



تالیف و تدوین:

دکتر ناصر مدیری

مهندس مریم جدی



Publication **Mehregane Ghalam**

0	0	0	0	0	0
1	0	1	0	0	0
2	0	1	1	0	0
3	0	0	0	0	0
4	0	0	0	1	0
5	1	0	0	0	0
6	0	0	0	0	0

مدرسنامه: مدیری، ناصر

عنوان: مهندسی سیستم مدیریت امنیت اطلاعات

تالیف، و تدوین: ناصر مدیری، مریم جدی

مختصات نشر: تهران، مهرگان قلم

مختصات ظاهری: ۲۱۰ ص، مصور

شابک: 978-600-6236-29-2

وضعیت فهرست نویسی: فیا

یادداشت: واژه نامه

یادداشت: کتابنامه

موضوع: کامپیوترها - ایمنی اطلاعات - استانداردها

شناسه افزوده: مریم جدی

رده بندی کنگره: ۱۳۹۱ م ۵۹/۵۱۰۵ TK5۱۰

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۲۹۱۱۹۴۲



مهندسی سیستم مدیریت امنیت اطلاعات

www.mehreganeghalam.com

انتشارات مهرگان قلم

مؤلف: ناصر مدیری - مریم جدی

ناشر: مهرگان قلم

نویت چاپ اول: ۱۳۹۱

چاپ و صحافی: سپهر نوین

تیراژ: ۵۰۰ نسخه

قیمت: ۱۳۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۶۲۳۶-۲۹-۲

کلیه حقوق این اثر متعلق به انتشارات مهرگان قلم می باشد.

تهران، خیابان انقلاب، خیابان دانشگاد، بین خیابان روانپروخیابان نعلری، کوچه قدیری، پلاک ۲۲، واحد ۳

تلفن: ۶۶۹۶۰۷۶۳-۶۶۹۵۸۵۵۸

ن وَالْقَلَمِ وَمَا يَسْطُرُونَ

سه دشواری در کار تالیف وجود دارد:

نوشتن چیزی که قابل نشر باشد،

یافتن مرد شریفی که آنرا نشر دهد،

بیدا کردن مردان و زنان حساس و نکته سنجی که آنرا بخوانند!!

((کولتون))

به نام هستی بخش دانا

تاکنون کتب متعددی در زمینه امنیت اطلاعات در کشور تالیف و ترجمه شده است ولی تا به امروز کتابی که کلیه مباحث پیشرفته در سیستم مدیریت امنیت اطلاعات را به طور جامع شامل شود و مطابق با علم روز دنیا نیز باشد در دسترس نبوده است. پس از سالها تدریس و فعالیت در زمینه امنیت اطلاعات و با توجه به نیاز مبرم جامعه علمی و مسئولین، مصمم شدیم تلاش خود را در زمینه تالیف و گردآوری چنین منبع اطلاعاتی، به انجام رسانیم. پرداختن به مطالب کلیدی و به روز در زمینه سیستم مدیریت امنیت اطلاعات به نحوی که خواننده را به طریقی کاملاً ساده، روان و تخصصی تا انتها همراه خود کند از هم دغدغه های مولفین این کتاب بوده است. فصول کتاب "مهندسی سیستم مدیریت امنیت اطلاعات" در راستای نیل به اهداف ذکر شده به نحوی کاملاً مستقل و در عین حال از نظر مفهوم به هم پیوسته مطرح شده است.

با توجه به گستردگی این مباحث، در پایان هر فصل مطالبی جهت مطالعه ی بیشتر آورده شده است. خصوصیت بارز این کتاب، سادگی بیان به همراه استفاده از شکل ها و مثالهای ملموس جهت درک بهتر مفاهیم در هر مبحث است.

