

نقش حسابرسان فناوری اطلاعات در مدیریت ریسک فناوری اطلاعات

REZA SABRI

www.RezaSabri.com

RezaSabri Academy

نقش حسابرسان فناوری اطلاعات در مدیریت ریسک فناوری اطلاعات

مطابق تعریف جامع حسابرسی فناوری اطلاعات، یکی از وظایف حسابرسان فناوری اطلاعات در راستای اطمینان بخشی در سه حوزه IT GRC به مدیریت ارشد، دارای دو نقش است:

۱-حسابرسی فرایند مدیریت ریسک فناوری اطلاعات

۲- انجام حسابرسی مبتنی بر ریسک شامل ارزیابی و آزمون کنترلها بر اساس ریسکهای فناوری اطلاعات

همچنین موسسه ISACA، رهنمودی تحت عنوان COBIT For Risk منتشر نموده است که حسابرسان فناوری اطلاعات از آن جهت حسابرسی فرایند مدیریت ریسک فناوری اطلاعات و ارزیابی ریسکهای فناوری اطلاعات به منظور برنامه ریزی حسابرسی و ارزیابی و ازمون کنترلهای فرایندهای فناوری اطلاعات بهره بگیرند.



کنترلهای فناوری اطلاعات

کنترلهای فناوری اطلاعات، فعالیت و اقداماتی هستند به منظور کاهش تهدیدات و ریسکهای فناوری اطلاعات و تحقق اهداف فرایند توسط مدیریت به کار گرفته می شوند. کنترلهای فناوری اطلاعات شامل:

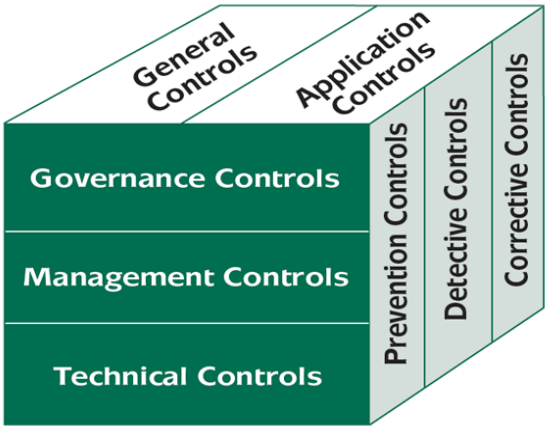
- سیاستها، خط مش ها و دستورالعمل حوزه فناوری اطلاعات
- تفکیک وظایف در فرایند
- مجوزدهی، تصویب و تائید



کنترلهای فناوری اطلاعات

مطابق رهنمودهای بین المللی حسابرسی فناوری اطلاعات GTAG1 ارائه شده توسط IIAدر خصوص کنترلهای فناوری اطلاعات کنترلهای مذکور را به ۳حوزه تقسیم نموده است:

- کنترلهای لایه حاکمیت، مدیریت و تکنیکی
- کنترل های کاربری و عمومی
- کنترل های پیشگیری کننده، کشف کننده، اصلاح کننده





کنترلهای لایه حاکمیت، مدیریت و تکنیکی

- **کنترلهای لایه حاکمیت:** کنترلهایی هستند هیئت مدیره جهت استقرار نظام حاکمیت فناوری اطلاعات در بانک و اطمینان از صحت عملکرد آن به کار می برد، که چارچوب COBIT در طریق اهداف و کنترلهای ارائه در ۵ فرایند EDM این کنترل را پوشش می دهد.

- **کنترلهای لایه مدیریت:** کنترلهای هستند که مدیریت فناوری اطلاعات به منظور ارائه خدمات و پشتیبانی از تحقق اهداف کسب و کار به کار می برد به عنوان نمونه ارائه دستورالعمل و بخشنامه ها، استقرار سیسم امنیت اطلاعات، استقرار میز خدمات و .....می باشد. که چارچوب COBIT از طریق اهداف و کنترلهای فرایندهای حوزه مدیریت که شامل ۳۲ فرایند برنامه ریزی، ساخت، اقدام و پشتیبانی تمامی این کنترل را پوشش می دهد.

- **کنترلهای تکنیکی:** کنترلهای هستند که به صورت چارچوب اصلی کنترلهای مدیریت را تشکیل می دهند در صورت ضعف در این بخش کنترلهای مدیریت بی اثر می شوند، به عنوان مثال مانند رمز نگاری، سطوح دسترسی، دسترسی به پایگاه داده و .... می باشد. در این بخش می توان از کنترلهای فنی و تکنیکی موجود در سایر استانداردها و چارچوبها مانند ITIL , ISMS به همراه چارچوب COBIT استفاده نمود.



❖ کنترلهای کاربردی

روش‌های دستی یا خودکاری است که به منظور کنترل پردازش نرم‌افزارهای اجرایی طراحی می‌شود و به کمک آنها از کامل‌بودن و صحت پردازش، تصویب و اعتبار معاملات اطمینان حاصل می‌شود.

❖ کنترلهای عمومی

خط‌مشی‌ها، رویه‌ها و اقداماتی هستند که به طور عمومی در اغلب سامانه‌های اطلاعاتی به کار گرفته می‌شود و به کمک آن‌ها از به‌کارگیری درست و مستمر این سامانه‌ها اطمینان حاصل می‌شود و کارکرد مؤثر کنترل‌های کاربردی را پشتیبانی می‌کند. این کنترل‌ها به طور معمول شامل کنترل‌های حاکم بر عملیات مرکز داده‌ها، تحصیل، تغییر و نگهداری نرم‌افزارها، کنترل‌های دسترسی، امنیتی و حفاظتی و ایجاد و نگهداری سیستم‌های کاربردی می‌باشند.



کنترلهای پیشگیری کننده، کشف کننده، اصلاح کننده

❖ کنترلهای پیشگیری کننده

کنترلهایی هستند که در لایه اول از وقوع تهدید، اسیب و عدم تحقق اهداف کنترلی پیشگیری می نماید مانند دیواره آتش، تهیه پشتیبان از اطلاعات و تعیین سطوح دسترسی کاربران

❖ کنترلهای کشف کننده

کنترلهایی هستند که در لایه دوم تهدید و اسیبهای وارد شده، ایرادات سیستمی و نقصهای فرایند را کشف می نماید مانند تست های نفوذپذیری

❖ کنترلهای اصلاح کننده

کنترلهایی هستند که در لایه سوم اشتباهات و نقص ها را اصلاح می کنند که شامل اقدامات اصلاحی جهت رفع یک مشکل و یا نقص است مانند اصلاح اطلاعات ورودی، بازیابی اطلاعاتی



RS REZA SABRI

www.RezaSabri.com



برای دریافت مشاوره و اطلاعات در مورد دوره ها

و شروع یادگیری نام و شماره تماس خود را در

واتس اپ به شماره زیر ارسال کنید.

09018303095