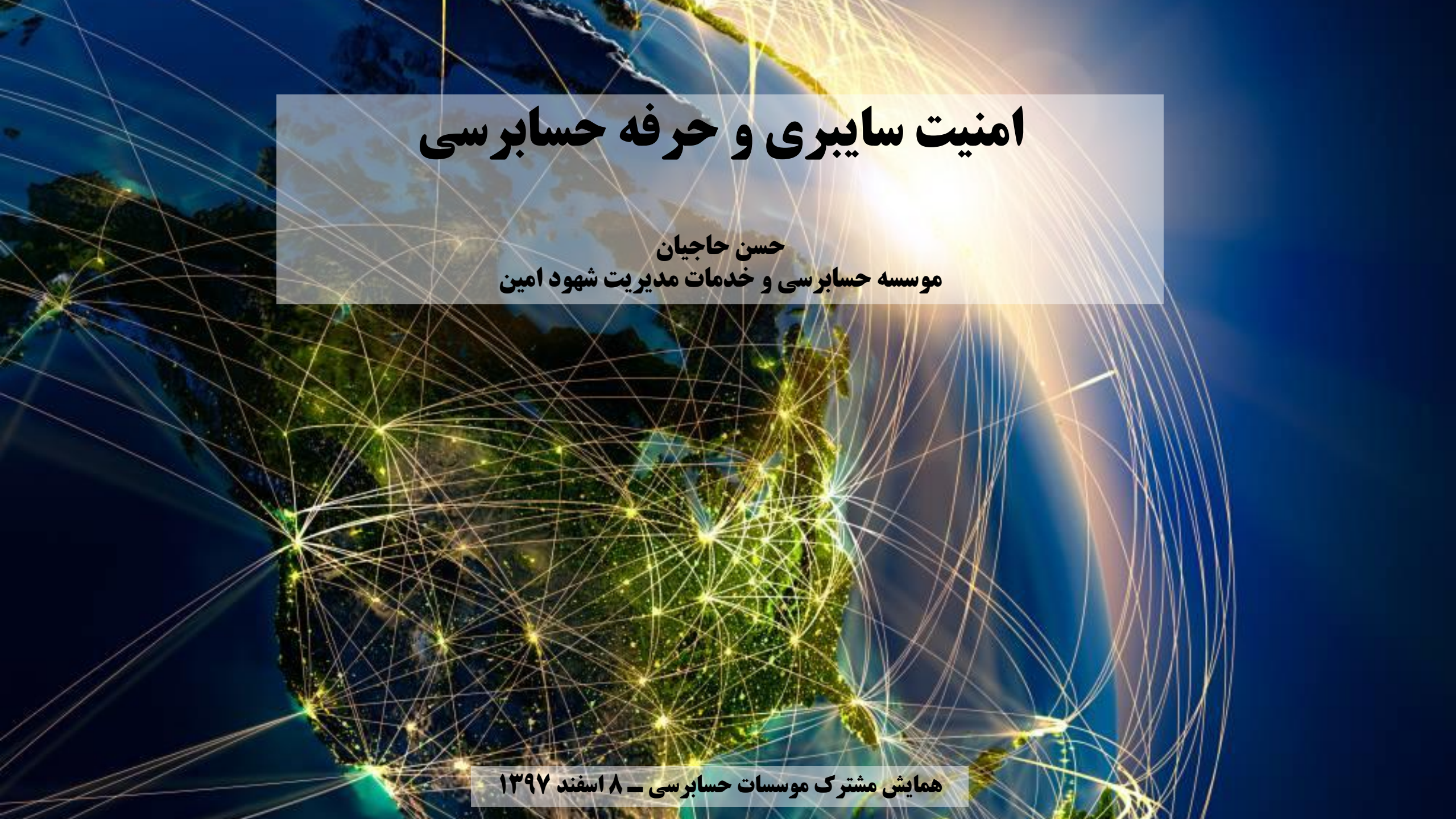


امنیت سایبری و حرفه حسابرسی

حسن حاجیان
موسسه حسابرسی و خدمات مدیریت شهود امین

همایش مشترک موسسات حسابرسی ــ ۸ اسفند ۱۳۹۷

سایبر (Cyber)؟

فضای سایبری (Cyberspace)

