



## سند ایجاد زیست‌بوم حسابرسی فناوری اطلاعات

تاریخ ویرایش	تعداد صفحات	نسخه
خرداد ۱۴۰۵	۲۸ (فاقد پیوست)	۱.۹

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 ۱.۹

## فهرست مطالب

۱. قلمرو	۳
۲. اصطلاحات و تعاریف	۴
۳. تاریخچه	۵
۴. برخی از حوزه‌های حسابرسی فناوری اطلاعات	۷
۵. جایگاه «نظام حسابرسی فناوری اطلاعات» از منظر نهادهای بین‌المللی و حرفه‌ای	۱۰
۶. نیاز و الزامات فعلی حسابرسی فناوری اطلاعات	۱۵
۷. چالش‌های قابل توجه	۱۶
۸. جایگاه سازمان نظام صنفی رایانه‌ای کشور	۱۷
۹. ذی‌نفعان زیست‌بوم حسابرسی فناوری	۱۸
۱۰. مجریان زیست‌بوم حسابرسی فناوری اطلاعات	۲۰
۱۱. پیشنهاد سازمان نصر جهت ایجاد زیست‌بوم حسابرسی فناوری اطلاعات	۲۲
۱۲. پیشنهاد ایجاد کارگروه حسابرسی فناوری اطلاعات	۲۷
پیوست شماره ۱ قلمرو حوزه حسابرسی فناوری اطلاعات	۲۸
پیوست شماره ۲ تاریخچه حسابرسی فناوری اطلاعات	۲۸
پیوست شماره ۳ نیازها و الزامات فعلی حسابرسی در عصر دیجیتال	۲۸
پیوست شماره ۴ چالش‌های قابل توجه حسابرسی فناوری اطلاعات	۲۸
پیوست شماره ۵ خلاصه مراجع و فرایندهای مورد استفاده جهت پیاده‌سازی نظام فوق	۲۸
پیوست شماره ۶ جایگاه CITP و تطبیق با سایر گواهینامه‌های حرفه‌ای در حسابرسی فناوری اطلاعات	۲۸
پیوست شماره ۷ شرح مشاغل	۲۸
پیوست شماره ۸ اصطلاحات و تعاریف	۲۸

در عصر دیجیتال کنونی، فناوری اطلاعات و ارتباطات<sup>۱</sup> 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، نه تنها 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<sup>۲</sup> 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

---

<sup>1</sup> Information and Communication Technologies

<sup>2</sup> Information System

- کنترل‌های عمومی و کاربردی فناوری اطلاعات
  - 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 خدمات‌گیرندگان 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: تشکیلی 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 درون‌داده‌ها استفاده کند.
- ۲/۳ شواهد<sup>۳</sup>: سوابق، اظهارات گویای واقعیت یا سایر اطلاعاتی که به معیارهای ممیزی مرتبط بوده و قابل راستی‌آزمایی باشند.
- ۲/۴ شواهد عینی<sup>۴</sup>: اطلاعات، سوابق، مشاهدات یا نتایج اندازه‌گیری قابل راستی‌آزمایی که به‌طور واقعی و مستقل از قضاوت شخصی، انطباق یا عدم انطباق با یک الزام را اثبات می‌کنند.
- ۲/۵ معیارهای ممیزی<sup>۵</sup>: 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<sup>۶</sup>: ممیزی فرایندی نظام‌یافته، مستقل و مدون برای به‌دست‌آوردن شواهد عینی و ارزیابی آن به‌صورت عینی برای تعیین میزان که معیارهای ممیزی برآورده می‌شوند.

