

حسابرس رسمی

سیستم‌های اطلاعاتی

ویراست بیست و هفتم

نویسنده:

انجمن کنترل و ممیزی سیستم‌های اطلاعاتی (ISACA)

مترجمان:

دکتر علی رحمانی

(عضو هیئت علمی دانشگاه الزهرا)

دکتر رامین مولاناپور

دکتر آمنه خدیور

(عضو هیئت علمی دانشگاه الزهرا)

حسابرس رسمی سیستم‌های اطلاعاتی

مترجمان: دکتر علی رحمانی، دکتر رامین مولاناپور، دکتر آمنه خدیور

ناشر: انتشارات آتی‌نگر

مدیر هنری و طراح جلد: همتا بیداریان

چاپ اول، ۱۴۰۳

شمارگان: ۱۰۰۰ نسخه

قیمت: ۸,۰۰۰,۰۰۰ ریال

شابک: ۹۷۸-۶۲۲-۸۲۴۵-۲۳-۲

ISBN: 978-622-8245-23-2

حق چاپ برای انتشارات آتی‌نگر محفوظ است.

آدرس دفتر فروش: خیابان جمالزاده جنوبی، روبه‌روی کوچه رشتچی، پلاک ۱۴۴، واحد ۱

تلفن: ۸-۶۶۵۶۵۳۳۶ نمابر: ۶۶۵۶۵۳۳۷

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



سرشناسه: انجمن کنترل و ممیزی سیستم‌های اطلاعاتی - Information Systems Audit and Control Association

حسابرس رسمی سیستم‌های اطلاعاتی / مترجمان: دکتر علی رحمانی، دکتر رامین مولاناپور، دکتر آمنه خدیور

تهران: آتی‌نگر، ۱۴۰۳

۶۱۶ ص: مصور، جدول، نمودار.

ISBN: 978-622-8245-23-2

فیپا.

عنوان اصلی کتاب: CISA review manual, 27th Edition, 2019.

موضوع: انجمن کنترل و ممیزی سیستم‌های اطلاعاتی -- آزمون‌ها -- راهنمای مطالعه

موضوع: Study guides Information Systems Audit and Control Association -- Examinations

موضوع: داده‌پرداززی -- کارمندان -- گواهی و گواهی‌نامه‌ها -- راهنمای مطالعه

موضوع: Electronic data processing personnel -- Certification -- Study guides

موضوع: حسابرسی -- آزمون‌ها -- راهنمای مطالعه - Study guides Auditing -- Examinations

