



مؤسسه فرهنگی هنری  
دیباگران تهران



مؤسسه فرهنگی هنری  
دیباگران تهران

به نام خدا

# امنیت اطلاعات

# مبتنی بر آزمون

# CISSP

مؤلف

مهندس احمد کبیری



هرگونه چاپ و تکثیر از محتويات اين کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می‌گيرند.

# عنوان کتاب: امنیت اطلاعات مبتنی بر آزمون CISSP

سرشناسه:کبیری،احمد،۱۳۵۸-

عنوان و نام پدیدآور:امنیت اطلاعات مبتنی بر آزمون  
مولف: احمد کبیری /CISSP

مشخصات نشر: تهران: دیباگران تهران: ۱۳۹۸

مشخصات ظاهری: ۲۸۰:ص:تصور،

شایدیک: ۹۷۸-۶۲۲-۲۱۸-۱۸۴۰

و ضعیت فهرست نویسی: فیبا یادداشت:کتابنامه:ص. ۲۸۰

موضوع: کامپیوترها-ایمنی اطلاعات  
موضوع: computer security

موضوع: شبکه های کامپیوتری-تدابیر ایمنی

موضوع: computer networks-security measures

موضوع: تکنولوژی اطلاعات -تدابیر ایمنی

information technology-security measures

رده بندی کنگره: QA ۷۶/۹

رده بندی دیوبی: ۰۰۵/۸

شماره کتابشناسی ملی: ۱۶۴۵۸۵۵

- ﴿ مهندس احمد کبیری : ناشر: موسسه فرهنگی هنری دیباگران تهران

﴿ آرایی: فرنوش عبدالهی : صفحه آرایی

﴿ طراح جلد: داریوش فرسایی : طراح جلد

﴿ نوبت چاپ: اول : نوبت چاپ

﴿ تاریخ نشر: ۱۳۹۸ : تاریخ نشر

﴿ چاپ و صحافی: صدف : چاپ و صحافی

﴿ تیراز: ۱۰۰ جلد : تیراز

﴿ قیمت: ۸۵۰۰۰ ریال : قیمت

﴿ شابک: ۹۷۸-۶۲۲-۲۱۸-۱۸۴۰ : شابک

﴿ نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، روبروی پاساژ مهستان، پلاک ۱۲۵۱ : نشانی واحد فروش

﴿ تلفن: ۰۰۴۱۱۱۱۱۸۰۲۲ : تلفن

نیشانه، اینسٹاگرام دیسکاؤنٹ @mftbook

هر کتاب دیاگر از، یک فرست حدید شغلی،

هر گوشی همراه، یک فروشگاه کتاب دیاگران تهران:

ایلکشن دیگر از سایتهای اینترنتی، مادریافت و نصب نمایند.

# فهرست مطالب

۲۱	مقدمه <sup>۴</sup>
۲۱	سیستم اطلاعاتی
۲۲	سازمان بین المللی (ISC) <sup>۲</sup>
۲۲	CISSP
۲۳	برنامه آموزشی CISSP
۲۴	چه مهارت‌ها و توانایی‌هایی خواهد آموخت
۲۵	این کتاب برای چه افرادی مناسب است
۲۵	درباره این کتاب
۲۵	پیش نیاز
۲۶	فصل اول : مدیریت ریسک و امنیت
۲۷	تعريف امنیت اطلاعات
۲۷	تفاوت امنیت اطلاعات و امنیت سایبری
۲۸	مجموعه سه تابی CIA
۲۸	محرمانگی
۲۹	یکپارچگی
۲۹	دسترس پذیری
۲۹	AAA
۲۹	احراز هویت
۳۰	اجازه
۳۰	حسابداری
۳۱	عدم انکار
۳۱	عامل و شیء
۳۱	حاکمیت امنیت اطلاعات
۳۲	حاکمیت فناوری اطلاعات و حاکمیت سازمان
۳۳	تفاوت حاکمیت فناوری اطلاعات و مدیریت فناوری اطلاعات
۳۳	خط مشی
۳۴	استاندارد
۳۵	خط مبنا
۳۶	رهنمون