مطالب مطرح شده در هر فصل:

- ♦ فصل اول، امنیت اطلاعات
- ♦ فصل دوم، سیاست های امنیتی
- ♦ فصل سوم، حاکمیت فن آوری
- ♦ فصل چهارم، حاکمیت امنیت فن آوری
- ♦ فصل پنجم، برنامه جامع مدیریت فن آوری
- ♦ فصل ششم، استانداردهای سری IEC/ISO 27000

- ♦ فصل هفتم، استاندارد 27001 IEC/ISO
- ♦ فصل هشتم، استاندارد 27002 IEC/ISO
- ♦ فصل نهم، پروسه سیستم مدیریت امنیت اطلاعات

امید است این کتاب بتواند در خدمت دانشجویان رشته‌های مختلف علوم کامپیوتر قرار گیرد.
در خاتمه بر خود لازم می‌دانیم از تمامی عزیزانی که به نوعی در گردآوری مطالب این کتاب ما را یاری رساندند کمال تشکر و قدردانی را بعمل آوریم.
بی‌صبرانه منتظر نظرات، انتقادات و پیشنهادات شما هستیم.
پست الکترونیکی انعکاس نظرات:

info@27000.ir

www.27000.ir

ناصر مدیری - مریم جدی

فهرست مطالب

۱۴.....	۱. امنیت اطلاعات.....
۱۴.....	۱.۱. خلاصه فصل.....
۱۴.....	۱.۲. مفاهیم بنیادی در امنیت اطلاعات.....
۱۵.....	۱.۳. امنیت اطلاعات.....
۱۷.....	۱.۴. پروسه امنیت اطلاعات.....
۱۷.....	۱.۵. مهندسی امنیت.....
۱۹.....	۱.۶. اصول مهندسی امنیت.....
۲۰.....	۱.۷. چرخه حیات مهندسی امنیت.....
۲۰.....	۱.۷.۱. بسط مراتب اهداف، تسلسل و خط مشی.....
۲۱.....	۱.۷.۲. جبهه‌های تکنیکالی امنیت سازمان.....
۲۲.....	۱.۸. مدیریت امنیت اطلاعات.....
۲۲.....	۱.۹. ارزیابی کیفیت مهندسی امنیت.....
۲۴.....	۱.۱۰. متدولوژی.....
۲۶.....	۱.۱۱. فرآیندهای سیستم مهندسی امنیت.....
۲۷.....	۱.۱۲. سوالات متداول.....
۲۷.....	۱.۱۳. منابعی برای مطالعه بیشتر.....
۳۰.....	۲. سیاست های امنیتی.....
۳۰.....	۲.۱. خلاصه فصل.....
۳۰.....	۲.۲. خط مشی امنیتی چیست؟.....
۳۱.....	۲.۳. سیاست امنیتی چیست؟.....
۳۲.....	۲.۴. اجزاء خط مشی امنیتی.....
۳۵.....	۲.۵. سوالات متداول.....
۳۵.....	۲.۶. منابعی برای مطالعه بیشتر.....
۳۸.....	۳. حاکمیت فن آوری.....
۳۸.....	۳.۱. خلاصه فصل.....
۳۹.....	۳.۲. خصیصه های حاکمیت مطلوب.....
۴۰.....	۳.۳. مفهوم حاکمیت فناوری اطلاعات.....

۳.۴	اهمیت حاکمیت فناوری اطلاعات	۴۲
۳.۵	تعاریف مختلف از حاکمیت فناوری اطلاعات	۴۳
۳.۶	ضرورت حاکمیت فناوری اطلاعات	۴۴
۳.۷	اهمیت متریک‌های کارایی برای حاکمیت فناوری	۴۵
۳.۸	محدودیت حاکمیت فناوری اطلاعات	۴۶
۳.۹	نواحی تمرکز حاکمیت فناوری اطلاعات	۴۶
۳.۱۰	معماری های حاکمیت فناوری اطلاعات	۴۷
۳.۱۰.۱	معرفی معماری COBIT	۴۸
۳.۱۰.۲	معرفی معماری ITIL	۵۰
۳.۱۱	منشأ ITIL کجاست؟	۵۳
۳.۱۲	نسخه های مختلف ITIL	۵۳
۳.۱۳	مشخصه های کلیدی ITIL	۵۵
۳.۱۴	موجودیتهای ITIL	۵۶
۳.۱۵	مزایای کاربرد ITIL در سازمان	۵۶
۳.۱۶	مایل استونیهای مهم پنج گانه در تحقق موفق ITIL	۵۶
۳.۱۷	سؤالات متداول	۵۶
۳.۱۸	منابعی برای مطالعه بیشتر	۵۸
۴	حاکمیت امنیت فن آوری	۶۰
۴.۱	خلاصه فصل	۶۰
۴.۲	تعریف برنامه ریزی استراتژیک فناوری اطلاعات	۶۱
۴.۳	ضرورت تدوین برنامه استراتژیک فناوری اطلاعات	۶۲
۴.۴	مزایای تدوین برنامه استراتژیک	۶۲
۴.۵	فرآیند برنامه ریزی استراتژیک فناوری اطلاعات	۶۳
۴.۶	مشکلات برنامه ریزی استراتژیک فناوری اطلاعات	۶۶
۴.۷	سؤالات متداول	۶۶
۴.۸	منابعی برای مطالعه بیشتر	۶۶
۵	برنامه جامع مدیریت فن آوری	۶۸
۵.۱	خلاصه فصل	۶۸
۵.۲	طرح جامع فناوری اطلاعات و ارتباطات	۶۹
۵.۳	اهداف طرح جامع فناوری اطلاعات و ارتباطات	۷۴