شناسه افزوده: رحمانی، علی، ۱۳۴۶ - مترجم

شناسه افزوده: مولاناپور، رامین، ۱۳۵۲ - مترجم

شناسه افزوده: خدیور، آمنه، ۱۳۶۰ - مترجم

شناسه افزوده: بیداریان، همتا، ۱۳۶۱ - مدیر هنری

رده‌بندی کنگره

QA۷۶/۳

رده‌بندی دیویی

۰۰۵/۷۱۳۷۶

شماره کتابشناسی ملی

۹۶۰۰۷۴۵

فهرست مطالب

پیشگفتار.....	۱۳
درباره این کتاب راهنما.....	۱۵
فصل ۱: فرایند حسابرسی سیستم اطلاعاتی.....	۲۱
بررسی اجمالی	۲۱
طرح کلی محتوای آزمون حوزه‌ی ۱	۲۱
بخش الف: برنامه‌ریزی	۲۱
بخش ب: اجرا.....	۲۱
اهداف یادگیری/شرح وظایف	۲۲
منابع پیشنهادی برای مطالعه بیشتر	۲۲
سؤالات خودارزیابی	۲۲
پاسخ به سؤالات خودارزیابی.....	۲۴
بخش الف: برنامه‌ریزی.....	۲۷
۱-۰ مقدمه	۲۷
۱-۱ استانداردهای حسابرسی، دستورعمل‌ها و کدهای اخلاقی سیستم‌های اطلاعاتی.....	۲۸
۱-۱-۱ استانداردهای حسابرسی و تضمین سیستم‌های اطلاعاتی انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی.....	۲۸
۱-۱-۲ دستورعمل‌های حسابرسی و اطمینان سیستم اطلاعاتی انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی.....	۲۹
۱-۱-۳ کد اخلاق حرفه‌ای انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی.....	۲۹
۱-۱-۴ ITAFTM	۳۰
۱-۲ فرایندهای کسب‌وکار.....	۳۰
۱-۲-۱ عملکرد حسابرسی داخلی سیستم اطلاعاتی	۳۰
۱-۲-۲ مدیریت عملکرد حسابرسی سیستم اطلاعاتی	۳۱
۱-۲-۳ برنامه‌ریزی حسابرسی.....	۳۱
۱-۲-۴ تأثیر قوانین و مقررات بر برنامه‌ریزی حسابرسی سیستم‌های اطلاعاتی.....	۳۳
۱-۲-۵ کاربردها و کنترل‌های فرایند کسب‌وکار.....	۳۴
۱-۲-۶ استفاده از خدمات دیگر حساب‌رسان و کارشناسان.....	۵۷
۱-۳ انواع کنترل‌ها.....	۵۸
۱-۳-۱ اهداف کنترل و مقیاس‌های آن	۶۰
۱-۳-۲ ارزیابی محیط کنترل	۶۱
۱-۳-۳ کنترل‌های عمومی	۶۲
۱-۳-۴ کنترل‌های خاص سیستم‌های اطلاعاتی.....	۶۲
۱-۴ برنامه‌ریزی حسابرسی مبتنی بر ریسک.....	۶۳
۱-۴-۱ ریسک حسابرسی و اهمیت	۶۴

۶۵.....	۱-۴-۲ ارزیابی ریسک
۶۶.....	۱-۴-۳ تکنیک‌های ارزیابی ریسک حسابرسی سیستم‌های اطلاعاتی.....
۶۸.....	۱-۴-۴ تحلیل ریسک
۶۹.....	۱-۵ انواع حسابرسی و ارزیابی
۷۱.....	بخش ب: اجرا.....
۷۱.....	۱-۶ مدیریت پروژه حسابرسی
۷۱.....	۱-۶-۱ اهداف حسابرسی
۷۲.....	۱-۶-۲ فازهای حسابرسی.....
۷۲.....	۱-۶-۳ برنامه‌های حسابرسی
۷۵.....	۱-۶-۴ گزارش‌های گروه تحقیق حسابرسی.....
۷۵.....	۱-۶-۵ تقلب، بی‌نظمی و اقدامات غیرقانونی.....
۷۶.....	۱-۷ روش نمونه‌گیری
۷۶.....	۱-۷-۱ آزمون انطباق در مقایسه با آزمون اساسی
۷۷.....	۱-۷-۲ نمونه‌گیری
۷۹.....	۱-۸ تکنیک جمع‌آوری مدرک حسابرسی
۸۲.....	۱-۸-۱ مصاحبه و مشاهده کارکنان در انجام وظایفشان
۸۳.....	۱-۹ تحلیل‌گری داده‌ها.....
۸۴.....	۱-۹-۱ تکنیک‌های حسابرسی به کمک کامپیوتر.....
۸۶.....	۱-۹-۲ پایش و حسابرسی مستمر.....
۸۷.....	۱-۹-۳ تکنیک‌های حسابرسی مستمر
۸۹.....	۱-۱۰ تکنیک‌های گزارش‌گیری و ارتباط
۸۹.....	۱-۱۰-۱ نتایج حسابرسی ارتباطی.....
۸۹.....	۱-۱۰-۲ اهداف گزارش حسابرسی
۹۰.....	۱-۱۰-۳ مفهوم و ساختار گزارش حسابرسی
۹۱.....	۱-۱۰-۴ مستندات حسابرسی.....
۹۲.....	۱-۱۰-۵ فعالیت‌های پیگیری.....
۹۳.....	۱-۱۰-۶ انواع گزارش‌های حسابرسی سیستم‌های اطلاعاتی
۹۳.....	۱-۱۱ تضمین کیفیت و بهبود فرایند حسابرسی.....
۹۴.....	۱-۱۱-۱ خودآزمایی کنترل
۹۵.....	۱-۱۱-۲ حسابرسی یکپارچه
۹۷.....	مطالعه‌ی موردی.....
۹۹.....	پاسخ به سؤالات مطالعه‌ی موردی

