارد. حسابرس سیستم‌های اطلاعاتی باید هر توافقی را به‌منظور تعیین پردازش دقیق و یکنواخت داده‌های مالی (توسط سیستم) بررسی کند.

۲-۴. چرا موافقت‌نامه‌های سطح خدمات درون‌سازمانی برای حسابرسان سیستم‌های اطلاعاتی مهم است ؟

حسابرس سیستم اطلاعاتی می‌تواند از موافقت‌نامه سطح خدمات درون‌سازمانی برای بررسی توانایی عملیات سیستم‌های اطلاعاتی در ردیابی و دستیابی به سطح خدمات مورد توافق با کاربران استفاده کند. حسابرس سیستم‌های اطلاعاتی می‌تواند سطح خدمات واقعی را با سطح خدمات برنامه‌ریزی شده مقایسه و درصد افزایش یا کاهش در دستیابی به هدف‌های سطح خدمات را تعیین کند. برای مثال، اگر عملیات سیستم‌های اطلاعاتی و کاربران بر دسترسی ۹۷ درصدی موافقت کرده‌اند و دسترسی واقعی تنها ۷۰ درصد است، حسابرس سیستم اطلاعاتی باید آثار تحقق نیافتن هدف‌ها را از سازمان بپرسد. اگر تأثیر شدید باشد، حسابرس می‌تواند این موضوع را به عنوان یک زمینه بالقوه حسابرسی در نظر بگیرد.

حسابرس سیستم اطلاعاتی باید موافقت‌نامه سطح خدمات درون‌سازمانی را همانند شاخص‌های کلیدی عملکرد، بررسی کند. این موضوع حسابرس را در شناسایی موضوع‌های کنترلی مربوط به تعیین دامنه حسابرسی، یاری می‌رساند.

۵. موافقت‌نامه‌های سطح خدمات برون‌سازمانی

موافقت‌نامه سطح خدمات برون‌سازمانی، توافق‌نامه‌ای است بین واحد فناوری اطلاعات و پیمانکاران تجاری، ارائه‌کنندگان و یا مشاوران سازمان که ذینفعان برون‌سازمانی کسب‌وکار هستند. پایبند نبودن به موافقت‌نامه‌های سطح خدمات برون‌سازمانی بر دستیابی به نیازهای تجاری سازمان، تأثیر می‌گذارد.

ذی‌نفع برون‌سازمانی سیستم‌های اطلاعاتی و سازمان باید دست‌کم در مورد ارائه خدمات فناوری اطلاعات زیر توافق کنند:

- مدیریت ظرفیت
- مدیریت مالی فناوری اطلاعات
- مدیریت دسترسی

به‌استثنای ذینفعان و مستندسازی، رویه برخورد با و اهمیت موافقت‌نامه سطح خدمات برون‌سازمانی، مشابه موافقت‌نامه سطح خدمات درون‌سازمانی است. از این دید، حسابرس فناوری اطلاعات باید از اصل راهنمای این موافقت‌نامه برای خدمتی مشخص به سازمان، آگاه باشد.

قرارداد تعمیر و نگهداری نیز می‌تواند به‌عنوان موافقت‌نامه سطح خدمات برون‌سازمانی مورد استفاده قرار گیرد.

۶. شیوه‌های مدیریت داده

۱-۶. شیوه‌های مدیریت داده چیست؟

از روش‌های مدیریت داده برای تعیین یکپارچگی و بهینه‌سازی بانک‌های اطلاعاتی استفاده می‌شود. مدیریت داده‌ها با بهره‌گیری از یک سیستم نرم‌افزاری صورت می‌گیرد که تعریف، ذخیره‌سازی، به اشتراک‌گذاری و پردازش داده‌های کاربر را فعال و پشتیبانی می‌کند و به فعالیت‌های مدیریت پرونده می‌پردازد. داده‌های کاربر و سیستم می‌توانند به‌صورت متوالی یا به‌صورت دسترسی تصادفی مستقیم باشند و سیستم‌های مدیریت بانک اطلاعاتی[1]، به ایجاد، سازماندهی، کنترل و استفاده از داده های مورد نیاز برنامه‌های کاربردی کمک می‌کند. وظایف اصلی یک سیستم مدیریت بانک اطلاعاتی شامل کاهش داده‌های اضافی[2]، کاهش زمان دسترسی و امنیت داده‌های حساس است.

افزونگی داده‌ها در آن سیستم بانک اطلاعاتی رخ می‌دهد که دارای فیلدی است که در دو یا چند جدول تکرار می‌شود. برای مثال، در مواردی که داده‌های سازمان تکرار و به هر کالای خریداری شده آن متصل می‌شوند و از آنجا که برای یک ویژگی خاص سازمان ممکن است مقادیر مختلفی وجود داشته باشد، این داده‌های افزونه، نمونه روشنی از ناسازگاری هستند.

1. Database Management Systems (DBMS)
2. Data Redundancy

۶-۲. چرا شیوه‌های مدیریت داده برای حسابرس سیستم اطلاعاتی مهم است ؟

از آنجا که کنترل‌های کافی و مناسبی باید برای بانک اطلاعاتی اصلی برنامه‌های کاربردی کلیدی وجود داشته باشد، شیوه‌های مدیریت داده از دیدگاه حسابرس سیستم‌های اطلاعاتی، حائز اهمیت است.

به بیان دیگر، در صورت وجود کنترل‌های کافی برای یک برنامه، کنترل‌های معادل برای بانک‌های اطلاعاتی زیربنایی آن نیز باید وجود داشته باشد؛ زیرا، این ریسک وجود دارد که با ایجاد تغییراتی مستقیم در بانک اطلاعاتی، بتوان کنترل‌های موجود در سطح برنامه را زیر پا گذاشت. حسابرس سیستم اطلاعاتی باید از مفاهیم فناوری مرتبط با نرم‌افزار سیستم و سیستم‌های مدیریت بانک اطلاعاتی آگاهی داشته باشد.

۶-۳. حسابرس سیستم اطلاعاتی در طول حسابرسی می‌تواند پرسش‌های زیر را بپرسد:

- ❖ آیا برای اطمینان از یکپارچگی نرم‌افزار مدیریت بانک اطلاعاتی، رویه‌های کافی برای تغییر در بانک اطلاعاتی وجود دارد؟
- ❖ آیا سیستم مدیریت بانک اطلاعاتی، افزونگی داده‌ها را به حداقل می‌رساند؟
- ❖ آیا در سیستم مدیریت بانک اطلاعاتی، یکپارچگی داده‌های فرهنگ لغت حفظ می‌شود؟

۷. ابزارها و فنون نظارت بر ظرفیت و عملکرد

۷-۱. ابزارها و فنون نظارت بر ظرفیت و عملکرد کدامند؟

این ابزارها و فنون به تعیین میزان دستیابی خدمات فناوری اطلاعات به هدف‌های سازمان، کمک می‌کنند. منابع رایانه‌ای چون سخت‌افزار، نرم‌افزار، ارتباطات از راه دور، شبکه‌ها، برنامه‌ها و داده‌ها باید در جهت منافع کل سازمان استفاده شوند. این موضوع شامل، ارائه اطلاعات به کارکنان مجاز در زمان و موقعیت مورد نیاز آنان با هزینه‌ای قابل شناسایی و در جهت سود سازمان است. نمونه‌هایی از ابزارها و فنون نظارت بر ظرفیت و عملکرد به‌شرح زیر است:

- ❖ **تجزیه و تحلیل‌کننده‌های شبکه**- ابزارهایی که پارامترهای شبکه‌ای را در شبکه‌های الکتریکی اندازه‌گیری می‌کنند.
- ❖ **توازن بار**- روشی برای شبکه‌سازی رایانه‌ای برای توزیع کار در چند رایانه یا خوشه‌های رایانه ای، پیوندهای شبکه، واحدهای پردازش مرکزی، دیسک گردان[1] یا منابع دیگر برای

---

۱. دیسک‌گردان (Disk Drive)، دستگاهی که عمل خواندن و نوشتن روی دیسک‌های مغناطیسی را انجام می‌دهد و مکانیسم چرخاندن و سایر مکانیسم‌های لازم برای این کار را دارد (م).

دستیابی به استفاده بهینه از منابع، حداکثرسازی توان آمایش و به حداقل رساندن زمان پاسخگویی و پیشگیری از اضافه‌بار است.

- **گزارش استفاده از سیستم**- نمایش پیکربندی سیستم عامل سرور عمومی و استفاده از اطلاعات مربوط این گزارش به صورت گرافیکی بر مبنای استفاده روزانه و هفتگی، شامل ساعات روزانه استفاده و زمان بیکار بودن سیستم، ارائه می‌شود.

۸-۲. چرا ابزارهای نظارت بر ظرفیت و عملکرد برای حسابرس سیستم اطلاعاتی مهم است؟

حسابرس سیستم اطلاعاتی باید از برنامه‌ریزی ظرفیت و ابزارها و فنون نظارت مربوط مورد استفاده سازمان آگاهی داشته باشد و درستی و مناسب بودن آن‌ها را تعیین کند. بررسی گزارش‌های مختلف نظارت بر عملکرد فناوری اطلاعات تهیه شده توسط سازمان، منبع خوبی از شواهد است برای تعیین این که عملکرد سیستم‌های فناوری اطلاعات، طبق برنامه‌ریزی سازمان می‌باشد.

۸-۳. حسابرس سیستم اطلاعاتی می‌تواند پرسش‌های زیر را بپرسد:

- آیا معیارهای مورد استفاده در برنامه نظارت بر عملکرد سخت‌افزارها، بر مبنای داده‌های تاریخی و تجزیه‌وتحلیل بدست آمده از سوابق ایرادهای سیستم اطلاعاتی، برنامه‌های پردازش، گزارش کارهای سیستم حسابداری، برنامه‌ها و گزارش‌های نگهداری پیشگیرانه است؟
- آیا ظرفیت عملکرد نرم‌افزارها و سخت‌افزارهای سیستم به‌طور مستمر بررسی می‌شود؟
- آیا در مورد تجهیزات برنامه‌ریزی شده‌ای که در صورت خرابی، بدون دخالت انسان با سازنده خود تماس می‌گیرند، نظارت کافی اعمال می‌شود؟

۸. مدیریت مسأله و بحران

۸-۱. مدیریت مسأله و بحران چیست؟

مدیریت مسأله و بحران عبارت است از سیستم‌ها و روش‌های مورد استفاده برای تعیین این‌که بحران‌ها، مسأله‌ها یا اشتباه‌ها به‌موقع ثبت، تحلیل و رفع می‌شوند. هدف مدیریت مسأله، حل آن از طریق بررسی و تحلیل ژرف یک بحران عمده به‌منظور شناسایی علت اصلی آن است. با شناسایی مسأله و تجزیه‌وتحلیل علت اصلی آن، مسأله به یک اشتباه شناخته شده تبدیل می‌شود و برای حل آن و پیشگیری از بروز آتی حوادث مرتبط، می‌توان راه حلی را طراحی کرد. برای تشخیص و مستندسازی شرایط غیرعادی که می‌تواند سبب شناسایی یک اشتباه شود باید مکانیسمی ایجاد کرد.

بخش عملیات فناوری اطلاعات باید رویه‌های شناسایی و ثبت شرایط غیرعادی را مستند کند. برای ثبت این شرایط می‌توان از یک دستورالعمل یا قفل رایانه‌ای استفاده کرد. مطالب مورد مستندسازی باید شامل موارد زیر باشد:

- **تاریخ شناسایی اشتباه یا نقص**- نقص، نخستین بار چه زمانی شناسایی شد؟
- **توضیح رفع اشتباه**- برطرف شده، در انتظار، در دست بررسی، هیچ اقدام دیگری صورت نگیرد یا غیرقابل حل.
- **کد اشتباه**.
- **توضیحات اشتباه**- شرح نوشته‌ای کوتاه از اشتباه و منشأ اشتباه.
- مشخصات افراد مسئول نگهداری سوابق، ثبت روزانه، بستن آن و بخش مسئول رسیدگی به مسأله.

۸-۲. چرا مدیریت یک مسأله و بحران برای حسابرس سیستم اطلاعاتی مهم است؟

حسابرس سیستم اطلاعاتی باید از شیوه‌های مدیریت مسأله و بحران موجود در سازمان آگاهی داشته باشد. حسابرس باید رعایت سیاست‌ها و رویه‌های سازمان را بررسی کند و شاید بخواهد قراردادهای نگهداری و برنامه‌ها را برای تعیین مناسب بودن رعایت انجام شده، رسیدگی کند. سرانجام، آزمون اصلی، تعیین کفایت اقدامات سازمان در زمینه رعایت، مدت ازکار افتادگی سیستم یا تعداد رخداد خدمات پشتیبانی ناشی از خرابی تجهیزات است.

نگهداری مؤثر سخت‌افزار و مدیریت مسأله، از وقفه‌های غیرمنتظره پیشگیری می‌کند. برای مشخص کردن الگوها و روندهای تکرارشونده، مسأله‌ها و تأخیرهای رخ داده، دلیل آن‌ها و زمان سپری شده برای حل مسأله، ثبت و تجزیه‌وتحلیل می‌شود. سیاست‌ها و رویه‌های مربوط به نگهداری سخت‌افزار باید وجود داشته و به‌روز باشند.

۸-۳. نمونه پرسش‌های مربوط به عملیات فناوری اطلاعات

نمونه‌هایی از پرسش‌های حسابرسی که حسابرس سیستم اطلاعاتی می‌تواند از کارکنان عملیات فناوری اطلاعات بپرسد، به شرح زیر است:

- آیا مسأله‌های عمده و تکرارشونده، شناسایی و اقدامات مناسب برای پیشگیری از باز رخداد آن‌ها انجام شده است؟
- آیا مسأله‌های پردازش، به‌موقع برطرف شده و راه حل آن‌ها کامل و مناسب بوده است؟
- آیا مسأله‌های تکرارشونده‌ای وجود دارد که به مدیریت سیستم‌های اطلاعاتی گزارش نشده است؟

مؤلفه	نوع اندازه‌گیری سطح خدمات	در موافقت‌نامه گنجانده شده است؟
دسترسی		
سِروِرها		
سِروِرهای بانک اطلاعاتی	زمان کار لازم	
سِروِرهای برنامه‌های کاربردی	زمان کار لازم	
سرور پست الکترونیکی	زمان کار لازم	
سِروِرهای اینترنت	زمان کار لازم	
سِروِرهای پرونده	زمان کار لازم	
رایانه بزرگ	زمان کار لازم	
شبکه		
بخش شبکه گسترده[1]	زمان کار لازم	
بخش شبکه محلی[2]	زمان کار لازم	
حل مسأله		
سِروِرها		
حل مسأله سِروِرهای اصلی با اولویت اول کسب‌وکار در کمتر از X ساعت	درصد زمان لازم برای رسیدن به سطح خدمات مورد تعهد	
حل مسأله سِروِرهای اصلی با اولویت دوم کسب‌وکار در کمتر از X ساعت	درصد زمان لازم برای رسیدن به سطح خدمات مورد تعهد	
حل مسأله سِروِرهای اصلی با اولویت سوم کسب‌وکار در کمتر از X ساعت	درصد زمان لازم برای رسیدن به سطح خدمات مورد تعهد	
شبکه		
حل مسأله قطع شبکه محلی/ گسترده اصلی با اولویت اول کسب‌وکار در کمتر از X ساعت	درصد زمان لازم برای رسیدن به سطح خدمات مورد تعهد	
حل مسأله قطع شبکه محلی/ گسترده اصلی با اولویت دوم کسب‌وکار در کمتر از X ساعت	درصد زمان لازم برای رسیدن به سطح خدمات مورد تعهد	
حل مسأله قطع شبکه محلی/ گسترده اصلی با اولویت سوم کسب‌وکار در کمتر از X ساعت	درصد زمان لازم برای رسیدن به سطح خدمات مورد تعهد	
خدمات پشتیبانی		
زمان پاسخگویی به تماس‌ها در کمتر از xx ثانیه	درصد زمان لازم برای رسیدن به سطح خدمات مورد تعهد	
حل مسأله در تماس اول (تماس‌های قابل حل)	درصد زمان لازم برای رسیدن به سطح خدمات مورد تعهد	

1. Wide Area Network (WAN)
2. Local Area Network (LAN)

اصطلاحاتی که در فصل ۸ بر آن تأکید شده است:

سیستم‌های مدیریت بانک اطلاعاتی (*Database Management Systems* (DBMS))- سیستم‌های مدیریت بانک اطلاعاتی به ایجاد، سازماندهی، کنترل و استفاده از داده‌های مورد نیاز برنامه‌های کاربردی کمک می‌کند. وظایف اصلی یک سیستم مدیریت بانک اطلاعاتی شامل کاهش افزونگی داده‌ها، کاهش زمان دسترسی و امنیت داده‌های حساس است.

شاخص‌های کلیدی عملکرد (KPIs)- شاخص‌های کلیدی عملکرد، معیارهایی برای سنجش عملکرد فرآیند سازمان در دستیابی به هدف‌های تعیین شده، است. این شاخص‌ها نشانه اصلی آن است که دستیابی به یک هدف، احتمالاً ممکن خواهد شد یا نه. این شاخص‌ها فعالیت‌ها و هدف‌هایی را اندازه‌گیری می‌کنند که صاحبان فرآیندها باید برای دستیابی به عملکرد کارآمد اتخاذ نمایند.

شیوه‌های مدیریت داده (*Data Administration Practices*)- شیوه‌های مدیریت داده، برای تعیین یکپارچگی و بهینه‌سازی بانک اطلاعاتی استفاده می‌شود. مدیریت داده‌ها توسط نرم‌افزار سیستم فعال می‌شود که تعریف، ذخیره‌سازی، به اشتراک‌گذاری و پردازش داده‌های کاربر را فعال و پشتیبانی می‌کند و به فعالیت‌های مدیریت پرونده می‌پردازد.

عملیات فناوری اطلاعات (*IT Operation*)- فعالیت‌های روزانه سیستم‌های فناوری اطلاعات که فرآیندهای کسب‌وکار یک سازمان را پشتیبانی می‌کنند.

مدیریت مسأله و بحران (*Problem and Incident Management*)- عبارت است از سیستم‌ها و روش‌های مورد استفاده برای تعیین اینکه بحران‌ها، مسأله‌ها یا اشتباه‌ها به‌موقع ثبت، تحلیل و رفع می‌شوند. هدف مدیریت مسأله، حل مسأله‌ها از طریق بررسی و تحلیل ژرف یک بحران عمده به‌منظور شناسایی علت اصلی آن است.

موافقت‌نامه سطح خدمت (SLA)- به معنای توافقی بین واحد فناوری اطلاعات و سازمان (موافقت‌نامه سطح خدمت درون‌سازمانی) یا توافق‌نامه‌ای است بین واحد فناوری اطلاعات و پیمانکاران تجاری، ارائه‌کنندگان و یا مشاوران که ذینفعان برون‌سازمانی کسب و کارند (موافقت‌نامه سطح خدمت برون‌سازمانی).

فصل ۹

امنیت اطلاعات

۱. امنیت اطلاعات و اهمیت آن

اطلاعات، یک دارایی است و سازمان باید برای حفاظت از آن همانند سایر دارایی‌ها تلاش کند. امنیت اطلاعات به سازمان اجازه می‌دهد تا از اطلاعات و منابع اطلاعاتی خود (زیرساخت فناوری اطلاعات) در برابر کاربران غیرمجاز محافظت کند.

موضوع اصلی در امنیت اطلاعات، محرمانگی، یکپارچگی و در دسترس بودن است. امنیت سیستم اطلاعاتی در پی آن است که با کاهش ریسک از دست رفتن محرمانگی، یکپارچگی و در دسترس بودن اطلاعات تا سطحی پذیرفتنی، از اطلاعات سازمان حفاظت کند. محرمانگی یعنی پیشگیری از افشای اطلاعات یا دسترسی افراد غیرمجاز به آن. یکپارچگی، به دقیق و کامل بودن اطلاعات اشاره دارد. در دسترس بودن به معنای این است که اطلاعات و سایر منابع اطلاعاتی باید در دسترس کسانی باشد که به ارزیابی آن نیاز دارند.

چگونگی حفاظت یک سازمان از منابع اطلاعاتی خود را سیاست امنیتی تعیین می‌کند. سیاست امنیت اطلاعات باید امکان آموزش مسأله‌های امنیتی به کارکنان را تأمین کند و از رعایت/ پیروی رویه‌های تعیین شده برای دسترسی و کنترل داده‌ها اطمینان دهد. حسابرس سیستم اطلاعاتی باید از ریسک‌های ناشی از دستگاه‌های شخصی و تلفن‌های همراهی آگاه باشد که اطلاعات سازمان را ارزیابی می‌کند.

سازمان برای تهیه برنامه امنیت اطلاعات باید موارد زیر را داشته باشد:

- ❖ شناخت سازمان و دامنه امنیت اطلاعات.
- ❖ تعهد راهبران سازمان و داشتن برنامه‌ای برای دستیابی به هدف‌های امنیتی.
- ❖ داشتن منابع کافی و لازم برای دستیابی به امنیت اطلاعات.

۲. عناصر امنیت اطلاعات کدامند؟

دوازده زمینه زیر عموماً برای امنیت اطلاعات، شناخته شده است:

برآورد ریسک: برآورد ریسک، فرآیند شناسایی، تجزیه‌وتحلیل و ارزیابی ریسک‌های زیرساخت امنیت فناوری اطلاعات است. فرایند ارزیابی ریسک‌های مرتبط با امنیت از تهدیدات درون و برون‌سازمانی برای یک سازمان، دارایی‌های فناوری اطلاعات و کارکنان ناشی است.

خط‌مشی امنیت: مجموعه قوانین، قواعد و رویه‌هایی است که چگونگی مدیریت، محافظت و توزیع منابع برای دستیابی به هدف‌های امنیتی مشخص را تنظیم می‌کند. این قوانین، قواعد و رویه‌ها باید معیارهایی را برای اختیارات افراد، مشخص کند و ممکن است شرایطی که افراد، مجاز به اعمال اختیارات خود هستند را نیز تعیین نماید. برای آن‌که این خط‌مشی، معنادار باشد، قوانین، قواعد و رویه‌ها باید توانایی معقولی را برای افراد فراهم کند که بتوانند نقض کردن یا نکردن خط‌مشی را تعیین کنند.

سازمان امنیت اطلاعات: مدیریت ارتباطات و عملیات: سازمان باید بتواند فرآیندها و رویه‌های مورد استفاده در عملیات تجاری خود را ردیابی کند. این ردیابی، مجموعه‌ای از رویه‌ها و فرآیندهای سازمانی است که از پردازش درست داده‌ها در سازمان اطمینان می‌دهد. این مجموعه، شامل روش‌های لازم در موارد اضطراری، ورود به سیستم امنیت شبکه و رویه‌های پشتیبان‌گیری است. هدف، اطمینان یافتن از عملکرد درست و ایمن امکانات پردازش اطلاعات است.

مستندات رویه‌های عملیاتی: رویه‌های عملیاتی باید مستندسازی و نگهداری شوند و در دسترس همه کاربرانی قرار گیرند که به آن احتیاج دارند. کنترل شامل موارد زیر است:

- مستندسازی همه فعالیت‌های مهم سیستم از جمله راه‌اندازی، خاموش کردن، تهیه نسخه پشتیبان و نگهداری.
- برخورد با این اسناد و مدارک به‌عنوان سابقه رسمی سازمان، اما با تغییرات مناسب و مجاز، پیگیری تغییرات و بایگانی.
- تأمین امنیت مناسب برای این‌گونه اسناد، شامل کنترل توزیع (امنیت مستندسازی سیستم را نیز ببینید).

مدیریت دارایی: مدیریت دارایی به هر سیستمی گفته می‌شود که در آن، بر اشیای ارزشمند برای یک سازمان، نظارت و از آن نگهداری می‌شود. این می‌تواند برای دارایی‌های مشهود مانند ساختمان‌ها یا دارایی‌های نامشهود مانند حقوق مالکیت معنوی اعمال شود. مدیریت دارایی، یک فرآیند منظم از عملیات، نگهداری، به‌روزآوری و کنار گذاری بهای تمام شده دارایی‌ها به‌گونه‌ای مؤثر است. مدیریت دارایی برای یک نهاد دولتی و در شرایط مالی کنونی بسیار مهم است؛ زیرا، محدودیت‌های مالی به آن اجازه نمی‌دهد که دارایی‌های ازدست‌رفته یا دزدیده شده را به‌گونه‌ای منطقی جایگزین کند.

امنیت منابع انسانی: (با جزئیات بیشتر در بخش کنترل‌های منابع انسانی بحث شده است). کارکنان اداره‌کننده داده‌های شخصی در یک سازمان، برای محافظت از داده‌های واگذار شده به آنان، نیاز به آموزش آگاهی‌بخش مناسب و به‌روزرسانی منظم دارند. نقش‌ها و مسئولیت‌های مناسب اختصاص یافته به هر شرح شغل باید مطابق با سیاست امنیتی سازمان، تعریف و مستند شود. داده‌های سازمان باید از دسترسی، افشا، تغییر، تخریب یا مداخله غیرمجاز محافظت شود. مدیریت ریسک‌های امنیتی و حریم خصوصی منابع انسانی در همه مراحل اشتغال در سازمان، ضروری است.

هدف از آموزش، افزایش آگاهی افراد است. آموزش کارکنان برای پیشگیری از افشای داده‌ها، شناسایی مسأله‌ها و بحران‌های امنیتی و برخورد متناسب با آن‌ها با توجه به نیازهای نقش شغلی آنان است. تدابیر ایمن‌ساز شامل موارد زیر است:

- ❖ شرح شغل و نظارت،
- ❖ آگاهی و آموزش کاربر،
- ❖ وجود یک فرآیند انضباطی، و
- ❖ برای مجهز کردن کارکنان به کار ایمن و استفاده مناسب از اطلاعات باید یک فرآیند خروج منظم وجود داشته باشد و از این‌که با تغییر روابط کاربر با سازمان، امتیازات دسترسی نیز تغییر می‌یابد، اطمینان حاصل شود.

هدف از تأمین امنیت منابع انسانی این است که از صلاحیت‌دار بودن همه کارکنان، درک نقش و مسئولیت‌های وظایف شغلی و قطع دسترسی آنان پس از خاتمه خدمت، اطمینان حاصل شود. سه زمینه امنیت منابع انسانی عبارتند از:

- ❖ **پیش از استخدام:** این موضوع شامل تعریف نقش‌ها و مسئولیت‌های شغلی، تعریف دسترسی مناسب به اطلاعات حساس برای انجام وظیفه و تعیین ژرفای سطح نظارتی نامزدها، مطابق با سیاست امنیت اطلاعات سازمان است. در این مرحله، شرایط قرارداد نیز باید تنظیم شود.

- **در طول اشتغال:** کارکنانِ با دسترسی به اطلاعات حساس در یک سازمان باید یادآورهای دوره‌ای از مسئولیت‌های خود و آموزش آگاهی‌بخش امنیتی مستمر و به‌روز دریافت کنند تا از شناخت خود در مورد تهدیدهای جاری و اقدامات امنیتی کاهنده این تهدیدها مطمئن شوند.
- **پایان خدمت یا تغییر شغل:** با پایان خدمت/ جدایی کارمند باید دسترسی وی به اطلاعات حساس، بی‌درنگ لغو شود تا از دسترسی غیرمجاز به این‌گونه اطلاعات، پیشگیری گردد. هرگونه دارایی‌های سازمان که در اختیار کارمند بوده است نیز باید برگشت داده شود.

امنیت فیزیکی و زیست‌محیطی: امنیت فیزیکی و زیست‌محیطی[1] اقداماتی را توصیف می‌کند که برای پیشگیری از دسترسی فیزیکی افراد غیرمجاز به ساختمان، تأسیسات، منابع یا اطلاعات ذخیره شده و همچنین، ارائه رهنمودهایی برای طراحی ساختارهای لازم جهت مقاومت در برابر اقدامات خصمانه بالقوه، ایجاد شده است. امنیت فیزیکی می‌تواند به سادگی یک درب قفل شده یا به پیچیدگی قرار دادن لایه‌های مختلفی از موانع، نگهبان مسلح و واحد نگهبانی باشد.

امنیت فیزیکی در درجه اول به محدود کردن دسترسی فیزیکی افراد غیرمجاز به امکانات کنترل شده مربوط است، اگرچه ملاحظات و شرایط دیگری نیز وجود دارد که اقدامات امنیتی فیزیکی، ارزشمند می‌شود (برای مثال، محدود کردن دسترسی به تأسیسات یا دارایی‌های موجود در یک تأسیسات خاص و کنترل‌های زیست‌محیطی برای کاهش بحران‌های فیزیکی مانند آتش‌سوزی و سیل).

اطمینان از وجود کنترل‌های کافی برای محافظت از دارایی‌ها و منابع سازمان، وظیفه مدیریت است. مدیریت باید ارزیابی مناسبی از ریسک، شامل شناسایی تهدیدهای مربوط به سیستم و منابع سیستم، آسیب‌پذیری اجزای سیستم و تأثیر احتمالی رخداد حادثه، انجام دهد. سپس، مدیریت برای کاهشِ در معرض ریسک قرار گرفتن تا سطح پذیرفتنی، اقدامات پیشگیرانه را مشخص می‌کند.

امنیت به‌گونه‌ای گریزناپذیر هزینه‌زاست و هرگز نمی‌تواند کامل و بی‌عیب باشد- به‌بیان‌دیگر، امنیت می‌تواند ریسک‌ها را کاهش دهد، اما نمی‌تواند آن را به‌طور کامل حذف کند. با توجه به اینکه کنترل‌ها کامل نیستند، امنیت فیزیکی قوی با ترکیب مناسب همپوشانی و مکمل‌ها، اصل دفاع ژرف را اعمال می‌کند. برای مثال، کنترل دسترسی فیزیکی برای تأسیسات محافظت شده عموماً برای مقاصد زیر برقرار می‌شود:

- پیشگیری از متجاوزان بالقوه (مانند استفاده از کارت‌های عبور/ نشان‌ها و کلیدها).
- تشخیص افراد مجاز از افراد غیرمجاز.
- ایجاد تأخیر، ناکام کردن و به‌طور ایده آل، پیشگیری از تلاش‌های نفوذگران.
- آغاز واکنش‌های مناسب به این‌گونه رخدادها.

1. Physical and Environmental Security

کنترل‌های زیست‌محیطی را می‌توان به‌عنوان قرار گرفتن در معرض حوادث طبیعی مانند زلزله، رعدوبرق، سیلاب، خرابی برق و غیره تعریف کرد. مدیریت کنترل‌های زیست‌محیطی باید از برقراری کنترل‌های مناسبی، به شرح زیر، اطمینان حاصل کند:

- **سیستم‌های پیشگیری، تشخیص و مهار آتش:** این سیستم‌ها به‌گونه‌ای طراحی شده است که از رخداد آتش‌سوزی پیشگیری و در صورت رخداد، با آتش‌سوزی به روشی کارآمد مقابله می‌کند. این سیستم‌ها باید دستِ‌کم سالی یک‌بار کنترل شوند.
- **محافظت از آسیب در برابر آب:** تأسیسات پردازش اطلاعات باید ترجیحاً در موقعیتی قرار گیرند که کمتر با آب در تماس باشند. حتی در مواردی که تأسیسات رایانه‌ای در بالای سطح زمین قرار دارند، بازهم ممکن است ریسک آسیب‌دیدگی ناشی از ترکیدن لوله‌ها یا نشتی سقف وجود داشته باشد.
- **حفاظت و کنترل منبع تغذیه انرژی:** نگرانی اصلی حسابرس، احتمال تأثیر برق بر دسترسی به سیستم‌ها و یکپارچگی داده‌های پردازش شده است. سیستم سازمان باید کنترل‌هایی را داشته باشد که تأثیر قطع یا اتصالی برق را به حداقل برساند که معمولاً با نصب محافظ‌های الکتریکی و دستگاه‌های برق اضطراری (UPS)[1] حاصل می‌شود.

کنترل دسترسی: کنترل دسترسی به اِعمال کنترل بر روی افرادی اشاره دارد که می‌توانند با یک منبع، تعامل داشته باشند. اغلب، اما نه همیشه، این کنترل توسط مقامی مجاز انجام می‌شود. این منبع می‌تواند ساختمان، گروه ساختمان‌ها یا سیستم اطلاعات رایانه‌ای باشد. همچنین، می‌تواند یک سرویس بهداشتی باشد که دسترسی به آن، با استفاده از سکه امکان‌پذیر است.

کنترل دسترسی، در واقع، یک پدیده روزمره است. قفل بودن درب اتومبیل نوعی کنترل دسترسی است. لزوم استفاده از گذرواژه برای استفاده از دستگاه خودپرداز بانک، نمونه دیگری از کنترل دسترسی است. در محافظت از اطلاعات و تجهیزات مهم، محرمانه یا حساس، مالکیت کنترل دسترسی از اهمیت ویژه‌ای برخوردار است.

کنترل دسترسی در یک محیط دولتی از اهمیت ویژه‌ای برخوردار است؛ زیرا، بسیاری از دستگاه‌های دولتی، داده‌های حساسی را پردازش می‌کنند و نگرانی‌های حریم خصوصی، تعداد افرادی را که باید به بخش‌های مختلف اطلاعات دسترسی داشته باشند، محدود می‌کند. کنترل دسترسی از این‌که تنها کاربران مجاز، به داده‌های حساس دسترسی دارند، اطمینان می‌دهد.

1. Uninterruptible Power Supplies (UPS).

عناصر اساسی برای کنترل دسترسی منطقی عبارتند از:

- **شناسایی کاربر:** معمولاً شامل شناسایی کاربر با یک نام کاربری یا شناسه ورود.
- **تأیید اعتبار کاربر:** رایانه به این تأیید نیاز دارد که کاربر همان فردی است که خود را معرفی می‌کند. این امر با استفاده از آنچه کاربر دارد و/ یا می‌داند حاصل می‌شود. گذرواژه‌ها شکلی متداول از تأیید اعتبار هستند. شکل‌های دیگر تأیید اعتبار شامل شماره عددی، امضا یا بیومتریک‌ها هستند.

خرید، توسعه و نگهداری سیستم‌های اطلاعاتی: چرخه عمر توسعه سیستم، فرآیند ایجاد یا تغییر سیستم‌های اطلاعاتی و مدل‌ها و روش‌های مورد استفاده برای توسعه این سیستم‌ها است. در مهندسی نرم‌افزار، مفهوم چرخه عمر سیستم، زیربنای بسیاری از روش‌های توسعه نرم‌افزار است. این روش‌ها چارچوبی را برای برنامه‌ریزی و کنترل ایجاد سیستم اطلاعاتی یا فرایند توسعه نرم‌افزار تشکیل می‌دهند. توسعه سیستم، شامل تغییرات و بهبودهایی پیش از برچیدن و از بین رفتن سیستم است. نگهداری سیستم جنبه مهمی از چرخه عمر سیستم است. با تغییر در جایگاه کارکنان کلیدی سازمان، تغییرات جدیدی پیاده‌سازی می‌شود که به سیستم نیاز دارد.

مدیریت بحران امنیت اطلاعات: مدیریت بحران امنیت اطلاعات[1] در زمینه‌های امنیت رایانه و فناوری اطلاعات، شامل نظارت و شناسایی رویدادهای امنیتی در رایانه یا شبکه رایانه‌ای و برخورد مناسب با آن رویدادها است. مدیریت بحران امنیت اطلاعات، شکلی تخصصی از مدیریت بحران است که هدف اصلی آن، ایجاد یک برخورد خوب و قابل پیش‌بینی با رویدادهای آسیب‌رسان و نفوذهای رایانه‌ای است.

مدیریت تداوم فعالیت کسب‌وکار: برنامه‌ریزی تداوم فعالیت، فرآیندی است که سازمان برای برنامه‌ریزی و آزمون بازیابی خود پس از یک اختلال، از آن استفاده می‌کند. همچنین، چگونگی ادامه فعالیت در شرایط نامساعد را توصیف می‌کند (برای مثال، بلایای طبیعی یا سایر بلایا). برای اطلاعات بیشتر، به فصل برنامه‌ریزی تداوم فعالیت و بازیابی پس از بلایا مراجعه کنید.

انطباق/ رعایت: حسابرس سیستم اطلاعاتی باید انطباق قانونی، زیست‌محیطی و کیفیت اطلاعات و الزامات امنیتی را بررسی و ارزیابی کند. همه زمینه‌های امنیتی یاد شده در بالا در ایزو ۲۷۰۰۲، چارچوب امنیتی سازمان بین‌المللی استاندارد، تعریف شده است. افزون بر این، استانداردهای بین‌المللی دیوان‌های محاسبات بخش ۵۳۱۰، چارچوبی را برای کمک به حسابرسی امنیت اطلاعات فراهم می‌کند.

حسابرسی: استانداردهای بین‌المللی دیوان‌های محاسبات بخش ۵۳۱۰ و ایزو ۲۷۰۰۲ هر دو، راهنمایی‌هایی در مورد اقدامات امنیت اطلاعات نهادهای دولتی ارائه می‌کنند.

1. Information Security Incident Management

اصطلاحاتی که در فصل ۹ بر آن تأکید شده است:

امنیت اطلاعات (*Information Security*)– امنیت اطلاعات به سازمان اجازه می‌دهد تا از اطلاعات و منابع اطلاعاتی خود (زیرساخت فناوری اطلاعات) در برابر کاربران غیرمجاز محافظت کند. امنیت سیستم اطلاعاتی در پی حفاظت از اطلاعات سازمان با کاهش ریسک از دست رفتن محرمانگی، یکپارچگی و در دسترس بودن اطلاعات تا سطحی پذیرفتنی است.

عناصر امنیت اطلاعات (*Components of Information Security*)– دوازده زمینه پذیرفته شده برای امنیت اطلاعات که در این فصل به آن‌ها پرداخته شده است عبارتند از: برآورد ریسک؛ خط‌مشی امنیت؛ سازمان امنیت اطلاعات؛ مستندات رویه‌های عملیاتی؛ مدیریت دارایی؛ امنیت منابع انسانی؛ امنیت فیزیکی و زیست‌محیطی؛ کنترل دسترسی؛ خرید، توسعه و نگهداری سیستم‌های اطلاعاتی؛ مدیریت بحران امنیت اطلاعات؛ مدیریت تداوم فعالیت کسب‌وکار و انطباق/ رعایت.

فصل ۱۰

مدیریت تغییر

۱. مدیریت تغییر چیست؟

فرآیند مدیریت تغییر در سازمان‌های فناوری اطلاعات، معمولاً برای مدیریت و کنترل تغییرات در نرم‌افزار، سخت‌افزار و مستندات مرتبط استفاده می‌شود. مدیریت تغییر زمانی ضروری است که تأثیر یک تغییر تأیید نشده یا تصادفی به ریسک‌ها و پیامدهای مالی جدی برای سازمان منجر می‌شود. سازمان‌ها از یک‌رویه تعریف شده برای مدیریت تغییر پیروی می‌کنند که پیش از اجرا در محیط عملیاتی، هر تغییر به تصویب هیأت مدیره نیاز دارد.

۲. چرا این موضوع برای حسابرسان مهم است؟

سازمان‌های دولتی برای پردازش داده‌ها به سیستم‌های فناوری اطلاعات خود اتکا می‌کنند. این داده‌ها می‌تواند شامل داده‌های مالی، مراقبت‌های بهداشتی یا امنیتی باشد. قوانین حریم خصوصی و موضوعه مقرر می‌دارند که دسترسی به داده‌های حساس سازمان، کنترل شود و برای قابل اتکا بودن پردازش داده‌ها نیز کنترل‌های کافی اعمال گردد.

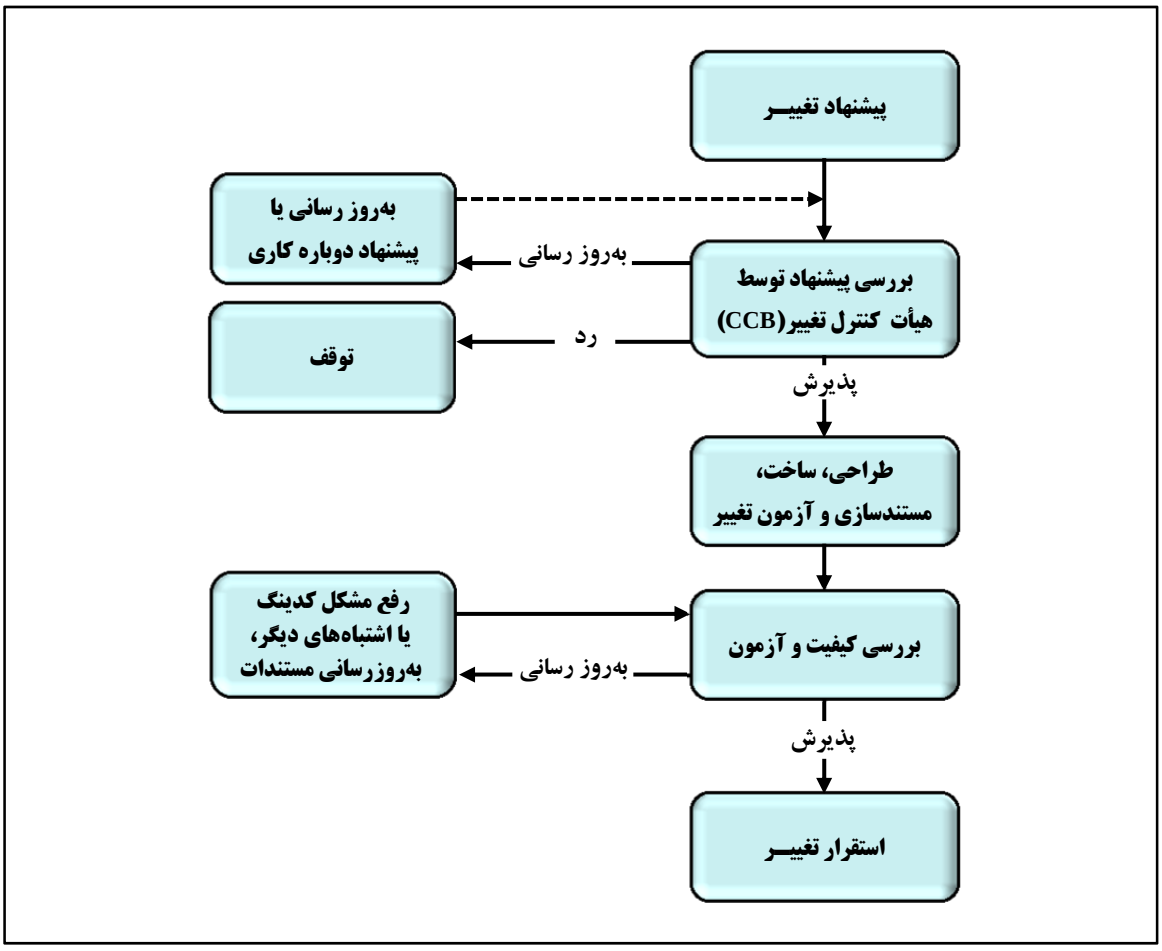
از آنجا که در دنیای نرم‌افزار، ایجاد تغییر در کدها برای پردازش متفاوت یا آسیب زدن به داده‌های حساس یا نوشتن این‌گونه اطلاعات در یک پوشه مخفی و خرابکارانه بسیار آسان است، سازمان‌ها مدیریت تغییر را ایجاد می‌کنند. در صورت پیاده‌سازی درست، از این‌که تنها تغییرات مجاز پس از کنترل کیفیت لازم، بر روی محیط عملیاتی اجرا می‌شوند، اطمینان به وجود می‌آید. حسابرسان باید از این‌که فرایند مدیریت تغییر پیاده‌سازی شده در سازمان، یکپارچگی داده‌ها، نرم‌افزارها و مستندسازی را تضمین می‌کند، اطمینان بدست آورند.

۳. چرا تغییرات در یک سیستم نرم‌افزاری یا سخت‌افزاری لازم است؟

کاربران ممکن است پس از توسعه سیستم‌ها و عملیاتی شدن آن‌ها، ویژگی‌ها یا عملکردهای (توابع) بیشتری را درخواست کنند. افزون بر این، زمانی که سیستم به‌کار گرفته می‌شود، کاربرانی که با سیستم تعامل دارند ممکن است متوجه شوند که برخی از عملیات به‌درستی انجام نمی‌شوند. هنگامی‌که در نتیجه عملکرد جدید یا اشتباه‌ها، لزوم یک تغییر شناسایی می‌شود، سازمان باید پیش از اصلاح نرم‌افزار، فرآیند مدیریت تغییر را رعایت کند. این امر برای پیشگیری از ایجاد اشتباه‌های بیشتر یا محدود کردن تعداد تغییرات در سیستم است. تغییرات سیستم برای سازمان، هزینه‌های توسعه، آزمایش و پیاده‌سازی به همراه دارد.

۴. نمونه یک فرایند مدیریت تغییر کدام است؟

سازمان‌های دولتی به دلیل وجود تفاوت در اندازه گروه فناوری اطلاعات مربوط، ممکن است فرایندهای مدیریت تغییر متفاوت داشته باشند. با این‌حال، عناصر مشترکی در یک فرآیند مدیریت تغییر وجود دارد. نمودار زیر یک نمونه از فرایند مدیریت تغییر را به تصویر می‌کشد:



- **پیشنهاد/ درخواست تغییر**[1]- این، پیشنهاد اولیه تغییر است. این پیشنهاد می‌تواند از اشتباه، عملکرد (های) از قلم افتاده یا عملکرد افزوده، ایجاد شده باشد. بیشتر سازمان‌ها، فرم درخواست تغییر شامل موضوع، ضرورت، اندازه یا مقدار کار، هزینه، برنامه و سیستم‌های نرم‌افزاری تحت تأثیر یا مرتبط را دارند. فرم درخواست تغییر ممکن است فرم درخواست برای تغییر نیز نامیده شود. این فرم ممکن است مواردی مانند اثر احتمالی بر سیستم‌های فناوری اطلاعات و خدمات به کاربران، اثر اعمال نکردن تغییر، منابع مورد نیاز برای اعمال تغییر و منابع مورد نیاز برآوردی برای حفظ این تغییر در آینده را شامل شود.