<sup>3</sup> Evidence

<sup>4</sup> Objective Evidence

<sup>5</sup> Audit Criteria

<sup>6</sup> Audit(ISO 19011:2018)

۲/۷ **حسابرسی فناوری اطلاعات**<sup>۷</sup> حسابرسی فناوری اطلاعات فرایندی رسمی، نظام‌مند و مستقل برای بررسی و راستی‌آزمایی کنترل‌ها، فرایندها، سیستم‌ها و اطلاعات مبتنی بر فناوری اطلاعات است که باهدف اطمینان بخشی 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<sup>۸</sup> (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<sup>۹</sup>، انجمن حسابرسان داخلی آمریکا<sup>۱۰</sup>، انجمن حسابداران رسمی آمریکا (AICPA)<sup>۱۱</sup> 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 می‌باشد.

#### 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<sup>۱۲</sup> با مصوبه مجلس شورای اسلامی تأسیس شده است.

7 Audit (ISACA Glossary)

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

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

از دهه ۱۳۹۰ به بعد، سازمان حسابرسی و جامعه حسابداران رسمی، توجه بیشتری به کنترل‌های عمومی فناوری اطلاعات<sup>13</sup> ITGC و چارچوب‌های نظارتی مانند COBIT، ISO 27001<sup>14</sup> و ITIL نشان دادند.

- دیوان محاسبات کشور  
هدف دیوان محاسبات کشور با توجه به اصول مندرج در قانون اساسی جمهوری اسلامی ایران عبارت است از اعمال کنترل و نظارت مستمر مالی به منظور پاسداری از بیت المال از طریق:  
الف - کنترل عملیات و فعالیتهای مالی کلیه وزارتخانه ها، مؤسسات، شرکتهای دولتی و سایر دستگاههایی که به نحوی از انحاء از بودجه کل کشور استفاده می کنند.  
ب - بررسی و حسابرسی وجوه مصرف شده و درآمدها و سایر منابع تأمین اعتبار در ارتباط با سیاستهای مالی تعیین شده در بودجه مصوب با توجه به گزارش عملیاتی و محاسباتی مأخوذه از دستگاههای مربوطه.
- طی سال‌های اخیر انجمن علمی حسابرسی فناوری اطلاعات ایران<sup>15</sup> توسط پیش‌کسوت‌ها و اساتید حسابداری، کامپیوتر، 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 باتوجه به 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:

13 Information Technology General Controls

14 Information Technology Infrastructure Library

15 Iranian Information Technology Auditing Scientific Association

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

#### ۴. 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 قابل اعتماد 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 برآورد شدن 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 کسب و کار (BCM<sup>۱۶</sup>) پشتیبانی می‌کند.

## ۴/۲ حسابرسی انطباق (رعایت)<sup>۱۷</sup>

این حسابرسی از جمله شامل آزمون کنترل‌ها برای نشان دادن پایبندی<sup>۱۸</sup> به مقررات، استانداردها یا رویه‌های خاص صنعت است.

## ۴/۳ حسابرسی مالی

حسابرسی مالی، اطمینان بخشی در مورد<sup>۱۹</sup> گزارشگری مالی سازمان‌ها است. اغلب شامل آزمون‌های دقیق کنترل و محتوا<sup>۲۰</sup> 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<sup>۲۱</sup> اطلاعات مالی مربوط می‌شود.<sup>۲۲</sup>

## 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<sup>۲۳</sup> 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.

---

17 Compliance Audit

18 Adherence

19 Accuracy

20 Substantive

21 Reliability

22 CISA

23 Configuration

## ۴/۷ حسابرسی تقلب

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

حسابرسان اغلب از ابزارها و فن‌های خاص تحلیل داده‌ها برای کشف طرح‌های تقلب و بی‌نظمی‌های<sup>۲۴</sup> تجاری استفاده می‌کنند.

## ۴/۸ حسابرسی جرم‌شناسی (دادگاهی) رایانه‌ای<sup>۲۵</sup>

تحقیق و رسیدگی است که شامل تجزیه و تحلیل دستگاه‌های محاسباتی الکترونیکی<sup>۲۶</sup> 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<sup>۲۷</sup>

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، هم‌راستایی، بلوغ و ارزش‌آفرینی آن را در تحقق اهداف کسب‌وکار و الزامات حاکمیت دیجیتال بررسی می‌نماید.

