
بسم الله الرحمن الرحیم

چک لیست ممیزی سیستم مدیریت

امنیت اطلاعات (ISMS)

مبتنی بر استاندارد ISO/IEC 27001:2013

راهنمای عملی و کاربردی ممیزی سیستم مدیریت امنیت اطلاعات

تألیف:

محمد مهدی واعظی نژاد

مدیر تولید و ناظر چاپ: حسین رعدشندی صفحه‌آرایی: همتا بیداریان
طراحی جلد: فاطمه نژادعباسی

چک‌لیست ممیزی سیستم مدیریت امنیت اطلاعات (ISMS) مبتنی بر استاندارد ISO/IEC 27001:2013 راهنمای عملی و کاربردی ممیزی سیستم مدیریت امنیت اطلاعات

مؤلف: محمد مهدی واعظی‌نژاد
ناشر: انتشارات آتی‌نگر
چاپ اول، ۱۳۹۵
شمارگان: ۱۰۰۰ نسخه
قیمت: ۱۸۰،۰۰۰ ریال
شابک: ۱-۲۰-۷۶۳۱-۶۰۰-۹۷۸

ISBN: 978-600-7631-20-1

نشانی دفتر فروش: خیابان جمالزاده جنوبی، روبه‌روی کوچه رشتچی، پلاک ۱۴۴، واحد ۲
تلفن: ۸-۶۶۵۶۵۳۳۶- ۰۹۳۶۰۸۹۵۸۴۸ نمابر: ۶۶۵۶۵۳۳۷
www.ati-negar.com*info@ati-negar.com

واعظی‌نژاد، محمد مهدی، ۱۳۶۱-
چک‌لیست ممیزی سیستم مدیریت امنیت اطلاعات (ISMS)- مبتنی بر استاندارد ISO/IEC 27001:2013 (راهنمای عملی و کاربردی ممیزی سیستم مدیریت امنیت اطلاعات)/
مؤلف: محمد مهدی واعظی‌نژاد. - تهران: آتی‌نگر، ۱۳۹۵
۲۶۴ص.: مصور، جدول؛ ۵/۹×۱۹ س‌م.
ISBN: 978-600-7631-20-1
فیپا.
موضوع: راهنمای علمی و کاربردی ممیزی سیستم مدیریت امنیت اطلاعات -- تکنولوژی اطلاعات -- تدابیر ایمنی -- استانداردها Information technology -- Security measures -- Standards
رده‌بندی کنگره ۱۳۹۵ ۸چ۲و/T۵۸/۵
رده‌بندی دیویی ۳۰۳/۴۸۳۳
شماره کتابشناسی ملی ۴۲۸۲۲۲۵

به نام خداوندی که به انسان برخاسته از خاک، خرد بخشید، از روح خود در او دمید و او را خلیفه خویش بر روی زمین قرار داد و پیامبرانش را با دلایل آشکار فرو فرستاد تا انسان‌ها را به سعادت و هدایت، بر پایه تفکر و تعقل رهنمون گردانند.

تقدیم به ساحت مقدس

حضرت قاسم بن الحسن علیه السلام

نام سازمان / شرکت ممیزی شونده:

.....

آدرس: .....

تلفن: ..... **نمابر:** .....

دامنه ممیزی: .....

تاریخ آخرین بازنگری بیانیه کاربست‌پذیری: .....

تاریخ انجام ممیزی: .....

سرممیز: .....

ممیزان: .....

کارشناسان فنی: .....

فهرست مطالب

مقدمه ۱۱

دستورالعمل استفاده از این چک‌لیست ۱۵

بخش صفر (برنامه ممیزی: فرایند قبل از شروع ممیزی)

برنامه ممیزی ۱۸

بخش اول (شروع ممیزی: ممیزی مرحله اول)

مستندات الزامی ۲۲

الزامات کلیدی ۲۴

بخش دوم (بازدید محلی: ممیزی مرحله دوم)

کنترل‌های کلیدی پیوست الف استاندارد ۶۲

کنترل‌های اضافی ۲۶۳

منابع ۲۶۴

مقدمه

امروزه با گسترش روز افزون فناوری اطلاعات در سازمان‌ها و بهره‌گیری از ابعاد گسترده آن در امر خدمات‌رسانی و حتی تولید محصولات، عنصر ارزشمندی به نام «اطلاعات» در سازمان‌ها پدید آمده است که مهمترین دارایی سازمانی هم به شمار می‌رود. استفاده از فناوری اطلاعات و بهره‌مندی از سیستم‌های ذخیره و پردازش اطلاعات، به عنوان ابزاری قدرتمند، باعث متمایز شدن سازمان‌ها از یکدیگر شده است و آن‌هایی که از این فرصت بی‌بدیل فناورانه توانسته‌اند در زمان مناسب خویش، به بهترین نحو ممکن بهره‌برداری کنند، گوی سبقت را از سایر رقبا ربوده و موجب سودآوری کسب و کار خود شده‌اند. بنابراین در دنیای رقابتی امروز، اطلاعات به عنوان گوهری حیاتی که بقای سازمان‌ها به شدت به آن وابسته است نیازمند راهکارهای حفاظتی مناسب جهت جلوگیری از تخریب، دستکاری، تغییر، حذف یا افشا است.

استاندارد ISO/IEC 27001:2013 زمینه مناسبی را برای بهره‌گیری از این رویکرد و حفاظت از اطلاعات سازمانی فراهم کرده است و به تمام سازمان‌ها با هر حجم، اندازه، ساختار، فرهنگ سازمانی و سطح بلوغی کمک می‌کند با پیاده‌سازی و استقرار سیستم مدیریت امنیت اطلاعات[1]، فرایندهای امنیتی خود را متناسب با الزامات خویش، به نحو مطلوبی بهبود بخشند.

پس از پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان، لازم است انطباق آن با کنترل‌ها و الزامات این استاندارد بین‌المللی بررسی شود تا از کارایی هر چه بهتر و بهبود مستمر این سیستم اطمینان حاصل شود. کتاب حاضر که چک‌لیست ممیزی سیستم مدیریت امنیت اطلاعات است با هدف آشنایی ممیزان با فرایندهای ممیزی این سیستم مدیریتی تدوین شده است و با استانداردهای ISO 19011:2011[2] و ISO/IEC 17021:2011[3] انطباق کامل دارد.

از این کتاب می‌توان برای انجام ممیزی‌های داخلی و شخص سوم (صدور گواهی) سیستم مدیریت امنیت اطلاعات یا هرگونه ارزیابی‌های درون سازمانی استفاده کرد. ممیزان داخلی با استفاده از این کتاب می‌توانند از طریق فرایند خودارزیابی، وضعیت سیستم مدیریت امنیت اطلاعات در حال پیاده‌سازی در سازمان مطبوع خویش را قبل از انجام ممیزی‌های شخص سوم، مورد

1- Information Security Management System (ISMS)
2- Guidelines for auditing management systems
3- Conformity assessment - Requirements for bodies providing audit and certification of management systems

ارزیابی قرار دهند.

در پایان، از تمام ممیزان سیستم مدیریت امنیت اطلاعات، کارشناسان امنیت و خوانندگان گرامی درخواست می‌کنم نظرها و پیشنهادهای اصلاحی یا تکمیلی خود را از طریق ایمیل Info@mvaezi.ir با اینجانب در میان گذارند تا در اصلاح‌های بعدی این کتاب مد نظر قرار گیرد.

خدایا چنان کن سرانجام کار، تو خشنود باشی و ما رستگار

محمد مهدی واعظی نژاد
بهار ۱۳۹۵