۷۵	۵.۴. اصول حاکم بر طرح
۷۶	۵.۵. متدولوژی طرح جامع
۷۷	۵.۶. تدوین طرح جامع فناوری اطلاعات
۷۸	۵.۷. فرآیند تدوین طرح جامع
۷۸	۵.۸. سیاست‌های اصلی طرح جامع فناوری اطلاعات
۷۸	۵.۹. مراحل تدوین طرح جامع
۸۰	۵.۱۰. نکات قابل تأمل
۸۲	۵.۱۱. سؤالات متداول
۸۲	۵.۱۲. منابعی برای مطالعه بیشتر
۸۴	۶. استانداردهای سری ISO/IEC 27000
۸۴	۶.۱. خلاصه فصل
۸۴	۶.۲. مروری بر استاندارد BS 7799
۸۴	۶.۳. تاریخچه استاندارد BS 7799
۸۵	۶.۴. نحوه عملکرد استاندارد
۸۵	۶.۵. ISO/IEC 27000
۸۷	۶.۶. ارتباط بین خانواده استانداردهای ISO/IEC 27000
۸۷	۶.۷. اهم مسائل دراستانداردهای سری IEC/ISO ۲۷۰۰۰
۸۸	۶.۸. ارتباط مهندسی امنیت و استاندارد ۲۷۰۰۰
۸۹	۶.۹. ۲۷۰۰۱: نیازمندی های ISMS
۸۹	۶.۱۰. ۲۷۰۰۲: موارد کاربردی ISMS
۸۹	۶.۱۱. ۲۷۰۰۳: راهنمای پیاده سازی ISMS
۹۰	۶.۱۲. ۲۷۰۰۴: اندازه گیری و تعیین سطح ISMS
۹۰	۶.۱۳. ۲۷۰۰۵: اندازه گیری و تعیین سطح ISMS
۹۰	۶.۱۴. ۲۷۰۰۶: نیازمندیهای بازرسی و تصدیق ISMS
۹۰	۶.۱۵. ۲۷۰۰۷: راهنمای میزان ISMS
۹۰	۶.۱۶. ۲۷۰۰۸: راهنمای میزان کنترل های ISMS
۹۱	۶.۱۷. ۲۷۰۱۰: راهنماهای ISMS برای ارتباطات بین بخش
۹۱	۶.۱۸. ۲۷۰۱۱: راهنمای برای تأمین ارتباطات راه دور سازمانها
۹۱	۶.۱۹. ۲۷۰۱۳: راهنماهایی برای پیاده‌سازی یکپارچه ۲۷۰۰۱ و ۲۰۰۰-۱
۹۱	۶.۲۰. ۲۷۰۱۴: چارچوب حاکمیت امنیت اطلاعات