## ۴/۱۱ حسابرسی فناوری‌های نوظهور

مثل اینترنت اشیا<sup>۲۸</sup>، هوش مصنوعی<sup>۲۹</sup>، بلاک‌چین، رمز ارز و فضای ابری

24 irregularities

25 Forensic audit

26 electronic computing

27 Readiness assessment

28 Internet of Things

29 Artificial intelligence

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

### ۵/۱ انجمن حسابداران رسمی آمریکا (AICPA)

ارائه‌دهنده گواهینامه حرفه‌ای بین‌المللی در حوزه بین رشته‌ای حسابرسی/حسابداری، فناوری اطلاعات و تحلیل داده به نام CITP<sup>۳۰</sup> 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 برنامه ریزی منابع سازمانی (ERP / Cloud Systems)

### ۵/۱/۲ مخاطبان اصلی

- حسابرسان (داخلی و مستقل) با تمرکز فناوری اطلاعات
- حسابداران رسمی CPA<sup>۳۱</sup>

- مشاوران ریسک و اطمینان بخشی
- مدیران GRC و تحول دیجیتال

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

### ۵/۱/۳ ساختار CPA Evolution

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

#### الف) Core (همه داوطلبان)

- حسابداری و گواهی دهی (AUD)،
- حسابداری و گزارشگری مالی (FAR)، و
- قوانین مالیات و مقررات (REG).

#### ب) Discipline (رشته انتخابی)

داوطلب تنها یکی از سه مسیر تخصصی را می گذراند:

- تحلیل کسب و کار و گزارشگری (BAR)،
- سیستم های اطلاعاتی و کنترل ها (ISC)، و
- برنامه ریزی 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 نقش ها و فرصت های شغلی فناوری محور

- سرپرست حسابداری فناوری اطلاعات (IT Audit Lead)
- مشاوره فناوری کسب و کار (Technology Advisory)
- تحلیلگر داده ها برای تصمیم گیری مالی (Data & Analytics Advisor)
- مشاور سامانه های سازمانی و ERP (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<sup>۳۲</sup>
- ارزیابی کنترل‌های برنامه‌های کاربردی<sup>۳۳</sup>
- 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<sup>۳۴</sup> قرار دارد.
- حسابرسان فناوری اطلاعات ممکن است به صورت تیم تخصصی در داخل واحد حسابرسی داخلی یا متخصصان فناوری اطلاعات در تیم‌های حسابرسی فعالیت کنند.
- گزارش‌دهی آن‌ها معمولاً به مدیر ارشد حسابرسی<sup>۳۵</sup> و در نهایت کمیته حسابرسی هیئت‌مدیره انجام می‌شود.

32 ITGC

33 Application Controls

34 Internal Audit Activity

35 Chief Audit Executive – CAE

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 اطمینان بخشی 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<sup>۳۷</sup> (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<sup>۳۸</sup> 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 به صورت کارآمد، ایمن و قابل اعتماد 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<sup>۳۹</sup> چارچوب حاکمیت و مدیریت فناوری اطلاعات سازمانی<sup>۴۰</sup> 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<sup>۴۱</sup>

- حاکمیت به‌درستی مستقر شده است؟
- آیا اهداف فناوری اطلاعات با استراتژی‌های کسب‌وکار هم‌سو<sup>۴۲</sup> هستند؟
- آیا ارزش‌آفرینی<sup>۴۳</sup> از طریق فناوری اطلاعات محقق شده است؟

۵/۳/۲ به‌عنوان ستون اصلی اطمینان‌بخشی

طبق چارچوب ITAF، حسابرسی فناوری اطلاعات در جایگاه “اطمینان‌بخشی مستقل<sup>۴۴</sup>” قرار دارد.