۳۶	روبه
۳۷	مستندسازی حاکمیت امنیت اطلاعات
۳۸	انطباق
۳۹	امنیت کارکنان
۳۹	بررسی پیشینه
۳۹	پایان استخدام
۴۰	امنیت فروشنده، مشاور و پیمانکار
۴۰	برونسپاری
۴۰	راهکارهای دفاعی
۴۱	کنترل پیشگیرانه
۴۱	کنترل تشخیصی
۴۱	کنترل اصلاحی
۴۲	کنترل بازیابی
۴۲	کنترل بازدارنده
۴۲	کنترل جبرانی
۴۳	کنترل‌های فیزیکی، فنی و مدیریتی
۴۴	استراتژی دفاع در عمق
۴۵	اخلاق کامپیوتر
۴۵	تحلیل ریسک
۴۵	دارایی‌ها
۴۶	تهدید و آسیب‌پذیری
۴۷	تاثیر
۴۷	ماتریس تحلیل ریسک
۴۹	محاسبه انتظار خسارت سالیانه
۴۹	ارزش دارایی
۴۹	ضریب درمعرض بودن
۵۰	انتظار خسارت واحد
۵۰	نرخ سالانه رخداد
۵۰	انتظار خسارات سالیانه
۵۰	مجموع هزینه مالکیت
۵۱	بازگشت سرمایه
۵۲	گرینه‌های مواجهه با ریسک
۵۲	قبول ریسک

۵۲	کاهش ریسک .....
۵۲	انتقال ریسک .....
۵۲	اجتناب از ریسک .....
۵۳	تحلیل کمی و کیفی ریسک .....
۵۳	فرآیند مدیریت ریسک .....
۵۴	انواع مهاجم ها .....
۵۴	هکرها .....
۵۴	بیگانهها .....
۵۴	خودی ها .....
۵۵	بات ها و باتنتها .....
۵۶	فیشرها و فیشرهای نیزه دار .....
<b>۵۷</b>	<b>فصل دوم : امنیت دارایی .....</b>
۵۸	طبقه بندی دادهها .....
۵۸	برچسبها .....
۵۸	مجوز رسمی .....
۵۹	تایید رسمی دسترسی .....
۵۹	نیاز به دانستن .....
۵۹	اطلاعات حساس و امنیت رسانه .....
۵۹	اطلاعات حساس .....
۵۹	دست زدن .....
۶۰	نگهداری اطلاعات .....
۶۰	مالکیت .....
۶۰	صاحبان کسب و کار و مدیران ارشد .....
۶۰	مالکان دادهها .....
۶۱	مالک سیستم .....
۶۱	متصدی .....
۶۱	کاربران .....
۶۱	کنترل کننده‌گان دادهها و پردازشگرهای دادهها .....
۶۲	ماندگاری و پاک سازی دادهها .....
۶۲	بازنویسی مجدد .....
۶۳	از بین بردن میدان مغناطیسی و تحریب .....
۶۳	تعیین کنترل‌های امنیتی .....
۶۳	تصدیق و اعتبار بخشی .....

۶۴	استانداردها و چارچوب‌های کنترل
۶۴	استانداردهای امنیت اطلاعات
۶۴	سری ISO/IEC 27000
۶۶	استاندارد PCI-DSS
۶۸	استاندارد NIST Special Publication 800-53
۶۸	چارچوب OCTAVE
۶۹	استاندارد معیارهای مشترک
۷۰	چارچوب COBIT
۷۰	چارچوب ITIL
۷۰	استاندارد ISO/IEC 20000
۷۱	تعیین محدوده و ایجاد تناسب
۷۱	حفظ از داده‌های در حال حرکت و داده‌های ساکن
۷۱	رمزگذاری درایو و نوار
۷۲	رسانه‌های ذخیره سازی و انتقال
۷۲	قانون پشتیبان‌گیری ۳-۲-۱
۷۳	محافظت از داده‌های درحال حرکت
<b>۷۴</b>	<b>فصل سوم : معماری و مهندسی امنیت</b>
۷۵	مدل‌های امنیتی
۷۵	مدل ماشین حالت
۷۶	مدل جریان اطلاعات
۷۶	مدل عدم تداخل
۷۷	مدل گرفتن-اعطا کردن
۷۸	خواندن پایین و نوشتن بالا
۷۸	مدل بل لایادولا
۷۹	کنترل دسترسی مبتنی بر شبکه
۸۰	مدل‌های یکپارچگی
۸۰	مدل بیبا
۸۱	مدل کلارک-ولیسون
۸۳	مفاهیم طراحی سیستم ایمن
۸۳	دامنه‌های امنیتی
۸۵	معماری سخت افزار ایمن
۸۵	ماژول پلتفرم قابل اطمینان
۸۵	ویژگی‌های «ممانعت از اجرای داده‌ها» و «تصادفی کردن طرح بندی فضای آدرسدهی»

