فناوری سپهر امن پارسین

چک‌لیست ممیزی ISMS

واحد خدمات افتا – بهمن‌ماه ۱۴۰۲

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
بند ٤- چارچوب سازمان						
٤-١- شناخت سازمان و چارچوب آن						
١	آیا سازمان، مسایل درونی و بیرونی مرتبط با اهداف سازمان و مسایل تأثیرگذار در امکان دستیابی به نتایج مدنظر سیستم مدیریت امنیت اطلاعات را شناسایی کرده است؟	٤-١	در سند خط مشی امنیت اطلاعات شرکت به بعضی از اهداف اشاره شده است ولی این اهداف بر اساس شناسایی و تجزیه و تحلیل مسایل درونی و بیرونی مرتبط با اهداف سازمان نیستند. در سند استراتژی شرکت به طور واضح به مسایل مرتبط با امنیت اطلاعات اشاره ای نشده است.			
٤-٢- درک نیازها و انتظارات طرف‌های ذینفع						
٢	آیا سازمان، طرف‌های ذینفع مرتبط با سیستم مدیریت امنیت اطلاعات را شناسایی و مشخص کرده است؟	٤-٢	سازمان، طرف های ذینفع مرتبط با سیستم مدیریت امنیت اطلاعات خود را شناسایی نکرده است و مستندی در خصوص انتظارات و خواسته های امنیت اطلاعات ذینفعان درون و برون سازمانی وجود ندارد.			
٤-٣- تعیین قلمرو سیستم مدیریت امنیت اطلاعات						
٣	آیا سازمان، قلمرو سیستم مدیریت امنیت اطلاعات را با در نظر گرفتن موضوعات بیرونی و درونی و همچنین الزامات طرف‌های ذینفع مشخص کرده است؟	٤-٣	قلمرو سیستم مدیریت امنیت اطلاعات، واحد ICT شرکت است. سوابقی که مشخص باشد سازمان چگونه و بر اساس چه تجزیه و تحلیلی به این دامنه رسیده است، وجود ندارد.			
٤-٤- سیستم مدیریت امنیت اطلاعات						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
٤	آیا سازمان، سیستم مدیریت امنیت اطلاعات را مطابق با الزامات استاندارد ایزو ۲۷۰۰۱ طراحی، پیاده‌سازی و نگهداری کرده و به صورت مستمر نیز آن را بهبود می‌بخشد؟	۴-۴	در راستای پیاده سازی سیستم مدیریت امنیت اطلاعات، تعدادی مستند در شرکت تدوین شده است. تنها به تدوین این مستندات اکتفا شده است و تاکنون اقدامی جهت بهبود فعالیت های انجام شده صورت نگرفته است.			
بند ۵- رهبری						
۵-۱- رهبری و تعهد						
٥	آیا مدیریت ارشد، استقرار خطمشی و اهداف امنیت اطلاعات را در راستای سازگاری با جهت‌گیری‌های راهبردی سازمان تضمین می‌کند؟	۵-۱				
٦	آیا مدیریت ارشد، ادغام الزامات سیستم مدیریت امنیت اطلاعات را در فرایندهای سازمانی تضمین می‌کند؟	۵-۱				
۷	آیا مدیریت ارشد، در دسترس بودن منابع مورد نیاز برای سیستم مدیریت امنیت اطلاعات را تضمین می‌کند؟	۵-۱				
۸	آیا مدیریت ارشد، اهمیت مدیریت امنیت اطلاعات اثربخش و انطباق با الزامات سیستم مدیریت امنیت اطلاعات را به پرسنل سازمان ابلاغ می‌نماید؟	۵-۱				
۹	آیا مدیریت ارشد از دستیابی به نتایج مورد انتظار در سیستم مدیریت امنیت اطلاعات، اطمینان حاصل می‌کند؟	۵-۱				

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱۰	آیا مدیریت ارشد، افراد را به منظور کمک به اثربخشی سیستم مدیریت امنیت اطلاعات جهت‌دهی و پشتیبانی می‌کند؟	۵-۱				
۱۱	آیا مدیریت ارشد، تعهد و رهبری خود را نسبت به ترویج بهبود مستمر سیستم مدیریت امنیت اطلاعات نشان می‌دهد؟	۵-۱				
۵-۲- خطمشی						
۱۲	آیا خطمشی امنیت اطلاعات توسط مدیریت ارشد، تعریف و مشخص شده است؟	۵-۲				
۱۳	آیا خطمشی امنیت اطلاعات، متناسب با اهداف سازمانی می‌باشد؟	۵-۲				
۱٤	آیا خطمشی امنیت اطلاعات، شامل اهداف امنیت اطلاعات بوده یا چارچوبی را برای تنظیم اهداف امنیت اطلاعات ارایه می‌دهد؟	۵-۲				
۱۵	آیا خطمشی امنیت اطلاعات، شامل تعهدی مبنی بر برآورده‌سازی الزامات کاربردپذیر مرتبط با امنیت اطلاعات می‌باشد؟	۵-۲				
۱٦	آیا خطمشی امنیت اطلاعات، شامل تعهدی جهت بهبود مستمر سیستم مدیریت امنیت اطلاعات می‌باشد؟	۵-۲				
۱۷	آیا خطمشی امنیت اطلاعات به عنوان اطلاعات مستند، در دسترس بوده و در داخل سازمان ابلاغ شده است؟	۵-۲				

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱۸	آیا خط‌مشی امنیت اطلاعات، به فراخور در دسترس طرف‌های ذینفع قرار داده شده است؟	۵-۲				
۱۹	آیا مدیریت ارشد، مسئولیت‌ها و اختیارات مرتبط با امنیت اطلاعات را تعیین و ابلاغ کرده است؟	۵-۲				
۵-۳- نقش‌های سازمانی، مسئولیت‌ها و اختیارات						
۲۰	آیا مدیریت ارشد، مسئولیت‌ها و اختیارات را برای اطمینان از اینکه سیستم مدیریت امنیت اطلاعات با الزامات استاندارد ایزو ۲۷۰۰۱ منطبق است، تعیین نموده است؟	۵-۳				
۲۱	آیا مدیریت ارشد، مسئولیت‌ها و اختیارات را برای گزارش‌دهی عملکرد سیستم مدیریت امنیت اطلاعات به مدیریت ارشد تعیین کرده است؟	۵-۳				
۲۲	آیا مدیریت ارشد، مسئولیت‌ها و اختیارات را برای گزارش‌دهی عملکرد سیستم مدیریت امنیت اطلاعات در داخل سازمان تعیین نموده است؟	۵-۳				
بند ٦- طرح‌ریزی						
٦-۱- اقداماتی برای مدیریت مخاطرات و فرصت‌ها						
٦-۱-۱- الزامات عمومی						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲۳	آیا سازمان، مخاطرات و فرصت‌ها را جهت اطمینان از دستیابی به نتایج مورد انتظار سیستم مدیریت امنیت اطلاعات تعیین می‌کند؟	۶-۱-۱				
۲۴	آیا سازمان، مخاطرات و فرصت‌ها را جهت جلوگیری از تأثیرات ناخواسته یا کاهش آنها تعیین می‌کند؟	۶-۱-۱				
۲۵	آیا سازمان، مخاطرات و فرصت‌ها را جهت دستیابی به بهبود مستمر تعیین می‌کند؟	۶-۱-۱				
۲۶	آیا جهت نشان‌دهی مخاطرات و فرصت‌های شناسایی شده، اقداماتی صورت گرفته است؟	۶-۱-۱				
۲۷	آیا سازمان، اقدامات مرتبط با شناسایی مخاطرات و فرصت‌ها را در فرایند سیستم مدیریت امنیت اطلاعات ادغام و پیاده‌سازی کرده است؟	۶-۱-۱				
۶-۱-۲- ارزیابی مخاطره امنیت اطلاعات						
۲۸	آیا سازمان در فرایند تعریف و اجرای ارزیابی مخاطرات امنیت اطلاعات، معیارهای پذیرش مخاطره و معیارهایی را برای اجرای ارزیابی‌های مخاطره امنیت اطلاعات تعریف نموده است؟	۶-۱-۲				
۲۹	آیا سازمان در فرایند ارزیابی‌های مخاطرات امنیت اطلاعات بعدی، از تولید نتایج نامتناقض، معتبر و مقایسه‌پذیر اطمینان حاصل می‌کند؟	۶-۱-۲				

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۳۰	آیا سازمان با به کارگیری فرایند ارزیابی مخاطره، مخاطرات مرتبط با فقدان محرمانگی، صحت و دسترس‌پذیری را برای اطلاعاتی که در قلمرو سیستم مدیریت امنیت اطلاعات هستند، شناسایی می‌کند؟	۶-۱-۲				
۳۱	آیا در راستای شناسایی مخاطرات امنیت اطلاعات، مالکان مخاطره‌ها نیز شناسایی می‌شوند؟	۶-۱-۲				
۳۲	آیا سازمان در فرایند تعریف و اجرای ارزیابی مخاطرات امنیت اطلاعات، پیامدهای بالقوه مخاطرات شناسایی شده را تحلیل می‌کند؟	۶-۱-۲				
۳۳	آیا سازمان در فرایند تعریف و اجرای ارزیابی مخاطرات امنیت اطلاعات، وقوع مخاطرات شناسایی شده را به صورت واقع‌بینانه تحلیل می‌کند؟	۶-۱-۲				
۳٤	آیا سازمان در فرایند تعریف و اجرای ارزیابی مخاطرات امنیت اطلاعات، سطوح مخاطرات شناسایی شده را تحلیل می‌کند؟	۶-۱-۲				
۳۵	آیا سازمان در فرایند ارزشیابی مخاطرات امنیت اطلاعات، نتایج تحلیل مخاطره را با معیارهای مخاطره ایجاد شده مقایسه می‌کند؟	۶-۱-۲				
۳٦	آیا سازمان در فرایند ارزشیابی مخاطرات امنیت اطلاعات، مخاطرات تحلیل شده را جهت مقابله با مخاطره اولویت‌بندی کرده است؟	۶-۱-۲				
۶-۱-۳- برطرف‌سازی مخاطره امنیت اطلاعات						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۳۷	آیا سازمان در فرایند مقابله با مخاطرات امنیت اطلاعات، گزینه‌های مقابله با مخاطره امنیت اطلاعات را با در نظر گرفتن نتایج ارزیابی مخاطرات انتخاب نموده است؟	۶-۱-۳				
۳۸	آیا سازمان در فرایند مقابله با مخاطرات امنیت اطلاعات، تمامی کنترل‌هایی که به منظور پیاده‌سازی گزینه‌های منتخب برای مقابله با مخاطرات امنیت اطلاعات ضروری هستند، تعیین نموده است؟	۶-۱-۳				
۳۹	آیا سازمان، کنترل‌های مشخص شده را با کنترل‌های استاندارد جهت اطمینان از در نظر گرفته شدن کلیه کنترل‌های ضروری، مقایسه و بررسی کرده است؟	۶-۱-۳				
٤٠	آیا بیانیه کاربردپذیری که شامل کنترل‌های لازم و توجیه استفاده از آنها (چه پیاده‌سازی شده باشند و چه خیر) و نیز توجیه عدم استفاده از کنترل‌های استاندارد می‌باشد، تدوین شده است؟	۶-۱-۳				
٤١	آیا طرحی برای مقابله با مخاطرات امنیت اطلاعات تدوین شده است؟	۶-۱-۳				
٤٢	آیا تأییدیه طرح مقابله با مخاطرات امنیت اطلاعات از مالکان مخاطره‌ها اخذ شده است؟	۶-۱-۳				
٤٣	آیا تأییدیه پذیرش مخاطرات امنیت اطلاعات باقی‌مانده از مدیریت ارشد سازمان اخذ شده است؟	۶-۱-۳				

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۶-۲- اهداف امنیت اطلاعات و برنامه‌ریزی برای دستیابی به آنها						
٤٤	آیا اهداف امنیت اطلاعات با خط‌مشی امنیت اطلاعات سازگار هستند؟	۶-۲				
٤٥	آیا اهداف امنیت اطلاعات قابل سنجش و اندازه‌گیری هستند؟	۶-۲				
٤٦	آیا اهداف امنیت اطلاعات مطابق با الزامات کاربردپذیر امنیت اطلاعات و همچنین نتایج ارزیابی مخاطره و مقابله با مخاطرات می‌باشد؟	۶-۲				
٤٧	آیا اهداف امنیت اطلاعات به نحو مقتضی به‌روزرسانی و ابلاغ شده است؟	۶-۲				
٤٨	آیا سازمان، اطلاعات مستندی را در رابطه با اهداف امنیت اطلاعات نگهداری می‌کند؟	۶-۲				
٤٩	آیا سازمان در جهت طرح‌ریزی دستیابی به اهداف امنیت اطلاعات، تعیین نموده که چه کاری انجام خواهد شد؟	۶-۲				
٥٠	آیا سازمان در جهت طرح‌ریزی دستیابی به اهداف امنیت اطلاعات، تعیین کرده که چه منابعی مورد نیاز هستند؟	۶-۲				
٥١	آیا سازمان در جهت طرح‌ریزی دستیابی به اهداف امنیت اطلاعات، تعیین کرده که چه کسی مسئول می‌باشد؟	۶-۲				

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۵۲	آیا سازمان در جهت طرح‌ریزی دستیابی به اهداف امنیت اطلاعات، تعیین کرده که چه زمانی کامل خواهد شد؟	۶-۲				
۶-۳- برنامه‌ریزی تغییرات						
۵۳	آیا سازمان هرگونه تغییری در سیستم مدیریت امنیت اطلاعات را به صورت برنامه‌ریزی شده انجام می‌دهد؟	۶-۳				
بند ۷- پشتیبانی						
۷-۱- منابع						
۵۴	آیا سازمان، منابع مورد نیاز را به منظور استقرار، پیاده‌سازی، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات، تعیین و فراهم کرده است؟	۷-۱				
۷-۲- صلاحیت						
۵۵	آیا سازمان صلاحیت افرادی که تحت کنترل آن کار می‌کنند و بر روی عملکرد امنیت اطلاعات تأثیرگذار هستند را تعیین نموده است؟	۷-۲				
۵۶	آیا سازمان صلاحیت افراد را بر مبنای تحصیلات، آموزش‌ها یا تجارب مناسب تضمین می‌کند؟	۷-۲				

