QUAY AUDIT LIMITED

(ISMS)

ایمن سازی فضای تبادل اطلاعات منطبق بر استاندارد ISO27001

Information Security Management Systems

مقدمه

در محیط اقتصادی ، اجتماعی و سیاسی امروز، پرداختن به موضوع امنیت به ضروری ترین امر برای سازمان ها (اگرچه نه برای همه) بدل گشته است . مشتریان به همان اندازه که برای موضوعاتی از قبیل محیط خصوصی خود و یا پیگیری سرقت های اتفاق افتاده اهمیت قائلند ، بطور قابل توجهی خواهان ارتقائ سطح امنیت می باشند. شرکای تجاری، تامین کنندگان و فروشندگان، پیوسته امنیت را از یکدیگر مطالبه کرده و مخصوصا" هنگامی که شبکه ای مشترک امکان دسترسی به اطلاعات را فراهم کنند

جاسوسی در شبکه ها برای کسب هوشمندی رقابتی به منظور اخاذی از سازم انها رایج تر شده است . بدین منظور در بسیاری از کشورها و سازمان های ناظر ، مقررات ملی و بین المللی جهت حفظ امنیت برای سازمان ها و رهبران آنها طراحی شده و بکار می روند.

در نظر بگیرید برای سازمان ها چقدر هزینه خواهد داشت اگر:

- داده های مشتری افشا شده و آن را به ییترهای خبری بدل کرده باشد.
- نام تجاری (BRAND) و شهرت آن در نتیجه عدم وجود وفاداری و محرمانگی در مشتری و سرمایه گذاران، به وسیله رخنه های امنیتی تحت تاثیرهای منفی قرار گرفته باشد
- دارایی های معنوی حساس (مانند اسرار تجاری یا اطلاعات مرتبط با محصول جدید) توسط رقیب ربوده شده ویا در سطحی عام انتشار یافته باشد.
- سازمان به صورتی ناسازگار با مقررات حفاظت کننده از اطلاعات و امنیت اطلاعات (ملی یا محلی) ایجاد شده باشد.
- شبکه کامپیوتری سازمان بدلیل وجود رخنه های امنیتی متوقف یا تخریب گردد
- ویا اینکه شما قادر به شناخت رخنه های امنیتی نباشید.

آدرس: تهران ، میرداماد ، میدان مادر، برج بیژن ، طبقه ۴ ، واحد۱
Www.QAL-IRAN.IR
Email : info@qal-iran.ir
*Tel/Fax : **021-22228386 - 22923396***

در دنیای امروز استفاده از شبکه های اطلاعاتی در بخشهای دولتی و خصوصی به شکل چشمگیری در حال رشد است که بدنبال آن خطرات امنیت و حفاظت اطلاعات هم به صورت داخلی و هم به صورت ارتباطات شبکه ای (عمومی) افزایش پیدا نموده است.

ISMS رویکردی پیشگیرانه در ریشه کنی و جلو گیری از ضعف های امنیتی و خطرات کنترل اطلاعات دارد که سازمان ها را قادر می سازد تا بهبود دوره ای در امنیت سیستم های اطلاعاتی را به وجود آورند و به مانند دیگر سیستم های مدیریتی در بهبود عملکرد آن اقدام نمایند.

این استاندارد بر سه اصل زیر به عنوان زیر ساخت امنیتی اطلاعاتی بنا نهاده شده است:

- محرمانگی(**Confidentiality**)
- یکپارچگی و صحت(**Integvity**)
- در دسترس بودن(**Availability**)

مزایای داشتن گواهینامه ISO27001 چیست؟

فرصت هایی که از وجود یک برنامه اثر بخش مدیریت ایمنی اطلاعات برای سازمان ایجاد می شود می تواند شامل موارد زیر باشد:

۱. قابلیت ارائه انواع محصولات و خدمات جدید و دستیابی به کانال های تازه برای نفوذ به بازارهای جدید.
۲. برقراری ارتباط با مشتریان به صورتی مطمئن، مقرون به صرفه و به موقع
۳. ایجاد مبادلات با یکپارچگی بیشتر و محیط خصوصی تر که موجب حصول اطمینان در کسب و کار ، رضایت مشتری و ایجاد فضای محرمانه برای او خواهد شد و وفاداری پایدار مشتری را در پی خواهد داشت.
۴. ارتقا سطح تعهد تامین کنندگان در پاسخ به مشریان جدید، بر اساس تعامل به موقع و مطمئن با زنجیره تامین سازمان

۵. ایجاد سطح دسترسی ایمن تر برای کارکنان داخلی و خارجی سازمان توسط نرم افزار های کاربردی.