- وظیفه: ارزیابی اینکه آیا کنترل‌های طراحی‌شده در سیستم‌های اطلاعاتی و فرایندهای فناوری اطلاعات، به‌طور 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<sup>۴۵</sup> 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<sup>۴۶</sup> 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<sup>۴۷</sup>، کویت<sup>۴۸</sup> 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 عملیاتی‌سازیان
- ارائه اطمینان معقول نسبت به حاکمیت فناوری اطلاعات و هم‌راستایی راهبردها، ساختارها و فرایندهای فناوری اطلاعات با اهداف کلان و عملیاتی سازمان.

#### ۶. 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 ثقل 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 رضایت مندی ذی‌نفعان از خدمات دریافتی
- تکمیل چرخه کسب و کارهای مرتبط با حوزه‌های امنیت، ممیزی و بیمه سایبری

## ۶/۲ الزامات فعلی حسابرسی فناوری اطلاعات

- الزامات حاکمیتی و قانونی
- الزامات حرفه‌ای و استاندارد
- 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<sup>۴۹</sup>
- حسابرسی مبتنی بر ریسک
- حسابرسی مبتنی بر ریسک سایبری<sup>۵۰</sup>
- یکپارچگی با GRC

## ۷. چالش‌های قابل توجه

### 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
- 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 بلنک 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.

## ۸,۴ 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 علمی کاربردی برای تأمین نیروی انسانی ماهر در اقتصاد دیجیتال یا سازمان فنی و حرفه‌ای و اخیراً دانشگاه ملی مهارت

## ۸,۶ 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 برنامه‌بودجه کشور
- دیوان محاسبات
- سازمان حسابرسی

- بانک مرکزی، بیمه مرکزی، سازمان بورس
- مرکز ملی فضای مجازی
- مرکز افتای ریاست جمهوری
- 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 اطلاعات

### ۱۰/۱ حسابرسیان و ارائهدهندگان خدمات حسابرسی فناوری اطلاعات

نقش: اجرای حسابرسی و اطمینانبخشی

- شرکتهای حسابرسی فناوری اطلاعات
- حسابرسیان داخلی و مستقل فناوری اطلاعات
- تیمهای حاکمیت، ریسک، انطباق<sup>۵۱</sup> 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 سکوهایی حاکمیت، ریسک، انطباق
- تولیدکنندگان ابزارهای تحلیل داده و هوش مصنوعی

- ارائه‌دهندگان خدمات ابری
- شرکت‌های امنیت سایبری و SOC<sup>52</sup>
- شرکت‌های دارای مجوز کاروران امنیت سازمان فناوری اطلاعات

#### ۱۰/۴ زیست‌بوم نوآوری و استارت‌آپ‌ها

نقش: تحول و نوآوری در حسابرسی فناوری اطلاعات

- استارت‌آپ‌های<sup>۵۳</sup> رگ‌تک و<sup>۵۴</sup> 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

باتوجه به 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.

