سازمان نظام صنفی رایانه‌ای کشور
استان تهران

سند ایجاد زیست‌بوم حسابرسی فناوری اطلاعات

نسخه	تعداد صفحات	تاریخ ویرایش
۲.۰	۳۶ (فاقد پیوست)	خرداد ۱۴۰۵
کمیسیون حسابرسی فناوری اطلاعات سازمان نظام صنفی رایانه‌ای استان تهران کپی رایت: کلیه حقوق این اثر متعلق به سازمان نصر استان تهران است.		

پیش نویس جهت دریافت نظرات متخصصان و کارشناسان

نسخه ۲.۰

فهرست مطالب

مقدمه

در عصر دیجیتال کنونی، فناوری اطلاعات و ارتباطات[1] به یکی از ارکان اساسی و حیاتی فعالیت‌های سازمانی در تمامی بخش‌های اقتصادی، دولتی و خصوصی تبدیل شده است. بخش عمده‌ای از فرایندهای مالی، عملیاتی، مدیریتی، تصمیم‌گیری و حتی ارائه خدمات سازمان‌ها بر پایه زیرساخت‌ها و سیستم‌های اطلاعاتی دیجیتال استوار گردیده و وابستگی روزافزون به این سیستم‌ها، سازمان‌ها را در معرض ریسک‌های متنوع فناوری اطلاعات از جمله تهدیدات سایبری، خطاهای پردازشی، نقض حریم خصوصی و امنیت داده‌ها، اختلالات عملیاتی و کاهش کارایی قرار داده است. حسابرسی فناوری اطلاعات یا حسابرسی سیستم‌های اطلاعاتی به‌عنوان فرایندی نظام‌مند برای **جمع‌آوری و ارزیابی شواهد از جمله کنترل‌ها، ریسک‌ها، امنیت، انطباق و کارایی سامانه‌های اطلاعاتی** یک سازمان است تا **اطمینان** حاصل شود فناوری اطلاعات در خدمت اهداف کسب‌وکار بوده و ریسک‌های آن به‌درستی مدیریت می‌شود.

این نوع حسابرسی، نه‌تنها مکمل حسابرسی مالی سنتی و حسابرسی داخلی است، بلکه با تمرکز ویژه بر کنترل‌های عمومی و کاربردی فناوری اطلاعات، حاکمیت شایسته فناوری اطلاعات و مدیریت ریسک‌های دیجیتال، نقش کلیدی در شناسایی به‌موقع ضعف‌ها (اقدام پیشگیرانه)، ارائه پیشنهادهای اصلاحی و تقویت تاب‌آوری سازمانی ایفا می‌نماید. ایجاد یک زیست‌بوم حرفه‌ای و منظم برای حسابرسی فناوری اطلاعات در کشور، گامی اساسی در جهت ارتقای امنیت سایبری، حمایت از اقتصاد دیجیتال و حفظ اعتماد عمومی به سیستم‌های اطلاعاتی[2] و دستیابی به اعتماد دیجیتال محسوب می‌شود.

۱. قلمرو

قلمرو حوزه حسابرسی فناوری اطلاعات به مجموعه مؤلفه‌ها، فرایندها و دارایی‌های فناوری اطلاعات اطلاق می‌شود که به‌منظور **ارزیابی ریسک، کنترل، امنیت، انطباق و اثربخشی فناوری اطلاعات و ارتباطات** مورد رسیدگی حسابرسی قرار می‌گیرند. این قلمرو حسابرسی در هر مأموریت، بسته به ماهیت فعالیت سازمان، الزامات قانونی و نظارتی، سطح بلوغ فناوری اطلاعات، رویکرد حسابرسی (سنتی یا برخط) و نتایج ارزیابی ریسک اولیه تعیین شده و می‌تواند شامل و نه محدود به یک یا چند حوزه از موارد زیر باشد:

- حاکمیت و مدیریت فناوری اطلاعات
- فرایندهای فناوری اطلاعات و ارتباطات
- کنترل‌های عمومی و کاربردی فناوری اطلاعات

[1] Information and Communication Technologies
[2] Information System

- امنیت اطلاعات و حفاظت از دارایی‌های اطلاعاتی
- تداوم کسب‌وکار و تاب‌آوری فناوری اطلاعات
- مدیریت خدمات فناوری اطلاعات
- تحصیل، توسعه و پیاده‌سازی سامانه‌های اطلاعاتی، زیرساخت‌ها و داده‌ها

قلمرو اجرای این طرح می‌تواند، تمامی حوزه‌های مرتبط با حسابرسی فناوری اطلاعات در بخش‌های دولتی، عمومی و خصوصی کشور را در برگیرد و شامل خدمات‌دهندگان و خدمات گیرندگان فناوری اطلاعات، نهادهای سیاست‌گذار و هماهنگ‌کننده، نهادهای نظارتی و نهادها/انجمن‌های علمی است. این قلمرو باهدف ایجاد هماهنگی جامع میان ذی‌نفعان و پوشش کامل نیازهای حسابرسی فناوری اطلاعات در سطح ملی تعریف شده است.

۲. اصطلاحات و تعاریف

۲/۱ **سازمان نظام صنفی رایانه‌ای کشور:** تشکلی صنفی - تخصصی در حوزه فناوری اطلاعات و ارتباطات در ایران است

۲/۲ **فرایند:** مجموعه‌ای از فعالیت‌های مرتبط به هم یا متعامل که جهت ارائه نتیجه موردنظر، از دروندادها استفاده کند.

۲/۳ **شواهد**[۳]: سوابق، اظهارات گویای واقعیت یا سایر اطلاعاتی که به معیارهای ممیزی مرتبط بوده و قابل راستی‌آزمایی باشند.

۲/۴ **شواهد عینی**[۴]: اطلاعات، سوابق، مشاهدات یا نتایج اندازه‌گیری قابل راستی‌آزمایی که به طور واقعی و مستقل از قضاوت شخصی، انطباق یا عدم انطباق با یک الزام را اثبات می‌کنند.

۲/۵ **معیارهای ممیزی**[۵]: مجموعه استانداردها، مقررات مرجع، خط‌مشی‌ها، روش‌های اجرایی یا الزامات که به‌عنوان مبنایی برای مقایسه و ارزیابی شواهد عینی با آنها استفاده می‌شود.

۲/۶ **تعریف ممیزی**[۶]: ممیزی فرایندی نظام‌یافته، مستقل و مدون برای به‌دست‌آوردن شواهد عینی و ارزیابی آن به‌صورت عینی برای تعیین میزانی که معیارهای ممیزی برآورده می‌شوند.

۲/۷ **حسابرسی فناوری اطلاعات**[۷]:حسابرسی فناوری اطلاعات فرایندی رسمی، نظام‌مند و مستقل برای بررسی و راستی‌آزمایی کنترل‌ها، فرایندها، سیستم‌ها و اطلاعات مبتنی بر فناوری اطلاعات است که باهدف

---

[3] Evidence
[4] Objective Evidence
[5] Audit Criteria
[6] Audit(ISO 19011:2018)
[7] Audit (ISACA Glossary)

اطمینان‌بخشی نسبت به رعایت استانداردها و دستورالعمل‌های مصوب، صحت و قابلیت اتکای سوابق و داده‌ها، و میزان **تحقق اهداف** کارایی، اثربخشی، امنیت و قابلیت اعتماد سیستم‌های اطلاعاتی انجام می‌شود.

۳. تاریخچه

۳/۱ تاریخچه در جهان

در سال ۱۹۷۰ مفهوم حسابرسی پردازش داده‌های الکترونیکی[8] (EDPA) پدید آمد. این نوع حسابرسی بر کنترل‌های سیستم‌های رایانه‌ای، صحت پردازش داده‌ها و امنیت اطلاعات متمرکز شد .

در دهه ۱۹۹۰، چارچوب‌های جدیدی مانند : COBIT ، ISO 17799 و بعدتر ISO 27001 برای حسابرسی و کنترل فناوری اطلاعات توسعه یافتند.

در حال حاضر سازمان‌هایی مانند انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی[9]، انجمن حسابرسان داخلی آمریکا[10] ، انجمن حسابداران رسمی آمریکا(AICPA) [11] و...، چارچوب‌های جدیدی برای **حسابرسی فناوری اطلاعات در حوزه‌های مالی و سیستم‌های اطلاعاتی** تدوین کرده‌اند. چارچوب حسابرسی فناوری اطلاعات (ITAF) منبع مهمی در این حوزه است.

۳/۲ تاریخچه در ایران

- سازمان حسابرسی (برای بخش دولتی)

سازمان وابسته به وزارت اقتصاد و دارایی است و در زمینه حسابرسی شرکت‌های دولتی به بخش‌های دولتی و تحت نظارت دولت و نیز تدوین استانداردها و ضوابط حسابداری و حسابرسی و پایداری فعال است.