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۵۷	آیا سازمان اقدامات لازم را جهت کسب صلاحیت‌های لازم انجام داده و اثربخشی اقدامات انجام شده را در صورت لزوم ارزیابی کرده است؟	۷-۲				
۷-۳- آگاه‌سازی						
۵۸	آیا افراد مرتبط، از خط‌مشی امنیت اطلاعات آگاه هستند؟	۷-۳				
۷-٤- ارتباطات						
۵۹	آیا سازمان، زمینه ارتباطات درونی و بیرونی مرتبط با سیستم مدیریت امنیت اطلاعات را تعیین نموده است؟	۷-۴				
٦۰	آیا سازمان زمان انجام ارتباطات دورنی و بیرونی مرتبط با سیستم مدیریت امنیت اطلاعات را تعیین کرده است؟	۷-۴				
٦۱	آیا سازمان مشخص نموده که ارتباطات مرتبط با سیستم مدیریت امنیت اطلاعات، با چه کسی انجام شود؟	۷-۴				
٦۲	آیا سازمان مشخص نموده که چه کسی باید ارتباطات مرتبط با سیستم مدیریت امنیت اطلاعات را انجام دهد؟	۷-۴				
٦۳	آیا سازمان فرایندهایی که ارتباطات مرتبط با سیستم مدیریت امنیت اطلاعات از طریق آنها انجام شود را مشخص کرده است؟	۷-۴				

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۷-۵- اطلاعات مستند						
۷-۵-۱- الزامات عمومی						
٦٤	آیا سیستم مدیریت امنیت اطلاعات سازمان شامل اطلاعات مستندی که مورد نیاز استاندارد ایزو ۲۷۰۰۱ است، می‌باشد؟	۷-۵-۱				
٦٥	آیا سیستم مدیریت امنیت اطلاعات شامل اطلاعات مستندی که توسط سازمان به منظور اثربخشی این سیستم مدیریتی ضروری تشخیص داده شده است، می‌باشد؟	۷-۵-۱				
٦٦	آیا سیستم مدیریت امنیت اطلاعات متناسب با اندازه سازمان و نوع فعالیت‌ها، فرایندها، محصولات و خدمات آن می‌باشد؟	۷-۵-۱				
٦٧	آیا سیستم مدیریت امنیت اطلاعات سازمان شامل پیچیدگی فرایندها و تعاملات بین آنها با یکدیگر می‌باشد؟	۷-۵-۱				
۷-۵-۲- ایجاد و به‌روزرسانی						
٦٨	آیا سازمان در هنگام ایجاد و به‌روزرسانی اطلاعات مستند، از انجام شناسایی و توصیف (عنوان، تاریخ، نویسنده یا شماره ارجاع)، قالب (زبان، نسخه نرم‌افزار و گرافیک‌ها) و رسانه‌ها (کاغذی یا الکترونیکی) به شیوه مناسب، اطمینان حاصل می‌کند؟	۷-۵-۲				

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۳-۵-۷- کنترل اطلاعات مستند						
۶۹	آیا اطلاعات مستندی برای سیستم مدیریت امنیت اطلاعات، هر کجا و هر زمان که لازم باشد، در دسترس بوده و مناسب استفاده است؟	۷-۵-۳				
۷۰	آیا اطلاعات مستند سیستم مدیریت امنیت اطلاعات به میزان کافی حفاظت می‌شوند؟	۷-۵-۳				
۷۱	آیا سازمان به منظور کنترل اطلاعات مستند، اقداماتی همچون توزیع، دسترسی، بازیابی و استفاده را در صورت نیاز اجرا می‌نماید؟	۷-۵-۳				
۷۲	آیا سازمان به منظور کنترل اطلاعات مستند، اقداماتی همچون ذخیره و نگهداری (حفظ خوانایی) را در صورت نیاز اجرا می‌نماید؟	۷-۵-۳				
۷۳	آیا سازمان به منظور کنترل اطلاعات مستند، اقداماتی همچون کنترل تغییرات، نگهداری و امحا را در صورت نیاز اجرا می‌نماید؟	۷-۵-۳				
بند ۸- عملیات						
۱-۸- برنامه‌ریزی و کنترل عملیات						
۷۴	آیا سازمان، فرایندهای مورد نیاز را جهت برآورده‌سازی الزامات امنیت اطلاعات طرح‌ریزی، پیاده‌سازی و کنترل نموده است؟	۸-۱				

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۷۵	آیا سازمان طرح‌های دستیابی به اهداف امنیت اطلاعات را که در بند ۶-۲ استاندارد ایزو ۲۷۰۰۱ مشخص شده، اجرا نموده است؟	۸-۱				
۷۶	آیا سازمان، اطلاعات مستند جهت اطمینان از تطابق فرایندها با طرح‌ها را تا حد ضروری نگهداری می‌کند؟	۸-۱				
۷۷	آیا سازمان، تغییرات طرح‌ریزی شده را کنترل و پیامدهای تغییرات غیرعمدی را بازنگری کرده و اقدامات لازم را به منظور جلوگیری از عواقب جانبی اجرا می‌نماید؟	۸-۱				
۸-۲- ارزیابی مخاطره امنیت اطلاعات						
۷۸	آیا سازمان، ارزیابی مخاطرات امنیت اطلاعات را در بازه‌های زمانی طرح‌ریزی شده یا در صورت بروز هرگونه تغییر به وجود آمده یا پیشنهادی بر اساس معیارهای مشخص شده در بند ۶-۱-۲ استاندارد ایزو ۲۷۰۰۱ انجام می‌دهد؟	۸-۲				
۸-۳- برطرف‌سازی مخاطره امنیت اطلاعات						
۷۹	آیا سازمان، طرح مقابله با مخاطرات امنیت اطلاعات را اجرا کرده است؟	۸-۳				
بند ۹- ارزیابی عملکرد						
۹-۱- پایش، اندازه‌گیری، تحلیل و ارزیابی						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۸۰	آیا سازمان، عملکرد امنیت اطلاعات و اثربخشی سیستم مدیریت امنیت اطلاعات را ارزیابی نموده است؟	۹-۱				
۸۱	آیا سازمان مشخص کرده که چه چیزی باید در عملکرد امنیت اطلاعات و اثربخشی سیستم مدیریت امنیت اطلاعات پایش و اندازه‌گیری شود؟	۹-۱				
۸۲	آیا سازمان مشخص نموده که چه روش‌هایی برای پایش، اندازه‌گیری، تحلیل و ارزیابی عملکرد امنیت اطلاعات و اثربخشی سیستم مدیریت امنیت اطلاعات جهت حصول اطمینان از نتایج معتبر موجود می‌باشد؟	۹-۱				
۸۳	آیا سازمان مشخص نموده که چه زمانی پایش و اندازه‌گیری باید انجام شود؟	۹-۱				
۸٤	آیا سازمان مشخص نموده که توسط چه شخصی باید پایش و اندازه‌گیری انجام شود؟	۹-۱				
۸۵	آیا سازمان مشخص نموده که در چه زمانی باید نتایج مربوط به پایش و اندازه‌گیری، تحلیل و ارزیابی شوند؟	۹-۱				
۸٦	آیا سازمان مشخص نموده که نتایج باید توسط چه شخصی تحلیل و ارزیابی شوند؟	۹-۱				
۹-۲- ممیزی داخلی						
۹-۲-۱- الزامات عمومی						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۸۷	آیا سازمان در بازه‌های زمانی طرح‌ریزی شده، ممیزی‌های داخلی را انجام می‌دهد؟	۹-۲-۱				
۸۸	آیا سازمان در ممیزی‌های داخلی طرح‌ریزی شده، انطباق سیستم مدیریت امنیت اطلاعات را با الزامات خود سازمان مشخص می‌نماید؟	۹-۲-۱				
۸۹	آیا سازمان در ممیزی‌های داخلی طرح‌ریزی شده، انطباق سیستم مدیریت امنیت اطلاعات را با الزامات استاندارد ایزو ۲۷۰۰۱ مشخص می‌کند؟	۹-۲-۱				
۹۰	آیا سازمان در ممیزی‌های داخلی طرح‌ریزی شده، پیاده‌سازی و نگهداری سیستم مدیریت امنیت اطلاعات را به شیوه اثربخش مشخص می‌نماید؟	۹-۲-۱				
۹-۲-۲- برنامه ممیزی داخلی						
۹۱	آیا سازمان، برنامه‌های ممیزی که شامل تعداد دفعات، روش‌ها، مسئولیت‌ها، الزامات طرح‌ریزی و گزارش‌دهی می‌باشد را طرح‌ریزی، دایر، پیاده‌سازی و نگهداری می‌نماید؟	۹-۲-۲				
۹۲	آیا سازمان در ممیزی‌های داخلی طرح‌ریزی شده، معیارهای ممیزی و همچنین قلمروی هر ممیزی را مشخص می‌کند؟	۹-۲-۲				

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۹۳	آیا سازمان در ممیزی‌های داخلی طرح‌ریزی شده، ممیزان و هدایت ممیزی را به نحوی انتخاب می‌کند که از بی‌طرفی و عینی بودن نتایج ممیزی اطمینان حاصل شود؟	۹-۲-۲				
۹٤	آیا سازمان از گزارش‌دهی نتایج ممیزی به مدیریت مربوطه و مدیر ارشد اطمینان حاصل می‌نماید؟	۹-۲-۲				
۹-۳- بازنگری مدیریت						
۹-۳-۱- الزامات عمومی						
۹۵	آیا مدیریت ارشد، سیستم مدیریت امنیت اطلاعات سازمان را در بازه‌های زمانی مشخص شده بازنگری نموده و از تداوم سازگاری، کفایت و اثربخشی آن اطمینان حاصل می‌کند؟	۹-۳-۱				
۹-۳-۲- ورودی‌های بازنگری مدیریت						
۹٦	آیا مدیریت ارشد، وضعیت اقدامات از بازنگری‌های مدیریتی پیشین را در بازنگری‌های خود مدنظر قرار داده است؟	۹-۳-۲				
۹۷	آیا مدیریت ارشد، تغییرات در مسایل داخلی و بیرونی مرتبط با سیستم مدیریت امنیت اطلاعات را در بازنگری‌های خود مدنظر قرار داده است؟	۹-۳-۲				

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۹۸	آیا مدیریت ارشد، بازخورد عملکرد امنیت اطلاعات را که شامل عدم انطباق‌ها و اقدامات اصلاحی، نتایج پایش و اندازه‌گیری، نتایج ممیزی و تحقق اهداف امنیت اطلاعات می‌باشد، در بازنگری‌های مدیریتی مدنظر قرار داده است؟	۹-۳-۲				
۹۹	آیا مدیریت ارشد، بازخورد از طرف‌های ذینفع را در بازنگری‌های مدیریتی خود مدنظر قرار داده است؟	۹-۳-۲				
۱۰۰	آیا مدیریت ارشد، نتایج ارزیابی مخاطره و وضعیت طرح مقابله با مخاطرات را در بازنگری‌های مدیریتی خود مدنظر قرار داده است؟	۹-۳-۲				
۱۰۱	آیا مدیریت ارشد، فرصت‌ها برای بهبود مستمر را در بازنگری‌های مدیریتی خود مدنظر قرار داده است؟	۹-۳-۲				
۹-۳-۳- نتایج بازنگری مدیریت						
۱۰۲	آیا خروجی‌های بازنگری مدیریت شامل تصمیمات لازم جهت بهبود مستمر و انجام تغییرات لازم در سیستم مدیریت امنیت اطلاعات جهت افزایش کارایی و عملکرد آن می‌باشد؟	۹-۳-۳				
۱۰۳	آیا سوابق و مستندات جلسات بازنگری مدیریت به خوبی نگهداری می‌شوند؟	۹-۳-۳				
بند ۱۰- بهبود						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱۰-۱- بهبود مستمر						
۱۰۴	آیا سازمان به طور مستمر، سازگاری، کفایت و اثربخشی سیستم مدیریت امنیت اطلاعات را بهبود می‌بخشد؟	۱۰-۱				
۱۰-۲- عدم انطباق و اقدام اصلاحی						
۱۰۵	آیا سازمان هنگام وقوع یک عدم انطباق، در مقابل بروز آن واکنش نشان داده و در صورت مقتضی اقداماتی را به منظور کنترل و اصلاح آن انجام می‌دهد؟	۱۰-۲				
۱۰۶	آیا سازمان هنگام وقوع یک عدم انطباق، با پیامدهای آن مقابله می‌کند؟	۱۰-۲				
۱۰۷	آیا اقداماتی جهت بازنگری عدم انطباق و مشخص نمودن علل عدم انطباق جهت حذف علل آن به منظور عدم وقوع مجدد یا وقوع در جای دیگر صورت می‌گیرد؟	۱۰-۲				
۱۰۸	آیا سازمان هرگونه اقداماتی را که لازم است، اجرا و پیاده‌سازی می‌کند؟	۱۰-۲				
۱۰۹	آیا سازمان، اثربخشی هر اقدام اصلاحی انجام شده را بازنگری می‌کند؟	۱۰-۲				
۱۱۰	آیا سازمان، در صورت نیاز تغییراتی را در سیستم مدیریت امنیت اطلاعات ایجاد می‌کند؟	۱۰-۲				