شهر سایبری (Cybercity)

شهروند سایبری (Cybercitizen)

ارتش سایبری (Cyberarmy)

جنگ سایبری (Cyber War)

حمله سایبری (Cyber-attack)

جُرم سایبری (Cyber crime)

امنیت سایبری (Cybersecurity)

امنیت سایبری، به حفاظت از سیستم‌های اطلاعاتی، شامل سخت‌افزار، نرم‌افزار و اطلاعات، در برابر سرقت یا صدمه گفته می‌شود.

مراحل حملات سایبری

استانداردهای حسابرسی صورتهای مالی و فناوری اطلاعات

فناوری اطلاعات، کنترلهای داخلی واحد تجاری را در معرض خطرهای خاصی همچون موارد زیر قرار می دهد:

- اعتماد به سیستمها یا برنامه هایی که داده ها را نادرست پردازش می کنند، داده های نادرست را پردازش می کنند، یا هردو.
- دسترسی غیر مجاز به داده ها، که ممکن است موجب ازبین رفتن داده ها یا تغییر نابجا در داده ها، شامل ثبت معاملات غیر مجاز یا واهی، یا ثبت نادرست معاملات شود.
- احتمال برخورداری کارکنان فناوری اطلاعات از امکان دسترسی بیش از حد نیاز برای انجام وظایف خود و از اینرو، نقض تفکیک وظایف.
- تغییرات غیر مجاز داده ها در پرونده های اصلی.
- تغییرات غیر مجاز در سیستمها یا برنامه ها.
- قصور در انجام تغییرات لازم در سیستمها و برنامه ها.
- دخالتهای دستی نا مناسب.
- احتمال از دست رفتن داده ها یا ناتوانی در دسترسی به داده های مورد نیاز. (بند ت ـ ٦٣ استاندارد ٣١٥)

استانداردهای حسابرسی صورتهای مالی و فناوری اطلاعات

استفاده از فناوری اطلاعات، نحوه اعمال فعالیتهای کنترلی را تحت تاثیر قرار می دهد. از نظر حسابرس، کنترلهای حاکم بر سیستمهای اطلاعاتی هنگامی موثر است که درستی اطلاعات و امنیت داده های مورد پردازش در این سیستمها را حفظ کند و شامل کنترلهای اثربخش عمومی و کاربردی فناوری اطلاعات باشد. (بند ت ـ ۱۰۳ استاندارد ۳۱۵)

کنترلهای عمومی فناوری اطلاعات، سیاستها و روشهایی است که به نرم افزارهای کاربردی متعددی مربوط می شود و از کارکرد موثر کنترلهای کاربردی پشتیبانی می کند. کنترلهای عمومی در محیط رایانه های بزرگ، رایانه های متوسط و کاربران نهایی کاربرد دارد. کنترلهای عمومی فناوری اطلاعات که درستی اطلاعات و امنیت داده ها را حفظ می کنند معمولا شامل کنترلهای مربوط به موارد زیر است:

- مرکز داده ها و عملیات شبکه
- تحصیل، تغییر و نگهداری نرم افزار سیستم
- تغییر برنامه
- امنیت دسترسی
- تحصیل، توسعه و نگهداری سیستم کاربردی (بند ت ـ ۱۰٤ استاندارد ۳۱۵)