- جامعه حسابداران رسمی ایران (برای بخش خصوصی)

در سال ۱۳۸۰، جامعه حسابداران رسمی ایران[12] با مصوبه مجلس شورای اسلامی تأسیس شده است.

مؤسسات حسابرسی بخش خصوصی با مجوز و تحت نظارت جامعه فعالیت می‌کنند.

8 Electronic Data Processing Auditing

9 Information Systems Audit and Control Association

10 Institute of Internal Auditors

11 American Institute of Certified Public Accountants

12 Iranian Association of Certified Public Accountants

از دهه ۱۳۹۰ به بعد، سازمان حسابرسی و جامعه حسابداران رسمی، توجه بیشتری به کنترل‌های عمومی فناوری اطلاعات ITGC[13] و چارچوب‌های نظارتی مانندCOBIT ، ISO 27001واITIL [۱۴] نشان دادند.

- دیوان محاسبات کشور

هدف دیوان محاسبات کشور باتوجه‌به اصول مندرج در قانون اساسی جمهوری اسلامی ایران عبارت است از اعمال کنترل و نظارت مستمر مالی به‌منظور پاسداری از بیت‌المال از طریق:

الف -کنترل عملیات و فعالیت‌های مالی کلیه وزارتخانه‌ها، مؤسسات، شرکت‌های دولتی و سایر دستگاه‌هایی که به‌نحوی از انحا از بودجه کل کشور استفاده می‌کنند.

ب -بررسی و حسابرسی وجوه مصرف شده و درآمدها و سایر منابع تأمین اعتبار در ارتباط با سیاست‌های مالی تعیین شده در بودجه مصوب باتوجه‌به گزارش عملیاتی و محاسباتی مأخوذه از دستگاه‌های مربوطه.

- طی سال‌های اخیر **انجمن علمی حسابرسی فناوری اطلاعات ایران**[۱۵] توسط پیش‌کسوت‌ها و اساتید حسابداری، رایانه، فناوری اطلاعات و حسابرسان مالی برای حسابرسی فناوری اطلاعات تشکیل گردیده است که مرجع دانشی آن بر اساس انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی است. این انجمن تاکنون کتاب‌ها و دوره‌های مختلفی را برای معرفی و ترویج فناوری اطلاعات برای حسابرسان فناوری اطلاعات بانک‌ها، حسابرسان داخلی، مدیران و کارشناسان ارشد فناوری اطلاعات و حسابرسان مالی برگزار نموده است و باتوجه‌به رابطه خوب با بانک‌ها، سازمان حسابرسی، بورس، وزارت اقتصاد و بانک مرکزی در تلاش برای ایجاد ساختار و جایگاه برای حسابرسان فناوری اطلاعات است.
- کمیسیون حسابرسی فناوری اطلاعات نصر تهران

کمیسیون حسابرسی فناوری اطلاعات یک مرجع تخصصی، مشورتی و راهبردی است که با رویکرد ساماندهی و یکپارچه‌سازی زیست‌بوم حسابرسی فاوا مبتنی بر اصول حاکمیت فناوری، مدیریت ریسک و انطباق(GRC) ، باهدف توسعه چارچوب‌ها، استانداردها، آیین‌نامه‌ها و ظرفیت‌های حرفه‌ای حسابرسی در حوزه فناوری اطلاعات و ارتباطات تشکیل گردیده است.

اهداف کلان کمیسیون فوق به شرح ذیل است:

- تدوین، ترویج و نهادینه‌سازی استانداردهای حسابرسی فاوا مبتنی بر اصولGRC
- ایجاد و توسعه بستر حرفه‌ای، مشارکتی و شبکه‌ای حسابرسی فناوری اطلاعات و ارتباطات
- ارتقای شفافیت، تاب‌آوری و اعتماد دیجیتال در سازمان‌ها و ذی‌نفعان

13 Information Technology General Controls

14 Information Technology Infrastructure Library

15 Iranian Information Technology Auditing Scientific Association

- تقویت ظرفیت‌های تخصصی، مشورتی و سیاست‌گذاری در حوزه حسابرسی فاوا و حاکمیت ریسک
- تقویت حسابرسی فناوری اطلاعات و ارتباطات در حکمرانی دولت الکترونیک
- پاسخ به انتظارات ماده دوم سند مورخ ۱۴۰۴/۰۶/۰۹ با موضوع الزامات ارتقای امنیت فضای مجازی کشور ابلاغی توسط مرکز ملی فضای مجازی کشور
- تهیه و تدوین آیین‌نامه‌ها، دستورالعمل‌ها و چارچوب‌های بیمه سایبری مبتنی بر مدل‌های ارزیابی ریسک و حسابرسی دیجیتال

٤. برخی از حوزه‌های حسابرسی فناوری اطلاعات

۴/۱ حسابرسی سیستم‌های اطلاعاتی(IS Audit)

حسابرسی سیستم‌های اطلاعاتی برای جمع‌آوری و ارزیابی شواهد طراحی شده است تا مشخص شود آیا

سیستم‌های اطلاعاتی سازمان شامل داده‌ها، فرایندها و کنترل‌های مرتبط با آن‌ها به‌گونه‌ای طراحی، پیاده‌سازی، محافظت و نگهداری شده‌اند تا:

- اهداف کسب‌وکار را پشتیبانی کنند،
- یکپارچگی و دسترس بودن داده‌ها و سیستم حفظ شود،
- اطلاعات مرتبط و قابل‌اعتماد ارائه شود،
- به اهداف سازمانی به طور مؤثر دست یابند،
- منابع به طور کارآمد مصرف شوند،
- از دارایی‌های اطلاعاتی محافظت شود،
- دارای کنترل‌های داخلی هستند که اطمینان معقولی در خصوص برآوردشدن اهداف تجاری، عملیاتی و کنترلی ارائه شود،
- از رویدادهای نامطلوب جلوگیری یا شناسایی و به‌موقع اصلاح شوند،
- با قوانین، مقررات و سیاست‌ها منطبق باشند.
- از تداوم کسب‌وکار (BCM[۱۶]) پشتیبانی می‌کند.

۴/۲ حسابرسی انطباق (رعایت) [۱۷]

16 Business Continuity Management

17 Compliance Audit

این حسابرسی از جمله شامل آزمون کنترل‌ها برای نشان‌دادن پایبندی[18]به مقررات، استانداردها یا رویه‌های خاص صنعت است.

۴/۳ حسابرسی مالی

حسابرسی مالی، اطمینان‌بخشی در مورد[19] گزارشگری مالی سازمان‌ها است. اغلب شامل آزمون‌های دقیق کنترل و محتوا[20] است. حسابرسان سیستم‌های اطلاعاتی و هم حسابرسان مالی به طور فزاینده‌ای بر رویکرد حسابرسی مبتنی بر ریسک و کنترل تأکید بیشتری دارند. حسابرسی مالی همچنین به یکپارچگی و اتکاپذیری[21] اطلاعات مالی مربوط می‌شود.[22]

۴/۴ حسابرسی عملیاتی

حسابرسی عملیاتی بر کارایی، صرفه اقتصادی و اثربخشی سازمان یا حوزه‌های خاص آن مثل فناوری اطلاعات تأکید دارد. در بخش دولتی به حسابرسی عملکرد شناخته می‌شود.

۴/۵ حسابرسی عملکردی

حسابرسی عملکردی، ارزیابی مستقلی از محصولات نرم‌افزاری ارائه می‌دهد و تأیید می‌کند که عملکرد و کارایی پیکربندی[23] با مشخصات الزامات مطابقت دارد. به طور خاص، حسابرسی عملکردی یا قبل از تحویل نرم‌افزار یا پس از پیاده‌سازی انجام می‌شود.

۴/۶ حسابرسی شخص ثالث

حسابرسی فرایندهای مالی و تجاری برون‌سپاری شده به ارائه‌دهندگان خدمات شخص ثالث را که ممکن است در حوزه‌های مختلف فعالیت کنند، مورد بررسی قرار می‌دهد. گزارش‌های حسابرسی شخص ثالث، می‌تواند توسط حسابرس سیستم‌های اطلاعاتی مورد استفاده قرار گیرد.

۴/۷ حسابرسی تقلب

حسابرسی تخصصی است که برای کشف فعالیت‌های متقلبانه طراحی شده است.

---

18 Adherence
19 Accuracy
20 Substantive
21 Reliability
22 CISA
23 Configuration

حسابرسان اغلب از ابزارها و فن‌های خاص تحلیل داده‌ها برای کشف طرح‌های تقلب و بی‌نظمی‌های[۲۴] تجاری استفاده می‌کنند.