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱۱۱	آیا سازمان، اطلاعات مستندی همچون ماهیت عدم انطباق‌ها و اقداماتی که متعاقب آنها انجام شده و نیز نتایج هر یک از اقدامات اصلاحی را به عنوان شواهد نگهداری می‌کند؟	۱۰-۲				
الف ۵- کنترل‌های سازمانی						
الف ۵-۱- خط‌مشی‌های امنیت اطلاعات						
۱	آیا خط‌مشی امنیت اطلاعات و خط‌مشی‌های موضوعی خاص، تدوین و مستند شده‌اند؟	الف-۵-۱				
۲	آیا خط‌مشی امنیت اطلاعات و خط‌مشی‌های موضوعی خاص، به طور رسمی توسط مدیرعامل و سایر مدیران ارشد تصویب شده‌اند؟					
۳	آیا خط‌مشی‌های امنیتی، ابلاغ و به اطلاع تمام کارکنان رسیده است؟					
٤	آیا خط‌مشی‌های امنیتی به اطلاع اشخاص مرتبط بیرونی، پیمانکاران و تأمین‌کنندگان رسیده است؟					
۵	آیا خط‌مشی‌های امنیتی در فواصل زمانی طرح‌ریزی شده یا هنگامی که تغییرات عمده‌ای در محیط کسب‌وکار و مسایل قانونی، حقوقی، مقرراتی و فنی به وجود آید، بازنگری می‌شوند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
٦	آیا در بازنگری خط‌مشی‌های امنیتی از تناسب، کفایت و اثربخشی آنها اطمینان حاصل می‌شود؟					
۷	آیا در بازنگری خط‌مشی‌های امنیتی، نتایج بازنگری‌های مدیریت مدنظر قرار می‌گیرد؟					
الف ۵-۲- نقش‌ها و مسئولیت‌های امنیت اطلاعات						
۱	آیا تمام مسئولیت‌های امنیتی مطابق با خط‌مشی‌های امنیت اطلاعات، به روشنی تعریف و مشخص شده‌اند؟					
۲	آیا مسئولیت‌های امنیتی کارکنان (در خصوص دارایی‌های اطلاعاتی)، به روشی مناسب تعریف و ابلاغ شده است (در شرح شغل کارکنان)؟					
۳	آیا مسئولیت‌های افراد نسبت به حفاظت از دارایی‌ها و انجام فرایندهای امنیت اطلاعات، به صورت شفاف مشخص شده است؟					
٤	آیا سطوح اختیارات افراد، تعریف و مستند شده است؟					
٥	آیا مسئولیت‌های امنیتی اشخاص سوم و طرف‌های مرتبط بیرونی، به صورت مناسب تعریف و ابلاغ می‌شود؟					
الف ۵-۳- تفکیک وظایف						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا به منظور کاهش فرصت‌های دستکاری سهوی/ غیرمجاز یا سوءاستفاده از دارایی‌های اطلاعاتی، وظایف و حدود مسئولیت‌ها تفکیک شده است؟					
الف ۵-٤- مسئولیت‌های مدیریت						
۱	آیا مدیریت ارشد شرکت، کلیه کارکنان و پیمانکاران را به رعایت خط‌مشی‌ها و رویه‌های امنیتی شرکت ملزم کرده است؟					
۲	آیا مدیریت ارشد، یک کانال ارتباطی ویژه برای گزارش نقض الزامات امنیتی ایجاد کرده است؟					
۳	آیا کارکنان و پیمانکاران درباره نقش‌ها و مسئولیت‌های امنیت اطلاعات خود، پیش از اعطای مجوز دسترسی به اطلاعات محرمانه یا سامانه‌های اطلاعاتی توجیه شده‌اند؟					
الف ۵-۵- ارتباط با مراجع معتبر						
۱	آیا به منظور مدیریت رخدادهای امنیتی، رویه‌ای در شرکت وجود دارد که مشخص کند چه زمانی و با کدام یک از مراجع دارای اختیار باید ارتباط برقرار شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا ارتباط با مسئولان سازمان‌هایی که بر امنیت اطلاعات تأثیر داشته یا می‌توانند رخدادهای امنیتی را مدیریت کنند، برقرار و حفظ شده و لیست اطلاعات تماس آنها نیز به‌روزرسانی می‌شود؟					
الف ۶-۵- ارتباط با گروه‌های ذینفع ویژه						
۱	آیا فهرستی از اطلاعات تماس گروه‌های ذینفع ویژه وجود داشته و به‌روزرسانی می‌شود (مثلاً انجمن‌ها، مشاوران و مراکز امنیتی)؟					
۲	آیا ارتباطات با گروه‌های دارای گرایش فنی و امنیتی، برقرار و حفظ شده است؟					
الف ۷-۵- هوش تهدید						
۱	آیا اطلاعات مربوط به تهدیدهای امنیت اطلاعات به منظور ایجاد هوش تهدید، جمع‌آوری و تحلیل می‌شوند؟					
الف ۸-۵- امنیت اطلاعات در مدیریت پروژه						
۱	آیا در مدیریت تمامی پروژه‌ها صرف نظر از ماهیت آنها الزامات امنیت اطلاعات مورد توجه قرار گرفته است؟ آیا این الزامات امنیتی، پیوست قراردادهای کاری شده است؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا برای تمامی پروژه‌ها ارزیابی مخاطرات امنیت اطلاعات انجام می‌شود؟					
۳	آیا مخاطرات امنیت اطلاعات، به صورت دوره‌ای در تمامی پروژه‌ها بررسی و در صورت لزوم بازنگری می‌شوند؟					
٤	آیا در مدیریت پروژه‌ها مسئولیت‌های امنیت اطلاعات تعریف می‌شود؟					
٥	آیا به منظور شناسایی درست الزامات امنیت اطلاعات، از روش‌های متنوعی استفاده می‌شود (مثلاً الزامات انطباق با خط‌مشی‌ها و مقررات، مرور حوادث امنیتی و درس آموزه‌های آنها، مدل‌سازی تهدید یا استفاده از آسیب‌پذیری‌های شناسایی شده)؟					
٦	آیا الزامات و کنترل‌های امنیتی، متناسب با ارزش کسب‌وکاری اطلاعات بوده و با در نظر گرفتن تأثیر منفی ناشی از نداشتن امنیت وضع شده‌اند؟					
۷	آیا هنگام خرید یا توسعه محصولات نرم‌افزاری، الزامات امنیت اطلاعات در نظر گرفته می‌شود؟					
الف ۹-۵- موجودی اطلاعاتی و سایر دارایی‌های مربوطه						
۱	آیا تمام تجهیزات و دارایی‌های اطلاعاتی شرکت شناسایی شده‌اند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا فهرستی از دارایی‌های اطلاعاتی مهم، گردآوری و به صورت مناسب از آنها حفاظت می‌شود؟					
۳	آیا فهرست دارایی‌های اطلاعاتی به‌روزرسانی می‌شود؟					
٤	آیا برای هر دارایی اطلاعاتی، مالکی تعیین شده است؟					
٥	آیا کارکنان، مسئولیت‌های امنیتی دارایی‌هایی که مالکیت آنها را بر عهده دارند، به خوبی دانسته و این مسئولیت به صورت رسمی به آنها ابلاغ شده است؟					
الف ۱۰-۵- استفاده پسندیده از اطلاعات و دارایی‌ها						
۱	آیا قوانینی که استفاده پسندیده از اطلاعات و دارایی‌ها را تعریف می‌کنند مشخص، مستند و رعایت می‌شود؟					
۲	آیا کارکنان، پیمانکاران و اشخاص سومی که از دارایی‌های شرکت استفاده می‌کنند، از الزامات امنیت اطلاعات آنها آگاهی لازم را دارند؟					
۳	آیا رویه‌هایی برای کنترل، تبادل و ذخیره اطلاعات مطابق با سطح طبقه‌بندی دارایی‌ها ایجاد شده است؟					
الف ۱۱-۵- بازگرداندن دارایی‌ها						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا کارکنان و پیمانکاران، تمامی دارایی‌ها را در هنگام خاتمه استخدام یا قرارداد همکاری‌شان، بر اساس یک رویه رسمی به شرکت عودت می‌دهند؟					
الف ۱۲-۵- طبقه‌بندی اطلاعات						
۱	آیا اصول و مبنایی برای طبقه‌بندی اطلاعات در شرکت ایجاد شده است؟					
۲	آیا سند خط‌مشی طبقه‌بندی اطلاعات، با توجه به ارزش و حساسیت اطلاعات شرکت تدوین شده است؟					
۳	آیا رویه طبقه‌بندی اطلاعات، مطابق با آخرین تغییرات صورت گرفته در ارزش، حساسیت و اهمیت دارایی‌های شرکت به‌روزرسانی می‌شود؟					
٤	آیا نیازمندی‌های کسب‌وکار و الزامات قانونی، قراردادی و بالادستی، در رویه طبقه‌بندی اطلاعات شرکت لحاظ شده است؟					
٥	آیا تمام دارایی‌های اطلاعاتی شرکت، از لحاظ سطح محرمانگی اطلاعات آنها طبقه‌بندی شده‌اند؟					
الف ۱۳-۵- برچسب‌گذاری اطلاعات						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا روال مشخصی برای کنترل و برچسب‌گذاری اطلاعات طبقه‌بندی شده، تدوین گردیده است؟					
۲	آیا رویه‌های تدوین شده، به درستی توسط کارکنان رعایت می‌شوند؟					
۳	آیا دارایی‌های اطلاعاتی به صورت مناسب برچسب‌گذاری می‌شوند (مشخص شدن سطح طبقه‌بندی محرمانگی آنها)؟					
الف ۱۴-۵- تبادل اطلاعات						
۱	آیا خط‌مشی‌ها و رویه‌هایی جهت تبادل امن اطلاعات، به واسطه استفاده از تمامی انواع امکانات ارتباطی ایجاد شده است؟					
۲	آیا یک روش اجرایی برای امنیت تبادل اطلاعات در مقابل حملات خرابکارانه‌ای همچون کپی‌برداری، دستکاری، تخریب، حذف، تغییر غیرمجاز و غیره تدوین شده است؟					
۳	آیا یک روش اجرایی برای تشخیص و حفاظت در مقابل بدافزارها که ممکن است توسط تبادل اطلاعات از طریق شبکه منتشر شوند، تدوین شده است؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
٤	آیا در این روش اجرایی به منظور حفاظت از اطلاعات حساس تبادلی مانند ضمیمه پیام‌ها الزاماتی گفته شده است؟					
٥	آیا از فنون رمزنگاری برای تبادل اطلاعات استفاده می‌شود؟					
٦	آیا امکانات و ابزارهای ارتباط جمعی (مثل ایمیل)، کنترل و محدود شده است؟					
٧	آیا آموزش‌های اولیه و احتیاطی لازم در خصوص تبادل امن اطلاعات به کاربران داده شده است؟					
٨	آیا توافق‌نامه‌هایی جهت کنترل و مدیریت تبادل اطلاعات بین شرکت و اشخاص سوم بیرونی ایجاد شده است؟					
٩	آیا اطلاعات ارسالی از طریق پیام‌رسانی الکترونیکی (مانند ایمیل) محافظت می‌شوند؟					
الف ۱۵-۵- کنترل دسترسی						
١	آیا خط‌مشی کنترل دسترسی، مطابق با نیازمندی‌های امنیت اطلاعات شرکت تهیه، تدوین و ابلاغ شده است؟					
٢	آیا این خط‌مشی، به صورت دوره‌ای بازنگری و به‌روزرسانی می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۳	آیا این خط‌مشی، نیازمندی‌های امنیتی برنامه‌های کاربردی کسب‌وکار را پوشش می‌دهد؟					
٤	آیا سطوح دسترسی عمومی برای کارکنان دارای مشاغل متعارف در شرکت مشخص شده است؟					
٥	آیا در روال اعطای دسترسی به کاربران، نقش‌های کنترل دسترسی مانند تقاضای دسترسی، مجوزدهی دسترسی و اعطای دسترسی تفکیک شده‌اند؟					
٦	آیا سوابقی مبنی بر مجوزهای کاربرانی که به اطلاعات حساس دسترسی دارند، وجود دارد؟					
۷	آیا روال دسترسی به نحوی انجام می‌شود که دسترسی عموم به اطلاعات محدود گردد، مگر آنکه به صراحت اجازه دسترسی داده شده باشد؟					
۸	آیا کنترل‌های مدیریتی و رویه‌ای برای حفاظت از دسترسی به شبکه و سرویس‌های آن وجود دارد؟					
۹	آیا این اطمینان حاصل می‌شود که کاربران تنها در صورت اعطای مجوز رسمی، اجازه دسترسی به شبکه و سرویس‌های آن را دارند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱۰	آیا رویه‌ای برای تعیین سطوح دسترسی به شبکه و سرویس‌های آن و نیز احراز هویت کاربران ایجاد شده است؟					
۱۱	آیا از ابزار خاصی برای دسترسی به شبکه و سرویس‌های آن استفاده می‌شود (مانند VPN یا توکن)؟					
	الف ۱۶-۵- مدیریت هویت					
۱	آیا چرخه عمر هویت‌ها به صورت کامل مدیریت می‌شود؟					
۲	آیا فرایند مدونی برای اعطا و لغو دسترسی کاربران و راهبران به شبکه و سرویس‌های آن و همچنین برنامه‌های کاربردی وجود دارد؟					
	الف ۱۷-۵- اطلاعات احراز هویت					
۱	آیا یک فرایند مدیریتی برای کنترل تخصیص کلمه‌های عبور کاربران ایجاد شده است؟					
۲	آیا اطلاعات مربوط به احراز هویت، تنها در اختیار کاربر مورد نظر قرار می‌گیرد؟					
۳	آیا اطلاعات احراز هویت پیش‌فرض تولیدکنندگان تجهیزات و برنامه-های کاربردی، بلافاصله پس از نصب و عملیاتی شدن تغییر می‌کند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
٤	آیا کاربران به پیروی از دستورالعمل‌های سازمانی در خصوص استفاده از اطلاعات محرمانه احراز هویت ملزم شده‌اند؟					
٥	آیا کاربران، شیوه‌های امنیتی مناسبی را برای انتخاب و نگهداری کلمه عبور خود انتخاب می‌کنند؟					
٦	آیا کلمات عبور کاربران دارای حداقل نیازمندی‌های لازم و کافی می‌باشد (مانند طول کافی، پیچیدگی، عدم امکان حدس زدن و غیره)؟					
٧	آیا سازوکاری وجود دارد که از تولید یا استفاده از واژگان تکراری در احراز هویت کاربران جلوگیری کند؟					
٨	آیا از سیستم مدیریت کلمه عبور استفاده می‌شود؟					
٩	آیا سیستم مدیریت کلمه عبور می‌تواند به صورت تعاملی کیفیت لازم را برای تولید کلمات عبور تضمین کند؟					
١٠	آیا سیستم مدیریت کلمه عبور، کاربران را وادار به تغییر کلمات عبور در اولین ورود به سیستم می‌کند؟					
١١	آیا سیستم مدیریت کلمه عبور، انتخاب کلمات عبور باکیفیت را اجبار می‌کند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱۲	آیا سیستم مدیریت کلمه عبور، تغییرات کلمات عبور را به طور منظم و در صورت نیاز اجبار می‌کند؟					
۱۳	آیا سیستم مدیریت کلمه عبور، سابقه‌ای از کلمات عبور را نگهداری و از استفاده مجدد آنها جلوگیری می‌کند؟					