- **هیأت کنترل تغییر، پیشنهاد را بررسی می‌کند**- درخواست تغییر توسط هیأت کنترل تغییر[2] بررسی می‌شود. این هیأت مرجع نهایی است که به صورت دوره‌ای پیشنهادها را بررسی می‌کند. این هیأت مرجع نهایی پذیرش یا رد یک پیشنهاد است. یک پیشنهاد ممکن است به دلایل گوناگون از جمله اولویت پایین، هزینه و ریسک، رد شود.

  حسابرس فناوری اطلاعات باید ساختار سازمانی و کمیته‌های مدیریت سازمان را مورد توجه قرار دهد. یک سازمان می‌تواند وظایف این هیأت را توسط بخشی از سازمان انجام دهد که ممکن است آن را به این نام نامیده نباشد. بررسی و صدور مجوز تغییرات سیستم توسط مدیریت یا مقامات مجاز آن از اهمیت برخوردار است.

- **پیشنهاد به‌روز رسانی/ دوباره‌کاری**- گاه ممکن است به دلیل کمبود جزئیات کافی، پیشنهادی امکان تصمیم‌گیری را برای هیأت فراهم نسازد. در این حالت، هیأت ممکن است جزئیات بیشتر یا مدارک پشتیبانی را درخواست کند: شامل برآورد بهتر هزینه، راهبردهای کاهش ریسک پیشنهاد تغییر یا جزئیات بیشتر در برآورد برنامه که بخشی از درخواست تغییر است.

- **طراحی، ساخت، مستندسازی و آزمون تغییر**- پس از تصویب درخواست تغییر توسط هیأت، گروه پروژه به تحلیل جزئیات نیازمندی‌ها، طراحی و به روز کردن اسناد مرتبط می‌پردازند. آنان معمولاً تغییر را با استفاده از روش چرخه توسعه عمر سیستم، ایجاد و آزمون می‌کنند. هنگامی‌که تغییر، همه نیازمندی‌ها را برآورده کرد، سپس به گروه کنترل کیفیت منتقل می‌شود (که ممکن است دوباره تغییر را آزمون و با نسخه قبلی و غیره مقایسه کند تا کد مخرب در آن نباشد) و اگر نتیجه آزمون موفقیت‌آمیز بود، تغییر برای اعمال در محیط تولید پیشنهاد می‌شود. گروه پروژه در مرحله طراحی و ساخت، از مجموعه روش‌های کنترل داخلی خاص خود استفاده می‌کند. همچنین،

1. Change Proposal/Request
2. The Change Control Board (CCB)

کاربرانی که تغییر را درخواست داده‌اند باید بخشی از فرآیند آزمون باشند تا مطمئن شوند که تغییر، همان‌گونه که درخواست شده است، عمل می‌کند.

❖ **اعمال تغییر**- پس از تأیید کد توسط گروه کنترل کیفیت، کد در محیط تولید اعمال می‌شود. برای اطمینان از اعمال نسخه درست نرم‌افزار و وجود راهی برای بازگرداندن تغییرات در صورت بُروز اختلال جدی ناشی از تغییر، سازمان باید یک کتابخانه نرم‌افزار یا کنترل مشابهی داشته باشد.

شرح	ریسک	پرسش‌های مربوط به حسابرسی
درخواست تغییر	❖ افزایش احتمال تغییرات غیرمجاز در سیستم‌های کلیدی کسب‌وکار. ❖ کنترل ناکافی بر تغییرات اضطراری. ❖ نبود ردیابی مناسب تغییرات. ❖ کاهش در دسترس بودن سیستم. ❖ مستندات پیکربندی، پیکربندی سیستم فعلی را نشان ندهد. ❖ نبود مستندات فرآیندهای تجاری. ❖ قصور در به‌روزرسانی تغییرات سخت‌افزاری و نرم‌افزاری.	❖ آیا سازمان، سیاست کنترل تغییر دارد؟ ❖ در صورت نبود سیاست جداگانه، کنترل تغییر در سیاست فناوری‌های اطلاعات و ارتباطات (ICT) پوشش داده شده است؟ ❖ فرم درخواست تغییر کجا مستند می‌شود؟ ❖ چه کسی می‌تواند درخواست تغییر بدهد؟ ❖ چگونه سازمان، وضعیت درخواست‌های تغییر را ردیابی می‌کند؟ ❖ شماره‌گذاری درخواست‌های تغییر سازمان چگونه است؟ (برای تسهیل ردیابی در یک بانک اطلاعاتی) ❖ آیا درخواست‌های تغییر، ثبت می‌شوند و شماره منحصربه‌فردی دارند؟ ❖ آیا درخواست‌های تغییر، طبقه‌بندی و اولویت‌بندی می‌شوند؟
بررسی هیأت کنترل پیشنهادها	❖ افزایش احتمال تغییرات غیرمجاز در سیستم‌های کلیدی کسب‌وکار. ❖ کنترل ناکافی بر تغییرات اضطراری. ❖ نبود ردیابی مناسب تغییرات. ❖ کاهش دسترسی به سیستم. ❖ مستندات پیکربندی، پیکربندی سیستم فعلی را نشان ندهد. ❖ نبود مستندات فرآیندهای تجاری. ❖ قصور در به‌روزرسانی تغییرات سخت‌افزاری و نرم‌افزاری.	❖ ساختار سازمانی هیأت کنترل تغییر را درخواست کنید. ❖ برای بررسی پیشنهاد تغییر، هیأت چند نشست برگزار می‌کند؟ ❖ چگونه هیأت، تغییرات اضطراری را کنترل می‌کند؟ ❖ فرایند مدیریت شرایط اضطراری پس از تصویب درخواست تغییر توسط هیأت، چیست؟ ❖ فهرستی از درخواست‌های تغییر تأیید شده و همچنین درخواست‌های تغییر رد شده را درخواست کنید. ❖ چه کسی درخواست تغییر را تأیید می‌کند؟

شرح	ریسک	پرسش‌های مربوط به حسابرسی
طراحی، ساخت، مستندسازی و آزمون تغییر	❖ افزایش احتمال تغییرات غیر مجاز در سیستم‌های کلیدی کسب‌وکار. ❖ کنترل ناکافی بر تغییرات اضطراری. ❖ نبود ردیابی مناسب تغییرات. ❖ کاهش دسترسی به سیستم. ❖ مستندات پیکربندی، پیکربندی سیستم فعلی را نشان ندهد. ❖ نبود مستندات فرآیندهای تجاری. ❖ قصور در به‌روزرسانی تغییرات سخت‌افزاری و نرم‌افزاری.	❖ آیا گروه فناوری اطلاعات می تواند فرایند کنترل تغییر هیأت را زیر پا بگذارد؟ ❖ پیش از پیاده‌سازی سیستم، چه کنترل‌های کیفیتی روی آن انجام می‌شود؟ ❖ چه کسی پیاده‌سازی نهایی تغییر را تأیید می‌کند؟ ❖ سازمان کنترل کیفیت یا هر مقام مجاز دیگر چه تعداد تغییر را پذیرفته و چه تعداد را رد کرده است؟ ❖ چه اتفاقی برای تغییرهای رد شده می‌افتد؟ ❖ چگونه از به‌روز شدن مستندات و انطباق با نرم‌افزار اصلاح شده در جریان، اطمینان می‌یابید؟ (به دنبال نکاتی در مستندات باشید که نشان می‌دهند چرا تغییر ایجاد شده است).
اعمال تغییر	❖ افزایش احتمال تغییرات غیرمجاز در سیستم‌های کلیدی کسب‌وکار. ❖ کنترل ناکافی بر تغییرات اضطراری. ❖ نبود ردیابی مناسب تغییرات. ❖ کاهش دسترسی به سیستم ❖ مستندات پیکربندی، پیکربندی سیستم فعلی را نشان ندهد. ❖ نبود مستندات فرآیندهای تجاری. ❖ قصور در به‌روزرسانی تغییرات سخت‌افزاری و نرم‌افزاری.	❖ آیا یک کتابخانه نرم‌افزار دارید که از آن برای پیاده‌سازی نرم‌افزار استفاده می‌کنید؟ ❖ چگونه اطمینان می‌یابید که نسخه درست نرم‌افزار، پیاده‌سازی شده است؟ ❖ چگونه می توانید تغییرات را به نسخه پیشین ردیابی کنید؟ ❖ آخرین بار که مجبور شدید به نسخه پیشین برگردید چه زمانی بود؟ ❖ چه تغییراتی در نتیجه پاسخ به پرسش بالا در روند درخواست تغییر ایجاد کرده‌اید؟

اصطلاحاتی که در فصل ۱۰ بر آن تأکید شده است:

مدیریت تغییر (Change Management)- در سازمان‌های فناوری اطلاعات، معمولاً فرآیند مدیریت تغییر برای مدیریت و کنترل تغییرات در نرم‌افزار، سخت‌افزار و مستندات مرتبط استفاده می‌شود.

نمونه فرآیند مدیریت تغییر (Typical Change Management Process)- عناصر مشترکی در یک فرآیند مدیریت تغییر وجود دارد که عبارتند از: درخواست/ پیشنهاد تغییر؛ بررسی پیشنهاد تغییر توسط هیأت کنترل تغییر؛ طراحی، ساخت، مستندسازی؛ آزمون تغییر و اعمال تغییر.

هیأت کنترل تغییر (Change Control Board)- این هیأت، مرجع نهایی است که به‌صورت دوره‌ای پیشنهادهای تغییر را بررسی می‌کند.

فصل ۱۱

حسابرسی تداوم کسب‌وکار و بازیابی فاجعه

۱. برنامه‌ریزی تداوم کسب و کار و برنامه‌ریزی بازیابی فاجعه کدامند؟

برنامه‌ریزی تداوم کسب وکار (BCP) به فرآیندی گفته می‌شود که در صورت بروز فاجعه، سازمان را قادر می‌سازد تا عملیات عادی خود را ادامه دهد. هدف اصلی برنامه تداوم کسب‌وکار، حفظ یکپارچگی داده‌های سازمان همراه با وظایف عملیاتی و امکانات پردازشی و در صورت لزوم، ارائه خدمات موقت یا محدود تا زمان ازسرگیری خدمات عادی است.

محرمانگی، یکپارچگی و در دسترس بودن سیستم‌ها یا داده‌ها همچنان یک اصل راهنما در مراحل طراحی برنامه‌ریزی تداوم کسب‌وکار و برنامه‌ریزی بازیابی فاجعه (DRP)[1] است.

۲. تفاوت بین برنامه‌ریزی تداوم کسب‌وکار و برنامه‌ریزی بازیابی فاجعه

برنامه‌ریزی تداوم کسب‌وکار به کل سازمان مربوط است و به رویه اولویت‌بندی مأموریت فرآیندهای فراگیر کسب‌وکار، اطمینان یافتن از انجام مناسب آن‌ها پس از یک اختلال یا امکان بازیابی آن‌ها در مدت زمانی معقول، اشاره دارد. این برنامه‌ریزی ممکن است به استفاده از فرآیندهای دستی یا خودکار سازمان برای کار با ظرفیت محدود نیاز داشته باشد. برنامه‌ریزی بازیابی فاجعه معمولاً با کفایت توان/ توانمندی زیرساخت‌های فناوری اطلاعات برای بازیابی فاجعه سروکار دارد. این برنامه‌ریزی با برنامه‌ریزی تداوم کسب‌وکار نیز همسو است؛ تا از بحرانی تلقی شدن فرآیندهای مأموریت بحرانی موجود در برنامه‌ریزی تداوم کسب‌وکار که توسط سیستم‌های فناوری اطلاعات پشتیبانی می‌شوند، به‌وسیله واحد فناوری اطلاعات اطمینان به دست آید.

---

1. Disaster Recovery Planning (DRP)

۳. اهمیت برنامه‌ریزی تداوم کسب‌وکار و برنامه‌ریزی بازیابی فاجعه برای یک سازمان فناوری اطلاعات

سازمان‌های دولتی در بیست سال گذشته به‌طور فزاینده‌ای بر در دسترس بودن و عملکرد درست سیستم‌های رایانه‌ای برای انجام تعهدات قانونی خود، اتکا کرده‌اند. سیستم‌های رایانه‌ای در فعالیت‌های گوناگونی چون تشخیص و وصول مالیات و درآمدهای گمرک، پرداخت حقوق بازنشستگی کشوری و مزایای تأمین اجتماعی و همچنین، پردازش آمارهای ملی (زاد و ولد، مرگ‌ومیر، جرم، بیماری و غیره) نقش مهمی ایفا می‌کنند. در واقع، اکنون بسیاری از فعالیت‌ها نمی‌توانند بدون پشتیبانی رایانه، به‌گونه‌ای مؤثر انجام شوند.

قطعی برق، اعتصاب‌های کارگران صنایع، آتش‌سوزی و آسیب‌های مخرب عمدی، همگی می‌توانند آثار مخربی بر سیستم‌های رایانه‌ای داشته باشند. چنانچه سازمانی یک برنامه‌ریزی تداوم کسب‌وکار کاربردی نداشته باشد (و حادثه‌ای رخ دهد)، بازگشت به شرایط عادی عملیات مؤثر تجاری اگر ناممکن نباشد، ممکن است هفته‌ها به درازا بکشد.

خدمات یا محصولات فراگیر (اساسی) آن‌هایی هستند که برای اطمینان از بقا، پیشگیری از ایجاد آسیب و رعایت تعهدات قانونی یا سایر تعهدات یک سازمان باید ارائه شوند. برنامه‌ریزی تداوم کسب‌وکار یک فرایند برنامه‌ریزی فعال است که هنگام اختلال، از ارائه خدمات یا محصولات فراگیر اطمینان می‌دهد.

۴. برنامه

یک سازمان باید سیاست‌های زیربنایی برای توسعه برنامه‌ریزی تداوم کسب‌وکار و برنامه‌ریزی بازیابی فاجعه داشته باشد که دست‌کم موارد زیر را پوشش دهد:

- هدف کلی سازمان برای بازیابی یا راهبرد بازیابی.
- توانمندسازی افراد درگیر در برنامه‌ریزی تداوم کسب‌وکار یا برنامه‌ریزی بازیابی فاجعه.
- هدف‌های بازیابی - زمان و نقطه.
- فراخوان.
- وابستگی‌ها.
- گروه‌های بازیابی:
  - زیرساخت - شناسایی.
  - برنامه‌های کاربردی - شناسایی.
  - هماهنگی و تدارکات.
  - روابط عمومی و نظارت.
- گروه‌های کسب‌وکار.
- چک‌لیست آزمون بازیابی.
- روش‌های بازیابی.

۵. چرا حسابرسی برنامه‌ریزی تداوم کسب‌وکار و برنامه‌ریزی بازیابی فاجعه؟

برنامه‌ریزی تداوم کسب‌وکار و برنامه‌ریزی بازیابی فاجعه از این‌که فرآیند کسب‌وکار و زیرساخت‌های فناوری اطلاعات یک سازمان توان پشتیبانی از نیازهای مأموریت سازمان پس از فاجعه یا سایر اختلالات را دارند، اطمینان می‌دهند. دستگاه‌های دولتی، خدماتی ضروری را ارائه می‌کنند که اگر این خدمات برای مدتی نسبتاً طولانی مختل شوند، به زیان‌های مالی و سایر انواع زیان‌ها منجر می‌شود. حسابرسان باید از این موضوع اطمینان یابند که همه دستگاه‌های دولتی، فرآیند لازم برنامه‌ریزی تداوم کسب‌وکار و برنامه‌ریزی بازیابی فاجعه را دارند که از امکان ادامه ارائه خدمات به شهروندان، اطمینان می‌دهد.

۶. حسابرسی برنامه‌ریزی تداوم کسب‌وکار و برنامه‌ریزی بازیابی فاجعه

سازمان‌های دولتی باید مراحل خاصی را برای برنامه‌ریزی راهبردهای بازیابی، طی کنند. این مراحل، هیچ نام ثابتی ندارند و برای بهبود اثر یا تحلیل ممکن است برخی از آنها چندین بار انجام شوند. حسابرسان فناوری اطلاعات برای شناسایی مسأله‌های مربوط به حسابرسی، می‌توانند مرحله ایجاد یا توسعه برنامه‌ریزی تداوم کسب‌وکار و برنامه‌ریزی بازیابی فاجعه را بررسی کنند.

۶-۱. سناریوهای تأثیر در کسب‌وکار و شناسایی تهدید

کاربران سیستم و کارکنان پشتیبانی فناوری اطلاعات در سازمان برای ارزیابی دقیق هر سیستم کسب وکار مورد بررسی و شناسایی دامنه تهدیدهایی که ممکن است از عملکرد درست آن‌ها پیشگیری کند، با یکدیگر همکاری می‌کنند. شناسایی و تجزیه وتحلیل تهدیدها، فرآیند بررسی تهدیدهای احتمالی و ارزیابی چگونگی اثر آن‌ها بر کسب‌وکار است. تهدیدها ممکن است بلایای طبیعی و رویدادهای انسانی مانند بمب و غیره را در برگیرد.

هدف از بررسی تأثیر بر کسب‌وکار، شناسایی سیستم‌های کسب‌وکار سازمان و رتبه‌بندی آن‌ها بر اساس اهمیت برای کسب‌وکار است. در این بررسی مراحل زیر وجود دارد:

- **سناریوهای تأثیر بر کسب‌وکار**- شناسایی آثار احتمالی بر کسب‌وکار، با در نظر گرفتن **"سناریوهای اثر کسب‌وکار"** گوناگون همراه است. برای مثال، سناریوهای اثر بر کسب‌وکار در یک سازمان دولتی مسئول امور مزایای تأمین اجتماعی ممکن است شامل مواردی به شرح زیر باشد که برای این سازمان، مهم تلقی می‌شود:
  - ادعاهای مربوط به حقوق بازنشستگی کشوری و مزایای تأمین اجتماعی قابل پردازش نیست؛
  - پرداخت مزایا امکان‌پذیر نیست؛
  - وام‌ها قابل بازیافت نیست؛ و
  - ایجاد حساب کاربری امکان‌پذیر نیست.

شناسایی سناریوهای تأثیر، با تمایز بین آنچه واقعی و آنچه غیر واقعی است، سروکار دارد. این امر به ترکیبی از قضاوت و درک همه‌جانبه از کسب‌وکار نیاز دارد.

- **اندازه‌گیری یا تجزیه‌وتحلیل اثر بر کسب‌وکار**- پس از شناسایی سناریوهای واقع‌بینانه مؤثر بر کسب‌وکاری که بر عملکردهای مهم سازمان اثر می‌گذارد، اثر آن‌ها بر کسب‌وکار توسط سازمان اندازه‌گیری می‌شود. این اندازه‌گیری‌ها برای مثال ممکن است چگونگی اثرگذاری افزایش هزینه اضافه‌کاری یا هزینه تعمیرات و غیره بر عملیات سازمان را شامل شود. اندازه‌گیری و تجزیه‌وتحلیل اثر بر کسب‌وکار توسط سازمان، برای تعیین این است که کدام‌یک از عملکردهای مأموریتی، اساسی هستند و بازیابی نکردن آنها در یک مدت مشخص، برای سازمان چقدر هزینه خواهد داشت. عموماً، انجام نشدن یک کارکرد تجاری، به محدودیت عملیاتی قابل توجهی منجر می‌شود.

  اثر بر کسب‌وکار، برآوردی است از خسارت احتمالی به کسب‌وکار که می‌تواند از رخداد یک سناریوی تأثیر ناشی شود. این آثار برای هر فرآیند اساسی تجاری یا گروهی از فرآیندها برآورد می‌شود و درک اینکه این آثار با توجه به زمان، تغییر می‌کنند، اهمیت دارد. به‌طور کلی، هرچه سناریو طولانی‌تر ادامه یابد، اثر آن بر کسب‌وکار بیشتر خواهد شد.

- **تعریف مهلت و مستندسازی بازیابی**- هنگامی‌که سازمان بتواند زیان‌های مالی یا سایر زیان‌های اجرا نشدن عملکردهای اساسی را برآورد کند، می‌تواند تعیین مهلت برای بازیابی را آغاز کند. این تعیین زمان‌ها به سازمان بستگی دارد اما، برای مثال، می‌تواند شامل گروه‌بندی‌هایی به شرح زیر باشد:
  - **دسته ۱ :** مدت زمان بازیابی در **"n"** دقیقه.
  - **دسته ۲ :** مدت زمان بازیابی در **"n"** ساعات.
  - **دسته ۳ :** مدت زمان بازیابی در **"n"** روز.
  - **دسته ۴ :** دفعات بازیابی در **"n"** هفته.
  - **دسته ۵ :** با توجه به تاریخ، به صورت اساسی فرق می‌کند.
  - **دسته ۶ :** برنامه‌هایی که اساسی نیستند.

- **مستندسازی بازیابی**- مستندسازی بازیابی، منابع مورد نیاز دسترسی را هنگام بازیابی از یک فاجعه، فهرست می‌کند. سازمان برای اطمینان یافتن از وجود منابع مورد نیاز در مکان مورد نظر، با تنظیمات مناسب و در وضعیت کاری خوب، از مدیریت دارایی در زمینه امنیت اطلاعات، استفاده می‌کند. از این مستندات بازیابی، برای طراحی راه حل در مرحله بعد استفاده می‌شود.

- **روش‌های کاهش ریسک**- گروه حسابرسی باید در طول بررسی، زمینه‌هایی را شناسایی کند که در آن‌ها، با اعمال کنترل‌های بیشتر می‌توان ریسک بروز فاجعه را کاهش داد. با این‌حال، از آنجا که این بررسی، یک بررسی تفصیلی امنیت فناوری اطلاعات نیست، این امر باید به کنترل‌های آشکارتر پیشگیری‌کننده از بروز فاجعه محدود شود.

- **گزارشگری به مدیریت**- گزارش بررسی تأثیر بر کسب‌وکار به مدیریت دربرگیرنده میزان زیان سازمان از یک فاجعه یا حادثه دیگر و سرعت انباشت زیان‌ها است. بنابراین، این گزارش فرآیندهای کلیدی کسب‌وکار را به ترتیب اهمیت آنها برای سازمان طبقه‌بندی می‌کند و برای هر یک، موارد زیر را شرح می‌دهد:
  - ❖ شکلی که احتمال دارد آسیب یا زیان به سازمان وارد شود.
  - ❖ تا چه اندازه احتمال افزایش میزان خسارات پس از حادثه وجود دارد.
  - ❖ حداقل نیروی انسانی، امکانات و خدماتی که برای ازسرگیری سطح خدمات اضطراری لازم خواهد بود.
  - ❖ حداکثر زمان قابل تحمل برای هر دو وضعیت اضطراری و بازیابی کامل خدمات.

۶-۲. راهبرد بازیابی

گروه بررسی باید در طول مرحله برنامه‌ریزی راهبرد بازیابی، همه تهدیدهایی را شناسایی کند که با اجرای کنترل‌های قوی‌تر پیشگیرانه و کشف‌کننده، کاهش می‌یابند. کنترل‌های قوی‌تر باعث کاهش ریسک کلی رخداد فاجعه می‌شود و با ایجاد اطمینان از کشف و مدیریت زودهنگام فاجعه، به پیشگیری از آسیب جدی، کمک خواهند کرد.

۶-۳. طراحی راه حل

هدف از طراحی راه حل، ایجاد راه‌کاری است که با استفاده از دارایی‌های سازمان، تداوم عملکرد تجاری را پس از ایجاد اختلال ممکن می‌سازد. سازمان می‌تواند از منابع درون و برون‌سازمانی استفاده کند و به‌طور معمول، هزینه را با زمان بازیابی می‌سنجد. ممکن است لازم باشد برخی کارکردها به صورت دستی انجام شوند و طراحی راه حل، فرآیند این کار را مستند می‌کند. طراحی راه حل همچنین، شامل مراحل پشتیبان‌گیری و بازیابی خاصی است که سازمان باید از آن‌ها پیروی کند تا به صورت دوره‌ای از داده‌ها، پشتیبان تهیه شود. مراحل بازیابی از این‌که داده‌های پشتیبان‌گیری شده قابل بازیابی هستند و نسخه‌های کافی از پشتیبان‌ها در سایت محلی و در سایت راه دور نگهداری می‌شوند، اطمینان می‌دهد.

سازمان برای دستیابی به راهبرد و راه حل باید هدف‌های زمانی بازیابی (RTO)[1] و هدف‌های نقطه بازیابی (RPO)[2] را برای سیستم‌های اطلاعاتی خود برقرار کند. این‌ها اساساً طراحی راه حل برای برنامه‌ریزی بازیابی فاجعه که اجرا خواهد شد را تعیین می‌کنند.

هدف زمانی بازیابی، دوره یا مدت زمانی است که در آن، یک فرآیند تجاری باید در صورت رخداد یک رویداد پیش‌بینی نشده، بازیابی شود.

هدف نقطه بازیابی، میزان داده‌های از دست رفته در صورت اختلال است که انتظار می‌رود مورد پذیرش مدیریت عملیاتی باشد. برای مثال، اگر هدف زمانی بازیابی روی ۲ ساعت تنظیم شده باشد، یک نسخه پشتیبان کاملاً مشابه باید خارج از سایت به‌عنوان راه حل برنامه‌ریزی تداوم کار و بازیابی فاجعه نگهداری شود.

هرچه یک سیستم برای فعالیت‌های سازمان مهم‌تر باشد، هدف‌های زمان و نقطه بازیابی نیز کمتر خواهد بود.

۴-۶. پیاده‌سازی و آزمون

سازمان، در این مرحله راه حل‌ها را کنار هم قرار می‌دهد و اجزای مختلف راه‌حل‌ها را جدا جدا آزمون می‌کند و یک آزمون کامل نیز انجام می‌دهد. اغلب، انجام یک آزمون کامل برای سازمان مختل‌کننده است و نباید به دفعات انجام شود. با این‌حال، آزمون اجزا به‌صورت دوره‌ای انجام می‌شود. رویکردهای مختلفی وجود دارد که سازمان می‌تواند از آن‌ها برای آزمون برنامه استفاده کند:

- **آزمون زنده**- این آزمون باید در شرایط تا حد ممکن واقع‌بینانه انجام شود. این آزمون باید در یک سناریوی اصلی انجام شود و شامل انتقال حجم کار در جریان روی سیستم‌های اصلی مورد آزمون به یک سیستم آماده به‌کار باشد. این آزمون همچنین باید زیر نظر گروه مدیریت بحران در مرکز کنترل اضطراری انجام شود و شامل جابجایی برخی از کاربران کسب‌وکار طبق سناریوی آزمون و الزام برنامه باشد. آزمون کلی باید موارد زیر را اثبات کند:
  - سیستم مورد آزمون در یک رایانه آماده به‌کار، قابل بازیابی است.
  - از سیستم‌ها و پرونده‌های داده‌های درست، پشتیبان تهیه می‌شود.

1. Recovery Time Objective (RTO)
2. Recovery Point Objective (RPO)

- ❖ سیستم آماده به‌کار با سیستم اصلی سازگار است.
- ❖ پیوندهای ارتباطی را می‌توان به سایت آماده به‌کار انتقال داد.
- ❖ روش‌های جابجایی کارکنان در یک کار (حالت) اضطراری وجود دارد.
- ❖ خدمات پشتیبانی کاربر می‌تواند ارائه شود.

▣ **بازیابی سیستم**- سیستم‌های بازیابی، به‌ویژه در یک رایانه آماده به‌کار باید به صورت دوره‌ای آزمون شود. حتی اگر سیستم بازیابی شده فقط حجم کار شبیه‌سازی شده را داشته باشد، این آزمون، دست‌کم این اطمینان را به وجود می‌آورد که جنبه‌های این طرح، قابل اجرا باقی مانده است. تغییرات در این نوع آزمون ممکن است شامل موارد زیر باشد:

- ❖ آزمون‌های اعلام نشده.
- ❖ انتخاب تصادفی کارکنان برای شرکت در این آزمون، کاهش نیروی کار و کنارگذاری برخی از اعضای اصلی/ کلیدی گروه.
- ❖ غیرفعال کردن اجزای اصلی سیستم برای شبیه‌سازی شکست‌ها.

▣ **ابزارهای آماده‌به‌کار**- این آزمون‌ها عمدتاً شامل تجهیزات آماده‌به‌کار برق، آب و ارتباطات است. ژنراتورهای آماده به‌کار و منبع تغذیه اضطراری دست‌کم هرماه باید به‌طور کامل آزمایش شوند. در مواقع اضطراری، منبع تغذیه آماده‌به‌کار ممکن است لازم باشد از سیستم‌های رایانه‌ای کلیدی، تجهیزات محیطی پشتیبان آنها و سیستم‌های ارتباطی پشتیبانی کند.

▣ **آزمون تخلیه**- آزمون تخلیه[1] می‌تواند برای آزمون مدیر برنامه‌ریزی مستمر و مرکز کنترل اضطراری استفاده شود، اما مفیدترین استفاده آن، حفظ آگاهی کارکنان است.

▣ **اجرای خشک**- اجرای خشک[2] با رویکرد بازی گروهی سروکار دارد. یک سناریوی فرضی تهیه می‌شود و اعضای گروه درگیر آن، درباره نقش خود در پیاده‌سازی و مدیریت بازیابی، گفتگو می‌کنند.

1. Practice Evacuations
2. Dry Running

۵-۶. ارزیابی نتایج و به‌روز رسانی طرح

ارزیابی نتایج- آزمون، تنها اجرای نقش‌ها نیست؛ هدف باید اثبات عملی بودن طرح باشد. بنابراین، آزمون باید بر مبنای معیارهایی انجام شود که بتوان در آینده از آن برای ارزیابی نتایج آزمون استفاده کرد. معیارهای آزمون معمولاً مرتبط با زمان هستند و شامل موارد زیر می‌شوند:

- **زمان بازیابی سیستم مورد آزمون**- اگر این آزمون، بیش از حد باشد و عملیات کسب وکار در مهلت بحرانی بازیابی نشود، آزمایش‌های بعدی برای بهبود آشنایی با اجرای طرح، لازم خواهد بود یا بعضی جهات سیستم، به اصلاح نیاز خواهد داشت.

- **زمان اتصال مجدد کاربران به سیستم مورد آزمون**- بازیابی یک سیستم دسته‌ای[1] می‌تواند برای آنانی که به‌طور برخط متصل هستند دشواری‌های گوناگونی داشته باشد و مشکلاتی را در انتقال مدارهای/ خطوط ارتباطی و بازیابی شبکه‌ها ایجاد کند. زمان توزیع خروجی‌های چاپی- اگر خروجی به‌صورت متمرکز چاپ می‌شود، آیا می‌توان آنها را به دست درخواست‌دهندگان واقعی رسانید؟

- **بارِ پردازش**- سیستم آماده به‌کار پس از بازیابی ممکن است حتی با احتساب این احتمال که در شرایط اضطراری کاهش سطح خدمت می‌تواند پذیرفتنی باشد، نتواند حجم لازم اطلاعات را پردازش کند یا در مدت زمانی رضایت‌بخش، آن را انجام دهد.

سوابقی باید نگهداری شود که همه مشکلات رخ داده در طول آزمایش، در آن ثبت شود. پس از آزمون، دشواری‌های ثبت شده باید بر اساس نوع و شدت، اولویت‌بندی شوند. این اطلاعات، معیارهای بیشتری را برای قضاوت درباره موفقیت کلی آزمون فراهم می‌کند. همچنین، شاخص‌هایی را برای اصلاح برنامه تأمین می‌کند.

به‌روز رسانی برنامه- شاید مهم‌ترین الزام این است که طرح باید **"مالک"** شناخته شده‌ای داشته باشد، یعنی مدیری که برای نگهداری از تداوم برنامه در برابر هیأت مدیره پاسخگو باشد. نبود مالک مشخص، ناگزیر به منسوخ شدن برنامه منجر می‌شود.

1. Batch System

۶-۶. ریسک و ملاحظات حسابرسی

نرم‌افزارهای کاربردی، ستون فقرات عملیاتی سازمان را تشکیل می‌دهند. در صورت بروز اختلال، سازمان باید در کمترین زمان ممکن از اختلال بهبود یابد. میزان در خطر بودن فناوری اطلاعات و راه حل‌های مبتنی بر اولویت‌ها و چارچوب برنامه تداوم کسب‌وکار را برنامه‌های تداوم فناوری اطلاعات و بازیابی فاجعه، تعیین می‌کنند. نقش حسابرس، بررسی برنامه و ارائه ارزیابی خود به مدیریت از میزان آمادگی فناوری اطلاعات در صورت بروز اختلال و شناسایی مواردی است که باعث محدودیت در پردازش کسب‌وکار می‌شود. حسابرس همچنین، برآورد مستقل خود را از اثربخشی برنامه تداوم فناوری اطلاعات و انطباق آن با برنامه تداوم کسب‌وکار، به مدیریت ارائه می‌دهد.

ریسک‌های مرتبط با برنامه‌ریزی تداوم کسب‌وکار به شرح زیر است:

- ❖ نبود برنامه برای انعکاس تغییرات در نیازهای کسب‌وکار، برنامه‌های کاربردی یا فناوری؛
- ❖ نبود برنامه برای ارزیابی وضعیت و اجرای فرآیندهای جایگزین متناسب با شرایط پیش‌بینی نشده.
- ❖ برنامه‌ها و فرایندهای بازیابی نامناسب یا ناقص و در نتیجه، بازیابی دیرهنگام فرآیندها.
- ❖ برنامه‌های پردازش و پشتیبانی میان‌دوره‌ای و موقت ناقص یا آزمون نشده.
- ❖ آموزش ناکافی و آماده نبودن کارکنان برای اجرای برنامه به‌طور مؤثر و سریع.
- ❖ منابع انسانی ناکافی یا دور از دسترس برای بازیابی به‌موقع فرایندها.
- ❖ نبود دسترسی به داده‌های پشتیبان، ناتوانی در مکان‌یابی رسانه‌ها به هنگام نیاز، یا ناتوانی در انتقال داده‌ها در بازه زمانی مشخص شده.
- ❖ نقض مقررات و در نتیجه، از بین رفتن اعتماد سازمان.
- ❖ افزایش هزینه‌های مدیریت تداوم به دلیل تمرکز ناکارآمد بر ریسک‌ها و هزینه‌ها یا اولویت‌بندی نکردن بازیابی خدمات بر اساس نیاز کسب‌وکار.
- ❖ نبود تدوین سناریوهای تهدید واقع‌گرایانه بر اساس شرایط و رویدادهای احتمالی.

نمونه روش‌هایی که حسابرس می‌تواند برای برخورد با ریسک‌ها اجرا کند به شرح زیر است:

- ❖ آیا سازمان، برنامه تداوم کسب‌وکار و بازیابی حوادث دارد؟
- ❖ آیا نقش‌ها و مسئولیت‌های اعضای گروه در سطح مناسبی از اختیارات، تعیین شده است؟

- ❖ آیا ارزیابی اثر کسب وکار، همه عملکردهای مهم و ضروری کسب وکار و وابستگی منابع آن‌ها را شناسایی کرده است؟
- ❖ برآورد ریسک را بررسی و مستندسازی اقدامات کاهنده تهدیدهای موجود را تعیین کنید.
- ❖ آیا هدف‌های زمان بازیابی به همه اجزای مهم فرآیند کسب‌وکار اختصاص داده شده‌اند؟

اصطلاحاتی که در فصل ۱۱ بر آن تأکید شده است:

- ❑ **برنامه‌ریزی بازیابی فاجعه (*Disaster Recovery Planning*)**- برنامه‌ای برای بازیابی و بازسازی فعالیت سازمان در صورت بروز یک پیشامد.
- ❑ **برنامه‌ریزی تداوم کار (*Business Continuity Planning*)**- فرآیندی که سازمان را به ادامه فعالیت‌های خود در صورت بروز فاجعه، قادر می‌سازد.
- ❑ **هدف‌های زمان بازیابی (*Recovery Time Objective*)**- دوره یا مدت زمانی است که در آن، یک فرآیند کسب‌وکار باید در صورت رخداد یک رویداد پیش‌بینی نشده، بازیابی شود.
- ❑ **هدف‌های نقطه بازیابی (*Recovery Point Objective*)**- میزان داده‌های از دست رفته در صورت اختلال، که انتظار می‌رود مورد قبول مدیریت عملیاتی باشد.

فصل ۱۲

برون‌سپاری فناوری اطلاعات

۱. برون‌سپاری فناوری اطلاعات چیست؟

برون سپاری خدمات فناوری اطلاعات، زیرساخت‌ها یا پردازش برنامه‌ها به یک ارائه‌کننده (شرکت یا ارائه‌دهنده خدمات)، انعطاف‌پذیری و صرفه‌جویی در هزینه را برای سازمان فراهم می‌سازد. همچنین، برون‌سپاری ممکن است بخشی از راهبرد کاهش ریسک سازمان باشد. برون‌سپاری، به‌نوعی می‌تواند انتقال ریسک نیز باشد.

دامنه فعالیت‌های برون‌سپاری شده می‌تواند شامل موارد زیر باشد:

- ❖ زیرساخت عملیاتی (مرکز داده‌ها و فرآیندهای مرتبط) در مرکز داده‌های سازمان یا ارائه‌کننده خدمات؛
- ❖ پردازش یک برنامه اختصاصی توسط خدمت‌دهنده (ارائه‌دهنده خدمات برنامه)، توسعه سیستم یا نگهداری برنامه.
- ❖ مدیریت شبکه.
- ❖ مدیریت زیرساخت‌های امنیت اطلاعات و فرآیندهای پشتیبان.
- ❖ ترکیبی از هر یک از موارد بالا با سایر فرآیندهای کسب‌وکار و فناوری.

قرارداد برون‌سپاری، سندی قانونی است که دامنه، ویژگی‌ها، شرایط، مسئولیت‌های قانونی، دیگر مسئولیت‌ها و راه‌حل‌های جبران نقض قرارداد بین دو طرف را تعیین می‌کند. برای ایجاد ارتباط موفق بین سازمان و ارائه‌کننده، شرح روشن و جامع این موضوع‌ها، ضروری است. بسته به نوع ارائه خدمات برون‌سپاری شده، این مسأله‌ها متفاوت، اما شامل موارد زیر است:

- ❖ مالکیت یا اجاره سخت‌افزار، مجوزهای نرم‌افزار و غیره.
- ❖ انتقال کارکنان (به مرکز داده‌های ارائه‌کننده خدمات).
- ❖ برنامه‌های دارای مجوز.

- ❖ حقوق مالکیت معنوی.
- ❖ حق حسابرسی محیط و کنترل‌های اطمینان‌بخش شخص ثالث.
- ❖ نحوه صورتحساب کردن.
- ❖ منبع و اصلاح عملکرد نامطلوب.
- ❖ تمدید یا خاتمه خدمات.
- ❖ نقض قانونی مسئولیت داده‌ها.

توافق سطح خدمات، یکی از معیارهای اصلی برای اندازه‌گیری عملکرد است. بسته به نوع روابط برون‌سپاری، توافق سطح خدمات می‌تواند تعداد معاملات پردازش‌شده، به‌موقع بودن پردازش‌ها، مدت زمان رفع نشده باقی ماندن موضوع‌ها و غیره را تعیین کند. توافق سطح خدمات، مستندات پشتیبان ارزیابی روابط سازمان/ ارائه‌کننده را به حسابرس و مدیریت ارائه می‌کند.

یکی دیگر از کنترل‌ها و فرآیندهای اساسی، رابطه بین سازمان و ارائه‌کننده است. برون‌سپاری یک فرآیند مسئولیت عملیاتی را به ارائه‌کننده منتقل می‌کند. سازمان، مسئولیت مدیریت و پیروی از سیاست‌ها، رویه‌ها و الزامات نظارتی را برعهده دارد. اگر ارائه‌کننده نتواند کنترل‌ها و/ یا عملکرد مناسب را بر اساس شرایط قرارداد ارائه دهد، سازمان می‌تواند به قانون متوسل شود. با این‌حال، مقامات نظارتی، عموماً سازمان را در قبال رعایت نکردن مقررات، شامل مجازات‌های مربوط، مسئول می‌دانند. افزون بر این، جبران نقض قرارداد در صورت کوتاهی در ارائه سطح عملکرد کافی و مناسب، محدود است. مجازات‌های مالی می‌توانند اثر منفی داشته باشند (ارائه‌کننده پول را از دست می‌دهد مگر اینکه تابع قرارداد باشد)؛ زیرا، ارائه‌کننده با ادامه قرارداد بیش از فسخ قرارداد زیان می‌کند. هزینه‌های مرتبط با خاتمه خدمات می‌تواند بالا باشد و انتقال فرآیندها می‌تواند دامنه فاجعه‌بار مخربی داشته باشد. دستیابی به مالکیت معنوی می‌تواند روی ادامه فعالیت سازمان تأثیرگذار باشد و نیاز به رسیدگی دارد. مدیریت روابط سازمان و ارائه‌کننده، ضروری است.

واحد ارائه‌کننده خدمات، تمرکز خود را از ارائه فرآیندهای عملیاتی به اطمینان یافتن از اینکه ارائه‌کننده و رابطهای عملیاتی درون‌سازمانی از ارتباطات مناسب برخوردارند، بررسی‌های عملکرد و انگیزه برای دستیابی به هدف‌های مورد توافق، تغییر می‌دهد. مسئولیت ارائه‌کننده خدمات، تأیید این نیز است که کنترل‌های مناسب را برای اطمینان از عملکرد سازمان طبق تعهدات قراردادی خود به‌گونه‌ای برقرار کرده است که سازمان نتواند نافی عملکرد آن باشد. داشتن صلاحیت‌های لازم با تمرکز بر مهارت‌های فنی، مدیریت و ارتباطات برای ارائه‌کننده خدمات، ضروری است.

برون‌سپاری، روند حسابرسی و اطمینان بخشی را تغییر می‌دهد. وقتی مالکیت و اجرای فرآیندها برعهده سازمان است، وظیفه واحد حسابرسی داخلی، اجرای رویه‌های مناسب منطبق با منشور حسابرسی داخلی برای ارزیابی کنترل‌های داخلی است. انتقال فرآیند به ارائه‌کننده خدمات ممکن است چگونگی دستیابی به هدف‌های حسابرسی داخلی را تغییر دهد. هنگامی‌که ارائه‌کننده، خدماتی اختصاصی یا مشترک را ارائه می‌دهد، ممکن است به دلیل محرمانگی اطلاعات سایر سازمان‌ها یا احتمال اختلال در عملکرد خود، اجازه اجرای روش‌های حسابرسی را به سازمان ندهد. اطمینان‌بخشی شخص ثالث حرفه‌ای درباره‌ی فرآیندهای ارائه‌کننده خدمات، جایگزینی مناسب و پذیرفته شده است به‌جای اجرای روش‌های اطمینان بخشی مستقیم توسط سازمان. هدف‌ها، دامنه و روش‌های حسابرسی توسط شخص ثالث برای هر حسابرسی، با توجه به نیاز افراد متقاضی حسابرسی و خدمات ارائه شده توسط ارائه‌کننده، متفاوت است.

حسابرس ارائه‌کننده می‌تواند دو نوع گزارش ارائه دهد: گزارش نوع یک، فرآیندها و کنترل‌های ارائه‌کننده در یک زمان خاص و نظر حسابرس درباره منصفانه بودن ارائه و افشا و طراحی مناسب برای دستیابی به هدف‌های کنترل مربوط را توصیف می‌کند و گزارش نوع دو، از همان هدف‌های گزارش نوع اول استفاده می‌کند، اما شامل آزمون اثربخشی کنترل‌ها برای دستیابی به هدف‌های کنترلی مرتبط در دست‌کم طی یک دوره شش‌ماهه نیز می‌باشد. گزارش یا مستندات شخص ثالث باید شامل روش‌های پیشنهادی ارائه‌کننده خدمات باشد که سازمان باید برای پشتیبانی و تکمیل کنترل‌های ارائه‌کننده، اجرا کند. سازمان باید گزارش‌های شخص ثالث را تجزیه‌وتحلیل کند و تجزیه‌وتحلیل شکاف را با توجه به منشور حسابرسی و سایر استانداردها انجام دهد تا مشخص کند که رویه‌های اطمینان‌بخش بیشتری که به‌طور بالقوه مستلزم مجوز ارائه‌کننده برای دسترسی به امکانات می‌باشد، لازم است یا خیر.

مدیریت روابط یکی از مهم‌ترین نکات در محیط برون‌سپاری است. این نقش، روابط بین ارائه‌کننده و مدیریت سازمان است. این گروه، از رعایت شدن شرایط قرارداد، دقت فرآیند صدور صورتحساب، رضایت‌بخش بودن عملکرد ارائه‌کننده و شناسایی مسأله‌های روزانه، ارجاع به گروه‌های مدیریتی مناسب و برطرف شدن آن‌ها به‌گونه‌ای رضایت‌بخش، اطمینان می‌دهد. از آنجا که بیشتر مشکلات برون‌سپاری به مسأله‌های مدیریت ارتباط مربوط می‌شود، حسابرسی نیز بر آن، به‌عنوان یک جزء عمده بررسی تمرکز می‌یابد.

حسابرسی برون‌سپاری فناوری اطلاعات چندین مرحله از برون‌سپاری را، به شرح زیر، دربر می‌گیرد:

- ارزیابی الزامات برون‌سپاری فناوری اطلاعات؛
- ارزیابی فرایند انتخاب ارائه‌کننده؛
- ارزیابی فرآیند مذاکره و نهایی شدن قرارداد؛
- بررسی اجرای برون‌سپاری و انتقال فرایندها؛
- پایداری وضعیت تولید در محیط برون‌سپاری؛ و
- بررسی فرآیند تمدید/ خاتمه برون‌سپاری.