۴/۸ حسابرسی جرم‌شناسی (دادگاهی) رایانه‌ای[۲۵]

تحقیق و رسیدگی است که شامل تجزیه‌وتحلیل دستگاه‌های محاسباتی الکترونیکی[۲۶] باهدف جمع‌آوری و حفظ شواهد می‌شود. یک حسابرس سیستم‌های اطلاعاتی که دارای مهارت‌های لازم باشد، می‌تواند به مدیر امنیت اطلاعات یا متخصص جرم‌شناسی در انجام تحقیقات قانونی کمک کند و می‌تواند حسابرسی سیستم را انجام دهد تا از انطباق با رویه‌های جمع‌آوری شواهد برای تحقیقات قانونی اطمینان حاصل شود.

۴/۹ ارزیابی آمادگی[۲۷]

بررسی وضعیت فعلی سازمان از نظر انطباق یا پایبندی به استانداردها است. ارزیابی‌های آمادگی عموماً بر طراحی کنترل تمرکز دارند، نه بر اثربخشی عملیاتی و منجر به موارد قابل اقدام برای سازمان می‌شوند تا قبل از ممیزی رسمی، آنها را اصلاح کنند.

۴/۱۰ حسابرسی تحول دیجیتال

حسابرسی تحول دیجیتال فرایندی مستقل و مبتنی بر شواهد است که به ارزیابی راهبرد، حاکمیت، فرایندها، فناوری‌ها، سرمایه انسانی و مدیریت ریسک ابتکارات تحول دیجیتال سازمان می‌پردازد و میزان اثربخشی، هم راستایی، بلوغ و ارزش‌آفرینی آن را در تحقق اهداف کسب‌وکار و الزامات حاکمیت دیجیتال بررسی می‌نماید.

۴/۱۱ حسابرسی فناوری‌های نوظهور

مثل اینترنت اشیا[۲۸]، هوش مصنوعی[۲۹] ، بلاک‌چین، رمزارز و فضای ابری

۵. جایگاه «نظام حسابرسی فناوری اطلاعات» از منظر نهادهای بین‌المللی و حرفه‌ای

۵/۱ انجمن حسابداران رسمی آمریکا (AICPA)

24 irregularities
25 Forensic audit
26 electronic computing
27 Readiness assessment
28 Internet of Things
29 Artificial intelligence

ارائه‌دهنده گواهینامه حرفه‌ای بین‌المللی در حوزه بین‌رشته‌ای حسابرسی/حسابداری، فناوری اطلاعات و تحلیل داده به نام CITP[۳۰] است.

CITP نشان‌دهنده صلاحیت حرفه‌ای افرادی است که می‌توانند:

- ریسک‌ها و کنترل‌های فناوری اطلاعات را در چارچوب حسابداری و حسابرسی تحلیل کنند،
- از تحلیل داده، سیستم‌های اطلاعاتی، امنیت، اتوماسیون و AI برای تصمیم‌سازی و اطمینان‌بخشی استفاده کنند، نقش پل ارتباطی بین مالی، حسابرسی و فناوری اطلاعات را ایفا کنند.

۵/۱/۱ تمرکز محوری CITP

CITP برخلاف گواهینامه‌های صرفاً فناوری اطلاعات، از زاویه حرفه حسابداری و حسابرسی به فناوری نگاه می‌کند:

- IT Risk & Controls
- Data Analytics for Audit
- Cybersecurity & Privacy
- Automation & AI in Assurance
- IT Governance (از منظر مالی/کنترلی)
- کنترل‌های سیستم اطلاعاتی (Information Systems Controls)
- امنیت سایبری و ریسک اطلاعات (Cybersecurity)
- تحلیل شناسی داده و گزارشگری پیشرفته (Data Analytics)
- مشاوره فناوری در کسب‌وکار و حسابرسی (Technology Advisory)
- سامانه‌های ابری و برنامه‌ریزی منابع سازمانی (ERP / Cloud Systems)

۵/۱/۲ مخاطبان اصلی

- حسابرسان (داخلی و مستقل) با تمرکز فناوری اطلاعات
- حسابداران رسمی CPA[۳۱]
- مشاوران ریسک و اطمینان‌بخشی
- مدیران GRC و تحول دیجیتال

شرط مهم: معمولاً دارندگان یا واجدان شرایط CPA هستند (یا معادل آن).

---

30 Certified Information Technology Professional

31 Certified Public Accountants

۵/۱/۳ ساختار CPA Evolution

از ژانویه ۲۰۲۴، آزمون CPA به مدل Core + Discipline تغییر یافت:

الف) Core (همه داوطلبان)

- حسابرسی و گواهی‌دهی (AUD)،
- حسابداری و گزارشگری مالی (FAR)، و
- قوانین مالیات و مقررات (REG).

ب) Discipline (رشته انتخابی)

داوطلب تنها یکی از سه مسیر تخصصی را می‌گذراند:

- تحلیل کسب‌وکار و گزارشگری (BAR)،
- سیستم‌های اطلاعاتی و کنترل‌ها (ISC)،
- برنامه‌ریزی و رعایت قوانین مالیاتی (TCP).

بخش ISC به طور ویژه برای تمرکز بر فناوری اطلاعات، امنیت سیستم، کنترل داخلی و تحلیل داده طراحی شده است.

۵/۱/۴ نقش‌ها و فرصت‌های شغلی فناوری‌محور

- سرپرست حسابرسی فناوری اطلاعات (IT Audit Lead)
- مشاوره فناوری کسب‌وکار (Technology Advisory)
- تحلیلگر داده‌ها برای تصمیم‌گیری مالی (Data & Analytics Advisor)
- مشاور سامانه‌های سازمانی وERP (ERP / Cloud Consultant)
- مشاور ریسک سایبری (Cyber Risk Consultant)

۵/۲ انجمن حسابرسان داخلی آمریکا

از دیدگاه انجمن حسابرسان داخلی آمریکا، حسابرسی فناوری اطلاعات یک زیرمجموعه تخصصی از حسابرسی داخلی محسوب می‌شود و جایگاه آن در چارچوب حرفه‌ای حسابرسی داخلی و در نظام حاکمیت، مدیریت ریسک و کنترل‌های داخلی سازمان تعریف می‌شود.

- حاکمیت سازمانی
- مدیریت ریسک
- کنترل‌های داخلی

۵/۲/۱ نقش حسابرسی فناوری اطلاعات در چارچوب فوق

- ارزیابی کنترل‌های عمومی فناوری اطلاعات[۳۲]
- ارزیابی کنترل‌های برنامه‌های کاربردی[۳۳]
- بررسی امنیت اطلاعات و حفاظت از داده‌ها
- ارزیابی مدیریت ریسک‌های فناوری اطلاعات
- بررسی قابلیت اتکا و یکپارچگی سیستم‌های اطلاعاتی
- پشتیبانی از حسابرسی‌های مالی و عملیاتی از طریق ارزیابی سیستم‌های اطلاعاتی

۵/۲/۲ جایگاه سازمانی

- حسابرسی فناوری اطلاعات معمولاً در واحد حسابرسی داخلی[۳۴] قرار دارد.
- حسابرسان فناوری اطلاعات ممکن است به‌صورت تیم تخصصی در داخل واحد حسابرسی داخلی یا متخصصان فناوری اطلاعات در تیم‌های حسابرسی فعالیت کنند.
- گزارش‌دهی آن‌ها معمولاً به مدیر ارشد حسابرسی[۳۵] و در نهایت کمیته حسابرسی هیئت‌مدیره انجام می‌شود.

---

32 ITGC

33 Application Controls

34 Internal Audit Activity

35 Chief Audit Executive – CAE

۵/۲/۳ ارتباط با مدل سه خط دفاع[۳۶]

در مدل سه خط دفاع، جایگاه حسابرسی فناوری اطلاعات چنین است:

- خط اول دفاع
  - مدیریت فناوری اطلاعات و مالکان فرایندها (مسئول اجرای کنترل‌ها)
- خط دوم دفاع
  - مدیریت ریسک و امنیت اطلاعات (پایش و سیاست‌گذاری)
- خط سوم دفاع
  - حسابرسی داخلی شامل حسابرسی فناوری اطلاعات (ارائه اطمینان‌بخشی مستقل)

بنابراین، حسابرسی فناوری اطلاعات در خط سوم دفاع قرار می‌گیرد و نقش آن ارائه اطمینان مستقل نسبت به کفایت کنترل‌ها و مدیریت ریسک‌های فناوری اطلاعات است و مدیریت ریسک فناوری و کمیته‌های عالی فناوری در خط دوم قرار می‌گیرند.

۵/۳ حسابرسی فناوری اطلاعات از منظر ایساکا

انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی[۳۷] (ISACA) یکی از مهم‌ترین نهادهای حرفه‌ای بین‌المللی در حوزه حاکمیت فناوری اطلاعات، مدیریت ریسک، کنترل و حسابرسی سیستم‌های اطلاعاتی است. این نهاد از طریق چارچوب‌ها، استانداردها و راهنماهای حرفه‌ای، به توسعه و استقرار نظام حسابرسی فناوری اطلاعات در سازمان‌ها کمک می‌کند.