	الف ۱۸-۵- حقوق دسترسی					
۱	آیا برای اعطا یا لغو دسترسی به سیستم‌ها، سرویس‌ها و سامانه‌های اطلاعاتی، یک روش اجرایی رسمی دسترسی برای ثبت و حذف کاربر وجود دارد؟					
۲	آیا روش اجرایی کنترل دسترسی، چگونگی اعطای دسترسی به سرویس‌ها و سیستم‌های اطلاعاتی را توضیح می‌دهد؟					
۳	آیا روش اجرایی کنترل دسترسی توضیح می‌دهد پس از خروج افراد از شرکت، چگونه دسترسی به سرویس‌ها و سیستم‌های اطلاعاتی لغو می‌شوند؟					
٤	آیا در روش اجرایی کنترل دسترسی، اختصاص یک شناسه کاربری یکتا به هر یک از کاربران الزامی شده است؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۵	آیا بررسی‌های دوره‌ای برای حذف یا مسدود کردن شناسه‌ها یا حساب‌های کاربری بدون استفاده و اضافی انجام می‌شود؟					
٦	آیا برای اعطا یا لغو حقوق دسترسی تمام کاربران به سامانه‌ها و سرویس‌ها یک روش اجرایی رسمی تأمین دسترسی کاربر، تدوین و اجرا شده است؟					
۷	آیا سطح دسترسی اعطا شده به کاربران، با خط‌مشی دسترسی و وظایف سازمانی آنها تناسب دارد؟					
۸	آیا اخذ مجوز دسترسی برای استفاده از سامانه‌های اطلاعاتی یا سرویس‌ها از مالک آنها صورت می‌گیرد؟					
۹	آیا اعطای حقوق دسترسی کاربران صرفاً پس از گذراندن روال مجوزدهی و احراز هویت انجام می‌شود؟					
۱۰	آیا سوابق حقوق دسترسی اعطا شده برای دسترسی به سامانه‌های اطلاعاتی و سرویس‌ها نگهداری می‌شود؟					
۱۱	آیا حقوق دسترسی کاربران، پس از تغییر شغل یا وظیفه سازمانی آنها بلافاصله بازنگری و به‌روزرسانی می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱۲	آیا حقوق دسترسی کاربران، به صورت دوره‌ای و منظم بررسی و در صورت نیاز بازنگری می‌شود؟					
۱۳	آیا روش‌های اجرایی رسمی برای بازنگری حقوق دسترسی و اختیارات ویژه کاربران وجود دارد؟					
۱٤	آیا مدیران، حقوق دسترسی و اختیارات ویژه کاربران را جهت اطمینان از عدم وجود حقوق ویژه غیرمجاز، به طور منظم بازنگری می‌کنند؟					
۱۵	آیا حقوق دسترسی کاربران، در زمان تغییر یا ترفیع شغل آنها بررسی و بازنگری می‌شود؟					
۱٦	آیا تغییرات در حقوق دسترسی حساب‌های کاربری دارای حقوق ویژه به صورت منظم گزارش‌گیری می‌شود؟					
۱۷	آیا حقوق دسترسی کارکنان به اطلاعات و امکانات پردازش اطلاعات به محض خاتمه خدمت آنها لغو می‌شود؟					
۱۸	آیا حقوق دسترسی پیمانکاران و مشتریان به اطلاعات و امکانات پردازش اطلاعات به محض خاتمه قرارداد آنها لغو می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱۹	آیا در هنگام تغییر وظایف/ سمت شغلی، دسترسی افراد به اطلاعات و امکانات پردازش اطلاعات مجدداً بازنگری و تنظیم می‌شود؟					
الف ۱۹-۵- امنیت اطلاعات در روابط با تأمین‌کنندگان						
۱	آیا یک خط‌مشی برای دسترسی تأمین‌کنندگان به دارایی‌های اطلاعاتی شرکت وجود دارد؟					
۲	آیا با تأمین‌کنندگان بر روی الزامات امنیت اطلاعات جهت کاهش مخاطرات مرتبط با دسترسی آنها توافق می‌شود؟					
۳	آیا نوع اطلاعاتی که تأمین‌کنندگان می‌توانند به آنها دسترسی داشته باشند، مشخص شده است؟					
الف ۲۰-۵- لحاظ کردن امنیت اطلاعات در توافق‌نامه‌های با تأمین‌کنندگان						
۱	آیا توافق‌نامه‌های امنیتی (مانند NDA) با اشخاص سوم منعقد شده است؟					
۲	آیا الزامات امنیت اطلاعات در توافق‌نامه‌ها و قراردادهای هر یک از تأمین‌کنندگان لحاظ می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۳	آیا توافق‌نامه‌های امنیتی با اشخاص سوم به صورت دوره‌ای یا در صورت بروز موارد نقض امنیت اطلاعات مورد بازنگری قرار می‌گیرد؟					
٤	آیا توافق‌نامه سطح ارایه خدمات (SLA) در موارد مورد نیاز در قراردادهای تأمین‌کنندگان، به صورت مستند پیوست یا جزئی از قرارداد آنها آورده شده است؟					
الف ۲۱-۵- مدیریت امنیت اطلاعات در زنجیره تأمین ICT						
۱	آیا توافق‌نامه با تأمین‌کنندگان، دربرگیرنده مخاطرات امنیت اطلاعات مرتبط با خدمات اطلاعات و ارتباطات و زنجیره تأمین محصول است؟					
الف ۲۲-۵- پایش، بازنگری و مدیریت تغییر خدمات تأمین‌کننده						
۱	آیا بر روی تحویل خدمت، فعالیت‌ها، گزارش‌ها، سوابق و عملکرد اشخاص سوم (اعم از تأمین‌کنندگان و پیمانکاران) نظارت می‌شود؟					
۲	آیا تغییرات در تحویل خدمات شخص سوم، کنترل و مدیریت می‌شود (کنترل‌ها می‌توانند در رابطه با حساسیت اطلاعات کسب‌وکار، سیستم‌ها و فرایندهای درگیر و نیز ارزیابی مجدد مخاطره باشند)؟					
الف ۲۳-۵- امنیت اطلاعات در استفاده از خدمات ابری						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا فرایندهایی برای اکتساب، استفاده، مدیریت و خاتمه خدمت ابری مطابق با الزامات امنیت اطلاعات شرکت ایجاده شده است؟					
۲	آیا دسترسی ارایه‌دهنده خدمات ابری به داده‌ها و اطلاعات میزبانی شده، تحت کنترل قرار دارد؟					
الف ۲۴-۵- برنامه‌ریزی و آمادگی برای مدیریت رخدادهای امنیت اطلاعات						
۱	آیا تمهیداتی به منظور اطمینان از پاسخ سریع، مؤثر و منظم به حوادث امنیت اطلاعات در نظر گرفته شده است؟					
۲	آیا مسئولیت‌های پاسخ به حوادث امنیت اطلاعات تعیین شده است؟					
۳	آیا مسائل مربوط به حوادث امنیت اطلاعات، توسط پرسنل شایسته راهبری و مدیریت می‌شوند؟					
٤	آیا یک نقطه تماس (PoC) برای تشخیص حوادث امنیتی و گزارش-دهی آنها تعیین شده است؟					
٥	آیا روش اجرایی پاسخ به حوادث امنیت اطلاعات ایجاد شده است؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
٦	آیا رویه‌های پاسخ به حوادث امنیت اطلاعات، شامل فعالیت‌های اولیه‌ای که کاربران در هنگام مواجهه با حادثه باید آنها را انجام دهند، می‌باشد؟					
۷	آیا کارایی و اثربخشی رویه‌های پاسخ به حوادث، به صورت دوره‌ای یا هنگام تغییر در دارایی‌های اطلاعاتی و فرایندهای اجرایی مورد بازنگری قرار می‌گیرد؟					
الف ۲۵-۵- ارزیابی و تصمیم‌گیری درباره رویدادهای امنیت اطلاعات						
۱	آیا رویدادها و رخدادهای امنیت اطلاعات بر اساس یک معیار توافق شده دسته‌بندی می‌شوند؟					
۲	آیا رویدادهای امنیت اطلاعات به منظور تعیین اینکه حادثه محسوب می‌شوند یا خیر، مورد تحلیل و بررسی قرار می‌گیرند؟					
۳	آیا نتایج تصمیم و ارزیابی برای ارجاعات آتی ثبت و نگهداری می‌شود؟					
الف ۲۶-۵- پاسخ به رخدادهای امنیت اطلاعات						
۱	آیا روش اجرایی مستند شده‌ای به منظور پاسخ به رخدادهای امنیت اطلاعات وجود دارد؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا پس از وقوع یک حادثه، شواهد آن به موقع جمع‌آوری می‌شود؟					
۳	آیا تجزیه‌وتحلیل قانونی (Forensic) رخدادهای امنیت اطلاعات انجام می‌شود؟					
٤	آیا برای تحلیل‌های آتی، فعالیت‌های پاسخگویی به حوادث امنیت اطلاعات به درستی ثبت و نگهداری می‌شوند؟					
٥	آیا با ضعف‌های امنیت اطلاعات که سبب بروز حادثه امنیتی شده یا به وقوع آن کمک می‌کنند، به طور مناسب برخورد می‌شود؟					
٦	آیا تیمی به منظور پاسخ به رخدادهای امنیت اطلاعات وجود دارد؟					
۷	آیا وقوع حوادث امنیت اطلاعات یا جزئیات آن با افراد داخلی، خارجی یا سازمان‌های مرتبط (که نیاز به این اطلاعات دارند) به اشتراک گذاشته می‌شود؟					
الف ۲۷-۵- یادگیری از رخدادهای امنیت اطلاعات						
۱	آیا دانش کسب شده از تحلیل و رفع حوادث امنیت اطلاعات برای کاهش احتمال یا اثر حوادث آتی مورد استفاده قرار می‌گیرد؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا سازوکارهایی برای ایجاد امکان نظارت بر نوع، وسعت و هزینه حوادث امنیت اطلاعات وجود دارد؟					
۳	آیا اطلاعاتی که از شواهد حوادث امنیت اطلاعات به دست می‌آیند برای شناسایی تکرار یا شدت اثر حوادث استفاده می‌شوند؟					
	الف ۲۸-۵- جمع‌آوری شواهد					
۱	آیا رویه‌هایی برای شناسایی، جمع‌آوری، اکتساب و حفظ اطلاعاتی که می‌توانند به عنوان شواهد مورد استفاده قرار گیرند، تعریف شده است؟					
۲	آیا شواهد لازم برای پیگیری علیه یک فرد یا سازمان (به عنوان عامل حادثه) پس از وقوع یک حادثه امنیت اطلاعات گردآوری می‌شود؟					
۳	آیا حفظ شواهد مربوط به حوادث امنیتی، هر زمان که یک اقدام مدنی یا کیفری ممکن است لازم باشد، انجام می‌شود؟					
٤	آیا مدارک و شواهد جمع‌آوری شده مبنی بر وقوع حادثه امنیتی به عنوان اطلاعات دارای طبقه‌بندی بایگانی می‌شوند؟					
٥	آیا از افشای مدارک و شواهد جمع‌آوری‌شده مبنی بر وقوع حادثه امنیتی جلوگیری می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
	الف ۲۹-۵- امنیت اطلاعات در هنگام اختلال					
۱	آیا طرح‌هایی برای تداوم کسب‌وکار و بازیابی و از سرگیری عملیات کسب‌وکار بعد از ایجاد وقفه یا بروز نقص در فرایندهای حیاتی کسب‌وکار، طراحی و مستند شده است؟					
۲	آیا الزامات تداوم امنیت اطلاعات در فرایندهای مدیریت تداوم کسب-وکار و بازیابی از بحران دیده شده است؟					
۳	آیا رویدادهایی که می‌توانند باعث ایجاد وقفه در فرایندهای کسب‌وکاری شرکت شوند، شناسایی شده‌اند؟					
٤	آیا احتمال آنکه در فرایندهای کسب‌وکاری، توسط رویدادهای مشخص شده وقفه‌ای ایجاد شود، تخمین زده شده است؟					
٥	آیا تأثیری که روند وقفه‌ها می‌تواند بر امنیت اطلاعات شرکت داشته باشد، برآورد شده است؟					
٦	آیا الزاماتی برای امنیت اطلاعات و تداوم آن در شرایط نامطلوب مانند وقوع بحران تعیین شده است؟					
	الف ۳۰-۵- آمادگی ICT برای تداوم کسب‌وکار					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا یک ساختار مدیریتی با استفاده از پرسنل شایسته و دارای تجربه و اختیارات لازم، جهت آمادگی و پاسخگویی به رویدادهای مخرب در نظر گرفته شده است؟					
۲	آیا پرسنل دارای اختیارات، مسئولیت و صلاحیت لازم برای مدیریت حوادث و حفظ امنیت اطلاعات تعیین شده‌اند؟					
۳	آیا طرح‌ها و روش‌هایی برای پاسخگویی و بازیابی بحران، مستند و تأیید شده است؟ طرح‌هایی مبنی بر اینکه چگونه شرکت سطح امنیت اطلاعات خود را در یک سطح از پیش تعیین شده حفظ کند.					
٤	آیا طرح‌های تداوم کسب‌وکار و بازیابی از بحران، نقش‌ها و مسئولیت‌ها را به صورت شفاف جهت از سرگیری فرایندهای کسب‌وکار مشخص نموده است؟					
٥	آیا نیازمندی‌های پیش‌بینی شده در طرح‌های تداوم کسب‌وکار و بازیابی از بحران تأمین شده است؟					
٦	آیا حیاتی‌ترین فرایندهای کسب‌وکار، مشخص و اولویت‌بندی شده‌اند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۷	آیا طرح‌های تداوم کسب‌وکار امکان از سرگیری سرویس‌های اطلاعاتی را در بازه‌های زمانی مورد نیاز فراهم می‌کنند؟					
۸	آیا مخاطره‌هایی که باعث تهدید امنیت فرایندها و دارایی‌های کسب‌وکار می‌شوند، مشخص شده‌اند؟					
۹	آیا جهت اطمینان از مطابقت عملکرد فرایندهای تداوم امنیت اطلاعات و روش‌ها و کنترل‌های آن با اهداف تداوم امنیت اطلاعات، مانور و آزمایش انجام می‌شود؟					
۱۰	آیا طرح‌های تداوم امنیت اطلاعات، روش‌ها و کنترل‌های آن به طور مرتب به منظور بررسی مؤثر و به‌روز بودن آنها آزمایش می‌شوند (از نظر میزان اعتبار و اثربخشی)؟					
۱۱	آیا نقاط قوت و ضعف طرح‌های تداوم امنیت اطلاعات بررسی شده و در صورت نیاز، طرح‌های جایگزین تدوین می‌شوند؟					
الف ۳۱-۵- الزامات قانونی، حقوقی، مقرراتی و قراردادی						
۱	آیا الزامات قانونی، قراردادی و آیین‌نامه‌ای بالاسری و متناسب با رویکرد شرکت در خصوص امنیت اطلاعات به وضوح تعریف، مدون و به‌روز نگه داشته می‌شوند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا الزامات قانونی، قراردادی و آیین‌نامه‌ای بالادستی و متناسب با رویکرد شرکت در خصوص امنیت اطلاعات رعایت می‌شوند؟					
۳	آیا اسناد، در راستای انطباق سیستم‌های اطلاعاتی با الزامات قانونی و قراردادی بالادستی به‌روزرسانی می‌شوند؟					
