



پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات

راهنمای کامل اخذ گواهینامه ISO 27000

مرجعی برای دروس مدیریت امنیت اطلاعات، معماری امنیت اطلاعات
مدل‌ها و استانداردهای امنیت اطلاعات

مؤلف:

دکتر محمدعلی ترکمانی

سرشناسه	:	ترکمانی، محمدعلی، ۱۳۵۴-
عنوان و نام پدیدآور	:	پایه‌سازی سیستم‌های مدیریت امنیت اطلاعات : راهنمای کامل اخذ گواهینامه ISO 27000
مشخصات نشر	:	مشهد: ارسطو، ۱۳۹۴ .
مشخصات ظاهری	:	۲۷۲ص: مصور، جدول، نمودار ؛ ۱۷×۲۴س.م.
شابک	:	978-600-7558-50-8
وضعیت فهرست نویسی	:	فیبای مختصر
یادداشت	:	این مدرک در آدرس http://opac.nlai.ir قابل دسترسی است.
شماره کتابشناسی ملی	:	۳۷۶۶۴۴۰

نام کتاب : پایه‌سازی سیستم‌های مدیریت امنیت اطلاعات

مؤلف : دکتر محمدعلی ترکمانی

ناشر : ارسطو (با همکاری سامانه اطلاع‌رسانی چاپ و نشر ایران)

صفحه‌آرایی، تنظیم و طرح جلد : محمدعلی ترکمانی و علی بیات

تیراژ: ۱۰۰۰ جلد

نوبت چاپ : ششم - ۱۳۹۸

تعداد صفحات: ۲۶۱ صفحه

چاپ : مدیران

قیمت : ۵۳۰۰۰ تومان

شابک : ۹۷۸ - ۶۰۰ - ۷۵۵۸ - ۵۰ - ۸

تلفن‌های مرکز پخش : ۰۹۱۷۷۱۶۴۹۴۰ - ۵۰۹۶۱۴۶ - ۰۵۱۱

این اثر مشمول قانون حمایت از مولفان و مصنفان و هنرمندان است. هر کس تمام یا قسمتی از این اثر را بدون اجازه مولف نشر یا پخش یا عرضه کند، مورد پیگرد قانونی قرار خواهد گرفت.

فهرست مطالب

فصل اول: تعاریف و اصول پایه	۱۹
۱-۱- تعریف امنیت اطلاعات و سیستم امن	۱۹
۱-۱-۱- سیستم امن	۱۹
۱-۲- اصطلاحات امنیتی	۲۰
۱-۲-۱- آسیب پذیری	۲۰
۱-۲-۲- حمله	۲۰
۱-۲-۳- تهدید	۲۰
۱-۲-۴- مفهوم AAA در امنیت اطلاعات	۲۱
۱-۳- سرویس‌های امنیتی	۲۲
۱-۴- مکانیزم‌های امنیتی	۲۲
۱-۵- خط‌مشی‌ها یا سیاست‌های امنیتی	۲۳
۱-۵-۱- سیاست‌های کلمه عبور	۲۴
۱-۵-۲- سیاست‌های اینترنتی	۲۴
۱-۵-۳- پشتیبان‌گیری و احیای اطلاعات	۲۵
۱-۶- مفهوم سیستم مدیریت امنیت اطلاعات	۲۵
۱-۷- استانداردهای مدیریتی ارائه‌شده در خصوص امنیت اطلاعات	۲۵
۱-۸- استانداردهای خانواده ISO27000	۲۶
۱-۹- گزارش فنی ISO/IEC TR ۱۳۳۳۵	۲۶
۱-۱۰- مراحل ایمن‌سازی بر اساس گزارش فنی ISO/IEC TR ۱۳۳۳۵	۲۷

- ۱-۱۱- مزایای پیاده‌سازی و صدور گواهینامه ایزو ۲۷۰۰۱ ۲۷
- ۱-۱۲- مشکلات پیاده‌سازی ISMS ۲۸
- ۱-۱۳- مستندات ISMS ۲۹
- ۱-۱۴- حوزه‌های چهارده‌گانه ISO 27001:2013 ۲۹
- ۱-۱۵- سؤالات تشریحی ۳۰
- ۱-۱۶- سؤالات چهارگزینه‌ای ۳۱
- پاسخ سؤالات ۳۳

فصل دوم: خط‌مشی‌های امنیتی سازمان ۳۵

- ۲-۱- مقدمه ۳۵
- ۲-۲- خط‌مشی‌های امنیتی ۳۵
- ۲-۲-۱- تدوین مستند خط‌مشی امنیت اطلاعات ۳۵
- ۲-۲-۲- بازنگری و ارزیابی خط‌مشی امنیت اطلاعات سازمان ۳۷
- ۲-۳- سؤالات تشریحی ۳۸
- ۲-۴- سؤالات چهارگزینه‌ای ۳۸
- پاسخ سؤالات ۳۹

فصل سوم: سازمان‌دهی امنیت اطلاعات ۴۱

- ۳-۱- مقدمه ۴۱
- ۳-۲- سازمان‌دهی مدیریت امنیت اطلاعات در داخل سازمان ۴۱
- ۳-۲-۱- کمیته‌ای راهبری امنیت اطلاعات ۴۲
- ۳-۲-۲- تیم‌های پشتیبانی امنیت اطلاعات ۴۳
- ۳-۲-۳- تعیین و تخصیص مسئولیت‌های افراد مرتبط با امنیت اطلاعات ۴۳
- ۳-۲-۳-۱- شرح وظائف و مسئولیت‌های کمیته راهبردی امنیت ۴۴