۸۷	مجازی سازی و رایانش توزیع شده
۸۷	مجازی سازی
۸۷	انواع هایپروایزور
۸۸	رایانش ابری
۸۸	مدل‌های سرویس دهی رایانش ابری
۹۰	تین کلاینت
۹۰	برنامه‌های کاربردی تین کلاینت
۹۱	ایستگاه کاری بدون دیسک
۹۱	اینترنت اشیا
۹۱	آسیب پذیری سیستم، تهدیدها و اقدامات متقابل
۹۱	کانال‌های پوششی
۹۲	کانال مستقیم و کانال غیر مستقیم
۹۳	انواع کانال‌های پوششی
۹۳	مقابله با کانال‌های پوششی
۹۴	درهای پشتی
۹۵	قلاب‌های نگهداری
۹۵	روش‌های تشخیص و محافظت در برابر در پشتی
۹۶	بدافزار
۹۶	اکسلپویت
۹۶	اکسلپویت‌های روز صفر
۹۶	ویروس‌های کامپیوتری
۹۷	انواع ویروس
۹۸	کرم‌ها
۹۸	تروجان
۹۹	روت کیت
۱۰۰	بسته بند
۱۰۰	بمب‌های منطقی
۱۰۰	نرم‌افزار آنتی ویروس
۱۰۱	ابزارهای آنالیز بدافزار
۱۰۱	حمله‌های سمت سرویس دهنده
۱۰۲	حمله‌های DDoS و DoS
۱۰۳	حملات سمت سرویس گیرنده
۱۰۴	حملات وب

۱۰۴	اپلت‌ها
۱۰۴	OWASP
۱۰۵	Burp suite Pro
۱۰۵	مهندسی اجتماعی
۱۰۶	حملات وسیله قابل حمل
۱۰۷	پدآفند دستگاه قابل حمل
۱۰۷	مفاهیم رمز نگاری
۱۰۸	محرمانگی، یکپارچگی، احراز هویت و عدم انکار
۱۰۸	درهم پیچیدگی، انتشار، جایگزینی، و جایگشت
۱۰۸	استحکام رمزگذاری
۱۰۹	رمزهای تک الفبایی و چند الفبایی
۱۰۹	یای انحصاری
۱۰۹	حاکمیت پروتکل
۱۰۹	انواع رمزگذاری
۱۱۰	رمزگذاری متقارن
۱۱۰	رمزهای دنباله‌ای و قالبی
۱۱۱	DES
۱۱۳	پایه رمزنگاری
۱۱۳	TK مرحله‌ای
۱۱۳	DES سه گانه
۱۱۳	IDEA
۱۱۳	AES
۱۱۴	RC4
۱۱۴	رمزگذاری نامتقارن
۱۱۵	روش‌های نامتقارن
۱۱۵	پروتکل توافق کلید Diffie-Hellman
۱۱۶	مقایسه متقارن و نامتقارن
۱۱۶	RSA
۱۱۶	ECC
۱۱۶	توابع درهم سازی
۱۱۷	تصادم
۱۱۷	کاربردهای درهم سازی
۱۱۷	حملات رمزنگاری