٤	آیا کنترل‌های رمزنگاری در انطباق با توافق‌نامه‌ها، قوانین و آیین‌نامه‌ها به کار گرفته می‌شوند؟					
٥	آیا محدودیت‌های فنی و کسب‌وکاری جهت استفاده از کنترل‌های رمزنگاری برطرف شده است؟					
الف ۳۲-۵- حقوق مالکیت معنوی						
۱	آیا رویه‌ای برای اطمینان از انطباق شرکت با حقوق و الزامات مالکیت معنوی و نرم‌افزارهای دارای حقوق تجاری وجود دارد؟					
۲	آیا در فرایند تهیه محصولات نرم‌افزاری، مسایل مربوط به حق کپی‌رایت رعایت می‌شود؟					
۳	آیا از نسخه‌برداری، تبدیل و ... محصولات دارای حقوق مالکیت معنوی جلوگیری می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
٤	آیا مدارکی مبنی بر مشخص کردن مالکیت معنوی محصولاتی که دارای حقوق مالکیت معنوی هستند، وجود دارد؟					
٥	آیا نرم‌افزارهای نصب شده، به صورت قانونی خریداری شده‌اند؟					
٦	آیا یک خط‌مشی جهت امحا یا انتقال محصولات دارای حقوق مالکیت معنوی به دیگران وجود دارد؟					
الف ۳۳-۵- حفاظت از سوابق						
١	آیا از سوابق در برابر گم شدن، تخریب و تحریف محافظت می‌شود؟					
٢	آیا روش‌های موجود برای محافظت از سوابق سازمانی، مطابق با الزامات مقرراتی و آیین‌نامه‌ای، قراردادی و کسب‌وکاری هستند؟					
٣	آیا الزاماتی برای نگهداری، ذخیره، اداره کردن و همچنین امحای اطلاعات و سوابق تدوین شده‌اند؟					
الف ۳۴-۵- حریم خصوصی و حفاظت از اطلاعات هویت شخصی						
١	آیا از حریم خصوصی و اطلاعات کارکنان مطابق با مقررات و آیین‌نامه‌های مرتبط محافظت می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
الف ۳۵-۵- بازنگری مستقل امنیت اطلاعات						
۱	آیا مدیریت، بازنگری مستقلی از کفایت، تناسب و اثربخشی رویکرد امنیت اطلاعات شرکت انجام می‌دهد (در فواصل زمانی برنامه‌ریزی شده یا در صورت وقوع تغییرات مهم)؟					
الف ۳۶-۵- انطباق با خط‌مشی‌ها، قوانین و استانداردهای امنیت اطلاعات						
۱	آیا مدیران از اینکه روش‌های اجرایی امنیتی در حیطه مسئولیت‌شان به درستی اجرا می‌شوند، اطمینان حاصل می‌کنند؟					
۲	آیا روش‌های اجرایی امنیتی، در انطباق با خط‌مشی‌های امنیتی شرکت هستند؟					
۳	آیا مدیران، علت عدم انطباق‌های شناسایی شده را بررسی می‌کنند؟					
٤	آیا مدیران، اقدام‌های اصلاحی مناسب را جهت رفع عدم انطباق‌ها تعیین و اجرا می‌نمایند؟					
٥	آیا مدیران، اثربخشی یا ضعف‌های اقدام‌های اصلاحی انجام شده را بررسی می‌کنند؟					
الف ۳۷-۵- رویه‌های عملیاتی مدون						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا روش‌های اجرایی مدیریت تجهیزات و سیستم‌های اطلاعاتی، تدوین و نگهداری می‌شود؟					
۲	آیا روش‌های اجرایی مدون شده، به درستی در دسترس تمام کاربرانی که به آنها نیاز دارند، قرار می‌گیرند؟					
۳	آیا دستورالعمل‌هایی جهت مشخص نمودن جزئیات هر یک از وظایف در هر شغل وجود دارد؟					
الف ۶- کنترل‌های فردی						
الف ۱-۶- گزینش						
۱	آیا رویه‌های اجرایی، معیارها و محدودیت‌هایی جهت بررسی پیشینه داوطلبان استخدام وجود دارد؟					
۲	آیا بررسی پیشینه، مطابق با قوانین کار، آیین‌نامه‌های مرتبط و اصول اخلاقی انجام می‌شود؟					
۳	آیا پیشینه افرادی که اطلاعات و امکانات حساس پردازش اطلاعات را در اختیار دارند، به صورت دقیق‌تر انجام می‌شود؟					
الف ۲-۶- شرایط و ضوابط استخدام						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا مفاد و شرایط قرارداد استخدام، نمایانگر مسئولیت‌های شرکت، کارکنان و پیمانکاران در قبال امنیت اطلاعات است؟					
۲	آیا مسئولیت‌های امنیت اطلاعات، در قرارداد کارکنان ذکر شده است؟					
۳	آیا مسئولیت‌های امنیت اطلاعات، در قرارداد پیمانکاران گفته شده است؟					
٤	آیا نقش‌ها و مسئولیت‌های امنیتی داوطلبان، در طول فرایند پیش از استخدام به ایشان ابلاغ می‌شود؟					
۵	آیا اقدام‌هایی که در صورت نادیده گرفتن الزامات امنیتی انجام می‌شوند، در قرارداد کارکنان، پیمانکاران و اشخاص سوم بیان شده است؟					
الف ۳-۶- آگاهی‌بخشی، تحصیل و آموزش امنیت اطلاعات						
۱	آیا فرایندی برای آموزش و آگاهی‌بخشی امنیتی در شرکت وجود دارد (شامل آموزش تخصصی، آگاهی‌بخشی عمومی به کارکنان و پیمانکاران در صورت نیاز)؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا کارکنان و پیمانکاران، آموزش‌های مورد نیاز را در خصوص خط‌مشی‌ها و روش‌های اجرایی مرتبط با وظایف کاری خود را می‌بینند؟					
۳	آیا کارکنان، آموزش امنیت اطلاعات که با نقش و مسئولیت‌های آنها مرتبط است را می‌بینند؟					
٤	آیا کارکنان از نسخه‌های به‌روز روش‌های اجرایی و خط‌مشی‌های امنیتی آگاه شده و در صورت نیاز، در دسترس آنها قرار می‌گیرد؟					
٥	آیا پیمانکاران از نسخه‌های به‌روز روش‌هایی اجرایی و خط‌مشی‌های امنیتی آگاه شده و در صورت نیاز، در دسترس آنها قرار می‌گیرد؟					
الف ۴-۶- فرایند انضباطی						
۱	آیا یک فرایند انضباطی رسمی برای برخورد با کارکنانی که مرتکب نقص امنیتی شده‌اند، وجود دارد؟					
الف ۵-۶- مسئولیت‌های پس از خاتمه یا تغییر شغل						
۱	آیا مسئولیت‌ها و وظایف امنیت اطلاعات، در زمان خاتمه/ تغییر شغل (کارمندان و پیمانکاران) تعریف شده و مورد ارزیابی قرار می‌گیرد؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا واحد منابع انسانی، بر فرایند خاتمه یا تغییر شغل کارکنان نظارت دارد؟					
۳	آیا مسئولیت‌ها و وظایف امنیت اطلاعات پس از تغییر شغل یا خاتمه اشتغال، به شیوه مناسبی به کارکنان و پیمانکاران اطلاع‌رسانی می‌شود؟					
الف ۶-۶- توافق‌نامه‌های محرمانگی یا عدم افشا						
۱	آیا الزامات در راستای نیازهای شرکت برای توافقات محرمانگی شناسایی شده‌اند؟					
۲	آیا تعهدنامه عدم افشای اطلاعات (NDA) از کارکنان گرفته می‌شود؟					
۳	آیا کفایت تعهدنامه عدم افشای اطلاعات بازنگری می‌شود؟					
٤	آیا در این تعهدنامه، الزامات قانونی و بالادستی مدنظر قرار گرفته است؟					
الف ۷-۶- دورکاری						
۱	آیا خط‌مشی و الزامات امنیتی برای کنترل و حفاظت از فعالیت‌های کار از راه دور، تدوین و تصویب شده است؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا تمهیدات امنیتی در خصوص دورکاری به کار گرفته می‌شوند (مثل محدودیت زمانی، نحوه دسترسی، کانال‌های ارتباطی و ...)؟					
۳	آیا عملیات لاگ‌برداری و پایش بر روی ارتباطات کار از راه دور به درستی انجام می‌شود؟					
الف ۸-۶- گزارش‌دهی رویداد امنیت اطلاعات						
۱	آیا رویدادهای امنیت اطلاعات با استفاده از کانال‌های گزارش‌دهی مدیریتی مناسب گزارش می‌شوند؟					
۲	آیا رویدادهای امنیتی در کمترین زمان ممکن گزارش می‌شوند؟					
۳	آیا تمامی پرسنل، نقطه تماس (PoC) گزارش‌دهی حوادث امنیتی را می‌شناسند؟					
٤	آیا نقطه تماس جهت گزارش‌دهی حوادث امنیتی، همیشه در دسترس است؟					
۵	آیا همه کارکنان به طور رسمی ملزم به ثبت و گزارش تمامی نقاط ضعف امنیتی مشاهده شده یا مشکوک در سیستم‌های اطلاعاتی و سرویس‌ها می‌باشند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
٦	آیا همه پیمانکاران به طور رسمی ملزم به ثبت و گزارش تمامی ضعف‌های امنیتی مشاهده شده یا مشکوک در سیستم‌های اطلاعاتی و سرویس‌ها هستند؟					
۷	آیا سازوکار گزارش‌دهی ضعف‌های امنیت اطلاعات ساده و در دسترس می‌باشد؟					
الف ۷- کنترل‌های فیزیکی						
الف ۱-۷- حصارهای امنیت فیزیکی						
۱	آیا یک خط‌مشی جهت حفظ امنیت فیزیکی و مدیریت مخاطرات به منظور جلوگیری از دسترسی‌های غیرمجاز به اماکن پردازش اطلاعات وجود دارد؟					
۲	آیا حصارها و موانع امنیت فیزیکی و محل قرارگیری و قدرت هر یک از حصارها متناسب با الزامات امنیتی دارایی‌های آن و نتایج ارزیابی مخاطرات است؟					
۳	آیا حصارهای امنیتی برای حفاظت از نواحی حاوی اطلاعات حساس یا حیاتی و تسهیلات پردازش اطلاعات، تعریف شده و مورد استفاده قرار می‌گیرد؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
٤	آیا از باجه‌ها یا میزهای پذیرش دارای خدمه برای محافظت از مکان‌های نگهداری اطلاعات و امکانات پردازش اطلاعات استفاده می‌شود؟					
٥	آیا سامانه کشف مزاحم جهت پوشش‌دهی درب‌ها و پنجره‌های قابل دسترس، متناسب با استانداردهای ملی و بین‌المللی نصب شده و مورد آزمون قرار می‌گیرد؟					
٦	آیا سیستم هشداردهنده و نظارت تصویری، در اماکن حیاتی مانند مرکز داده/ اتاق سرور وجود دارد؟					
٧	آیا تجهیزات پردازش اطلاعاتی که توسط شرکت مدیریت می‌شوند از تجهیزاتی که توسط اشخاص سوم بیرونی مدیریت می‌شوند، از نظر فیزیکی تفکیک شده‌اند؟					
الف ۲-۷- ورودی فیزیکی						
١	آیا از کنترل‌های مداخل فیزیکی برای محافظت از نواحی امن استفاده می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا کنترل‌های مداخل فیزیکی تنها به کارکنان مجاز اجازه دسترسی به نواحی امن را می‌دهند و توسط کنترل‌های دسترسی مناسب محدود شده‌اند؟					
۳	آیا تاریخ و ساعات ورود و خروج بازدیدکنندگان از نواحی امن ثبت می‌شود؟					
٤	آیا تمامی بازدیدکنندگان از نواحی حیاتی به همراه کارکنان بخش شبکه و حراست همراهی می‌شوند؟					
٥	آیا نواحی ورود و خروج نواحی حیاتی، توسط سامانه نظارت تصویری (دوربین)، کنترل و پایش می‌شوند؟					
٦	آیا کنترلی بر دسترسی اشخاص سومی که پشتیبانی سرویس‌ها را در نواحی امن انجام می‌دهند، وجود داشته و امکان دسترسی محدود و در مواقع ضروری برای آنها تعریف شده است؟					
۷	آیا حقوق دسترسی به نواحی امن به طور منظم بازنگری شده و در زمان لازم ابطال می‌گردد؟					
۸	آیا نقاط دسترسی عمومی، به منظور پیشگیری از ورود افراد غیرمجاز به ساختمان‌ها کنترل می‌شوند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۹	آیا نقاط دسترسی مانند نواحی تخلیه و بارگیری، از مناطق حاوی تسهیلات پردازش اطلاعات جدا شده‌اند؟					
۱۰	آیا از دستکاری تجهیزات وارد شده به شرکت، حین انتقال محافظت می‌شود؟					
۱۱	آیا تجهیزات وارد شده، در زمان ورود به محل ثبت می‌شوند؟					
الف ۳-۷- امن‌سازی دفاتر، اتاق‌ها و امکانات						
۱	آیا کنترل‌های امنیت فیزیکی برای دفاتر، اتاق‌ها، ساختمان‌ها و تجهیزات، طراحی و به کار گرفته شده است؟					
۲	آیا فعالیت‌ها و اطلاعات محرمانه از بیرون از محوطه قابل مشاهده هستند؟					
الف ۴-۷- پایش امنیت فیزیکی						
۱	آیا اماکن، به صورت مداوم از لحاظ دسترسی فیزیکی غیرمجاز، پایش و کنترل می‌شوند؟					
الف ۵-۷- حفاظت در برابر تهدیدات فیزیکی و محیطی						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا در خصوص حوادث بزرگ، فجایع طبیعی و حملات مخرب، تمهیداتی اندیشیده شده است؟					
۲	آیا راهنماهای ویژه‌ای جهت اجتناب از آسیب در زمان وقوع حادثه و حملات مخرب به کار گرفته شده است؟					
الف ۶-۷- کار در نواحی امن						
۱	آیا الزاماتی برای کنترل چگونگی انجام کار در محیط‌های امن وجود دارد؟					
۲	آیا نواحی امن به صورت فیزیکی قفل شده و به صورت دوره‌ای بازرسی می‌شوند؟					
۳	آیا کنترلی جهت ورود تجهیزات عکس‌برداری، فیلم‌برداری، ضبط صوت، گوشی هوشمند و غیره به نواحی امن وجود دارد؟					
الف ۷-۷- میز پاک و صفحه نمایش پاک						
۱	آیا خط‌مشی میز پاک برای کاغذها و رسانه‌های ذخیره‌سازی قابل حمل وجود دارد؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا خط‌مشی صفحه نمایش پاک برای تسهیلات پردازش اطلاعات وجود دارد؟					
۳	آیا الزامات امنیتی برای محافظت از اطلاعات محرمانه کاغذی یا رسانه‌های ذخیره‌سازی رعایت می‌گردد (برای مثال قرار دادن اطلاعات محرمانه در کشوهای قفل شده یا کمدهای قفل‌دار)؟					
٤	آیا الزامات امنیتی جهت قفل شدن صفحه نمایش به صورت خودکار در زمانی که مورد استفاده قرار نمی‌گیرد، رعایت می‌گردد؟					