- ۳-۲-۳-۲- شرح وظایف و مسئولیت‌های مدیر امنیت شبکه ۴۴
- ۳-۲-۳-۳- شرح وظایف و مسئولیت‌های واحد پشتیبانی امنیت ۴۵
- ۳-۲-۳-۴- شرح وظائف نظارت و بازرسی امنیتی ۴۷
- ۳-۲-۳-۵- شرح وظائف مدیریت تغییرات ۴۹
- ۳-۲-۳-۶- شرح وظائف نگهداری امنیت شبکه کامپیوتری ۴۹
- ۳-۲-۳-۷- مسئولیت مدیران میانی سازمان ۵۰
- ۳-۲-۳-۸- تأمین ارتباط با مسئولین و بالاترین مقام سازمان ۵۰
- ۳-۲-۳-۹- برقراری ارتباطات با گروه‌ها و انجمن‌های امنیتی متخصص ۵۰
- ۳-۲-۳-۱۰- امنیت اطلاعات در مدیریت پروژه‌های سازمان ۵۱
- ۳-۳- مدیریت امنیت اطلاعات در تعاملات با طرف‌های خارج از سازمان، دستگاه‌های سیار و دورکاری ۵۱
- ۳-۳-۱- اطمینان از امنیت اطلاعات در زمان استفاده از کامپیوترهای قابل حمل ۵۲
- ۳-۳-۲- شناسایی ریسک‌های دسترسی طرف‌های خارج از سازمان و دستگاه‌های سیار ۵۲
- ۳-۳-۳- توجه به امنیت در قرارداد با طرف‌های خارج از سازمان ۵۲
- ۳-۳-۴- دور کاری ۵۳
- ۳-۴- سؤالات تشریحی ۵۳
- ۳-۵- سؤالات چهارگزینه‌ای ۵۴
- پاسخ سؤالات ۵۵
- فصل چهارم: امنیت منابع انسانی ۵۷**
- ۴-۱- مقدمه ۵۷
- ۴-۲- لحاظ نمودن امنیت قبل از به‌کارگیری ۵۸
- ۴-۳- لحاظ نمودن امنیت در حین خدمت ۵۹

- ۱-۳-۴- آگاهی‌رسانی کسب مهارت و آموزش امنیت ۵۹
- ۲-۳-۴- فرآیندهای انضباطی ۵۹
- ۴-۴- شیوه مناسب خاتمه دادن به همکاری کارکنان ۵۹
- ۵-۴- سؤالات تشریحی ۶۰
- ۶-۴- سؤالات چهارگزینه‌ای ۶۰
- پاسخ سؤالات ۶۰

فصل پنجم: مدیریت دارایی‌ها ۶۳

- ۱-۵- مقدمه ۶۳
- ۲-۵- طبقه‌بندی اطلاعات و اسناد ۶۳
- ۳-۵- شناسایی دارایی‌های مرتبط با اطلاعات در سازمان ۶۴
- ۴-۵- نشانه‌گذاری (برچسب) و پشتیبانی از اطلاعات ۶۴
- ۵-۵- مدیریت رسانه‌ها ۶۵
- ۶-۵- فهرست کلی اقدامات حفاظتی ۶۵
- ۷-۵- اصول حفاظتی ۶۷
- ۸-۵- سؤالات تشریحی ۶۸
- ۹-۵- سؤالات چهارگزینه‌ای ۶۹
- پاسخ سؤالات ۶۹

فصل ششم: کنترل دسترسی ۷۱

- ۱-۶- سیاست‌گذاری و خط‌مشی کنترل دسترسی ۷۱
- ۲-۶- پیشگیری از دسترسی غیرمجاز به سرویس‌های شبکه ۷۲
- ۳-۶- اطمینان از دسترسی مجاز به اطلاعات و سیستم‌ها ۷۳
- ۴-۶- ملزم نمودن کاربران به محافظت از اطلاعات احراز هویت ۷۴

۶-۵- کنترل دسترسی به سیستم و برنامه ۷۴

۶-۵-۱- محدودیت دسترسی به اطلاعات سیستم ۷۴

کنترل : دسترسی به اطلاعات و کارکردهای سیستم برنامه ، باید مطابق با خطمشی

کنترل دسترسی ، محدود شود ۷۴

۶-۵-۲- ورود امن به سیستم ۷۴

۶-۶- سیستم مدیریت کلمه عبور ۷۴

۶-۷- اعمال محدودیت استفاده از ابزارهای جانبی ۷۵

۶-۸- پیشگیری از دسترسی غیرمجاز به سیستم‌عامل‌ها ۷۶

۶-۸-۱- کنترل دسترسی به کد منبع برنامه ها ۷۶

۶-۹- سؤالات تشریحی ۷۶

۶-۱۰- سؤالات چهارگزینه‌ای ۷۷

پاسخ سؤالات ۷۸

فصل هفتم: رمزنگاری ۷۹

۷-۱- مفاهیم و اصطلاحات رمزنگاری ۷۹

۷-۲- سیستم‌های رمزنگاری ۸۰

۷-۲-۱- رمزنگاری متقارن ۸۰

۷-۲-۲- رمزنگاری نامتقارن ۸۱

۷-۳- رمزنگاری با کلید عمومی ۸۱

۷-۴- صحت پیام با استفاده از MAC ۸۲

۷-۵- الگوریتم‌های MAC ۸۴

۷-۶- امضای دیجیتال ۸۴

۷-۷-گواهینامه	۸۵
۷-۸-حملات ممکن علیه امضای دیجیتالی	۸۷
۷-۹-تأمین محرمانگی، اصالت و صحت اطلاعات	۸۸
۷-۹-۱-سیاست استفاده از مکانیزم کنترل‌های رمزنگاری	۸۸
۷-۹-۲-مدیریت کلید	۸۸
۷-۱۰-سئوالات تشریحی	۸۸
۷-۱۱-سئوالات چهارگزینه‌ای	۸۸
پاسخنامه:	۹۰

فصل هشتم: امنیت فیزیکی و محیطی ۹۱

۸-۱-مقدمه	۹۱
۸-۲-نواحی امن	۹۱
۸-۲-۱-حصار امنیت فیزیکی	۹۱
۸-۲-۲-کنترل‌های مداخل فیزیکی (کنترل تردد)	۹۱
۸-۲-۳-ایمن‌سازی دفاتر اتاق‌ها و تأسیسات	۹۲
۸-۲-۴-محافظت در برابر تهدیدهای بیرونی و محیطی	۹۳
۸-۲-۵-جداسازی فضاهای دسترسی عمومی تخلیه، بارگیری و ارسال و دریافت	۹۳
۸-۳-امنیت تجهیزات و تجهیزات امن	۹۳
۸-۳-۱-استقرار و حفاظت از تجهیزات	۹۴
۸-۳-۱-۱-میز کار	۹۴
۸-۳-۲-امکانات پشتیبانی (منابع تغذیه)	۹۴
۸-۳-۳-امنیت کابل‌کشی	۹۶
۸-۳-۴-نگهداری از تجهیزات	۹۶