۱۱۷	حمله جستجوی فرآگیر
۱۱۸	مهندسی اجتماعی
۱۱۸	متن آشکار شناخته شده
۱۱۸	کلید شناخته شده
۱۱۹	حمله متن آشکار منتخب
۱۱۹	حمله متن رمز شده منتخب
۱۲۰	حمله متن رمز شده محض
۱۲۰	حمله‌های کانال جانبی
۱۲۰	خوشه بندی کلید
۱۲۱	پیاده سازی رمزنگاری
۱۲۱	امضای دیجیتال
۱۲۲	زیر ساخت کلید عمومی
۱۲۳	مرجع صدور گواهی دیجیتال و دفتر ثبت‌نام
۱۲۳	لیست لغو گواهی
۱۲۴	انواع گواهی دیجیتال
۱۲۴	درخواست امضا گواهی
۱۲۵	مراحل ایجاد و بررسی گواهی دیجیتال
۱۲۷	حملات ممکن علیه امضا دیجیتال
۱۲۷	مدیریت کلید
۱۲۸	TLS و SSL
۱۲۹	نحوه عملکرد گواهی SSL
۱۲۹	دست تکانی SSL
۱۳۰	IPsec
۱۳۰	ESP و AH
۱۳۲	حالت تونل و انتقال
۱۳۳	IKE
۱۳۳	S/MIME
۱۳۳	VPN
۱۳۵	پنهان نگاری
۱۳۷	تنه نقش گذاری دیجیتال
۱۳۷	پدافند محیطی
۱۳۷	حصار
۱۳۷	دروازه
۱۳۸	بولارد ترافیکی

۱۳۹	چراغ.....
۱۳۹	دوربین مداربسته.....
۱۴۰	قفل.....
۱۴۲	کارت هوشمند و کارت مغناطیسی .....
۱۴۴	RFID.....
۱۴۴	دبال کردن.....
۱۴۴	تله آدم گیر و در گردان.....
۱۴۵	بازرسی اشیای غیر مجاز.....
۱۴۶	آشکارساز حرکت و هشداردهنده‌های محیطی دیگر .....
۱۴۷	درها و پنجره‌ها.....
۱۴۷	نگهبان.....
۱۴۷	مناطق محدود شده و اسکورت ها .....
۱۴۸	انتخاب، طراحی و پیکربندی سایت .....
۱۴۸	مسائل مربوط به انتخاب سایت .....
۱۴۸	مکان نگاری.....
۱۴۹	قابلیت اطمینان خدمات.....
۱۴۹	جُرم.....
۱۴۹	مسائل مربوط به طراحی و پیکربندی سایت.....
۱۴۹	علامت‌گذاری سایت .....
۱۴۹	اجاره مشترک و ساختمان‌های مجاور .....
۱۵۰	اتفاق سیم‌کشی.....
۱۵۱	دیمارک مشترک .....
۱۵۱	اتفاق سرور.....
۱۵۲	امکانات نگهداری رسانه .....
۱۵۳	پدافند سیستم.....
۱۵۳	رديابي داريabi .....
۱۵۴	کنترل‌های مربوط به پورت‌ها و گذرگاه‌های خارجی .....
۱۵۴	کنترل‌های محیطی .....
۱۵۴	الكتريسته .....
۱۵۵	محافظ نوسان برق، ups و ژنراتور.....
۱۵۵	EMI.....
۱۵۵	اتصال ارت.....
۱۵۶	HVAC.....
۱۵۹	آشکارسازهای حرارت، شعله و دود .....