کنترلهای کاربردی، روشهای دستی یا خودکاری است که معمولا در سطح فرآیندهای تجاری اجرا می شود و برای پردازش معاملات توسط نرم افزارهای کاربردی خاص بکار می رود. کنترلهای کاربردی می تواند ماهیت پیشگیری کنندگی یا کشف کنندگی داشته باشد و برای حصول اطمینان از درستی سوابق حسابداری طراحی می شود. از این رو، کنترلهای کاربردی به روشهای مورد استفاده در انجام، ثبت، پردازش، و گزارش معاملات یا سایر اطلاعات مالی مربوط می شود. به کمک این کنترلها اطمینان حاصل می شود که معاملات انجام شده، به تصویب رسیده و بطور کامل و درست ثبت و پردازش شده اند.
(بند ت ـ ۱۰۵ استاندارد ۳۱۵)

استانداردهای حسابرسی داخلی و فناوری اطلاعات

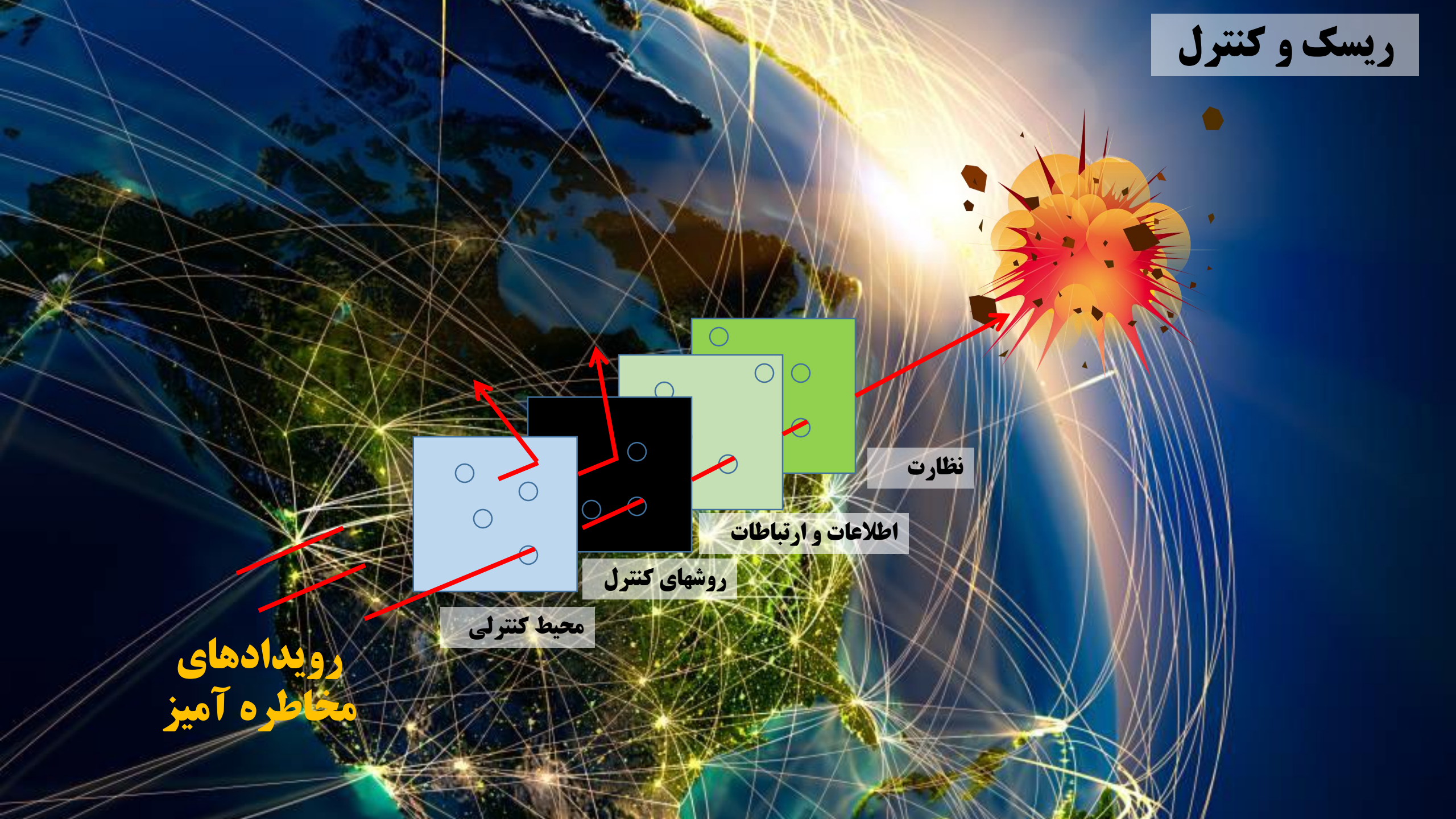
حسابرس داخلی باید از دانش کافی درباره ریسکهای مهم حوزه فناوری اطلاعات و کنترلها و تکنیکهای حسابرسی مبتنی بر فناوری، برای اجرای وظایف محول در این حوزه برخوردار باشد. (استاندارد ۱۲۱۰-A3)