- ۸-۳-۵- راه‌های خروج تجهیزات از سازمان ۹۷
- ۸-۳-۶- امنیت تجهیزات خارج از محل‌های اصلی ۹۷
- ۸-۳-۷- امحاء یا استفاده مجدد از تجهیزات به‌صورت امن ۹۷
- ۸-۳-۷-۱- خطمشی اسقاط یا استفاده مجدد از تجهیزات ۹۸
- ۸-۳-۸- تجهیزات رهاشده و بدون مراقبت توسط کاربر ۹۸
- ۸-۳-۹- سیاست نمایشگر پاک و میز پاک ۹۹
- ۸-۳-۹-۱- خطمشی نمایشگر پاک ۹۹
- ۸-۴- سؤالات تشریحی ۱۰۰
- ۸-۵- سؤالات چهارگزینه‌ای ۱۰۰
- پاسخ سؤالات ۱۰۱

فصل نهم: امنیت عملیات ۱۰۳

- ۹-۱- اطمینان از عملکرد صحیح و امن امکانات پردازش اطلاعات. ۱۰۳
- ۹-۲- حفاظت در برابر بدافزارها ۱۰۴
- ۹-۳- پشتیبان‌گیری ۱۰۴
- ۹-۴- ثبت رویدادها و پایش ۱۰۵
- ۹-۴-۱- نظارت بر ثبت وقایع ۱۰۵
- ۹-۴-۲- ثبت خطاها ۱۰۶
- ۹-۴-۳- محافظت از فایل‌های log ۱۰۶
- ۹-۴-۴- ثبت عملکرد مدیران و اپراتورهای سیستم‌ها. ۱۰۶
- ۹-۴-۵- هم‌زمان نمودن ساعت سیستم‌ها ۱۰۶
- ۹-۵- کنترل نرم‌افزارهای عملیاتی ۱۰۶
- ۹-۶- مدیریت آسیب‌پذیری فنی ۱۰۷

- ۱-۶-۹- استخراج اطلاعات مربوط به آسیب‌پذیری‌های فنی ۱۰۷
- ۲-۶-۹- محدودیت‌های نصب نرم‌افزار ۱۰۷
- ۷-۹- ممیزی سامانه‌های اطلاعاتی ۱۰۷
- ۸-۹- سؤالات تشریحی ۱۰۷
- ۹-۹- سؤالات چهارگزینه‌ای ۱۰۸
- پاسخ سؤالات ۱۰۸

فصل دهم: امنیت ارتباطات ۱۰۹

- ۱-۱۰- مدیریت امنیت شبکه ۱۰۹
- ۱-۱۰-۱- مکانیزم‌های کنترل شبکه کامپیوتری ۱۰۹
- ۲-۱۰-۱- امنیت در سرویس‌های شبکه ۱۰۹
- ۳-۱۰-۱- تفکیک در شبکه‌ها ۱۰۹
- ۲-۱۰- تأمین امنیت انتقال اطلاعات ۱۱۰
- ۱-۱۰-۲- خط‌مشی‌ها و روش اجرایی انتقال اطلاعات ۱۱۰
- ۲-۱۰-۲- تفاهم‌نامه یا قرارداد انتقال اطلاعات ۱۱۰
- ۳-۱۰-۲- امنیت پست الکترونیک ۱۱۰
- ۴-۱۰-۲- تفاهم‌نامه محرمانگی یا عدم افشا ۱۱۰
- ۳-۱۰- سؤالات تشریحی ۱۱۱
- ۴-۱۰- سؤالات چهارگزینه‌ای ۱۱۱
- پاسخ سؤالات ۱۱۲

فصل یازدهم: استفاده، توسعه و نگهداری سیستم‌های اطلاعاتی ۱۱۳

- ۱-۱۱- الزامات امنیتی سیستم‌های اطلاعاتی ۱۱۳

- ۱۱-۱-۱- تحلیل و تعیین الزامات امنیت اطلاعات ۱۱۳
- ۱۱-۱-۲- تأمین امنیت خدمات کاربردی بر روی شبکه‌های عمومی ۱۱۳
- ۱۱-۱-۳- محافظت از تراکنش‌های خدمات کاربردی ۱۱۳
- ۱۱-۲- امنیت در فرایندهای توسعه و پشتیبانی ۱۱۴
- ۱۱-۲-۱- امنیت خط‌مشی توسعه ۱۱۴
- ۱۱-۲-۲- روش‌های اجرای کنترل تغییرات سامانه ۱۱۴
- ۱۱-۲-۳- بازنگری فنی نرم‌افزارهای کاربردی بعد از تغییرات بستر عملیاتی ۱۱۴
- ۱۱-۲-۴- محدودیت‌های تغییرات بسته‌های نرم‌افزاری ۱۱۴
- ۱۱-۲-۵- امنیت اصول مهندسی سامانه ۱۱۵
- ۱۱-۲-۶- امنیت محیط توسعه ۱۱۵
- ۱۱-۲-۷- توسعه برون‌سپاری ۱۱۵
- ۱۱-۲-۸- تست امنیت سامانه ۱۱۵
- ۱۱-۲-۹- تست پذیرش سامانه ۱۱۵
- ۱۱-۳- محافظت از داده‌های بکار رفته جهت تست ۱۱۵
- ۱۱-۴- سؤالات تشریحی ۱۱۵
- ۱۱-۵- سؤالات چهارگزینه‌ای ۱۱۶
- پاسخ سؤالات ۱۱۷

فصل دوازدهم: ارتباط با تأمین‌کنندگان ۱۱۹

- ۱۲-۱- امنیت اطلاعات در ارتباط با تأمین‌کنندگان ۱۱۹
- ۱۲-۱-۱- خط‌مشی امنیت اطلاعات برای ارتباط با تأمین‌کنندگان ۱۱۹
- ۱۲-۱-۲- پرداختن به امنیت در تفاهم‌نامه با تأمین‌کنندگان ۱۱۹