از دیدگاه ایساکا، حسابرسی فناوری اطلاعات بخشی از خدمات اطمینان‌بخشی[۳۸] محسوب می‌شود که هدف آن ارزیابی کفایت و اثربخشی کنترل‌های فناوری اطلاعات، قابلیت اتکای سیستم‌های اطلاعاتی، حفاظت از دارایی‌های اطلاعاتی و میزان انطباق با استانداردها و مقررات است. در این چارچوب، حسابرسی فناوری اطلاعات با تمرکز بر ارزیابی ریسک‌های مرتبط با فناوری اطلاعات، به سازمان‌ها کمک می‌کند تا اطمینان یابند که فناوری اطلاعات از تحقق اهداف کسب‌وکار پشتیبانی کرده و منابع فناوری اطلاعات به‌صورت کارآمد، ایمن و قابل‌اعتماد مدیریت می‌شوند.

36 IIA Three Lines Model

37 Information Systems Audit and Control Association

38 IT Assurance

ایساکا برای استقرار نظام حرفه‌ای حسابرسی فناوری اطلاعات مجموعه‌ای از چارچوب‌ها و استانداردهای تخصصی ارائه کرده است که مهم‌ترین آن‌ها عبارت‌اند از: چارچوب اطمینان‌بخشی فناوری اطلاعات[۳۹]چارچوب حاکمیت و مدیریت فناوری اطلاعات سازمانی [۴۰] و راهنماهای حرفه‌ای مرتبط با حسابرسی و کنترل سیستم‌های اطلاعاتی است.

از دیدگاه ISACA، جایگاه این نظام در سه سطح زیر تبیین می‌گردد:

۵/۳/۱ به‌عنوان یک جزء کلیدی از حاکمیت فناوری اطلاعات[۴۱]

- حاکمیت به‌درستی مستقر شده است؟
- آیا اهداف فناوری اطلاعات با استراتژی‌های کسب‌وکار هم‌سو[۴۲] هستند؟
- آیا ارزش‌آفرینی[۴۳] از طریق فناوری اطلاعات محقق شده است؟

۵/۳/۲ به‌عنوان ستون اصلی اطمینان‌بخشی

طبق چارچوب ITAF، حسابرسی فناوری اطلاعات در جایگاه "اطمینان‌بخشی مستقل[۴۴]" قرار دارد.

- وظیفه: ارزیابی اینکه آیا کنترل‌های طراحی‌شده در سیستم‌های اطلاعاتی و فرایندهای فناوری اطلاعات، به طور مؤثر کار می‌کنند یا خیر.
- جایگاه عملیاتی: برخلاف مدیریت فناوری اطلاعات که وظیفه اجرا را دارد، حسابرسی فا از نظر ایساکا باید مستقل باشد تا بتواند بدون سوگیری، ریسک‌های سیستمی را شناسایی و به مدیریت ارشد و هیئت‌مدیره گزارش کند.

۵/۳/۳ به‌عنوان بازوی ارزیاب در مدل COBIT

در مدل COBIT 2019، جایگاه حسابرسی فناوری اطلاعات ذیل یکی از اهداف حاکمیتی تحت عنوان "نظارت، ارزیابی و سنجش"MEA [۴۵]تعریف می‌شود.

- **MEA01**: پایش و ارزیابی عملکرد و انطباق.

---

39 ITAF
40 COBIT
41 Governance of IT
42 Aligned
43 Value Delivery
44 Independent Assurance
45 Monitor, Evaluate and Assess - MEA

- جایگاه: در اینجا حسابرسی فناوری اطلاعات به‌عنوان ابزاری برای **پایش مستمر** کنترل‌ها و انطباق با قوانین و استانداردها[۴۶] شناخته می‌شود تا از "یکپارچگی و سلامت عملیات فا" اطمینان حاصل شود.

۵/۴ حسابرسی فناوری اطلاعات از دیدگاه جامعه حسابداران رسمی ایران

- ارائه اطمینان نسبت به محرمانگی، یکپارچگی، دسترس‌پذیری و قابلیت اتکای اطلاعات و سامانه‌های اطلاعاتی.
- ارزیابی میزان انطباق فناوری اطلاعات با قوانین، مقررات، الزامات نهادهای ناظر و تعهدات قراردادی، بر مبنای چارچوب‌ها و استانداردهای حرفه‌ای پذیرفته‌شده به‌عنوان معیارهای ارزیابی. همانند ایزو[47]، کوبیت [۴۸]و قوانین داخلی.
- ارزیابی کفایت و اثربخشی نظام مدیریت ریسک‌های فناوری اطلاعات، شامل ریسک‌های سایبری، عملیاتی، انطباقی و تداوم کسب‌وکار.
- ارائه اطمینان نسبت به طراحی و اثربخشی کنترل‌های داخلی فناوری اطلاعات به‌منظور حفاظت از دارایی‌های اطلاعاتی و پشتیبانی از اهداف کسب‌وکار.
- ارزیابی نقش و اثربخشی فناوری اطلاعات در پشتیبانی از صحت اطلاعات مالی و عملیاتی.
- ارزیابی امنیت و حفاظت دارایی‌های اطلاعاتی در برابر تهدیدات داخلی و خارجی.
- کارایی، اثربخشی و بهینگی سیستم‌های اطلاعاتی در حمایت از دستیابی به اهداف استراتژیک و عملیاتی‌سازمان.
- ارائه اطمینان معقول نسبت به حاکمیت فناوری اطلاعات و هم‌راستایی راهبردها، ساختارها و فرایندهای فناوری اطلاعات با اهداف کلان و عملیاتی سازمان.

٦. نیاز و الزامات فعلی حسابرسی فناوری اطلاعات

۶/۱ نیازهای کلیدی حسابرسی در شرایط کنونی

- افزایش ریسک‌های دیجیتال و سایبری
- داده‌محوری و هوش مصنوعی
- افزایش الزامات پاسخگویی و شفافیت
- تغییر ماهیت تقلب و خطا
- تقاضاهای فزاینده در قالب افزایش الزامات قانونی و مقرراتی
- پاسخ به انتظارات سند الزامات ارتقای امنیت فضای مجازی کشور ابلاغی توسط مرکز ملی فضای مجازی کشور

46 Compliance

47 International Organization for Standardization

48 Control Objectives for Information and Related Technologies

- افزایش رضایت‌مندی ذی‌نفعان از خدمات دریافتی
- تکمیل چرخه کسب‌وکارهای مرتبط با حوزه‌های امنیت، ممیزی و بیمه سایبری

۶/۲ الزامات فعلی حسابرسی فناوری اطلاعات

- الزامات حاکمیتی و قانونی
- الزامات حرفه‌ای و استانداردی
- الزامات فنی و فناورانه
- الزامات سازمانی
- الزامات روش‌شناختی
- الزامات اخلاقی و حرفه‌ای

۶/۳ الزامات نوظهور

- حسابرسی برخط و مستمر
- حسابرسی هوش مصنوعی
- استفاده از هوش مصنوعی در حسابرسی
- حسابرسی خودکار مبتنی بر مدل‌های داده[۴۹]
- حسابرسی مبتنی بر ریسک
- حسابرسی مبتنی بر ریسک سایبری [۵۰]
- یکپارچگی باGRC

۷. چالش‌های قابل‌توجه

۷/۱ چالش‌های کلی

- پیچیدگی فزاینده محیط‌های فناوری
- تحول سریع فناوری و عقب ماندن چارچوب‌های سنتی
- کمبود نیروی انسانی متخصص میان‌رشته‌ای
- چالش‌های دسترسی به داده و شفافیت اطلاعات
- حسابرسی سیستم‌های ابری و برون‌سپاری شده

---

49 Data-driven Continuous Audit

50 Cyber Risk–based Audit

- چالش‌های حسابرسی امنیت سایبری
- حسابرسی داده و هوش مصنوعی
- چالش‌های استقلال و جایگاه سازمانی حسابرسی فناوری اطلاعات
- مقاومت سازمانی و فرهنگ حسابرسی گریز
- فقدان بومی‌سازی چارچوب‌ها و استانداردها

۷/۲ چالش‌های داخلی

- سازمان حسابرسی باتوجه‌به جایگاه و مسئولیت آن در نهادهای مالی و بورسی و دستورالعمل بانک مرکزی موظف به ارائه گزارش حسابرسی فناوری اطلاعات است که عملاً می‌بایست از خدمات افراد حوزه فناوری اطلاعات استفاده نماید که در حال حاضر چارچوب مشخصی برای احراز صلاحیت افراد یا شرکت‌های متولی این حوزه نمی‌باشد.
- پیش‌نیاز راه‌اندازی بیمه امنیت فضای مجازی ایجاد نظام حسابرسی فاوا و تربیت نیروهای متخصص بر اساس استاندارد واحد یا مجموعه‌ای از استانداردها و الگوها است که در کشور متولی یا مبنای مشخصی ندارد.
- برخلاف نظام DCAS نهاد گواهی‌دهنده و اعتباربخش حوزه فوق مشخص نیست.
- ابلاغ آیین‌نامه و دستورالعمل‌های جزیره‌ای برای امنیت یا الزامات حسابرسی توسط نهادهای مختلف مانند بانک مرکزی، افتا، پدافند غیرعامل، بیمه مرکزی، مرکز ملی و... که باعث چندصدایی در حوزه مهم امنیت و حسابرسی فا می‌گردد.
- باتوجه‌به دسترسی به ساختار، اطلاعات، مشکلات و... سازمان‌های مورد حسابرسی فا، بحث احراز صلاحیت حراستی اشخاص حقیقی و حقوقی اهمیت زیادی دارد.

