باسمه تعالی

یکی از مراحل اولیه حسابرسی فناوری اطلاعات، کسب شناخت عمومی و کلی نسبت به سازمان و وضعیت کلی فناوری اطلاعات آن است. پرسشنامه حاضر حسابرسان فناوری اطلاعات را در کسب چنین شناختی یاری می کند.

به ازای هر سوال یکی از وضعیت های بله یا خیر مشخص شده و توضیحات تکمیلی در صورت وجود در ستون توضیحات قید گردد. همچنین در صورتی که برای هر سوال مدارکی یا مستنداتی در دسترس است، عنوان مدرک مربوطه در ستون مدارک ثبت شده و مدارک نیز پیوست گردد.

ردیف	سوال	جواب		توضیحات	مدارک
		بله	خیر		
اهداف					
۱.	برنامه استراتژیک سازمان تدوین شده است؟				
۲.	در صورتی که برنامه استراتژیک سازمان تدوین شده، آیا به صورت رسمی تصویب شده است؟				
۳.	برنامه استراتژیک سازمان در حال حاضر به روز می باشد؟				
٤.	این برنامه مورد تایید مدیران ارشد است؟				
۵.	این برنامه مبنای اقدامات و کنترل های استراتژیک سازمان است؟				
٦.	آیا سند برنامه استراتژیک سازمان قابل ارائه است؟				
۷.	آیا تحلیل نقاط قوت و ضعف و فرصت و تهدید در سازمان انجام شده است؟				
۸.	آیا عبارت چشم انداز در سند برنامه استراتژیک سازمان تدوین شده است؟				
۹.	آیا عبارت ماموریت ها در سند برنامه استراتژیک سازمان تدوین شده است؟				
۱۰.	آیا اهداف در سند برنامه استراتژیک سازمان تدوین شده است؟				

ردیف	سوال	جواب		توضیحات	مدارک
		بله	خیر		
۱۱.	آیا راهبردها در سند برنامه استراتژیک سازمان تدوین شده است؟				
۱۲.	آیا سیاست ها در سند برنامه استراتژیک سازمان تدوین شده است؟				
ساختار و فرآیندها					
۱۳.	آیا ساختار سازمانی به صورت مصوب ارائه شده است؟				
۱٤.	آیا شرح وظایف سازمانی به صورت مصوب ارائه شده است؟				
۱۵.	آیا فرآیندهای سازمان مدلسازی و مستند شده اند؟				
۱٦.	آیا فرآیندهای مدل شده به روز بوده و مورد تایید مالکان فرآیندها هستند؟				
۱۷.	آیا نظام مدیریت کیفیت (ISO) در سازمان استقرار یافته است؟				
مدیریت ریسک					
۱۸.	آیا فرآیند رسمی مدیریت ریسک در سازمان تعریف و اجرایی شده است؟				
۱۹.	آیا واحد یا نقش خاصی برای مدیریت ریسک در ساختار سازمانی تعریف شده است؟				
۲۰.	آیا تاکنون تحلیل ریسک در سطح سازمان یا هریک از واحدهای سازمانی یا حوزه های کسب و کاری انجام شده است؟				
۲۱.	آیا مستندات تحلیل ریسک سازمان به روز و قابل اتکا هستند؟				
۲۲.	آیا مستندات تحلیل ریسک در دسترس هستند؟				
۲۳.	آیا فرآیند مدیریت ریسک از دیدگاه حسابرسی داخلی تحلیل شده و مورد ارزیابی قرار گرفته است؟				
کنترل های داخلی					