حسابرس داخلی باید ارزیابی کند که آیا فرآیند نظام راهبری فناوری اطلاعات سازمان اجرا می شود و هدفها و راهبردهای سازمان را پشتیبانی می کند؟ (استاندارد ۲۱۱۰-A2)

حسابرس داخلی، باید ریسکهای پیش روی سیستمهای اطلاعات سازمان را ارزیابی کند. (استاندارد ۲۱۲۰-A1)

حسابرس داخلی، باید کفایت و اثر بخشی کنترلها را در واکنش به ریسکهای فناوری اطلاعات سازمان ارزیابی کند. (استاندارد ۲۱۳۰-A1)

ریسک و کنترل


نظارت
اطلاعات و ارتباطات
روشهای کنترل
محیط کنترلی
رویدادهای
مخاطره آمیز

آنچه مورد تهدید است، دارائیهای رایانه ای است.

سخت افزار(Hardware)

نرم افزار (Software)

داده ها (Data)

هدف تمهیداتِ امنیت داده ها :

- حفظ وِیژگی محرمانگی داده ها (Confidentiality)
- حفظ ویژگی بی عیبی داده ها (Integrity)
- حفظ ویژگی در دسترس بودن داده ها (Availibility)

جرائم رایانه ای (طبق قانون مصوب ۱۳۸۸/۳/۵) :

جرائم علیه محرمانگی داده ها و سیستم های رایانه ای و مخابراتی

- دسترسی غیرمجاز
- شنود غیرمجاز
- جاسوسی رایانه ای

جرائم علیه صحت و تمامیت داده ها و سامانه های رایانه ای و مخابراتی

- جعل رایانه ای
- تخریب و اخلال در داده ها یا سیستم های رایانه ای و مخابراتی

سرقت و کلاهبرداری مرتبط با رایانه

جرایم علیه عفت و اخلاق عمومی

هتک حیثیت و نشر اکاذیب

سایر جرائم مرتبط با این حوزه

راهکار مقابله با تهدیدهای امنیتیِ دارائیهای رایانه ای، برقراری کنترلهای امنیتی است.

کنترلهای پیشگیرانه

کنترلهای کشف کننده

کنترلهای اصلاح کننده

کنترلهای ترمیمی

کنترلهای قانونی

کنترلهای مدیریتی

کنترلهای فیزیکی

کنترلهای فنی

ماده ۱ قانون جرائم رایانه ای:

هرکس به طور غیرمجاز به داده ها یا سامانه های رایانه ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به ..... محکوم خواهد شد.

اثر بخشی تدابیر امنیتی، مستلزم برخورداری از طرح امنیتی است. حسابرسان نباید نسبت به نبود طرح امنیتیِ دارائیهای رایانه ای بی تفاوت باشند؛ بلکه لازم است ضمن اطلاع رسانی پیامدهای آن به ارکان راهبری، هنگام تعیین راهبرد حسابرسی نیز به این مهم توجه کنند.