۶. ایجاد و برقرار نگه داشتن سطوح محرمانگی در ساختار امنیت سازمان ، بطوریکه احتمال مراجعه مشتریان را برای دریافت کالا یا خدمت افزایش می دهد. به عبارت دیگر همان طور که قوانین و مقررات در ایجاد فضای اطمینان برای کسب و کار دارای کاربردی موثر است ، وجود جلوه ای از یک سازمان مبتنی بر اخلاق ، با فرهنگی دال بر انجام کارهای درست و انجام درست کارها بصورت توامان به همراه امنیت ، دارای ارزشهای مشهود در بازارهای بین المللی است.

۷. نشانگر اعتبار و قابل اطمینان بودن یک سازمان است.

۸. این اعتبار می تواند منجر به کنترل هزینه ها شود.حتی رخنه ای جزئی در اطلاعات می تواند زیان های عمده به همراه داشته باشد.

۹. در مقابل سایر رقبا برای شما وجه تمایزی ایجاد می کند.

۱۰. باعث بالا رفتن اطمینان شرکای تجاری و مشتریان می شود.

ISO27001 :2005

سیستم مدیریت امنیت اطلاعات و داده ها

استاندارد **BS 7799-2:2002** به طور رسمی تغییر یافت و به استانداردهای **ISO/IEC 27001:2005** و می باشد و این استاندارد برای همه بخش ها اعم از صنعتی و تجاری از جمله بانک ها موثر خواهد بود.

امنیت اطلاعات می تواند برای محافظت از موارد زیر باشد:

- ✓ محرمانگی: حصول اطمینان از دسترسی کنترل شده به اطلاعات
- ✓ یکپارچگی: محافظت از صحت و کامل بودن اطلاعات و روش های پردازش آنها
- ✓ قابلیت دسترسی: حصول اطمینان از در دسترس بودن اطلاعات برای کاربران مجاز در صورت نیاز

BS7799 در برگیرنده اهداف کنترلی و کنترل های متعددی می باشد که عبارتند از:

- ✓ خط مشی امنیتی
- ✓ امنیت سازمانی
- ✓ طبقه بندی و کنترل اموال
- ✓ امنیت فردی
- ✓ امنیت فیزیکی و محیطی
- ✓ مدیریت ارتباطات و عملیات
- ✓ کنترل دسترسی
- ✓ نگهداری و توسعه سیستم
- ✓ مدیریت تداوم تجارت
- ✓ انطباق

آدرس: تهران ، میرداماد ، میدان مادر، برج بیژن ، طبقه ۴ ، واحد۱
Www.QAL-IRAN.IR
Email : info@qal-iran.ir
*Tel/Fax : **021-22228386 - 22923396***

منافع حاصل از دریافت گواهینامه ISO27001

دریافت گواهینامه از سازمان های ثبت و صدور گواهی نامه نشان دهنده این است که سازمان سیستم مدیریت امنیت اطلاعات خود را شناسایی، پیاده سازی و کنترل نموده است . همچنین دستیابی به منافع زیر میسر می گردد:

- ✓ دستیابی به یک سیستم امنیت اطلاعات ساده و صرفه جویی در هزینه
- ✓ رعایت قوانین و مقررات مرتبط
- ✓ حصول اعتبار و اطمینان
- ✓ وجود تعهد در سراسر سازمان نسبت به امنیت اطلاعات
- ✓ کمک به انطباق با الزامات مختلف موثر بر نگهداری و مدیریت اطلاعات
- ✓ ایجاد مزیت نسبی در بازار
- ✓ ارتقا سطح اطمینان مشتریان و شرکای تجاری

استقرار ISO27001

مراحل استقرا استاندارد عبارتند از :

۱. سازمان باید اموال (مادی و معنوی) سازمان را در چارچوب دامنه کاربرد **ISMS** شناسایی و ارزشگذاری کند.که نتیجه آن کنترل موجودی اموال خواهد بود.