۸. جایگاه سازمان نظام صنفی رایانه‌ای کشور

سازمان نظام صنفی رایانه‌ای کشور تشکلی صنفی - تخصصی در حوزه فناوری اطلاعات و ارتباطات در ایران است. برخی از مأموریت‌ها و وظایف کلیدی نصر شامل موارد ذیل می‌گردد:

۸/۱ تنظیم روابط بخش خصوصی با دولت

این سازمان به‌عنوان نماینده فعالان صنعت فناوری اطلاعات و ارتباطات بخش خصوصی، تلاش می‌کند مناسبات بخش خصوصی و دولت را در حوزه فناوری اطلاعات تنظیم نماید.

۸,۲ حمایت از حقوق و منافع صنفی فعالان فاوا

نصر از حقوق شرکت‌ها، فروشگاه‌ها، مشاوران و فعالان حوزه نرم‌افزار و سخت‌افزار حمایت می‌کند، و تسهیلات یا امتیازاتی برای اعضایش فراهم می‌آورد

۸,۳ ساماندهی بازار کسب‌وکارهای رایانه‌ای و فناوری اطلاعات

یکی از مأموریت‌های مشخص، «ساماندهی و نظم‌بخشی بازار کسب‌وکارهای رایانه‌ای» است.

۸,٤ تدوین تعرفه‌ها، استانداردها و مقررات صنفی

با همکاری فعالان صنعت، در حوزه تدوین استانداردها، تعرفه خدمات فناوری اطلاعات و ارتباطات و سایر مقررات اقدام می‌نماید.

۸,۵ افزایش مهارت‌ها، آموزش و توسعه سرمایه انسانی در فاوا

در همکاری با مراکز آموزشی، در راستای ارتقای مهارت نیروی انسانی متخصص در حوزه فناوری اطلاعات تفاهم‌نامه‌های مختلفی دارد. مثلاً تفاهم‌نامه با دانشگاه جامع علمی‌کاربردی برای تأمین نیروی انسانی ماهر در اقتصاد دیجیتال یا سازمان فنی و حرفه‌ای و اخیراً دانشگاه ملی مهارت

۸,٦ عمده نمایندگی بخش خصوصی در تصمیم‌سازی‌های حوزه فاوا

در فرایند قانون‌گذاری و ساماندهی فضای کسب‌وکار فناوری اطلاعات، نصر در مقام بیان دیدگاه بخش خصوصی فعالیت می‌کند.

۹. ذی‌نفعان زیست‌بوم حسابرسی فناوری

ذی‌نفعان زیست‌بوم حسابرسی فناوری اطلاعات مجموعه‌ای از بازیگران حاکمیتی، علمی، حرفه‌ای، اجرایی، فناورانه و مصرف‌کنندگان هستند که در **تولید، تنظیم‌گری، اجرا، استفاده و توسعه خدمات حسابرسی فناوری اطلاعات و ارتباطات** نقش دارند. این زیست‌بوم ذاتاً **چندبخشی، داده‌محور و بین‌رشته‌ای** است.

۹/۱ نهادهای حاکمیتی و سیاست‌گذار

نقش :تنظیم‌گری، الزام قانونی، نظارت کلان

- دولت و هیئت وزیران
- سازمان برنامه‌وبودجه کشور
- دیوان محاسبات
- سازمان حسابرسی

- بانک مرکزی، بیمه مرکزی، سازمان بورس
- مرکز ملی فضای مجازی
- مرکز افتای ریاست‌جمهوری
- سازمان پدافند غیرعامل
- پلیس فتا
- مجلس (کمیسیون‌های تخصصی)

۹/۲ نهادهای حرفه‌ای و صنفی

نقش :توسعه استاندارد، صلاحیت حرفه‌ای، فرهنگ‌سازی

- سازمان نظام صنفی رایانه‌ای کشور (نصر)
- انجمن علمی حسابرسی فناوری اطلاعات
- جامعه حسابداران رسمی ایران

۹/۳ دانشگاه‌ها، مراکز آموزشی و پژوهشی

نقش :تولید دانش، مدل‌سازی و تربیت متخصص

- دانشگاه‌ها و دانشکده‌ها
- پژوهشگاه‌ها و اندیشکده‌ها
- دانشجویان تحصیلات تکمیلی
- مؤسسات و نهادهای دارای مجوز آموزش

۹/۴ سازمان‌ها و بنگاه‌های اقتصادی

نقش **:**مصرف‌کننده خدمات حسابرسی

- سازمان‌های دولتی و عمومی
- بانک‌ها و مؤسسات مالی

- شرکت‌های بیمه
- اپراتورها و شرکت‌های فناوری
- سازمان‌های داده‌محور و پلتفرمی

۱۰. مجریان زیست‌بوم حسابرسی فناوری اطلاعت

۱۰/۱ حسابرسان و ارائه‌دهندگان خدمات حسابرسی فناوری اطلاعات

نقش :اجرای حسابرسی و اطمینان‌بخشی

- شرکت‌های حسابرسی فناوری اطلاعات
- حسابرسان داخلی و مستقل فناوری اطلاعات
- تیم‌های حاکمیت، ریسک، انطباق[۵۱]و امنیت اطلاعات
- مشاوران ریسک و انطباق فناوری

۱۰/۲ نهادهای اعتباردهی، ارزیابی و صدور گواهی

نقش :تضمین صلاحیت و کیفیت

- مراکز صدور گواهی امنیت اطلاعات
- نهادهای ارزیابی انطباق
- مراجع اعتباربخشی حرفه‌ای

۱۰/۳ ارائه‌دهندگان فناوری و ابزارهای حسابرسی

نقش :توانمندسازی فنی حسابرسی

- شرکت‌های دارای سکوهای حاکمیت، ریسک، انطباق
- تولیدکنندگان ابزارهای تحلیل داده و هوش مصنوعی

51 Governance, Risk, and Compliance

- ارائه‌دهندگان خدمات ابری
- شرکت‌های امنیت سایبری وSOC[52]
- شرکت‌های دارای مجوز کاروران امنیت سازمان فناوری اطلاعات

۱۰/۴ زیست‌بوم نوآوری و استارتاپ‌ها

نقش :تحول و نوآوری در حسابرسی فناوری اطلاعات

- استارتاپ‌های[۵۳] رگ‌تک و[۵۴] ساپ‌تک
- فین‌تک‌ها و اینشورتک‌ها
- شرکت‌های هوش مصنوعی و تحلیل داده

52 security operations center

53 Regulatory technology

54 Supervisory Technology

۱۱. پیشنهاد سازمان نصر جهت ایجاد زیست‌بوم حسابرسی فناوری اطلاعات

باتوجه‌به بررسی‌های انجام‌گرفته از لحاظ حقوقی و قوانین کشور، به نظر می‌رسد از دو مسیر ذیل جهت ایجاد زیست‌بوم حسابرسی فناوری اطلاعات می‌توان اقدام گردد. بدیهی است جهت تسریع، هم‌زمان هر دو پیشنهاد در حال پیگیری است.