فصل ۲: حاکمیت و مدیریت فناوری اطلاعات..... ۱۰۱

۱۰۱.....	بررسی اجمالی
۱۰۱.....	مرور اجمالی محتوای آزمون حوزه ۲.....
۱۰۱.....	اهداف آموزش/بیانیه‌های وظیفه.....
۱۰۲.....	منابع پیشنهادی برای مطالعات بیشتر.....
۱۰۲.....	سؤالات خودآزمایی

پاسخ سؤالات خودآزمایی.....	۱۰۴
بخش الف: حاکمیت فناوری اطلاعات.....	۱۰۷
۲-۰ مقدمه.....	۱۰۷
۲-۱ حاکمیت فناوری اطلاعات و راهبرد فناوری اطلاعات.....	۱۰۷
۲-۱-۱ حاکمیت بنگاهی اطلاعات و فناوری.....	۱۰۷
۲-۱-۲ شیوه‌های خوب برای حاکمیت بنگاهی اطلاعات و فناوری.....	۱۰۹
۲-۱-۳ نقش حسابرسی در حاکمیت بنگاهی اطلاعات و فناوری.....	۱۱۰
۲-۱-۴ حاکمیت امنیت اطلاعات.....	۱۱۰
۲-۱-۵ راهبرد سیستم‌های اطلاعاتی.....	۱۱۳
۲-۱-۶ برنامه‌ریزی راهبردی.....	۱۱۳
۲-۱-۷ هوشمندی کسب‌وکار.....	۱۱۴
۲-۲ چارچوب‌های مرتبط با فناوری اطلاعات.....	۱۱۷
۲-۳ استانداردها، سیاست‌ها و رویه‌های فناوری اطلاعات.....	۱۱۸
۲-۳-۱ استانداردها.....	۱۱۸
۲-۳-۲ سیاست‌ها.....	۱۱۹
۲-۳-۳ رویه‌ها.....	۱۲۱
۲-۳-۴ دستورعمل‌ها.....	۱۲۲
۲-۴ ساختار سازمانی.....	۱۲۲
۲-۴-۱ کمیته‌های حاکمیت فناوری اطلاعات.....	۱۲۲
۲-۴-۲ نقش‌ها و مسئولیت‌های مدیریت ارشد و هیئت مدیره.....	۱۲۳
۲-۴-۳ مسئولیت‌ها و ساختار سازمانی فناوری اطلاعات.....	۱۲۷
۲-۴-۴ تفکیک وظایف در فناوری اطلاعات.....	۱۳۳
۲-۴-۵ حسابرسی و پیاده‌سازی ساختار حاکمیت فناوری اطلاعات.....	۱۳۷
۲-۵ معماری سازمانی.....	۱۳۸
۲-۶ مدیریت ریسک سازمانی.....	۱۳۹
۲-۶-۱ توسعه برنامه مدیریت ریسک.....	۱۳۹
۲-۶-۲ فرایند مدیریت ریسک.....	۱۴۰
۲-۶-۳ روش‌های تحلیل ریسک.....	۱۴۲
۲-۷ مدل‌های بلوغ.....	۱۴۳
۲-۷-۱ ادغام مدل بلوغ قابلیت.....	۱۴۴
۲-۷-۲ مدل شروع، تشخیص، ایجاد، اقدام و یادگیری (IDEAL).....	۱۴۵
۲-۸ قوانین، مقررات و استانداردهای صنعت مؤثر بر سازمان.....	۱۴۵
۲-۸-۱ حاکمیت، ریسک و انطباق.....	۱۴۵
۲-۸-۲ تأثیر قوانین، مقررات و استانداردهای صنعت بر حسابرسی سیستم اطلاعاتی.....	۱۴۵
بخش ب: مدیریت فناوری اطلاعات.....	۱۴۷
۲-۹ مدیریت منابع فناوری اطلاعات.....	۱۴۷
۲-۹-۱ ارزش فناوری اطلاعات.....	۱۴۷
۲-۹-۲ پیاده‌سازی مدیریت پورتفوی فناوری اطلاعات.....	۱۴۷
۲-۹-۳ شیوه‌های مدیریت فناوری اطلاعات.....	۱۴۸
۲-۹-۴ مدیریت منابع انسانی.....	۱۴۸