۱۶۰	آموزش و آگاهی رسانی به کارکنان.....
۱۶۰	سیستم هشدار اضطراری .....
۱۶۰	آتش‌سوزی‌های ABCDK و اطفای حریق .....
۱۶۰	کلاس‌های آتش و عوامل اطفای حریق.....
۱۶۱	انواع عوامل اطفای حریق.....
۱۶۱	روش‌های محافظت در برابر آتش.....
۱۶۳	سیستم اطفای حریق اسپرینکلر .....
۱۶۴	<b>فصل چهارم : امنیت شبکه و ارتباطات</b>
۱۶۵	ناحیه امنیتی .....
۱۶۸	فایروال .....
۱۶۸	فایروال فیلتر بسته .....
۱۶۹	فایروال حالتمند .....
۱۷۰	فایروال پروکسی .....
۱۷۱	فایروال‌های مبتنی بر شبکه و میزبان .....
۱۷۲	انواع معماری فایروال .....
۱۷۲	میزبان Dual-homed .....
۱۷۳	میزبان سنگر .....
۱۷۳	میزبان نمایش داده شده .....
۱۷۴	شبکه DMZ و معماری زیرشبکه نمایش داده شده .....
۱۷۵	معماری‌های پیاده سازی فایروال .....
۱۷۷	فایروال سخت افزاری و نرم افزاری .....
۱۷۷	شبکه‌های بی‌سیم .....
۱۷۷	انتخاب محل آنتن .....
۱۷۸	روش کلی امنیت Wi-Fi .....
۱۷۸	سیستم ممانعت از نفوذ بی‌سیم .....
۱۸۱	<b>فصل پنجم : مدیریت دسترسی و هویت</b>
۱۸۲	روش‌های احراز هویت .....
۱۸۲	احراز هویت نوع ۱: چیزی که شما می‌دانید .....
۱۸۲	رمزهای عبور.....
۱۸۳	حدس زدن رمز عبور.....
۱۸۴	هش رمز عبور و شکستن رمز عبور .....
۱۸۷	احراز هویت نوع ۲: چیزی که شما دارید .....
۱۸۷	توکن پویای همگام .....

۱۸۸	توكن پویای ناهمگام
۱۸۹	احراز هویت نوع ۳: چیزی که شما هستید
۱۹۰	ثبت‌نام بیومتریک و توان عملیاتی
۱۹۰	دقت سیستم‌های بیومتریک
۱۹۱	انواع کنترل‌های بیومتریک
۱۹۱	اثر انگشت
۱۹۲	اسکن شبکیه چشم
۱۹۲	اسکن عنایی
۱۹۳	شکل هندسی دست
۱۹۳	پویایی شناسی کیبورد
۱۹۳	امضای پویا
۱۹۴	سخن‌نگاری
۱۹۴	اسکن چهره
۱۹۴	تشخیص سیاه‌رگ دست
۱۹۴	جایی که شما هستید
۱۹۴	فناوری‌های کنترل دسترسی
۱۹۵	کنترل دسترسی متمرکز
۱۹۵	کنترل دسترسی غیرمتمرکز
۱۹۵	تک ثبت نام
۱۹۶	حقوق کاربر، بررسی دسترسی و حسابرسی
۱۹۶	مدیریت هویت فدرال
۱۹۷	استاندارد SAML
۱۹۷	هویت به عنوان یک سرویس
۱۹۸	پروتکل LDAP
۱۹۸	کربروس
۱۹۸	پروتکل‌ها و چارچوب‌های کنترل دسترسی
۱۹۹	استاندارد ۸۰۲.۱X
۲۰۰	RADIUS پروتکل
۲۰۰	Diameter پروتکل
۲۰۱	TACACS+ و TACACS
۲۰۲	پروتکل‌های PAP و CHAP
۲۰۳	EAP چارچوب
۲۰۳	استانداردهای امنیتی در شبکه‌های بی‌سیم