۲. ارزیابی ریسک(**RA**) را برای دامنه کاربرد با در نظر گرفتن اموال شناسایی شده ، مخاطرات و صدمات ناشی از آنها انجام دهید.

این ارزیابی بر اساس سه پارامتر ارزش اموال ،احتمال خطر شدت صدمات می باشد .نتیجه این ارزیابی مستندات ارزیابی ریسک خواهد بود.

۳. سازمان پس از تصمیم گیری جهت پیاده سازی **ISO27001** ، سازمان باید مسولیت های لازم را مشخص کند و مدیریت ارشد تعهد لازم را برای اجرای پروژه و ادامه آن ایجاد نماید

آدرس: تهران ، میرداماد ، میدان مادر، برج بیژن ، طبقه ۴ ، واحد۱
Www.QAL-IRAN.IR
Email : info@qal-iran.ir
*Tel/Fax : **021-22228386 - 22923396***

۴. در صورتی که خط مشی امنیت اطلاعات در حال حاضر در دسترس نباشد، سازمان باید خط مشی امنیت اطلاعات را تهیه نماید.

۵. در صورتی که محتوای خط مشی امنیت اطلاعات مورد تصویب قرار گیرد باید به کلیه پرسنل آموزش داده شود که لا زمه ی آن تدوین خط مشی امنیت اطلاعات خواهد بود

۶. سازمان باید تصمیم بگیرد که در کدام بخش و قسمت ها پیاده سازی استاندارد **ISO27001** انجام شود،به عبارت دیگر باید دامنه کاربرد **ISMS** را تعیین کنید.

۷. باید رویکردی ریسک پذیر را مشخص و انتخاب کندو درجه ای از ریسک را بپذیرد.

۸. سطح ریسک اموال سازمان و سطح ریسکی که سازمان آماده برای پذیرش آن است ، مشخص کننده چگونگی مدیریت ریسک های شناسایی شده خواهد بود.

۹. **ISO27001** در کنترل مرتبط برای مدیریت ریسک ها تا سطوح قابل قبولی یاری رسان خواهد بود و گسترش آن توسط استانداردهای دیگر پشتیبانی می شود.

۱۰. مدیریت ریسک ها، اقدامات ، پاسخگویی ها و مسولیت ها برای مدیریت آنها باید مدون شود.

۱۱. کنترل های مرتبط باید با استفاده از **ISO27001** یا سایر منابع برای پیاد سازی انتخاب شوند. خط مشی امنیتی و روش های اجرایی پشتیبانی کننده و ساختار امنیتی نیز باید در این کنترل ها لحاظ گردند.

۱۲.کنترل های انتخاب شده باید مدون شوند و قابلیت ردیابی به ریسک های مرتبط با خود را دارا باشند. نتیجه این امر ، بیانیه قابلیت کاربرد **SOA** می باشد.

۱۳.در این مرحله باید کنترل ها (انتخاب و مدون شده) به کار بسته شوند.

۱۴.تجزیه و تحلیل فاصله بین وضعیت فعلی و وضعیت ایده آل را انجام دهید تا کنترل های که به طور کامل انجام نشده اند،شناسایی شوند .کاربران باید آموزش ببینند .در صورتی که تجزیه و تحلیل فاصله بین وضعیت فعلی و وضعیت ایده آل توسط سر ممیزان ، منابع داخلی یا مشاوران خارجی ثبت شده **ISO27001** انجام شود برای سازمان مفید خواهد بود.

۱۵.اقدامات اصلاحی براساس تجزیه و تحلیل فاصله بین وضعیت فعلی و وضعیت ایده آل انجام شود

۱۶.از سازمان های گواهی دهنده که گواهی **ISO27001** را صادر می کنند، برای ممیزی و ثبت و صدور گواهی نامه دعوت گردد.

۱۷.سازمان های صدور گواهی نامه ،ممیزی رسمی را انجام خواهند داد . در صورتی که همه کنترل ها به کار بسته شده باشند سازمان موفق به دریافت گواهی نامه می شود.