٥	آیا الزامات امنیتی جهت عدم دسترسی غیرمجاز به اطلاعات محرمانه، بر روی چاپگرها رعایت شده است؟					
	الف ۸-۷- استقرار و حفاظت از تجهیزات					
۱	آیا تجهیزات پردازش اطلاعات در برابر مخاطرات ناشی از تهدیدها و خطرات محیطی مانند سرقت، آتش‌سوزی، انفجار، گردوغبار، تداخل منابع برق و غیره محافظت می‌شوند؟					
۲	آیا تجهیزات پردازش اطلاعات که با اطلاعات حساس سروکار دارند در برابر مخاطره قابل مشاهده بودن در هنگام استفاده محافظت می‌گردند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۳	آیا تجهیزات در موقعیت مناسب فیزیکی خارج از دسترسی غیرمجاز استقرار یافته‌اند؟					
٤	آیا رهنمودهایی جهت منع غذا خوردن، نوشیدن و سیگار کشیدن در اطراف تجهیزات پردازش اطلاعات تهیه شده است؟					
٥	آیا از دستکاری غیرمجاز و سرقت تجهیزات جلوگیری می‌شود؟					
٦	آیا برای تغییرات دما و تأثیر آن بر روی تجهیزات، تمهیداتی اندیشیده شده است؟					
۷	آیا برای تغییرات رطوبت و تأثیر آن بر روی تجهیزات، تمهیداتی اندیشیده شده است؟					
۸	آیا برای نوسانات برق و تأثیر آن بر روی تجهیزات، تمهیداتی اندیشیده شده است؟					
۹	آیا تجهیزات، در برابر لرزش و تکان خوردن محافظت می‌شوند؟					
۱۰	آیا جهت محافظت ساختمان در برابر رعدوبرق، تمهیداتی اندیشیده شده است؟					
الف ۹-۷- امنیت دارایی‌های خارج از سازمان						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا الزامات امنیتی برای حفاظت از تجهیزات خارج از محوطه رعایت می‌شود؟					
۲	آیا استقرار تجهیزات در خارج از ابنیه شرکت، پس از اخذ مجوز مدیریت انجام می‌شود؟					
۳	آیا دستورالعمل‌هایی جهت محافظت از تجهیزات خارج از محوطه وجود دارد (مانند محافظت در برابر قرار گرفتن در معرض میدان الکترومغناطیسی قوی)؟					
٤	آیا تجهیزات پردازش اطلاعات خارج از محوطه، متصدی و مالک مشخصی دارند؟					
الف ۱۰-۷- رسانه ذخیره‌سازی						
۱	آیا رویه‌هایی به منظور مدیریت رسانه‌های قابل حمل وجود دارد؟					
۲	آیا لیستی از رسانه‌های ذخیره‌سازی قابل حمل تهیه شده است؟					
۳	آیا انتقال رسانه‌های ذخیره‌سازی به محیط بیرون از شرکت، با اخذ مجوز انجام می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
٤	آیا اطلاعات حساس موجود بر روی رسانه‌های ذخیره‌سازی قابل حمل رمزنگاری می‌شوند؟					
٥	آیا افزونگی اطلاعات حساس موجود در رسانه‌های ذخیره‌سازی قابل حمل رعایت شده و عملیات پشتیبان‌گیری روی آنها انجام می‌شود؟					
٦	آیا برای امحای امن رسانه‌های ذخیره‌سازی که دیگر مورد نیاز نیستند، رویه‌ای وجود دارد؟					
٧	آیا روال امحای رسانه‌های ذخیره‌سازی به صورت امن انجام می‌شود؟					
٨	آیا رسانه‌های ذخیره‌سازی آسیب‌دیده یا تجهیزاتی که حاوی اطلاعات حساس هستند، به صورت فیزیکی امحا می‌شوند؟					
٩	آیا رسانه‌های حاوی اطلاعات از دسترسی غیرمجاز، سوءاستفاده یا پاک شدن احتمالی حفاظت می‌گردند؟					
١٠	آیا پیک یا حامل رسانه‌های اطلاعاتی، از لحاظ مدیریت شرکت مورد تأیید است؟					
١١	آیا رویه‌ای جهت تأیید هویت پیک‌ها وجود دارد؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱۲	آیا سوابق مربوط به محتوای رسانه‌ها و زمان انتقال و رسید مقصد نگهداری می‌شود؟					
۱۳	آیا از خروج دارایی‌های اطلاعاتی شرکت، بدون اخذ مجوز قبلی جلوگیری می‌شود؟					
۱٤	آیا کارکنان و اشخاص سومی که مجوز خروج دارایی‌ها را صادر می‌کنند، مشخص شده‌اند؟					
۱۵	آیا جهت بازگرداندن دارایی‌های اطلاعاتی، محدودیت زمانی مشخص شده و تاریخ برگشت جهت انطباق بررسی می‌گردد؟					
۱٦	آیا دارایی‌های اطلاعاتی در زمان خروج و بازگشت ثبت می‌شوند؟					
الف ۱۱-۷- امکانات پشتیبانی						
۱	آیا تجهیزات در برابر قطعی ناشی از خرابی امکانات پشتیبانی محافظت می‌شوند؟					
۲	آیا در هنگام قطعی برق از UPS استفاده می‌شود؟					
۳	آیا تجهیزات پردازشی در صورت از کار افتادن تجهیزات تهویه مطبوع و اعلان و اطفای حریق به خوبی محافظت می‌شوند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
٤	آیا درستی عملکرد امکانات پشتیبانی بررسی و تست می‌شود؟					
٥	آیا امکانات پشتیبانی در صورت لزوم برای تشخیص اختلال در عملکرد هشداردهی می‌شوند؟					
	الف ۱۲-۷- امنیت کابل‌کشی					
١	آیا از کابل‌کشی‌های برق و ارتباطات مورد استفاده برای انتقال داده یا پشتیبانی از سرویس‌های اطلاعاتی محافظت می‌شود؟					
٢	آیا کابل‌کشی برق جهت جلوگیری از تداخل، از کابل‌های شبکه تفکیک شده است؟					
٣	آیا از کابل‌های برق و کابل‌های ارتباطی در مقابل از بین رفتن و پوسیدگی محافظت می‌شود؟					
٤	آیا از کابل‌های برق و کابل‌های ارتباطی در مقابل قطع شدن غیرمجاز محافظت می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۵	آیا جهت امنیت کابل‌کشی سامانه‌های حساس، کنترل‌های لازم لحاظ شده است (مانند استفاده از محافظ‌های تداخل الکترومغناطیسی برای محافظت کابل‌ها، دسترسی کنترل شده به پنل‌های اتصال و اتاق‌های اتصالات کابل‌ها)؟					
الف ۱۳-۷- نگهداری از تجهیزات						
۱	آیا از تجهیزات به منظور حصول اطمینان از تداوم دسترس‌پذیری و صحت عملکردشان به درستی نگهداری می‌شود؟					
۲	آیا تجهیزات بر اساس مشخصات فنی و فواصل زمانی پیشنهاد شده از سمت تأمین‌کننده نگهداری می‌شوند؟					
۳	آیا سابقه فعالیت‌های نگهداری، اقدامات اصلاحی و پیشگیرانه و سابقه تمام خرابی‌ها و مشکلات ثبت می‌شود؟					
٤	آیا کارکنان سرویس و نگهداری تجهیزات، پیش از انجام کارشان مجوز دسترسی مربوطه را دریافت می‌کنند؟					
۵	آیا تجهیزات، قبل از بهره‌برداری و پس از تعمیر و نگهداری جهت اطمینان از عدم نقص بازرسی می‌شوند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
٦	آیا تمامی تعهدات قید شده در گارانتی‌ها برآورده می‌شود؟					
۷	آیا تمامی تعهدات قید شده در قراردادها توسط اشخاص سوم در خصوص پشتیبانی از تجهیزات رعایت می‌شود؟					
الف ۱۴-۷- امحا یا استفاده دوباره امن از تجهیزات						
۱	آیا برای امحا یا استفاده مجدد از اجزای تجهیزاتی که دارای حافظه هستند، رویه‌ای وجود دارد؟					
۲	آیا داده‌های رسانه‌های ذخیره‌سازی، قبل از امحا حذف یا به شیوه امنی بازنویسی می‌شوند؟					
۳	آیا تجهیزاتی که حاوی اطلاعات محرمانه یا حق نشر هستند، جهت امحا از نظر فیزیکی تخریب می‌شوند؟					
الف ۸- کنترل‌های فنی						
الف ۱-۸- دستگاه کاربر نهایی						
۱	آیا یک خط‌مشی امنیتی برای در نظر گرفتن مخاطرات تجهیزات ارتباطی و پردازشی تدوین شده است؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا تمهیدات امنیتی مانند سازوکارهای امنیتی، جداسازی، حفاظت فیزیکی، محدودیت نصب نرم‌افزار، فنون رمزنگاری، کنترل دسترسی، محافظت در برابر بدافزارها، آموزش و اطلاع‌رسانی در خصوص تجهیزات، اجرا و به کارگیری می‌شود؟					
۳	آیا الزامات امنیتی جهت استفاده از تجهیزات قابل حمل شخصی وجود دارد؟					
٤	آیا کاربران، اقداماتی را برای اطمینان از اینکه تجهیزات بدون متصدی به طور مناسبی حفاظت می‌شوند، انجام می‌دهند؟					
٥	آیا الزامات امنیتی و روش‌های اجرایی جهت محافظت از تجهیزات بدون مراقبت وجود داشته و کاربران نیز آگاهی لازم را از مسئولیت‌هایشان در این خصوص دارند؟					
الف ۲-۸- حقوق دسترسی ویژه						
۱	آیا تخصیص و استفاده از اختیارات ویژه (مانند اختیارات در سطح راهبر/ مدیر سیستم)، محدود و کنترل شده است؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا اختصاص دسترسی ویژه بنا به نیاز و نقش کاربر و مطابق با خط-مشی کنترل دسترسی و اصل کمترین حق سطح دسترسی انجام می-گردد؟					
۳	آیا در زمان اتمام نیازمندی‌های کاربر، حقوق دسترسی اعطا شده دوباره پس گرفته می‌شود؟					
٤	آیا سازوکارهای حفظ محرمانگی و اطلاعات احراز هویت در شناسه-های دسترسی مدیر سیستم استفاده، حفظ و نگهداری می‌شود؟					
الف ۳-۸- محدودسازی دسترسی به اطلاعات						
۱	آیا دسترسی کاربران به اطلاعات و سامانه‌های نرم‌افزاری شرکت مطابق با خط‌مشی کنترل دسترسی محدود شده است؟					
الف ۴-۸- دسترسی به کد منبع						
۱	آیا دسترسی به کد منبع نرم‌افزارها محدود به کاربران مجاز شده است؟					
۲	آیا از خرابی و از بین رفتن برنامه‌ها با قرار دادن کد منبع آنها در یک مکان مرکزی نظیر کتابخانه‌های کد منبع جلوگیری می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۳	آیا از خرابی و از بین رفتن برنامه‌ها با محدود کردن و کنترل دسترسی به کتابخانه‌های کد منبع آنها جلوگیری می‌شود؟					
٤	آیا از قرار دادن کتابخانه کد منبع برنامه‌ها بر روی سیستم‌های عملیاتی اجتناب می‌شود؟					
٥	آیا به‌روزرسانی کتابخانه‌های کد منبع برنامه و توزیع منابع برنامه برای برنامه‌نویس‌ها با اخذ مجوز مناسب انجام می‌شود؟					
٦	آیا هرگونه دسترسی به کتابخانه‌های کد منبع، نظارت و لاگ‌برداری می‌گردد؟					
۷	آیا اعمال هر تغییری در کتابخانه‌های کد منبع برنامه‌ها توسط رویه کنترل تغییرات محدود شده است؟					
الف ۵-۸- احراز هویت امن						
۱	آیا مطابق با نیازمندی‌های خط‌مشی کنترل دسترسی، سیستم‌ها و برنامه‌های کاربردی توسط فرایند ورود امن کنترل می‌گردند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا در زمانی که احراز هویت و سازوکار تشخیصی مناسبی مورد نیاز است از سازوکارهای رمزنگاری، کارت هوشمند، توکن‌ها و ابزار زیست-سنجی استفاده می‌شود؟					
۳	آیا سازوکار ورود، به صورتی امن شده است که تا قبل از زمان ورود معتبر کاربران، قسمتی از اطلاعات از سامانه فاش نشود؟					
٤	آیا سرویس تلاش برای ورود کاربران به سامانه‌ها از حملات متداول مانند Brute Force حفاظت شده است؟					
٥	آیا نقض امنیتی در عملیات ورود کاربران و نیز کلیه ورود و خروج به سامانه‌ها لاگ‌برداری می‌شود؟					
٦	آیا از راهکار عدم نمایش کلمه عبور در حین ورود اطلاعات توسط کاربر استفاده می‌شود؟					
۷	آیا کلمات عبور در حین عبور از محیط شبکه رمزنگاری می‌شوند؟					
۸	آیا نشست‌های غیرفعال کاربران در زمانی مشخص خاتمه می‌یابد؟					
۹	آیا زمان‌های اتصال جهت افزایش امنیت بیشتر در برنامه‌های کاربردی پرمخاطره و کاهش فرصت دسترسی‌های غیرمجاز محدود شده است؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
	الف ۶-۸- مدیریت ظرفیت					
۱	آیا فرایندی برای مدیریت ظرفیت در استفاده از منابع وجود دارد؟					
۲	آیا سیستم‌های اطلاعاتی و سرویس‌های عملیاتی که نیاز به مدیریت ظرفیت دارند، شناسایی شده‌اند؟					
۳	آیا نحوه پیکربندی و تنظیمات سیستم‌های اطلاعاتی و سرویس‌های عملیاتی به نحو مطلوبی انجام شده تا نیازهای ظرفیتی آنها با حفظ کیفیت سرویس کاهش یابد؟					
٤	آیا شاخص‌های عملکرد سیستم برای هر یک از سیستم‌های اطلاعاتی و سرویس‌های عملیاتی مشخص شده است؟					
٥	آیا میزان استفاده از منابع سیستم‌ها (و منابع انسانی) به منظور اطمینان از نیازمندی‌های آتی آنها پایش و بررسی می‌شود؟					
٦	آیا نیازهای آتی سیستم‌ها مطابق با مستند طرح مدیریت ظرفیت انجام می‌گردد؟					
	الف ۷-۸- حفاظت در برابر بدافزار					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا اقداماتی جهت محافظت در برابر بدافزارها صورت گرفته است (مانند تشخیص، پیشگیری، بازیابی، آگاهی‌رسانی و ...)؟					
۲	آیا یک خط‌مشی در خصوص جلوگیری از استفاده از نرم‌افزارهای غیرمجاز و نیز مخاطره تبادل فایل در محیط شبکه تدوین و اجرا شده است؟					
۳	آیا کنترل‌هایی در خصوص شناسایی و جلوگیری از دسترسی به برنامه‌های غیرمجاز و وب‌سایت‌های مخرب وضع و اجرا شده است؟					
٤	آیا برای کاهش آسیب‌پذیری‌های مورد بهره‌برداری بدافزارها از فرایندهای مدیریت آسیب‌پذیری استفاده می‌گردد؟					
٥	آیا یک سامانه به‌روز پایشی جهت کشف و برطرف کردن تهدیدات بدافزاری وجود دارد؟					