۲۰۳	پروتکل امنیتی WEP
۲۰۴	استاندارد امنیتی WPA
۲۰۵	مدل‌های کنترل دسترسی
۲۰۵	کنترل دسترسی اختیاری
۲۰۵	کنترل دسترسی اجباری
۲۰۶	کنترل دسترسی غیراختیاری
۲۰۷	کنترل دسترسی مبتنی بر قانون
۲۰۷	کنترل دسترسی متکی بر محتوا و متکی بر موقعیت
<b>۲۰۸</b>	<b>فصل ششم : آزمون و ارزیابی امنیتی.</b>
۲۰۹	ارزیابی کنترل دسترسی
۲۰۹	آزمون نفوذ
۲۱۰	ابزارها و روش شناسی آزمون نفوذ
۲۱۳	اطمینان از محرومگی، یکپارچگی داده‌ها و یکپارچگی سیستم
۲۱۳	آزمون آسیب پذیری
۲۱۴	ممیزی امنیتی
۲۱۴	ابزارهای ممیزی امنیتی
۲۱۵	منابع مربوط به هاردینگ شبکه و سیستم‌های کامپیوتری
۲۱۶	ارزیابی امنیتی
۲۱۷	بررسی ثبت وقایع
۲۱۷	روش‌های آزمون نرم‌افزار
۲۱۷	آزمون‌های ایستا و پویا
۲۱۸	ماتریس ردیابی
۲۱۸	تراکنش‌های مصنوعی
۲۱۸	فازینگ
۲۱۹	آزمون ترکیبی نرم‌افزار
<b>۲۲۰</b>	<b>فصل هفتم : عملیات امنیتی</b>
۲۲۱	امنیت اداری
۲۲۱	کنترل‌های اداری پرسنل
۲۲۱	کمترین امتیاز
۲۲۱	تفکیک وظایف
۲۲۱	چرخش وظایف
۲۲۲	ترک اجباری یا تعطیلات اجباری
۲۲۲	تواافقنامه عدم افشا

۲۲۲	بررسی پیشینه
۲۲۲	جرائم شناسی
۲۲۳	تحلیل جرم شناسی رسانه
۲۲۳	جرائم شناسی شبکه
۲۲۳	مدیریت واکنش به حادثه
۲۲۴	روش شناسی
۲۲۴	آماده سازی
۲۲۵	تشخیص
۲۲۶	واکنش
۲۲۶	کاهش
۲۲۶	گزارش نویسی
۲۲۷	بازیابی
۲۲۷	بازسازی
۲۲۷	درس‌های آموخته شده
۲۲۸	تحلیل علت ریشه‌ای
۲۲۹	کنترل‌های عملیاتی پیشگیرانه و تشخیصی
۲۲۹	سیستم‌های تشخیص نفوذ و سیستم‌های ممانعت از نفوذ
۲۳۱	انواع رویدادها در سیستم‌های تشخیص نفوذ
۲۳۲	سیستم تشخیص و ممانعت از نفوذ مبتنی بر شبکه
۲۳۳	SPAN
۲۳۴	سیستم تشخیص و ممانعت از نفوذ مبتنی بر میزبان
۲۳۴	Network tap
۲۳۴	SWG
۲۳۵	WAF
۲۳۵	UTM
۲۳۵	NGFW
۲۳۵	SIEM
۲۳۶	ممانعت از نشت داده‌ها
۲۳۷	امنیت نقطه پایانی
۲۳۸	آنٹی ویروس
۲۳۸	ایجاد لیست سفید برنامه کاربردی
۲۳۸	جعبه شنی
۲۳۹	کنترل‌های رسانه جداسدنی
۲۳۹	رمزگذاری دیسک

۲۳۹	های پات.....
۲۴۰	های نت.....
۲۴۱	مدیریت دارایی .....
۲۴۱	مدیریت پیکربندی .....
۲۴۲	اعمال خط مبنا.....
۲۴۲	مدیریت آسیب پذیری.....
۲۴۳	مدیریت تغییر .....
۲۴۴	تداوم عملیات.....
۲۴۴	تواافقنامه سطح خدمات .....
۲۴۴	تحمل خرابی.....
۲۴۴	RAID.....
۲۴۹	دسترس پذیری بالا و افزونگی .....
۲۵۰	فرآیند BCP و DRP .....
۲۵۰	برنامه ریزی تداوم کسب و کار .....
۲۵۰	برنامه ریزی بازیابی از فاجعه .....
۲۵۰	رابطه بین DRP و BCP .....
۲۵۱	رخدادهای مخرب .....
۲۵۲	فرآیند بازیابی از فاجعه .....
۲۵۲	واکنش .....
۲۵۲	فعال کردن تیم .....
۲۵۲	برقراری ارتباط .....
۲۵۲	ارزیابی .....
۲۵۳	بازسازی .....
۲۵۳	ایجاد BCP/DRP .....
۲۵۴	آماده سازی پروژه .....
۲۵۴	ارزیابی وضعیت بحرانی .....
۲۵۵	تحلیل تاثیر بر کسب و کار .....
۲۵۵	شناسایی دارایی های حیاتی .....
۲۵۶	ارزیابی ریسک متمرکز بر BCP/DRP .....
۲۵۶	تعیین حداقل زمان از کار افتادگی قابل قبول .....
۲۵۶	معیارهای خرابی و بازیابی .....
۲۵۸	شناسایی کنترل های پیشگیرانه .....
۲۵۸	استراتژی بازیابی .....