۱۵۲	۲-۹-۵ مدیریت تغییر سازمانی
۱۵۲	۲-۹-۶ شیوه‌های مدیریت مالی
۱۵۳	۲-۹-۷ مدیریت امنیت اطلاعات
۱۵۳	۲-۱۰ اکتساب و مدیریت ارائه‌دهنده خدمات فناوری اطلاعات
۱۵۴	۲-۱۰-۱ شیوه‌ها و راهبردهای برون‌سپاری
۱۵۸	۲-۱۰-۲ برون‌سپاری و گزارش‌های حسابرسی شخص ثالث
۱۵۹	۲-۱۰-۳ حکمرانی ابری
۱۵۹	۲-۱۰-۴ حاکمیت در برون‌سپاری
۱۶۰	۲-۱۰-۵ برنامه‌ریزی ظرفیت و رشد
۱۶۱	۲-۱۰-۶ مدیریت تحویل خدمات شخص ثالث
۱۶۱	۲-۱۰-۷ پایش و بازبینی خدمات شخص ثالث
۱۶۱	۲-۱۰-۸ مدیریت تغییرات در خدمات شخص ثالث
۱۶۲	۲-۱۱ پایش و گزارش‌دهی عملکرد فناوری اطلاعات
۱۶۳	۲-۱۱-۱ بهینه‌سازی عملکرد
۱۶۴	۲-۱۱-۲ ابزارها و تکنیک‌ها
۱۶۷	۲-۱۲ تضمین کیفیت و مدیریت کیفیت فناوری اطلاعات
۱۶۷	۲-۱۲-۱ تضمین کیفیت
۱۶۸	۲-۱۲-۲ مدیریت کیفیت
۱۶۸	مطالعه موردی
۱۷۰	پاسخ به سؤالات مطالعه موردی

فصل ۳: اکتساب، توسعه و پیاده‌سازی سیستم‌های اطلاعاتی..... ۱۷۳

۱۷۳	بررسی اجمالی
۱۷۳	طرح کلی محتوای آزمون حوزه ۳
۱۷۳	اهداف یادگیری/دستور وظایف
۱۷۴	منابع پیشنهادی برای مطالعه بیشتر
۱۷۴	سؤالات خودارزیابی
۱۷۶	پاسخ به سؤالات خودارزیابی
۱۷۹	بخش الف: اکتساب و توسعه سیستم‌های اطلاعاتی
۱۷۹	۳-۰ مقدمه
۱۷۹	۳-۱ حاکمیت و مدیریت پروژه
۱۸۰	۳-۱-۱ شیوه‌های مدیریت پروژه
۱۸۰	۳-۱-۲ ساختار مدیریت پروژه
۱۸۱	۳-۱-۳ نقش‌ها و مسئولیت‌های مدیریت پروژه
۱۸۳	۳-۱-۴ تکنیک‌های مدیریت پروژه
۱۸۴	۳-۱-۵ مدیریت پورتفو/برنامه
۱۸۴	۳-۱-۶ دفتر مدیریت پروژه
۱۸۵	۳-۱-۷ تحقق مزایای پروژه
۱۸۷	۳-۱-۸ شروع پروژه