۲۷۰۱۵.۶.۲۱	راهنمای ISMS برای خدمات مالی و بیمه‌ای	۹۱
۲۷۰۳۴.۶.۲۲	راهنمای امنیت برنامه کاربردی	۹۲
۲۷۰۳۳.۶.۲۳	استاندارد چندبخشی	۹۲
۲۷۰۳۶.۶.۲۴	راهنمای امنیتی برای ارتباطات خارج از سازمان	۹۴
۶.۲۵	سوالات متداول	۹۶
۶.۲۶	منابعی برای مطالعه بیشتر	۹۶
۷	استاندارد ISO/IEC 27001	۹۸
۷.۱	خلاصه فصل	۹۸
۷.۲	آشنایی با استاندارد ISO/IEC 27001	۹۸
۷.۳	فواید استاندارد ISO/IEC 27001	۹۹
۷.۴	مزایای استاندارد ISO/IEC 27001	۱۰۰
۷.۵	BS7799 / ISO 27001	۱۰۱
۷.۶	معرفی سه مؤلفه اصلی حفاظت اطلاعات (CIA)	۱۰۱
۷.۷	استاندارد ISO/IEC 27001، پردازش مدیریت داده‌ها	۱۰۲
۷.۸	همسویی با سایر استانداردهای سیستم مدیریت	۱۰۲
۷.۹	ISO 27001 و مدیریت آن	۱۰۲
۷.۱۰	متدولوژی ISO/IEC 27001	۱۰۴
۷.۱۱	گامهای الزامی در پیاده‌سازی ISO/IEC 27001	۱۰۴
۷.۱۲	ساختار ISO/IEC 27001	۱۰۵
۷.۱۳	پروژه اجرای ISO/IEC 27001	۱۰۶
۷.۱۴	بکارگیری ISO 9001 برای پیاده‌سازی ISO 27001	۱۰۶
۷.۱۵	FAQهایی برای ISO/IEC 27001	۱۰۸
۷.۱۶	حوزه‌های مدیریت اطلاعات	۱۰۸
۷.۱۷	حوزه اول - خط مشی امنیتی	۱۰۸
۷.۱۸	جزء ۱ خط مشی امنیتی	۱۰۹
۷.۱۹	حوزه دوم - سازماندهی امنیت اطلاعات	۱۱۰
۷.۲۰	حوزه سوم - مدیریت دارایی‌ها	۱۱۰
۷.۲۱	حوزه چهارم - امنیت منابع انسانی	۱۱۱
۷.۲۲	حوزه پنجم - امنیت محیطی و فیزیکی	۱۱۲
۷.۲۳	حوزه ششم - مدیریت اطلاعات و ارتباطات	۱۱۳

۷.۲۴	حوزه هفتم - کنترل دسترسی	۱۱۵
۷.۲۵	حوزه هشتم - تهیه، نگهداری و توسعه سیستم	۱۱۶
۷.۲۶	حوزه نهم - مدیریت حوادث امنیت اطلاعات	۱۱۷
۷.۲۷	حوزه دهم - طرح تداوم کسب و کار	۱۱۸
۷.۲۸	حوزه یازدهم - مطابقت با قوانین	۱۱۸
۷.۲۹	گامهای مهم در پیاده سازی و اخذ گواهینامه ۲۷۰۰۱	۱۱۹
۷.۳۰	فرآیند دریافت گواهی ISO/IEC 27001	۱۱۹
۷.۳۱	سوالات متداول	۱۲۰
۷.۳۲	منابعی برای مطالعه بیشتر	۱۲۰
۸	استاندارد ISO/IEC 27002	۱۲۲
۸.۱	خلاصه فصل	۱۲۲
۸.۲	استاندارد ISO/IEC 27002	۱۲۲
۸.۳	حوزه استاندارد	۱۲۳
۸.۴	حوزه های مدیریت اطلاعات در ISO/IEC 27002	۱۲۳
۸.۵	هدف و دیدگاه استاندارد	۱۲۳
۸.۶	سازگاری با سایر استانداردهای مدیریتی	۱۲۵
۸.۷	کاربرد	۱۲۵
۸.۸	واژگان و تعاریف	۱۲۵
۸.۹	استاندارد ملی	۱۲۷
۸.۱۰	سرفصلها	۱۲۹
۸.۱۱	معرفی استاندارد ISO/IEC 27005	۱۲۹
۸.۱۲	پروژه مدیریت ریسک و استاندارد ISO ۲۷۰۰۵	۱۳۰
۸.۱۳	فلوچارت مدیریت ریسک توسط ISO/IEC 27005	۱۳۱
۸.۱۴	سوالات متداول	۱۳۱
۸.۱۵	منابعی برای مطالعه بیشتر	۱۳۲
۹	پروژه سیستم مدیریت امنیت اطلاعات	۱۳۴
۹.۱	خلاصه فصل	۱۳۴
۹.۲	سیستم مدیریت امنیت اطلاعات	۱۳۵
۹.۳	سیستم مدیریت امنیت اطلاعات	۱۳۶
۹.۴	اهداف کلان سیستم مدیریت امنیت اطلاعات	۱۳۷