۱۲۰-۱-۳- زنجیره تأمین فناوری اطلاعات و ارتباطات ۱۲۰

۱۲۰-۲- مدیریت تحویل خدمات تأمین‌کننده ۱۲۰

۱۲۰-۲-۱- نظارت و بازرنگری خدمات تأمین‌کننده ۱۲۰

۱۲۱-۲-۲- مدیریت تغییرات خدمات تأمین‌کننده ۱۲۱

۱۲۱-۳- سؤالات تشریحی ۱۲۱

۱۲۱-۴- سؤالات چهارگزینه‌ای ۱۲۱

۱۲۲- پاسخ سؤالات ۱۲۲

فصل سیزدهم: مدیریت حوادث امنیتی ۱۲۳

۱۲۳-۱- مدیریت و بهبود رخدادهای امنیت اطلاعات ۱۲۳

۱۲۳-۱-۱- مسئولیت‌ها و رویه‌ها ۱۲۳

۱۲۳-۱-۲- گزارش دهی رویدادهای امنیت اطلاعات ۱۲۳

۱۲۳-۱-۳- گزارش دهی نقاط ضعف امنیت اطلاعات ۱۲۳

۱۲۴-۱-۴- ارزیابی و تصمیم‌گیری درباره رویدادهای امنیت اطلاعات ۱۲۴

۱۲۴-۱-۵- پاسخ به رخدادهای امنیت اطلاعات ۱۲۴

۱۲۴-۱-۶- جمع‌آوری شواهد ۱۲۴

۱۲۴-۱-۷- مسئولیت‌ها و رویه‌ها ۱۲۴

۱۲۴-۲- برخی نکات مهم درزمینه مدیریت و بهبود رخدادهای امنیت اطلاعات ۱۲۴

۱۲۵-۳- سؤالات تشریحی ۱۲۵

۱۲۵-۴- سؤالات چهارگزینه‌ای ۱۲۵

۱۲۶- پاسخ سؤالات ۱۲۶

فصل چهاردهم: جنبه‌های امنیت اطلاعات در مدیریت تداوم کسب‌وکار ۱۲۷

۱۴-۱-مقدمه	۱۲۷
۱۴-۲-مزایای پیاده‌سازی مدیریت تداوم کسب‌وکار	۱۲۷
۱۴-۳-چارچوب طرح پیوستگی کسب‌وکار	۱۲۸
۱۴-۴-جنبه‌های امنیت اطلاعات در مدیریت تداوم کسب‌وکار	۱۲۹
۱۴-۴-۱-طرح‌ریزی تداوم امنیت اطلاعات	۱۲۹
۱۴-۴-۲-پیاده‌سازی تداوم امنیت اطلاعات	۱۲۹
۱۴-۴-۳-بررسی، بازنگری و ارزیابی تداوم امنیت اطلاعات	۱۲۹
۱۴-۵-افزونگی	۱۲۹
۱۴-۶-سؤالات تشریحی	۱۳۰
۱۴-۷-سؤالات چهارگزینه‌ای	۱۳۰
پاسخ سؤالات	۱۳۱

فصل پانزدهم: سازگاری با قوانین(انطباق) ۱۳۳

۱۵-۱-مفهوم سازگاری با قوانین	۱۳۳
۱۵-۲-انطباق با الزامات قانونی و قراردادی	۱۳۳
۱۵-۲-۱-شناسایی الزامات قانونی و قراردادی قابل اجرا	۱۳۳
۱۵-۲-۲-حقوق مالکیت معنوی	۱۳۴
۱۵-۲-۳-حفاظت از سوابق	۱۳۴
۱۵-۲-۴-حریم خصوصی و حفاظت از اطلاعات هویت شخصی	۱۳۴
۱۵-۲-۵-قواعد کنترل‌های رمزنگاری	۱۳۵
۱۵-۳-بازنگری‌های امنیت اطلاعات	۱۳۵
۱۵-۳-۱-بازنگری مستقل امنیت اطلاعات	۱۳۵
۱۵-۳-۲-انطباق با خط‌مشی و استانداردهای امنیتی	۱۳۵

- ۱۳۶ بازنگری انطباق فنی ۱۵-۳-۳
- ۱۳۶ سؤالات تشریحی ۱۵-۴
- ۱۳۶ سؤالات چهارگزینه‌ای ۱۵-۵
- ۱۳۷ پاسخنامه

فصل شانزدهم: مدیریت ریسک ۱۳۹

- ۱۳۹ مقدمه ۱۶-۱
- ۱۳۹ مخاطره (ریسک) چیست؟ ۱۶-۲
- ۱۴۰ مراحل مدیریت مخاطرات ۱۶-۳
- ۱۴۰ شناسایی دارایی‌ها ۱۶-۳-۱
- ۱۴۲ شناسایی تهدیدها ۱۶-۳-۲
- ۱۴۷ شناسایی نقاط آسیب‌پذیری ۱۶-۳-۳
- ۱۴۷ ارزیابی مخاطرات ۱۶-۳-۴
- ۱۵۰ روش‌های مواجه‌شدن با ریسک‌ها ۱۶-۳-۵
- ۱۵۲ عوامل موفقیت پروژه مدیریت خطرات امنیتی ۱۶-۴
- ۱۵۳ پروژه NSC ۱۶-۵
- ۱۵۵ سؤالات تشریحی ۱۶-۶
- ۱۵۵ سؤالات چهارگزینه‌ای ۱۶-۷
- ۱۵۸ پاسخ سؤالات

فصل هفدهم: پیاده‌سازی سیستم مدیریت امنیت اطلاعات ۱۵۹

- ۱۵۹ مقدمه ۱۷-۱
- ۱۵۹ نحوه پیاده‌سازی ISMS در سازمان‌ها و مراحل اخذ گواهینامه ۱۷-۲
- ۱۵۹ چرخه استمرار پیاده‌سازی ISMS ۱۷-۳