۱۸۸.....	۳-۱-۹ اهداف پروژه.....
۱۸۹.....	۳-۱-۱۰ برنامه‌ریزی پروژه.....
۱۹۵.....	۳-۱-۱۱ پیاده‌سازی پروژه.....
۱۹۵.....	۳-۱-۱۲ کنترل و پایش پروژه.....
۱۹۶.....	۳-۱-۱۳ پایان پروژه.....
۱۹۶.....	۳-۱-۱۴ نقش حسابرس سیستم اطلاعاتی در مدیریت پروژه.....
۱۹۷.....	۳-۲ طرح توجیهی و تحلیل امکان‌سنجی.....
۱۹۸.....	۳-۲-۱ نقش حسابرس سیستم اطلاعاتی در توسعه طرح توجیهی.....
۱۹۹.....	۳-۳ متدولوژی‌های توسعه سیستم.....
۱۹۹.....	۳-۳-۱ توسعه برنامه کاربردی کسب‌وکار.....
۲۰۰.....	۳-۳-۲ مدل‌های SDLC.....
۲۰۲.....	۳-۳-۳ فازهای SDLC.....
۲۱۳.....	۳-۳-۴ نقش حسابرس سیستم اطلاعاتی در مدیریت پروژه SDLC.....
۲۱۳.....	۳-۳-۵ روش‌های توسعه نرم‌افزار.....
۲۲۳.....	۳-۳-۶ ابزارهای توسعه سیستم و کمک‌های بهره‌وری.....
۲۲۵.....	۳-۳-۷ شیوه‌های توسعه/اکتساب زیرساخت.....
۲۳۰.....	۳-۳-۸ اکتساب سخت‌افزار/نرم‌افزار.....
۲۳۳.....	۳-۳-۹ اکتساب نرم‌افزار سیستم.....
۲۳۷.....	۳-۴ شناسایی و طراحی کنترل.....
۲۳۷.....	۳-۴-۱ کنترل‌های ورودی/مبدأ.....
۲۴۰.....	۳-۴-۲ رویه‌ها و کنترل‌های پردازش.....
۲۴۴.....	۳-۴-۳ کنترل‌های خروجی.....
۲۴۵.....	۳-۴-۴ کنترل‌های برنامه کاربردی.....
۲۴۷.....	۳-۴-۵ رویه‌های کاربر.....
۲۴۸.....	۳-۴-۶ سیستم تصمیم‌یار.....
۲۵۱.....	بخش ب: پیاده‌سازی سیستم‌های اطلاعاتی.....
۲۵۱.....	۳-۵ متدولوژی‌های آزمون.....
۲۵۱.....	۳-۵-۱ طبقه‌بندی آزمون.....
۲۵۲.....	۳-۵-۲ آزمون نرم‌افزار.....
۲۵۵.....	۳-۵-۳ آزمون جامعیت داده‌ها.....
۲۵۵.....	۳-۵-۴ آزمون سیستم‌های برنامه کاربردی.....
۲۵۸.....	۳-۵-۵ نقش حسابرس در آزمون سیستم‌های اطلاعاتی.....
۲۵۸.....	۳-۶ پیکربندی و مدیریت عرضه.....
۲۵۹.....	۳-۷ انتقال سیستم، استقرار زیرساخت و تبدیل داده.....
۲۶۰.....	۳-۷-۱ مهاجرت داده‌ها.....
۲۶۱.....	۳-۷-۲ تکنیک‌های تغییر (عملیاتی شدن یا گذار).....
۲۶۵.....	۳-۷-۳ پیاده‌سازی سیستم.....
۲۶۷.....	۳-۷-۴ رویه‌های تغییر سیستم و فرایند مهاجرت برنامه‌ها.....
۲۶۸.....	۳-۷-۵ پیاده‌سازی نرم‌افزار سیستم.....
۲۶۸.....	۳-۷-۶ صدور گواهی‌نامه/اعتبارنامه.....