سوالات موثر در ارزیابی طرح امنیتی دارائیهای رایانه ای:

آیا دارائیهای رایانه ای مستلزمِ حفاظت ویژه، مشخص شده اند؟
آیا عوامل تهدید کننده دارائیهای مستلزم حفاظت ویژه مشخص شده است؟
آیا میزان تلاش و منابع مالی توجیه پذیربرای تامین امنیت دارائیهای رایانه ای مشخص شده است؟
آیا روشهای واکنش سریع نسبت به حمله ها / تهدیدها تعریف شده است؟
آیا رویه های مقابله با حمله ها / تهدیدها، صریح، قابل فهم و به روز هستند؟
آیا تمهیدات لازم برای ترمیم صدمه ها به خصوص موارد ناشی از بلایای طبیعی پیش بینی شده است؟
آیا منابع و تجهیزات کافی برای واکنشهای مناسب نسبت به تهدیدها تدارک دیده شده است؟
آیا دستورالعمل های لازم برای چگونگی تماس کارکنان با کارشناسان امنیت تهیه شده است؟
آیا نحوه عمل در شرایط عدم دسترسی به کارشناسان امنیت و چگونگی اطلاع رسانی موضوع به مدیریت، مشخص شده است؟
آیا روشی برای مطلع نمودن مدیران ارشد(به خصوص مدیر فناوری اطلاعات) از وقوع حوادث احتمالی تعریف شده است؟
آیا روالی برای تماس با افراد خارج از سازمان(شامل شرایط و زمان تماس) به منظور درخواست کمک پیش بینی شده است؟
آیا کارکنان کلیدی برای اجرای روشهای مقابله با حمله ها / تهدیدها مشخص شده و آموزش دیده اند؟
آیا ابزارهای شناسایی حمله بدافزارها و اقدامات خرابکارانه مشخص شده و بر روی سیستمها نصب شده است؟
آیا نحوه ردیابی و تعقیب حمله ها بر روی شبکه مد نظر قرار گرفته است؟ -

تمهیدات مواجهه با ریسک تقلب در حوزه فناوری اطلاعات

- انجام دوره ای و گسترده ارزیابی ریسک تقلب در حوزه فناوری اطلاعات.
- برگزاری دوره های آموزشی آشنایی با امنیت فناوری اطلاعات و نحوه شناسایی تقلب برای تمامی کارکنان.
- تاکید بر تفکیک وظایف.
- محدود کردن سطوح دسترسی کاربران به سیستمها و داده ها، متناسب با نیازهای اطلاعاتی واقعی آنها برای انجام وظایف.
- تدوین الزامات سختگیرانه در رابطه با تعیین و استفاده از کلمات عبور.
- سابقه نگاری، پایش وممیزی اقدامات کارکنان در محیط شبکه.
- اِعمال دقت نظر مضاعف نسبت به عملکرد مدیران سیستمهای اطلاعاتی و کاربرانِ دارای اختیارات ویژه در آن سیستمها.
- استفاده از لایه های متعدد دفاعی در مقابل متجاوزین به شبکه.
- تدوین طرح واکنش موثر نسبت به سوانح تقلب و تشکیل یک تیم مناسب برای عکس العمل لازم و به موقع.
- غیر فعال کردن شناسه و کلمه عبور کارکنان در دوره عدم حضور آنها در سازمان .
- جمع آوری و نگهداری اطلاعات دادگاههای برگزار شده در رابطه با جرایم رایانه ای به منظور تجسس های آتی.
- تشویق تهیه نسخ پشتیبان امن و بازیابی های مدیریت شده داده ها.
- استقرار برنامه های مفید برای مدیریت آسیب پذیری سیستمها. –

سوالات کلیدی برای ارزیابی ریسک تقلب در حوزه فناوری اطلاعات

I.آیا سازمان از نظام راهبری برای کنترل تقلب در حوزه فناوری اطلاعات مشتمل بر تخصیص مسئولیتهای تحقیق و بررسی تقلب برخوردار است؟