ردیف	سوال	جواب		توضیحات	مدارک
		بله	خیر		
۲٤.	آیا فرآیند رسمی برای نیازسنجی، تعریف، تدوین، تصوب و ابلاغ دستورالعمل های سازمانی وجود دارد؟				
۲۵.	آیا دستورالعمل های سازمانی به صورت متمرکز نگهداری و به روزرسانی می شوند؟				
۲٦.	آیا تاکنون کنترل های داخلی در سطح سازمان شناسایی و مستندسازی شده است؟				
۲۷.	آیا کنترل های فناوری اطلاعات شناسایی و مستندسازی شده است؟				
سوابق حسابرسی					
۲۸.	آیا تاکنون حسابرسی فناوری اطلاعات برای هیچ یک از دارایی های اطلاعاتی سازمان انجام شده است؟				
۲۹.	آیا آزمون های رسمی و معتبر امنیتی برای هیچ یک از دارایی های اطلاعاتی سازمان انجام شده است؟				
۳۰.	آیا سیستم های اطلاعاتی سازمان دارای گواهینامه امنیتی معتبر می باشند؟				
۳۱.	آیا قوانین و مقررات تاثیرگذار بر فناوری اطلاعات در سازمان شناسایی، گردآوری و اجرا شده است؟				
۳۲.	آیا تاکنون حسابرسی رعایت در سازمان انجام شده است؟				
۳۳.	آیا تاکنون حسابرسی تقلب در سازمان انجام شده است؟				
۳٤.	آیا تاکنون در حوزه های مرتبط با فناوری اطلاعات، حسابرسی داخلی یا عملیاتی انجام شده است؟				
۳۵.	آیا مستنداتی در خصوص تحلیل وضعیت موجود و نقاط ضعف و قوت دارایی های اطلاعاتی سازمان وجود دارد؟				
۳٦.	آیا در گزارش های حسابرسی داخلی یا حسابرسی مالی سازمان به موارد ضعف فناوری اطلاعات اشاره شده است؟				
مستندات فناوری اطلاعات					

ردیف	سوال	جواب		توضیحات	مدارک
		بله	خیر		
۳۷.	آیا وضعیت موجود شبکه ارتباطی سازمان مستند شده است؟				
۳۸.	آیا مستندات تحلیل و طراحی سیستم های اطلاعاتی سازمان در دسترس است؟				
۳۹.	آیا مستندات کاربری و راهبری سیستم های اطلاعاتی سازمان در دسترس است؟				
٤٠.	آیا اطلاعات پیکره بندی دارایی های اطلاعاتی سازمان به صورت متمرکز مستند شده و به روزرسانی می گردند؟				
امنیت اطلاعات					
٤١.	آیا نقش یا واحد سازمانی خاصی برای امنیت اطلاعات تعیین شده است؟				
٤٢.	آیا کمیته امنیت اطلاعات در سازمان شکل گرفته است؟				
٤٣.	آیا فرآیند مدیریت امنیت اطلاعات در سازمان استقرار یافته است؟				
٤٤.	آیا سیاست های امنیتی سازمان مستند، مدون و مصوب شده اند؟				
٤٥.	آیا ریسک های امنیتی سازمان شناسایی و تحلیل شده است؟				
٤٦.	آیا آسیب پذیری های دارایی های اطلاعاتی سازمان شناسایی و تحلیل شده است؟				
٤٧.	آیا کنترل های امنیت اطلاعات شناسایی و مستندسازی شده است؟				
٤٨.	آیا کنترل های امنیت اطلاعات مورد آزمون قرار گرفته اند؟				
٤٩.	آیا مستندات آزمون کنترل های امنیتی در دسترس هستند؟				
٥٠.	آیا طرح بازیابی بحران (DRP) برای سازمان تهیه شده است؟				
انتظارات ذینفعان					

ردیف	سوال	جواب		توضیحات	مدارک
		بله	خیر		
۵۱.	آیا انتظارات هیات مدیره و مدیران ارشد سازمان در خصوص حسابرسی فناوری اطلاعات مشخص شده است؟				
۵۲.	آیا به صورت مکتوب و رسمی انتظارات فوق مستند شده است؟				
۵۳.	آیا اهداف حسابرسی فناوری اطلاعات در سازمان مستندسازی و مدون شده است؟				
۵٤.	آیا در خصوص اولویت ها و محدوده حسابرسی فناوری اطلاعات توافقی در سازمان وجود دارد؟				
۵۵.	آیا اولویت ها و توافق فوق الذکر مستند و مصوب شده است؟				