۲. مزایای برون‌سپاری کدامند؟

- **انعطاف‌پذیری مدیریت کارکنان**- برون‌سپاری این امکان را به وجود می‌آورد که نیروهای بیشتری را در اجرای عملیات فصلی یا چرخه‌ای به‌کار گرفت و پس از انجام عملیات، به خدمت آنان پایان داد.
- **پرورش کارکنان**- اگر پروژه‌ای به مهارت‌هایی نیاز دارد که سازمان در حال حاضر در اختیار ندارد، می‌تواند آن را برون‌سپاری کند تا کارکنان سازمان نیز آموزش ببینند. افزون بر این، سازمان می‌تواند با توجه به موقعیت‌های مکانی ارائه‌کننده، کارکنان خود را در کنار کارکنان ارائه‌کننده برای مدتی مشغول به‌کار کند.
- **کاهش هزینه‌ها در اثر برون‌سپاری**- برون‌سپاری معمولاً با انتقال هزینه نیروی کار و سایر هزینه‌ها به ارائه‌کننده که هزینه نیروی کار پایین‌تری دارد، به کاهش هزینه‌ها می‌انجامد. واحدهای فناوری اطلاعات کارهایی را برون‌سپاری می‌کنند که انجام آن‌ها در داخل سازمان، هزینه بیشتری دارد.
- **کارشناسان در دسترس**- برون‌سپاری به سازمان این امکان را می‌دهد که برای کمک به حل مسأله‌های موجود یا در حال ظهور، متخصصان را در دسترس داشته باشد. همچنین، سازمان می‌تواند با کمک کارشناسان، به‌سرعت به نیازهای تجاری در حال تغییر (مأموریت جدید یا به عهده گرفتن وظایف اضافی) واکنش نشان دهد.
- **نیروی کار بیشتر**- یکی دیگر از مزایای استفاده از برون‌سپاری، بهره‌مندی از نیروی کار بیشتر و بدون دردسرِ حفظ آنان، در موارد نیاز است. سازمان‌هایی که برون‌سپاری می‌کنند می‌توانند در زمان رونق، بدون نگرانی از (هزینه‌های) بی‌کار کردن یا حفظ اجباری آنان، کارکنان بیشتری را به صورت قراردادی به‌کار گیرند.
- **انعطاف‌پذیری**- انعطاف‌پذیری یکی دیگر از مزایای قابل‌توجه برون‌سپاری است. حتی پروژه‌های دارای بهترین برنامه‌ریزی، ممکن است به دلیل اشتباه‌های جزئی، تغییر در برنامه‌ها یا سایر فعالیت‌های پیش‌بینی نشده، دچار تأخیر یا بحران زمانی شوند.
- **پردازش ابری**- نوعی برون‌سپاری است که سازمان، پردازش داده‌های خود را به رایانه‌های در مالکیت ارائه‌کننده، برون‌سپاری می‌کند. برون‌سپاری ممکن است شامل استفاده از رایانه‌های در مالکیت ارائه‌کننده، پشتیبان گیری و دسترسی برخط به داده‌های سازمان باشد. اگر سازمان بخواهد کارکنان یا کاربران آن به داده‌ها یا حتی برنامه‌ای که پردازش داده‌ها را انجام می‌دهد دسترسی کامل داشته باشند، به دسترسی به اینترنت پرسرعت نیاز خواهد داشت. امروزه، داده‌ها یا برنامه‌های کاربردی از طریق سیستم عامل‌های همراه نیز در دسترس هستند.

- **کاهش ریسک**- گاه ممکن است برون‌سپاری و انجام برخی از خدمات یا فرآیندها بیرون از سازمان، یک راهبرد مؤثر برای مقابله با ریسک‌های ناشی از مدیریت همان خدمات در درون سازمان باشد. برای مثال، کشوری که برای انتخابات آماده می‌شود، ممکن است چاپ برگه‌های رأی‌گیری را در خارج از کشور (برون‌سپاری) چاپ کند، درحالی که خود توانایی چاپ آن‌ها را دارد. نمونه‌های دیگر در بانک‌ها، چاپ پول، پردازش پرداخت‌های برخط، پردازش فرآیند ویزای مهاجرت، گذرنامه‌ها و غیره است. بنابراین، جدا از جنبه ارائه خدمات بهتر، برون‌سپاری ممکن است به کاهش ریسک‌های مرتبط با اجرای چنین فرآیندهای حساسی در درون سازمان کمک کند.

۳. ریسک‌های برون‌سپاری فناوری اطلاعات و پرسش‌های حسابرسی

ریسک‌های مرتبط با برون‌سپاری	پرسش‌های حسابرسی
دشواری دسترسی به سیستم برون‌سپاری شده، برای هدف‌های حسابرسی	❖ آیا در قرارداد برون‌سپاری به‌روشنی اشاره شده است که سازمان حق حسابرسی سیستم برون‌سپاری شده را توسط خود یا شخص ثالث منصوب شده، دارد؟
عدم موفقیت راه‌حل‌ها در برآورده کردن الزامات تجاری و کاربر	❖ ارائه کردن یا نکردن کتابچه راهنمای کنترل‌های پیشنهادی یا مورد نیاز کاربر توسط ارائه‌کننده را تعیین کنید. ❖ تجزیه‌وتحلیل شکاف بین کنترل‌های پیشنهادی ارائه‌کننده و کنترل‌های موجود در سازمان را انجام دهید و شکاف‌های کنترل را شناسایی کنید.
اختلاف قراردادی و شکاف بین انتظارات تجاری و قابلیت‌های ارائه‌کننده	❖ مستند بودن تصویب قانونی و رسمی مطابق رویه‌های تصویب قرارداد را مشخص کنید. ❖ وجود درک روشنی از اینکه مالکیت معنوی به کدام‌یک از دو طرف قرارداد تعلق دارد را تعیین کنید. ❖ مشخص بودن روند حل مسأله برای هر دو طرف به‌طور کامل را تعیین کنید.
در معرض ریسک بودن امنیت سیستم و محرمانگی	❖ مشخص بودن سطح دسترسی امنیتی برای نمایندگان هر دو طرف را تعیین کنید. ❖ کنترل‌های سیستم‌عامل را برای اطمینان از موارد زیر بررسی کنید: • پیکربندی با حداکثر امنیت در دامنه قرارداد برون‌سپاری. • دستیابی به هدف‌های اطمینان‌بخشی مندرج در برنامه حسابرسی سیستم عملیاتی. • پیروی سیستم از حداقل رویه‌ها و سیاست‌های سازمان مورد رسیدگی.

ریسک‌های مرتبط با برون‌سپاری	پرسش‌های حسابرسی
تراکنش‌های بی‌اعتبار یا تراکنش‌های اشتباه پردازش شده	❖ برنامه‌های نگهداری و کنترل‌های پشتیبانی را برای اطمینان از این موضوع بررسی کنید که مدیریت تغییر، برای امنیت حداکثری، طراحی و پیکربندی شده است و هدف‌های اطمینان‌بخشی مندرج در برنامه حسابرسی مدیریت تغییر را برآورده می‌کند و پایبند به حداقل سیاست‌ها و استانداردهای سازمانی است.
کیفیت پایین نرم‌افزار، آزمون‌های ناکافی و تعداد خرابی‌های زیاد	❖ قابل اندازه‌گیری بودن توافق‌های سطح خدمات تعیین شده در قرارداد ارائه‌کننده از نظر کیفیت خدمات ارائه شده توسط وی را بازبینی کنید. ❖ وجود سیستم ردیابی حادثه/ مشکل را بازبینی کنید.
مسئولیت‌ها و پاسخگویی نامشخص	❖ یک فرآیند برای نظارت مداوم بر تمام سطوح خدمات مورد توافق را تعریف کنید. ❖ گزارشی منظم و رسمی از عملکرد توافق سطح خدمات، شامل انحراف از ارزش‌های توافق شده را تهیه و این گزارش را در سطوح مختلف سازمان توزیع کنید. ❖ بررسی‌های منظمی برای پیش‌بینی و شناسایی روند عملکرد سطح خدمات انجام دهید.
پوشش نداشتن یا پوشش ناکافی سیستم‌های برون‌سپاری شده توسط برنامه‌ریزی‌های تداوم کسب‌وکار یا بازیابی فاجعه	❖ آیا زمینه‌ها یا جنبه‌های سیستم‌ها یا فرآیندهای تجاری برون‌سپاری شده، توسط برنامه‌ریزی‌های تداوم کسب‌وکار یا بازیابی فاجعه سازمان به‌گونه‌ای مؤثر پوشش داده می‌شود؟ ❖ آیا واحد برون‌سپاری دارای برنامه‌ریزی تداوم کسب‌وکار یا برنامه‌ریزی بازیابی فاجعه اختصاصی خود است که مکمل برنامه‌ریزی‌های تداوم کسب‌وکار یا بازیابی فاجعه سازمانی است که برون‌سپاری می‌کند و آیا این موارد در توافق سطح خدمات، پوشش داده شده است؟

۴. چگونه برخی از ریسک‌های برون‌سپاری، مدیریت یا کاهش داده می‌شود؟

موافقت‌نامه سطح خدمات، ابزار اصلی یا قراردادی مستند بین سازمان و ارائه‌کننده‌ای است که خدمات برون‌سپاری را ارائه می‌دهد. ارائه‌کننده و سازمان با منظور کردن عناصر مهم یا اساسی در این موافقت‌نامه، به شرایط خاصی متعهد می‌شوند. این شرایط با تعیین محدودیت‌های زمانی و مشخص‌کردن جرایم یا سایر روش‌های کاهنده سود، ریسک تحویل ندادن به‌موقع توسط ارائه‌کننده را مدیریت می‌کند. روش دیگری که موافقت‌نامه سطح خدمات، ریسک‌ها را مدیریت می‌کند، درخواست انواع و جزئیات اسناد پروژه برنامه‌های توسعه یافته توسط ارائه‌کننده است.

افزون بر این، موافقت‌نامه باید خدمات مورد انتظار از ارائه‌کننده و همچنین، ویژگی‌های فنی آن خدمات را مشخص کند؛ زیرا، قراردادی قانونی و الزام‌آور بین ارائه‌کننده و سازمان است.

یک موافقت‌نامه خوب سطح خدمات باید موارد زیر را دربر گیرد:

- ❖ انواع خدمات مورد ارائه توسط ارائه‌کننده؛
- ❖ تفکیک مسئولیت‌ها بین سازمان و ارائه‌کننده؛
- ❖ خدمات مورد اندازه‌گیری، دوره اندازه‌گیری، طول دوره، مکان و جدول زمانی گزارشگری (نرخ نقص، زمان پاسخگویی، ساعات میز خدمت کارکنان و غیره)؛
- ❖ زمان اجرای قابلیت‌های جدید، سطح دوباره‌کاری؛
- ❖ نوع مستندات مورد نیاز برای برنامه‌های توسعه‌یافته توسط ارائه‌کننده؛
- ❖ مکانی که خدمات در آنجا ارائه می‌شود؛
- ❖ تناوب تهیه نسخ پشتیبان، ویژگی‌های بنیادی بازیابی اطلاعات؛
- ❖ روش‌ها و قالب‌های فسخ و تحویل داده‌ها؛ و
- ❖ بندهای تشویق و تنبیه.

اصطلاحاتی که در فصل ۱۲ بر آن تأکید شده است:

- ❑ **برون‌سپاری فناوری اطلاعات (*IT Outsourcing*)**- انتقال خدمات، زیرساخت‌ها یا پردازش برنامه‌ها به یک ارائه‌کننده (شرکت یا ارائه‌دهنده خدمات).
- ❑ **سطح ارائه خدمات (*Service Level Agreement*)**- توافق سطح خدمات یکی از معیارهای اصلی برای اندازه‌گیری عملکرد است. بسته به نوع روابط برون‌سپاری، توافق سطح خدمات می‌تواند تعداد معاملات پردازش شده، به‌موقع بودن پردازش‌ها، مدت زمان رفع نشده باقی ماندن موضوع‌ها و غیره را تعیین کند. توافق سطح خدمات، مستندات پشتیبان ارزیابی روابط سازمان/ ارائه‌کننده را به حسابرس و مدیریت ارائه می‌کند.
- ❑ **قرارداد برون‌سپاری (*Outsourcing Contract*)**- قرارداد برون‌سپاری، سندی قانونی است که دامنه، ویژگی‌ها، شرایط، مسئولیت‌های قانونی، مسئولیت‌ها و راه‌حل‌های جبران نقض قرارداد بین دو طرف را تعیین می‌کند. برای ایجاد ارتباط موفق بین سازمان و ارائه‌کننده، شرح روشن و جامع این موضوع‌ها، ضروری است.

فصل ۱۳

حسابرسی سیستم‌های برنامه‌ریزی منابع سازمانی

۱. معرفی سیستم‌های برنامه‌ریزی منابع سازمانی

در گذشته، بخش‌های مختلف مأموریتی سازمان مانند امور مالی، فروش و منابع انسانی به‌طور سنتی بر اساس مأموریت‌های جداگانه ساخته شده بودند و لزوماً دارای فرآیندهای مشترک یا متمرکز بر کسب وکار نبودند. بخش‌های مختلف، مستقل از یکدیگر عمل می‌کردند و در بیشتر موارد، هر بخش دارای سیستم کاربردی جداگانه خود یا تعدادی از سیستم‌ها برای پشتیبانی بود. در برخی موارد، نرم‌افزارهای مختلف می‌توانستند با یکدیگر ارتباط برقرار کنند، اما این همگانی نبود. این رویکرد به وقفه‌های زمانی، هزینه‌های اضافی و نیاز به تطبیق داده‌ها و افزونگی داده‌ها منجر می‌شد. در رویکرد مدیریت سنتی، هنگام صدور گزارش یا تطبیق حساب‌ها، بر کنترل‌های دستی، زیاد اتکا می‌شد. برای مثال، سفارش‌های خرید به‌صورت دستی از پرونده‌های کاغذی بازیابی و پیش از مجوز پرداخت، به فاکتور خرید پیوست می‌شدند.

یک سیستم برنامه‌ریزی منابع سازمانی (ERP) با ادغام وظایف گوناگونی که اطلاعات بین آن‌ها مبادله می‌شود، در پی حذف رویکرد مدیریت پراکنده اطلاعات تجاری است. هدف اصلی سیستم برنامه‌ریزی منابع سازمانی، آسان‌سازی جریان اطلاعات بین همه بخش‌های تجاری سازمان و مدیریت ارتباطات با ذینفعان برون‌سازمانی می‌باشد. یک سیستم برنامه‌ریزی منابع سازمانی با استفاده از یک بانک اطلاعاتی[1] به‌عنوان مخزن اطلاعات، معمولاً بر روی تعدادی از سخت‌افزارهای مختلف و پیکربندی‌های شبکه، قابل اجرا است.

سیستم برنامه‌ریزی منابع سازمانی، یک بسته نرم‌افزار تجاری است که انجام موارد زیر را برای سازمان امکان‌پذیر می‌کند:

- خودکار و یکپارچه کردن اکثر فرآیندهای تجاری سازمان؛
- به اشتراک‌گذاری داده‌ها و روش‌های معمول در سراسر سازمان؛
- تولید و دسترسی دادن به اطلاعات در یک محیط بی‌درنگ؛

1. Database/ Data Bank

نمونه‌هایی از سیستم‌های برنامه‌ریزی منابع سازمانی عبارت است از: SAP، Oracle، ACCPAC و EPICOR.

سیستم اطلاعاتی مدیریت مالی یکپارچه

سیستم اطلاعاتی مدیریت مالی یکپارچه (IFMIS) یا سیستم مدیریت مالی یکپارچه (IFMS) یک پلتفرم معمول فناوری اطلاعات و ارتباطات (ICT)[1] است که عملکردهای اصلی مدیریت مالی عمومی را (مانند بودجه‌بندی، عملیات خزانه‌داری، حسابداری، مدیریت وجوه نقد/ بدهکاران، حسابرسی/ گزارشگری) برای اطمینان از مدیریت کارآمد منابع عمومی، یکپارچه می‌کند. سیستم اطلاعاتی مدیریت مالی یکپارچه یا سیستم مدیریت مالی یکپارچه، یک سیستم برنامه‌ریزی منابع سازمانی است که در بسیاری از وزارتخانه‌ها و بخش‌ها بکار گرفته شده است. حسابرس سیستم اطلاعاتی باید با نحوه پیاده‌سازی سیستم اطلاعاتی مدیریت مالی یکپارچه آشنا باشد تا بتواند نقاط ضعف آن را شناسایی کند. قابلیت اتکای کلی بر یک سیستم در هر سازمانی را کنترل‌های برقرار شده در آن، تعیین می‌کند. برای مثال، سیستم مرکزی ممکن است به گذرواژه‌های پیچیده برای ورود نیاز داشته باشد. وجود بخشی که در آن، کاربران، حساب‌های خود را به اشتراک می‌گذارند یا گذرواژه خود را به رایانه می‌چسبانند، باعث افزایش ریسک سیستم می‌شود.

۲. ویژگی‌های سیستم‌های برنامه‌ریزی منابع سازمانی

- سیستم یکپارچه که به صورت بی‌درنگ عمل می‌کند؛ بانک اطلاعاتی مشترک.
- نظارت و کنترل مستمر هر ماژول.
- نصب سیستم بدون برنامه کاربردی دقیق/ یکپارچه‌سازی داده‌ها توسط بخش فناوری اطلاعات.

۳. مزایای سیستم‌های برنامه‌ریزی منابع سازمانی

در سیستم‌های برنامه‌ریزی منابع سازمانی، پردازش اطلاعات به صورت خودکار برای همه وظایف کسب‌وکار انجام می‌شود. داده‌ها در برنامه‌های کاربردی مختلف اما یکپارچه در دسترس است و سازمان، درک بهتری از فرآیند کسب‌وکار و نحوه گردش داده‌ها بین این فرآیندها دارد. در یک محیط برنامه‌ریزی منابع سازمانی، هر معامله تجاری به‌صورت خودکار در ماژول حسابداری مالی ثبت و کنترل و پردازش، به‌صورت خطی و بی‌درنگ[2] انجام می‌شود. مدیریت، به اطلاعات به‌روز از نحوه عملکرد سازمان دسترسی دارد.

1. Information and Communication Technology (ICT)
2. Inline and in Real-Time

سیستم‌های برنامه‌ریزی منابع سازمانی، برای پشتیبانی از عملیات یک سازمان پیاده‌سازی می‌شوند و برای موفق بودن آن، همه ماژول‌ها در همه فرآیندهای گوناگون و مهم باید به‌طور کامل، یکپارچه شوند. حسابرس باید شناختی از محیط فعالیت سازمان و همچنین، محیط نظارتی آن داشته باشد تا ریسک‌های فنی، کاربردی و رفتاری مرتبط با سیستم و محیطی که در آن فعالیت می‌کند را شناسایی کند.

۴. چرا حسابرس باید نگران سیستم‌های برنامه‌ریزی منابع سازمانی باشد؟

از آنجا که سیستم‌های برنامه‌ریزی منابع سازمانی، بیشتر فرآیندهای دستی موجود را خودکار می‌سازند، حسابرس باید از برقرار بودن کنترل‌های مناسب، اطمینان یابد. به‌ویژه، سیستم‌های برنامه‌ریزی منابع سازمانی بر کنترل‌های خودکار، امنیت دسترسی منطقی و کنترل‌های پیکربندی[1] تأکید بیشتری دارند. فعال‌سازی سیستم‌های برنامه‌ریزی منابع سازمانی تحت وب و یکپارچه کردن سیستم‌های پسین[2] با سیستم‌های پیشین[3] تحت وب همچنان تغییر در فرآیند کسب‌وکار و زیرساخت فنی را در پی دارند. همه این موارد، ریسک‌هایی را به پیاده‌سازی برنامه‌ریزی منابع سازمانی اضافه می‌کند و حسابرس باید عملکرد سازمان را برای کاهش این ریسک‌ها، بررسی کند.

۵. ریسک‌های مرتبط با پیاده‌سازی سیستم برنامه‌ریزی منابع سازمانی

به نظر می‌رسد پیاده‌سازی سیستم‌های برنامه‌ریزی منابع سازمانی، ریسک‌های بیشتری نسبت به سایر سیستم‌ها دارد و حسابرس سیستم‌های اطلاعاتی هنگام حسابرسی سیستم‌های برنامه‌ریزی منابع سازمانی باید آنها را مورد توجه قرار دهد.

برخلاف یک برنامه کاربردی عادی که برای خودکارسازی یک فرآیند کسب‌وکار به‌خصوص تدوین می‌شود، برنامه کاربردی برنامه‌ریزی منابع سازمانی، روابط متقابل بین وظایف گوناگون کسب‌وکار را نیز خودکار می‌کند. این امر متضمن درک متقابل از نقش هر بخش توسط بخش‌های دیگر و نیاز برخی فرآیندها به مهندسی مجدد برای متناسب شدن، است.

---

1. Configuration Controls
2. Back End
3. Front End

* Front End و Back End عباراتی هستند که توسط برنامه نویسان و متخصصان رایانه برای توصیف لایه‌هایی استفاده می‌شود که سخت‌افزار، یک برنامه رایانه‌ای یا یک وب‌سایت را تشکیل می‌دهند که بر اساس میزان در دسترس بودن آن‌ها برای کاربر، مشخص شده است. Back End به بخش‌هایی از یک برنامه رایانه‌ای یا کد یک برنامه اشاره دارد که به آن اجازه کار می‌دهد و کاربر نمی‌تواند به آن دسترسی پیدا کند. معماری‌های سیستم برای هدف‌های مختلف به اجزای پیش (Front) و پس (Back) تقسیم می‌شوند. رایج‌ترین آنها در نرم‌افزار توسعه وب برای تجزیه پروژه‌ها از نظر مهارت‌های مورد نیاز است. جنبه پیشین یک پروژه معمولاً توسط متخصصانی مانند طراحان وب انجام می‌شود درحالی‌که قسمت پسین، توسط مهندسان و توسعه‌دهندگان انجام می‌شود (م).

نخستین گام مهم، تکمیل مستندسازی برنامه‌ریزی است. سازمان باید از کامل بودن مستندات برنامه‌ریزی همه پروژه‌ها اطمینان حاصل کند. در بیشتر موارد، سازمان‌ها برای کمک در پیاده‌سازی سیستم برنامه‌ریزی منابع سازمانی از ارائه‌کنندگان استفاده می‌کنند. اگر مستندات پروژه تکمیل نشده باشد، این ریسک وجود دارد که سیستم به‌گونه‌ای اثربخش، عملیاتی نشود، به‌گونه‌ای مناسب پیکربندی نگردد و ممکن است هزینه بیش از واقع تحمل شود.

پرسش‌های مرتبط با حسابرسی:

- ❖ چه کسی پیاده‌سازی سیستم برنامه‌ریزی منابع سازمانی را مدیریت می‌کند؟
- ❖ تجربه آنان در مدیریت سیستم‌های برنامه‌ریزی منابع سازمانی چه اندازه است؟
- ❖ فرآیندهای کسب‌وکار سازمان برای امور مالی، منابع انسانی، حقوق و دستمزد و غیره کجا مستند می‌شوند؟
- ❖ چگونه اطمینان می‌یابید که مدیر برنامه سیستم برنامه‌ریزی منابع سازمانی/ مدیر پروژه، آخرین مستندات فرآیند کسب‌وکار را دریافت می‌کند؟
- ❖ اسناد مرتبط با پروژه سیستم برنامه‌ریزی منابع سازمانی کجا نگهداری می‌شود؟
- ❖ چه کسی اسناد مربوط به پروژه را بررسی و تأیید می‌کند؟

برخی از ریسک‌های مرتبط با سیستم‌های برنامه‌ریزی منابع سازمانی شامل موارد زیر است:

۶. تعهد مدیریت

اگر مدیریت تعهد خود را نسبت به پروژه نشان ندهد، ریسک شکست وجود دارد. کارکنان ممکن است بر این باور باشند که وقتی مدیریت متعهد نیست، چرا آنان باید به پروژه متعهد باشند.

پرسش‌های مرتبط با حسابرسی:

- ❖ آیا پروژه سیستم برنامه‌ریزی منابع سازمانی، تعهد مدیریت ارشد را جلب کرده است؟
- ❖ آیا صاحبان فرآیندهای مختلف، برای گفتگو درباره نحوه عملکرد فرآیندهای تجاری خود، در دسترس هستند؟
- ❖ آیا مدیریت با درخواست از کارکنان برای تخصیص وقت به پروژه، کمک به پروژه با طرح پرسش‌های خود و بررسی مستندات مربوط، زمان کافی برای پیاده‌سازی سیستم برنامه‌ریزی منابع سازمانی اختصاص داده است؟
- ❖ آیا مدیریت ارشد، به برنامه پیاده‌سازی سیستم برنامه‌ریزی منابع سازمانی و صرف زمان لازم برای تنظیم سیستم برای تولید داده‌های ارزش‌آفرین متعهد است.

۷. تبدیل داده

انتقال از سیستم قدیمی (موروثی)[1] به سیستم‌های استاندارد شده و یکپارچه، پیچیدگی فرآیند تبدیل را افزایش می‌دهد. گاه سیستم جدید به داده‌های نوینی نیاز دارد که در سیستم قدیمی وجود ندارد. یکی دیگر از ریسک‌های مرتبط با تبدیل داده‌های سیستم قدیمی به سیستم جدید این است که داده‌های نادرست ممکن است به سیستم جدید منتقل شود. سازمان باید از در دسترس بودن داده‌های سیستم قدیم نیز اطمینان یابد.

پرسش‌های مرتبط با حسابرسی:

- ❖ الزامات داده برای پروژه سیستم برنامه‌ریزی منابع سازمانی را کجا مستند کرده‌اید؟
- ❖ برنامه‌های کاربردی داده‌های خود را از کجا شناسایی کرده‌اید و منشأ و نوع داده‌ها را چگونه می‌خواهید تعریف کنید؟
- ❖ چگونه از پاک بودن داده‌ها اطمینان می‌یابید؛ یعنی، فیلدهای اطلاعاتی از قلم افتاده وجود ندارند، اجزای آن درست است و غیره؟

۸. بازده سرمایه‌گذاری

پیاده‌سازی یک سیستم برنامه‌ریزی منابع سازمانی، یک سرمایه‌گذاری بزرگ زمانی و پولی است. مدیریت ممکن است در برآورد مبلغ وجه مورد نیاز به این واقعیت توجه نکند که چنین طرحی جز در صورت پیاده‌سازی، آموزش و استفاده مناسب، تضمینی برای منافع مورد ادعا نیست. ارزش بیشتر سیستم‌های برنامه‌ریزی منابع سازمانی زمانی نشان داده می‌شود که سازمان برای مدتی آن‌ها را اجرا کرده باشد و بتواند بر روند بهبود فرآیندهای کسب‌وکار تأثیر گرفته از سیستم، تمرکز کند.

پرسش‌های مرتبط با حسابرسی:

- ❖ آیا بهای تمام شده پیاده‌سازی را برآورد کرده‌اید؟
- ❖ آیا برنامه پیاده‌سازی سیستم برنامه‌ریزی منابع سازمانی را برآورد کرده‌اید؟
- ❖ راهبرد مدیریت ریسک شما برای زمان انحراف از برنامه و افزایش هزینه‌ها چیست؟
- ❖ از چه زمانی انتظار دارید مزایای پیاده‌سازی سیستم برنامه‌ریزی منابع سازمانی تحقق پیدا کند؟

---

1. Legacy System

یک سیستم، فناوری یا نرم‌افزار قدیمی است که همچنان توسط یک سازمان استفاده می‌شود زیرا هنوز عملکردهایی را که در ابتدا برای آن در نظر گرفته شده بود، انجام می‌دهد. به طور کلی، سیستم‌های قدیمی دیگر پشتیبانی و نگهداری ندارند و از نظر رشد، محدود هستند (م).

۹. الزامات کاربر

انتظارات و نیازمندی‌های کاربر باید به‌درستی مستند و مدیریت شود. نیازمندی‌های کاربر باید در مستندات پروژه نوشته شود و همه طرف‌های درگیر باید در مورد آن‌ها توافق کنند. اگر نیازمندی‌های کاربر به‌درستی مستند نشود، ریسک تغییر در دامنه به وجود می‌آید. به این معنا که با پیشرفت پروژه، نیازمندی‌های بیشتری ایجاد می‌شود و احتمال دست نیافتن به مهلت زمانی پدید می‌آید.

پرسش‌های مرتبط با حسابرسی:

- ❖ انتظارات کاربر خود را چگونه مدیریت می‌کنید؟
- ❖ چه برنامه‌ای برای اولویت‌بندی و مدیریت نیازمندی‌های کاربر دارید؟

۱۰. مشاوران برون‌سازمانی

بیشتر سازمان‌ها هنگام پیاده‌سازی سیستم‌ها، به استفاده از مشاوران اتکا می‌کنند. این ریسک وجود دارد که دانش مربوط و لازم به کارکنان سازمان منتقل نشود و سبب گردد که سازمان، به‌شدت به مشاوران وابسته شود.

پرسش‌های مرتبط با حسابرسی:

- ❖ چگونه می‌توانید از پشتیبانی سیستم برنامه‌ریزی منابع سازمانی پس از پیاده‌سازی، اطمینان یابید؟
- ❖ مستندات مربوط به سیستم برنامه‌ریزی منابع سازمانی کجا نگهداری می‌شود؟
- ❖ آیا کارکنان فناوری اطلاعات درون سازمان درباره نرم‌افزار سیستم برنامه‌ریزی منابع سازمانی آموزش دیده‌اند؟
- ❖ آیا مشاوران حق دسترسی به سیستم برنامه‌ریزی منابع سازمانی را دارند؟

دیگر چالش‌های مشاهده شده هنگام پیاده‌سازی سیستم برنامه‌ریزی منابع سازمانی (شامل اطلاعات و سیستم مدیریت مالی یکپارچه) به‌شرح زیر است:

- ❖ کمبود ظرفیت درون‌سازمانی.
- ❖ مقاومت کاربران (به‌عنوان نگرانی امنیتی).
- ❖ انتقال و ذخیره اطلاعات.
- ❖ متناسب‌سازی برای انجام استفاده خاص سازمان.
- ❖ تأمین مالی برای به‌روز نگه‌داشتن زیرساخت‌ها.
- ❖ نبود کنترل‌ها.

۱۱. عملیات بکارگیری یک سیستم برنامه‌ریزی منابع سازمانی

ماژول[1]های یک سیستم برنامه‌ریزی منابع سازمانی، بسیار به یکدیگر متکی هستند. برای درک حسابرسی سیستم برنامه‌ریزی منابع سازمانی باید ارتباط و گردش داده‌ها را بین ماژول‌ها، بشناسیم. بنابراین، بکارگیری رویکرد فرآیندی/ چرخه‌ای در مقایسه با رویکرد ماژولی (جداگانه) در حسابرسی سیستم‌های برنامه‌ریزی منابع سازمانی مناسب است.

برنامه حسابرسی انجمن حسابرسان سیستم‌های اطلاعاتی برای حسابرسی سیستم‌های Oracle، EBS و SAP، از روش حسابرسی فرآیندی/ چرخه‌ای استفاده می‌کند. افزون بر این، این برنامه‌ها شامل برخی پیکربندی‌های اصلی است که باید انجام شوند.

یک سیستم برنامه‌ریزی منابع سازمانی متداول شامل ماژول‌های زیر است:

۱۲. دفتر کل

- **امور مالی**- ماژول مالی[2]، هسته اصلی بسیاری از سیستم‌های نرم‌افزاری برنامه‌ریزی منابع سازمانی است که می‌تواند داده‌های مالی را از بخش‌های عملکردی گوناگون گردآوری و گزارش‌های مالی چون دفتر کل، تراز آزمایشی، ترازنامه و صورت‌های مالی سه‌ماهه را تهیه کند. زمینه‌های زیر در ماژول مالی پوشش داده می‌شود:

- **دفتر کل**- مخزن اصلی همه اطلاعات مالی است. همه ماژول‌های دیگر، داده‌ها را به دفتر کل تغذیه می‌کنند و گزارش‌های مالی مانند صورت سود و زیان، ترازنامه و غیره از دفتر کل تهیه می‌شوند.

کارکردهای گوناگون دفتر کل به شرح زیر است:

- ورود داده‌های مربوط به دفاتر معین در قالب ثبت‌های روزنامه؛
- ورود مستقیم ثبت‌ها به دفتر کل برای ثبت معاملات واقعی و بودجه‌ای. ورود ثبت‌های تعهدی[3] برای ردیابی تعهدها از طریق فرآیند تأیید خرید و کنترل هزینه‌ها با مبالغ بودجه شده؛

---

1. Module
ماژول یک واحد مجزا از نرم‌افزار یا سخت‌افزار است. ویژگی‌های معمولی اجزای ماژولی عبارتند از قابل انتقال بودن، که به آن‌ها اجازه می‌دهد در سیستم‌های مختلف استفاده شوند، و قابلیت همکاری (عملکرد مشترک)، که به آنها اجازه می‌دهد با اجزای سایر سیستم‌ها کار کنند (م).

2. Financial Module

3. Encumbrance Journals
ثبت‌های روزنامه تعهدی، گاه، حسابداری تعهدی نامیده می‌شود. این نام‌گذاری زمانی منطقی‌تر می‌شود که متوجه می‌شوید تعهد، کنترل بودجه را با ثبت پولی که برای پروژه‌های آینده تخصیص داده می‌شود، امکان‌پذیر و از هزینه بیش از حد بودجه پیشگیری می‌کند (م).

- ❖ اصلاح اطلاعات واقعی، بودجه شده و تعهدها؛
- ❖ بررسی مانده‌حساب‌ها به‌صورت برخط یا از طریق گزارش‌های استاندارد یا پرسش‌های موردی[1].

ریسک‌های مرتبط با دفتر کل:

- ❖ صورت مغایرت‌های بانکی به‌صورت مرتب تهیه نمی‌شود.
- ❖ ثبت‌های تکراری به دفتر کل منتقل می‌شوند.
- ❖ ثبت‌های روزنامه در دوره حسابداری درست ثبت نمی‌شوند. تغییرات غیرمجاز در فهرست حساب‌ها داده می‌شود.

پرسش‌های مرتبط با حسابرسی:

- ❖ آیا صورتحساب‌های بانکی به‌طور منظم با دفتر کل مطابقت داده می‌شوند؟
- ❖ از نقل تنها یک بارِ اقلام دفتر روزنامه به دفتر کل اطمینان یابید.

۱۳. خرید و پرداختنی‌ها

ماژول‌های خرید

ماژول خرید[2] برای ایجاد و نگهداری نام تأمین‌کنندگان مواد و کالا، وارد کردن درخواست‌ها، درخواست استعلام و صدور سفارش‌های خرید استفاده می‌شود. ماژول خرید با ماژول‌های دیگر به‌صورت زیر ادغام می‌شود:

- ❖ **ماژول پرداختنی‌ها**- هنگامی که صورتحساب‌ها در حساب‌های پرداختنی ایجاد و به یک سفارش خرید ردیابی می‌شوند، داده‌های سفارش خرید از ماژول خرید گرفته و به ماژول پرداختنی‌ها منتقل می‌شود.
- ❖ **ماژول دفتر کل**[3]- ماژول خرید در قالب ثبت تعهدها، اطلاعات تعهد را به دفتر کل انتقال می‌دهد.

1. Ad Hoc Queries
پرسش‌های موردی زمانی ایجاد می‌شوند که پرسش‌های طرح شده، با مجموعه داده‌های از پیش تعیین یا تعریف شده قابل حل نیستند (م).
2. Purchasing Module
3. General Ledger Module

ماژول پرداختنی‌ها

ماژول پرداختنی‌ها، برای وارد کردن صورتحساب‌های دریافت شده از تأمین‌کنندگان مواد و کالا و پرداخت با صدور چک یا انتقال الکترونیکی وجه[1] استفاده می‌شود. ماژول پرداختنی‌ها با ماژول‌های دیگر به صورت صفحه آتی ادغام می‌شود:

- **ماژول خرید**- اطلاعات سفارش خرید برای مطابقت با صورتحساب‌ها از ماژول خرید بدست می‌آید. بانک اطلاعاتی تأمین‌کنندگان مواد و کالا نیز بین ماژول خرید و پرداختنی‌ها به اشتراک گذاشته می‌شود.
- **ماژول دفتر کل**- ثبت‌های حسابداری به دفتر کل منتقل می‌شوند.

ریسک‌های مربوط به ماژول خرید و پرداختنی‌ها:

- سازمان ممکن است از فروشندگان تأیید نشده استفاده کند؛
- درخواست‌های بدون مجوز ممکن است در سیستم پردازش شوند؛
- سفارش‌های خرید ممکن است با سیاست‌ها و رویه‌های تدارکاتی (پشتیبانی) مربوط، مطابق نباشند؛
- پرداخت سفارش‌های خرید لغو شده ممکن است مورد پردازش قرار گیرد.

روش‌های حسابرسی که حسابرس می‌تواند اجرا کند:

- چگونه با سیستم برنامه‌ریزی منابع سازمانی از بکارگیری تأمین‌کنندگان مواد و کالای تأیید نشده پیشگیری می‌کنید؟
- چگونه ورود درخواست توسط کارکنان غیرمجاز در سیستم را کنترل می‌کنید؟
- چه کسی اجازه دسترسی به اجزای مختلف سیستم برنامه‌ریزی منابع سازمانی را صادر و چه کسی امتیاز دسترسی را تأیید می‌کند؟
- چگونه از زیرِ پا گذاری یا نادیده گرفتن کنترل‌های دسترسی در سیستم برنامه‌ریزی منابع سازمانی توسط کارکنان، پیشگیری می‌کنید؟

1. Electronic Funds Transfer (EFT)

۱۴. مدیریت وجوه نقد

مدیریت وجوه نقد مستلزم موارد زیر است:

- دسترسی به اطلاعات بودجه، دریافت وجوه نقد و بانکداری توسط وزارتخانه‌ها، دریافت از خزانه‌داری و پرداخت‌ها.
- تهیه صورت مغایرت حساب‌های بانکی (دستی یا برخط).
- تمهیدات بانکی گوناگون.
- پیش‌بینی وجوه نقد.

ریسک‌های مربوط به مدیریت دریافت‌های نقدی:

- همه مبالغ دریافت شده، ثبت نشوند.
- دریافت‌های نقدی ثبت شده ممکن است نادرست، ناقص و بی‌موقع باشند.

پرسش‌های مرتبط با حسابرسی:

- چگونه از ثبت همه وجوه دریافتی در سیستم برنامه‌ریزی منابع سازمانی اطمینان می‌یابید؟
- چگونه از ثبت درست، کامل و به‌موقع وجوه دریافتی، اطمینان حاصل می‌کنید؟

۱۵. دریافتنی‌ها

اطلاعات حساب‌های دریافتنی و دریافت‌های متفرقه، پردازش و در دفتر کل یکپارچه می‌شوند.

ریسک‌های مرتبط با حساب‌های دریافتنی:

- مدیریت ضعیف بدهکاران.
- پرداخت‌های نامنظم توسط بدهکاران.
- تکراری بودن حساب‌های بدهکاران.
- حذف حساب‌های دریافتنی مشکوک‌الوصول.

پرسش‌های مرتبط با حسابرسی:

- برای تعیین وجود کنترل‌های مناسب برای مدیریت درست بدهکاران، سیستم برنامه‌ریزی منابع سازمانی را بررسی کنید.
- فهرستی از همه بدهکاران ثبت شده در سیستم برنامه‌ریزی منابع سازمانی را درخواست و نبود تکرار در آن را بررسی کنید.
- سیاست‌های مربوط به حذف مطالبات مشکوک‌الوصول را درخواست و بکارگیری کنترل‌ها را در سیستم برنامه‌ریزی منابع سازمانی مطابق با این سیاست‌ها، آزمون کنید.

۱۶. بودجه‌بندی

ماژول بودجه‌بندی بخش عمومی، بودجه مصوب و اطلاعات تکمیلی بودجه را برای دفتر کل فراهم می‌کند. بودجه‌ها برای تخصیص و اجرا به ماژول دفتر کل منتقل می‌شوند. اطلاعات موجود بودجه برای تخصیص، به بخش مالی عمومی منتقل می‌شوند. اطلاعات مربوط به این تخصیص توسط ماژول‌های خرید، پرداختنی و دفتر کل، برای انجام معامله استفاده می‌شود.

ریسک‌های مرتبط با ماژول بودجه‌بندی:

- منابع مالی بیش از بودجه مصرف می‌شود (مصرف بیش از بودجه منابع مالی).
- بازنگری‌های غیرمجاز در بودجه، در گزارش‌های نادرست بودجه در سیستم برنامه‌ریزی منابع سازمانی انجام می‌شود.

پرسش‌های مرتبط با حسابرسی:

- حسابرس چگونه مصرف وجوه بیش از بودجه را آزمون می‌کند؟
- رویه‌های بازنگری در بودجه را بررسی کنید تا از وجود کنترل‌های لازم در سیستم برنامه‌ریزی منابع سازمانی برای اینکه تنها کارکنان مجاز می‌توانند تغییرات لازم را در بودجه ایجاد کنند، اطمینان یابید.
- گزارش‌های بودجه را بررسی و درستی و کامل بودن گزارش‌ها را تأیید کنید.
- مطابق با قوانین و مقررات مربوط به مدیریت مالی عمومی، وجود فهرست حساب‌ها را تعیین کنید.

۱۷. فروش و بازاریابی

ماژول فروش، وظایف دریافت سفارش فروش، برنامه‌ریزی سفارش‌ها، ارسال و صدور صورتحساب را اجرا می‌کند. ماژول فروش به مقدار بسیار زیادی با وب‌سایت‌های تجارت الکترونیک سازمان یکپارچه شده است. بسیاری از فروشندگان سیستم برنامه‌ریزی منابع سازمانی، درگاه فروشگاه برخط را به‌عنوان بخشی از ماژول فروش ارائه می‌دهند. ماژول بازاریابی سیستم برنامه‌ریزی منابع سازمانی همراه با پشتیبانی برنامه‌ریزی ارتباط با مشتری[1] به تولید، ارسال مستقیم و دیگر کارهای بازاریابی منجر می‌شود.

1. Customer Relationship Planning (CRP)

۱۸. موجودی‌های مواد و کالا

ماژول موجودی‌های مواد و کالا، فرآیندهای نگهداری سطح مناسب کالا در انبار را آسان می‌کند. فعالیت‌های کنترل موجودی‌ها شامل شناسایی نیاز به موجودی، تعیین هدف (مقدار لازم)، ارائه فنون و گزینه‌های تجدید دوباره، نظارت بر مصرف اقلام، تطبیق مانده موجودی‌ها و گزارش وضعیت موجودی‌ها است. ادغام ماژول کنترل موجودی با ماژول‌های فروش، خرید و مالی به سیستم‌های برنامه‌ریزی منابع سازمانی این امکان را می‌دهد تا گزارش‌های هوشمند مدیریتی تولید کنند.

۱۹. مدیریت منابع انسانی

این ماژول، مدیریت منابع انسانی را ساده‌تر می‌کند. همچنین، بانک اطلاعاتی کاملی از کارکنان شامل اطلاعات تماس، جزییات حقوق و دستمزد، حضور، ارزیابی عملکرد و ارتقای همه کارکنان را به وجود می‌آورد.

۲۰. ماژول تولید

ماژول تولید، برنامه‌ریزی تولید، استفاده از ظرفیت تولیدی، قطعات، اجزا و منابع مواد اولیه را با بکارگیری داده‌های تاریخی، بهینه‌سازی می‌کند.

۲۱. امنیت برنامه کاربردی

امنیت برنامه بر موارد زیر متمرکز است:

- در دسترس بودن مستمر سیستم.
- یکپارچگی اطلاعات ذخیره شده در سیستم.
- حفظ محرمانگی داده‌های ذخیره شده یا در جریان انتقال.
- پیروی از الزامات و تعهد به قوانین و مقررات لازم‌الاجرا.

ریسک‌های مرتبط با امنیت برنامه کاربردی:

- قصور در شناسایی نقص‌های سیستم عامل.
- دسترسی غیرمجاز.
- از دست دادن محرمانگی و حریم خصوصی.
- در دسترس نبودن سیستم/ نقض قوانین و مقررات تداوم کسب وکار.

- ❖ سوء جریان‌ها[1]، تقلب[2]، اقدامات نادرست، اشتباه‌ها و از قلم انداختن‌ها.
- ❖ از دست دادن زنجیره عطف حسابرسی.
- ❖ قصور در شناسایی تهدیدهای امنیتی.

ویژگی‌های بنیادی گذرواژه از یک سازمان به سازمان دیگر، فرق می‌کند. سیاست‌های فناوری اطلاعات و ارتباطات باید قوانین قابل قبولی را به‌روشنی بیان کند که حسابرس فناوری اطلاعات باید براساس آن‌ها، سیستم‌ها را آزمون کند. برخی از روش‌های رسیدگی و پرسش‌هایی که حسابرس ممکن است بررسی کند، در زیر آمده است:

- ❑ کنترل‌های دسترسی منطقی موجود برای سیستم برنامه‌ریزی منابع سازمانی را بررسی و انطباق آن را با شرح‌های شغل، تعیین کنید.
- ❑ حسابرس باید موارد زیر را بررسی کند:
  - ❖ حسابرس باید از اینکه طول، ترکیب، تاریخچه و سایر ویژگی‌های بنیادی گذرواژه با خط‌مشی سازمان منطبق است، اطمینان یابد.
  - ❖ گذرواژه‌های پیش‌فرض باید هنگام اجرای سیستم برنامه‌ریزی منابع سازمانی تغییر کنند.
  - ❖ کاربر باید تنها سه بار بتواند گذرواژه نادرست را وارد کند پیش از آنکه سیستم امکان استفاده کاربر را قطع کند.
  - ❖ نقش‌ها/ پروفایل‌های کاربران پراستفاده، از جمله حساب‌های کاربری پیش‌فرض خاص باید مطابق با مسئولیت‌های عملکردی، اختصاص داده شوند.
  - ❖ دسترسی به جداول/ بانک‌های اطلاعاتی حساس باید بر مبنای نیاز کسب‌وکار باشد.
  - ❖ حسابرس باید از فعال بودن زنجیره عطف حسابرسی در سیستم برنامه‌ریزی منابع سازمانی و بررسی مرتب آن، اطمینان بدست آورد.