٦	آیا یک روال اجرایی برای آموزش، نحوه گزارش‌دهی و بازیابی سیستم‌ها در مقابل بدافزارها برای کاربران و مدیران وجود دارد؟					
۷	آیا یک محیط ایزوله و جداسازی شده در زمان‌های وقوع حادثه ناشی از بدافزار و اثرات سوء آن وجود دارد؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
	الف ۸-۸- مدیریت آسیب‌پذیری‌های فنی					
۱	آیا یک روش اجرایی جهت مدیریت آسیب‌پذیری‌های فنی وجود دارد؟					
۲	آیا اطلاعات به‌روز شده در مورد آسیب‌پذیری‌های فنی سیستم‌های اطلاعاتی، تهیه و نگهداری می‌شود؟					
۳	آیا فعالیت‌های مناسب و به موقع در پاسخ به شناسایی آسیب‌پذیری‌های فنی بالقوه صورت می‌گیرد؟					
٤	آیا نقش‌ها و مسئولیت‌ها و فناوری‌های مناسب در خصوص مدیریت آسیب‌پذیری‌ها مانند پایش آسیب‌پذیری، ارزیابی مخاطره آسیب-پذیری، مدیریت وصله و ردیابی دارایی‌ها و غیره تعریف و اجرا می-شود؟					
٥	آیا جهت واکنش مناسب به اعلان آسیب‌پذیری‌های فنی مرتبط، زمان‌بندی مشخصی تعریف شده است؟					
٦	آیا وصله‌های امنیتی قبل از نصب بر روی سیستم‌های عملیاتی، مورد آزمون و ارزیابی قرار می‌گیرند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۷	آیا مخاطرات ناشی از آسیب‌پذیری‌های فنی سیستم‌های اطلاعاتی ارزیابی می‌شود؟					
۸	آیا اقدامات و معیارهای مناسبی برای برطرف کردن مخاطرات و کاهش آسیب‌پذیری‌های فنی در نظر گرفته شده است؟					
۹	آیا فرایند مدیریت آسیب‌پذیری‌های فنی به صورت منظم پایش شده و به منظور اطمینان از کارایی و اثربخشی آنها ارزیابی می‌شود؟					
۱۰	آیا سیستم‌های اطلاعاتی به طور مرتب به منظور اطمینان از اینکه در انطباق با استانداردهای امنیتی هستند، بررسی می‌شوند؟					
۱۱	آیا برای بررسی انطباق فنی از ابزارهای خودکار استفاده می‌شود؟					
۱۲	آیا جهت تحلیل گزارش ابزارهای ارزیابی خودکار، از متخصصان و افراد خبره استفاده می‌شود؟					
۱۳	آیا از مهندسان و کارشناسان باتجربه برای بررسی و ارزیابی انطباق فنی استفاده می‌شود؟					
۱۴	آیا از آزمون‌های نفوذپذیری و ارزیابی آسیب‌پذیری‌ها به منظور شناسایی آسیب‌پذیری‌های فنی امنیتی سیستم‌ها استفاده می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
	الف ۹-۸- مدیریت پیکربندی					
۱	آیا پیکربندی‌ها از جمله تنظیمات امنیتی سخت‌افزارها، نرم‌افزارها، سرویس‌ها و شبکه مشخص، مستند، پیاده‌سازی، نظارت و بازنگری می‌شوند؟					
	الف ۱۰-۸- پاک‌سازی اطلاعات					
۱	آیا اطلاعات ذخیره شده در سیستم‌های اطلاعاتی، دستگاه‌ها یا هر رسانه ذخیره‌ساز، در مواقعی که دیگر به آنها نیازی نیست به نحو مناسبی پاک و امحا می‌شوند؟					
	الف ۱۱-۸- داده‌پوشانی					
۱	آیا پوشاندن داده‌ها با در نظر گرفتن قوانین قابل اجرا و متناسب با خط‌مشی موضوعی خاص شرکت در زمینه کنترل دسترسی و سایر خط‌مشی‌های موضوعی خاص و نیز الزامات کسب‌وکاری انجام می‌شود؟					
۲	آیا از فنون گمنام‌سازی برای عملیات‌های آزمون برنامه‌ها استفاده می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
	الف ۱۲-۸- جلوگیری از نشت داده‌ها					
۱	آیا تدابیری برای جلوگیری از نشت داده‌ها از سیستم‌ها، شبکه‌ها و هر دستگاهی که اطلاعات حساس را پردازش، ذخیره یا انتقال می‌کند در نظر گرفته شده است؟					
	الف ۱۳-۸- پشتیبان‌گیری از اطلاعات					
۱	آیا برای جلوگیری از رخداد از دست رفتن اطلاعات، خط‌مشی پشتیبان‌گیری از اطلاعات تدوین و پیاده‌سازی شده است؟					
۲	آیا نسخ پشتیبان از اطلاعات و برنامه‌ها به صورت منظم تهیه و مورد آزمون بازیابی قرار می‌گیرند؟					
۳	آیا برنامه‌ریزی نوع و زمان‌بندی پشتیبان‌گیری برای همه سامانه‌ها و سیستم‌ها به صورت مناسب انجام شده و مطابق با نیازمندی‌های شرکت و فعالیت‌های کسب‌وکاری آن است؟					
٤	آیا اطلاعات پشتیبان، در زمان بحران قابل دسترس بوده و همچنین در معرض آسیب و صدمه قرار نمی‌گیرند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۵	آیا برای حفاظت از اطلاعات محرمانه پشتیبان، از سازوکارهای رمزنگاری استفاده می‌شود؟					
الف ۱۴-۸- افزونگی امکانات پردازش اطلاعات						
۱	آیا فرایندها و روش‌های اجرایی به منظور تداوم امنیت اطلاعات ایجاد، مستند، پیاده‌سازی و نگهداری می‌شوند؟					
۲	آیا نیازمندی‌های کسب‌وکار برای دسترس‌پذیری سیستم‌های اطلاعاتی شناسایی شده‌اند؟					
۳	آیا در مواردی که تداوم دسترس‌پذیری تضمین نمی‌شود برای تسهیلات پردازش اطلاعات جایگزین‌های کافی در نظر گرفته شده است؟					
٤	آیا مخاطرات نقض صحت و محرمانگی مربوط به جایگزین‌های تسهیلات پردازش اطلاعات (تسهیلات افزونه) در هنگام طراحی سیستم‌های اطلاعاتی در نظر گرفته شده است؟					
الف ۱۵-۸- واقعه‌نگاری						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا به منظور پایش و رویدادنگاری تجهیزات پردازش اطلاعات، رویدادهای فعالیت‌های کاربران و رویدادهای امنیت اطلاعات، یک خط‌مشی وجود دارد؟					
۲	آیا گزارش فعالیت‌های کاربران، اشکالات و رخدادهای امنیت اطلاعات تولید، نگهداری و به صورت منظم بررسی می‌گردد؟					
۳	آیا از لاگ‌ها نسخه پشتیبان تهیه می‌شود؟					
٤	آیا سوابق مربوط به لاگ‌ها در زمان‌های مورد نیاز در دسترس می‌باشد؟					
٥	آیا حفظ محرمانگی اطلاعات گزارش شده رعایت می‌گردد (اطلاعات پایش و رویدادنگاری)؟					
٦	آیا امکانات واقعه‌نگاری و اطلاعات ثبت شده وقایع در برابر دسترسی غیرمجاز یا تغییر و دستکاری محافظت می‌شوند؟					
۷	آیا فعالیت‌های مدیران سیستم ثبت، حفاظت و به صورت منظم بررسی می‌شود؟					
الف ۱۶-۸- فعالیت‌های نظارتی						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا شبکه‌ها، سیستم‌ها و برنامه‌ها از نظر رفتار غیرعادی، تحت نظارت و پایش قرار گرفته و اقدام‌های مناسبی برای ارزیابی رخدادهای امنیت اطلاعات انجام می‌شود؟					
الف ۱۷-۸- همزمان‌سازی ساعت‌ها						
۱	آیا دستورالعملی در خصوص همزمان‌سازی و دقیق بودن زمان سامانه‌ها به صورت مستند وجود دارد؟					
۲	آیا ساعت‌های سیستم‌های پردازش اطلاعات، با یک مرجع زمانی واحد همزمان‌سازی می‌شوند؟					
الف ۱۸-۸- استفاده از برنامه‌های کمکی ویژه						
۱	آیا استفاده از برنامه‌ها و ابزارهایی که ممکن است امکان دور زدن کنترل‌های سامانه و برنامه‌های کاربردی را فراهم کنند، به حد کافی محدود و کنترل شده‌اند؟					
۲	آیا مجوزدهی لازم جهت استفاده از برنامه‌های کمکی ویژه انجام می‌گردد؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۳	آیا سطح اختیارات مربوط به استفاده از برنامه‌های کمکی ویژه تعریف و مستند شده است؟					
٤	آیا از کلیه کاربردها و موارد استفاده این برنامه‌ها گزارش‌گیری می‌شود؟					
	الف ۱۹-۸- نصب نرم‌افزار در سیستم‌های عملیاتی					
۱	آیا روش‌های اجرایی برای کنترل نصب نرم‌افزارها بر روی سیستم‌های عملیاتی تدوین شده است؟					
۲	آیا تنها راهبران آموزش دیده، مجوز به‌روزرسانی نرم‌افزارهای عملیاتی، برنامه‌های کاربردی و کتابخانه‌ها را دارند؟					
۳	آیا آزمایش برنامه‌های کاربردی و سیستم‌عامل‌ها قبل از به کارگیری، بر روی سیستم‌های مجزا آزمون عملکرد و پایداری شده‌اند؟					
٤	آیا کتابخانه‌های منبع برنامه‌ها زمان نصب یک برنامه یا سیستم‌عامل جدید به‌روزرسانی می‌شوند؟					
٥	آیا از سیستم‌های کنترل پیکربندی برای مدیریت نرم‌افزارهای نصب شده استفاده می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
٦	آیا راهبرد برگشت به حالت اولیه قبل از پیاده‌سازی تغییرات نرم‌افزار روی سامانه‌های عملیاتی وجود دارد؟					
۷	آیا نسخه قبلی برنامه کاربردی همراه با پیکربندی آن، آرشیو و نگهداری می‌گردد؟					
۸	آیا لاگ‌برداری در زمان به‌روزرسانی برنامه‌های کاربردی انجام می‌شود؟					
۹	آیا جهت جلوگیری از انجام تغییرات غیرمجاز در برنامه‌های کاربردی و سیستم‌عامل‌ها که می‌تواند باعث ایجاد ضعف‌های امنیتی شود، پایش و کنترلی انجام می‌شود؟					
۱۰	آیا قوانینی برای مدیریت نصب نرم‌افزار توسط کاربران تهیه شده و اعمال می‌شود؟					
۱۱	آیا اصل حداقل سطح دسترسی برای نصب نرم‌افزارها اعمال شده است؟					
۱۲	آیا سطوح دسترسی جهت نصب نرم‌افزارها با توجه به نقش کاربران مرتبط تعریف شده است؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱۳	آیا نوع نرم‌افزارهایی که کاربران می‌توانند و آنهایی که نمی‌توانند نصب کنند، مشخص شده است؟					
الف ۲۰-۸- امنیت شبکه						
۱	آیا شبکه‌ها برای حفاظت از اطلاعات سیستم‌ها و برنامه‌های کاربردی کنترل و مدیریت می‌شوند؟					
۲	آیا روال‌ها و مسئولیت‌هایی برای مدیریت تجهیزات شبکه مشخص شده است؟					
۳	آیا کنترل‌های ویژه‌ای به منظور ایجاد امنیت و حفاظت کاربران در شبکه‌های عمومی و شبکه‌های بی‌سیم پیاده‌سازی شده است؟					
٤	آیا کلیه فعالیت‌های سیستم‌های اطلاعاتی در محیط شبکه پایش و رویدادنگاری می‌شود؟					
٥	آیا سیستم‌ها و تجهیزات در محیط شبکه احراز هویت می‌گردند؟					
٦	آیا اتصالات سیستم‌ها به شبکه محدود شده است؟					
الف ۲۱-۸- امنیت سرویس‌های شبکه						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا سازوکارهای امنیتی، سطوح سرویس‌دهی و الزامات سرویس‌های شبکه شناسایی، پیاده‌سازی و پایش می‌شوند؟					
۲	آیا از توافق‌نامه‌های سطح سرویس (SLA) برای سرویس‌های شبکه که به صورت داخلی ارایه شده یا برون‌سپاری شده‌اند، استفاده می‌شود؟					
الف ۲۲-۸- تفکیک شبکه‌ها						
۱	آیا شبکه‌ها از لحاظ سرویس‌دهی، کاربران و سیستم‌های اطلاعاتی تفکیک (منطقی یا فیزیکی) شده‌اند؟					
الف ۲۳-۸- فیلترینگ وب						
۱	آیا دسترسی به وب‌سایت‌های بیرونی برای کاهش میزان قرار گرفتن در معرض محتوای مخرب مدیریت می‌شود؟					
الف ۲۴-۸- استفاده از رمزنگاری						
۱	آیا خط‌مشی استفاده از کنترل‌های رمزنگاری برای حفاظت از اطلاعات تدوین و پیاده‌سازی شده است؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا خط‌مشی رمزنگاری، رویکردی را که مدیران شرکت (زمانی که کنترل‌های رمزنگاری مدنظر است) باید دنبال کنند، توصیف کرده است؟					
۳	آیا در خط‌مشی رمزنگاری، نقش‌ها و مسئولیت‌ها جهت اجرای خط‌مشی و مدیریت کلید مشخص شده است؟					
٤	آیا کنترل‌های رمزنگاری، کلیه اهداف خط‌مشی امنیت اطلاعات را پوشش می‌دهند؟					
٥	آیا مطابق با ارزیابی مخاطره، سطح نیازمندی حفاظت از داده مشخص شده است (مانند نوع رمزنگاری، طول کلید، کیفیت، قدرت و الگوریتم مورد استفاده)؟					
٦	آیا قبل از انتخاب الگوریتم‌های رمزنگاری، سطح مورد نیاز امنیت برای انتخاب مناسب الگوریتم‌ها مشخص شده است؟					
۷	آیا در تجهیزات سیار و رسانه‌های ذخیره‌سازی قابل حمل، به خصوص در ارتباطات شبکه‌ای، رمزنگاری داده و ترافیک انجام می‌شود؟					
۸	آیا یک خط‌مشی برای نحوه تولید، استفاده، حفاظت و طول عمر کلیدهای رمزنگاری تدوین و استفاده می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۹	آیا یک سیستم مدیریت کلید، در جهت استفاده درست از روش‌های رمزنگاری ایجاد شده است؟					
۱۰	آیا سازوکاری برای حفاظت از تغییر یا جلوگیری از گم شدن کلید یا عدم دسترسی غیرمجاز (منطقی و فیزیکی) به کلیدها وجود دارد (مدیریت کلید)؟					
الف ۲۵-۸- چرخه عمر توسعه امن						
۱	آیا در زمان ایجاد یا توسعه یک نرم‌افزار، فنون و استانداردهای کدنویسی امن رعایت می‌شود؟					
۲	آیا در زمان برون‌سپاری یک نرم‌افزار اطمینان حاصل می‌شود که اشخاص سوم، استانداردهای کدنویسی امن را رعایت می‌کنند؟					
۳	آیا در کلیه فرایندهای چرخه عمر سیستم‌های اطلاعاتی و برنامه‌های کاربردی حساس و راهبردی به استانداردهای بین‌المللی و بهترین تجارب توجه می‌شود؟					
الف ۲۶-۸- الزامات امنیتی برنامه‌های کاربردی						