۳-۸	بازبینی پس از پیاده‌سازی.....	۲۶۹
۳-۸-۱	نقش حسابرس در بازبینی پس از پیاده‌سازی.....	۲۷۰
	پاسخ به سؤالات مطالعه موردی.....	۲۷۳

فصل ۴: عملیات سیستم‌های اطلاعاتی و تاب‌آوری کسب‌وکار ۲۷۵

	بررسی اجمالی.....	۲۷۵
	طرح کلی محتوای آزمون حوزه ۴.....	۲۷۵
	بخش الف: عملیات سیستم‌های اطلاعاتی.....	۲۷۵
	بخش ب: تاب‌آوری کسب‌وکار.....	۲۷۵
	اهداف یادگیری/شرح وظایف.....	۲۷۶
	منابع پیشنهادی برای مطالعه بیشتر.....	۲۷۶
	سؤالات خودارزیابی.....	۲۷۶
	پاسخ به سؤالات خودارزیابی.....	۲۷۸
	بخش الف: عملیات سیستم‌های اطلاعاتی.....	۲۸۱
۴-۰	مقدمه.....	۲۸۱
۴-۱	مؤلفه‌های فناوری رایج.....	۲۸۱
۴-۱-۱	مؤلفه‌ها و معماری‌های سخت‌افزار کامپیوتر.....	۲۸۱
۴-۱-۲	دستگاه‌های بک‌اند سازمانی رایج.....	۲۸۳
۴-۱-۳	گذرگاه سریال عمومی.....	۲۸۴
۴-۱-۴	شناسایی فرکانس رادیویی.....	۲۸۶
۴-۱-۵	برنامه نگهداری سخت‌افزار.....	۲۸۸
۴-۱-۶	بازبینی‌های سخت‌افزاری.....	۲۸۹
۴-۲	مدیریت دارایی فناوری اطلاعات.....	۲۹۰
۴-۳	اتوماسیون زمان‌بندی کار و فرایند تولید.....	۲۹۱
۴-۳-۱	نرم‌افزار زمان‌بندی کار.....	۲۹۱
۴-۳-۲	زمان‌بندی بازبینی‌ها.....	۲۹۱
۴-۴	رابط‌های سیستم.....	۲۹۳
۴-۴-۱	ریسک مربوط به رابط‌های سیستم.....	۲۹۴
۴-۴-۲	معضلات امنیتی در رابط‌های سیستم.....	۲۹۴
۴-۴-۳	کنترل‌های مرتبط با رابط‌های سیستم.....	۲۹۴
۴-۵	رایانش کاربر نهایی.....	۲۹۵
۴-۶	حکمرانی داده.....	۲۹۶
۴-۶-۱	مدیریت داده.....	۲۹۶
۴-۶-۲	چرخه حیات داده.....	۲۹۶
۴-۷	مدیریت عملکرد سیستم.....	۲۹۸
۴-۷-۱	معماری و نرم‌افزار سیستم اطلاعاتی.....	۲۹۸
۴-۷-۲	سیستم عامل.....	۲۹۹
۴-۷-۳	نرم‌افزار کنترل دسترسی.....	۳۰۳
۴-۷-۴	نرم‌افزار ارتباطات داده.....	۳۰۳
۴-۷-۵	برنامه‌های سودمند.....	۳۰۴