ماژول‌های یاد شده، ماژول‌های معمول و رایج هستند. ماژول‌های سیستم برنامه‌ریزی منابع سازمانی در سازمان‌ها بنا بر سیستم و صنعت، متفاوت خواهد بود. برای مثال، سیستم برنامه‌ریزی منابع سازمانی یک دانشگاه دارای ماژول‌هایی است که سیستم برنامه‌ریزی منابع سازمانی شهرداری، آن‌ها را ندارد.

1. Irregularities
2. Fraud

۲۲. ابزارهای موجود برای کمک به حسابرسی سیستم برنامه‌ریزی منابع سازمانی

تعداد زیادی ابزار برای کمک به حسابرسی سیستم برنامه‌ریزی منابع سازمانی وجود دارد. برخی از آن‌ها به شرح زیر است:

- SAP- سیستم اطلاعات حسابرسی- حسابرس می‌تواند گزارش‌های گوناگون مربوط به کسب‌وکار و سیستم را تهیه کند.
- Audit Vault- برای حسابرسی اوراکل می‌تواند مورد استفاده قرار گیرد.
- ACL- کدهای دستوری[1] قابل‌اجرا برای گرفتن مستقیم داده‌ها از جداول و همچنین، دریافت هشدارهای مشخص.
- IDEA[2].
- حسابرس برای درک چگونگی عملکرد یک سیستم برنامه‌ریزی منابع سازمانی خاص و تراکنش لازم برای کسب اطلاعات مشخصی از سیستم، می‌تواند در دوره‌هایی شرکت کند که همه فروشندگان اصلی سیستم برنامه‌ریزی منابع سازمانی برگزار می‌کنند.

اصطلاحاتی که در فصل ۱۳ بر آن تأکید شده است:

- **سیستم برنامه‌ریزی منابع سازمانی (Enterprise Resource Planing System)**- با ادغام وظایف گوناگونی که اطلاعات بین آن‌ها مبادله می‌شود، در پی حذف رویکرد مدیریت پراکنده اطلاعات تجاری است. هدف اصلی یک سیستم برنامه‌ریزی منابع سازمانی، آسان‌سازی جریان اطلاعات بین همه بخش‌های تجاری سازمان و مدیریت ارتباطات با ذینفعان برون‌سازمانی می‌باشد. یک سیستم برنامه‌ریزی منابع سازمانی با استفاده از یک بانک اطلاعاتی به‌عنوان مخزن اطلاعات، معمولاً بر روی تعدادی از سخت‌افزارهای مختلف و پیکربندی‌های شبکه، قابل اجرا است.

- **عملیات یک سیستم برنامه‌ریزی منابع سازمانی (Operation of an ERP Application)**- ماژول‌های یک سیستم برنامه‌ریزی منابع سازمانی، بسیار به یکدیگر متکی هستند. برای درک حسابرسی برنامه‌ریزی منابع سازمانی باید ارتباط و گردش داده‌ها در بین ماژول‌ها را بشناسیم. بنابراین، بکارگیری رویکرد فرآیندی/ چرخه‌ای در مقایسه با رویکرد ماژولی (جداگانه) در حسابرسی سیستم‌های برنامه‌ریزی منابع سازمانی مناسب است. یک سیستم برنامه‌ریزی منابع سازمانی متداول شامل ماژول‌های دفتر کل، خرید و پرداختنی‌ها، مدیریت وجوه نقد، دریافتنی‌ها، بودجه‌بندی، فروش و بازاریابی، موجودی‌های مواد و کالا، مدیریت منابع انسانی، تولید و امنیت برنامه است.

---

1. Scripts

۲. یک سیستم خبره مبتنی بر رایانه است که راه حل‌هایی را برای کار در زمینه نظارت بر ادغام و ارزیابی داخلی ارائه می‌دهد.

فصل ۱۴

گزارشگری

۱. استانداردهای گزارشگری

استاندارد بین‌المللی دیوان‌های محاسبات بخش ۱۷۰۰ با نام **"اظهار نظر و گزارش درباره صورت‌های مالی"**، مقرر می‌دارد نظر حسابرس باید به شکل تعیین شده در استاندارد، ارائه شود.

چارچوب اطمینان‌بخش فناوری اطلاعات (ITAF)، راهنمایی‌هایی را در زمینه طراحی، انجام و گزارشگری حسابرسی فناوری اطلاعات و وظایف اطمینان بخشی ارائه می‌کند. اصطلاحات فنی و مفاهیم خاص اطمینان‌بخشی فناوری اطلاعات را تعریف و استانداردهایی را برای تعیین نقش‌ها و مسئولیت‌های حرفه‌ای متخصصان فناوری اطلاعات و الزامات دانش و مهارت‌های آنان، اجرای کار و گزارشگری نیز تعیین می‌کند.

حسابرس در پایان حسابرسی باید گزارشی کتبی را به‌گونه‌ای مناسب، تهیه و یافته‌ها را به شکلی مناسب ارائه کند. محتوا باید به‌آسانی قابل‌درک باشد، ابهام یا پیچیدگی نداشته باشد و تنها شامل اطلاعات با پشتوانه کافی و مربوط، مستقل، عینی، منصفانه و سودمند باشد.

- ❑ در حالت ایده‌آل، حسابرسی فناوری اطلاعات بخشی از حسابرسی مالی است.
- ❑ اگر ضعف‌های پوشش داده نشده دارای اهمیت باشند، یافته‌های حسابرسی فناوری اطلاعات ممکن است به‌عنوان بخشی از نامه مدیریت حسابرسی مالی، گزارش شود که باید شامل موارد زیر باشد:
  - ❖ طبقه‌بندی یافته‌ها؛
  - ❖ شرح یافته‌ها؛
  - ❖ آثار یافته‌ها؛
  - ❖ پیشنهادها؛
  - ❖ پاسخ مدیریت؛ و پیشنهادهای حسابرس.
- ❑ برخی از دیوان‌های محاسبات، تلخیصی از نامه مدیریت را به‌عنوان یک گزارش عمومی- مطابق با رویه عمل استاندارد بخش ۱۷۰۰ قسمت ۵ - منتشر می‌کنند.

استاندارد بین‌المللی دیوان‌های محاسبات بخش ۱۷۰۶، گزارش مسأله‌های فناوری اطلاعات را در بخش‌هایی از گزارش حسابرسی صورت‌های مالی به شرح زیر پیشنهاد می‌کند:

- **تأکید بر مطلب خاص:**
  - ضعف با اهمیت در کنترل‌های داخلی.
  - مسأله‌های مربوط به عدم رعایت.
- **سایر موارد:**
  - نقاط ضعف کنترلی.

۲. سطوح گزارشگری

حسابرس باید یافته‌های خود را به‌موقع گزارش دهد و (گزارش) باید برای سازمان مورد رسیدگی، سازنده و سودمند باشد. حسابرس ممکن است بنابر علت انجام حسابرسی، به نهادهای گوناگون گزارش دهد. برای مثال:

- سازمان ممکن است از حسابرس خواسته باشد که کنترل‌ها را بررسی کند.
- سازمان حامی ممکن است درخواست بررسی داشته باشد.
- بررسی ممکن است بخشی از حسابرسی مالی سالانه باشد و یافته‌های حسابرس در گزارش سالانه حسابرس گنجانده شود.
- حسابرسی ممکن است به نمایندگی از یک نهاد نظارتی انجام شده باشد.

سطوح گزارشگری بدون در نظر گرفتن موارد بالا قابل ارائه است، اما الزامات گزارشگری برای هر یک از موارد بالا از یک سازمان به سازمان دیگر و از یک دیوان به دیوان دیگر متفاوت خواهد بود. حسابرس باید دریافت‌کننده نهایی گزارش را تعیین و گزارش را مطابق نیاز آن تنظیم کند.

سه سطح گزارشگری در فرآیند حسابرسی وجود دارد:

- پیش‌نویس گزارش- فرآیند گزارشگری با خواندن پیش‌نویس اول شروع می‌شود. این پیش‌نویس پیش از نشست پایانی برای مدیریت میانی سازمان فرستاده می‌شود. سپس، این پیش‌نویس برای گفتگو در نشست پایانی در نظر گرفته می‌شود. این امر سبب می‌شود مطالب حساسیت‌زا، اشتباه‌های واقعی یا ناهماهنگی‌ها در همان مراحل اولیه شناسایی، اصلاح یا حذف شود. حسابرس پس از گفتگو درباره این پیش‌نویس با سازمان، اصلاحات لازم را انجام می‌دهد و نخستین پیش‌نویس رسمی خود را برای سازمان می‌فرستد.

- نامه مدیریت (پیش‌نویس رسمی)- این پیش‌نویس رسمی به سازمان ارائه می‌شود تا بتواند به مسأله‌های مطرح شده، پاسخ دهد. بدین ترتیب مدیریت می‌تواند بر یافته‌ها، نتیجه‌گیری‌ها و پیشنهادهای ارائه شده در پیش‌نویس رسمی که دریافت می‌کند، متمرکز شود. در این مرحله، مدیریت وظیفه دارد که به‌طور رسمی، نظرها و پاسخ‌های خود را درباره همه یافته‌های حسابرس، بنویسد.
- گزارش حسابرس (گزارش نهایی حسابرس)- حسابرس پس از دریافت نظرهای سازمان، پاسخی را که نشان‌دهنده موضع حسابرس است، ارائه می‌دهد. این امر با قرار دادن نظرهای حسابرس و پاسخ سازمان در یک گزارش که گزارش حسابرس است، حاصل می‌شود.

۳. اجزای گزارش‌های استاندارد

هر استاندارد بین‌المللی عموماً شامل یک یا چند نوع گزارش و الگوهایی است که از آن‌ها برای انواع گوناگون گزارش استفاده می‌شود. اما، مضامین مشترکی در همه گزارش‌های حسابرسی وجود دارد. دو قالب استاندارد گزارش در زیر آمده است که به ترتیب می‌توانند برای گزارش یافته‌های حسابرسی مالی و گزارش حسابرسی فناوری اطلاعات استفاده شوند. این قالب‌ها مطابق با استاندارد بخش ۱۷۰۰ هستند.

۴. گزارش حسابرسی مالی

۴-۱. گزارش استاندارد حسابرس

حسابرس گزارش استانداردی را ارائه می‌دهد که بیانگر نظر حسابرس است. اجزای اصلی و الزامی گزارش حسابرس برای مطابقت با استانداردهای بین‌المللی حسابرسی به شرح زیر است:

- گزارش، کتبی است.
- گزارش حسابرس باید عنوانی داشته باشد که مشخصاً نشان دهد گزارش یک حسابرس مستقل است.
- مخاطب گزارش حسابرس باید با توجه به شرایط قرارداد و یا الزامات قانونی مشخص شود.
- حسابرس هنگامی گزارش استاندارد ارائه می‌کند که اظهارنظر وی، تعدیل نشده باشد.

محتوای یک گزارش- گزارش استاندارد حسابرس شامل ۹ بخش زیر است:

بند مقدمه

در بند مقدمه گزارش حسابرس باید مطالب زیر تصریح شود:

- نام سازمانی که صورت‌های مالی آن، حسابرسی شده است؛
- اینکه صورت‌های مالی، حسابرسی شده است؛
- برشمردن عناوین صورت‌های مالی حسابرسی شده؛
- عطف یادداشت‌های توضیحی صورت‌های مالی؛
- تاریخ و دوره زیر پوشش صورت‌های مالی.

مسئولیت مدیریت در قبال صورت‌های مالی

گزارش حسابرس باید شامل بخشی با نام **"مسئولیت هیأت مدیره (یا ارکان مشابه آن) در قبال صورت‌های مالی"** باشد. در این بخش از گزارش حسابرس، مسئولیت‌های اشخاصی که در قبال تهیه صورت‌های مالی مسئولیت دارند، توصیف می‌شود. این مسئولیت عموماً به عهده هیأت مدیره سازمان یا ارکان مشابه آن است. حسابرس می‌تواند برای توصیف این مسئولیت از اصطلاحات قانونی و مقرراتی در صورت مشابهت با عبارت‌های گزارش استاندارد حسابرسی، استفاده کند.

مسئولیت حسابرس

گزارش حسابرس باید شامل بخشی با نام **"مسئولیت حسابرس"** باشد. در گزارش حسابرس باید بیان شود که مسئولیت حسابرس، اظهارنظر نسبت به صورت‌های مالی بر اساس حسابرسی انجام شده طبق استانداردهای حسابرسی است و نشان دهد که حسابرسی، طبق استاندارد بین‌المللی حسابرسی دیوان‌های محاسبات یا مطابق با دستورالعمل قانونی دیوان‌های محاسبات انجام شده است. در صورت تهیه صورت‌های مالی مطابق با چارچوب ارائه منصفانه متناسب با شرایط موجود، در گزارش حسابرس به **"تهیه و ارائه منصفانه صورت‌های مالی که تصویری درست و منصفانه ارائه می‌کند"** اشاره می‌شود. در گزارش حسابرس باید تصریح شود که حسابرس اعتقاد دارد، شواهد حسابرسی کسب شده به‌عنوان مبنایی برای اظهارنظر، کافی و مناسب است.

اظهارنظر حسابرس

گزارش باید شامل بخشی با نام **"اظهارنظر"** باشد که نظر ارائه شده بر اساس ارزیابی حسابرس را نشان دهد. هنگام ارائه اظهار نظر تعدیل نشده در مورد صورت‌های مالی تهیه شده، متن اظهارنظر

تعدیل نشده متناسب با چارچوب گزارشگری مالی است که از آن استفاده می‌شود. طبق یک چارچوب ارائه منصفانه، اظهارنظر حسابرس، مگر در مواردی که قانون یا مقررات تصریح کرده باشد، به یکی از عبارت‌های زیر بیان می‌شود، که معادل یکدیگر تلقی می‌شوند.

۱. ... به‌طور منصفانه نشان می‌دهد[1].

۲. ... به نحو مطلوب نشان می‌دهد[2].

۵. سایر مسئولیت‌های گزارشگری

گزارشگری عمومی

حسابرس باید توجه داشته باشد که برخی از موارد گزارش شده در حسابرسی سیستم‌های اطلاعاتی، ممکن است آسیب‌پذیری آن سیستم را برای دسترسی توسط افراد غیرمجاز، به‌شدت افزایش دهد. دیوان‌های محاسبات باید برای چگونگی ارائه این موارد در پارلمان و انجام اقدامات اصلاحی راهی بیابند.

ارتباط با حسابرسان قانونی و گزارشگری در مورد سیستم‌های اطلاعاتی مالی کلیدی

حسابرسان فناوری اطلاعات باید همیشه حسابرسان مالی (یا دیگر حسابرسانی) را در نظر بگیرند که اطلاعات مالی تولید شده توسط سیستم‌های اطلاعاتی را حسابرسی می‌کنند. نقاط ضعف شناسایی‌شده، به‌ویژه موارد اثرگذار بر قابلیت اتکا بر سیستم تهیه صورت‌های مالی واقعی و منصفانه باید با حسابرسان مالی در میان گذاشته شود. حسابرس باید از بکارگیری اصطلاحات فوق تخصصی بپرهیزد تا مسأله‌ها، توسط حسابرس مالی نیز قابل فهم باشد.

سیستم‌های مالی کلیدی (به‌اختصار IFMIS)، بخش عمده‌ای از صورت‌های مالی مورد رسیدگی دیوان محاسبات را تولید می‌کنند. اهمیت حسابرسان فناوری اطلاعات در این است که این سیستم‌ها را حسابرسی و نقاط ضعف کنترلی را به گروه حسابرسی مالی اعلام می‌کنند. در صورت نیاز به انجام روش‌های حسابرسی بیشتر توسط حسابرس مالی در وزارتخانه‌ها یا سازمان‌ها، این موضوع باید به دریافت‌کنندگان گزارش‌ها نیز اطلاع داده شود. توجه به صلاحیت حسابرسان مالی برای انجام این روش‌ها نیز باید مورد توجه قرار گیرد.

1. … Give a true and fair view of […]
2. … Present Fairly …

اصطلاحاتی که در فصل ۱۴ بر آن تأکید شده است:

- **گزارش استاندارد حسابرس (The Auditor's Standard Report)**- حسابرس هنگامی گزارش استاندارد صادر می‌کند که اظهارنظر وی، تعدیل شده نباشد. اجزای گزارش استاندارد حسابرس در این فصل آمده است.

- **گزارشگری (Reporting)**- استاندارد بین‌المللی دیوان‌های محاسبات بخش ۱۷۰۰ با نام **"اظهار نظر و گزارش در مورد صورت‌های مالی"**، مقرر می‌دارد نظر حسابرس باید به شکل تعیین شده در استاندارد، ارائه شود. حسابرس باید در پایان حسابرسی، گزارش کتبی خود را به‌گونه‌ای مناسب، تهیه و یافته‌ها را به شکلی مناسب ارائه کند. محتوا باید به‌آسانی قابل درک باشد، ابهام یا پیچیدگی نداشته باشد و تنها شامل اطلاعات با پشتوانه کافی و مربوط، مستقل، عینی، منصفانه و سودمند باشد.

پیوست‌ها

فهرست پیوست‌ها

پیوست ۴: ارزیابی ریسک

۱) فرآیند کسب‌وکار و شناسایی ریسک

- ❖ راهنما
- ❖ شرح سیستم

۱-۱) شرح سیستم و ارزیابی ریسک فرآیند کسب‌وکار- نمونه

۱-۲) فهرست ریسک‌ها

- ❖ کلیات
- ❖ یادداشت‌های راهنما
- ❖ فهرست ریسک‌ها

۲) ارزیابی ریسک و برخورد با آن

- ❖ کلیات
- ❖ یادداشت‌های راهنما
- ❖ ارزیابی ریسک و برخورد با آن

۳) مستندسازی نشست گروه کاری

۴) طرح کلی حسابرسی

پیوست۵: اجرای حسابرسی

۱) برنامه حسابرسی

- ❖ کلیات
- ❖ یادداشت‌های راهنما
- ❖ برنامه حسابرسی

۲) استفاده از کار حسابرس دیگر

۳) استفاده از کار کارشناس

۴) کاربرگ بازخورد پشتیبانی حسابرسی فناوری اطلاعات

پیوست ۶: گزارشگری

۱) نامه مدیریت

۲) تأییدیه مدیران

۳) گزارش حسابرس

۴) تأییدیه مدیر حسابرسی

۵) نکات قابل توجه در حسابرسی سال آتی

پیوست ۱:
طرح حسابرسی و برنامه‌ریزی سالانه

برآورد ریسک طرح کلی حسابرسی
سیستم‌های اطلاعاتی

توجه: این کاربرگ **"دامنه حسابرسی و برآورد ریسک کلی حسابرسی"** باید همواره توسط دیوان محاسبات (SAI) به‌روزآوری شود تا حجم حسابرسی دیوان محاسبات و پروفایل ریسک سیستم‌های اطلاعاتی مختلف سازمان مورد رسیدگی را در برگیرد. برای مثال این کاربرگ باید دستِ‌کم هر سال یک‌بار و هر زمان که ممکن باشد، بررسی و به‌روزآوری شود.

الزامات خاص استانداردهای استفاده شده در این کاربرگ

۱) استاندارد بین‌المللی دیوان‌های محاسبات بخش ۵۳۰۰

۲) استانداردهای انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۱-۱۲۰۲

هدف

هدف این کاربرگ، برآورد ریسک سیستم‌های اطلاعاتی در درون سازمان برای تهیه طرح کلی حسابرسی و تعیین اولویت‌ها برای تخصیص مؤثر منابع در اجرای حسابرسی است.

راهنمای رتبه‌بندی ریسک

تهیه‌کننده:		بررسی‌کننده:	نام	رتبه
رتبه:		سطح ۱:		
تاریخ:		سطح ۲:		
		سطح ۳:		

یادداشت‌های توضیحی

این کاربرگ، حسابرس را در تکمیل کاربرگ برآورد **ریسک کلی حسابرسی** راهنمایی می‌کند. رتبه انتخابی برای یک عامل در ضریب انتخابی همان عامل ضرب می‌شود تا امتیاز شاخص آن ریسک به‌دست آید. لطفاً توجه کنید که حسابرس باید هنگام تصمیم‌گیری درباره عوامل، رتبه‌ها و ضریب‌ها از قضاوت حرفه‌ای استفاده نماید. (رتبه‌بندی در این کاربرگ برای نمونه است).

جمع ضریب‌ها باید ۱۰۰ باشد.

	عوامل	ضریب	رتبه‌بندی	
۱	آیا سیستم به عملیات مهم بنگاه مرتبط است؟	۱۵	سیستم از عملکرد مهم بنگاه پشتیبانی می‌کند.	۱
			با راهبری الکترونیک ارتباط دارد.	۰/۷۵
			برای سایر عملکردهای پشتیبانی استفاده می‌شود (حقوق و دستمزد، موجودی کالا، حسابداری مالی، تدارکات و غیره).	۰/۵
۲	تعداد کاربران سیستم	۵	بیش از ۱۰۰	۱
			بیش از ۵۰ اما کمتر از ۱۰۰	۰/۷۵
			بیش از ۱۰ اما کمتر از ۵۰	۰/۵
			کمتر از ۲۵	۰/۲۵
۳	تعداد رابط‌های سیستم	۱۰	بیش از ۵	۱

	عوامل	ضریب	رتبه‌بندی	
			۳ یا ۴ رابط	۰/۷۵
			۱ یا ۲ رابط	۰/۵
			بدون رابط	۰
۴	روش اتصال به شبکه (شبکه داخلی، شبکه خارجی یا مبتنی بر وب/ دامنه عمومی)	۱۰	صفحه وب/ دامنه عمومی	۱
			شبکه گسترده (WAN)، شبکه شهری (MAN) و/ یا شبکه خارجی	۰/۷۵
			شبکه داخلی (LAN) و/یا روی شبکه داخلی	۰/۵
			غیر متصل به هیچ شبکه‌ای	۰
۵	تعداد سال‌های فعالیت سیستم	۵	کمتر از یک سال	۱
			بین ۲ تا ۵ سال	۰/۷۵
			بین ۷ تا ۱۰ سال	۰/۵
			بیش از ۱۰ سال	۰/۲۵
۶	حجم داده‌ها در سیستم	۱۰	بیش از ۱ ترابایت	۱
			۵۰۰ گیگابایت تا ۱ ترابایت	۰/۷۵
			۱۰۰ گیگابایت تا ۵۰۰ گیگابایت	۰/۵
			کمتر از ۱۰۰ گیگابایت	۰/۲۵
۷	حسابرسی سال پیش	۵	انجام نشده	۱
			۱ یا ۲ سال	۰/۷۵
			۳ یا ۴ سال	۰/۵
			۵ سال یا بیشتر	۰/۲۵

	عوامل	ضریب	رتبه‌بندی	
۸	انواع سیستم‌ها (خریداری شده به‌صورت آماده یا تدوین درون‌سازمانی)	۱۵	تدوین درون‌سازمانی بدون فرآیند توسعه قابل تأیید	۱
			تدوین درون‌سازمانی با فرآیند توسعه قابل تأیید	۰/۷۵
			خریداری شده به‌صورت آماده و با تغییرات	۰/۵
			خریداری شده به‌صورت آماده و بدون تغییرات	۰/۲۵
۹	بودجه یا وجوهی که در سیستم پردازش می‌شوند.	۱۵	بیش از ۷۵ درصد	۱
			بیش از ۵۰ درصد اما کمتر از ۷۵ درصد	۰/۷۵
			بیش از ۲۵ درصد اما کمتر از ۵۰ درصد	۰/۵
			کمتر از ۲۵ درصد	۰/۲۵
۱۰	منافع ذینفعان	۱۰	منافع و قدرت بسیار زیاد(برای مثال مجلس/ رئیس‌جمهور)	۱
	★ منافع ذینفعان ممکن است بسیار ذهنی (غیرعینی) باشد و دیوان محاسبات باید روشی برای تصمیم‌گیری در مورد این عامل داشته باشد.		منافع و قدرت زیاد	۰/۷۵
			منافع زیاد و قدرت کم (یا منافع کم و قدرت زیاد)	۰/۵
			منافع و قدرت کم	۰/۲۵
	جمع	**۱۰۰**		

برآورد ریسک کلی دامنه حسابرسی

تهیه‌کننده:		بررسی‌کننده:	نام	رتبه	تاریخ
رتبه:		سطح ۱			
تاریخ:		سطح ۲			
		سطح ۳			

ردیف	نام سازمان مورد رسیدگی	نام سیستم اطلاعاتی	آیا سیستم با عملیات مهم بنگاه مرتبط است			تعداد کاربران سیستم			تعداد رابط‌های سیستم			روش اتصال به شبکه (شبکه داخلی، شبکه خارجی یا مبتنی بر وب / دامنه عمومی)			تعداد سال‌های فعالیت سیستم			حجم داده‌ها در سیستم			حسابرسی سال پیش			نوع سیستم‌ها (خریداری شده به‌صورت آماده یا تدوین درون‌سازمانی)			بودجه یا وجوه پردازش‌شده توسط سیستم			منافع ذینفعان			جمع امتیازات	رتبه (بالا، متوسط،پایین)	توضیحات رتبه
			ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز			
۱					۰			۰			۰			۰			۰			۰			۰			۰			۰			۰			۰		
۲																																		۰		
۳																																		۰		
۴																																		۰		
۵																																		۰		
۶																																		۰		

برآورد ریسک کلی دامنه حسابرسی

تهیه‌کننده:	حسابرسی فناوری اطلاعات	بررسی‌کننده:	نام	رتبه	تاریخ
رتبه:	سرپرست حسابرسی فناوری اطلاعات	سطح ۱	مدیر فنی حسابرسی فناوری اطلاعات	مدیر فنی حسابرسی فناوری اطلاعات	۱۳۹۹/۱۲/۲۷
تاریخ:	۱۳۹۹/۱۲/۲۵	سطح ۲	مدیر ارشد حسابرسی فناوری اطلاعات	مدیر ارشد حسابرسی فناوری اطلاعات	۱۳۹۹/۱۲/۲۸
		سطح ۳			

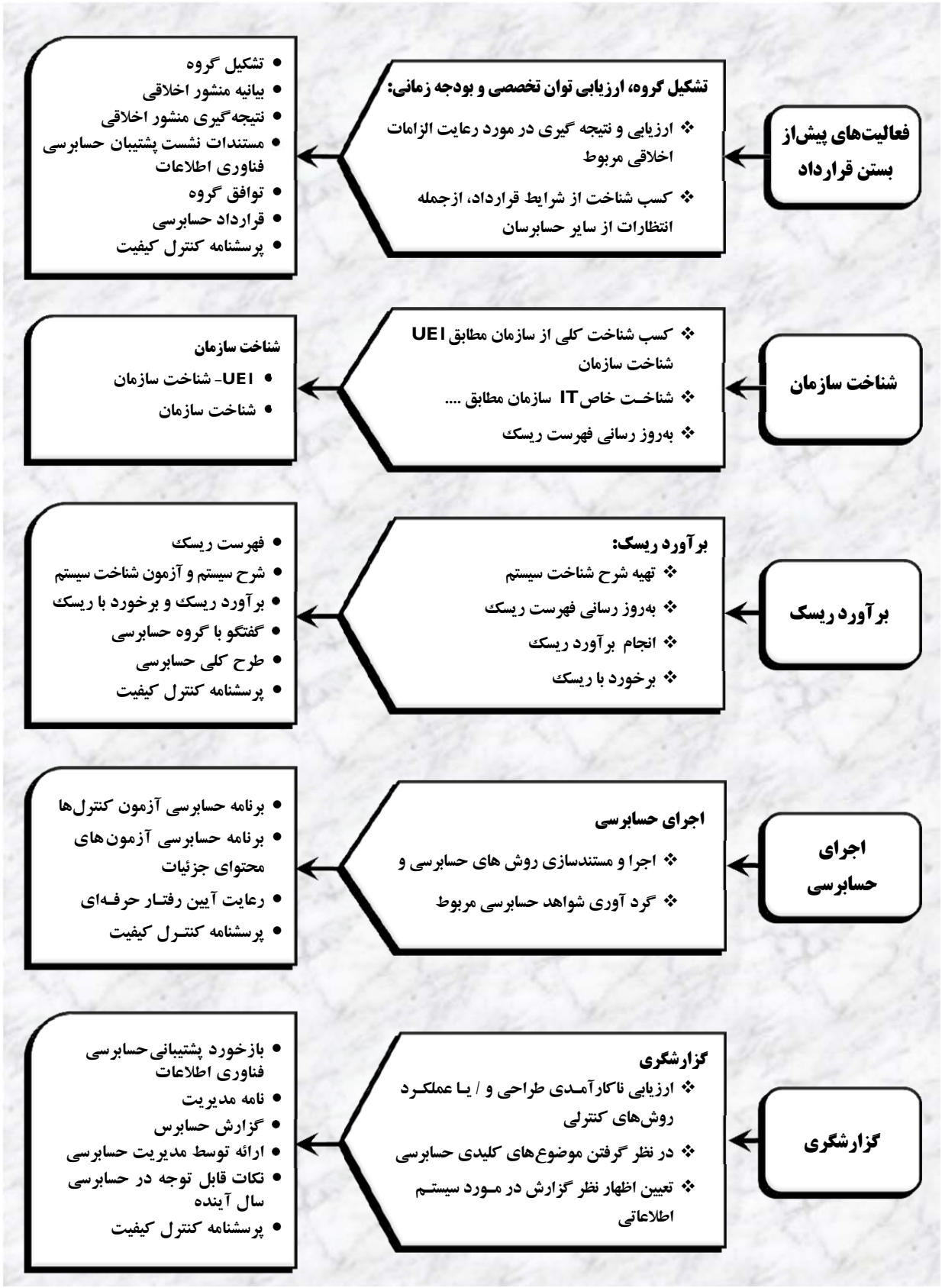
ردیف	نام سازمان مورد رسیدگی	نام سیستم اطلاعاتی	آیا سیستم با عملیات مهم بنگاه مرتبط است			تعداد کاربران سیستم			تعداد رابط‌های سیستم			روش اتصال به شبکه (شبکه داخلی، شبکه خارجی یا مبتنی بر وب/ دامنه عمومی)			تعداد سال‌های فعالیت سیستم			حجم داده‌ها در سیستم			حسابرسی سال پیش			نوع سیستم‌ها (خریداری شده به‌صورت آماده یا تدوین درون‌سازمانی)			بودجه یا وجوه پردازش شده توسط سیستم			منافع ذینفعان			جمع امتیازات	رتبه (بالا، متوسط،پایین)	توضیحات رتبه
			ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز	ضریب	رتبه	امتیاز			
۱	وزارت امور اقتصادی و دارایی	سیستم اطلاعاتی یکپارچه مدیریت مالی (IFMIS)	۱۵	۱	۱۵	۵	۱	۵	۱۰	۰/۵	۵	۱۰	۰/۷۵	۷/۵	۵	۰/۲۵	۱/۲۵	۱۰	۱	۱۰	۵	۰/۷۵	۳/۷۵	۱۵	۰/۵	۷/۵	۱۵	۱	۱۵	۱۰	۱	۱۰	۸۰	زیاد	
۲	وزارت امور اقتصادی و دارایی	سیستم مدیریت بدهی‌ها	۱۵	۱	۱۵	۵	۰/۵	۲/۵	۱۰	۰/۲۵	۲/۵	۱۰	۰/۵	۵	۵	۰/۲۵	۱/۲۵	۱۰	۰/۲۵	۲/۵	۵	۰/۷۵	۳/۷۵	۱۵	۰/۳	۳/۷۵	۱۵	۰/۵	۷/۵	۱۰	۰/۷۵	۷/۵	۵۱/۲۵	متوسط	
۳	وزارت زمین و شهرسازی	سیستم مدیریت املاک و مستغلات	۱۵	۱	۱۵	۵	۰/۵	۲/۵	۱۰	۰/۲۵	۲/۵	۱۰	۰/۷۵	۷/۵	۵	۰/۷۵	۳/۷۵	۱۰	۱	۱۰	۵	۰/۷۵	۳/۷۵	۱۵	۱	۱۵	۱۵	۱	۱۵	۱۰	۱	۱۰	۸۵	زیاد	
۴	سازمان برنامه و بودجه	سیستم خودکار داده‌های گمرکی جهانی (ASYCUDA)*	۱۵	۱	۱۵	۵	۱	۵	۱۰	۱	۱۰	۱۰	۱	۱۰	۵	۰/۲۵	۱/۲۵	۱۰	۱	۱۰	۵	۰/۲۵	۱/۲۵	۱۵	۰/۵	۷/۵	۱۵	۱	۱۵	۱۰	۰/۷۵	۷/۵	۸۲/۵	زیاد	
۵	اداره اتباع خارجی	مهاجرت الکترونیکی	۱۵	۱	۱۵	۵	۱	۵	۱۰	۱	۱۰	۱۰	۱	۱۰	۵	۰/۲۵	۱/۲۵	۱۰	۱	۱۰	۵	۰/۷۵	۳/۷۵	۱۵	۰/۵	۷/۵	۱۵	۰/۳	۳/۷۵	۱۰	۰/۵	۵	۷۱/۲۵	متوسط	
۶																																				۰		

* سیستم خودکار کنفرانس تجارت و توسعه سازمان ملل متحد برای داده‌های گمرکی (ASYCUDA) یک سیستم مدیریت گمرکی یکپارچه برای تجارت بین‌المللی و عملیات حمل‌ونقل در یک محیط خودکار مدرن است.

ریسک بالا ۷۵ تا ۱۰۰

ریسک متوسط ۵۰ تا ۷۵

ریسک پایین کمتر از ۵۰


فعالیت‌های پیش‌از بستن قرارداد
تشکیل گروه، ارزیابی توان تخصصی و بودجه زمانی:
❖ ارزیابی و نتیجه گیری در مورد رعایت الزامات اخلاقی مربوط
❖ کسب شناخت از شرایط قرارداد، ازجمله انتظارات از سایر حسابرسان
• تشکیل گروه
• بیانیه منشور اخلاقی
• نتیجه‌گیری منشور اخلاقی
• مستندات نشست پشتیبان حسابرسی فناوری اطلاعات
• توافق گروه
• قرارداد حسابرسی
• پرسشنامه کنترل کیفیت
شناخت سازمان
❖ کسب شناخت کلی از سازمان مطابق UEI شناخت سازمان
❖ شناخت خاص IT سازمان مطابق ....
❖ به‌روز رسانی فهرست ریسک
شناخت سازمان
• UEI- شناخت سازمان
• شناخت سازمان
برآورد ریسک
برآورد ریسک:
❖ تهیه شرح شناخت سیستم
❖ به‌روز رسانی فهرست ریسک
❖ انجام برآورد ریسک
❖ برخورد با ریسک
• فهرست ریسک
• شرح سیستم و آزمون شناخت سیستم
• برآورد ریسک و برخورد با ریسک
• گفتگو با گروه حسابرسی
• طرح کلی حسابرسی
• پرسشنامه کنترل کیفیت
اجرای حسابرسی
اجرای حسابرسی
❖ اجرا و مستندسازی روش های حسابرسی و
❖ گرد آوری شواهد حسابرسی مربوط
• برنامه حسابرسی آزمون کنترل‌ها
• برنامه حسابرسی آزمون‌های محتوای جزئیات
• رعایت آیین رفتار حرفه‌ای
• پرسشنامه کنترل کیفیت
گزارشگری
گزارشگری
❖ ارزیابی ناکارآمدی طراحی و / یا عملکرد روش‌های کنترلی
❖ در نظر گرفتن موضوع‌های کلیدی حسابرسی
❖ تعیین اظهار نظر گزارش در مورد سیستم اطلاعاتی
• بازخورد پشتیبانی حسابرسی فناوری اطلاعات
• نامه مدیریت
• گزارش حسابرس
• ارائه توسط مدیریت حسابرسی
• نکات قابل توجه در حسابرسی سال آینده
• پرسشنامه کنترل کیفیت

پیوست ۲:
پیش از شروع قرارداد

پیش از شروع قرارداد ۱
تشکیل گروه حسابرسی– صلاحیت و بودجه زمانی

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه:		سطح ۳			
تاریخ:					

صلاحیت کارکنان					
جنبه‌های خاص صلاحیت	رهبر گروه	حسابرس ۱	حسابرس ۲	حسابرس ۳	حسابرس ۴
تعداد سال‌های تجربه					
نگرش حسابرسی و کاربرگ‌های دیوان محاسبات					
حضور در حسابرسی سال پیش سازمان مورد رسیدگی					
شناخت از سیستم‌ها و فرآیندهای سازمان مورد رسیدگی					
شناخت از سیستم‌های IT حسابرسی شده و محیط کامپیوتری					

بودجه زمانی اولیه (نفر روز / نفر ساعت)

فعالیت‌ها	بودجه	حسابرس ۱	حسابرس ۲	حسابرس ۳	حسابرس ۴
پیش از شروع قرارداد					
برآورد ریسک					
برخورد با ریسک					
اجرای حسابرسی- اجزاء اجرای حسابرسی- کلی					
گزارشگری					
جمع					

نتیجه‌گیری:

گروه حسابرسی درمجموع، دارای توانایی مناسب، صلاحیت و زمان برای اجرای حسابرسی را دارند. هرگونه آموزش لازم، شناسایی شده است و پیش از شروع کار انجام خواهد شد.

امضای فرد مسئول گزارش	تاریخ

پیش از شروع قرارداد ۲ – بیانیه آیین رفتار حرفه‌ای

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه:		سطح ۳			
تاریخ:					

(این بیانیه باید توسط همه اعضای گروه حسابرسی، تکمیل شود)

بیانیه آیین رفتار حرفه‌ای

سازمان مورد رسیدگی: (نام سازمان مورد رسیدگی را بنویسید)

سال مالی مورد رسیدگی: (تاریخ پایان سال مالی مورد رسیدگی را بنویسید)

برای هدف‌های حسابرسی ..... **(نام سازمان مورد رسیدگی را بنویسید)** ..... ، تأیید می‌کنم که:

۱. به‌طور کامل از الزامات آیین رفتار حرفه‌ای INTOSAI که در این حسابرسی لازم‌الاجرا است، شناخت دارم.

۲. من یا هیچ‌یک از بستگان نزدیک من، منافع مالی[۱] در **(نام سازمان مورد رسیدگی را بنویسید)** نداریم.

۳. من هیچ ارتباط تجاری با سازمان مورد رسیدگی یا هیچ‌یک از مدیران، اداره‌کنندگان و کارکنان آن ندارم.

۴. من در گذشته هیچ‌گونه مزایا یا هدیه‌ای از افراد شاغل یا مرتبط با حسابرسی شونده دریافت نکرده‌ام.

۵. من در دو سال مالی گذشته، اداره‌کننده، کارمند یا مدیر سازمان مورد رسیدگی نبوده و نیستم.

۶. من یا هیچ‌یک از بستگان نزدیک من[۲]، در حال حاضر یا در طول سال مالی مورد رسیدگی، نقش گزارشگری مالی و نظارتی[۳] در سازمان مورد رسیدگی نداشته‌ایم.

---

۱. شامل مالکیت سهام، وام یا ضمانت‌نامه به یا از سازمان، مدیران یا اداره‌کنندگان آن.

۲. شامل بستگان اعضای گروه حسابرسی، والدین، والدین ناتنی، فرزندان، فرزندان ناتنی و خواهر و برادر.

۳. نقش نظارتی گزارشگری مالی به افرادی گفته می‌شود که بر سوابق حسابداری یا صورت‌های مالی اعمال‌نفوذ می‌کنند؛ که شامل یکی از اعضای هیأت مدیره یا سایر ارکان راهبری مشابه، مدیر اجرایی، رئیس، مدیر ارشد مالی/ عملیاتی/ حسابداری، کنترل‌کننده، مدیر حسابرسی داخلی، مدیر گزارش‌های مالی، خزانه‌دار، یا هر سمت معادلی می‌شود.

۷. من هیچ رابطه دیگری با هیچ‌یک از مدیران و کارکنان سازمان مورد حسابرسی ندارم که ممکن است به استقلال من خدشه وارد کند.

۸. نگرش مدیریت و/ یا کارکنان سازمان مورد رسیدگی از طریق ارعاب، استقلال من را مختل نکرده است.

۹. من نسبت به الزامات آیین رفتار حرفه‌ای INTOSAI شناخت دارم، شامل اینکه:

۹-۱. باید دقت لازم را داشته باشم و حسابرسی را به شیوه‌ای حرفه‌ای و در حد توانم انجام دهم.

۹-۲. من باید حسابرسی را با صداقت، درستکاری، واقع‌بینی و بی‌طرفی سیاسی انجام دهم.

۹-۳. محرمانگی اطلاعات به‌دست آمده در طول فرآیند حسابرسی و اینکه نباید چنین اطلاعاتی را در اختیار اشخاص ثالث قرار دهم.

شرایطی که ممکن است بر رعایت گزاره‌های بالا، تأثیر بگذارد عبارتند از:

(در صورت وجود، شرایط را فهرست کنید).

بیانیه

من، امضاءکننده این بیانیه، الزامات و مسئولیت‌های نوشته شده در منشور اخلاقی را کاملاً درک می‌کنم. شرایطی را که ممکن است به انطباق من با آنها آسیب وارد کند، در صورت وجود، افشا کرده‌ام. افزون بر این، درصورتی‌که ضمن حسابرسی شرایطی ایجاد شود که موجب اختلال در انطباق اینجانب با هر یک از مفاد بالا شود، متعهد می‌شوم که آنها را بی‌درنگ اعلام کنم.

نام عضو گروه	رتبه	امضای عضو گروه

پیش از شروع قرارداد ۳ – نتیجه‌گیری در مورد رعایت الزامات اخلاقی

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه:		سطح ۳			
تاریخ:					

سازمان مورد رسیدگی:

دوره مورد رسیدگی:

(این نتیجه‌گیری باید توسط شخص مسئول حسابرسی در بخش بیانیه آیین رفتار حرفه‌ای آورده شود. این کاربرگ، بخشی از بیانیه سایر اعضای گروه حسابرسی نیست).

نام اعضای گروه حسابرسی	تهدیدهای شناسایی شده توسط اعضای گروه	اقدامات لازم برای برخورد با تهدیدها
	(تهدیدهای شناسایی شده هر بیانیه آیین رفتار حرفه‌ای را فهرست کنید)	

پس از بررسی بیانیه‌های بالا توسط گروه حسابرسی و مصاحبه با اعضای گروه، به این نتیجه رسیدم که همه الزامات مندرج در بیانیه رفتار حرفه‌ای INTOSAI برای قرارداد حسابرسی، به‌درستی در نظر گرفته شده و رعایت شده است. هرگونه تهدید برای استقلال گروه حسابرسی حذف شده یا به سطحی پذیرفتنی کاهش یافته است.

امضای شخص مسئول گزارش	تاریخ

قرارداد حسابرسی

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه:		سطح ۳			
تاریخ:					

(روی سربرگ دیوان محاسبات)

حسابرسی [نام سازمان مورد حسابرسی را بنویسید] **انجام شده توسط دیوان محاسبات**

مخاطب [عنوان مسئول حسابداری]

تاریخ

خانم/آقای محترم

حسابرسی فناوری اطلاعات [نام سازمان یا وزارتخانه] برای سال مالی...

این قرارداد شناخت ما را از شرایط و هدف‌های کار و ماهیت و دامنه خدمات حسابرسی مستقلی که ارائه خواهد شد، بیان می‌کند. موضوع قرارداد مطابق با الزامات استانداردهای بین‌المللی دیوان‌های محاسبات (ISSAIs) و همچنین، استانداردهای انجمن حسابرسان سیستم‌های اطلاعاتی (ISACA) است. این قرارداد برای محدود کردن مسئولیت‌های حرفه‌ای من به سطحی پایین‌تر از استانداردهای مورد انتظار حرفه‌ای نیست.

هدف این قرارداد تعیین موارد زیر است:

- شرایط قرارداد حسابرسی، ماهیت و محدودیت‌های حسابرسی سالانه.
- مسئولیت‌های مربوط به حسابرس و مدیریت [نام سازمان مورد رسیدگی] در حسابرسی سالانه.
- شرایط قرارداد حسابرسی به شرح زیر تنظیم شده است. این قرارداد تا زمانی معتبر خواهد بود که قرارداد حسابرسی جدیدی صادر نشود.

هدف(های) حسابرسی

هدف‌های حسابرسی سالانه به شرح زیر است:

- بررسی کنترل‌های سیستم‌های فناوری اطلاعات برای اطمینان یافتن از کفایت و اثربخشی آنها.
- ارزیابی سیستم‌ها و فرآیندهای موجود که منابع اطلاعاتی را محافظت می‌کنند و در دسترس قرار می‌دهند.
- ارزیابی عملکرد سیستم‌های اطلاعاتی و امنیت آنها.
- آزمون فرآیند توسعه سیستم و رویه‌ها.
- تعیین مطابقت فرآیندهای مدیریت اطلاعات با قوانین، سیاست‌ها و استانداردهای مربوط.

مسئولیت‌های حسابرس

- من ملزم به بررسی اثربخشی و کارایی کنترل‌های عمومی و کاربردی هستم که بر اساس [قوانین مرتبط، هدف‌های کنترلی پذیرفته‌شده بین‌المللی در مورد اطلاعات و فناوری‌های مرتبط و بهترین نحوه عمل‌های صنعت - در صورت لزوم اصلاح شود] سنجیده می‌شوند.
- حسابرسی (من) براساس استانداردهای بین‌المللی دیوان‌های محاسبات (ISSAIs) و همچنین، استانداردهای انجمن حسابرسان سیستم‌های اطلاعاتی (ISACA) و بهترین نحوه عمل‌های صنعت انجام خواهد شد. حسابرسی برای کسب اطمینان معقول از قابلیت اتکای سیستم‌های اطلاعاتی، برنامه‌ریزی و اجرا خواهد شد. مسئولیت من تعیین محرمانگی، یکپارچگی و در دسترس بودن منابع سیستم اطلاعاتی خواهد بود.