۲۵۹	سایت افزونه.....
۲۵۹	سایت داغ.....
۲۵۹	سایت گرم.....
۲۶۰	سایت سرد.....
۲۶۰	توافقنامه متقابل.....
۲۶۰	سایت سیار.....
۲۶۰	سطح مرکز داده.....
۲۶۲	برنامه های مرتبط با BCP.....
۲۶۳	برنامه تداوم عملیات.....
۲۶۴	برنامه بازیابی کسب و کار.....
۲۶۴	برنامه تداوم پشتیبانی.....
۲۶۴	برنامه واکنش به حادثه سایبری.....
۲۶۴	برنامه اضطراری استقرار.....
۲۶۴	برنامه مدیریت بحران.....
۲۶۴	برنامه ارتباطات بحرانی.....
۲۶۵	درخت تماس.....
۲۶۵	مرکز عملیات اضطراری.....
۲۶۶	پشتیبان گیری و دسترس پذیری.....
۲۶۶	نسخه چاپی داده ها.....
۲۶۶	پشتیبان های الکترونیکی.....
۲۶۶	پشتیبان گیری کامل.....
۲۶۶	پشتیبان گیری افراشی.....
۲۶۷	پشتیبان گیری تفاصیلی.....
۲۶۷	روش های گردش نوار.....
۲۶۷	پرش الکترونیکی.....
۲۶۸	ژورنالینگ راه دور.....
۲۶۸	سایه انداختن پایگاه داده.....
۲۶۹	گزینه های دسترس پذیری بالا.....
۲۶۹	آزمون، آموزش و آگاهی رسانی DRP.....
۲۶۹	آزمون DRP.....
۲۶۹	بازبینی DRP.....
۲۷۰	خواندن.....
۲۷۰	گام به گام.....

۲۷۰	شبیه سازی یا تمرین گام به گام
۲۷۰	پردازش موازی
۲۷۱	وقفه کامل و یا بخشی از کسبوکار
۲۷۱	نگهداری مدام BCP/DRP
۲۷۱	مدیریت تغییر
۲۷۱	اشتباهات متدالو در BCP و DRP
۲۷۲	چارچوب های مخصوص BCP/DRP
۲۷۲	NIST sp800-34
۲۷۲	ISO/IEC-27031
۲۷۲	BS-25999 and ISO22301
۲۷۳	BCI
<b>۲۷۴</b>	<b>فصل هشتم : امنیت توسعه نرم افزار</b>
۲۷۵	ارزیابی کارایی امنیت نرم افزار
۲۷۵	آسیب پذیری های نرم افزار
۲۷۵	انواع آسیب پذیری های نرم افزار
۲۷۷	مدل تکامل قابلیت نرم افزار
۲۷۷	انواع ابزارهای آزمون آسیب پذیری نرم افزار
۲۷۸	آزمون پذیرش
۲۷۹	نرم افزار تجاری آماده استفاده
۲۷۹	محصولات سفارشی ایجاد شده شخص ثالث
<b>۲۸۰</b>	<b> منابع</b>

## مقدمه ناشر

# خط میشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب های است که بتواند خواسته های بر روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد. هر کتاب دیباگران تهران، یک فرصت جدید شغلی

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گامهایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید. در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرستل ورزیده و ماهر در زمینه امور نشر در صدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُربار، معترض و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت "مهندس احمد کبیری" و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

### کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانشپژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران  
bookmarket@mft.info