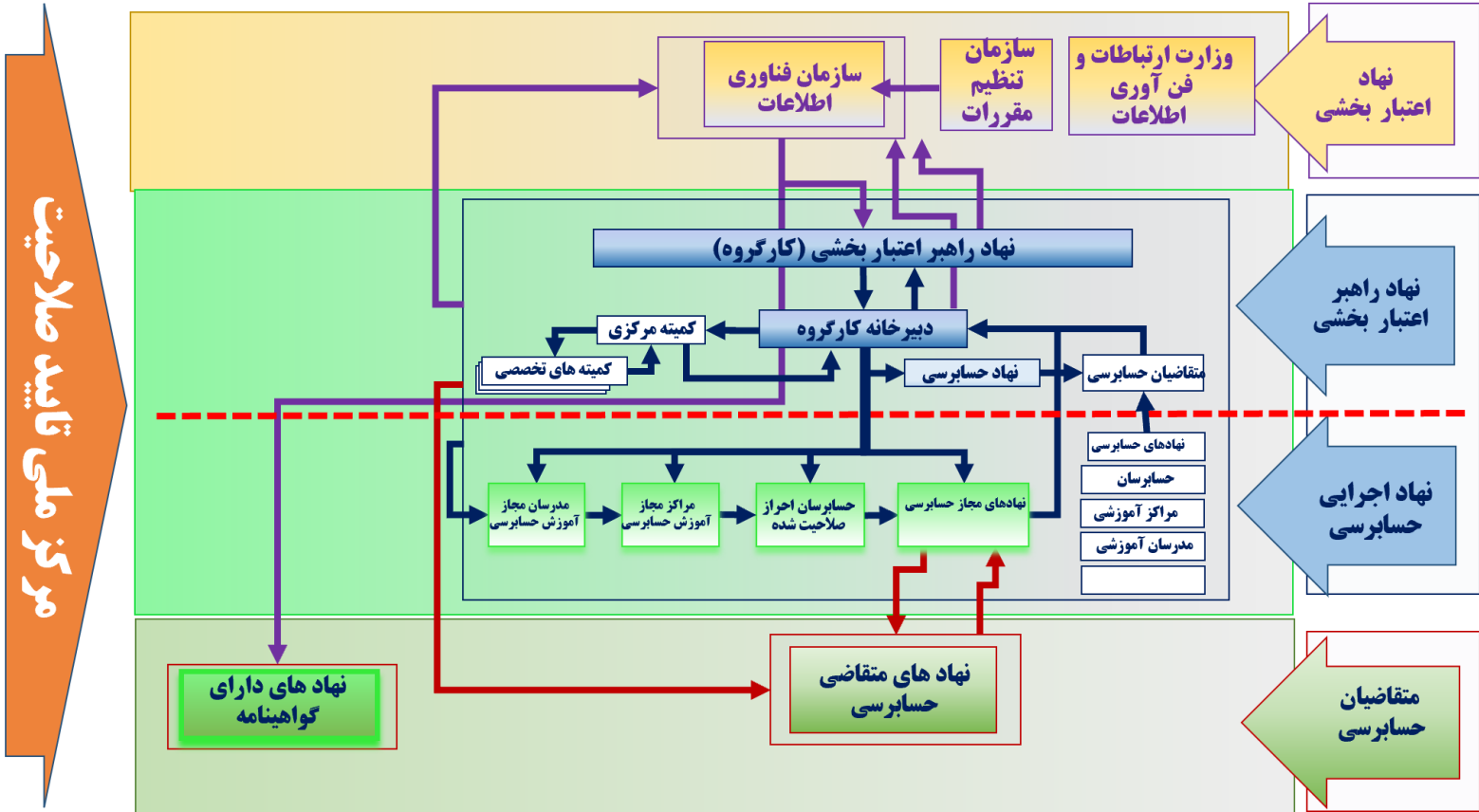
### ۱۱/۱ ایجاد، راهبری و اجرای نظام حسابرسی فناوری اطلاعات بر اساس تجربه DCAS

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

از جمله 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 باتوجه به جایگاه ضمن بررسی ماهیت موضوع نسبت به ارائه‌طریق برای نحوه ادامه مسیر از جنبه‌های حاکمیتی و قانونی اقدام نماید.



مدل پیشنهادی نظام حساسی 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 ریاست جمهوری

باتوجه به 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 سیاست گذار 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 پنج ساله توسعه» تعیین می شود.

وظایف اصلی این سازمان در ۶ محور دسته بندی شده است:

- سیاست گذاری و برنامه ریزی کلان اداری
- مدیریت ساختار و تشکیلات دولت
- مدیریت منابع انسانی (استخدام و جذب)
- حقوق، دستمزد و مزایا
- آموزش و توسعه صلاحیت های مدیریتی
- نظارت و ارزیابی عملکرد

بر اساس وظایف فوق، در حال حاضر سازمان اداری و استخدامی تعداد ۷ عنوان شناسنامه مشاغل حوزه فناوری اطلاعات دستگاه های اجرایی را تدوین و ابلاغ نموده است که باتوجه به مذاکرات انجام گرفته، امکان اضافه شدن 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 توسعه دهنده نرم افزار
- پشتیبان فناوری اطلاعات، سخت افزار 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 نقش محوری 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 ریاست جمهوری، از این پس 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.

