

برنامہ خدا

اندازہ گیری اثربخشی مدیریت امنیت اطلاعات

(استاندارد ISO/IEC27004: فناوری اطلاعات، فنون امنیتی،
سیستم های مدیریت امنیت اطلاعات، اندازہ گیری)

ترجمہ و تالیف:

معزالدین حجت الاسلامی

ویراستار فنی:

علیرضا براتی فرد

(معاون مرکز توسعه دولت الکترونیک و فناوری اطلاعات وزارت کشور)

اندازه‌گیری اثربخشی مدیریت امنیت اطلاعات

ترجمه و تألیف: معزالدين حجت‌الاسلامی

ویراستار فنی: سیرضا براتی فرد

ناشر: انتشارات وینا

ناشر همکار: انتشارات آتی‌نند

چاپ اول، ۱۳۹۶

شمارگان: ۵۰۰ نسخه

قیمت: ۹۰.۰۰۰ ریال

شابک: ۹۷۸-۹۶۴-۸۸۱۶-۴۴-۰

ISBN: 978-964-8816-44-0

حق چاپ برای انتشارات وینا محفوظ است.

نشانی دفتر فروش: خیابان جمالزاده جنوبی، ردیف ۱۴۴ کوچه رشتچی، پلاک ۱۴۴ واحد ۱

شماره: ۶۶۵۶۵۳۳

تلفن: ۸-۶۶۵۶۵۳۳۶

www.ati-negar.com * info@ati-negar.com



اندازه‌گیری اثربخشی مدیریت امنیت اطلاعات: استاندارد ISO/IEC 27004 فناوری اطلاعات، فناوری، سیستم‌های مدیریت امنیت اطلاعات، اندازه‌گیری / ترجمه و تألیف [صحیح: ترجمه] معزالدين حجت‌الاسلامی؛ ویراستار فنی: سیرضا براتی فرد
تهران: وینا، آتی‌نگر ۱۳۹۶
۹۲ ص.: مصور، جدول، نمودار.

ISBN: 978-964-8816-44-0

فیبا.

یادداشت: عنوان اصلی: International standard. ISO/IEC 27004. Information technology - Security techniques - Information security management- Measurement.

موضوع: تکنولوژی اطلاعات - تدابیر ایمنی - استانداردها

موضوع: حفاظت داده‌ها - استانداردها - کامپیوترها - ایمنی اطلاعات - استانداردها

موضوع: شبکه‌های کامپیوتری - تدابیر ایمنی - استانداردها

شناسه افزوده: حجت‌الاسلامی، معزالدين، ۱۳۶۴ - مترجم

شناسه افزوده، براتی فرد، علیرضا، ۱۳۵۵ - ویراستار

رده‌بندی کنگره

رده‌بندی دیوبی

شماره کتابشناسی ملی

۱۳۹۶ الف/۵/۵۸/۵

۳۰۳/۴۸۳۳

۴۶۹۵۶۲۱

فهرست مطالب

۵	فهرست منابع
۷	فهرست منابع
۹	فهرست منابع
۹	۱-۱ مقادیر
۱۱	۱-۲ جای ملی مدیریت
۱۱	۱-۲-۱ عدد اختصاص منابع بیش از حد به فرایند ISMS
۱۲	۱-۲-۲ بصریه‌های استاندارد ۲۷۰۰۴ برای تحقق نیازمندی‌های اندازه‌گیری
۱۲	۱-۲-۳ اندازه‌گیری استاندارد
۱۳	۱-۳ قلمرو استاندارد
۱۳	۱-۴ مراجع اصلی
۱۳	۱-۵ نمای کلی اندازه‌گیری امنیت اطلاعات
۱۳	۱-۵-۱ اهداف اندازه‌گیری امنیت اطلاعات
۱۵	۱-۶ برنامه اندازه‌گیری امنیت اطلاعات برنامه
۱۵	۱-۶-۱ اندازه‌گیری امنیت اطلاعات
۱۶	۱-۶-۲ عوامل موفقیت
۱۶	۱-۷ مدل اندازه‌گیری امنیت اطلاعات (ISMM)
۱۸	۱-۷-۱ معیارهای پایه (B) و روش اندازه‌گیری (M)
۲۰	۱-۷-۲ معیار مشتق و تابع اندازه‌گیری
۲۱	۱-۷-۳ شاخص‌ها و مدل تحلیلی
۲۳	۱-۷-۴ نتایج اندازه‌گیری و ضوابط تصمیم‌گیری
۲۴	۱-۸ مسئولیت‌های مدیریت
۲۴	۱-۸-۱ نمای کلی
۲۵	۱-۸-۲ مدیریت منابع
۲۵	۱-۸-۳ آموزش و آگاه‌سازی اندازه‌گیری
۲۵	۱-۹ توسعه معیارها و اندازه‌گیری
۲۵	۱-۹-۱ نمای کلی
۲۶	۱-۹-۲ تعریف قلمرو اندازه‌گیری

۲۷	۱-۹-۳ شناسایی نیازهای اطلاعاتی
۲۷	۱-۹-۴ انتخاب شیء و صفت
۲۹	۱-۹-۵ توسعه ساختار اندازه‌گیری
۳۲	۱-۹-۶ ساختار اندازه‌گیری