- ۱۶۲ ۱۷-۳-۱- مراحل اجرای ISMS بر اساس چرخه دمینگ
- ۱۶۵ ۱۷-۴- متدولوژی اجرای ISMS
- ۱۶۵ ۱۷-۴-۱- پایه‌گذاری ISMS
- ۱۶۶ ۱۷-۴-۲- تعریف هدف نهایی سیستم مدیریت امنیت اطلاعات
- ۱۶۸ ۱۷-۴-۳- واگذاری طراحی سیستم مدیریت امنیت اطلاعات
- ۱۶۹ ۱۷-۴-۴- ارزیابی مخاطرات و رفع مخاطرات با تأثیر زیاد
- ۱۷۰ ۱۷-۴-۵- طراحی سیستم مدیریت امنیت اطلاعات
- ۱۷۰ ۱۷-۴-۶- واگذاری پیاده‌سازی سیستم مدیریت امنیت اطلاعات
- ۱۷۱ ۱۷-۴-۷- پیاده‌سازی سیستم مدیریت امنیت اطلاعات
- ۱۷۱ ۱۷-۴-۸- آموزش امنیت اطلاعات
- ۱۷۱ ۱۷-۴-۹- پشتیبانی ISMS برای مدت ۲ تا ۳ ماه
- ۱۷۲ ۱۷-۵- مستندات تعریف و واگذاری طراحی / پیاده‌سازی
- ۱۷۲ ۱۷-۵-۱- RFP پروژه ISMS
- ۱۷۲ ۱۷-۵-۱-۱- قلمرو ISMS
- ۱۷۴ ۱۷-۵-۱-۲- قرارداد عدم افشاء اطلاعات کارفرما
- ۱۷۵ ۱۷-۵-۱-۳- جدول ارزیابی پیشنهاد
- ۱۷۸ ۱۷-۶- متدولوژی ارزیابی ریسک بر اساس NIST SP 800-30
- ۱۷۸ ۱۷-۷- طرح Risk Treatment
- ۱۷۹ ۱۷-۸- طرح پشتیبانی حوادث بر اساس مستند NIST SP800-61
- ۱۸۰ ۱۷-۹- متدولوژی پشتیبانی حوادث بر اساس مستند NIST SP800-61
- ۱۸۱ ۱۷-۱۰- طرح آگاهی‌رسانی، کسب مهارت و آموزش امنیت بر اساس NIST SP800- ۵۰

۱۷-۱۱-متدولوژی آگاهی‌رسانی، کسب مهارت و آموزش امنیت بر اساس مستند 50 NIST	SP800-.....
۱۸۲	
۱۷-۱۲-سؤالات تشریحی
۱۸۳	
۱۷-۱۳-سؤالات چهارگزینه‌ای
۱۸۴	
پاسخ سؤالات
۱۸۷	

فصل هجدهم: نمونه‌ای از سیاست‌های امنیتی ۱۸۹

۱۸-۱-مقدمه
۱۸۹	
۱۸-۲-سیاست امنیت اطلاعات
۱۸۹	
۱۸-۳-سیاست‌های امنیتی کامپیوتری
۱۹۵	
۱۸-۴-سیاست‌های امنیتی شبکه
۱۹۸	
۱۸-۵-سیاست‌های امنیتی کنترل دسترسی
۲۰۱	
۱۸-۶-سیاست‌های امنیتی کنترل دسترسی از راه دور
۲۰۸	
۱۸-۷-سیاست‌های امنیتی دیوار آتش
۲۱۳	
۱۸-۸-سیاست امنیتی پست الکترونیک
۲۱۶	

فصل نوزدهم: متن استاندارد ISO/IEC 27001:2013 ۲۲۱

۲،۶ اهداف امنیت اطلاعات و طرح‌ریزی برای دستیابی به آنها
۲۲۸	
جدول الف.۷ - اهداف کنترلی و کنترل‌ها
۲۳۵	
الف.۱۲، ۶: مدیریت آسیب‌پذیری فنی
۲۴۲	
پیوست
۲۴۹	
نمونه چک‌لیست ممیزی ISO/IEC 27001:2013
۲۴۹	
منابع:
۲۶۱	

مقدمه:

علیرغم پیشرفت تکنیک‌ها و مکانیزم‌های امنیتی، بازهم شاهد انتشار اخبار نفوذ مهاجمین به شبکه‌های رایانه‌ای سازمان‌ها هستیم. ظاهراً هم‌زمان با پیشرفت‌های امنیت شبکه مهاجمین نیز از تکنیک‌های جدیدی برای حمله سیستم‌های رایانه‌ای استفاده می‌کنند. این موضوع باعث شده است که حفظ محرمانگی، صحت اطلاعات حیاتی سازمان‌ها و جلوگیری از قطع سرویس‌های ارائه‌شده توسط سازمان‌ها به یک چالش اساسی برای مدیران تبدیل شود. برای مقابله با این چالش سازمان‌ها باید به‌صورت نظام‌مند و سیستماتیک با مسئله امنیت اطلاعات برخورد کنند. راه‌حلی که برای این مسئله ارائه شده است، استقرار سیستم مدیریت امنیت اطلاعات (ISMS) در سازمان و دریافت گواهینامه مربوط به آن است. در حال حاضر محبوب‌ترین استاندارد در حوزه امنیت اطلاعات، استانداردهای خانواده ISO 27000 است که در کشور ما نیز به‌شدت در حال گسترش است. در این کتاب مجموعه استانداردهای امنیتی ISO 27000 مورد بررسی قرار می‌گیرد. در کنار این استاندارد می‌توان استانداردهای دیگری را نیز به کاربرد که متخصصین به این کار اجرای موازی استانداردها در سازمان می‌گویند. لذا در این کتاب برخی از استانداردهای دیگر نظیر استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس، استاندارد ISO/IEC 17799، گزارش فنی ISO/IEC TR 13335، استاندارد BS25999 منتشرشده توسط موسسه استاندارد انگلستان (BSI) و همچنین برخی از مستندات مهم در حوزه امنیت اطلاعات نظیر مستندات NIST SP 800-30، NIST SP 800-61 و NIST SP 800-50 و بررسی شده است. این کتاب راهنمای مناسبی برای اخذ گواهینامه ISO 27000 بوده و مرجعی برای متقاضیان شرکت در آزمون‌های مرتبط خواهد بود.

ساختار این کتاب به شرح ذیل است:

فصل اول کتاب اصول و مفاهیم پایه موردنیاز را بررسی می‌کند. در پایان این فصل حوزه‌های کنترلی ISO 27001:2013 معرفی می‌گردد.

فصل‌های دوم تا شانزدهم کتاب به بررسی ۱۴ حوزه کنترلی استاندارد ISO 27001:2013 اختصاص دارد.

از آنجاکه مدیریت ریسک‌های امنیت اطلاعات اهمیت زیادی در تأمین امنیت اطلاعات سازمان و اخذ گواهی‌نامه دارد، فصل هفدهم کتاب نیز به مدیریت ریسک اختصاص داده شده است.