مرکز مدیریت راهبردی افتا، زیر نظر نهاد ریاست جمهوری، به عنوان 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:

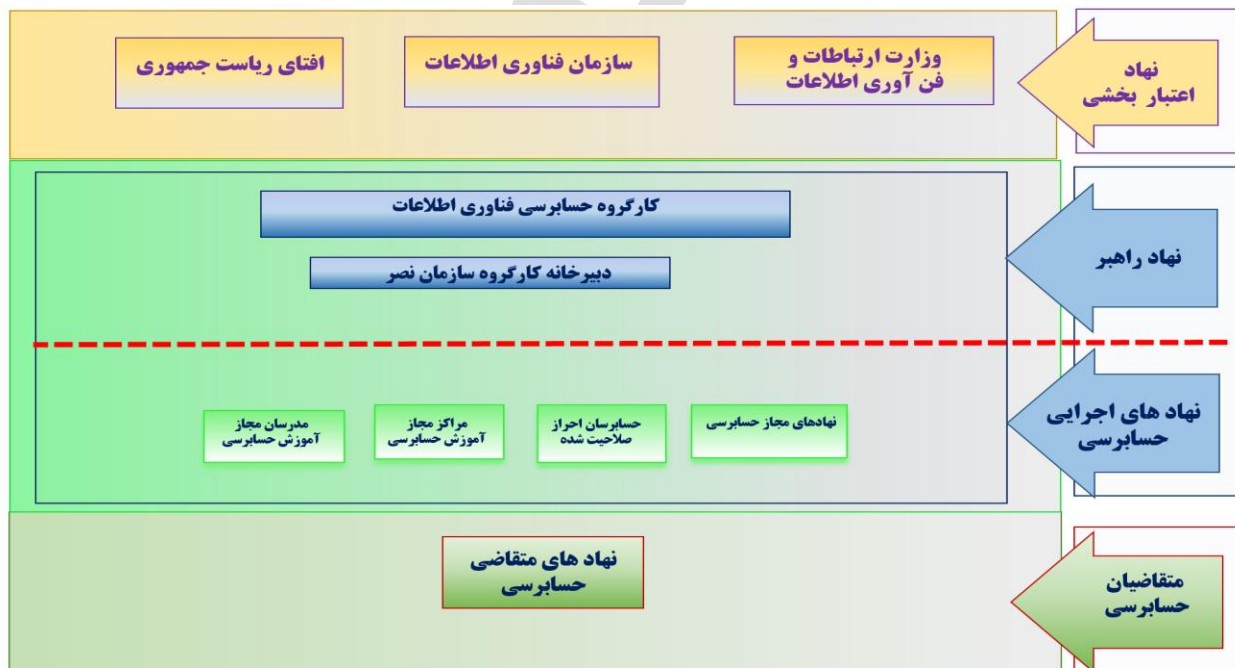
- سیاست‌گذاری و راهبری راهبردی امنیت
- مدیریت مخاطرات و مقابله با حوادث سایبری
- ساماندهی و صدور پروانه برای محصولات و خدمات
- نظارت و بازرسی امنیتی
- ارتقای توانمندی‌های بومی و آموزش

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.

## ۱۲. پیشنهاد ایجاد کارگروه 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 کارگروه عضویت داشته باشند:

- مرکز ملی فضای مجازی
- نماینده دیوان محاسبات
- نماینده سازمان فناوری اطلاعات
- نماینده سازمان افتا
- نماینده سازمان پدافند
- 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)
- یک نفر نماینده از کمیسیون حسابرسی فناوری اطلاعات با پیشنهاد رئیس کارگروه به‌عنوان دبیر



مدل پیشنهادی نظام 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 قابل توجه 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