چرا QAL را به عنوان شرکت ثبت و صدور گواهی نامه انتخاب کنیم؟

QAL دارای اعتبار صدور گواهی نامه **ISO27001** از طرف **ASCB(E)** می باشد. تیم ممیزی **QAL** این رویکرد را درک کرده اند .این ممیزان دارای تجارب غنی در صنایعی که ممیزی می کنند، هستند. این امر ممیزی کاربردی و سودمندی را در محیطی با درک متقابل در پی دارد.**QAL** قویا بر این باور است که ممیزی باید برای سازمان ها ارزش افزوده و منافع ایجاد نماید

چگونه QAL می تواند به شما کمک کند؟

۱. **QAL** ، چارچوب تایید شده و ر وش های کاملی را برای ممیزی **ISO27001** به خدمت گرفته است، که شامل معیار های ممیزی با توجه به دامنه کاربرد سازمان های مرتبط می باشد و به مشتریان اطمینان خواهد داد خدماتی با کیفیت بالا به آن ها ارائه می کند
۲. **QAL** سر ممیزان ثبت شده **ISO27001** را به کار میگیرد و مشاوران ثبت شده ی این استاندارد را بر ای کمک به پیاده سازی استاندارد **ISO27001** به سازمان های مشتری معرفی می کند.
۳. ما می توانیم دوره آموزشی متنوعی را برای بالا بردن آگاهی و کسب اطمینیان از انطباق کنترل های بکار بسته شده فراهم کنیم.

آدرس: تهران ، میرداماد ، میدان مادر، برج بیژن ، طبقه ۴ ، واحد۱
Www.QAL-IRAN.IR
Email : info@qal-iran.ir
*Tel/Fax : **021-22228386 - 22923396***

شرح مراحل دریافت گواهینامه ISO27001:2005

- **مرحله اول:**

پرسشنامه مربوطه را از دفتر شرکت **QAL** دریافت و تکمیل نمایید. این پرسشنامه ابزار مهمی برای شرکت **QAL** می باشد. زیرا به کمک آن اطلاعات کافی در مورد محصولات و یا خدمات سازمان و فرایند ها و فعالیت های مرتبط در اختیار شرکت **QAL** قرار خواهد گرفت. با استفاده از پرسشنامه شرکت **QAL** قادر خواهد بود پس از بررسی کارشناسی پیشنهاد قیمت را ارائه نموده و تیم ممیزی مناسب را تخصیص می دهد.

- **مرحله دوم:**

در این مرحله پس از توافق در خصوص شرایط همکاری ، پیش نویس قرارداد تهیه و جهت امضا به سازمان ارائه می گردد ، سپس قرارداد نهایی و امضا ش ده و همراه با پیش پرداخت مورد توافق با شرکت **QAL** ارسال خواهد گردید ، همچنین ارسال یک نسخه از مستندات سیستم **ISMS** جهت بررسی ضروری میباشد.

- **مرحله سوم:**

در صورت نیاز ، ممیز از سازمان بازدیدی به عمل می آورد تا از نظر گرفتن کلیه جنبه های اساسی و انتخاب تیم ممیزی مناسب اطمینان حاصل کند.

بازدید مذکور در بر گیرنده ی مجموعه ای از پرسش و پاسخ برای ممیز و سازمان می باشد که نشان دهنده درک متقابل خواهد بود.

آدرس: تهران ، میرداماد ، میدان مادر، برج بیژن ، طبقه ۴ ، واحد۱
Www.QAL-IRAN.IR
Email : *info@qal-iran.ir*
Tel/Fax : ***021-22228386 - 22923396***

- **مرحله چهارم:**

ممیزی اصلی انجام می شود . یک گزارش رسمی تهیه می شود. توصیه برای صدور گواهینامه ویا سایر موارد مقتضی در جلسه اختتامیه ممیزی نهای به سازمان اعلام می شود.

- **مرحله پنجم:**

پس از انجام اقدامات اصلاحی مشخص شده،گواهینامه رسمی صادر و سازمان در برنامه ممیزی مراقبتی قرار می گیرد.

- **مرحله ششم:**

ممیزی مراقبی سالانه انجام می شوند .ممیزی مراقبتی پس از کسب توافقهای لازم در مورد هزینه ها و برنامه ممیزی انجام می شود.

تعدادنفر-روز ممیزی بر اساس پیچیدگی سایت ها و سیستم ها **ISMS** تعیین می شود.

با آرزوی بهترین ها

آدرس: تهران ، میرداماد ، میدان مادر، برج بیژن ، طبقه ۴ ، واحد۱
Www.QAL-IRAN.IR
Email : info@qal-iran.ir
*Tel/Fax : **021-22228386 - 22923396***