در فصل هجدهم کتاب نمونه سیاست‌های امنیتی ارائه گردیده است. شکل و محتوای سیاست امنیتی ممکن است از سازمانی به سازمان دیگر متفاوت باشد و به فاکتورهای زیادی از قبیل اندازه سازمان، اهداف سازمان، میزان حساسیت اطلاعات سازمان، تعداد و انواع سیستم‌های محاسباتی و اطلاعاتی که مورداستفاده قرار می‌گیرند، بستگی دارد. بررسی در نمونه سیاست‌های امنیتی از پیش آماده و تهیه شده توسط سایر مراکز موفق، در ایجاد دید کلی از سیاست‌های امنیتی و موارد مربوط به آن‌ها کمک زیادی خواهد کرد. در نوشتن یک سیاست امنیتی می‌توان از نمونه سیاست‌های موجود استفاده کرد ولی باید همواره توجه کرد که عوامل تأثیرگذار و مرتبط سازمان باسیاست امنیتی را هم مدنظر قرار دهیم.

در فصل نوزدهم کتاب متن کامل استاندارد ISO27001:2013 ارائه گردید است. همچنین در پیوست ۱، چک‌لیست کاربردی ممیزی بر اساس الزامات و اهداف کنترلی استاندارد ISO27001 آورده شده است.

از این کتاب می‌توان به‌عنوان مرجع دروس معماری امنیت اطلاعات و مدیریت امنیت اطلاعات در رشته‌های فناوری اطلاعات و کامپیوتر استفاده نمود. در پایان هر فصل تعدادی سؤال تشریحی و چهارگزینه‌ای آورده شده است تا خوانندگان بهتر بتوانند خود را برای آزمون‌هایی که در پیش رودارند آماده نمایند. امید است این اثر مورد توجه اساتید، دانشجویان، سازمان‌های متقاضی دریافت استاندارد و همچنین ممیزین ISO 27000 قرار گیرد. از خوانندگان عزیز تقاضا دارم نقطه نظرات خود را از طریق ایمیل m.a.torkamani@gmail.com با اینجانب در میان بگذارند تا ان‌شاءالله در ویرایش‌های بعدی اشکالات یا کاستی‌های احتمالی کتاب مورد تجدیدنظر قرار گیرد. در پایان از زحمات آقای مهندس علی بیات به خاطر طراحی جلد کتاب و همچنین از مدیریت انتشارت ارسطو جناب آقای حسین قنبری تشکر و قدردانی نمایم.

محمدعلی ترکمانی

تابستان ۱۳۹۵

فصل اول

تعاریف و اصول پایه

۱-۱- تعریف امنیت اطلاعات و سیستم امن

امنیت اطلاعات عبارت است از حفاظت اطلاعات و به حداقل رساندن دسترسی غیرمجاز به اطلاعات، همچنین علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر تغییرات غیرمجاز از محرمانگی، تمامیت و دسترس‌پذیری اطلاعات. سایر ویژگی‌های دیگر امنیت اطلاعات از قبیل اصالت، اعتبار، انکارناپذیری، قابلیت جابجایی و قابلیت اطمینان اطلاعات نیز می‌تواند مشمول این حفاظت باشند.

۱-۱-۱- سیستم امن

یک سیستم امن سیستمی است که اگر حمله‌کننده به آن ورودی بد بدهد، سیستم خراب نشود. خصوصیات اصلی یک سیستم امن عبارتند از:

- **محرمانگی:** محرمانگی یعنی اطلاعات تنها توسط افرادی که تأیید صلاحیت شده‌اند، قابل دیدن باشد. به‌عنوان مثال در یک سایت دانشگاه که تنها دانشجویان و اساتید و کارمندان دانشگاه حق ورود به سایت را دارند.
- **صحت:** صحت یعنی داده‌ها نباید به‌صورت تصادفی یا عمدی تغییر داده شوند، نابود شده و یا گم شوند.

¹ Confidentiality

² Integrity

- **دسترسی‌پذیری:** هرگاه کاربر به سیستم نیاز داشت سیستم وجود داشته باشد. به‌عبارت‌دیگر سیستم باید قادر باشد هنگام درخواست کاربر، سرویس یا سرویس‌های موردنظر را ارائه دهد.

۲-۱- اصطلاحات امنیتی

۱-۲-۱- آسیب‌پذیری^۲

- آسیب‌پذیری، یک خطا یا نقص در طراحی، پیاده‌سازی یا عملیات سیستم است. آسیب‌پذیری می‌تواند در یکی از موارد زیر باشد:
- طراحی سیستم: به‌عنوان مثال طراحی پروتکل TCP/IP درست انجام‌نشده و بسته‌های TCP/IP به‌صورت متن ساده^۳ (رمز نشده) هستند.
 - پیاده‌سازی: به‌عنوان مثال در پیاده‌سازی TCP/IP با توابع C یک سری آسیب‌پذیری‌هایی دیده می‌شود که علت آن اشکالات موجود در زبان C است.
 - ایراد در عملیات سیستم: فرآیندها درست انجام نمی‌شود. به‌عنوان مثال یک فرم پرشده و باید به دست یک نفر برسد ولی به فرد دیگری می‌رسد که نباید آن را ببیند.

۲-۲-۱- حمله^۴

حمله عبارت است از بهره‌برداری از آسیب‌پذیری‌های یک سیستم.

۲-۳-۱- تهدید^۵

مجموعه‌ای از شرایط و پیشامدها که پتانسیل صدمه زدن به سیستم را دارد. فردی بدخواه که انگیزه و توانایی حمله را داشته باشد و یا یک سیستم که امکان یک حمله را فراهم می‌کند یک تهدید است.