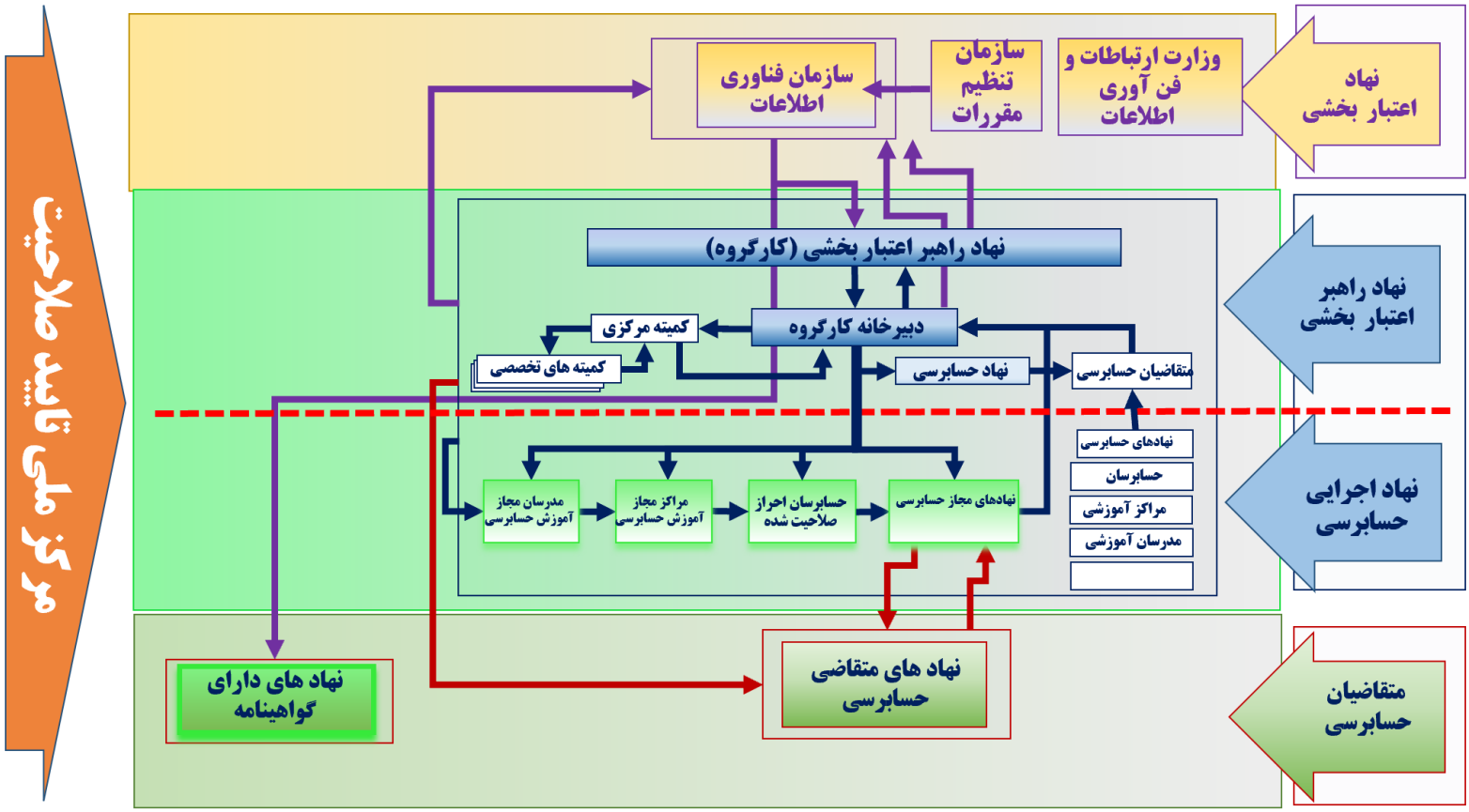
۱۱/۱ ایجاد، راهبری و اجرای نظام حسابرسی فناوری اطلاعات بر اساس تجربه DCAS

باتوجه‌به تجربه موفق نصر کشور در ایجاد، راهبری و اجرای نظام DCAS و مدل انعطاف‌پذیر طراحی شده می‌توان به‌راحتی بر اساس مدل DCAS ، با لحاظ الزامات و هم‌افزایی با ذی‌نفعان حوزه حسابرسی (ممیزی) فناوری اطلاعات اقدام به طراحی و اجرای آن نمود.

ازجمله قابلیت‌هایی که نصر را متمایز می‌نماید می‌توان به موارد ذیل اشاره کرد

- داشتن کمیسیون‌های تخصصی در حوزه حسابرسی فناوری اطلاعات، امنیت، زیرساخت، سرویس، بانکی، هوش مصنوعی، فین‌تک و...در سطح کشور
- تدوین آیین‌نامه‌های نظام‌مهندسی امنیت اطلاعات
- تشکیل کمیسیون حسابرسی فناوری اطلاعات
- داشتن روابط کلیدی با نهادهای تصمیم‌ساز و حاکمیتی
- داشتن مرکز داوری تخصصی
- اعضای حقیقی و حقوقی متخصص در حوزه‌های موردنیاز حسابرسی فا
- داشتن تفاهم‌نامه‌های کلیدی با سایر انجمن‌های مرتبط

لذا پیشنهاد می‌گردد سازمان فناوری اطلاعات باتوجه‌به جایگاه ضمن بررسی ماهیت موضوع نسبت به ارائه‌طریق برای نحوه ادامه مسیر از جنبه‌های حاکمیتی و قانونی اقدام نماید.



مدل پیشنهادی نظام حسابرسی فناوری اطلاعات مبتنی بر نظام DCAS

۱۱/۲ ایجاد نظام حسابرسی فناوری اطلاعات بر اساس ساختار سازمان اداری و استخدامی کشور، سازمان فناوری اطلاعات و افتای ریاست‌جمهوری

باتوجه‌به شفاف نبودن نهاد اعتباربخش برای حسابرسی فناوری اطلاعات در کشور، مسیر ذیل به نظر بهتر و در حال پیگیری است:

۱۱/۲/۱ سازمان اداری و استخدامی کشور

سازمان اداری و استخدامی کشور، نهاد حاکمیتی و سیاست‌گذار اصلی در حوزه مدیریت منابع انسانی، ساختار سازمانی و فرایندهای اداری در کشور است. وظایف این سازمان بر اساس «قانون مدیریت خدمات کشوری» و «قانون برنامه پنج‌ساله توسعه» تعیین می‌شود.

وظایف اصلی این سازمان در ۶ محور دسته‌بندی شده است:

- سیاست‌گذاری و برنامه‌ریزی کلان اداری
- مدیریت ساختار و تشکیلات دولت
- مدیریت منابع انسانی (استخدام و جذب)
- حقوق، دستمزد و مزایا
- آموزش و توسعه صلاحیت‌های مدیریتی
- نظارت و ارزیابی عملکرد

بر اساس وظایف فوق، در حال حاضر سازمان اداری و استخدامی تعداد ۷ عنوان شناسنامه مشاغل حوزه فناوری اطلاعات دستگاه‌های اجرایی را تدوین و ابلاغ نموده است که باتوجه‌به مذاکرات انجام‌گرفته، امکان اضافه‌شدن شناسنامه برای مشاغل حسابرسی فناوری اطلاعات است. مشاغل فعلی به شرح ذیل است (بر اساس بخشنامه شماره ۳۱۷۷۸ مورخ ۱۴۰۴/۰۴/۱۱):

- مدیر فناوری اطلاعات
- مهندس شبکه و زیرساخت
- مهندس امنیت فناوری اطلاعات
- متخصص علم داده
- طراح و راهبر خدمات و معماری سازمانی
- طراح و توسعه‌دهنده نرم‌افزار
- پشتیبان فناوری اطلاعات، سخت‌افزار و خدمات

لذا در اولین اقدام می‌بایست نسبت به تعریف شرح شغل‌های موردنیاز اقدام گردد.

۱۱/۲/۲ سازمان فناوری اطلاعات ایران

سازمان فناوری اطلاعات ایران، به‌عنوان یکی از سازمان‌های تابعه وزارت ارتباطات و فناوری اطلاعات، مسئول سیاست‌گذاری اجرایی، راهبری، توسعه و نظارت بر برنامه‌های ملی حوزه فناوری اطلاعات و دولت الکترونیکی در کشور است. این سازمان نقش‌محوری در توسعه زیرساخت‌های خدمات دیجیتال، یکپارچه‌سازی سامانه‌های دستگاه‌های اجرایی و ارتقای حکمرانی دیجیتال ایفا می‌کند.

اهم وظایف سازمان فناوری اطلاعات ایران

- توسعه و راهبری دولت الکترونیکی
- ایجاد و مدیریت زیرساخت‌های ملی فناوری اطلاعات
- یکپارچه‌سازی و تعامل‌پذیری سامانه‌ها
- تدوین استانداردها و الزامات فنی
- پایش و ارزیابی پروژه‌های فناوری اطلاعات
- توسعه اقتصاد دیجیتال
- ارزیابی امنیتی و اعتباربخشی محصولات و خدمات

پس از تهیه مشاغل موردنیاز حوزه حسابرسی فناوری اطلاعات مانند سایر مجوزهای افتا می‌توان از سازمان برای تأیید، احراز فنی و حراستی حسابرسان فا استفاده نمود.