حسابرسی من بر زمینه‌های زیر تمرکز خواهد داشت: [زمینه‌هایی که حسابرسی خواهند شد را فهرست کنید]

- راهبری فناوری اطلاعات
- مدیریت امنیت
- مدیریت تغییر برنامه
- کنترل‌های حفاظت فیزیکی
- کنترل‌های زیست‌محیطی
- تداوم خدمات فناوری اطلاعات
- کنترل‌های دسترسی منطقی

دامنه حسابرسی‌های بالا با واحد حسابرسی داخلی...[نام سازمان مورد حسابرسی] نیز هماهنگ خواهد شد تا از دوباره‌کاری حسابرسی پیشگیری شود. روش‌های حسابرسی که به‌صورت نمونه‌ای انجام خواهد شد، شامل آزمون‌هایی خواهد بود که ضروری تلقی می‌شوند و از طریق گفتگو با کارکنان کلیدی، مشاهده

عملکردها و وظایف خاص، آزمون مستندسازی و آزمون سیستم، در موارد لازم، انجام می‌شود. [هر روش دیگری را که لازم می‌دانید اضافه کنید].

حسابرسی همچنین، شامل رسیدگی نمونه‌ای به شواهد پشتیبان رعایت همه جنبه‌های بااهمیت قوانین و مقررات مربوط به سیستم‌های اطلاعاتی می‌باشد که مورد توجه اینجانب قرار گرفته است.

مسئولیت‌های مدیریت

مدیریت، مسئول برقراری کنترل‌های لازم برای اطمینان از یکپارچگی، قابلیت اطمینان و در دسترس بودن سیستم‌های اطلاعاتی است.

حسابرسی من بر اساس مسئولیت‌های مدیریت، به شرح زیر، انجام خواهد شد:

- ایجاد و حفظ کنترل‌های داخلی لازم برای اطمینان از کارایی و اثربخشی سیستم‌های اطلاعاتی؛
- ارائه موارد زیر به من:
  - همه اطلاعات مربوط به سیستم‌های اطلاعاتی مانند سوابق، اسناد و سایر موارد.
  - هرگونه اطلاعات اضافی دیگری که ممکن است برای حسابرسی از مدیریت درخواست کنم، و
  - دسترسی نامحدود به اشخاصی در درون سازمان که لازم می‌دانم شواهد حسابرسی از آنها به‌دست آید.

به‌عنوان بخشی از فرآیند حسابرسی خود، از مدیریت و در صورت لزوم، ارکان راهبری، درخواست تأییدیه کتبی در مورد اظهاراتی خواهم داشت که در ارتباط با حسابرسی به من ارائه شده است.

گزارشگری

پس از پایان کار، یافته‌های خود را با ارکان راهبری سازمان در میان خواهم گذاشت.

شواهد حسابرسی پشتیبان یافته‌های حسابرسی و نتیجه‌گیری‌ها در همین راستا گردآوری می‌شود و نامه مدیریت به‌صورت زیر ساختار می‌یابد: [متناسب با هر دیوان محاسبات]

- **یافته‌ها:** ضعف شناسایی شده در جریان حسابرسی جاری، با پشتوانه مثال‌های کمی مناسب، در حد ممکن.
- **ریسک/ پیامد:** ریسک‌ها یا پیامدهای مربوط به یافته‌های حسابرسی.
- **پیشنهاد:** زمینه(های) ممکن برای بهبود.
- **پاسخ مدیریت:** نظرهای مدیریت درباره یافته‌های حسابرسی.
- **ارزیابی پاسخ مدیریت:** ارزیابی من از نظرهای مدیریت در مورد یافته‌های حسابرسی.

فرآیند حسابرسی مشمول فرآیند بررسی کیفی درون‌سازمانی دفتر من در انطباق با استانداردهای حرفه‌ای خواهد بود.

تاریخ هدف برنامه‌ریزی شده برای تکمیل این حسابرسی، ... (شروع و پایان) ... است.

تأییدیه مدیران

به‌عنوان بخشی از رویه‌های معمول حسابرسی خود، از مدیریت درخواست خواهم کرد تا درباره اظهارات شفاهی مدیریت در طول اجرای حسابرسی، تأییدیه کتبی نیز ارائه کند.

حق‌الزحمه [تنها در صورتی قابل‌اعمال است که حق‌الزحمه حسابرسی یا کمک هزینه‌ای از سازمان مورد رسیدگی قابل دریافت باشد– در غیر این صورت، حذف شود]

حق‌الزحمه من بر اساس مدت زمانی تعیین می‌شود که مدیران و کارکنانم در هر سطح مهارتی و مسئولیت‌های مربوط برای امور شما صرف می‌کنند. حق‌الزحمه در فواصل زمانی ماهانه در طول اجرای حسابرسی صورتحساب می‌شود و تسویه‌حساب ظرف ۳۰ روز از تاریخ صورتحساب انجام می‌شود. {تنها در صورت بازیابی حق‌الزحمه حسابرسی قابل‌اعمال است}.

سایر شرایط

این قرارداد تا زمانی که جایگزین نشود به قوت خود باقی خواهد ماند. لطفاً موافقت خود را با شرایط این قرارداد با امضا کردن و بازگرداندن نسخه پیوست، تأیید کنید، یا اگر این شرایط قرارداد برای شما ابهامی دارد، به ما اطلاع دهید.

ما مشتاقانه خواهان همکاری کامل کارکنان شما در طول حسابرسی هستیم.

با احترام

مدیر کل حسابرسی

نام و نام خانوادگی

تلفن:

ایمیل:

تأیید مفاد قرارداد حسابرسی		
مفاد این قرارداد حسابرسی توسط ..... [سِمت امضاکننده] ..... از سوی ..... [نام سازمان] ..... مورد تأیید و توافق است.		
نام و سمت	**امضا**	**تاریخ**

صورتجلسه نشست پشتیبان حسابرسی فناوری اطلاعات

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه:		سطح ۳			
تاریخ:					

تاریخ نشست: [تاریخ نوشته شود]

فهرست اعضای گروه مشارکت‌کننده در نشست:

نام	رتبه

یافته‌های حسابرسی سال پیش (یافته‌های سال پیش و آن دسته از ضعف‌های فناوری اطلاعات را فهرست کنید که سبب ایجاد این یافته‌ها شده است)		انتقال به کاربرگ فهرست ریسک
یافته‌های سال پیش(ریسک)	کدام ضعف‌های فناوری اطلاعات ممکن است سبب ایجاد این یافته‌ها شده باشد	

درخواست‌های ویژه حسابرسی فناوری اطلاعات (فهرست موارد قابل بررسی که توسط حسابرسان مالی یا سایر حسابرسان در طول قرارداد حسابرسی به‌صورت ویژه درخواست شده‌اند)		
محور بحث	راهکارها/ یادداشت‌ها	انتقال به کاربرگ فهرست ریسک

هدف‌های حسابرسی (هدف‌های حسابرسی مالی و چگونگی پشتیبانی حسابرسی فناوری اطلاعات از آن را بنویسید)	
هدف‌های حسابرسی مالی(یا سایر حسابرسی‌ها)	پشتیبانی حسابرسی فناوری اطلاعات از هدف‌های حسابرسی

محور بحث	راهکارها / یادداشت‌ها
سایر ملاحظات	
نکات قابل توجه حاصل از گفتگوی اعضای گروه.	
نکات حاصل از برنامه‌ریزی حسابرسی مالی و شناخت سازمان.	
ملاحظات تقلب تهیه شده توسط سایر حسابرسان که به فناوری اطلاعات مربوط است.	
سایر موارد مطرح شده و تصمیم‌های گرفته شده را بنویسید.	

امضا:

نام و امضای مدیر گروه حسابرسی فناوری اطلاعات	تاریخ

نام و امضای مدیر گروه حسابرسی مالی	تاریخ

(لطفاً توجه داشته باشید که صورتجلسه گفتگو با حسابرسان مالی باید بایگانی شود.)

پیوست ۳:
شناخت سازمان

راهنمای چک‌لیست کنترل فناوری اطلاعات

چک‌لیست کنترل فناوری اطلاعات جنبه‌های زیر را در برمی‌گیرد:

راهبری فناوری اطلاعات

وجود کمیته راهبری فناوری اطلاعات، یک جز اصلی راهبری فناوری اطلاعات است؛ زیرا، همسویی راهبردی لازم را برای دستیابی به هدف‌های سازمان ایجاد می‌کند. مدیریت ارشد معمولاً این کمیته را برای نظارت بر عملکرد و فعالیت‌های سیستم‌های اطلاعاتی تشکیل می‌دهد. این کمیته، تضمین‌کننده هماهنگی بخش فناوری اطلاعات با مأموریت و هدف‌های شرکت است.

برخی از نقش‌های اصلی و مسئولیت‌های قابل اجرا توسط این کمیته به شرح زیر است:

- اطمینان از همسویی راهبری فناوری اطلاعات با راهبری سازمان؛
- افزایش درک و رضایت از ارزش سرمایه‌گذاری فناوری اطلاعات؛
- ترویج ارتباط دو طرفه بین کسب و کار و فناوری اطلاعات؛
- بررسی و تصویب خریدهای عمده؛
- بررسی و تصویب پروژه‌های بزرگ فناوری اطلاعات؛
- بررسی و تصویب طرح‌های برون‌سپاری فعالیت‌های فناوری اطلاعات؛
- بررسی کفایت و تخصیص منابع؛
- تصمیم‌گیری در مورد تمرکز و تمرکز زدایی؛
- پشتیبانی از توسعه و اجرای برنامه مدیریت امنیت اطلاعات در سطح سازمان؛ و
- گزارش فعالیت‌های فناوری اطلاعات به هیأت مدیره.

برنامه راهبردی فناوری اطلاعات

هنگامی که کمیته راهبری فناوری اطلاعات، در مورد سمت‌وسوی آینده فناوری اطلاعات توافق کرد، تصمیم‌ها باید رسمیت یابند و در یک برنامه مستند شوند. سند راهبردی فناوری اطلاعات در واقع نقطه شروع هر سرمایه‌گذاری در فناوری اطلاعات است، زیرا آن دسته از تغییرات آتی را مشخص می‌کند که باید برای آنها بودجه‌بندی شود. تصمیم‌ها و تغییرات پیش‌بینی شده در راهبرد فناوری اطلاعات، احتمالاً تأثیر حداقلی بر حسابرسی فعلی خواهد داشت، اما، ممکن است تأثیر قابل توجهی بر حسابرسی‌های آینده داشته باشد.

بررسی راهبرد فناوری اطلاعات سازمان مورد رسیدگی می‌تواند حسابرس را از مشکلاتی آگاه سازد که ممکن است در سال‌های آینده به وجود بیاید. برای مثال، راهبرد فناوری اطلاعات ممکن است بیانگر این باشد که سازمان طی دو سال آینده، سیستم مالی خود را جایگزین خواهد کرد. این ممکن است بر کار حسابرس تأثیر بگذارد.

اندازه، جزئیات و محتوای راهبرد فناوری اطلاعات با توجه به عوامل گوناگونی چون اندازه سازمان و واحد فناوری اطلاعات آن و اهمیت یا ضرورت سیستم‌های فناوری اطلاعات، متفاوت خواهد بود. برای مثال، یک وزارتخانه بزرگ دولتی احتمالاً راهبردهای دقیق فناوری اطلاعات دارد که بیش از صدها صفحه را شامل می‌شود، از سوی دیگر، راهبرد فناوری اطلاعات یک وزارتخانه کوچک ممکن است از یک سند یک‌برگی تشکیل شده باشد. حسابرس هنگام بررسی راهبرد باید آنچه را که برای سازمان مناسب است در نظر بگیرد. هدف اصلی برای یک برنامه راهبردی فناوری اطلاعات، نه‌تنها حداکثر سازی مزایای فناوری اطلاعات و اجرای برنامه‌ریزی برای یک دوره سه‌ساله است، بلکه اطمینان از همسویی فناوری اطلاعات با کسب وکار سازمان است.

مدیریت امنیت

نرم‌افزارهای غیرمجاز یا مخرب ممکن است ریسک‌های امنیتی خاصی برای شبکه سازمان مورد رسیدگی داشته باشند. در بسیاری از موارد (طبق بهترین نحوه عمل‌ها) سازمان‌های مورد حسابرسی، سیاستی دارند که کارکنان را از داشتن نرم‌افزار غیرمجاز بر روی رایانه‌های خود منع می‌کند.

نمونه اقداماتی که می‌تواند توسط مدیریت برای پیشگیری از نصب نرم‌افزارهای غیرمجاز اجرا شود به شرح زیر است:

- غیرفعال کردن دیسک‌گردان (سی دی-رام)[1] در رایانه؛
- محدودیت در اندازه فایل قابل ارسال از طریق شبکه سازمان مورد رسیدگی؛
- محدودیت در اندازه فایل قابل دانلود از اینترنت؛
- امکان مسدود کردن وب‌سایت‌ها؛ و
- بررسی‌های دوره‌ای حافظه اصلی[2] رایانه برای شناسایی نرم‌افزارهای غیرمجاز.

برای برخورد با کارمندی که مشخص می‌شود نرم‌افزار غیرمجاز در رایانه خود دارد، باید اقدامات انضباطی مصوبی وجود داشته باشد.

1. CD-ROM
2. Hard drives

تعریف نقش‌ها و مسئولیت‌ها

منابع انسانی فناوری اطلاعات معمولاً بخشی از مدیریت منابع انسانی سازمان را تشکیل می‌دهد. موارد زیر باید در نظر گرفته شود:

۱. مرخصی اجباری؛
۲. چرخش کارکنان؛
۳. رویه‌هایی برای عملکردهای ضروری که نیازمند مستندسازی و نظارت مناسب هستند.
۴. شرح شغل؛
۵. قراردادهای عملکرد؛ و
۶. تفکیک وظایف.

حسابرس هنگام بررسی فرآیند باید وجود یا نبود تفکیک وظایف کافی را تعیین کند. سازمان‌های کوچک ممکن است عملکردهای فناوری اطلاعات ترکیبی داشته باشند، بااین حال، عملکردهای زیر را نمی‌توان ترکیب کرد:

- برنامه‌نویس و مدیر پایگاه داده؛
- مدیر سیستم و مدیر پایگاه داده؛
- مدیر امنیت و مدیر پایگاه داده؛ و
- مدیر شبکه و مدیر پایگاه داده.

مدیریت تغییر برنامه

کنترل های تغییر بخشی از فرآیند مدیریت تغییر هستند و بر کارهایی تمرکز می‌کند که یک کارمند باید هنگام درخواست تغییرات سیستم انجام دهد. یک خط مشی رسمی مستند برای فرآیندی که باید اجرا شود و فرم(های) استاندارد شده‌ای که هنگام درخواست این تغییرات توسط کارمند درخواست‌کننده تغییر تکمیل شود، باید وجود داشته باشد.

کنترل‌های دسترسی فیزیکی

کنترل‌های دسترسی فیزیکی برای محافظت از سازمان در برابر دسترسی‌های غیرمجاز طراحی شده‌اند که نه‌تنها شامل دسترسی به اتاق رایانه بلکه دسترسی به ساختمان نیز می‌باشد.

حسابرس می‌تواند از ساختمان سازمان بازدید کند تا شناخت و درکی کلی از تأسیسات مورد بررسی به‌دست آورد. بیشتر رویه‌هایی که حسابرس انجام خواهد داد می‌تواند بر اساس همین مشاهده امکانات سازمان انجام شود. همچنین، در آزمون دسترسی فیزیکی، دسترسی به رایانه‌های شخصی یا لپ‌تاپ‌ها نیز گنجانده شده است. حسابرس باید به کنترل‌هایی توجه کند که برای اطمینان از حفاظت مناسب از این موارد اعمال می‌شود. ایمن‌سازی لپ‌تاپ‌ها و رایانه‌های شخصی تنها به کنترل‌های دسترسی فیزیکی محدود نمی‌شود، بلکه کنترل‌های دسترسی منطقی را نیز شامل می‌شود. نمونه‌هایی از کنترل‌هایی که یک سازمان می‌تواند برای کاهش ریسک افشای داده‌های حساس ذخیره شده در لپ‌تاپ اجرا کند، به شرح زیر است:

- حک کردن نام تجاری یا شماره‌سریال و نام شرکت روی لپ‌تاپ با استفاده از برچسب‌های مقاوم در برابر دستکاری؛
- استفاده از سیستم قفل کابلی برای قفل‌کردن لپ‌تاپ‌ها روی میز؛
- پشتیبان‌گیری از داده‌های حساس به‌طور منظم؛
- رمزگذاری داده‌ها با استفاده از نرم‌افزار رمزگذاری معتبر؛
- اختصاص گذرواژه به هر فایل جداگانه برای پیشگیری از دسترسی دیگران به فایل؛ و
- فعال کردن سیستم قفل خودکار در لپ‌تاپ‌ها درصورتی‌که چند دقیقه از آن استفاده نشود.

کنترل‌های محیطی

قرار گرفتن در معرض ریسک‌های محیطی در درجه اول به رویدادهای طبیعی مانند زلزله و طوفان مربوط می‌شود. نتیجه این اتفاقات طبیعی می‌تواند به انواع مشکلات گوناگون مانند نوسانات برق منجر شود که تأثیر منفی بر زیرساخت اطلاعاتی دارد.

کنترل‌های گوناگونی برای کاهش خطرات ناشی از قرار گرفتن در معرض ریسک‌های محیطی، به‌شرح زیر وجود دارد که یک سازمان می‌تواند اعمال کند:

- ردیاب/ سنسور آب[1]؛
- کپسول‌های آتش‌نشانی دستی؛
- اعلام حریق دستی؛

1. Water Detector ردیاب آب، یک دستگاه الکترونیکی است که برای تشخیص وجود آب برای هدف‌هایی مانند اعلام هشدار به‌موقع برای پیشگیری از نشت آب طراحی شده است.

- ردیاب/ سنسور دود؛
- سیستم‌های آتش‌نشانی؛
- بازرسی‌های منظم توسط اداره آتش‌نشانی؛
- دیوارها، کف‌ها و سقف‌های نسوز در اطراف اتاق رایانه؛
- محافظ‌های الکتریکی؛
- دستگاه‌های برق اضطراری / ژنراتورها؛ و
- کلید قطع کن اضطراری برق.

تداوم خدمات فناوری اطلاعات

هنگامی‌که یک فاجعه رخ می‌دهد، سازمان باید برنامه‌ای برای کمک و راهنمایی کارکنان در بازیابی زود و به‌موقع داده‌های عملکردهای کلیدی داشته باشد.

هنگام تدوین طرح تداوم کسب‌وکار و طرح بازیابی فاجعه، مراحل گوناگونی وجود دارد که یک سازمان باید طی کند. فرآیند برنامه‌ریزی تداوم کسب‌وکار را می‌توان به مراحل زیر تقسیم کرد:

تجزیه‌وتحلیل اثر بر کسب‌وکار

این فرآیند شامل شناسایی رویدادهای گوناگونی است که می‌تواند بر تداوم خدمات چه ازنظر مالی، منابع انسانی یا شهرت تأثیر بگذارد. افراد درگیر در این مرحله باید شناخت کاملی از کسب‌وکار، فرآیندهای کلیدی کسب‌وکار و منابع فناوری اطلاعات مورد استفاده سازمان برای پشتیبانی از فرآیندهای کلیدی کسب‌وکار داشته باشند. افراد درگیر در این فرآیند عمدتاً نمایندگان مدیریت ارشد و مدیریت فناوری اطلاعات خواهند بود.

فرآیندی برای طبقه‌بندی اهمیت منابع اطلاعاتی مانند شبکه‌ها، زیرساخت فناوری اطلاعات، برنامه‌های کاربردی، داده‌ها و غیره باید توسط مدیریت ایجاد و تأیید شود. هنگام رخداد یک فاجعه باید جنبه‌های گوناگونی ازجمله فرآیند بازیابی، در نظر گرفته شود. سیستم‌ها را می‌توان بر اساس اهمیت آنها برای سازمان به چهار گروه زیر تقسیم کرد:

- **سیستم‌های حیاتی(بحرانی)**[1] - عملکرد این سیستم‌ها را نمی‌توان انجام داد مگر اینکه سیستمی با همان قابلیت‌ها جایگزین شود. برنامه‌های کاربردی مهم را نمی‌توان با روش‌های دستی جایگزین کرد. تحمل وقفه، بسیار کم است و هزینه بازیابی بسیار بالا خواهد بود.

1. Critical

- **سیستم‌های مهم** - عملکرد این سیستم‌ها را می‌توان برای مدت کوتاهی به‌صورت دستی انجام داد و تحمل وقفه بالاتری نسبت به سیستم‌های حیاتی دارند. هزینه بازیابی به شرطی کمتر است که این عملکردها در یک بازه زمانی معین بازیابی شوند.
- **سیستم‌های حساس**- عملکرد این سیستم‌ها را می‌توان به‌صورت دستی با هزینه قابل تحمل و برای مدت زمان طولانی‌تر انجام داد. و
- **سیستم‌های کم‌اهمیت (غیر بحرانی)** - عملکرد این سیستم‌ها را می‌توان به‌صورت دستی برای مدت زمان طولانی و با هزینه اندک یا بدون هزینه برای سازمان انجام داد و در صورت بازیابی، به حداقل به‌روزرسانی نیاز دارد.

تدوین راهبردهای بازیابی کسب‌وکار

پس از شناسایی رخدادهای گوناگونی که می‌توانند بر سازمان تأثیر بگذارند، شناسایی راهبردهای بازیابی ممکن برای آن رخدادها و انتخاب مناسب‌ترین راهبرد برای بازیابی فاجعه، مرحله بعدی است.

انتخاب یک راهبرد بازیابی، به اهمیت فرآیندهای تجاری، هزینه و زمان بازیابی فرآیندهای تجاری و امنیتی بستگی دارد. مناسب ترین راهبردی که یک سازمان می‌تواند انتخاب کند این است که هزینه زمان بازیابی در مقایسه با احتمال رخداد تعیین شده در تجزیه‌وتحلیل اثر بر کسب‌وکار، معقول باشد.

سازمان باید هنگام تدوین راهبردهای بازیابی، راهبردهای جایگزینی موجود را در نظر بگیرد. هنگامی‌که فاجعه‌ای سایت اصلی را مختل می‌کند، سازمان باید به امکانات خارج از سایت دسترسی داشته باشد که می‌تواند به‌عنوان جایگزین‌های پشتیبان استفاده شوند. این‌گونه امکانات شامل موارد زیر است:

امکانات پردازش تکراری (Duplicate processing facilities)- این امکانات سایت‌های بازیابی اختصاصی و توسعه‌یافته‌ای هستند که می‌توانند از برنامه‌های کاربردی مهم نسخه پشتیبان تهیه کنند. این سایت‌ها از نظر شکل می‌توانند از یک سایت آماده بکارگیری تا یک توافق متقابل، متغیر باشند. یکی از مزایای استفاده از چنین امکاناتی این است که در صورت بروز فاجعه، مشکلات کمتری در هماهنگی برای سازگاری و در دسترس بودن وجود دارد. هنگام انتخاب این روش، اصول خاصی به شرح زیر، وجود دارد که باید در نظر داشت:

- سایت انتخاب شده نباید در معرض بلایای طبیعی مشابه سایت اصلی قرار داشته باشد؛
- بین راهبردهای سخت‌افزاری و نرم‌افزاری باید هماهنگی وجود داشته باشد؛
- از در دسترس بودن منابع باید اطمینان حاصل شود؛

- در مورد اولویت افزودن برنامه‌ها باید توافق وجود داشته باشد؛ و
- آزمون منظم لازم است.

سایت‌های آماده (Hot sites)- که به‌طور کامل پیکربندی شده‌اند و در مدت زمان کوتاهی آماده فعالیت هستند. سخت‌افزار و نرم‌افزار آن کاملاً با سازمان سازگار است. سازمان هنگام استفاده از این امکانات، تنها به این نیاز دارد که کارکنان وارد محل شوند و وظایف خود را ادامه دهند. هزینه‌های این سایت‌ها معمولاً زیاد است، اما اگر به‌درستی برنامه‌ریزی شود، می‌تواند با بیمه مناسب، جبران شود. این امکانات تنها برای مدت‌زمان محدودی استفاده می‌شوند؛

سایت‌های نیمه آماده (Warm sites)- این سایت‌ها تا حدی با اتصالات شبکه و تجهیزات جانبی خاصی پیکربندی شده‌اند. سایت‌های نیمه آماده هزینه کمتری نسبت به سایت‌های آماده دارند و می‌توانند در عرض چند ساعت آماده‌به‌کار شوند؛

سایت‌های سرد (Cold sites)- این سایت‌ها تنها محیط زیربنایی را فراهم می‌کنند و سایر تجهیزات باید همگی توسط سازمان آورده شوند. فعال‌سازی سایت ممکن است بیشتر طول بکشد زیرا تمام تجهیزات مورد نیاز باید خریداری و نصب شوند؛ و

توافق متقابل (Reciprocal agreements) با شعب سازمان یا سایر سازمان‌ها - این توافق‌ها بین شعبه‌های داخل سازمان یا سایر سازمان‌ها با زیرساخت‌ها یا برنامه‌های مشابه می‌باشد. این سازمان‌ها تعهد می‌دهند که در صورت رخداد شرایط اضطراری، زمان رایانه را در اختیار یکدیگر قرار دهند.

تهیه یک طرح تفصیلی

طرح تفصیلی باید به همه مسائل مربوط به بازیابی یک فاجعه بپردازد. عواملی که در تدوین طرح باید در نظر گرفته شود به شرح زیر است:

- آمادگی پیش از فاجعه؛
- طرح تخلیه؛
- نحوه اعلام فاجعه؛
- شناسایی فرآیندهای تجاری و منابع فناوری اطلاعات که باید ابتدا بازیابی شوند؛
- تعریف دقیق مسئولیت‌ها در طرح؛
- تعیین دقیق افراد مسئول هر یک از عملکردهای طرح؛
- شناسایی روشن و دقیق اطلاعات قرارداد؛

- توضیح گام‌به‌گام گزینه‌های بازیابی.
- شناسایی روشن منابع گوناگون لازم برای بازیابی و تداوم فعالیت سازمان؛ و
- اجرای گام‌به‌گام طرح.

طرح باید قابل‌فهم و مستند باشد. رونوشت جدیدترین نسخه طرح نه‌تنها باید خارج از سایت نگهداری شود، بلکه همه مشارکت‌کنندگان در طرح نیز باید یک نسخه از آن را داشته باشند.

اجرا، آزمون و نگهداری طرح

آزمون طرح باید به‌گونه‌ای برنامه‌ریزی شود که کمترین اختلال را در عملیات عادی پدید آورد. آزمون باید به‌گونه‌ای انجام شود که موارد زیر را به‌دست دهد:

- کامل بودن و دقت طرح؛
- ارزیابی عملکرد کارکنان درگیر؛
- ارزیابی آموزش و آگاهی اعضای خارج از گروه تداوم کسب‌وکار؛
- اندازه‌گیری توانایی و ظرفیت سایت پشتیبان برای انجام پردازش‌های مورد نظر؛
- ارزیابی قابلیت بازیابی سوابق حیاتی؛
- ارزیابی وضعیت و مقدار تجهیزات و لوازمی که جابجا شده‌اند؛ و
- اندازه‌گیری عملکرد کلی عملیات و فعالیت‌های پردازش سیستم‌های اطلاعاتی.

انواع آزمون‌های زیر را می‌توان انجام داد:

- آزمون کاغذی- آزمون شناخت طرح، شامل همه بازیگران اصلی در اجرای طرح. آزمون کاغذی معمولاً پیش از آزمون آمادگی انجام می‌شود؛
- آزمون آمادگی- معمولاً یک نسخه ساده شده از آزمون کامل. این آزمون باید به‌طور منظم در جنبه‌های گوناگون طرح انجام شود و رویکرد مقرون به‌صرفه‌تر برای آزمون طرح است؛ و
- آزمون عملیات کامل- این آزمون یک گام با اختلال واقعی خدمات فاصله دارد.

همه نتایج آزمون(ها) باید مستند و نگهداری شوند. برنامه باید بر اساس نتایج هر آزمون، متناسب با آن به‌روز شود.

کنترل‌های دسترسی منطقی

کنترل‌های دسترسی منطقی، کنترل‌هایی در برنامه هستند که برای پیشگیری از استفاده کاربران غیرمجاز از یک برنامه کاربردی تعبیه شده‌اند. در بیشتر موارد، سازمان از کاربر می‌خواهد زمان ورود به شبکه، احراز هویت کند. هنگامی‌که شخص وارد سیستم می‌شود، برنامه از وی نام کاربری و گذرواژه می‌خواهد. اگر کاربر برای نخستین بار وارد سیستم می‌شود، مدیر باید یک نام کاربری و گذرواژه به او ارائه دهد. گذرواژه باید چنان تنظیم شود که هنگام ورود به سیستم، کاربر را مجبور به تغییر آن کند. طول و دشواری گذرواژه به خط‌مشی سازمان در مورد گذرواژه بستگی دارد. در برخی موارد، سازمان‌ها می‌توانند از یک گذرواژه استفاده کنند. کاربر تنها از یک گذرواژه برای ورود به شبکه و سیستم برنامه سازمان استفاده می‌کند. نام کاربری و گذرواژه تنها روشی نیست که یک سازمان می‌تواند برای ورود به شبکه و برنامه از آن استفاده کند. در مواردی که اطلاعات مهمی در مورد برنامه وجود دارد، می‌توان ویژگی‌های امنیتی بیشتری را برای احراز هویت از شخص درخواست کرد.

هنگامی‌که کاربر از برنامه استفاده می‌کند، پروفایلی که برای کاربر تنظیم شده است باید مطابق با شرح شغل و وظایفی باشد که انجام می‌دهد. معمولاً درخواست ثبت‌نام کاربر در برنامه با تأیید مدیر به بخش مربوط داده می‌شود.

کارکنان باید با توجه به نقشی که در سازمان دارند، برخی از دسترسی‌ها را نداشته باشند. برای مثال، شخصی که صورتحساب‌ها را دریافت می‌کند نباید به تأیید آنها نیز دسترسی داشته باشد. هنگامی‌که یکی از کارکنان، سازمان را ترک می‌کند، دسترسی ارائه شده به آن فرد در سیستم باید قطع شود.

گذرواژه‌ها برای کارکنان به دلایل زیر تعریف می‌شود:

- ❖ دسترسی به شبکه سازمان و سیستم‌های کاربردی؛ و
- ❖ اطمینان از پاسخ‌دهی در مورد برنامه‌ها.

در شرایط خاص (به دلیل اندازه یا کمبود دانش)، سازمان ممکن است از پیمانکاران برای انجام برخی از وظایف فناوری اطلاعات استفاده کند. لازم به تأکید است که در چنین مواردی سازمان همچنان باید از وجود کنترل‌های مناسب در مورد پیمانکاران اطمینان حاصل کند.

کسب شناخت از سازمان و محیط آن

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

کسب شناخت از سازمان و محیط آن

۱. اطلاعات عمومی

الف– اطلاعات مورد نیاز را در جدول‌ها تکمیل کنید.

۱ - نوع سازمان

۲ - نشانی سازمان مورد رسیدگی

نشانی	
کد پستی	
شماره تماس	
شماره فکس	
سایر	

۳ - رابطان کلیدی سازمان مورد رسیدگی

تغییر در افراد کلیدی یا جاهای خالی در این موقعیت‌ها نشان‌دهنده ریسک حسابرسی است.

نام	سمت	جزئیات تماس	
		ایمیل	شماره تلفن

۴ . آیا قراردادهای حسابرسی دیگری در سازمان مورد رسیدگی در جریان است؟

آری/ خیر

نوع قرارداد	فرد مسئول	تاریخ شروع	تاریخ تکمیل	وضعیت حسابرسی در صورت تکمیل نشدن	تعیین زمینه حسابرسی تأثیر گرفته	یافته‌های مربوط به این حسابرسی
برای مثال: حسابرسی دادگاهی، عملکرد یا مالی						

ب – تعیین ریسک‌ها یا کمبودهای کنترل داخلی شناسایی شده.

۱ . آیا ریسکی در ارتباط با موارد بالا شناسایی شده است؟

آری/ خیر

اگر آری، عوامل ریسک را در لیست زیر فهرست کنید.

	عطف به کاربرگ ارزیابی ریسک

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

کسب شناخت از سازمان و محیط آن

الف– اطلاعات مورد نیاز را در جدول‌ها تکمیل کنید.

۱. ارکان راهبری (برای این بخش لطفاً به نمودار سازمانی مراجعه کنید)

	ملاحظات	آری/خیر	کارهای انجام شده یا نظرات	شاخص‌های ریسک قابل توجه	راهنما
۱	ارکان راهبری چه کسانی هستند؟				
۲	ارکان راهبری فناوری اطلاعات چه کسانی هستند؟				
۳	آیا ارکان راهبری هر مسئولیتی را به یک کمیته تفویض کرده است؟ برای مثال، کمیته راهبرد فناوری اطلاعات یا کمیته راهبری فناوری اطلاعات؟				
۴	آیا سازمان، وظایف راهبری فناوری اطلاعات و مدیریت فناوری اطلاعات را از هم جدا کرده است؟ (برای مثال، وظایف راهبری فناوری اطلاعات از عملیات فناوری اطلاعات جدا شده است؟) (به COBiT5 (هدف‌های کنترلی برای اطلاعات و فناوری‌های مرتبط)- فرآیند توانمندسازی، فصل۴ مراجعه کنید).				
۵	آیا ارکان راهبری از مهارت‌ها و تجربه لازم برای انجام مسئولیت‌های نظارتی خود برخوردارند؟ (برای مثال، مهارت‌های راهبری فناوری اطلاعات، مدیریت پروژه فناوری اطلاعات، مهارت مالی، مهارت مدیریت ریسک، مهارت رعایت و غیره).				

	ملاحظات	آری/ خیر	کارهای انجام شده یا نظرات	شاخص‌های ریسک قابل توجه	راهنما
۶	آیا ارکان راهبری، بر توسعه کنترل داخلی فناوری اطلاعات نظارت می‌کنند؟ (برای مثال، سیاست‌ها و رویه‌های فناوری اطلاعات).				
۷	آیا ارکان راهبری، مدیریت ریسک فناوری اطلاعات را در مدیریت ریسک سازمانی (ERM) گنجانده‌اند؟				
۸	آیا ارکان راهبری فناوری اطلاعات، اطلاعات دریافتی از مدیریت و/ یا از اشخاص برون‌سازمانی را به‌دقت بررسی و بازخورد به‌موقع ارائه می‌کنند؟ برای مثال، توصیه‌هایی برای تأمین مالی پروژه‌های جدید فناوری اطلاعات.				
۹	آیا ارکان راهبری فناوری اطلاعات، در صورت لزوم، به‌طور منظم با حسابرسان داخلی و مستقل و سایرین در ارتباط هستند تا در مورد اثربخشی کنترل‌های داخلی فناوری اطلاعات گفتگو کنند؟				
۱۰	آیا برای اطمینان از برخورد به‌موقع مدیریت با ضعف‌های شناسایی شده در کنترل داخلی، ارکان راهبری فناوری اطلاعات اقدامات مناسبی انجام می‌دهند؟				
۱۱	آیا در سال گذشته تغییراتی در سازمان فناوری اطلاعات سازمان مورد رسیدگی رخ داده است؟ (برای مثال، تغییرات کارکنان/ مشاوران یا برون‌سپاری).				

	ملاحظات	آری/ خیر	کارهای انجام شده یا نظرات	شاخص‌های ریسک قابل توجه	راهنما
۱۲	آیا در دو سال آینده تغییراتی در سازمان فناوری اطلاعات سازمان مورد رسیدگی پیش‌بینی شده است؟ (برای مثال، تغییرات کارکنان/ مشاوران یا برون‌سپاری) (جزئیات مربوط به ماهیت و تاریخ تغییرات را ارائه دهید).				
۱۳	اشخاص ثالث				
۱۴	آیا سازمان از اشخاص ثالث/ مشاوران برون‌سازمانی در محیط فناوری اطلاعات استفاده می‌کند؟			حسابرس باید قراردادهایی را که سازمان با اشخاص برون‌سازمانی منعقد کرده است بررسی و از انجام تدابیر ایمنی برای حفاظت از دارایی‌های سازمان اطمینان حاصل کند.	
	الف) کدام زمینه‌ها را مشاوران پوشش می‌دهند؟ (برای مثال، شبکه)			حسابرس باید اطمینان حاصل کند که محدودیت‌های کافی، به‌ویژه برای حوزه‌های حساس، وجود دارد. حسابرس همچنین، ممکن است بودن یا نبودن سیاست طبقه‌بندی در سازمان را بررسی کند.	
	ب) آیا روابط در قالب یک قرارداد/ توافقنامه سطح خدمات/ مجوز قرارداد مدیریت می‌شود؟			توافقنامه سطح خدمات برای تعریف سطوح خدمات، به‌ویژه برای عملیات اصلی سازمان، ضروری است.	
۱۵	چه کسی دسترسی پیمانکاران را هنگام نیاز به ورود به سیستم، تأیید می‌کند؟			حسابرس باید اطمینان حاصل کند که دسترسی داده شده به اشخاص برون‌سازمانی به‌دقت کنترل و فقط برای دوره مورد نیاز ارائه می‌شود. سازمان باید رویه‌ها و مکانیسم‌هایی برای نظارت و ثبت چنین کارهایی توسط طرف‌های برون‌سازمانی داشته باشد.	

۲. حسابرسی داخلی

قابلیت اتکای کار حسابرسی داخلی را ارزیابی کنید.

	ملاحظات	آری/خیر	کارهای انجام شده یا نظرات	شاخص‌های ریسک قابل توجه	راهنما
۱	آیا سازمان، واحد حسابرسی داخلی فناوری اطلاعات یا کارکنان حسابرسی فناوری اطلاعات دارد؟				
۲	آیا کارکنان حسابرسی فناوری اطلاعات مستقیماً به رئیس حسابرسی داخلی و درنهایت به ارکان راهبری گزارش می‌دهند؟				
۳	آیا گزارش‌های حسابرسی داخلی فناوری اطلاعات مستقیماً به ارکان راهبری داده می‌شود؟				
۴	آیا حسابرسی داخلی، حسابرسی را برای همه زمینه‌های پر ریسک شناسایی شده فناوری اطلاعات و ارتباطات، برنامه‌ریزی کرده است؟				
۵	آیا محدودیت‌های شناخته شده‌ای بر عملکرد حسابرسی داخلی فناوری اطلاعات وجود دارد؟ آیا دسترسی نامحدود به اسناد، امنیت محل کار و غیره وجود دارد؟				
۶	بر اساس بررسی صلاحیت‌ها و تجربه شما، آیا گروه حسابرسی داخلی ظرفیت و شایستگی کافی برای انجام حسابرسی‌های برنامه‌ریزی‌شده فناوری اطلاعات را دارد؟ (حسابرسی فناوری اطلاعات).				

استفاده از کار حسابرسی داخلی

گزارش‌های حسابرسی داخلی فناوری اطلاعات صادر شده	تعیین مؤلفه‌های حسابرسی فناوری اطلاعات تحت تأثیر قرار گرفته	کیفیت کار حسابرسی داخلی قابل قبول است؟	آیا قصد دارید بر کارهای انجام شده اتکا کنید؟	آیا قصد دارید میزان کار حسابرسی انجام شده را کاهش دهید؟	تأثیر اتکا بر دامنه و ماهیت کار حسابرسی را مستند کنید	راهنما
						یادداشت توضیحی ۲

۳. ساختار راهبری برون‌سازمانی

	ملاحظات	جزئیات مستندات				
	آیا انتظاراتی از قانون‌گذار در مورد گزارش حسابرس وجود دارد یا خیر.					
	اخبار مطبوعات را مستند کنید و اثر آن را بر حسابرسی در نظر بگیرید.					

۳-۱. تصمیم‌های کلیدی و تصمیم‌های مؤثر بر حسابرسی

نام مجمع / کمیته	نقش‌ها و مسئولیت‌ها	پیشرفت کار	عطف به صورت‌جلسات

ب : تعیین هر نوع ریسک شناسایی شده

آیا ریسک‌هایی در ارتباط با موارد بالا شناسایی شده است؟

۱ . اگر آری، عوامل ریسک را در زیر فهرست کنید:

آری/ خیر

	عطف به کاربرگ ارزیابی ریسک

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

کسب شناخت از سازمان و محیط آن

۳. ملاحظات تقلب

الف- اطلاعات مورد نیاز را در جدول‌ها تکمیل کنید:

یادداشت راهنمای ۳

ردیف	ملاحظات حسابرسی	آری/ خیر	کارهای انجام شده یا نظرات
۱	آیا سازمان در سال گذشته با تخلف یا عمل غیرقانونی مواجه شده است؟		
۲	آیا مدیریت، سیاست‌ها و دستورالعمل‌هایی را برای پیشگیری از تقلب و سوء جریان‌ها تدوین کرده است؟		
۳	آیا مواردی وجود دارد که مدیریت بتواند کنترل‌ها را نادیده بگیرد یا آنها را زیر پا بگذارد؟		
۴	آیا تغییرات زیادی در مدیریت، عملیات یا سیستم‌های اطلاعاتی و سمت‌وسوی راهبردی کنونی سازمان رخ‌داده است؟		
۵	آیا سازمان از یک سیستم برنامه کاربردی توسعه‌یافته/ نگهداری شده در درون سازمان برای عملکردهای اصلی کسب‌وکار استفاده می‌کند یا از یک بسته نرم‌افزاری آماده؟		
۶	آیا سازمان در یک یا دو سال گذشته، تعداد قابل‌توجهی سخت‌افزار/ نرم‌افزار خریداری کرده است؟		
۷	آیا سازمان، برنامه نویسان/مشاوران/ اشخاص ثالث دیگری دارد که به سیستم‌های تولید (اطلاعات) دسترسی داشته باشد؟		

ردیف	ملاحظات حسابرسی	آری/ خیر	کارهای انجام شده یا نظرات
۸	آیا دسترسی مستقیم به پایگاه داده‌ها برای هریک از کارکنان مجاز است؟		
۹	چگونه از دارایی‌های موجود و خدمات ارائه شده در برابر سوءاستفاده، پیشگیری می‌شود؟		
۱۰	آیا سازمان اجازه استفاده از دستگاه‌های شخصی را برای انجام کسب‌وکار رسمی می‌دهد؟		
۱۱	آیا کارکنانی دارید که دسترسی فوق‌العاده به برنامه‌های کاربردی مهم کسب‌وکار داشته باشند؟		
۱۲	آیا وظایف اداری کلیدی به‌اندازه کافی تفکیک شده‌اند؟ (برای مثال، مدیریت سیستم و پایگاه داده‌ها یا مدیریت سیستم و توسعه برنامه)		
۱۳	آیا مواردی وجود دارد که استفاده از پردازش دسته‌ای در هماهنگ‌سازی سیستم‌های غیرمتمرکز به‌طور غیرعادی به تأخیر انداخته شده باشد؟		

ب : تعیین هر نوع ریسک شناسایی شده

آیا ریسکی در ارتباط با موارد بالا شناسایی شده است؟

۱ . اگر آری، عوامل ریسک را در زیر فهرست کنید:

آری/خیر

	عطف به کاربرگ ارزیابی ریسک

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

کسب شناخت از سازمان و محیط آن

۱-۳. اطلاعات کلی فناوری اطلاعات

الف: اطلاعات مورد نیاز را در جداول تکمیل کنید.

یادداشت راهنمای ۴

ردیف	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
	اطلاعات عمومی							
۱	تاریخ پیاده‌سازی				حسابرس باید تاریخ پیاده‌سازی را پرس و جو کند و تأیید آن را بگیرد؛ زیرا، برنامه‌های پیاده‌سازی شده اخیر ماهیتاً از برنامه‌های پیشین پر ریسک تر هستند.			
۲	برنامه: نسخ و انتشار				حسابرس باید به بررسی نسخه‌های جدیدتر توجه کند			
۳	اطلاعات مجوز				حسابرس باید درباره استفاده سیستم‌های اطلاعاتی از مجوزهای معتبر، تأییدیه بگیرد.			
	تعداد مجوزها/ کاربران دارای مجوز:				حسابرس باید تعداد مجوزها را با تعداد مجوزهای در حال استفاده بررسی کند تا از هدر رفتن منابع پیشگیری شود.			
	مجوزهای فعلی کجا و توسط چه‌کسانی نگهداری می‌شوند:							
۴	شرح و هدف برنامه				برنامه‌های مورد استفاده برای عملکردهای اصلی کسب‌وکار ذاتاً پر ریسک تر از برنامه‌های مورد استفاده برای عملکردهای پشتیبانی هستند.			