۳۰۵.....	۴-۷-۶ معضلات مجوز نرم افزار
۳۰۶.....	۴-۷-۷ مدیریت کد منبع
۳۰۷.....	۴-۷-۸ مدیریت ظرفیت
۳۰۹.....	۴-۸ مدیریت مشکل و حادثه
۳۰۹.....	۴-۸-۱ مدیریت مشکل
۳۱۰.....	۴-۸-۲ فرایند مدیریت حادثه
۳۱۰.....	۴-۸-۳ تشخیص، مستندسازی، کنترل، حل و گزارش شرایط غیرعادی
۳۱۱.....	۴-۸-۴ پشتیبانی/میز راهنما
۳۱۲.....	۴-۸-۵ ابزارهای مدیریت شبکه
۳۱۳.....	۴-۸-۶ بازبینی های گزارش مدیریت مشکل
۳۱۳.....	۴-۹ تغییر، پیکربندی، عرضه و مدیریت وصله
۳۱۴.....	۴-۹-۱ مدیریت وصله
۳۱۴.....	۴-۹-۲ مدیریت عرضه
۳۱۶.....	۴-۹-۳ عملیات سیستم اطلاعاتی
۳۱۸.....	۴-۱۰ مدیریت سطح خدمت فناوری اطلاعات
۳۱۹.....	۴-۱۰-۱ قراردادهای سطح خدمات
۳۲۰.....	۴-۱۰-۲ پایش سطوح خدمت
۳۲۱.....	۴-۱۰-۳ سطوح خدمت و معماری سازمانی
۳۲۱.....	۴-۱۱ مدیریت پایگاه داده
۳۲۲.....	۴-۱۱-۱ معماری DBMS
۳۲۳.....	۴-۱۱-۲ ساختار پایگاه داده
۳۲۶.....	۴-۱۱-۳ کنترل های پایگاه داده
۳۲۷.....	۴-۱۱-۴ بازبینی های پایگاه داده
۳۲۹.....	بخش ب: تاب آوری کسبوکار
۳۲۹.....	۴-۱۲ تحلیل تأثیر کسبوکار
۳۳۲.....	۴-۱۲-۱ طبقه بندی عملیات و تحلیل حیاتی بودن
۳۳۳.....	۴-۱۳ تاب آوری سیستم
۳۳۳.....	۴-۱۳-۱ روش های تاب آوری و بازیابی پس از وقوع بلایای طبیعی برنامه کاربردی
۳۳۳.....	۴-۱۳-۲ روش های تاب آوری و بازیابی پس از وقوع بلایای طبیعی شبکه های مخابراتی
۳۳۵.....	۴-۱۴ پشتیبان گیری، ذخیره سازی و بازیابی داده ها
۳۳۵.....	۴-۱۴-۱ روش های تاب آوری ذخیره سازی داده ها و بازیابی پس از وقوع بلایای طبیعی
۳۳۶.....	۴-۱۴-۲ پشتیبان گیری و بازیابی
۳۴۰.....	۴-۱۴-۳ زمان بندی های پشتیبان گیری
۳۴۳.....	۴-۱۵ برنامه تداوم کسبوکار
۳۴۴.....	۴-۱۵-۱ برنامه ریزی تداوم کسبوکار فناوری اطلاعات
۳۴۶.....	۴-۱۵-۲ فاجعه ها و سایر رویدادهای مخرب
۳۴۸.....	۴-۱۵-۳ فرایند برنامه ریزی تداوم کسبوکار
۳۴۸.....	۴-۱۵-۴ سیاست تداوم کسبوکار
۳۴۹.....	۴-۱۵-۵ مدیریت حادثه برنامه ریزی تداوم کسبوکار
۳۵۰.....	۴-۱۵-۶ توسعه برنامه های تداوم کسبوکار