## ❖ پیشگفتار ❖

زمانی که سازمان‌ها متوجه منافع بسیار استفاده از فناوری اطلاعات شدند و کارهای خود را تا حد ممکن به آن سپردهند و آن هنگام که عرضه کنندگان فناوری اطلاعات مشغول شگفتی کاربران خود بودند، گویا همگی مانند دیدن کودکی نوپا فقط از دیدن آن لذت می‌برند. ولی زمانی که استفاده از این فناوری تار و پود منافع جامعه و سازمان‌ها را شکل می‌داد، امنیت اطلاعات به یکباره تبدیل به حرف اول در این دنیای مدرن گردید. تجربه‌های ویرانگر ناشی از ضعف در امنیت اطلاعات به سازمان‌ها نشان داد که کارایی، خدمات و امکانات یک محصول، فناوری یا یک سیستم اطلاعاتی بدون در نظر گرفتن همه جانبه امنیت می‌تواند خسارت‌های بزرگی به کسب‌وکار سازمان‌ها تحمیل نماید تا جایی که جبران آن بسیار سخت یا حتی غیر ممکن گردد.

استفاده از فناوری اطلاعات یک شمشیر دو لبه است. آیا می‌خواهید از منافع بی‌انتهای آن استفاده کنید و یا اینکه به کسب‌وکار و دارایی‌های خود آسیب برسانید، در هر صورت انتخاب آن با خود شماست و به این شکل که برای امنیت اطلاعات خود چه قدر اهمیت داده اید. اگر می‌خواهید بدانید که چه مقدار اهمیت داده اید، به این فکر کنید که برای طراحی، پیاده‌سازی، مدیریت و نگهداری امنیت اطلاعات خود چه قدر هزینه کرده اید، منظورم هزینه‌های مادی و معنوی است. چه تعداد از کارشناسان شما به طور ویژه بر روی امنیت اطلاعات کار می‌کنند و چه قدر خروجی آنها و پیشنهادهای آنها مورد توجه شما و سازمان است. امنیت اطلاعات به معنی امنیت تمامی دارایی‌های مرتبط با اطلاعات است و تخصص در حوزه امنیت اطلاعات مستلزم دانشی فراگیر و عمیق در حوزه فناوری اطلاعات بوده و با وجود ده‌ها زیرشاخه در حوزه امنیت اطلاعات، تصور و ادعای کامل بودن یک فرد در این حوزه مضحک به نظر می‌رسد. در هر صورت باید در یک سازمان چندین متخصص امنیت با گرایش‌ها و مهارت‌های متفاوت در کنار هم کار کنند تا امنیت معقولی را برای سازمان تأمین نمایند.

من بیش از بیست و دو سال است که عمر خود را وقف پژوهش و کار در حوزه فناوری اطلاعات کرده ام و فکر می‌کنم کتاب حاضر خواننده را پنج سال به جلو می‌برد! یعنی اگر شما بخواهید به دانش و از آن مهم‌تر به بینشی از امنیت اطلاعات برسید که در این کتاب به آن دست خواهید یافت، باید پنج سال پژوهش نموده و تجربه کسب نمایید. CISSP به دلیل جامع بودن و سطح بالای بینشی که ارائه می‌دهد، فوق العاده است. این کتاب بر اساس جدیدترین آزمون CISSP استاندارد شده و نهایت دقیقت در آن لحاظ شده است، البته سعی بر آن بوده که بر مطالب کاربردی تاکید شده و به طور کلی، مطالب به صورت فشرده بیان شوند. این کتاب اولین منبع CISSP به زبان فارسی است و برای تالیف آن از دو کتاب cissp official study guide Eighth Edition و Guide Third Edition بهره بسیار برده شده و البته مطالب چندین کتاب دیگر و همچنین

تجربیات بنده در حوزه شبکه و امنیت اطلاعات در سازمان‌های بزرگ در آن لحاظ شده است. اگر پیشنهادی داشتید پذیرا خواهم بود.

شاد و پیروز باشد

احمد کبیری

تابستان ۱۳۹۸

[ad.kabiri@gmail.com](mailto:ad.kabiri@gmail.com)