در حال حاضر بر اساس اعلام رسمی سازمان فناوری اطلاعات ایران، مرکز مدیریت راهبردی افتای ریاست‌جمهوری، ازاین‌پس تنها مرجع صدور و استعلام مجوزهای افتا است، تمامی فرایندهای ارزیابی امنیتی و اعتباربخشی محصولات و خدمات مؤثر بر امنیت فضای مجازی، بر عهده آن مرکز خواهد بود؛ لذا متقاضیان دریافت مجوزهای جدید، تمدید و یا اصلاح پروانه باید موارد را از طریق آن مرکز پیگیری نمایند.

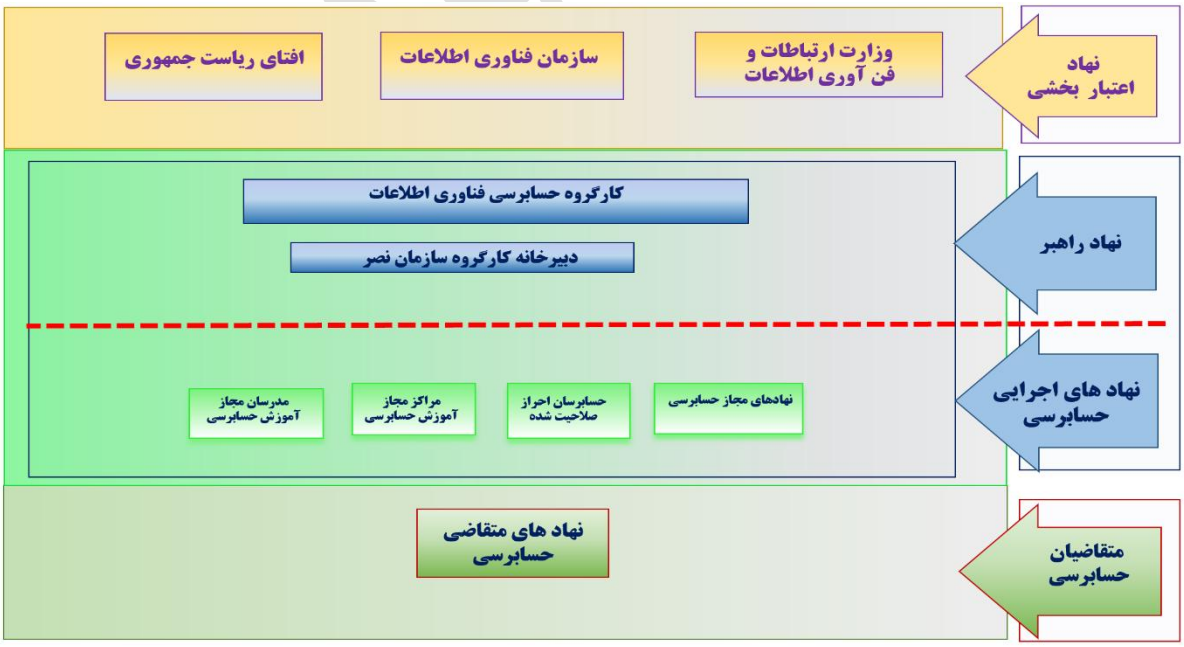
۱۱/۲/۳ مرکز مدیریت راهبردی افتای ریاست‌جمهوری

مرکز مدیریت راهبردی افتا، زیر نظر نهاد ریاست‌جمهوری، به‌عنوان مرجع حاکمیتی و سیاست‌گذار در حوزه امنیت فضای تولید و تبادل اطلاعات کشور فعالیت می‌کند. مأموریت اصلی این مرکز، صیانت از زیرساخت‌های حیاتی کشور در برابر تهدیدات سایبری، ارتقای سطح تاب‌آوری ملی و ساماندهی محصولات و خدمات امنیتی در سطح دستگاه‌های اجرایی است.

اهم وظایف و مأموریت‌های مرکز مدیریت راهبردی افتا:

- سیاست‌گذاری و راهبری راهبردی امنیت
- مدیریت مخاطرات و مقابله با حوادث سایبری
- ساماندهی و صدور پروانه برای محصولات و خدمات
- نظارت و بازرسی امنیتی
- ارتقای توانمندی‌های بومی و آموزش

در حال حاضر افتا در گرایش خدمات مدیریتی افتا، پروانه ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات دارد که بر اساس شرح شغل سازمان اداری و استخدامی می‌تواند پروانه حسابرسی فناوری اطلاعات را نیز صادر و شرکت‌های متقاضی مانند سایر گرایش‌ها، از این طریق مجوز فعالیت دریافت نمایند.



مدل پیشنهادی نظام حسابرسی فناوری اطلاعات

۱۲. پیشنهاد ایجاد شورای راهبری حسابرسی فناوری اطلاعات

جهت بهره‌مندی از نظرات، پیشنهادها، استفاده از خرد جمعی و پیشگیری از تضاد منافع با بررسی‌های انجام‌گرفته پیشنهاد می‌گردد نمایندگان نهاد و سازمان‌های ذیل که در این زیست‌بوم ذی‌نفع هستند در شورای راهبری عضویت داشته باشند:

- نماینده مرکز ملی فضای مجازی
- نماینده دیوان محاسبات
- نماینده سازمان اداری و استخدامی
- نماینده سازمان فناوری اطلاعات
- نماینده مرکز مدیریت راهبردی افتای ریاست‌جمهوری
- نماینده سازمان پدافند غیرعامل
- نماینده بانک مرکزی
- نماینده بیمه مرکزی
- نماینده سازمان حسابرسی یا جامعه حسابداران رسمی ایران
- نماینده انجمن علمی حسابرسی فناوری اطلاعات ایران
- نماینده سازمان نظام صنفی رایانه‌ای (متولی و راهبر)
- نماینده کمیسیون حسابرسی فناوری اطلاعات با پیشنهاد رئیس شورا به‌عنوان دبیر کارگروه

۱۳. نقشه راه برای پیاده‌سازی زیست‌بوم حسابرسی فناوری اطلاعات

الزامات اجرای «پیش‌نویس سند زیست‌بوم حسابرسی فناوری اطلاعات» به ترتیب پیشنهاد می‌گردد تا مبنای اقدام اجرایی و تصمیم‌گیری قرار گیرد.

۱۳/۱ استقرار ساختار حکمرانی و راهبری

- تشکیل شورای راهبری زیست‌بوم حسابرسی فناوری اطلاعات.
- تعیین دبیرخانه اجرایی و مسئولیت‌های آن.
- تعریف کارگروه‌های تخصصی شامل:
  - کارگروه استانداردها و چارچوب‌ها
  - کارگروه صلاحیت حرفه‌ای
  - کارگروه آموزش و توسعه حرفه‌ای
  - کارگروه نظارت و کنترل کیفیت
- تعیین سازوکار تصمیم‌گیری، گزارش‌دهی و نظارت.

۱۳/۲ تدوین چارچوب‌ها و استانداردهای حرفه‌ای

- شناسایی و تطبیق استانداردهای بین‌المللی مرتبط با حسابرسی فناوری اطلاعات.
- تدوین چارچوب ملی حسابرسی فناوری اطلاعات.
- تهیه دستورالعمل‌ها و راهنماهای حرفه‌ای برای اجرای حسابرسی.
- تعریف اصول اخلاق حرفه‌ای و الزامات رفتار حرفه‌ای.

۱۳/۳ تعریف نظام صلاحیت حرفه‌ای حسابرسان فناوری اطلاعات

- تدوین معیارهای احراز صلاحیت حرفه‌ای.
- تعریف مسیرهای حرفه‌ای برای متخصصان این حوزه.
- تعیین الزامات تحصیلی، تجربی و مهارتی.
- شناسایی و تطبیق گواهینامه‌های حرفه‌ای بین‌المللی با چارچوب ملی.

۱۳/۴ ایجاد نظام ارزیابی و تأیید صلاحیت

- طراحی فرایند ارزیابی متقاضیان.
- ایجاد سازوکار صدور گواهی حرفه‌ای.

- تعریف سطوح و رتبه‌های حرفه‌ای.
- تعیین فرایند تمدید و بازبینی صلاحیت‌ها.

۱۳/۵ ایجاد بانک اطلاعاتی متخصصان و حسابرسان فناوری اطلاعات

- طراحی و راه‌اندازی پایگاه‌داده متخصصان.
- ثبت اطلاعات حرفه‌ای، سوابق کاری و مهارت‌ها.
- ایجاد امکان جستجو و دسترسی برای سازمان‌ها و کارفرمایان.
- توسعه دایرکتوری حرفه‌ای برای معرفی خدمات تخصصی.

۱۳/۶ توسعه زیرساخت‌های آموزشی و توانمندسازی

- طراحی برنامه‌های آموزشی تخصصی در حوزه حسابرسی فناوری اطلاعات.
- همکاری با دانشگاه‌ها و مؤسسات آموزشی.
- برگزاری دوره‌های تخصصی و کارگاه‌های آموزشی.
- ایجاد نظام توسعه حرفه‌ای مستمر.