ردیف	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
۵	**ماژول‌ها / زیر سیستم‌های برنامه مورد استفاده**				حسابرس باید ماژول‌های در حال استفاده را با ماژول‌های خریداری شده با سیستم مقایسه کند؛ زیرا، ممکن است هدر رفتن بودجه در ماژول‌های غیرضروری سیستم را آشکار سازد.			
۶	**رابط کاربری با سایر برنامه‌ها (شرح مختصری از ماهیت و تناوب رابط کاربری ارائه دهید)**				حسابرس باید به رابط‌های کاربری دستی روی سیستم توجه داشته باشد، زیرا آنها سیستم را نسبت به رابط‌های خودکار پر ریسک‌تر می‌کنند.			
۷	**آیا سیستم دارای سِرورِ پشتیبان است؟**				نبود سِرورِ پشتیبان نشان‌دهنده ریسک بالاتری نسبت به وجود سِرورِ پشتیبان است.			
	پشتیبان‌گیری در کجا صورت می‌گیرد؟				پشتیبان‌گیری خارج از سایت، ایمن‌تر و پشتیبان‌گیری در داخل سایت، پر ریسک‌تر می‌باشد.			
۸	**مالک سیستم برنامه**				سیستمی که متعلق به سازمان نباشد، ممکن است از سیستمی که متعلق به سازمان است، ریسک بیشتری داشته باشد.			
۹	**آخرین پَچ منتشر شده سیستم**				حسابرس باید بررسی پچ‌های از قلم افتاده را مورد توجه قرار دهد.			
۱۰	**آخرین پچ پیاده‌سازی شده توسط سازمان**				حسابرس باید به بررسی پچ‌های از قلم افتاده بپردازد.			
۱۱	**مدیر سیستم یا اداره‌کننده**				صلاحیت، تجربه و درستکاری مدیر سیستم بر مشخصات ریسک سیستم تأثیر دارد. برای مثال، مدیر بی‌صلاحیت یا تجربه یا عدم درستکاری مدیر، سیستم را در معرض ریسک بیشتری قرار می‌دهد.			

ردیف	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
۱۲	**تعداد تراکنش‌های پردازش شده (در روز/ماه/سال)**				سیستمی که حجم زیادی از تراکنش‌ها را پردازش می‌کند ذاتاً ریسک بیشتری نسبت به سیستمی دارد که تراکنش‌های کمتری را پردازش می‌کند.			
۱۳	**ارزش معاملات پردازش شده**				معاملات باارزش بالاتر ممکن است حاکی از ریسک بالاتر و تأثیر بیشتر نسبت به معاملات باارزش کمتر باشد.			

ب : هرگونه ریسک شناسایی شده

آیا ریسکی در ارتباط با موارد بالا شناسایی شده است؟

۱. اگر آری، عوامل ریسک را در زیر فهرست کنید:

آری/ خیر

*** نکته: حسابرس ممکن است به حوزه‌هایی توجه کند که در آنها، شاخص‌های ریسک، بالا یا متوسط شناسایی شده است.**

	عطف به کاربرگ ارزیابی ریسک

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

کسب شناخت از سازمان و محیط آن

۲-۳. ارزیابی زیرساخت‌های کاربردی سازمان مورد رسیدگی

الف: اطلاعات مورد نیاز را در جدول‌ها تکمیل کنید.

یادداشت راهنمای ۴

	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
	اطلاعات فنی در سِرورِهای برنامه							
۱	سیستم عامل: نسخه و انتشار				حسابرس باید به بررسی نسخه‌های جدیدتر بپردازد؛ زیرا، نسخه‌های قدیمی نسبت به نسخه‌های جدیدتر ریسک بیشتری دارند.			
۲	نرم‌افزار کنترل دسترسی (در صورت وجود): نسخه و انتشار				حسابرس باید در دسترس بودن نرم‌افزار کنترل دسترسی را بررسی کند. نبود آن نشان‌دهنده ریسک بالاتر است.			
۳	چه کسی مسئولیت مدیریت، نگهداری و عملیات سیستم عامل را بر عهده دارد؟ نام، اطلاعات تماس و مسئولیت‌های اساسی همه کارکنان سیستم عامل را به‌دست آورید.				حسابرس باید صلاحیت، درستکاری و سِمت شخص/ اشخاص را در نظر بگیرد.			
۴	آیا از زمان آخرین کار حسابرسی، تغییرات قابل توجهی در زمینه پلتفرم برنامه ایجاد شده است؟ (جزئیات مربوط به ماهیت و تاریخ تغییر را گردآوری کنید).				تغییرات اخیر در پلتفرم نشان‌دهنده ریسک بالاتر است.			

	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
۵	آیا تغییراتی در زمینه پلتفرم برنامه در سال آینده پیش‌بینی‌شده است؟ (جزئیات مربوط به ماهیت و تاریخ تغییر را گردآوری کنید).				تغییرات پیش‌بینی‌شده نشان‌دهنده ریسک بالاتر است.			
	مدیریت پایگاه داده‌ها (فقط در صورتی قابل اجرا است که یک پایگاه داده جداگانه وجود داشته باشد).							
۶	صاحبکار از چه سیستم مدیریت پایگاه داده‌ای استفاده می‌کند؟							
۷	الف) آیا پایگاه داده متمرکز/ غیرمتمرکز است؟				اگر پایگاه داده‌ها غیرمتمرکز باشد، ریسک بیشتر است؛ زیرا، سازمان برای اطمینان از امنیت کافی در تمام سایت‌هایی که پایگاه داده‌ها در آن قرار دارد به منابع بیشتری نیاز دارد.			
	ب) محل سِروِرهای پایگاه داده را مشخص کنید.							
۸	اطلاعات فنی سِروِرهایی که پایگاه داده‌ها در آن قرار دارند:							
	الف) سیستم عامل: نسخه و انتشار							
	ب) نرم‌افزار کنترل دسترسی (در صورت وجود): نسخه و انتشار							
۹	چه کسی مسئول نگهداری پایگاه داده‌ها است؟ (نام‌ها، جزئیات تماس و مسئولیت‌های اساسی همه مدیران و کارکنان پایگاه داده‌ها، همراه با عملکردهای مرتبط با پایگاه داده‌ها را گردآوری کنید).				حسابرس باید این موضوع را بررسی کند که آیا مدیران، به برنامه زنده دسترسی دارند یا با استفاده از برنامه، هر کاری را انجام می‌دهند.			

	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
۱۰	آیا استفاده از انبار داده‌ها/ سیستم اطلاعاتی مدیریت، برای سازمان مورد رسیدگی مهم است (برای مثال، گزارش‌ها برای تصمیم‌گیری‌های مدیریت/ کنترل بودجه استفاده می‌شود؛ داده‌ها برای هدف‌های معاملاتی استفاده می‌شوند).							
۱۱	اطلاعات فنی سِرورهایی که انبار داده‌ها/ سیستم اطلاعاتی مدیریت، در آن قرار دارد (تنها در صورت بااهمیت بودن):				اگر اطلاعات فنی به‌راحتی در دسترس نباشد، می‌تواند بر تداوم فعالیت کسب‌وکار تأثیر بگذارد.			
	الف) سیستم‌عامل: نسخه و انتشار				اگر سیستم‌عامل انتشار یافته بود، ب را نادیده بگیرید.			
	ب) نرم‌افزار کنترل دسترسی (در صورت وجود): نسخه و انتشار							
۱۲	آیا تغییرات قابل‌توجهی در مورد پایگاه داده‌ها یا انبار داده‌های برنامه کاربردی از زمان آخرین کار حسابرسی ایجاد شده است؟ (جزئیات مربوط به ماهیت و تاریخ تغییر را ارائه دهید).				حسابرس باید توجه داشته باشد که تغییر جدید یا تغییرات زیادی رخ داده است.			
۱۳	آیا در یک سال آینده تغییراتی در مورد پایگاه داده‌ها و انبارهای داده برنامه کاربردی پیش‌بینی‌شده است؟ (جزئیات مربوط به ماهیت و تاریخ تغییر را گردآوری کنید).				اگر سازمان تغییرات آتی را پیش‌بینی کند، به این معنا است که برنامه دارای مشکلاتی است که باید برطرف شود. این، برنامه را پر ریسک تر می‌کند.			
	ورود کاربر به برنامه و احراز هویت							
۱۴	مراحل ورود کاربر به برنامه را توضیح دهید.				حسابرس باید برای اطمینان از اجرای روش‌های کافی و ایمن برای ورود، سطوح احراز هویت را بررسی کند.			

	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
۱۵	آیا مراحل ورود به سیستم یک کاربر دور کار (در صورت وجود) متفاوت است؟							
۱۶	کدام مؤلفه سیستم‌های اطلاعاتی، دسترسی کاربران به برنامه را تأیید می‌کند (یعنی شناسه و گذرواژه کاربر کجا تعریف شده است؟).							
	الف) سیستم‌عامل							
	ب) برنامه/ پایگاه داده‌ها /شبکه							
	پ) سیستم‌عامل / دسترسی دیگر							
	ت) نرم‌افزار کنترل							
۱۷	حق دسترسی برنامه (پروفایل‌های کاربر) کجا تعریف شده است- در برنامه/ پایگاه داده/ سیستم‌عامل شبکه/ سایر نرم‌افزارهای کنترل دسترسی؟							
۱۸	آیا دسترسی به برنامه از طریق یک شبکه محلی یا شبکه گسترده به دست می‌آید یا روی یک رایانه مستقل است؟							
۱۹	چه کسی مسئولیت مدیریت امنیت کاربران را بر عهده دارد؟ (یعنی تعریف کاربران جدید و غیره).				حسابرس باید دخالت داشتن یا نداشتن کاربران را در فرآیند کسب‌وکار سیستم بررسی کند.			
	(اطلاعات مربوط به نام و اطلاعات تماس را گردآوری کنید).							

	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
۲۰	آیا تغییرات قابل‌توجهی در رابطه با ورود به سیستم و احراز هویت کاربران برنامه، از آخرین کار حسابرسی، ایجاد شده است؟ (جزئیات مربوط به ماهیت و تاریخ تغییر را گردآوری کنید).				حسابرس باید موارد زیر را در نظر بگیرد: بررسی هرگونه پیشنهاد/ درخواست تغییر توسط مدیران سیستم به ارکان راهبری، درخواست تغییر ارائه شده، اما بدون پاسخ از سوی ارکان راهبری، هیچ تغییری در پاسخ به یافته‌های کار حسابرسی پیشین ایجاد نشده است.			
۲۱	آیا تغییراتی در سال‌های آینده در ارتباط با ورود و احراز هویت کاربران برنامه پیش‌بینی شده است؟ (جزئیات مربوط به ماهیت و تاریخ تغییر را گردآوری کنید).				حسابرس باید بودن برنامه مستند برای تغییرات آتی را بررسی کند			
	ورودی و پردازش							
۲۲	آیا ورودی برنامه متمرکز است یا غیرمتمرکز؟ (جزئیات مربوط به مکان سایت‌های ورودی را گردآوری کنید)				حسابرس باید موارد زیر را بررسی کند: ❖ اگر ورودی برنامه غیرمتمرکز است، آیا سازمان، منبعی برای اطمینان از کنترل کافی ورودی‌ها دارد یا خیر. ❖ اگر متمرکز است، کنترل‌های مربوط به ورودی‌های برنامه را ارزیابی کند.			
۲۳	آیا پردازش برنامه متمرکز، غیرمتمرکز یا توزیع شده است؟ (کسب جزئیات درمورد محل پردازش).				حسابرس باید موارد زیر را بررسی کند: ❖ اگر پردازش برنامه غیرمتمرکز است، آیا سازمان منبعی برای اطمینان از کنترل کافی بر پردازش دارد یا خیر. ❖ اگر متمرکز است، کنترل‌های مربوط به پردازش برنامه را ارزیابی کند.			

	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
۲۴	ماهیت محیط پردازش را شناسایی کنید:							
	الف) پردازنده مرکزی بزرگ							
	ب) سِروِر سازمان مورد رسیدگی							
	پ) تین‌کلاینت (یک رایانه‌ی کوچک و آماده برای شبکه‌های رایانه‌ای است که در عین استفاده از کمترین منابع سخت‌افزاری، بالاترین کارایی و امنیت را برای شبکه‌های رایانه‌ای به همراه می‌آورد. تین‌کلاینت می‌تواند دارای سیستم‌عامل یا بدون سیستم عامل باشد. م) تیک کلاینت (یک ایستگاه کاری محاسباتی است که شامل اکثر یا تمام اجزای ضروری برای عملکرد و اجرای برنامه‌های نرم‌افزاری مستقل است. تیک‌کلاینت یکی از اجزای معماری محاسباتی سرویس‌گیرنده-سِروِر است که از طریق اتصال شبکه به سِروِر متصل می‌شود و هیچ‌یک از منابع محاسباتی سِروِر را برای اجرای برنامه‌ها مصرف نمی‌کند. م).							
	ت) میان‌افزار							
	ث) پردازش رایانه شخصی (محدود/ بدون پردازش روی سرور).							
۲۵	آیا پردازش، بی‌درنگ یا پردازش دسته‌ای انجام می‌شود؟				حسابرس باید موارد زیر را بررسی کند: ❖ در صورت پردازش بی‌درنگ، سازمان پیش از انجام پردازش کنترل‌های کافی دارد یا خیر.			

	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
					❖ اگر پردازش دسته‌ای انجام می‌شود، کنترل‌های سازمان در مورد یکپارچگی داده‌ها، کدگذاری، تصحیح خطای ورودی و غیره را شناسایی کند.			
۲۶	آیا داده‌ها برای انتقال به رایانه‌ها یا برنامه‌های دیگر برای ورودی، پردازش یا خروجی، دانلود می‌شوند؟ (جزئیات مربوط به زمان، چگونگی و چرایی انتقال را دریافت کنید).				حسابرس باید ارزیابی ریسک دستکاری داده‌ها را با توجه به انتقال داده‌ها در نظر بگیرد			
۲۷	چه کسی مسئول حفظ داده‌های ثابت در سیستم است؟ (نام و مشخصات فرد مسئول را یادداشت کنید).				حسابرس باید ریسک تغییرات غیرمجاز در داده‌های اصلی را ارزیابی کند			
۲۸	آیا اپراتورهای تمام‌وقت، پردازش و زمان‌بندی کار را انجام می‌دهند یا عملیات، خودکار است؟ (در صورت وجود، نام و مشخصات اپراتورها را ارائه دهید).							
۲۹	آیا پایگاه داده‌های برنامه، یکپارچه است یا یک پایگاه داده جداگانه با یک سیستم مدیریت پایگاه داده وجود دارد؟				حسابرس باید ریسک به‌روزرسانی غیرمجاز برنامه را با استفاده از پایگاه داده‌ها ارزیابی کند.			
۳۰	آیا تغییرات قابل‌توجهی در ورودی و پردازش برنامه از زمان حسابرسی پیشین ایجاد شده است؟ (جزئیات مربوط به ماهیت تغییرات و داده‌های تغییر را ارائه دهید).				حسابرس باید احتمال عدم یکپارچگی داده‌ها را به دلیل ایجاد تغییرات، ارزیابی کند.			
۳۱	آیا تغییرات پیش‌بینی شده‌ای در سال‌های آینده درباره ورودی و پردازش برنامه وجود دارد؟ (جزئیات مربوط به ماهیت تغییر و تاریخ تغییر را ارائه دهید).				حسابرس باید چگونگی احتمال پیدایش ریسک در دسترس بودن، محرمانگی و یکپارچگی داده‌ها در اثر انجام تغییرات پیش‌بینی شده را ارزیابی کند.			

	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
	کنترل‌های تغییر							
۳۲	آیا برنامه:							
	الف) در درون سازمان توسعه یافته است؟ (به ۳۳ بروید).				حسابرس باید در دسترس بودن فرآیند توسعه تأییدشده را بررسی کند.			
	ب) سیستم آماده یا بسته نرم‌افزاری تجاری است؟ (به ۳۴ بروید).				حسابرس باید نبود رویه‌های اجرایی را بررسی کند.			
۳۳	اگر برنامه، در درون سازمان توسعه یافته است، به پرسش‌های زیر پاسخ دهید.							
	الف) آیا سازمان مورد رسیدگی فرآیند توسعه قابل تأییدی دارد؟				حسابرس باید فرآیند توسعه مستند شده را بررسی کند			
	ب) آیا برنامه نویسان از درون یا برون از سازمان هستند؟				حسابرس باید این موضوع را بررسی کند که اگر برنامه نویسان درون‌سازمانی دسترسی بیشتری به اجزای مختلف سیستم دارند، این یک تهدید است، برای مثال، دستکاری داده‌ها.			
	پ) آیا برنامه‌نویس به محیط تولید دسترسی دارد؟				حسابرس باید دسترسی برنامه‌نویس به محیط تولید، چه اندک چه زیاد، را بررسی کند. این ممکن است به ایجاد گلوگاه تغییرات تأیید نشده منجر شود.			
	ت) آیا سازمان مورد رسیدگی کد منبع را در کنترل یا مالکیت دارد؟				حسابرس باید داشتن منبع توسط سازمان را دست‌کم از دیدگاه هدف‌های تداوم (فعالیت) بررسی کند.			
	ث) میزان تغییرات برنامه از انجام کار حسابرسی پیشین (هیچ، کم، متوسط، زیاد).				حسابرس باید تغییرات پیشنهاد شده از حسابرسی پیشین را که اجرا نشده است، بررسی کند.			

	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کار برگ یا شواهد
	ج) کنترل‌های تغییر و نسخه نرم‌افزار کنترل.				حسابرس باید نسخه‌های جدیدتر را بررسی کند؛ زیرا، نسخه‌های قدیمی ریسک بیشتری نسبت به نسخه‌های جدیدتر و بهبود یافته دارند.			
	چ) محیط‌های در حال استفاده؟ (تولید، توسعه، آزمایش/ آموزش و غیره) (مشخص کنید که از چه محیط‌هایی برای توسعه و آزمایش تغییرات برنامه استفاده می‌شود).				حسابرس باید در طول اجرای تغییرات به بررسی سیستم‌هایی بپردازد که تنها در محیط تولید اجرا می‌شوند زیرا، مستعد ایجاد گلوگاه هستند.			
	ح) اطلاعات فنی مربوط به سِرورهایی که محیط توسعه و آزمایش در آنها قرار دارد را، در صورت وجود، ارائه دهید:							
	سیستم‌عامل:				حسابرس باید نسخه‌های جدیدتر را بررسی کند؛ زیرا، نسخه‌های قدیمی ریسک بیشتری نسبت به نسخه‌های جدیدتر و بهبود یافته دارند.			
	نسخه و انتشار:				حسابرس باید نسخه‌های جدیدتر را بررسی کند، زیرا نسخه‌های قدیمی ریسک بیشتری نسبت به نسخه‌های جدیدتر و بهبود یافته دارند.			
	نرم‌افزار کنترل دسترسی (در صورت وجود)							
	نسخه و انتشار:				حسابرس باید نسخه‌های جدیدتر را بررسی کند، زیرا نسخه‌های قدیمی ریسک بیشتری نسبت به نسخه‌های جدیدتر و بهبود یافته دارند.			

	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
	خ) اگر پردازش غیرمتمرکز/ توزیع شده باشد، سیستم‌ها در سایت‌ها چگونه با تغییرات برنامه به‌روزرسانی می‌شوند؟							
	د) چه کسی مسئولیت نگهداری نرم‌افزار را بر عهده دارد؟ (اسامی، جزئیات تماس و مسئولیت‌های اصلی همه کارکنان برنامه‌نویسی را ارائه دهید).				حسابرس باید از وجود کارکنان آموزش‌دیده اطمینان یابد.			
۳۴	اگر سیستم آماده یا بسته نرم‌افزاری تجاری است، پرسش‌های زیر را پاسخ دهید:							
	الف) فروشنده/ تأمین‌کننده نرم‌افزار							
	ب) میزان متناسب‌سازی در سازمان مورد رسیدگی؟				حسابرس باید از بودن رویه متناسب‌سازی اطمینان بدست آورد.			
	پ) میزان و ماهیت متناسب‌سازی/ اصلاح پس از پیاده‌سازی.				حسابرس باید از بودن رویه متناسب‌سازی اطمینان بدست آورد.			
	ت) چه کسی مسئول متناسب‌سازی برنامه است (تأمین‌کننده یا سازمان مورد رسیدگی)؟				حسابرس باید از بودن رویه متناسب‌سازی اطمینان بدست آورد.			
	ث) اگر سازمان مورد رسیدگی مسئول متناسب‌سازی است موارد زیر را بررسی کنید:				حسابرس باید از بودن رویه متناسب‌سازی اطمینان بدست آورد.			
	۱. نام، اطلاعات تماس و مسئولیت‌های اصلی همه کارکنان برنامه‌نویسی را ارائه دهید.							
	۲. اطلاعات فنی مربوط به سِرورهایی که محیط توسعه و/ یا آزمایش بر روی آنها قرار دارد (در صورت وجود).							

	نام برنامه	برنامه ۱	برنامه ۲	برنامه ۳	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کار بر گ یا شواهد
	سیستم‌عامل: نسخه و انتشار				حسابرس باید نسخه‌های به‌روز شده را بررسی و از نصب پچ‌ها اطمینان حاصل کند.			
	نرم‌افزار کنترل دسترسی (در صورت وجود).							
	نسخه و انتشار:				حسابرس باید نسخه‌های به‌روز شده را بررسی و از نصب پچ‌ها اطمینان حاصل کند.			
	ج) آیا روابط (ترتیبات) امانی وجود دارد؟				حسابرس باید توافق‌نامه‌های قراردادی را برای اطمینان از ایمنی داده‌های سازمان، بررسی کند.			
	چ) اگر پردازش غیرمتمرکز/توزیع شده باشد، سایت‌ها چگونه با تغییرات ایجاد شده به‌روز می‌شوند؟				حسابرس باید فرآیند تغییر را مشاهده کند تا از در معرض ریسک اختلال نبودن برنامه، اطمینان بدست آورد.			
	ح) اگر تأمین‌کننده، مسئول متناسب‌سازی باشد، سیستم چگونه با تغییرات ایجاد شده (همچنین در سایت‌های غیرمتمرکز/ توزیع شده) به‌روز می‌شود؟				حسابرس باید فرآیند تغییر را مشاهده کند تا از در معرض ریسک اختلال نبودن برنامه، اطمینان بدست آورد.			
	خ) آیا برنامه نویسان (سازمان مورد رسیدگی یا تأمین‌کننده) به موارد زیر دسترسی دارند: محیط تولید (در صورت وجود)، محیط توسعه و/یا آزمایش (در صورت وجود).							
۳۵	مستندات سیستم‌ها کجا نگهداری می‌شود؟							

ب : هرگونه ریسک شناسایی شده را مشخص کنید.

آیا ریسک‌هایی در ارتباط با موارد بالا شناسایی شده است؟

۱. اگر آری، عوامل ریسک را در زیر فهرست کنید:

آری/ خیر

	عطف به کاربرگ ارزیابی ریسک

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

کسب شناخت از سازمان و محیط آن

۳-۳. ارزیابی زیرساخت شبکه سازمان مورد رسیدگی

الف: اطلاعات مورد نیاز را در جدول‌ها تکمیل کنید.

یادداشت راهنمای ۴

		پاسخ‌ها	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
	اطلاعات محیط شبکه					
۱	سیستم عامل شبکه: نسخه و انتشار.		حسابرس باید به بررسی پـچ‌هـای ازقلم‌افتاده بپردازد.			
۲	آیا سازمان مورد رسیدگی به اینترنـت دسترسی دارد و دسترسی، به کارکنان خاصی محدود است یا برای همه کارکنان دسترسی وجود دارد؟		حسابرس باید ضعف عملکرد شبکه یا مشکلات اتصال را بررسی کند.			
۳	آیا سازمان مورد رسیدگی وب‌سـایت دارد؟ (ارائه آدرس وب‌سایت).					
۴	یک نمودار از واحد شبکه ارائه دهیـد. مشخص کنید که آیا موارد زیر وجـود دارد:					
	الف) سِروِرهای احراز هویت					
	ب) سِروِرهای برنامه		حسابرس بایـد شـبکه محیطـی ضعیف و تنظیمات امنیتی (فایروال) و همچنین، امکانـات غیرضـروری فعال یا نصب شده را بررسی کند.			

		پاسخ‌ها	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
	پ) سِروِرهای پایگاه داده					
	ت) سِروِرهای انتقال فایل (FTP)					
	ث) سِروِرهای وب					
	ج) سِروِرهای پست الکترونیکی					
	چ) سایر سِروِرهای ذخیره‌سازی					
	ح) فایروال‌ها و پراکسی‌ها					
	خ) روترها و سوئیچ‌ها					
	د) منطقه غیرنظامی					
	ذ) سِروِرهای دریافت‌کنندگان گزارش‌ها					
۵	اطلاعات فایروال (در صورت وجود):					
	الف) نرم‌افزار فایروال: نسخه و انتشار		حسابرس باید به بررسی نسخه‌های جدیدتر و پچ‌های ازقلم‌افتاده بپردازد.			
	ب) سیستم‌عامل: نسخه و انتشار (سِروِری که فایروال روی آن قرار دارد).		حسابرس باید به بررسی نسخه‌های جدیدتر و پچ‌های ازقلم‌افتاده بپردازد.			
۶	آیا اشخاص برون‌سازمانی به شبکه دسترسی دارند؟		حسابرس باید خطاها یا اقدامات غیرمجاز (دسترسی نادرست، افشا، تغییر یا تخریب اطلاعات) توسط اشخاص برون‌سازمانی را بررسی کند.			
	الف) هدف از دسترسی را مشخص کنید.					
	ب) روش دسترسی (مودم/ اتصال شخص برون سازمانی/ سِروِر دریافت‌کنندگان اطلاعات)					
۷	چه کسی مسئولیت مدیریت شبکه را بر عهده دارد؟ (ارائه نام، مشخصات تماس و مسئولیت‌های اصلی همه مدیران و کارکنان شبکه همراه با عملکردهای مرتبط با شبکه).		حسابرس باید تخصص و مهارت مدیران فناوری و امنیت را بررسی کند. مثلاً خطای پیکربندی، دسترسی غیرمجاز.			

		پاسخ‌ها	شاخص‌های ریسک قابل توجه	کارهای انجام شده یا نظرات	شاخص ریسک اولیه (پایین، متوسط یا بالا)	عطف به کاربرگ یا شواهد
۸	آیا از حسابرسی پیشین فناوری اطلاعات در ارتباط با شبکه، تغییری ایجاد شده است؟ (جزئیات مربوط به ماهیت و تاریخ تغییرات را ارائه دهید).					
۹	آیا تغییراتی در سال آینده در ارتباط با شبکه پیش‌بینی شده است؟ (جزئیات مربوط به ماهیت و تاریخ را ارائه دهید).					
۱۰	چالش‌های شناسایی شده سیستم: معافیت‌هایی که درباره این موارد اعطاشده است (در صورت وجود) و توسط چه کسی:					
۱۱	سایر اطلاعات ضروری سیستم.					

ب : هرگونه ریسک شناسایی شده را مشخص کنید.

آیا ریسک‌هایی در ارتباط با موارد بالا شناسایی شده است؟

اگر آری، عوامل ریسک را در زیر فهرست کنید:

آری/ خیر

	عطف به کاربرگ ارزیابی ریسک

پیوست ۴:
ارزیابی ریسک

یادداشت‌های راهنما

ریسک‌های شناسایی شده در این کاربرگ باید به کاربرگ ارزیابی ریسک منتقل شود.

یادداشت راهنمای شماره ۱

هنگام تهیه شرح سیستم و ارزیابی ریسک فرآیند کسب‌وکار در جریان حسابرسی سیستم‌های اطلاعاتی، بهترین رویه عمل، تقسیم فرآیندهای تجاری به چندین سطح است. برای مثال.

فرآینـد سطح ۱: فرآیند پیوسته (end-to-end) را کامل کنید، برای مثال. ماژولی برای مدیریت زنجیره تأمین.

فرآیند سطح ۲: به یک جزء اصلی از فرآیند پیوسته اشاره دارد. برای مثال، پردازش پرداختنی‌ها، مدیریت دریافتنی‌ها، مدیریت دارایی‌های ثابت، مدیریت موجودی، پردازش حقوق و دستمزد، فروش، مدیریت وجوه نقد، پشتیبانی و غیره.

فرآیند سطح ۳: این سطح، اجزای فرعی یا جزئی هر یک از فرآیندهای اصلی را در برمی‌گیرد. مانند درخواست و ایجاد سفارش خرید در فرآیند اصلی سطح بالاتر در پشتیبانی.

فرآیند سطح ۴- فعالیت: این سطح نهایی، تراکنش‌های سیستمی را فهرست می‌کند که به ایجاد، تغییر یا حذف داده‌ها برای هر یک از اجزای فرعی یا جزئی منجر می‌شود.

دیوان محاسبات باید رتبه‌بندی‌های مورد استفاده را برای ارزیابی ریسک، تأثیر و شدت ریسک تعیین کند.

لطفاً به مثال انجام شده در ادامه توجه کنید.

یادداشت راهنمای شماره ۲

شرح فرآیند/ سیستم

شرح فرآیند/ سیستم باید به‌اندازه کافی دقیق باشد تا حسابرس بتواند همه ریسک‌های فرآیند و کنترل‌های لازم برای برخورد با این ریسک‌ها را شناسایی کند. حسابرس باید مالکان فرآیندها یا فرآیندهای فرعی و نقطه شروع و پایان فرآیندها/ فرایندهای فرعی را به‌روشنی شناسایی کند.

یادداشت راهنمای شماره ۳

در فرآیند فرعی، چه چیزی می‌تواند اشتباه باشد. حسابرس سیستم‌های اطلاعاتی باید از جامع بودن فهرست تهدیدهای احتمالی اطمینان بدست آورد.

حسابرس سیستم‌های اطلاعاتی در تصمیم‌گیری در مورد شدت ریسک، احتمال و اثر برآوردی رخداد تهدید را در نظر می‌گیرد.

یادداشت راهنمای شماره ۴

فعالیت‌های کنترلی، خط‌مشی‌ها، رویه‌ها و تکنیک‌هایی هستند که به اطمینان از دستیابی مؤثر مدیریت به هدف‌های کنترل کمک می‌کنند. حسابرس فناوری اطلاعات باید فعالیت‌های کنترلی مرتبط با هدف کنترلی مورد بررسی را شناسایی کند.

یادداشت راهنمای شماره ۵

حسابرس سیستم‌های اطلاعاتی باید به کاربرگی که ریسک شناسایی شده در آن ارزیابی می‌شود، عطف دهد (کاربرگ ارزیابی ریسک و برخورد با آن).

فرآیند کسب و کار و شناسایی ریسک

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

فرایندهای کسب‌وکار پشتیبانی شده توسط سیستم‌های اطلاعاتی را شناسایی کنید.

شناسایی فرآیند				شناسایی ریسک فرآیند				
سطح ۱: نام فرآیند /توضیحات	سطح ۲: نام فرآیند/توضیحات	سطح ۳: نام فرآیند/توضیحات	سطح ۴: نام فرآیند/توضیحات	شرح فرآیند/ سیستم	ریسک‌های ذاتی	کنترل‌های داخلی	رتبه‌بندی ریسک (پایین، متوسط و بالا)	عطف به کاربرگ ارزیابی ریسک و برخورد با آن
یادداشت راهنمای ۱	یادداشت راهنمای ۱	یادداشت راهنمای ۱	یادداشت راهنمای ۱	یادداشت راهنمای ۲	یادداشت راهنمای ۳	یادداشت راهنمای ۴		یادداشت راهنمای ۵
خرید تا پرداخت	فرآیند پشتیبانی	برنامه پشتیبانی						

یادداشت‌های راهنما

بهترین رویه عمل هنگام تهیه شرح سیستم و ارزیابی ریسک فرآیند کسب وکار در جریان حسابرسی سیستم‌های اطلاعاتی، تقسیم فرآیندهای تجاری ممکن به چندین سطح است. برای مثال.

فرآیند سطح ۱: فرآیند پیوسته (end-to-end) را کامل کنید. برای مثال. ماژولی برای مدیریت زنجیره تأمین.

فرآیند سطح ۲: به یک جزء اصلی از فرآیند پیوسته اشاره دارد. برای مثال، پردازش پرداختنی‌ها، مدیریت دریافتنی‌ها، مدیریت دارایی‌های ثابت، مدیریت موجودی، پردازش حقوق و دستمزد، فروش، مدیریت وجوه نقد، پشتیبانی و غیره.

فرآیند سطح ۳: این سطح، اجزای فرعی یا جزئی هر یک از فرآیندهای اصلی را دربر می‌گیرد. مانند درخواست و ایجاد سفارش خرید در فرآیند اصلی سطح بالاتر در پشتیبانی.

فرآیند سطح ۴– فعالیت: این سطح نهایی، تراکنش‌های سیستمی را فهرست می‌کند که به ایجاد، تغییر یا حذف داده‌ها برای هر یک از اجزای فرعی یا جزئی منجر می‌شود.

دیوان محاسبات باید رتبه‌بندی‌های مورد استفاده را برای ارزیابی ریسک، تأثیر و شدت ریسک تعیین کند.

توجه: ریسک‌های شناسایی‌شده در این کاربرگ باید هنگام تدوین برنامه‌های حسابرسی به فهرست ریسک منتقل شود و مورد توجه قرار گیرد.

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

شرح سیستم ۱: سطح ۱ – ارزیابی فرآیند

وظایف اصلی سازمان مورد رسیدگی کدامند؟

_____

_____

_____

_____

_____

شرح سیستم ۲: سطح ۲ – تجزیه و تحلیل فرآیند

سطح ۱ نام فرآیند: برای مثال مدیریت زنجیره تأمین

نام/ شرح فرآیندهای سطح ۲	فرآیندهای سطح ۳	ملاحظات فناوری اطلاعات و ارتباطات (سیستم‌های مهم پشتیبانی عمومی و برنامه‌های کاربردی اصلی را که برای پشتیبانی از یک فرآیند تجاری استفاده می‌شوند، شناسایی کنید)
برای مثال، پشتیبانی	برای مثال: پردازش سفارش خرید	از نسخه R2 سال ۲۰۱۳ نرم‌افزار Microsoft Dynamics Navision استفاده کنید
	برای مثال: پردازش دریافت کالا	
	برای مثال: پردازش برگشت کالا	

شرح سیستم ۳: سطح ۳ – تجزیه و تحلیل فرآیندها

برای هر یک از فرآیندهای فرعی شناسایی شده در بالا، از این الگو برای مستندسازی جزئیات فرآیندهای فرعی استفاده کنید.

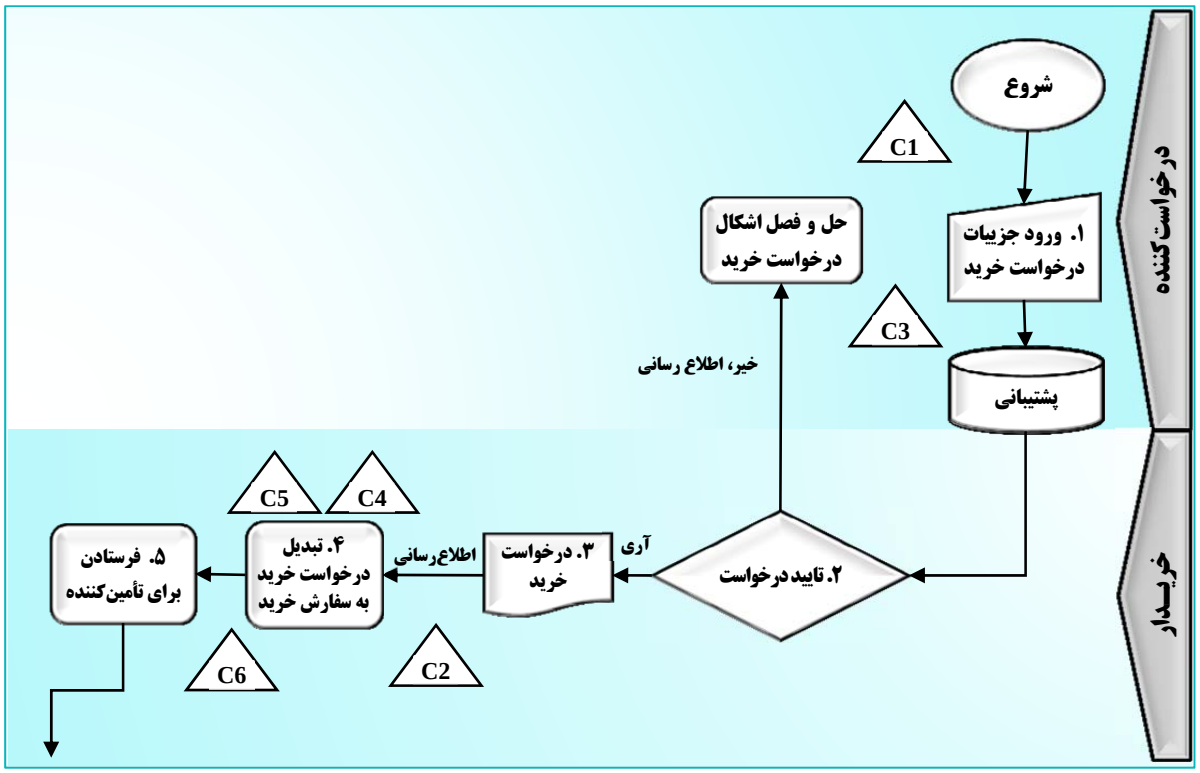
نام فرآیند اصلی: پشتیبانی

نام فرآیند فرعی:	برای مثال: پردازش سفارش خرید	تاریخ گردآوری داده‌ها:
مالک فرآیند	برای مثال: مدیر پشتیبانی	عطف به برنامه حسابرسی (در صورت وجود)
نقطه شروع فرآیند ورودی‌ها [مثال] ❖ اقدام به درخواست کالا. ❖ موجودی به سطح سفارش دوباره رسیده است. ❖ نیازهای جدید مستلزم تأمین کالاهای جدید.	هدف‌ها و فعالیت‌های کنترلی. برای مثال: ❖ اطمینان از اینکه تنها، کالاهای مورد نیاز خریداری می‌شود. ❖ اطمینان از اینکه تنها، درخواست‌های مجاز انجام می‌شود.	نقطه پایان فرآیند خروجی‌ها [مثال] سفارش خرید برای تأمین‌کننده فرستاده شد.

مستندسازی فرآیند [مثال انجام شده در زیر]

- ❖ هنگامی که بخش زنجیره تأمین، قصد خرید موجودی اضافی را دارد، گزارشی از موجودی‌های کمتر از سطح سفارش دوباره موجودی به‌صورت دستی تهیه می‌شود، سپس توسط یکی از کارکنان خرید، یک درخواست خرید در برنامه پشتیبانی ثبت می‌شود (کنترل C1).
- ❖ هنگامی‌که درخواست ایجاد شد، مدیر پشتیبانی، درخواست خرید را از نظر مناسب بودن، کامل بودن و دقت آن بررسی می‌کند. اجزای درخواست خرید که بررسی می‌شوند، اما بررسی به آنها محدود نمی‌شود عبارتند از: فروشنده، کالا، مقدار و کد حساب.
- ❖ چنانچه این بررسی هیچ‌گونه ایرادی را نشان ندهد، مدیر پشتیبانی درخواست خرید را تأیید می‌کند. درصورتی‌که مدیر پشتیبانی به هر دلیل درخواست خرید را رد کند، به درخواست‌کننده اطلاع داده می‌شود.
- ❖ سرانجام، اگر مشکلات درخواست خرید، حسب مورد، حل شود، مدیر پشتیبانی درخواست را تأیید می‌کند. تمام درخواست‌های خرید به صورت ماهانه بررسی می‌شوند تا هرگونه درخواست غیرمجاز و همچنین، مقادیر سفارش بیش از حد شناسایی شود (کنترل‌های C2 و C3).

- هنگامی که درخواست خرید توسط مدیر پشتیبانی تأیید شد، او یک عطف برای سفارش خرید در برنامه پشتیبانی ایجاد می‌کند (Control C4).
- سپس، خریدار یک نسخه از سفارش خرید را برای تأمین‌کننده می‌فرستد. همه سفارش‌های خرید برای شناسایی هرگونه سفارش خرید غیرمجاز و همچنین ،مقادیر بیش از حد سفارش به صورت ماهانه بررسی می‌شوند (کنترل‌های C5 و C6).



شکل۱- نمودگر فرآیند سفارش خرید

آزمون شناخت: [برای مستند کردن یک مورد از ورودی تا تبدیل به خروجی می‌توانید از یک نمودگر همان‌طور که در مثال زیر نشان داده شده است، استفاده کنید]

درخواست خرید شماره ۴۵۷۶ به‌عنوان نمونه انتخابی (نسخه پیوست) در تاریخ ۱۳۹۷/۰۲/۲۴ ایجاد شد. حسابرس مقادیر درخواست شده را با سطح موجودی مورد نیاز در سیستم در آن روز مقایسه و دو مقدار را با هم مطابقت می‌کند. اقلام موجود در درخواست شماره ۴۵۷۶ در سفارش خرید شماره ۷۸۷۴ به شرکت مشهد منظور شده بود. کالاها در تاریخ ۲۴ خرداد ۱۳۹۷ تحویل و برگه دریافت کالای شماره ۸۹۰ در سیستم صادر شد.

نکات حاصل از آزمون شناخت سیستم

مقادیر موجود در برگ دریافت کالا با سفارش خرید و مقادیر موجود در برگه ارسال کالا مطابقت نداشت، اما سیستم این استثناء را در نظر نگرفت.

تهدید (چه چیزی می‌تواند در فرآیند فرعی اشتباه باشد)	احتمال تحقق تهدید (یعنی احتمال بسیار بعید، بعید، محتمل، بسیار محتمل)	اثر[2] برآوردی تهدید بر تحقق (یعنی تأثیر کم، متوسط، زیاد و بسیار زیاد)	شدت ریسک یعنی رتبه کلی ریسک (پایین، متوسط، بالا و خیلی بالا).	رویه‌های کنترل ریسک موجود[2]	اثربخشی کنترل‌ها (مؤثر، غیر مؤثر)	کنترل‌های بازدارنده[1]	رتبه‌بندی ریسک کلی با در نظر گرفتن کنترل‌های بازدارنده (پایین، متوسط، بالا و خیلی بالا).
درخواست اقلامی که از پیش در انبار موجود است یا اقلامی که مورد نیاز نیست.	بسیار محتمل	زیاد	بسیار زیاد	تفکیک وظایف (کارمند پشتیبانی به‌جای مدیر پشتیبانی، درخواست ورودی اصلی را دریافت می‌کند)- کنترل C1	اثربخش		بالا
درخواست‌های تأیید نشده	بعید	زیاد	کم	همه درخواست‌ها را به‌صورت ماهانه بررسی کنید تا هرگونه درخواست غیرمجاز را شناسایی کنید- کنترل C2 و C3	اثربخش		پایین
اقلام دریافتی با اقلام سفارش خرید مطابقت ندارد	کم	زیاد	زیاد	سفارش خرید ایجاد شده از طریق سیستم- کنترل C4	غیراثربخش	تطبیق ماهانه سفارش خریدها و درخواست‌های خرید- کنترل C5 و C6	بالا

پروفایل ریسک کلی فرآیند

نتیجه کلی	
بالا	رتبه‌بندی کلی ریسک فرآیند سیستم‌های فرعی (پایین، متوسط، بالا و بسیار بالا)
آری	انتخاب فرآیند برای آزمون حسابرسی (آری/ خیر)

۱. اگر بتوان تاثیر ارزش برآوردی را یافت، تأثیر پیش‌بینی‌شده را به صورت ریالی در اینجا نشان می‌دهد.

۲. روش کنترل ریسک موجود برای کاهش ریسک را مستند کنید.

۳. اگر کنترل‌های موجود، غیر مؤثر تلقی شوند، حسابرس فناوری اطلاعات، کنترل‌های بازدارنده را بررسی می‌کند.

صورت ریز / فهرست ریسک

نام سازمان مورد رسیدگی:
پایان دوره مالی:

هدف
این کاربرگ، مرجع خلاصه‌ای از همه ریسک‌های ذاتی شناسایی شده طی مراحل شناسایی و شرح سیستم سازمان می‌باشد. همچنین، برخورد حسابرس با ریسک ذاتی را خلاصه‌سازی می‌کند.

الزامات خاص استانداردهای استفاده شده در این کاربرگ

استانداردهای بین‌المللی دیوان محاسبات بخش ۲۰۰	❖ شناخت سازمان مورد رسیدگی.
استانداردهای بین‌المللی دیوان محاسبات بخش ۵۳۰۰	❖ دستورالعمل‌های مربوط به حسابرسی فناوری اطلاعات.
استانداردهای بین‌المللی دیوان محاسبات بخش ۱۳۱۵	❖ شناسایی و ارزیابی ریسک‌های تحریف بااهمیت از طریق شناخت سازمان و محیط آن.
استانداردهای بین‌المللی دیوان محاسبات بخش ۱۳۳۰	❖ برخورد حسابرس با ریسک‌های ارزیابی شده.
انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۱۲۰۱	❖ برنامه‌ریزی قرارداد.
انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۱۲۰۲	❖ ارزیابی ریسک.
انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۱۲۰۴	❖ سطح اهمیت.

یادداشت‌های راهنما

فهرست ریسک باید به‌عنوان مرجعی برای همه ریسک‌های ذاتی شناسایی شده در مرحله شناخت سازمان و تهیه شرح سیستم عمل کند. همچنین، برخوردهای مناسب با این ریسک‌ها را مستند می‌کند. پس از تکمیل این کاربرگ می‌توان از آن به‌عنوان مبنای حسابرسی سال آتی استفاده کرد.

یادداشت راهنمای شماره ۱

اجزای حسابرسی

سیستم اطلاعاتی، اجزای مختلفی دارد که مبنایی برای تقسیم وظایف بین اعضای گروه می‌باشد. این اجزا، مثلاً، شامل شبکه، پایگاه داده، برنامه‌ها یا اجزای فرعی برنامه و غیره است.

یادداشت راهنمای شماره ۲

مستندسازی ریسک ذاتی

ریسک(های) ذاتی شناسایی شده برای اجزای مختلف را مستند کنید. از اشاره به ریسک‌های کنترلی خودداری کنید. نمونه‌هایی از ریسک‌هایی که می‌توان آنها را در نظر گرفت شامل موارد زیر است:

۱) ممکن است شبکه در دسترس افراد غیرمجاز قرار گیرد (محرمانگی).

۲) منابع شبکه ممکن است گم یا دزدیده شوند (در دسترس بودن).