¹ Availability
² vulnerability
³ Clear Text
⁴ Attack
⁵ Threat

۴-۲-۱- مفهوم AAA در امنیت اطلاعات

در دنیای امنیت اطلاعات به واژه مخفف AAA برخورد می‌کنیم که مخفف سه کلمه ذیل است:

- **Authentication:** تأیید هویت (احراز هویت) مکانیزمی است که هویت حقیقی افراد بر اساس آن اثبات می‌شود. احراز هویت مکانیزمی است که بر اساس آن هر موجودیت (مانند یک شخص یا یک سرویس‌دهنده بانکی) بررسی می‌کند که آیا شریک او در یک ارتباط، همان فردی است که ادعا می‌کند یا یک شخص اخلاص‌گر ثالث است که خود را به جای طرف واقعی جا زده است.
- **Authorization:** اجازه^۱ مکانیزمی است که بر اساس آن مشخص می‌شود فرد یا موجودیتی که هویت آن احراز شده، مجوز انجام چه کارها و عملیاتی را در سیستم دارد.
- **Accounting:** حسابداری مکانیزمی است که مشخص می‌کند فرد مورد نظر چه سهمی از منابع سیستمی و خدماتی را می‌برد. یعنی به‌عنوان مثال اعتبار کافی دارد یا خیر.

در میان این سه واژه، مهم‌ترین مرحله Authentication است که تأمین دو مورد دیگر را نیز بسیار ساده می‌سازد.

به‌عنوان مثال وقتی فردی می‌خواهد به سیستم دسترسی پیدا کند، ما می‌خواهیم بدانیم آیا همان فرد مورد نظر است یا خیر، تأیید هویت انجام می‌دهیم. اما اجازه، بیشتر مفهوم کنترل سطح دسترسی را می‌دهد. به‌عنوان مثال، در سیستم اینترنتی یک دانشگاه، کاربر هنگام ورود ابتدا تأیید هویت می‌شود که مشخص شود کاربری مجاز است یا خیر. در این سیستم اساتید و دانشجویان و سایر کارکنان دانشگاه مجاز به ورود هستند. اما در خصوص اجازه دسترسی، واضح است که یک دانشجو تأیید هویت شده و وارد سیستم می‌شود ولی اجازه ویرایش نمرات را ندارد.

در خصوص حسابداری نیز به این مثال توجه کنید. فرض کنید شخصی تأیید هویت می‌شود و وارد یک فروشگاه الکترونیکی می‌شود. وی اجازه خرید کردن را دارد. بنابراین

^۱Authorization

Authorization نیز با موفقیت انجام می‌شود. اما ممکن است موجودی این فرد در سایت برای خرید کردن کافی نباشد. بنابراین فرایند Accounting به وی اجازه خرید را نخواهد داد.

۳-۱- سرویس‌های امنیتی

سرویس امنیتی سرویسی است که برای ارتقاء امنیت داده مورد استفاده قرار می‌گیرد. تحقق سرویس‌های امنیتی، با استفاده از یک یا چند مکانیزم امکان‌پذیر است. سرویس‌های امنیتی سیاست‌های امنیتی را ارائه کرده و توسط مکانیزم‌های امنیتی اجرا می‌شوند. RFC 2196 سیاست امنیتی را به این شکل تعریف می‌کند:

سیاست‌های امنیتی قوانینی است که باید توسط افرادی که به فناوری‌ها و دارایی‌های اطلاعاتی سازمان شما دسترسی دارند، رعایت شود.

دو نوع سرویس امنیتی متداول وجود دارد که عبارتند از:

- سرویس امنیتی RFC2828
- سرویس امنیتی X.800

برخی از سرویس‌های امنیتی X.800 عبارتند از: احراز هویت، کنترل دسترسی، محرمانگی، جامعیت داده، عدم انکار و قابلیت دسترسی.

۴-۱- مکانیزم‌های امنیتی

مکانیزم‌های امنیتی، روش‌ها و راهکارهایی برای تشخیص و جلوگیری از حمله‌های امنیتی هستند. همان‌طور که ذکر شد سرویس‌های امنیتی توسط مکانیزم‌های امنیتی اجرا می‌شوند. برخی از مکانیزم‌های امنیتی عبارتند از:

۱. رمزنگاری: رمزنگاری نقشی کلیدی در امنیت دارد. بسیاری از نیازهای امنیتی و سرویس‌های امنیتی نظیر تأیید هویت، محرمانگی به‌وسیله رمزنگاری تأمین می‌شوند.

۲. امضای دیجیتال: این مکانیزم برای تأیید اعتبار فرستنده و صحت اطلاعات فرستاده شده به کار می‌رود.

۳. کنترل دسترسی: اجازه دستیابی به اطلاعات (خواندن و نوشتن) را فقط به افراد مجاز می‌دهد.

۴. کنترل مسیر: مسیریابی امن از هر مسیر امکان عبور مقدار مشخصی از داده را ممکن می‌سازد. در غیر این صورت یک شکاف امنیتی رخ می‌دهد. به‌طور کلی وظیفه یک الگوریتم مسیریابی خوب فقط یافتن کوتاه‌ترین مسیر نیست، بلکه الگوریتم مسیریابی باید منصف باشد و بتواند ترافیک شبکه را روی مسیرهای مختلف توزیع نماید.

۵. کنترل ترافیک: در کانال‌های ارتباطی ناامن اطلاعات به‌صورت رمز شده ارسال می‌گردد تا چنانچه مهاجم پیام‌ها را شنود کند، نتواند پیام اصلی را از داخل آن استخراج نماید. اما حمله‌کننده می‌تواند اطلاعاتی از قبیل مبدأ، مقصد و اندازه پیام‌ها را تحلیل نموده و از آن‌ها برای یافتن برخی از پیام‌ها یا تعیین کلید رمزنگاری استفاده نماید. به‌عنوان مثال در یک سیستم نظامی ممکن است دشمن حجم داده‌های ارسالی را تحلیل کرده و چنانچه در یک روز خاص حجم اطلاعات بیش‌ازاندازه معمول باشد، حدس بزنند که احتمالاً قرار است عملیاتی انجام گردد.

مکانیزم کنترل ترافیک در پیام ارسالی بیت‌هایی جاگذاری کرده تا تلاش تحلیل ترافیک را خنثی نماید.

۵-۱ - خط‌مشی‌ها یا سیاست‌های امنیتی

عناصر دخیل در سیاست‌های امنیتی در RFC 2196 لیست و ارائه شده‌اند.