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱	آیا داده‌ها و اطلاعاتی که توسط سرویس‌های برنامه‌های کاربردی در شبکه‌های عمومی عبور می‌کنند در مقابل حملات کلاهبرداری، تحریف، افشا و غیره محافظت می‌گردند؟					
۲	آیا به منظور حفاظت اطلاعات برای تراکنش‌های برنامه‌های کاربردی در برابر تهدیدات، تمهیداتی اندیشیده شده است (تهدیداتی مثل انتقال ناقص، مسیردهی اشتباهی، تغییر غیرمجاز پیام، افشای غیرمجاز و ...)؟					
الف ۲۷-۸- اصول معماری و مهندسی امن سیستم‌ها						
۱	آیا اصول مهندسی سیستم‌های امن ایجاد، مستند، نگهداری و در پیاده‌سازی هر سیستم اطلاعاتی اعمال می‌گردد؟					
۲	آیا اصول مهندسی سیستم‌های امن در خدمات برون‌سپاری شده مورد توجه و توافق قرار می‌گیرد؟					
الف ۲۸-۸- کدنویسی امن						
۱	آیا در هنگام توسعه نرم‌افزارها اصول کدنویسی امن رعایت می‌شود؟					
۲	آیا تمامی برنامه‌نویسان با اصول کدنویسی امن آشنا هستند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
الف ۲۹-۸- ارزیابی امنیتی در مراحل توسعه و پذیرش						
۱	آیا برنامه‌ها به منظور اطمینان از رعایت اصول کدنویسی امن در طراحی و توسعه آنها مورد آزمون و ارزیابی امنیتی قرار می‌گیرند؟					
۲	آیا در توسعه‌های برون‌سپاری شده این تست‌ها انجام می‌شود؟					
۳	آیا معیارهایی جهت پذیرش سیستم‌های اطلاعاتی، ایجاد شده است (کارایی، اثربخشی و امنیتی)؟					
الف ۳۰-۸- توسعه برون‌سپاری شده						
۱	آیا بر پروژه‌های تولید و توسعه نرم‌افزارهای برون‌سپاری شده نظارت می‌شود؟					
۲	آیا تدابیر امنیتی و الزامات قراردادی در تولید و توسعه سیستم‌های اطلاعاتی برون‌سپاری شده رعایت می‌شود؟					
الف ۳۱-۸- جداسازی محیط‌های توسعه، آزمون و عملیات						
۱	آیا محیط‌های توسعه، آزمون و عملیاتی به منظور کاهش مخاطرات دسترسی غیرمجاز یا تغییرات احتمالی از هم تفکیک شده‌اند؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۲	آیا قوانینی جهت انتقال نرم‌افزار از حالت توسعه به حالت عملیاتی تعریف و مستند شده است؟					
۳	آیا برای توسعه سیستم و یکپارچگی آن یک محیط توسعه امن ایجاد شده است؟					
٤	آیا پشتیبان‌گیری از داده‌ها و کدهای داخل محیط صورت می‌گیرد و این نسخ به صورت امن در خارج از محیط توسعه نگهداری می‌شوند؟					
٥	آیا محیط توسعه از سایر بخش‌ها تفکیک شده است؟					
٦	آیا کنترل دسترسی به محیط توسعه مورد توجه قرار گرفته است؟					
۷	آیا امنیت فیزیکی محیط توسعه مورد توجه قرار گرفته است؟					
	الف ۳۲-۸- مدیریت تغییر					
۱	آیا مسئولیت‌ها و رویه‌های مدیریتی رسمی برای تضمین کنترل تغییرات در تجهیزات، نرم‌افزارها و رویه‌ها تعیین شده است؟					
۲	آیا تغییرات در شرکت، فرایندهای کسب‌وکاری و امکانات پردازش اطلاعات و سیستم کنترل می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۳	آیا زمانی که تغییراتی در سیستم‌ها اعمال می‌گردد گزارش مربوط به تغییرات، ثبت و نگهداری می‌گردد؟					
٤	آیا لیستی از دارایی‌های مهم و حیاتی که تغییرات در آنها بایستی کنترل شود، تهیه شده است؟					
٥	آیا فهرست تغییراتی که نیاز به مجوز دارند، تهیه شده است؟					
٦	آیا تغییرات قبل از اعمال شدن، برنامه‌ریزی و آزمایش می‌شوند؟					
۷	آیا تأثیرات تغییرات (شامل تأثیرات امنیت اطلاعات) ارزیابی می‌شوند؟					
۸	آیا روال یا روشی برای بازگردانی تغییرات ناموفق وجود دارد؟					
۹	آیا مسئولیت‌ها و رویه‌های مدیریتی رسمی برای تضمین کنترل تغییرات در تجهیزات، نرم‌افزارها و رویه‌ها تعیین شده است؟					
۱۰	آیا روش‌های اجرایی رسمی برای کنترل و مدیریت تغییرات ایجاد شده است؟					
۱۱	آیا روش‌های اجرایی کنترل تغییرات، از مسئولیت تغییرات اعمال شده پشتیبانی می‌کند (در روش اجرایی ذکر شده که چه کسی مسئول تغییر است)؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۱۲	آیا از روش‌های اجرایی کنترل تغییرات برای پیاده‌سازی تغییرات استفاده می‌شود؟					
۱۳	آیا قبل از به‌روزرسانی اصلی یا تغییر نسخه سیستم‌عامل، سیستم‌های اطلاعاتی و نرم‌افزارهای کاربردی، آزمون عملکرد و بازنگری انجام می‌گیرد؟					
۱٤	آیا زمانی‌که تغییراتی در بسترهای عملیاتی به وجود می‌آید، برنامه‌های کاربردی حیاتی شرکت مورد ارزیابی و آزمون عملکرد قرار می‌گیرند؟					
۱۵	آیا تغییرات بر روی بسته‌های نرم‌افزاری محدود و کنترل می‌شود؟					
الف ۳۳-۸- اطلاعات آزمون						
۱	آیا داده‌های عملیاتی زمانی که برای آزمون سیستم مورد استفاده قرار می‌گیرند با دقت انتخاب، محافظت و کنترل می‌شوند؟					
۲	آیا از یک روش اجرایی کنترل دسترسی یکسان برای اعمال محدودیت دسترسی به سیستم‌های عملیاتی و همچنین سیستم‌هایی که برای انجام آزمون سیستم‌های کاربردی در نظر گرفته شده است، استفاده می‌شود؟					

ردیف	شرح سؤال‌های ممیزی	بند/ کنترل استاندارد	یافته‌های ممیز و سوابق مربوطه	نتیجه		
				انطباق	عدم انطباق	نیاز به بهبود
۳	آیا سیستم رویدادنگاری و حسابرسی رویدادها زمانی که داده‌های عملیاتی (واقعی) برای انجام فرایند آزمون کپی می‌شوند، فعال می‌شود؟					
الف ۳۴-۸- حفاظت از سیستم‌های عملیاتی						
۱	آیا الزامات و فعالیت‌های ممیزی مرتبط با بررسی‌های سیستم‌های عملیاتی، طرح‌ریزی شده و مورد توافق قرار گرفته‌اند؟					
۲	آیا فعالیت‌های ممیزی سیستم‌های عملیاتی به نحوی طراحی می‌شوند که کمترین اختلال را در فرایندهای کسب‌وکار ایجاد نمایند (مثلاً اجرای فعالیت‌های ممیزی فنی در خارج از ساعات کار)؟					
۳	آیا دامنه فنی آزمون ممیزی مشخص و توافق شده است؟					
٤	آیا آزمون‌های ممیزی، محدود به دسترسی فقط خواندنی به نرم‌افزار می‌باشد؟					