۱۳۸	۹.۵. دامنه و راهبردهای سیستم مدیریت امنیت اطلاعات
۱۳۹	۹.۶. هدف سیستم مدیریت امنیت اطلاعات
۱۳۹	۹.۷. استانداردهای مدیریت امنیت اطلاعات
۱۳۹	۹.۷.۱. رهیافت استفاده از استانداردهای مدیریتی
۱۴۰	۹.۷.۲. مروری بر استانداردهای مدیریت امنیت اطلاعات
۱۴۳	۹.۸. کیفیت سیستم مدیریت امنیت اطلاعات
۱۴۳	۹.۹. اندازه گیری سیستم مدیریت امنیت اطلاعات
۱۴۴	۹.۱۰. تشکیلات تأمین امنیت فضای تبادل اطلاعات
۱۴۶	۹.۱۰.۱. شرح وظایف تشکیلات امنیتی
۱۴۸	۹.۱۱. ایجاد سیستم مدیریت امنیت اطلاعات
۱۵۱	۹.۱۲. پیاده سازی و اجرای ISMS
۱۵۲	۹.۱۳. پایش و بازنگری ISMS
۱۵۳	۹.۱۴. چرخه استمرار سیستم مدیریت امنیت اطلاعات
۱۶۳	۹.۱۵. مستندات ISMS
۱۶۳	۹.۱۵.۱. اهداف، راهبردها و سیاست های امنیتی
۱۶۵	۹.۱۵.۲. طرح تحلیل مخاطرات امنیتی
۱۶۶	۹.۱۵.۳. مستندات مفید
۱۶۶	۹.۱۶. فاکتورهای مهم در موفقیت ISMS
۱۶۸	۹.۱۷. نیازهای ISMS
۱۶۹	۹.۱۸. نگهداری و بهبود ISMS
۱۶۹	۹.۱۹. مشکلات پیاده سازی ISMS
۱۷۰	۹.۲۰. ساختار ISMS
۱۷۱	۹.۲۱. مزایای ISMS
۱۷۲	۹.۲۲. مسئولیتها و تعهدات
۱۷۲	۹.۲۳. مسیر دستیابی به گواهینامه - الزامات گواهینامه
۱۷۳	۹.۲۴. پروسه اخذ گواهینامه ISMS (فازها و وظایف)
۱۷۶	۹.۲۵. FAQ های برای ISMS
۱۷۷	۹.۲۶. سؤالات متداول
۱۷۸	۹.۲۷. منابعی برای مطالعه بیشتر

۱۸۰.....	۱. ضمیمه اول
۱۸۰.....	فرآیندهای فناوری اطلاعات برای هریک از حوزه های اصلی COBIT
۱۸۲.....	۲. ضمیمه دوم
۱۸۲.....	استانداردهای سری ۲۷۰۰۰
۱۸۵.....	۳. ضمیمه سوم
۱۸۵.....	پیوست الف- اهداف کنترلی و کنترل ها (الزامی)
۲۰۹.....	۴. ضمیمه چهارم ۱۱ حوزه قابل پیاده سازی برای ISMS
۲۱۶.....	۵. ضمیمه پنجم: حوزه دارایی های اطلاعاتی
۲۳۳.....	۶. ضمیمه ششم: مدیریت منابع انسانی
۲۴۷.....	۷. ضمیمه هفتم: مدیریت امنیت فیزیکی و محیطی
۲۷۸.....	۸. ضمیمه هشتم: مدیریت حوادث اطلاعات امنیتی
۲۹۸.....	۹. ضمیمه نهم
۲۹۸.....	واژگان و عبارات (انگلیسی به فارسی)
۳۰۳.....	۱۰. ضمیمه دهم
۳۰۳.....	فهرست علائم اختصاری