۳۳	فصل ششم: اندازه‌گیری برای ساختار اندازه‌گیری امنیت اطلاعات
----	--

۳۳	۲-۱ آگویی برای ساختار اندازه‌گیری امنیت اطلاعات
----	---

۳۹	فصل هفتم: اندازه‌گیری برای ساختارهای اندازه‌گیری
----	--

۳۹	۳-۱ آموزش ISM
----	---------------

۳۹	۳-۱-۱ آموزش درباره ISMS
----	-------------------------

۴۲	۳-۱-۲ آموزش امنیت
----	-------------------

۴۵	۳-۱-۳ تطابق آگاهی امنیت اطلاعات
----	---------------------------------

۵۰	۳-۲ سیاست‌های کلمه عبور
----	-------------------------

۵۰	۳-۲-۱ کیفیت کلمه عبور - دسته
----	------------------------------

۵۴	۳-۲-۲ کیفیت کلمه عبور - به‌طور خاص
----	------------------------------------

۵۸	۳-۳ فرایند بازبینی ISMS
----	-------------------------

۶۱	۳-۴ بهبود مستمر ISMS
----	----------------------

۶۱	۳-۴-۱ اثربخشی مدیریت رخداد امنیت اطلاعات
----	--

۶۳	۳-۴-۲ پیاده‌سازی اقدامات اصلاحی
----	---------------------------------

۶۹	۳-۵ التزام مدیریت
----	-------------------

۷۵	۳-۶ محافظت در برابر کدهای بدخواه (برنامه‌های مخرب)
----	--

۷۷	۳-۷ کنترل‌های ورودی فیزیکی
----	----------------------------

۸۰	۳-۸ بررسی فایل‌های لاگ (Log Files)
----	------------------------------------

۸۳	۳-۹ مدیریت نگهداری و تعمیر
----	----------------------------

۸۶	۳-۱۰ امنیت در توافقیات‌های شخص ثالث
----	-------------------------------------

پیشگفتار مترجم

زندگی بشر از عصر تولید انبوه به عصر ارتباطات و اطلاعات ارتقا یافته و حرکت تکاملی کشورهای جهان به سوی جوامع اطلاعاتی و دانش‌بنیان، کلیه فرایندها و فعالیت‌های اقتصادی، فرهنگی، صنعتی و روابط اجتماعی را تحت تأثیر قرار داده است.

چارچوب ساختاری تشکیل‌دهنده این عصر را تولید، پردازش، انتقال و مدیریت اطلاعات و ارتباطات به‌منظور ایجاد پایگاه‌های دانش و معرفت فردی، گروهی، سازمانی و کشور تشکیل می‌دهد و لذا فناوری اطلاعات را که شامل فناوری‌های به کار گرفته شده در فرایند مذکور می‌باشد برای جوامع بشری به‌عنوان عامل حیاتی و تعیین‌کننده مطرح ساخته است.

در دنیای امروز، اطلاعات نه تنها به‌عنوان یکی از منابع و دارایی‌های اصلی سازمان‌ها شناخته می‌شود بلکه در حکم وسیله و ابزاری برای مدیریت اثربخش بر سایر منابع و دارایی‌های سازمان نیز محسوب می‌شود و لذا از اهمیت و ارزش ویژه‌ای برخوردار گشته است. اما این ارزش تنها در صورتی محقق و دست‌یافتنی خواهد بود که اطلاعات بتوانند با امنیت قابل قبول در اختیار افراد قرار گیرد. لازمه تأمین امنیت اطلاعات، وجود روش و راهکاری مناسب برای سنجش و بهبود مستمر آن است.

امروزه اندازه‌گیری امنیت اطلاعات جهت بهبود سیستماتیک اثرگذاری سیستم مدیریت امنیت اطلاعات در سازمان‌های مختلف به‌خصوص در بخش فناوری اطلاعات سازمان‌ها از اهمیت ویژه‌ای برخوردار است. در این کتاب به ترجمه و بررسی اندازه‌گیری میزان اثربخشی مدیریت

امنیت اطلاعات با توجه به استاندارد بین‌المللی ISO/IEC 27004 از سری استانداردهای امنیت اطلاعات ISO/IEC 27000 پرداخته شده است. در این نوشتار سعی شده که به‌طور کامل این استاندارد مورد بررسی قرار گرفته شود تا راهنمایی برای ممیزان و مدیران امنیتی ISMS، برای اندازه‌گیری و سنجش امنیت اطلاعات سازمان‌ها باشد.

هدف از این مستند کمک به سازمان‌ها (به‌خصوص سازمان‌های دولتی و دفاعی) برای اندازه‌گیری، گزارش و بهبود نظام‌مند اثرگذاری سیستم مدیریت امنیت اطلاعات (ISMS) است. اهم اهداف و نتایج این نوشتار به بخش‌های اصلی زیر تقسیم می‌شود:

✓ بررسی کلی سنجش یا اندازه‌گیری امنیت اطلاعات

✓ مسئولیت‌های مدیران سازمان

✓ ایجاد و توسعه اندازه‌گیری معیارهای آن

✓ عملیات اندازه‌گیری

✓ گزارش‌گیری از نتایج اندازه‌گیری و تحلیل داده‌ها

✓ توسعه و ارزیابی برنامه اندازه‌گیری امنیت اطلاعات

امید است این کتاب بتواند راهنمای مناسبی جهت توسعه و بهبود مستمر امنیت اطلاعات در سازمان‌های دولتی و غیردولتی باشد. از تمامی اساتید به‌خصوص آقای مهندس براتی (معاونت محترم مرکز توسعه دولت الکترونیک، فناوری اطلاعات و آمادگی درایت کشور) که در زمینه ویرایش فنی و ادبی این اثر به بنده کمک شایانی نمودند کمال تقدیر و تشکر را دارم.

معزالدين حجت‌الاسلامی

بهار ۹۵