۳) ریسک ذاتی مرتبط با سیستم‌های عامل بدون کنترل‌های مناسب معمولاً زیاد است؛ زیرا، تغییرات یا حتی افشای داده‌ها یا برنامه‌ها از طریق ضعف‌های امنیتی سیستم عامل می‌تواند به اطلاعات مدیریتی نادرست یا زیان رقابتی منجر گردد.

از گنجانده شدن همه ریسک‌های شناسایی شده در کاربرگ شناخت سازمان در اینجا اطمینان یابید.

یادداشت راهنمای شماره ۳

ریسک فراگیر

ریسک فراگیر ریسکی است که به کل محیط سیستم‌های اطلاعاتی مربوط می‌شود و، بنابراین، بر تمام سیستم‌های اطلاعاتی تأثیر می‌گذارد.

یادداشت راهنمای شماره ۴

رتبه‌بندی ریسک کلی

این ستون، رتبه‌بندی کلی ریسک را که از شناخت سازمان، شرح سیستم، بازخورد پشتیبانی حسابرسی فناوری اطلاعات یا هر کاربرگ دیگری که ریسک در آن شناسایی شده است، مستند می‌کند.

یادداشت راهنمای شماره ۵

ریسک‌های عمده

آیا ریسک، عمده است. به خاطر داشته باشید که همه ریسک‌ها ریسک عمده(بالا) نیستند.

ضعف بااهمیت– نارسایی یا ترکیبی از کاستی‌ها در کنترل داخلی به‌گونه‌ای که به‌احتمال معقول نتواند یک تحریف بااهمیت را به‌موقع کشف یا از رخداد آن پیشگیری کند.

ضعف کنترل داخلی زمانی بااهمیت تلقی می‌شود که نبود کنترل، به عدم اطمینان معقول از تحقق هدف کنترلی منجر شود. ضعف طبقه‌بندی شده بااهمیت به این معناست که:

- کنترل‌ها وجود ندارد و/ یا استفاده نمی‌شوند و/ یا نارسا هستند.
- احتمال افزایش اثر وجود دارد.

بین اهمیت و سطح ریسک پذیرفتنی حسابرسی سیستم‌های اطلاعاتی یا متخصصان اطمینان بخشی یک رابطه معکوس وجود دارد؛ یعنی، هر چه سطح اهمیت بالاتر باشد، پذیرش ریسک حسابرسی کمتر است و برعکس.

نارسایی عمده– کمبود یا ترکیبی از نارسایی‌ها در کنترل داخلی، که شدت کمتری نسبت به یک ضعف بااهمیت دارد، اما به‌اندازه کافی مهم است که قابل توجه ارکان نظارتی باشد.

توجه: ضعف بااهمیت، یک نارسایی عمده یا ترکیبی از نارسایی‌های عمده است که در اثر احتمال بیش از بعید رخداد و رویداد(های) نامطلوبی حاصل می‌شود که پیشگیری یا کشف نشده است.

یادداشت راهنمای شماره ۶

اتکا به کنترل‌ها

این ستون پس از انجام آزمون کنترل‌ها و بر اساس میزان اتکای نهایی بر کنترل‌های مربوط به هر جزء حسابرسی، تکمیل می‌گردد.

یادداشت راهنمای شماره ۷

عطف به کاربرگ شناسایی ریسک

عطف به کاربرگ کسب شناخت از سازمان، شرح سیستم، صورتجلسه پشتیبانی حسابرسی فناوری اطلاعات یا هر کاربرگ دیگری که ریسک در آن شناسایی شده است.

یادداشت راهنمای شماره ۸

عطف به کاربرگ‌های برخورد حسابرس با ریسک

ایجاد ارتباط بین کاربرگ‌هایی که حاوی برخورد با ریسک است.

فهرست ریسک

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

فهرست ریسک باید به‌عنوان مرجعی از همه ریسک‌های ذاتی شناسایی شده در مرحله شناخت سازمان و تهیه شرح سیستم، عمل کند. همچنین، برخوردهای مناسب برای رسیدگی به این ریسک‌ها را مستند می‌کند. پس از تکمیل این کاربرگ می‌توان از آن به‌عنوان مبنای حسابرسی سال آتی استفاده کرد.

اجزای حسابرسی	شرح ریسک ذاتی	آیا ریسک فراگیر است (آری/ خیر)	رتبه‌بندی ریسک کلی (بالا، متوسط، پایین)	آیا نارسایی در کنترل‌های داخلی، عمده است	اتکا بر کنترل‌ها	عطف به کاربرگ شناسایی ریسک	عطف به کاربرگ برخورد حسابرس با ریسک
یادداشت راهنمای ۱	یادداشت راهنمای ۲	یادداشت راهنمای ۳	یادداشت راهنمای ۴	یادداشت راهنمای ۵	یادداشت راهنمای ۶	یادداشت راهنمای ۷	یادداشت راهنمای ۸

ارزیابی ریسک و برخورد با آن از دیدگاه گزاره‌ها (ادعاها)

سازمان مورد رسیدگی:

دوره مالی:

هدف

هدف این کاربرگ، آسان‌سازی ارزیابی ریسک‌ها و کنترل‌های مرتبط و طراحی برنامه‌های حسابرسی مناسب برای برخورد با این ریسک‌ها است.

الزامات خاص استانداردهای استفاده شده در این کاربرگ

استانداردهای بین‌المللی دیوان محاسبات بخش ۲۰۰	❖ شناخت سازمان مورد رسیدگی.
استانداردهای بین‌المللی دیوان محاسبات بخش ۵۳۰۰	❖ دستورالعمل‌های مربوط به حسابرسی فناوری اطلاعات.
استانداردهای بین‌المللی دیوان محاسبات بخش ۱۳۱۵	❖ شناسایی و ارزیابی ریسک‌های تحریف بااهمیت از طریق شناخت سازمان و محیط آن.
استانداردهای بین‌المللی دیوان محاسبات بخش ۱۳۳۰	❖ برخورد حسابرس با ریسک‌های ارزیابی شده.
انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۱۲۰۱	❖ برنامه‌ریزی قرارداد.
انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۱۲۰۲	❖ ارزیابی ریسک.
انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۱۲۰۴	❖ سطح اهمیت.

یادداشت‌های راهنما

هدف، ارزیابی ریسک شناسایی شده و تعیین برخورد با آن ریسک بر اساس سطح ریسک و اهمیت هرگونه نارسایی کنترلی شناسایی شده، است. این کاربرگ برای هر جزء بااهمیت یا گروهی از اجزای با ریسک‌های مشابه، تکمیل می‌شود.

یادداشت راهنمای شماره ۱

اجزای قابل حسابرسی

سیستم اطلاعاتی اجزای مختلفی دارد (کنترل‌های عمومی و کاربردی) که بر اساس آن‌ها، وظایف به اعضای گروه اختصاص داده می‌شود. سیستم اطلاعاتی ممکن است شامل شبکه، پایگاه داده، برنامه‌ها یا اجزای فرعی برنامه و غیره باشند.

اجزای قابل حسابرسی، زمینه‌هایی هستند که در ابتدا با ریسک بالا یا متوسط شناسایی شده‌اند. حسابرس با این کاربرگ تصمیم خواهد گرفت که برای کدام‌یک از این زمینه‌ها، اقدامات حسابرسی بیشتری انجام دهد.

یادداشت راهنمای شماره ۲

مستندسازی ریسک‌های ذاتی

ریسک(های) ذاتی شناسایی شده برای اجزای مختلف قابل حسابرسی را مستندسازی کنید. از گنجاندن ریسک کنترلی خودداری کنید. نمونه‌هایی از ریسک‌ها به شرح زیر است:

۱. شبکه ممکن است توسط افراد غیرمجاز ارزیابی شود (محرمانگی).

۲. منابع شبکه ممکن است گم یا دزدیده شوند (در دسترس بودن).

۳. ریسک ذاتی مرتبط با سیستم‌های عامل بدون کنترل‌های مناسب معمولاً بالا است؛ زیرا، تغییرات یا حتی افشای داده‌ها یا برنامه‌ها از طریق ضعف‌های امنیتی سیستم عامل می‌تواند به اطلاعات مدیریتی نادرست یا زیان رقابتی منجر گردد.

این ستون، از فهرست ریسک، تکمیل شده است.

یادداشت راهنمای شماره ۳

گزاره‌ها

گزاره‌های مربوط به اجزای حسابرسی شده را مستند کنید. در صورت نیاز از گزاره‌های زیر انتخاب کنید:

ادعا	تعریف
محرمانگی	حفظ محدودیت‌های مجاز در دسترسی و افشا، شامل ابزارهای حفاظت از حریم خصوصی و مالکیت اطلاعات
یکپارچگی	اطلاعات، شواهد و سایر داده‌های دریافتی از منابع قابل‌اعتماد و قابل اتکا بدست می‌آیند؛ برای مثال، سوابق تغییر درخواست شده توسط متخصصان، از مدیر انطباق، یک منبع قابل اعتماد و قابل اتکا در شرکت دریافت می‌شود.
در دسترس بودن	اطلاعات، شواهد و سایر داده‌های مورد نیاز برای کار حسابرسی، موجود و در دسترس است؛ برای مثال، سوابق تغییر درخواست شده، وجود دارد و در برنامه ردیابی مدیریت تغییر، در دسترس است.

یادداشت راهنمای شماره ۴

گزاره‌ها

گزاره‌های مربوط به اجزای حسابرسی شده را مستند کنید. در صورت نیاز از گزاره‌های زیر انتخاب کنید:

گزاره‌های حسابرسی مالی	تعریف
رخداد/ وجود	معاملات و رویدادهایی که ثبت شده‌اند، رخ داده‌اند و به سازمان مربوط می‌باشد و دارایی‌ها، بدهی‌ها و حقوق صاحبان سهام وجود دارند.
کامل بودن	همه معاملات، رویدادها، دارایی‌ها و بدهی‌هایی که باید ثبت می‌شد، ثبت شده‌اند.

گزاره‌های حسابرسی مالی	تعریف
درستی و ارزشیابی	مبالغ و سایر داده‌های مربوط به تراکنش‌های ثبت‌شده، رویدادها و هرگونه تعدیل، به‌گونه‌ای مناسب و با مقادیر درست ثبت شده‌اند.
انقطاع زمانی	معاملات و رویدادها در دوره حسابداری درست ثبت شده است.
طبقه‌بندی	معاملات و رویدادها در حساب‌های درست ثبت شده است.
حقوق و تعهدات	معامله یا رویداد مربوط به مخارج، نشان‌دهنده تحصیل اقتصادی و همچنین، استفاده کارآمد و اثربخش از منابع است.
ارائه و افشا	همه موارد افشای مورد نیاز مطابق با چارچوب گزارشگری مالی انجام شده است و در صورت‌های مالی به‌گونه‌ای مناسب، ارائه و به‌طور مطلوب افشا شده است.
سودمندی	معامله یا رویداد مربوط به دارایی‌ها، موجودی‌ها و بدهی‌ها نشان‌دهنده تحصیل اقتصادی و همچنین، استفاده کارآمد و اثربخش از منابع است.
رعایت	اطلاعات، شواهد و سایر داده‌ها مطابق با سازمان، مقررات نظارتی یا سایر مقررات قابل اجرا، ثبت شده است، برای مثال، فیلدهای مورد نیاز، براساس پیش‌بینی‌های قابل اجرا، در سوابق تغییر برنامه ردیابی مدیریت تغییر وجود دارد.

حسابرس باید گزاره‌های انتخاب شده برای کار حسابرسی را بررسی و از موارد زیر اطمینان حاصل کند:

کافی: کافی بودن برای برآورده کردن هدف کار حسابرسی، شامل ارائه نظر یا نتیجه‌گیری در مورد مربوط بودن موضوع به دامنه کار.

معتبر: موضوع در دامنه کار، قابل آزمون است.

مربوط: ارتباط مستقیم با موضوع دامنه دارد و به تحقق هدف انجام کار حسابرسی کمک می‌کند.

یادداشت راهنمای شماره ۵

اجزای حسابرسی مالی

ریسک‌ها بنا بر ماهیت، کنترل‌های عمومی را بیشتر تهدید می‌کنند؛ برای مثال. شبکه، بر بیش از یک مؤلفه مالی اثر می‌گذارد. اجزای متأثر از ریسک مورد بررسی در این ستون فهرست می‌شود.

یادداشت راهنمای شماره ۶

هدف‌های کنترلی

هدف‌های کنترلی به‌عنوان یک راهنما در ارزیابی سطح اهمیت عمل می‌کنند. نبود کنترل زمانی بااهمیت تلقی می‌شود که نبودن آن، به عدم اطمینان معقول از تحقق هدف کنترلی منجر شود.

یادداشت راهنمای شماره ۷

آزمون شناخت سیستم را برای شناسایی کنترل‌های مرتبط با ریسک‌های مربوط، اجرا کنید.

با انجام آزمون شناخت، کنترل‌های داخلی موجود برای برخورد با ریسک‌ها را شناسایی کنید. کنترل‌های کلیدی که ریسک را کاهش می‌دهند و ارجاع به موارد قانونی را، در صورت وجود، در نظر بگیرید.

یادداشت راهنمای شماره ۸

نتیجه‌گیری درباره اثربخش بودن طراحی کنترل‌های داخلی برای برخورد با ریسک

با ارزیابی کنترل‌های داخلی که با آزمون شناخت سیستم شناسایی می‌شوند باید از قضاوت حرفه‌ای برای تعیین اثربخش بودن یا نبودن طراحی کنترل‌های داخلی استفاده کنید؛ یعنی، آیا آنها به‌طور مؤثر با ریسک‌های شناسایی شده برخورد می‌کنند؟

پاسخ(های) این ستون بر اساس قضاوت حرفه‌ای است. شما باید درباره بودن یا نبودن کنترل‌هایی برای برخورد با ریسک‌ها و عملکرد آنها تصمیم‌گیری کنید.

یادداشت راهنمای شماره ۹

کنترل بازدارنده

اگر کنترلی غیر اثربخش ارزیابی شود، حسابرس سیستم‌های اطلاعاتی باید هرگونه کنترل بازدارنده را، در صورت وجود، شناسایی کند. روش‌های کنترلی که برای پیشگیری از ریسک وجود دارد باید فهرست شوند.

یادداشت راهنمای شماره ۱۰

سطح اتکای برنامه‌ریزی شده بر کنترل‌ها را مشخص کنید.

چنانچه نتوان بر کنترل‌ها اتکا کرد، رویکرد کاملاً مبتنی بر آزمون‌های محتوا اجرا می‌شود. از سوی دیگر، زمانی که بتوان بر کنترل‌ها اتکا کرد، آزمون کنترل‌ها برای ارزیابی اجرای مؤثر کنترل‌های داخلی انجام می‌شود. این ارزیابی می‌تواند به انجام آزمون‌های محتوای محدود یا گسترده منجر شود.

یادداشت راهنمای شماره ۱۱

حسابرس سیستم‌های اطلاعاتی باید ریسک کلی فرآیند فرعی را پس از ارزیابی همه ریسک‌های مربوط به آن فرآیند فرعی، تعیین کند. این، مبنایی است برای تعیین حسابرسی شدن یا نشدن فرآیند فرعی.

یادداشت راهنمای شماره ۱۲

ارتباط با برنامه حسابرسی

بر اساس ارزیابی خود از ریسک، در مورد استفاده از آزمون‌های رعایت یا آزمون‌های محتوا تصمیم‌گیری کنید. گروه حسابرسی باید هنگام انتخاب یک زمینه قابل حسابرسی، درباره آستانه‌ی ریسک ارزیابی شده‌ای تصمیم‌گیری کند که باید با آن برخورد شود.

افزون بر این، دیگر اجزا(ی حسابرسی) می‌تواند بر اساس هدف‌های تعیین شده یا درخواست (سازمان) برای حسابرسی انتخاب شوند.

ارزیابی ریسک

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

هدف این کاربرگ، ارزیابی ریسک شناسایی شده و تعیین برخورد با ریسک بر اساس سطح ریسک و اهمیت هر یک از ضعف‌های کنترلی شناسایی شده، است.

ارزیابی ریسک									برخورد با ریسک					
اجزای/ فرآیندهای قابل حسابرسی	مستندسازی ریسک‌های ذاتی	گزاره سیستم اطلاعاتی	گزاره مالی	اجزای حسابرسی مالی	هدف‌های کنترلی	فهرست کنترل‌های داخلی بازدارنده ریسک	نتیجه‌گیری حسابرس در مورد اثربخشی کنترل‌های داخلی بازدارنده ریسک‌ها	کنترل بازدارنده	سطح برنامه‌ریزی شده اتکا بر کنترل‌ها [بالا، متوسط، کم/ نبود]	رتبه‌بندی کلی ریسک فرآیندهای فرعی	انتخاب فرآیندهای فرعی برای اجرای حسابرسی	عطف به برنامه حسابرسی (آزمون کنترل‌ها و/یا آزمون‌های محتوا)
یادداشت راهنمای ۱	یادداشت راهنمای ۲	یادداشت راهنمای ۳	یادداشت راهنمای ۴	یادداشت راهنمای ۵	یادداشت راهنمای ۶	یادداشت راهنمای ۷	یادداشت راهنمای ۸	یادداشت راهنمای ۹	یادداشت راهنمای ۱۰	یادداشت راهنمای ۱۱	یادداشت راهنمای ۱۲	یادداشت راهنمای ۱۲
برنامه	صورت‌حساب‌های تأمین‌کنندگان تکراری است که به بیش از واقع بودن مانده‌حساب‌های پرداختنی منجر می‌شود.	یکپارچگی	رخداد		برنامه، کنترل‌های پیشگیرانه‌ای دارد که از ورود داده‌های نادرست پیشگیری می‌کند		خیر		کم/ نبود			مورد ندارد
پایگاه داده	تغییر داده‌ها	یکپارچگی	رخداد/ کامل بودن		پایگاه داده به‌طور مؤثری برای محافظت از تغییر داده‌ها پیکربندی شده است		آری		بالا			عطف

مستندسازی نشست گروه کاری

نام سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه:		سطح ۳			
تاریخ:					

تاریخ نشست: [تاریخ را بنویسید]

نام اعضای گروه مشارکت‌کننده در نشست

نام	رتبه شغلی

موضوع گفتگو	تصمیم‌گیری / یادداشت‌ها
مشخصات قرارداد (برای مثال: چارچوب گزارشگری مالی و قانونی؛ محل‌های جغرافیایی سازمان مورد رسیدگی).	
هدف‌های گزارشگری (برای مثال: مهلت‌های زمانی؛ تاریخ‌های مهم: گزارشگری نهایی؛ گفتگو با مدیریت).	
عوامل مهمی که نقاط تمرکز برای کارگروه حسابرسی را تعیین می‌کنند (یعنی: اهمیت، ارزیابی محیط کنترلی، حوزه‌های خاص با ریسک تحریف بااهمیت و سایر یافته‌ها).	
نشانه‌هایی برای اصلاح طرح کلی حسابرسی.	

موضوع گفتگو	تصمیم‌گیری / یادداشت‌ها
نوع و ماهیت، زمان‌بندی و میزان سمت‌وسو و نظارت بر اعضای گروه حسابرسی و بررسی سطح استفاده از فناوری اطلاعات توسط کارکنان حسابرسی.	
پشتیبانی از یک حسابرسی دیگر (عضوی از آن گروه حسابرسی دیگر نیز باید در نشست حضور یابد)	
آیا هدف‌های حسابرسی دیگرِ مورد پشتیبانی، توسط حسابرسان فناوری اطلاعات درک شده است؟	
آیا اجزای حسابرسی یا گزاره‌های مورد ارزیابی، شناخته شده‌اند؟	
زمینه‌های بررسی برای گروه حسابرسی قانونی، حسابرسی عملکرد و حسابرسی رعایت یا سایر گروه‌های حسابرسی.	
ارائه یافته‌ها و پیامدهای سایر حسابرسی‌ها باید مورد گفتگو و توافق قرار گیرد.	
تقلب	
اینکه چگونه و چرا صورت‌های مالی می‌تواند مستعد تقلب باشد، در گرو شناسایی موارد زیر است: ❖ زمینه‌ها یا اجزای حسابرسی شده صورت‌های مالی ممکن است مستعد تقلب باشند. ❖ مدیریت چگونه می‌تواند مرتکب گزارشگری مالی متقلبانه شود و آن را پنهان کند. ❖ چگونه دارایی‌های سازمان می‌تواند مورد سوءاستفاده قرار گیرد. ❖ شرایطی که می‌تواند نشان‌دهنده مدیریت سود باشد و رویه‌هایی که در صورت مواجه‌شدن با آنها ممکن است نشان‌دهنده احتمال تقلب باشد.	

موضوع گفتگو	تصمیم‌گیری / یادداشت‌ها
در نظر گرفتن عوامل شناخته شده‌ای که: ❖ انگیزه یا فشار برای مدیریت یا دیگران برای ارتکاب به تقلب را ایجاد می‌کند؛ ❖ فرصت انجام کلاهبرداری را پدید می‌آورد؛ و ❖ فرهنگ یا محیطی را که مدیریت یا دیگران را قادر می‌سازد ارتکاب به تقلب را توجیه کنند، شناسایی کنید.	
توجه به دخالت مدیریت در نظارت بر کارکنان با دسترسی به وجوه نقد یا سایر دارایی‌های مستعد سوءاستفاده.	
توجه به هرگونه تغییر غیرعادی یا توضیح داده نشده در رفتار یا سبک زندگی مدیریت یا کارکنان که مورد توجه گروه حسابرسی قرار گرفته است.	
سایر ملاحظات حسابرسی شامل: ❖ حفظ وضعیت ذهنی مناسب در مورد احتمال تحریف بااهمیت ناشی از تقلب در طول اجرای حسابرسی. ❖ چگونه یک جزء غیرقابل پیش‌بینی در اجرای روش‌های حسابرسی گنجانده می‌شود. ❖ کدام روش‌های حسابرسی برای کشف تقلب، مؤثرتر از سایر روش‌هاست. ❖ ادعاهای تقلب که مورد توجه حسابرس قرار گرفته است. ❖ ریسک زیرِ پا گذاری کنترل‌ها توسط مدیریت.	
سایر موارد مطرح شده و توافق‌های بدست آمده را بنویسید:	

دستورالعمل دریافتی از حسابرسی مالی

زمینه‌های حسابرسی	هدف یا گزاره (ادعا)	آنچه که حسابرسی فناوری اطلاعات باید رسیدگی کند	

طرح کلی حسابرسی

سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

۱. کلیات

۱-۱. هدف طرح کلی حسابرسی، مستندسازی دامنه، زمان‌بندی و سمت‌وسوی انجام حسابرسی است.

۲. شرایط قرارداد

۲-۱. گزارشگری در مورد سیستم‌های اطلاعاتی

هدف‌های کلی حسابرسی عبارتند از:

- .....
- .....
- .....

۲-۲. انتظارات سازمان مورد رسیدگی

ما از لزوم آگاهی‌رسانی به مدیریت درباره ضعف‌های کنترل داخلی شناسایی شده در جریان انجام حسابرسی، اثر آن و هرگونه انحراف از رویه‌های حسابداری، آگاه هستیم. برای برقراری ارتباط، راه‌هایی را به شرح جزئیات در بخش ۳-۲ زیر فراهم کرده‌ایم. درباره پرسش‌ها و نامه‌های مدیریت در حضور [مدیران تعیین‌شده را نام ببرید برای مثال، خزانه‌دار/ مدیر مالی] در نشست‌های برنامه‌ریزی شده گفتگو خواهد شد. در صورت نیاز به برگزاری نشست‌های بیشتر لطفاً با مدیر گروه حسابرسی[نام مدیر را بنویسید] تماس بگیرید.

۳-۲. گزارشگری

بازخوردهایی را در مورد پیشرفت حسابرسی و نقاط ضعف شناسایی شده در جریان حسابرسی به‌طور منظم هفتگی یا ماهانه به ارکان راهبری ارائه خواهیم داد. انتظار داریم که در یک بازه زمانی معقول، پاسخ‌های مکتوب به ارتباطات برقرار شده را دریافت کنیم.

بازخورد برنامه‌ریزی شده در مورد حسابرسی انتظار می‌رود در قالب زیر ارائه شود:

- ❖ پرس‌وجوهای حسابرسی
- ❖ نامه(های) میان‌دوره‌ای مدیریت
- ❖ نامه مدیریت پایانی
- ❖ پیش‌نویس گزارش

همچنین، نشست‌هایی را به شرح زیر برنامه‌ریزی کرده‌ایم.

[تاریخ برنامه‌ریزی شده و همچنین، اسناد مورد گفتگو را بنویسید].

۱) .....

۲) نامه مدیریت پایانی [در صورت وجود، تاریخ برنامه‌ریزی شده را مشخص کنید].

۳) پیش‌نویس گزارش [در صورت وجود، تاریخ‌های برنامه‌ریزی شده را بنویسید].

۴. رویکرد حسابرسی برنامه‌ریزی شده

۴-۱. نوع و ماهیت و میزان رسیدگی

بر اساس ارزیابی ریسک، جدول زیر ریسک(های) تحریف بااهمیت شناسایی شده و همچنین، برخورد مناسب مطابق تشخیص ما برای آن ریسک‌ها را نشان می‌دهد.

ریسک‌ها	ریسک فراگیر	ارتباط با گزاره‌ها	ارتباط با اجزای حسابرسی	برخوردها
[ارائه توضیحات]	[آری/خیر]	[آری/خیر]	[نام بردن جزء حسابرسی]	[برخوردها را بنویسید]

۴-۲. دامنه حسابرسی

با نگرش به شناخت از سازمان (به شناخت سازمان عطف دهید) و ریسک ذاتی به شرح بند۱-۴ بالا، دامنه حسابرسی شامل موارد زیر خواهد بود:

فهرست زمینه‌های زیر پوشش را بنویسید.

۴-۳. آزمون‌ها و رویه‌های حسابرسی

در این حسابرسی از ترکیبی از آزمون کنترل‌ها و آزمون‌های محتوا استفاده خواهد شد. آزمون کنترل‌ها با گردآوری شواهد آزمون میزان رعایت روش‌های کنترل داخلی توسط سازمان سروکار دارد، حال‌آنکه آزمون محتوا، با به دست آوردن شواهد حسابرسی درباره کامل بودن، درستی یا وجود فعالیت‌ها یا معاملات در طول دوره مورد حسابرسی، یکپارچگی پردازش واقعی را آزمون می‌کند.

۴-۴. بازدیدهای منطقه‌ای برنامه‌ریزی شده

[در صورت وجود، بازدیدهای منطقه‌ای برنامه‌ریزی شده و دلیل انتخاب مکان‌های مربوط را مشخص کنید].

۴-۵. مدت‌زمان حسابرسی

خلاصه‌ای از مدت‌زمان حسابرسی را بنویسید.

۵. منابع حسابرسی

این بخش، منابع مورد نیاز برای حسابرسی را بیان می‌کند:

۵-۱. اعضای گروه حسابرسی

گروه حسابرسی متشکل از: .....

۵-۲. استفاده از کارشناسان و/یا متخصصان

[در صورت لزوم، کارشناسان برون‌سازمانی را که در حسابرسی مشارکت خواهند داشت، نام ببرید همراه با بیان میزان و ضرورت مشارکت آنان، برای مثال: کارشناسان مالیاتی و غیره].

[مشخص کنید که آیا از حسابرسان دادگاهی یا عملکرد استفاده خواهد شد و میزان مشارکت آنان].

۵-۳. بودجه مالی

هزینه برآوردی این قرارداد ..... ریال به شرح پیوست X است.

پیوست ۵:
اجرای حسابرسی

ارزیابی ریسک و برخورد مربوط به گزاره‌ها

سازمان مورد رسیدگی:

پایان دوره:

هدف

هدف این کاربرگ، راهنمایی حسابرس فناوری اطلاعات در انجام قرارداد حسابرسی است و اجرای قرارداد حسابرسی، نقش‌ها و مسئولیت‌ها، گردآوری شواهد، مستندسازی کار انجام شده و تدوین یافته‌ها و نتیجه‌گیری‌ها را شامل می‌شود.

الزامات خاص استانداردهای استفاده شده در این کاربرگ

استانداردهای بین‌المللی دیوان محاسبات بخش ۵۳۰۰	❖ دستورالعمل‌های مربوط به حسابرسی فناوری اطلاعات
انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۱۲۰۴	❖ سطح اهمیت
انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۱۲۰۳	❖ عملکرد و نظارت

یادداشت‌های راهنما

یادداشت راهنمای ۱ استانداردها و دستورالعمل‌های انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۳-۲۲، بند ۱-۱-۲	عطف به کاربرگ
جزء حسابرسی: حسابرس فناوری اطلاعات باید بتواند زمینه‌های قابل حسابرسی (اجزای حسابرسی) را در جریان ارزیابی ریسک سازمان و محیط آن، شناسایی کند.	

یادداشت راهنمای ۱ استانداردها و دستورالعمل‌های انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۳-۲۲، بند ۲-۱-۲	عطف به کاربرگ
معیارها: حسابرس فناوری اطلاعات باید هدف کنترلی/ عطفی را مستند کند که شواهد حسابرسی با آن مقایسه می‌شود. نمونه‌هایی را می‌توان از استانداردها، سیاست‌ها، رویه‌ها، مقررات یا الزامات به دست آورد.	

یادداشت راهنمای ۴ استانداردها و دستورالعمل‌های انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۳-۲۲، بندهای ۱-۴-۲، ۲-۴-۲، ۳-۴-۲ و ۴-۴-۲	عطف به کاربرگ
آزمون کنترل‌ها/ آزمون‌های محتوا: حسابرس فناوری اطلاعات باید بر اساس ارزیابی خود از ریسک، شواهد کافی و مناسب برای اظهار نظر یا پشتیبانی از نتایج و دستیابی به هدف‌های حسابرسی را به‌دست آورد. حسابرس فناوری اطلاعات می‌تواند از ترکیبی از روش‌های حسابرسی برای آزمون کنترل‌ها و یا آزمون‌های محتوا استفاده کند. کارکنان حرفه‌ای در صورت شناسایی انحراف از انتظارات باید دلایل انحراف را از مدیریت بپرسند. اگر توضیح مدیریت کافی باشد، کارکنان حرفه‌ای باید با نگرش به قضاوت حرفه‌ای، انتظارات خود را تعدیل و شواهد و اطلاعات را دوباره تحلیل کنند.	

یادداشت راهنمای ۵ استانداردها و دستورالعمل‌های انجمن کنترل و حسابرسی سیستم‌های اطلاعاتی بخش ۳-۲۲، بندهای ۴-۴-۲، ۵-۴-۲، ۶-۴-۲ و ۷-۴-۲	عطف به کاربرگ
نتیجه آزمون‌ها/ یافته‌ها: حسابرس فناوری اطلاعات باید منبع و ماهیت شواهد به‌دست آمده را برای ارزیابی قابلیت اطمینان آن‌ها و نیاز به رسیدگی بیشتر، در نظر بگیرد. کارکنان حرفه‌ای باید تجزیه‌وتحلیل و تفسیر مناسبی را انجام دهند تا از یافته‌های حسابرسی پشتیبانی و نوع نتیجه‌گیری مشخص شود. انحرافات قابل توجه از انتظارات باید به یافته‌هایی بیانجامد و به مدیریت اجرایی ابلاغ شود.	

یادداشت راهنمای ۶ استانداردها و دستورالعمل‌های انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۳-۲۲، بندهای ۱-۵-۲، ۱-۶-۲ و ۴	عطف به کاربرگ
نتیجه‌گیری/ نکات نامه مدیریت (MLP): حسابرس فناوری اطلاعات باید مستندات کافی، مناسب و مرتبط را برای پوشش کل فرآیند آماده کند. نتیجه‌گیری و پیشنهادها باید بر این اساس در اینجا ثبت شود.	

یادداشت راهنمای ۷ استانداردها و دستورالعمل‌های انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۳-۲۲، بند ۲-۵-۳	عطف به کاربرگ
آزمون‌های حسابرسی پیشنهادی بیشتر: آزمون‌های حسابرسی پیشنهادی بیشتر، رویکرد یا زمینه‌های مربوط به حسابرس مالی را مستند کنید. این اطلاعات طبق شرایط مندرج در صورتجلسه نشست فناوری اطلاعات، به حسابرس مالی یا حسابرسان دیگر تحویل می‌شود.	

برنامه حسابرسی

سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

عناصر (اجزای) حسابرسی

هدف حسابرسی	معیارها	گزاره‌های مالی/ جزء مالی تحت تأثیر	هدف کنترل فناوری اطلاعات	آزمون‌های حسابرسی	نتیجه آزمون حسابرسی	نتیجه‌گیری/ نکات نامه مدیریت	آزمون‌های حسابرسی پیشنهادی بیشتر، رویکرد یا زمینه تمرکز حسابرسی مالی	عطف (شواهد حسابرسی یا کار انجام شده)
راهنمای ۲	راهنمای ۲			راهنمای ۴	راهنمای ۵	راهنمای ۶	راهنمای ۷	

استفاده از کارِ حسابرسِ دیگر

سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

گام نخست

شناسایی اجزای بااهمیت سیستم‌های اطلاعاتی / فناوری اطلاعات حسابرسی شده توسط حسابرس دیگر	نام حسابرس دیگر مسئول حسابرسی آن اجزاء	مبلغ (در صورت امکان)

گام دوم

صلاحیت حرفه‌ای حسابرس دیگر را بررسی کنید.

با گفتگو با حسابرس دیگر و هر شخص ثالث مرتبط، موارد زیر را بررسی کنید:

جنبه‌های مورد نظر	آری / خیر	منبع اطلاعات / عطف کاربرگ
حسابرس دیگر عضو یک انجمن حرفه‌ای، مانند انجمن حسابرسان سیستم‌های اطلاعاتی است.		
حسابرس دیگر به موسسه حسابرسی معتبر دیگری وابستگی دارد.		
حسابرس دیگر صلاحیت و تجربه حسابرسی مرتبط در این زمینه حسابرسی را دارد.		
حسابرس دیگر از استانداردهای حسابرسی برای انجام حسابرسی استفاده می‌کند.		

با در نظر گرفتن موارد بالا، آیا صلاحیت حرفه‌ای حسابرس دیگر کافی است؟ .....

آری	خیر

اگر پاسخ آری است، با گام سوم فرآیند را ادامه دهید و روش‌های زیر را اجرا کنید، تا اطمینان حاصل کنید که می‌توان بر کار حسابرس دیگر اتکا کرد. اگر پاسخ خیر است، نتیجه‌گیری (مرحله ۴) را بنویسید که نمی‌توان بر کار حسابرس دیگر اتکا کرد و محدودیت در دامنه را اعلام کنید یا اجرای روش‌های حسابرسی، ازجمله اجرای دوباره کار حسابرس دیگر را مورد توجه قرار دهید.

گام سوم

کارهای انجام شده توسط حسابرس دیگر را بررسی کنید.

	نوع و ماهیت و میزان روش‌های حسابرسی	ملاحظات	عطف به کاربرگ
۱	در مرحله برنامه‌ریزی حسابرسی، به حسابرس دیگر اطلاع دهید و تأییدیه موارد زیر را دریافت کنید: ❖ الزامات استقلال مربوط به اجزا و سازمان مورد حسابرسی؛ ❖ رویکرد حسابرسی حسابرس دیگر، شامل ریسک‌های قابل‌توجه شناسایی شده و پوشش کلیه هدف‌های حسابرسی؛ و ❖ الزامات قانونی، حسابداری، حسابرسی و گزارشگری.		
۲	موارد زیر را به حسابرس دیگر اطلاع دهید: ❖ مواردی که می‌خواهید از کار و گزارش حسابرس دیگر استفاده کنید؛ ❖ زمینه‌هایی که نیاز به توجه ویژه دارند؛ و ❖ جدول زمانی برای تکمیل حسابرسی.		

	نوع و ماهیت و میزان روش‌های حسابرسی	ملاحظات	عطف به کاربرگ
۳	خلاصه(ی) کتبی، جدول‌های پشتیبان و کاربرگ حسابرس دیگر را دریافت و بررسی کنید. کارهای انجام شده را بررسی و تحقق هدف‌های حسابرسی و پوشش کافی ریسک‌های عمده را بررسی کنید.		
۴	مناسب بودن شواهد حسابرسی را برای همه یافته‌های بااهمیت بررسی کنید.		
۵	در مواردی که به‌طور جزئی یا کلی نمی‌توان به‌طور منطقی بر کار انجام شده اتکا کرد، هرگونه آزمون‌های (بیشتر) اجزای سیستم اطلاعاتی و فناوری اطلاعات که توسط حسابرس دیگر حسابرسی شده است را مستند کنید.		

گام چهارم

نتیجه‌گیری

- **بر اساس روش‌های انجام شده، نتیجه‌گیری برای هدف حسابرسی را ارائه کنید.**
- **نتیجه‌گیری را در اینجا مستند کنید:**
  - **برای مثال می‌توان به کار حسابرس دیگر تکیه کرد. بااین‌حال روش(های) بیشتر برای کامل بودن کار حسابرسی انجام خواهد شد.**

یا

  - **نمی‌توان بر کار حسابرس دیگر اتکا کرد - این ممکن است به محدودیت در دامنه رسیدگی منجر شود یا اجرای رویه‌های بیشتر ضرورت یابد.**

خلاصه‌ای از یافته‌های بااهمیت حسابرس دیگر

یافته بااهمیت	آیا این یافته برای صورت‌های مالی سازمان به‌طور کلی بااهمیت است؟ آری/ خیر	عطف به استثناهای مطرح شده
هر یافته مهم حسابرس دیگر را خلاصه کنید.		استثناهای یافته‌های مربوط به اجزای حسابرسی را بنویسید.

استفاده از کارِ کارشناس

سازمان مورد رسیدگی:		**بررسی‌کننده:**	**نام**	**رتبه**	**تاریخ**
پایان دوره:		**سطح ۱**			
تهیه‌کننده:		**سطح ۲**			
رتبه شغلی :		**سطح ۳**			
تاریخ:					

گام نخست: تعیین نیاز به استفاده از کار کارشناس

تعیین زمینه‌های نیازمند استفاده از کارِ کارشناس	مبلغ / مانده / جزء مشخص	آیا مبلغ / مانده / جزء مشخص، بااهمیت است؟ آری / خیر	آیا دیگر شواهد حسابرسی برای پوشش مناسب هدف‌های حسابرسی کافی هستند؟ آری / خیر	آیا کار یک کارشناس لازم است؟ آری / خیر
برای مثال: ❖ بررسی دادگاهی پایگاه داده ❖ داده‌کاوی، ❖ اظهارنظر حقوقی، ❖ کار انجام شده بر روی قراردادهای در جریان.	(شواهد تحصیل / استخراج از پایگاه داده)	(آری، برای قابل قبول بودن شواهد در دادگاه)	(خیر)	اگر مانـده یا جزء مشخص، بااهمیت است و انجام رویه جایگزین دیگری برای کسب اطمینان، انجام‌پذیر نیست، پاسخ این، آری خواهد بود.

نام کارشناسان

[نام کارشناسان را بنویسید]

.....

گام‌های ۲ و ۳ برای کار انجام شده توسط هر کارشناس باید تکمیل شوند.

گام‌های دوم و سوم: روش‌های حسابرسی

نوع و ماهیت و میزان روش‌های حسابرسی	سوابق کار انجام شده	عطف به کاربرگ
صلاحیت حرفه‌ای و واقع‌بینی کارشناس با گفتگو با مدیریت سازمان مورد رسیدگی، کارشناس یا هر شخص ثالث مربوط دیگر، تأییدیه موارد زیر را دریافت کنید: ❖ گواهی حرفه‌ای یا پروانه کار یا عضویت در یک نهاد حرفه‌ای مناسب. ❖ تجربه و شهرت در زمینه مربوط به شواهد حسابرسی لازم		
با گفتگو با مدیریت سازمان مورد رسیدگی و کارشناس، از استقلال کارشناس با توجه به موارد زیر اطمینان کسب کنید: ❖ استخدام توسط سازمان مورد رسیدگی. ❖ هرگونه ارتباط با سازمان مورد رسیدگی؛ برای مثال، وابستگی مالی به سازمان یا سرمایه‌گذاری در آن.		
اگر صلاحیت یا واقع‌بینی کارشناس، نگرانی ایجاد می‌کند: ❖ درباره نگرانی‌های خود با مدیریت گفتگو کنید. ❖ برای اطمینان از قابلیت اتکا، یکپارچگی و مناسب بودن کار کارشناس، هرگونه اقدام جبرانی توسط مدیریت را در نظر بگیرید.		
دامنه کار کارشناس با نگرش به دستورالعمل ارائه شده به کارشناس توسط سازمان/ حسابرس (در صورت امکان) یا با گفتگو با کارشناس، شواهد حسابرسی کافی و مناسب درباره کافی بودن دامنه کار کارشناس برای هدف حسابرسی را بدست آورید و موارد زیر را بررسی و مستند کنید: ❖ هدف‌ها و دامنه کار کارشناس. ❖ رئوس کلی موارد خاصی که حسابرس انتظار دارد گزارش کارشناس، آنها را پوشش دهد.		

نوع و ماهیت و میزان روش‌های حسابرسی	سوابق کار انجام شده	عطف به کاربرگ
❖ استفاده مورد نظر حسابرس از کار کارشناس. ❖ حدود دسترسی کارشناس به سوابق و پرونده‌های لازم. ❖ تشریح روابط کارشناس با سازمان، در صورت وجود. ❖ محرمانگی اطلاعات سازمان. ❖ اطلاعات مربوط به مفروضات و روش‌های مورد نظر برای استفاده توسط کارشناس و مطابقت آنها با مفروضات و روش‌های استفاده شده در دوره‌های پیش.		
ارزیابی کار کارشناس گزاره‌های صورت‌های مالی که استفاده از کار کارشناس به‌عنوان یکی از شواهد حسابرسی برای آن‌ها ضرورت دارد را مستندسازی کنید.		
قابلیت اتکای منشأ داده‌های مورد استفاده کارشناس را ارزیابی کنید: ❖ درباره روش‌های کارشناس برای اطمینان یافتن از کامل بودن، مربوط بودن و قابلیت اتکای منشأ داده‌ها پرس و جو کنید. ❖ داده‌های استفاده شده توسط کارشناس را بررسی یا آزمون کنید.		
شناختی از مفروضات و شیوه‌های مورد استفاده بدست آورید و مناسب و منطقی بودن آن‌ها را براساس دانش حسابرس از کسب و کار و نتایج دیگر روش‌های حسابرسی، بررسی و مستند کنید.		
هرگونه روش‌های حسابرسی دیگر مربوط به کار کارشناس را در اینجا بنویسید.		

گام چهارم: درباره کار کارشناس نتیجه‌گیری کنید

[آیا کار کارشناس، شواهد حسابرسی کافی و مناسبی را فراهم می‌کند؟

اگر خیر، روش‌های بیشتری که لازم است اجرا شوند را بنویسید.]

_____

_____

_____

نوع و ماهیت و میزان روش‌های حسابرسی	سوابق کار انجام شده	عطف به کاربرگ
هنگامی که کار کارشناس، شواهد حسابرسی کافی و مناسبی را **فراهم نمی‌کند** یا نتایج آن با سایر شواهد حسابرسی هم‌راستا نیست: ❖ موضوع را با گفتگو با مدیریت و کارشناس حل کنید؛ ❖ روش‌های حسابرسی بیشتری را که ممکن است شامل استفاده از کارشناس دیگر باشد، اجرا کنید؛ یا ❖ یک استثناء در مورد ناکافی بودن شواهد حسابرسی را مطرح و اظهارنظر حسابرس را به‌طور مناسبی تعدیل کنید.		

گام پنجم: تعدیل گزارش

نوع و ماهیت و دامنه رویه‌های حسابرسی	سوابق کار انجام شده	عطف به کاربرگ
هنگامی‌که گزارش تعدیل شده حسابرس با عطف به کار کارشناس (برای مثال، معرفی کارشناس و حدود رسیدگی او) صادر می‌شود باید اجازه وی برای افشا دریافت شود.		
چنانچه کارشناس اجازه افشای نام خود را ندهد، نظر مشاور حقوقی را دریافت کنید.		

کاربرگ بازخورد پشتیبانی حسابرسی فناوری اطلاعات

سازمان مورد رسیدگی:		**بررسی‌کننده:**	**نام**	**رتبه شغلی**	**تاریخ**
پایان دوره:		**سطح ۱**			
تهیه‌کننده:		**سطح ۲**			
رتبه شغلی:		**سطح ۳**			
تاریخ:					

[این کاربرگ در پایان حسابرسی و برای روشن کردن یافته‌های کلیدی برای حسابرسان مالی یا سایر حسابرسان درخواست‌کننده پشتیبانی فناوری اطلاعات، تکمیل می‌شود.

عطف دهی به صورتجلسه نشست پشتیبانی فناوری اطلاعات باید انجام شود].

الف	ب	پ	ت	ث	ج
درخواست حسابرسی مالی (یا سایر اجزای ارزیابی شده توسط حسابرسان IT)	**قابلیت اتکای کنترل‌های اصلی فناوری اطلاعات مرتبط با این جزء**	**یافته‌های اصلی فناوری اطلاعات**	**آثار مترتب بر حسابرسی مالی**	**پیشنهاد آزمون‌های حسابرسی بیشتر، رویکرد یا زمینه‌هایی برای تمرکز حسابرسی مالی**	**عطف**

نتیجه‌گیری کلی درباره قابلیت اتکای سیستم‌های اطلاعاتی
بالا / متوسط / پایین

نام و امضای مدیر حسابرسی فناوری اطلاعات	**تاریخ**

نام و امضای مدیر حسابرسی مالی	**تاریخ**

پیوست ۶ : گزارشگری

نامه مدیریت

سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:		تاریخ:			

حسابرسی یک بخش انجام شده توسط حسابرس دیوان

گیرنده: [نام و سِمَت مسئول حسابداری]
تاریخ :

آقا/ خانم محترم

نامه مدیریت برای حسابرسی دوره [دوره مربوط را بنویسید]

حسابرسی فناوری اطلاعات [نام سازمان مورد رسیدگی و/یا نام سیستم(های) اطلاعاتی را بنویسید]. در انطباق با الزامات قانونی ... [به مواد قانونی مربوط عطف دهید] ... انجام شده و نامه مدیریت به شرح زیر است.