II.آیا سازمان از سیاستهای مشخص برخورد با رخدادهای تقلب در حوزه فناوری اطلاعات برخوردار است؟

III.آیا سازمان نسبت به قوانین و مقررات محیط کسب و کار خود در ارتباط با تقلب در حوزه فناوری اطلاعات آگاهی دارد؟

IV.آیا در برنامه مدیریت ریسک تقلب در حوزه فناوری اطلاعات سازمان ، مشورت و هماهنگی با حسابرسی داخلی در نظر گرفته شده است؟

V.آیا سازمان کانال ارتباطی امنی برای دریافت اخبار تقلب از مخبرین فراهم نموده است؟

VI.آیا نقش و مسئولیتهای حسابرس داخلی در رابطه با تقلب در حوزه فناوری اطلاعات بطور واضح مشخص شده است؟

VII.آیا مسئولیتهای کشف، پیشگیری، برخورد و اطلاع رسانی تقلب در حوزه فناوری اطلاعات تعریف و به افراد ذیصلاح محول شده است؟

VIII.آیا اطلاعات به روز در رابطه با تقلب در حوزه فناوری اطلاعات، توسط مدیر حسابرسی داخلی و مدیریت سازمان به کمیته حسابرسی ارائه شده است؟

IX.آیا مدیریت، قائل به توجه ویژه به تقلب در حوزه فناوری اطلاعات و برگزاری دوره های آموزشی در رابطه با آن است؟

X.آیا ارزیابی ریسک تقلب در حوزه فناوری اطلاعات تحت رهبری مدیریت سازمان انجام شده و حسابرس داخلی در این ارزیابی مشارکت داده شده است؟

ادامه سوالات کلیدی برای ارزیابی ریسک تقلب در حوزه فناوری اطلاعات

XI.آیا نتایج ارزیابی ریسک تقلب در حوزه فناوری اطلاعات، در برنامه ریزی کار حسابرسی در نظر گرفته شده است؟
XII.آیا برنامه های برگزاری دوره های آموزشی کارکنان پیرامون ریسک تقلب در حوزه فناوری اطلاعات، به حسابرسان ارائه شده است؟
XIII.آیا ابزار خودکار لازم برای پیشگیری، کشف و رسیدگی به تقلب در حوزه فناوری اطلاعات برای مسئولین مربوطه فراهم شده است؟
XIV.آیا مدیران، اشراف لازم نسبت به انواع ریسکهای تقلب در حوزه فناوری اطلاعات در حیطه مسئولیتهای خود دارند؟
XV.آیا مدیریت و مدیر حسابرسی داخلی، از نحوه دستیابی به دستورالعملهای مراجع حرفه ای در رابطه با تقلب در حوزه فناوری اطلاعات ، اطلاع دارند؟
XVI.آیا مدیریت و مدیر حسابرسی داخلی از حیطه مسئولیت خود در ارتباط با تقلب در حوزه فناوری اطلاعات، آگاهی دارند؟
XVII.آیا از سوی مدیریت، یکپارچگی مناسب بین کنترلها برای پیشگیری، کشف و رسیدگی به تقلب در حوزه فناوری اطلاعات ایجاد شده است؟
XVIII.آیا سازمان از مجموعه مهارتهای لازم برای تحقیق و بررسی تقلب در حوزه فناوری اطلاعات برخوردار است؟
XIX.آیا مدیریت و مدیر حسابرسی داخلی، بطور دوره ای، اثر بخشی و کارآیی کنترلهای تقلب در حوزه فناوری اطلاعات را مورد ارزیابی قرار می دهند؟
XX.آیا کاربرگها و مستندات رسیدگی به تقلب در حوزه فناوری اطلاعات به نحو مقتضی و امن نگهداری شده است؟


سپاس از توجه شما