۱۳/۷ طراحی سازوکار ارجاع و اجرای مأموریت‌های حسابرسی

- تعریف فرایند درخواست خدمات حسابرسی فناوری اطلاعات.
- تعیین سازوکار انتخاب و ارجاع حسابرسان.
- تدوین دستورالعمل‌های اجرایی انجام مأموریت‌های حسابرسی.
- تعریف چارچوب تهیه و ارائه گزارش‌های حسابرسی.

۱۳/۸ استقرار نظام نظارت و کنترل کیفیت

- ایجاد سازوکار ارزیابی کیفیت گزارش‌های حسابرسی.
- تعریف فرایند بازبینی حرفه‌ای.
- تدوین شاخص‌های کیفیت خدمات حسابرسی.
- ایجاد سازوکار رسیدگی به شکایات و تخلفات حرفه‌ای.

۱۳/۹ توسعه همکاری‌های نهادی و بین سازمانی

- تعامل با نهادهای حاکمیتی و نظارتی.
- همکاری با سازمان‌های تخصصی و حرفه‌ای.

- ایجاد ارتباط با نهادهای بین‌المللی مرتبط.
- استفاده از ظرفیت انجمن‌ها و تشکل‌های تخصصی.

۱۳/۱۰ فرهنگ‌سازی و توسعه زیست‌بوم حرفه‌ای

- اطلاع‌رسانی درباره اهمیت حسابرسی فناوری اطلاعات.
- معرفی ظرفیت‌های حرفه‌ای این حوزه به سازمان‌ها.
- ایجاد بستر تعامل میان متخصصان، سازمان‌ها و نهادهای نظارتی.
- انتشار گزارش‌ها و تحلیل‌های تخصصی.

۱۳/۱۱ پایش، ارزیابی و بهبود مستمر

- تعریف شاخص‌های ارزیابی عملکرد زیست‌بوم.
- پایش مستمر اجرای برنامه‌ها و فعالیت‌ها.
- دریافت بازخورد از ذی‌نفعان.
- به‌روزرسانی مستمر چارچوب‌ها و استانداردها.

۱۴. نقش حاکمیت برای الزام‌آور شدن نظام حسابرسی فناوری اطلاعات

۱۴،۱ شناسایی رسمی شغل «حسابرسی فناوری اطلاعات»

نخستین اقدام حاکمیتی، به‌رسمیت‌شناختن این شغل در ساختار اداری کشور است.

اقدامات لازم:

- تدوین و ابلاغ شرح شغل‌های مرتبط با حسابرسی فناوری اطلاعات
- تعریف مسیر شغلی حسابرسی فناوری اطلاعات در دستگاه‌های اجرایی
- تعیین طبقه‌بندی مشاغل تخصصی

نهاد مسئول:

- سازمان اداری و استخدامی کشور

خروجی موردانتظار:

- ایجاد جایگاه سازمانی برای حسابرس فناوری اطلاعات در دستگاه‌ها.

۱۴،۲ الزام قانونی حسابرسی فناوری اطلاعات در دستگاه‌ها

برای ایجاد تقاضای واقعی، حسابرسی فناوری اطلاعات باید در برخی حوزه‌ها الزام قانونی پیدا کند.

اقدامات لازم:

- الزام دستگاه‌ها به انجام حسابرسی دوره‌ای سامانه‌های اطلاعاتی
- درج الزامات حسابرسی فناوری اطلاعات در آیین‌نامه‌های نظارتی
- تعریف حوزه‌های پرریسک که نیازمند حسابرسی هستند.

نهادهای مسئول:

- دیوان محاسبات کشور
- سازمان بازرسی کل کشور
- سازمان حسابرسی
- شورای‌عالی فضای مجازی

خروجی:

- تبدیل حسابرسی فناوری اطلاعات به بخشی از نظام نظارتی کشور.

۱۴/۳ ایجاد الزامات در حوزه بیمه سایبری

یکی از مهم‌ترین محرک‌های بازار حسابرسی فناوری اطلاعات در دنیا **بیمه سایبری** است.

اقدامات:

- تدوین آیین‌نامه بیمه سایبری
- الزام سازمان‌ها برای ارائه گزارش‌های ارزیابی امنیت و حسابرسی فناوری اطلاعات
- تعیین حداقل کنترل‌های امنیتی برای دریافت بیمه

نهادهای مسئول:

- بیمه مرکزی
- وزارت امور اقتصادی و دارایی

خروجی:

- ایجاد تقاضای گسترده برای ارزیابی و حسابرسی فناوری اطلاعات.

۱۴/۴ تدوین استانداردها و چارچوب‌های ملی حسابرسی فناوری اطلاعات

وجود چارچوب استاندارد برای اجرای حسابرسی فناوری اطلاعات ضروری است.

اقدامات:

- تدوین استاندارد ملی حسابرسی فناوری اطلاعات
- تطبیق با استانداردهای بین‌المللی مانند:
  - ISACA
  - COBIT
  - ISO 27001
  - IIA

نهادهای مسئول:

- سازمان ملی استاندارد
- سازمان حسابرسی

- نهادهای تخصصی حرفه‌ای

خروجی:

- ایجاد چارچوب رسمی اجرای حسابرسی.

۱۴/۵ ایجاد نظام صلاحیت حرفه‌ای حسابرسان فناوری اطلاعات

برای تضمین کیفیت خدمات، باید نظام ارزیابی صلاحیت ایجاد شود.

اقدامات:

- تعریف گواهینامه حرفه‌ای ملی حسابرسی فناوری اطلاعات
- پذیرش و تطبیق گواهینامه‌های بین‌المللی
- ایجاد فرایند ارزیابی و تأیید صلاحیت

نهادهای مسئول:

- نهاد حرفه‌ای تخصصی
- وزارت علوم
- سازمان نظام صنفی رایانه‌ای

خروجی:

- ایجاد جامعه حرفه‌ای معتبر حسابرسان فناوری اطلاعات.

۱۴/۶ الزام حسابرسی فناوری اطلاعات در پروژه‌های دولتی

در بسیاری از کشورها، پروژه‌های فناوری اطلاعات دولتی بدون حسابرسی مستقل تأیید نمی‌شوند.

اقدامات:

- الزام انجام حسابرسی فناوری اطلاعات قبل از تحویل پروژه‌های فناوری اطلاعات.
- تعریف مرحله حسابرسی در چرخه پروژه‌های فناوری اطلاعات.
- بررسی انطباق امنیتی و کنترلی.

نهادهای مسئول:

- سازمان برنامه‌وبودجه
- مرکز ملی فضای مجازی
- وزارت ارتباطات و فناوری اطلاعات

خروجی:

- کنترل کیفیت پروژه‌های ملی فناوری اطلاعات.

۱۴٫۷ ایجاد سازوکار نظارت و کنترل کیفیت

برای حفظ اعتبار این نظام باید نظارت حرفه‌ای برقرار باشد.

اقدامات:

- ایجاد نظام کنترل کیفیت خدمات حسابرسی فناوری اطلاعات
- تعریف فرایند بازبینی هم‌تراز یا نظارت همتایان
- ایجاد نظام رسیدگی به تخلفات حرفه‌ای

نهادهای مسئول:

- نهاد حرفه‌ای تخصصی
- نهادهای نظارتی

خروجی:

- افزایش اعتماد سازمان‌ها به خدمات حسابرسی.

۱۴٫۸ ایجاد مشوق‌های اقتصادی برای سازمان‌ها

در کنار الزام، ایجاد مشوق نیز ضروری است.

اقدامات:

- اعطای تخفیف بیمه سایبری برای سازمان‌های دارای گزارش حسابرسی فناوری اطلاعات
- امتیاز در رتبه‌بندی امنیت سایبری
- مزایای مالیاتی برای سرمایه‌گذاری در امنیت و حسابرسی

نهادهای مسئول:

- وزارت اقتصاد
- بیمه مرکزی
- سازمان امور مالیاتی

خروجی:

- افزایش انگیزه سازمان‌ها برای استفاده از خدمات حسابرسی فناوری اطلاعات.

پیوست شماره ۱ قلمرو حوزه حسابرسی فناوری اطلاعات

پیوست شماره ۲ تاریخچه حسابرسی فناوری اطلاعات

پیوست شماره ۳ نیازها و الزامات فعلی حسابرسی در عصر دیجیتال

پیوست شماره ۴ چالش‌های قابل‌توجه حسابرسی فناوری اطلاعات

پیوست شماره ۵ خلاصه مراجع و فرایندهای مورد استفاده جهت پیاده‌سازی نظام فوق

پیوست شماره ۶ جایگاه CITP و تطبیق با سایر گواهینامه‌های حرفه‌ای در حسابرسی فناوری اطلاعات

پیوست شماره ۷ شرح مشاغل

پیوست شماره ۸ اصطلاحات و تعاریف