هدف از این نامه، جلب توجه مدیریت به یافته‌های به‌دست آمده در جریان حسابرسی است.

دامنه و هدف حسابرسی

هدف‌های حسابرسی عبارتند از:

- بررسی کنترل‌های سیستم‌های فناوری اطلاعات برای کسب اطمینان از کفایت و اثربخشی آنها.
- ارزیابی سیستم‌ها و فرآیندهای موجود که منابع اطلاعاتی را ایمن و در دسترس می‌کنند.
- ارزیابی عملکرد سیستم‌های اطلاعاتی و امنیت آنها.
- رسیدگی به فرآیند و روش‌های تدوین سیستم.
- تعیین منطبق بودن یا نبودن فرآیندهای مدیریت اطلاعات با قوانین، خط‌مشی‌ها و استانداردهای مربوط.

اثربخشی کنترل‌های کلیدی در سیستم‌های حساس کسب و کار [نام سازمان مورد حسابرسی] و در محیط کنترل فناوری اطلاعات آن در این حسابرسی مورد ارزیابی قرار گرفت. فرآیندهای کلیدی زیر مورد پوشش قرار گرفت:

[زمینه‌های اصلی را بیان کنید]. **برای مثال**:

- راهبری فناوری اطلاعات
- مدیریت امنیت
- مدیریت تغییر برنامه
- کنترل‌های دسترسی فیزیکی
- کنترل‌های زیست‌محیطی
- تداوم خدمات فناوری اطلاعات
- کنترل دسترسی منطقی

رویکرد حسابرسی

حسابرسی، مطابق با استانداردهای بین‌المللی دیوان‌های محاسبات (ISSAIs) و همچنین، استانداردهای انجمن حسابرسان سیستم‌های اطلاعاتی (ISACA) و بهترین شیوه عمل‌های صنعت انجام شد. این حسابرسی، برای کسب اطمینان معقول از قابلیت اتکای سیستم‌های اطلاعاتی، برنامه‌ریزی و انجام شد.

ترتیبات موجود سیستم‌های اطلاعاتی، در... [تاریخ انجام رسیدگی] ... توسط گروهی از حسابرسان حرفه‌ای فناوری اطلاعات مورد رسیدگی قرار گرفت.

نتیجه‌گیری کلی

[خلاصه‌ای از یافته‌ها را بنویسید]

محدودیت‌ها در دامنه و مسئولیت

[هرگونه محدودیتی که در اجرای حسابرسی با آن مواجه شده‌اید را بنویسید]

سپاسگزاری

از حسن نیت و کمک‌های ارائه شده توسط کارکنان ... [نام سازمان مورد حسابرسی] ... در جریان حسابرسی سپاسگزاری می‌کنیم.

با احترام

اداره حسابرسی

تفصیل یافته‌ها و پیشنهادها

معیـار/ هدف کنترلی/ طبقه‌بندی یافتـه‌ها

هدف کنترلی، قانون، استاندارد سیستم‌های اطلاعاتی که به‌طور کامل رعایت نشده یا اصلاً رعایت نشده است.

شرایط/ شرح یافته

مشاهدات حسابرس یا اقدامات سازمان درباره معیارها/ هدف کنترلی/ طبقه‌بندی یافته‌ها.

دلایل

چرا آن ناهنجاری رخ داد؟ توضیح لازم درباره علت رخ دادن این ناهنجاری.

ریسک/ پیامد

این اتفاق چه تأثیری بر سازمان یا کشور دارد.

پیشنهاد

[پیشنهادها باید شامل کنترل‌های پیشگیرانه، کشف کننده و اصلاحی باشد].

پاسخ مدیریت؛ و نظرات حسابرس

پاسخ کتبی مدیریت به یافته‌ها. حسابرس می‌تواند در صورت لزوم، در واکنش به پاسخ آنان، نظرات بیشتری ارائه دهد.

نامه مدیریت ... [نام سازمان مورد حسابرسی] ... برای سال منتهی به ... [تاریخ مربوط].

تأییدیه مدیران

سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

[به استاندارد انجمن حسابرسان سیستم‌های اطلاعاتی بخش ۲۴۰۱ مراجعه کنید].

به : مدیرکل حسابرسی **تاریخ: .....**

این تأییدیه در ارتباط با حسابرسی سیستم‌های اطلاعاتی ... [نام سازمان مورد حسابرسی]... برای دوره منتهی به [تاریخ پایان سال مالی] ... برای اظهار نظر درباره انطباق کنترل‌های داخلی فناوری اطلاعات، از همه جنبه‌های بااهمیت، با الزامات گزارشگری مربوط ارائه می‌گردد.

ما مسئولیت خود را برای ایجاد و حفظ کنترل‌های داخلی مناسب و مؤثر، شامل سیستم‌های کنترل‌های داخلی حسابداری و کنترل‌های اداری مربوط به فعالیت‌های عملیاتی و سیستم‌های اطلاعاتی مورد رسیدگی و انجام اقدامات لازم، برای شناسایی همه قوانین و مقررات حاکم بر سیستم‌های اطلاعاتی، می‌پذیریم.

سوابق و تراکنش‌های سیستم‌های اطلاعاتی

۱. همه سوابق سیستم‌های اطلاعاتی و مستندات پشتیبان و همه صورت‌جلسات نشست‌ها را در اختیار شما قرار داده‌ایم و هیچ اطلاعاتی از این دست را ناگفته نگذاشته‌ایم.

۲. همه اطلاعات درخواستی مرتبط با هدف‌های حسابرسی، در دسترس گروه حسابرسی قرار گرفته است:

- سوابق، داده‌های مرتبط، فایل‌های الکترونیکی و گزارش‌ها.
- سیاست‌ها و روش‌ها.
- کارکنان مربوط.
- نتایج حسابرسی داخلی و مستقل از بررسی‌های اجمالی و ارزیابی‌های سیستم‌های اطلاعاتی.

سایر موارد

۱. پس از پایان عملیات اجرایی حسابرسی، هیچ رویدادی(هایی) رخ نداده یا موضوع‌هایی کشف نشده است که اثر بااهمیتی بر کار حسابرسی داشته باشد.

۲. با هیچ‌گونه تقلب یا مورد مشکوک به تقلب، سوء جریان و اعمال غیرقانونی مرتبط با زمینه مورد رسیدگی، در ارتباط با مدیریت و کارکنان مسئول کنترل‌های داخلی که پیشتر افشا نشده است، برخورد نکرده‌ایم.

۳. از هیچ‌گونه ادعایی مبنی بر تقلب یا مشکوک به تقلب، سوء جریان و اعمال غیرقانونی مؤثر بر زمینه مورد حسابرسی، اعلام شده توسط کارکنان، مشتریان، پیمانکاران یا سایرین که پیشتر افشا نشده باشد، برخورد نکرده‌ایم.

۴. مسئولیت طراحی و اجرای برنامه‌ها و کنترل‌های لازم برای پیشگیری و کشف تقلب، سوء جریان و اعمال غیرقانونی را می‌پذیریم.

نام و امضای مسئول حسابداری	تاریخ

گزارش حسابرس

سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

گیرنده: [نام، سِمَت و نشانی مسئول حسابداری]

تاریخ:

خانم / آقای گرامی

گزارش حسابرسان مستقل در مورد حسابرسی [نام سازمان مورد حسابرسی و/یا نام سیستم(های) اطلاعاتی].

من [نام سیستم اطلاعاتی] [نام سازمان مورد حسابرسی] را مطابق با [بیان قوانین مربوط] حسابرسی کرده‌ام.

مسئولیت مدیریت

مدیریت، مسئول استقرار و حفظ کنترل‌های داخلی لازم برای اطمینان از محرمانگی، یکپارچگی و در دسترس بودن سیستم‌های اطلاعاتی و داده‌های پردازش شده توسط این سیستم‌ها و همچنین، ارائه اطمینان معقول از رعایت سیاست‌ها و روش‌های تجویز شده، شامل پیشگیری از خطاها و سوء جریان‌ها، از جمله تقلب و اعمال غیرقانونی می‌باشد.

مسئولیت حسابرس

مسئولیت حسابرس، اظهارنظر درباره اثربخشی طراحی و/ یا عملکرد روش‌های کنترلی سیستم‌های اطلاعاتی بر اساس حسابرسی انجام شده، است. حسابرسی، مطابق با استانداردهای بین‌المللی حسابرسی دیوان محاسبات عمومی انجام شده است. این استانداردها مستلزم رعایت الزامات اخلاقی و برنامه‌ریزی و اجرای حسابرسی برای اطمینان یافتن از کارایی، صرفه اقتصادی و اثربخشی سیستم فناوری اطلاعات و کنترل‌های مرتبط با آن یا شناسایی موارد نقض آن‌ها است.

حسابرسی شامل اجرای روش‌هایی برای به دست آوردن شواهد حسابرسی کافی و مناسب در مورد اثربخشی کنترل‌های سیستم اطلاعاتی است. روش‌های انتخاب شده به قضاوت حسابرس ازجمله ارزیابی ریسک‌های سیستم اطلاعاتی بستگی دارد.
من بر این باورم که شواهد حسابرسی بدست آمده، برای ارائه نظر حسابرسی، کافی و مناسب است.

اظهار نظر [برای ارائه نظر موافق (مقبول) انتخاب شود]

افراد حرفه‌ای زمانی باید نظر موافق (مقبول) ارائه کنند که به این نتیجه می‌رسند که از همه جنبه‌های بااهمیت، به نظر من، طراحی و/ یا اجرای روش‌های کنترلی مرتبط با [نام سیستم اطلاعاتی/جزء سیستم اطلاعاتی مورد حسابرسی] [نام حسابرسی شونده] از همه جنبه‌های بااهمیت، در [تاریخ انجام حسابرسی]، در انطباق با [معیارهای مورد استفاده] به‌گونه‌ای مؤثر انجام شده‌اند.

مبانی اظهار نظر مشروط/ مخالف (مردود)/ عدم اظهارنظر [برای ارائه نظر تعدیل شده انتخاب شود]

[شامل بند(های) حسابرسی که به اظهارنظر مشروط / مخالف (مردود) / یا عدم اظهارنظر منجر شده است. برای اظهارنظر موافق (مقبول)، این بند نوشته نمی‌شود].

اظهار نظر مشروط [برای ارائه نظر مشروط انتخاب شود]

به نظر من، به‌استثنای آثار احتمالی موضوع توضیح داده شده در بند مبانی اظهارنظر مشروط، طراحی و/ یا اجرای روش‌های کنترلی مربوط به [سیستم اطلاعاتی/ جزء سیستم اطلاعاتی مورد حسابرسی] [نام حسابرسی شونده] در [تاریخ انجام حسابرسی]، از همه جنبه‌های بااهمیت، مطابق با [معیارهای مورد استفاده] به‌گونه‌ای مؤثر انجام شده‌اند.

اظهار نظر مخالف (مردود) [برای ارائه نظر مخالف(مردود) انتخاب شود]

به نظر من، به دلیل اهمیت موضوعی که در بند مبنای اظهارنظر مخالف (مردود) بیان شده است، طراحی و/ یا اجرای روش‌های کنترلی مربوط به [سیستم اطلاعاتی/ جزء سیستم اطلاعاتی مورد حسابرسی] [نام حسابرسی شونده] در [تاریخ انجام حسابرسی]، از همه جنبه‌های بااهمیت، مطابق با [معیارهای مورد استفاده] به‌گونه‌ای مؤثر انجام نشده است.

عدم اظهار نظر [برای عدم اظهار نظر انتخاب شود]

به‌دلیل اهمیت موضوع های بیان شده در بند مبنای عدم اظهارنظر، من نتوانستم شواهد حسابرسی کافی و مناسب را برای ارائه مبنایی برای اظهارنظر حسابرسی به‌دست آورم. بر این اساس، من درباره [سیستم اطلاعاتی/ جزء سیستم اطلاعاتی مورد حسابرسی] نظری اظهار نمی‌کنم.

سایر مسئولیت‌های گزارشگری

[سایر الزامات قانونی و مقرراتی. شکل و محتوای این بخش از گزارش حسابرس با توجه به ماهیت سایر مسئولیت‌های گزارشگری حسابرس، متفاوت است].

[امضای حسابرس]

[تاریخ گزارش حسابرس]

[نشانی حسابرس]

تأییدیه مدیر حسابرسی

سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

نام بررسی‌کننده:

سِمَت بررسی‌کننده:

سطح مسئولیت بررسی در این حسابرسی [بررسی‌کننده سطح اول/ دوم/ سوم]

به این وسیله تأیید می‌کنم که:

۱. پیش از شروع عملیات اجرایی کار، طرح کلی حسابرسی و برنامه‌های حسابرسی را تکمیل و تأیید کرده‌ام یا درباره آنها با من مشورت شده است.

۲. من کار انجام شده توسط [بررسی‌کننده اول / دوم] در سطح پیش از من را بررسی کرده‌ام.

۳. من بر این باورم که رویکرد اجرا شده و تصمیمات گرفته شده در جریان حسابرسی، برحسب الزامات مربوط بوده است. نتیجه‌گیری‌های بدست آمده در کاربرگ‌ها، نامه مدیریت و پیش‌نویس گزارش حسابرس مطابق با یکدیگر است.

۴. من با نحوه انجام مشاوره‌های فنی موافق هستم.

۵. بررسی‌های کنترل کیفیت، مطابق با مفاد این راهنما انجام شده است.

بر اساس موارد یاد شده در بالا، به‌جز موارد زیر، با اظهارنظر ارائه شده حسابرس موافق هستم.

نظرات بررسی/ بازبینی کننده:

_____

_____

_____

پیشنهادهای اصلاحی بر گزارش حسابرس	دلیل (دلایل)

امضا:

[نام و سمت مربوط]

تاریخ

نکات قابل توجه در حسابرسی سال آتی

سازمان مورد رسیدگی:		بررسی‌کننده:	نام	رتبه شغلی	تاریخ
پایان دوره:		سطح ۱			
تهیه‌کننده:		سطح ۲			
رتبه شغلی:		سطح ۳			
تاریخ:					

ردیف	نکات قابل توجه	پیشنهادها	عطف به کاربرگ

واژه‌نامه

واژه‌نامه فارسی به انگلیسی

آ/ا

آزمون تخلیه	*Practice Evacuation*
آزمون رعایت کنترل‌ها	*Compliance Test of Controls*
آزمون شناخت سیستم	*System Walk-Through Test*
آزمون کنترل‌ها	*Test of Controls*
آزمون‌های محتوا	*Substantive Testing*
آیین رفتار حرفه‌ای انجمن حسابرسان سیستم‌های اطلاعاتی	*ISACA Code of Professional Ethics*
(انجمن) مدیران مالی بین‌المللی	*Financial Executives International (FEI)*
اجرای خشک	*Dry Running*
اخطار / اخطاریه	*Warning letter*
اسپرینت سی روزه	*Thirty Day Sprint*
اسپرینت	*Sprint*
استانداردهای بین‌المللی دیوان محاسبات	*International Standards of Supreme Audit Institutions*
استانداردهای پذیرفته شده بین‌المللی	*Internationally Accepted Standards*
استانداردهای حسابداری ملی	*National Accounting Standards*
اسکرام	*Scrum*
اسکرام روزانه	*Daily Scrum*
اصالت	*Authenticity*

واژه‌نامه فارسی به انگلیسی

اعتبارسنجی	*Validation*
اعتبارسنجی داده‌های ورودی	*Data Input Validation*
اقلام معوق	*Suspense Items*
الزامات اخلاقی	*Ethical Requirements*
امنیت (اطلاعات)	*Security*
امنیت فیزیکی و زیست‌محیطی	*Physical and Environmental Security*
انتقال الکترونیکی وجه (نقد)	*Electronic Funds Transfer (EFT)*
انجمن حسابداران رسمی آمریکا	*American Institute of Certified Public Accountants (AICPA)*
انجمن حسابداران مدیریت	*Institute of Management Accountants (IMA)*
انجمن حسابداری آمریکا	*American Accounting Association (AAA)*
انجمن حسابرسان داخلی	*Institute of Internal Auditors (IIA)*
انجمن حسابرسان سیستم‌های اطلاعاتی	*Information Systems Audit and Control Association (ISACA)*
انجمن صنعت ارتباطات از راه دور	*Telecommunication Industry Association (TIA)*
انجمن ملی استاندارد و فناوری	*National Institute of Standards and Technology (NIST)*
انجمن مهندسی نرم‌افزار	*Software Engineering Institute (SEI)*
انواع و دامنه حسابرسی‌های فناوری اطلاعات	*Types and Scope of IT Audits*

ب

بانک اطلاعاتی/ پایگاه داده	*Database/ Data Bank*
بدافزارها/ برنامه‌های مخرب	*Malicious Software / Programmes*
بررسی امنیت شبکه	*Network Security Review*
بررسی دوباره	*Duplicate Checks*
برنامه (طرح) حسابرسی	*Audit Plan*

واژه‌نامه فارسی به انگلیسی

برنامه حسابرسی	*Audit Programme*
برنامه رسیدگی	*Project plan*
برنامه زمانی بسته	*Timeboxed*
برنامه‌ریزی ارتباط با مشتری	*Customer Relationship Planning (CRP)*
برنامه‌ریزی بازیابی فاجعه	*Disaster Recovery Planning (DRP)*
برنامه‌ریزی تداوم کسب و کار	*Business Continuity Planning (BCP)*
برنامه‌ریزی منابع سازمانی	*Enterprise Resource Planning (ERP)*
برنامه‌نویسان سیستم	*System Programmers*
برنامه‌نویسان کاربردی	*Application Programmers*
برنامه‌های کاربردی	*Applications*
به ترتیب تاریخ	*Chronological*
به‌موقع بودن	*Timeliness*
بیانیه ریسک	*Risk Statement*
... به نحو مطلوب نشان می‌دهد	*Present Fairly …*
... به‌طور منصفانه نشان می‌دهد (گزارش حسابرس)	*Give a true and fair view of […]*

پ

پروژه تدوین سیستم‌های اطلاعاتی	*Information Systems (IS) Development Projects*
پشتیبانی از تصمیم‌گیری‌های تجاری	*Decision Support Systems*
پیدایش تراکنش	*Transaction Origination*
پیشنهاد/ درخواست تغییر	*Change Proposal/Request*
پیگرد (قانونی)	*Prosecution*

واژه‌نامه فارسی به انگلیسی

ت

تجزیه سنی	*Ageing*
تجزیه و تحلیل ورود کاربران	*User Log Analysis*
تحلیلگر سیستم	*Systems Analyst*
تشخیص شکاف‌ها	*Gap Detection*
تغییر غیرمجاز	*Unauthorised Modification*
تفکیک وظایف	*Segregation of Duties (SoD)*
تقلب	*Fraud*
تکنیک‌های حسابرسی به کمک رایانه	*Computer Assissted Audti Techniques (CAATs)*
توان آمایش	*Throughput*

ج

جرم جنایی	*Criminal Offence*
جریان از بالا به پایین	*Top Down Flow*
جزء جدایی‌ناپذیر	*Integral Part*
جمع دسته	*Batch Total*
جَوّ رأس سازمان	*Tone at the Top*

چ

چارچوب اطمینان‌بخش فناوری اطلاعات	*IT Assurance Framework (ITAF)*
چارچوب معماری اُوپِن گروپ	*Open Group Architecture Framework (TOGAF)*
چرخه عمر تدوین و توسعه سیستم	*System Development Life Cycle (SDLC)*

واژه‌نامه فارسی به انگلیسی

ح

حافظه اصلی	*Hard Drive*
حسابرس خبره سیستم‌های اطلاعاتی	*Certified Information System Auditor (CISA)*
حسابرس مالی (حسابرسی صورت‌های مالی)	*Financial Audit*
حسابرس مستقل	*External Auditor*
حسابرسی دادگاهی	*Forensic Audit*
حسابرسی رعایت	*Compliance Audit*
حسابرسی سیستم اطلاعاتی	*Information System Audit*
حسابرسی عملکرد	*Performance Audit*
حسابرسی قانونی	*Regularity Audit*
حسابرسی ویژه	*Specialised Audit*
حیاتی (بحرانی)	*Critieal*

خ

خطی و بیدرنگ (سیستم)	*Inline and in Real-Time*

د

داده‌های ایستا (کم تغییر)	*Standing Data*
داده‌های حساس	*Sensitive Data*
در دسترس بودن	*Availability*
دستگاه برق اضطراری	*Uninterruptible Power Supplies (UPS)*
دستورالعمل IDI	*INTOSAI Development Initiative (IDI)*
دستورالعمل حسابرسی و اطمینان‌بخشی ISACA	*ISACA IS Audit and Assurance Guideline 2205-Evidence*
دوره مرور زمان	*Timestamps*

واژه‌نامه فارسی به انگلیسی

دیسک‌گردان	*CD-ROM*

ر

رابط سیستم	*Interface to the System*
راهبری	*Governance*
راهبری و مدیریت فناوری اطلاعات	*Governance and Management of IT*
راه‌های اجرایی خودکار	*Automated Solutions Implemented*
رتبه‌بندی	*Impact Rating*
روش پیاده‌سازی سیستم	*System Implementation Method*
رویه برون سپاری	*Outsourcing Policy*
رویه‌های ارزیابی کارکنان	*Staff Assessment Policies*
رویه‌های پایان همکاری	*Termination Policies*
رویه‌های شناسایی و احراز هویت	*Identification and Authentication Mechanisms*
ریسک باقیمانده	*Residual Risk*
رییس دیوان محاسبات	*Auditor- General*

ز

زمینه‌ی حسابرسی	*Jurisdiction of Audit*
زنجیره عطف حسابرسی	*Audit Trail*
زیرساخت سیستم اطلاعاتی سازمان	*Entity's IS Infrastructure*

ژ

ژرفای رسیدگی‌ها	*Audit Scrutiny*

واژه‌نامه فارسی به انگلیسی

س

ساختار راهبری فناوری اطلاعات	*IT Governance Structure*
سازمان بین‌المللی استاندارد	*International Organization for Standardization (ISO)*
سازمان مورد رسیدگی	*Auditee*
سرریز حافظه موقت	*Buffer overflow*
سند راهبردی فناوری اطلاعات	*IT Strategy Document*
سوء جریان	*Irregularity*
سوابق حسابرسی	*Audit Logs*
سیستم اطلاعاتی مدیریت	*Management Information System*
سیستم اطلاعاتی یکپارچه مدیریت مالی	*Integrated Financial Management and Information System (IFMIS)*
سیستم بی‌درنگ	*Real-Time Systems*
سیستم پردازش دسته‌ای	*Batch Data Entry Systems*
سیستم پسین	*Back End*
سیستم پیشین	*Front End*
سیستم دسته‌ای	*Batch System*
سیستم عامل	*Operating System*
سیستم مدیریت بانک اطلاعاتی	*Database Management System (DBMS)*
سیستم معاملات پیوسته	*Continuous Transacting System*
سیستم‌های مالی آماده	*Off the Shelf Financial Packages*

ش

شاخص کلیدی عملکرد	*Key Performance Indicator*
شبکه گسترده	*Wide Area Network (WAN)*
شبکه محلی	*Local Area Network (LAN)*
شرح شغل	*Jobs Role*

واژه‌نامه فارسی به انگلیسی

ط

طرح تداوم کسب وکار	*Business Continuity Plan (BCP)*
طرح کلی حسابرسی	*Overall Audit Strategy*

ع

عطف‌گذاری کاربرگ‌ها	*Working Paper (W/p) Reference*

ف

فرایندهای تجاری اصلی	*Key Business Processes*
فناوری اطلاعات و ارتباطات	*Information and Communication Technology (ICT)*

ک

کارگروه حسابرسی فناوری اطلاعات	*Working Group on IT Audit (WGITA)*
کارگروه حسابرسی فناوری سیستم‌های اطلاعاتی	*Working Group on Information Technology Audit (WGITA)*
کاری که تنها یک‌بار انجام می‌شود	*Once off Job*
کاهش داده‌های اضافی	*Data Redundancy*
کتابخانه زیربنایی فناوری اطلاعات	*IT Infrastructure Library (ITIL)*
کدهای دستوری	*Scripts*
کمیته راهبری ساختار یافته	*Structured Steering Committee*
کمیته راهبری فناوری اطلاعات	*IT Steering Committee*
کنترل دسترسی	*Access Control*
کنترل‌های پیکربندی	*Configuration Controls*
کنترل‌های جبران کننده	*Compensating controls*
کنترل‌های جبرانی	*Mitigating Controls*

واژه‌نامه فارسی به انگلیسی

کنترل‌های دسترسی فیزیکی و منطقی	*Physical and Logical Access Controls*
کنترل‌های دسترسی منطقی	*Logical Access Control*
کنترل‌های عمومی	*General Controls*
کنترل‌های کاربردی	*Application Controls*
کوزو (کمیته سازمان‌های حمایت‌کننده کمیسیون تِرِدوی)	*Committee of Sponsoring Organisations of the Treadway Commission (COSO)*

گ

گزارش استثناها	*Exception Reporting*
گزارش گذشته‌نگر استثناها	*Retrospective batching exception*

م

ماژول پرداختنی‌ها	*Payables Module*
ماژول خرید	*Purchasing Module*
ماژول دفتر کل	*General Ledger Module*
ماژول مالی	*Financial Module*
مأمور امنیت فناوری اطلاعات	*IT Security Officer*
مجاز بودن	*Authorisation*
محاسبه فیلدهای مجازی	*Virtual Field Calculations*
محرمانگی	*Confidentiality*
مدل آبشاری	*Waterfall Model*
مدیر ارشد اطلاعات	*Chief Information Officer (CIO)*
مدیر امنیت (اطلاعات)	*Security Administrator*
مدیر بانک اطلاعاتی	*Database Administrator*
مدیر سیستم	*System Administrator*
مدیر سیستم عامل	*Operating System Administrator*
مدیر سیستم مدیریت داده	*Data Management System Administrator*
مدیر / معاون مالی	*Chief Financial Officer (CFO)*
مدیریت بحران امنیت اطلاعات	*Information Security Incident Management*

واژه‌نامه فارسی به انگلیسی

مرحله تدوین و توسعه	*Development stage*
مرحله تدوین و توسعه	*Stage of Development (SOD)*
مرکز امنیت اینترنت	*Centre for Internet Security (CIS)*
مرکز داده	*Data Centre*
مرکز کار	*Work Station*
منافع ذی‌نفعان	*Stakeholders Interest*
مواردی از یک Backlog که باید در یک اسپرینت انجام شود.	*Sprint Backlog*
موافقت‌نامه سطح خدمات	*Service Level Agreement (SLA)*
میانگین زمانی بین شکست‌ها	*Mean Time Between Failures (MTBF)*

ن

نقاط کلیدی کنترل‌های اصلی	*Key Critical Control Points*
نمودار سازمانی	*Organisational Chart*
نمونه کاربرگ‌ها	*Template Working Papers*
نمونه‌گیری	*Sampling*

و

واقع‌بینی	*Objectivity*

ه

هدف زمانی بازیابی	*Recovery Time Objective (RTO)*
هدف نقطه بازیابی	*Recovery Point Objective (RPO)*
هدف‌های کنترلی	*Control Objectives*
هدف‌های کنترلی اطلاعات و فناوری‌های مرتبط	*Control Objectives for Information and related Technology (COBiT)*
هیأت کنترل تغییـر	*Change Control Board (CCB)*

ی

یکپارچگی	*Integrity*

واژه‌نامه انگلیسی به فارسی

A

Access Control	کنترل دسترسی
Ageing	تجزیه سنی
American Accounting Association (AAA)	انجمن حسابداری آمریکا
American Institute of Certified Public Accountants (AICPA)	انجمن حسابداران رسمی آمریکا
Application Controls	کنترل‌های کاربردی
Application Programmers	برنامه‌نویسان کاربردی
Applications	برنامه‌های کاربردی
Audit Logs	سوابق حسابرسی
Audit Plan	برنامه (طرح) حسابرسی
Audit Programme	برنامه حسابرسی
Audit Scrutiny	ژرفای رسیدگی‌ها
Audit Trail	زنجیره عطف حسابرسی
Auditee	سازمان مورد رسیدگی
Auditor- General	رییس دیوان محاسبات
Authenticity	اصالت
Authorisation	مجاز بودن
Automated Solutions Implemented	راه‌های اجرایی خودکار
Availability	در دسترس بودن

B

Back End	سیستم پسین
Batch Data Entry Systems	سیستم پردازش دسته‌ای
Batch System	سیستم دسته‌ای
Batch Total	جمع دسته
Buffer overflow	سرریز حافظه موقت
Business Continuity Plan (BCP)	طرح تداوم کسب وکار
Business Continuity Planning (BCP)	برنامه‌ریزی تداوم کسب و کار

واژه‌نامه انگلیسی به فارسی

C

CD-ROM	**دیسک‌گردان**
Centre for Internet Security (CIS)	**مرکز امنیت اینترنت**
Certified Information System Auditor (CISA)	**حسابرس خبره سیستم‌های اطلاعاتی**
Change Control Board (CCB)	**هیأت کنترل تغییر**
Change Proposal/Request	**پیشنهاد/ درخواست تغییر**
Chief Financial Officer (CFO)	**مدیر / معاون مالی**
Chief Information Officer (CIO)	**مدیر ارشد اطلاعات**
Chronological	**به ترتیب تاریخ**
Committee of Sponsoring Organisations of the Treadway Commission (COSO)	**کوزو (کمیته سازمان‌های حمایت‌کننده کمیسیون تِرِدوی)**
Compensating controls	**کنترل‌های جبران کننده**
Compliance Audit	**حسابرسی رعایت**
Compliance Test of Controls	**آزمون رعایت کنترل‌ها**
Computer Assissted Audti Techniques (CAATs)	**تکنیک‌های حسابرسی به کمک رایانه**
Confidentiality	**محرمانگی**
Configuration Controls	**کنترل‌های پیکربندی**
Continuous Transacting System	**سیستم معاملات پیوسته**
Control Objectives	**هدف‌های کنترلی**
Control Objectives for Information and related Technology (COBiT)	**هدف‌های کنترلی اطلاعات و فناوری‌های مرتبط**
Criminal Offence	**جرم جنایی**
Critieal	**حیاتی (بحرانی)**
Customer Relationship Planning (CRP)	**برنامه‌ریزی ارتباط با مشتری**

واژه‌نامه انگلیسی به فارسی

D

Daily Scrum	اسکرام روزانه
Data Centre	مرکز داده
Data Input Validation	اعتبارسنجی داده‌های ورودی
Data Management System Administrator	مدیر سیستم مدیریت داده
Data Redundancy	کاهش داده‌های اضافی
Database Administrator	مدیر بانک اطلاعاتی
Database Management System (DBMS)	سیستم مدیریت بانک اطلاعاتی
Database/ Data Bank	بانک اطلاعاتی/ پایگاه داده
Decision Support Systems	پشتیبانی از تصمیم‌گیری‌های تجاری
Development stage	مرحله تدوین و توسعه
Disaster Recovery Planning (DRP)	برنامه‌ریزی بازیابی فاجعه
Dry Running	اجرای خشک
Duplicate Checks	بررسی دوباره

E

Electronic Funds Transfer (EFT)	انتقال الکترونیکی وجه (نقد)
Enterprise Resource Planning (ERP)	برنامه‌ریزی منابع سازمانی
Entity's IS Infrastructure	زیرساخت سیستم اطلاعاتی سازمان
Ethical Requirements	الزامات اخلاقی
Exception Reporting	گزارش استثناها
External Auditor	حسابرس مستقل

واژه‌نامه انگلیسی به فارسی

F

Financial Audit	حسابرس مالی (حسابرسی صورت‌های مالی)
Financial Executives International (FEI)	(انجمن) مدیران مالی بین‌المللی
Financial Module	ماژول مالی
Forensic Audit	حسابرسی دادگاهی
Fraud	تقلب
Front End	سیستم پیشین

G

Gap Detection	تشخیص شکاف‌ها
General Controls	کنترل‌های عمومی
General Ledger Module	ماژول دفتر کل
Give a true and fair view of […]	… به‌طور منصفانه نشان می‌دهد (گزارش حسابرس)
Governance	راهبری
Governance and Management of IT	راهبری و مدیریت فناوری اطلاعات

H

Hard Drive	حافظه اصلی

I

Identification and Authentication Mechanisms	رویه‌های شناسایی و احراز هویت
Impact Rating	رتبه‌بندی
Information and Communication Technology (ICT)	فناوری اطلاعات و ارتباطات
Information Security Incident Management	مدیریت بحران امنیت اطلاعات
Information System Audit	حسابرسی سیستم اطلاعاتی

واژه‌نامه انگلیسی به فارسی

Information Systems (IS) Development Projects	پروژه تدوین سیستم‌های اطلاعاتی
Information Systems Audit and Control Association (ISACA)	انجمن حسابرسان سیستم‌های اطلاعاتی
Inline and in Real-Time	حظی و بیدرنگ (سیستم)
Institute of Internal Auditors (IIA)	انجمن حسابرسان داخلی
Institute of Management Accountants (IMA)	انجمن حسابداران مدیریت
Integral Part	جزء جدایی‌ناپذیر
Integrated Financial Management and Information System (IFMIS)	سیستم اطلاعاتی یکپارچه مدیریت مالی
Integrity	یکپارچگی
Interface to the System	رابط سیستم
International Organization for Standardization (ISO)	سازمان بین‌المللی استاندارد
International Standards of Supreme Audit Institutions	استانداردهای بین‌المللی دیوان محاسبات
Internationally Accepted Standards	استانداردهای پذیرفته شده بین‌المللی
INTOSAI Development Initiative (IDI)	دستورالعمل IDI
Irregularity	سوء جریان
ISACA Code of Professional Ethics	آیین رفتار حرفه‌ای انجمن حسابرسان سیستم‌های اطلاعاتی
ISACA IS Audit and Assurance Guideline 2205-Evidence	دستورالعمل حسابرسی و اطمینان‌بخشی ISACA
IT Assurance Framework (ITAF)	چارچوب اطمینان‌بخش فناوری اطلاعات
IT Governance Structure	ساختار راهبری فناوری اطلاعات
IT Infrastructure Library (ITIL)	کتابخانه زیربنایی فناوری اطلاعات
IT Security Officer	مأمور امنیت فناوری اطلاعات
IT Steering Committee	کمیته راهبری فناوری اطلاعات
IT Strategy Document	سند راهبردی فناوری اطلاعات

واژه‌نامه انگلیسی به فارسی

J	
Jobs Role	شرح شغل
Jurisdiction of Audit	زمینه‌ی حسابرسی

K	
Key Business Processes	فرایندهای تجاری اصلی
Key Critical Control Points	نقاط کلیدی کنترل‌های اصلی
Key Performance Indicator	شاخص کلیدی عملکرد

L	
Local Area Network (LAN)	شبکه محلی
Logical Access Control	کنترل‌های دسترسی منطقی

M	
Malicious Software / Programmes	بد افزارها/ برنامه‌های مخرب
Management Information System	سیستم اطلاعاتی مدیریت
Mean Time Between Failures (MTBF)	میانگین زمانی بین شکست‌ها
Mitigating Controls	کنترل‌های جبرانی

N	
National Accounting Standards	استانداردهای حسابداری ملی
National Institute of Standards and Technology (NIST)	انجمن ملی استاندارد و فناوری
Network Security Review	بررسی امنیت شبکه

واژه‌نامه انگلیسی به فارسی

O

Objectivity	واقع‌بینی
Off the Shelf Financial Packages	سیستم‌های مالی آماده
Once off Job	کاری که تنها یک‌بار انجام می‌شود
Open Group Architecture Framework (TOGAF)	چارچوب معماری اُوپِن گروپ
Operating System	سیستم عامل
Operating System Administrator	مدیر سیستم عامل
Organisational Chart	نمودار سازمانی
Outsourcing Policy	رویه برون سپاری
Overall Audit Strategy	طرح کلی حسابرسی

P

Payables Module	ماژول پرداختنی‌ها
Performance Audit	حسابرسی عملکرد
Physical and Environmental Security	امنیت فیزیکی و زیست‌محیطی
Physical and Logical Access Controls	کنترل‌های دسترسی فیزیکی و منطقی
Practice Evacuation	آزمون تخلیه
Present Fairly …	… به نحو مطلوب نشان می‌دهد
Project plan	برنامه رسیدگی
Prosecution	پیگرد (قانونی)
Purchasing Module	ماژول خرید

واژه‌نامه انگلیسی به فارسی

R

Real-Time Systems	سیستم بی‌درنگ
Recovery Point Objective (RPO)	هدف نقطه بازیابی
Recovery Time Objective (RTO)	هدف زمانی بازیابی
Regularity Audit	حسابرسی قانونی
Residual Risk	ریسک باقیمانده
Retrospective batching exception	گزارش گذشته‌نگر استثناها
Risk Statement	بیانیه ریسک

S

Sampling	نمونه‌گیری
Scripts	کدهای دستوری
Scrum	اسکرام
Security	امنیت (اطلاعات)
Security Administrator	مدیر امنیت (اطلاعات)
Segregation of Duties (SoD)	تفکیک وظایف
Sensitive Data	داده‌های حساس
Service Level Agreement (SLA)	موافقت‌نامه سطح خدمات
Software Engineering Institute (SEI)	انجمن مهندسی نرم‌افزار
Specialised Audit	حسابرسی ویژه
Sprint	اسپرینت
Sprint Backlog	مواردی از یک Backlog که باید در یک اسپرینت انجام شود.
Staff Assessment Policies	رویه‌های ارزیابی کارکنان
Stage of Development (SOD)	مرحله تدوین و توسعه
Stakeholders Interest	منافع ذی‌نفعان
Standing Data	داده‌های ایستا (کم تغییر)

واژه‌نامه انگلیسی به فارسی

Structured Steering Committee	کمیته راهبری ساختار یافته
Substantive Testing	آزمون‌های محتوا
Suspense Items	اقلام معوق
System Administrator	مدیر سیستم
System Development Life Cycle (SDLC)	چرخه عمر توسعه سیستم
System Implementation Method	روش پیاده‌سازی سیستم
System Programmers	برنامه‌نویسان سیستم
System Walk-Through Test	آزمون شناخت سیستم
Systems Analyst	تحلیلگر سیستم

T

Telecommunication Industry Association (TIA)	انجمن صنعت ارتباطات از راه دور
Template Working Papers	نمونه کاربرگ‌ها
Termination Policies	رویه‌های پایان همکاری
Test of Controls	آزمون کنترل‌ها
Thirty Day Sprint	اسپرینت سی روزه
Throughput	توان آمایش
Timeboxed	برنامه زمانی بسته
Timeliness	به‌موقع بودن
Timestamps	دوره مرور زمان
Tone at the Top	جَوّ رأس سازمان
Top Down Flow	جریان از بالا به پایین
Transaction Origination	پیدایش تراکنش
Types and Scope of IT Audits	انواع و دامنه حسابرسی‌های فناوری اطلاعات

واژه‌نامه انگلیسی به فارسی

U

Unauthorised Modification	تغییر غیرمجاز
Uninterruptible Power Supplies (UPS).	دستگاه برق اضطراری
User Log Analysis	تجزیه و تحلیل ورود کاربران

V

Validation	اعتبارسنجی
Virtual Field Calculations	محاسبه فیلدهای مجازی

W

Warning letter	اخطار / اخطاریه
Waterfall Model	مدل آبشاری
Wide Area Network (WAN)	شبکه گسترده
Work Station	مرکز کار
Working Group on Information Technology Audit (WGITA)	کارگروه حسابرسی فناوری سیستم‌های اطلاعاتی
Working Group on IT Audit (WGITA)	کارگروه حسابرسی فناوری اطلاعات
Working Paper (W/p) Reference	عطف‌گذاری کاربرگ‌ها

منـابـع

1. AFROSAI-E regularity audit manual.
2. CISA Item Development Guide.
3. CISA Review Manual - 2011 & 2015.
4. COBIT 5- http://www.intosaiitaudit.org/intoit_articles/25_p30top35.pdf.
5. IFRS – reporting requirement on IT issues.
6. ISACA Audit Program: Business Continuity Management Audit/Assurance Program (Sep 2011).
7. ISACA Audit Program: Crisis Management Audit/Assurance Program (Aug 2010).
8. ISACA Audit Program: IT Continuity Planning Audit/Assurance Program (Jan 2009).
9. ISACA Audit Program: Mobile Computing Security Audit/Assurance Program (Oct 2010).
10. ISACA Audit Program: Outsourced IT Environments Audit/Assurance Program (Jan 2013).
11. ISACA Board briefing on IT governance, 2nd Edition, 2003.
12. ISACA Standard and guidelines.
13. ISO 27001.
14. ISO 27002.
15. ISO/IEC 38500 Corporate Governance of Information Technology.
16. The Risk IT Framework.
17. The Risk IT Practitioner's Guide.
18. ISSAIs 1220 and 1330.
19. ISSAI 5300, 1220, 1315, 1330, 5310, 5450.
20. Manual for Information Technology Audit- India.
21. Report on the Committee on the Financial Aspects of Corporate Governance, Sir Adrian Cadbury, London, 1992, ISBN 0 85258 9131.
22. WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.

فهرست انتشارات

مرکز آموزش و تحقیقات حسابداران رسمی

جامعه حسابداران رسمی ایران

شماره نشریه	عنوان نشریه
۱	پرسش‌های چهار گزینه‌ای حسابرسی
۲	پرسش و پاسخ‌های مالیاتی
۳	آشنایی با جامعه حسابداران رسمی ایران
۴	مجموعه قانون و مقررات جامعه حسابداران رسمی ایران
۵	آیین رفتار حرفه‌ای
۶	چک‌لیست‌های قانون تجارت و قانون محاسبات عمومی
۷	دستورالعمل حسابرسی
۸	دستورالعمل تهیه و تنظیم پرونده و گزارش حسابرسی مالیاتی
۹	دیباچه‌ای بر حقوق مدنی
۱۰	حسابداری اموال، ماشین‌آلات و تجهیزات: بر پایه استانداردهای حسابداری
۱۱	مبانی ارزیابی سهام
۱۲	راهنمای بکارگیری استانداردهای حسابرسی (۱)- گزارش حسابرس درباره‌ی صورت‌های مالی (استانداردهای حسابرسی بخش‌های ۷۰۰، ۷۰۵ و ۷۰۶)
۱۳	آیین رفتار حرفه‌ای برای حسابداران حرفه‌ای
۱۴	راهنمای بکارگیری استانداردهای حسابداری (۱)- استاندارد شماره ۱۶
۱۵	حسابداری سرمایه‌گذاری‌ها- جلد نخست
۱۶	راهنمای بکارگیری استانداردهای بین‌المللی حسابرسی در حسابرسی واحدهای تجاری کوچک و متوسط (کتاب دوم- رهنمودهای عملی)
۱۷	بایدها و نبایدها در پذیرش و نخستین کاربری استانداردهای بین‌المللی گزارشگری مالی
۱۸	استاندارد بین‌المللی گزارشگری مالی شماره ۶ اکتشاف و ارزیابی منابع معدنی
۱۹	استانداردهای بین‌المللی کار حرفه‌ای حسابرسی داخلی
۲۰	آیین رفتار حرفه‌ای برای حسابداران حرفه‌ای
۲۱	اهمیت در حسابرسی صورت‌های مالی
۲۲	ادغام مؤسسات حسابرسی در جهان

فهرست انتشارات

مرکز آموزش و تحقیقات حسابداران رسمی

جامعه حسابداران رسمی ایران

شماره نشریه	عنوان نشریه
۲۳	ادغام و تملیک بررسی قوانین و مقررات موجود
۲۴	آیین اخلاق و رفتار حرفه‌ای حسابداران رسمی
۲۵	پرسش و پاسخ‌های کارگروه‌های تخصصی جامعه حسابداران رسمی ایران
۲۶	آزمون‌های جامعه حسابداران رسمی ایران- (حسابداری)
۲۷	آشنایی با استارت آپ‌ها: بررسی و شناخت فین‌تک‌ها
۲۸	چارچوب کنترل داخلی برای حسابرسان مستقل
۲۹	دستورالعمل حسابرسی بنگاه‌های کوچک
۳۰	دستورالعمل حسابرسی بنگاه‌های متوسط و بزرگ (بازنگری شده ۲۰۱۸)
۳۳	رهنمودهای بکارگیری چارچوب بین‌المللی اجرای حرفه‌ای حسابرسی داخلی
۳۵	مباحث جاری مالیاتی
۳۶	تدوین برنامه حسابرسی داخلی مبتنی بر ریسک
۳۷	راهنمای بکارگیری استانداردهای حسابرسی (۳)- راهنمای مبارزه با پولشویی برای حسابرسان مستقل
۳۸	راهنمای بکارگیری استانداردهای حسابداری (۲)- حسابداری مالیات بر درآمد
۳۹	واکاوی فاصله بین تئوری و عمل در رشته‌های حسابداری و حسابرسی و تعیین سرفصل‌های مفقوده در آموزش دانشگاهی
۴۰	دستورالعمل حسابرسی بنگاه‌های کوچک (بازنگری شده کامل)
۴۱	دستورالعمل حسابرسی بنگاه‌های متوسط و بزرگ (بازنگری شده کامل)
۴۲	اصول مبارزه با پولشویی و تأمین مالی تروریسم
۴۳	راهنمای تحلیل داده‌ها در حسابرسی
۴۴	مواد ۳۸ و ۴۱ قانون تأمین اجتماعی- ضوابط و مقررات اجرایی (با آخرین اصلاحات و الحاقات)
۴۵	پرسش‌های حسابرسی- آزمون‌های انتخاب حسابدار رسمی (سال‌های ۱۳۹۶ تا ۱۴۰۰ با پاسخ تشریحی)