GIAC Security^{۱۰} سیاست‌های امنیتی را به شرح ذیل تعریف می‌کند:

"یک سیاست امنیتی انجام اعمالی است که باید صورت بگیرد تا بتوان از اطلاعات ذخیره شده در کامپیوتر محافظت کرد." یک سیاست امنیتی مؤثر باعث ایجاد امنیت نسبی

^{۱۰}Digital Signature

^{۱۱}Access Control

^{۱۲}Routing Control

^{۱۳}Traffic Control

^{۱۴}Global Information Assurance Certification

برای کاربران می‌شود و به کاربران اجازه می‌دهد تا بتوانند بدون ترس کارهای خود را انجام دهند. یک سیاست امنیتی چیزی جز یک راهبرد برای نگهداری اطلاعات و منابع شبکه نیست. در یک سازمان سیاست‌های امنیتی مختلفی تدوین می‌گردد که برخی از آن‌ها عبارتند از:

۱-سیاست‌های کلمه عبور

۲-سیاست‌های ایمیل

۶-سیاست‌های دستیابی به اینترنت

۷-سیاست‌های پشتیبان‌گیری

۸-سیاست‌های تشخیص نفوذ

۱-۵-۱- سیاست‌های کلمه عبور

سیاست‌های کلمه عبور یکی از مسائل مهم امنیت شبکه است. وجود یک سیاست امنیتی حساب شده برای پسوندها امری ضروری است. نمونه‌ای از این سیاست‌ها به شرح ذیل است:

۱-کلمات عبور نباید شامل لغات موجود در دیکشنری باشد.

۲-حتی‌الامکان اسم شخص یا چیزی نباشد (چون معمولاً اسم اشیاء در دیکشنری وجود دارد).

۳-نام مکان خاصی نباشد.

۴-ترکیب مشخصی از کلمات روی صفحه کلید نباشد (مانند ALI123).

۵-شماره تلفن نباشد.

۶-نباید ترکیبی از موارد بالا به‌علاوه یک حرف یا رقم باشد.

۲-۵-۱- سیاست‌های اینترنتی

اینترنت مجموعه شگفت‌آوری از اطلاعات است که تنها با چند کلیک ساده می‌توان به این اطلاعات دسترسی پیدا کرد. در میان این اطلاعات ممکن است بعضی از آن‌ها حاوی مطالب غیراخلاقی باشند. لذا شما صریحاً محتاج به یک سیاست مخصوص برای استفاده از اینترنت هستید.

۳-۵-۱- پشتیبان گیری و احیای اطلاعات

در این سیاست باید موارد زیر را مدنظر قرار دهید:

- ۱- برنامه پشتیبان گیری چه زمانی باید اجرا شود و هرچند وقت یکبار اجرا شود
- ۲- چه نوع پشتیبانی باید گرفته شود (کامل، تفاضلی، افزایشی، ترکیبی)
- ۳- از چه رسانه‌ای برای ذخیره‌سازی اطلاعات باید استفاده شود (CD یا نوار مغناطیسی)

۶-۱- مفهوم سیستم مدیریت امنیت اطلاعات

ISMS یا سیستم مدیریت امنیت اطلاعات استانداردهایی را برای ایمن‌سازی فضای تبادل اطلاعات در سازمان‌ها ارائه می‌دهد. این استانداردها شامل مجموعه‌ای از دستورالعمل‌هایی است تا بتواند فضای تبادل اطلاعات یک سازمان را با اجرای یک طرح مخصوص به آن سازمان ایمن نماید. امنیت اطلاعات بخشی از سیستم مدیریت کلی و سراسری در یک سازمان است که بر پایه‌ی رویکرد مخاطرات کسب‌وکار قرار داشته و هدف آن پایه‌گذاری، پیاده‌سازی، بهره‌برداری، نظارت، بازبینی و بهبود امنیت اطلاعات است.

۷-۱- استانداردهای مدیریتی ارائه‌شده در خصوص

امنیت اطلاعات

بر اساس نگرش سیستماتیک ISMS، تأمین امنیت فضای تبادل اطلاعات سازمان‌ها، به یک‌باره مقدور نیست و لازم است این امر به صورت مداوم در یک چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح، انجام گیرد. به این منظور استانداردهای مختلفی ارائه‌شده است که متداول‌ترین و معروف‌ترین آن‌ها عبارتند از:

- استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس
- استاندارد مدیریتی ISO/IEC 17799 موسسه بین‌المللی استاندارد
- استانداردهای مدیریتی سری ۲۷۰۰۰ موسسه بین‌المللی استاندارد
- گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد
- استاندارد ISO 31000 برای مدیریت ریسک

۸-۱- استانداردهای خانواده ISO27000

در سال ۲۰۰۵ موسسه بین‌المللی استاندارد به این نتیجه رسید که یک استاندارد واحد جوابگوی نیاز جامعه جهانی برای برقراری امنیت اطلاعات در حوزه‌های مختلف نیست. از این رو اقدام به تشکیل خانواده استاندارد ISO27000 نمود که جنبه‌های مختلف این امر را پوشش می‌دهد. جدول ۱-۱ استانداردهای خانواده ISO 27000 این استانداردها را نشان می‌دهد.

جدول ۱-۱: استانداردهای خانواده ISO 27000

شماره استاندارد	شرح
۲۷۰۰۰	مقدمه و مروری بر استانداردهای خانواده ISMS به همراه تعریف واژگان رایج مورد استفاده.
۲۷۰۰۱	ارائه الزامات استاندارد به منظور احراز صلاحیت سازمان‌ها جهت اخذ گواهینامه.
۲۷۰۰۲	مجموعه‌ای از تجربیات موفق در زمینه ISMS و راهنمای تمرین اجرای ISMS
۲۷۰۰۳	راهنمای پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS)
۲۷۰۰۴	استاندارد اندازه‌گیری و تعیین سطح مدیریت امنیت اطلاعات.
۲۷۰۰۵	استاندارد مدیریت ریسک در امنیت اطلاعات.
۲۷۰۰۶	راهنمای مراحل دریافت گواهینامه.
۲۷۰۰۷	راهنمای بازرسی و نظارت بر ISMS
۲۷۰۱۱	راهنمای پیاده‌سازی ISMS در صنعت مخابرات.
۲۷۷۹۹	راهنمای پیاده‌سازی ISMS در حوزه سلامت.

۹-۱- گزارش فنی ISO/IEC TR ۱۳۳۳۵

گزارش فنی ISO/IEC TR ۱۳۳۳۵ در قالب ۵ بخش مستقل در فواصل سال‌های ۱۹۹۶ تا ۲۰۰۱ توسط موسسه بین‌المللی استاندارد (ISO) منتشر شده است.