۳۵۱	۴-۱۵-۷ سایر معضلات در توسعه برنامه
۳۵۱	۴-۱۵-۸ مؤلفه‌های برنامه تداوم کسب‌وکار
۳۵۵	۴-۱۵-۹ آزمون برنامه
۳۵۸	۴-۱۵-۱۰ خلاصه تداوم کسب‌وکار
۳۵۹	۴-۱۵-۱۱ حسابرسی تداوم کسب‌وکار
۳۶۲	۴-۱۶ برنامه‌های بازیابی پس از وقوع بلایای طبیعی
۳۶۳	۴-۱۶-۱ هدف نقطه بازیابی و هدف زمان بازیابی
۳۶۴	۴-۱۶-۲ راهبردهای بازیابی
۳۶۵	۴-۱۶-۳ راهکارهای بازیابی
۳۶۸	۴-۱۶-۴ توسعه برنامه‌های بازیابی پس از وقوع بلایای طبیعی
۳۷۱	۴-۱۶-۵ روش‌های آزمون بازیابی پس از وقوع بلایای طبیعی
۳۷۴	۴-۱۶-۶ فراخوانی برنامه‌های بازیابی پس از وقوع بلایای طبیعی

فصل ۵: حفاظت از دارایی‌های اطلاعاتی ۳۷۵

۳۷۵	بررسی اجمالی
۳۷۵	طرح محتوای آزمون حوزه ۵
۳۷۵	بخش الف: امنیت و کنترل دارایی اطلاعاتی
۳۷۵	بخش ب: مدیریت رویدادهای امنیتی
۳۷۶	اهداف یادگیری/بیانیه‌های وظایف
۳۷۶	منابع پیشنهادی برای مطالعه بیشتر
۳۷۷	سؤالات خودآزمایی
۳۷۹	پاسخ به سؤالات خودآزمایی
۳۸۳	بخش الف: امنیت و کنترل دارایی اطلاعاتی
۳۸۳	۵-۰ مقدمه
۳۸۳	۵-۱ چارچوب‌ها، استانداردها و دستورعمل‌های امنیت دارایی‌های اطلاعاتی
۳۸۳	۵-۱-۱ حسابرسی چارچوب مدیریت امنیت اطلاعات
۳۸۹	۵-۲ اصول حریم خصوصی
۳۹۰	۵-۲-۱ ملاحظات حسابرسی برای حریم خصوصی
۳۹۱	۵-۳ دسترسی فیزیکی و کنترل‌های محیطی
۳۹۲	۵-۳-۱ کنترل‌های مدیریتی، فنی و فیزیکی
۳۹۳	۵-۳-۲ نظارت و اثربخشی کنترل
۳۹۳	۵-۳-۳ مواجهه‌ها و کنترل‌های محیطی
۳۹۸	۵-۳-۴ کنترل‌ها و مواجهه‌های دسترسی فیزیکی
۴۰۳	۵-۴ مدیریت هویت و دسترسی
۴۰۳	۵-۴-۱ مجوز دسترسی به سیستم
۴۰۵	۵-۴-۲ کنترل‌های دسترسی اجباری و اختیاری
۴۰۵	۵-۴-۳ امنیت اطلاعات و طرف‌های خارجی
۴۱۰	۵-۴-۴ دسترسی منطقی
۴۱۲	۵-۴-۵ نرم‌افزار کنترل دسترسی
۴۱۳	۵-۴-۶ شناسایی و احراز هویت

۴۱۶.....	۵-۴-۷ شناسه‌های ورود و گذرواژه.....
۴۱۸.....	۵-۴-۸ بیومتریک.....
۴۲۱.....	۵-۴-۹ شناسایی یکپارچه.....
۴۲۳.....	۵-۴-۱۰ معضلات مجوز.....
۴۲۶.....	۵-۴-۱۱ ورود حسابرسی در دسترسی به سیستم پایش.....
۴۲۸.....	۵-۴-۱۲ قراردادهای نام‌گذاری برای کنترل‌های دسترسی منطقی.....
۴۲۹.....	۵-۴-۱۳ مدیریت هویت باهمیده.....
۴۲۹.....	۵-۴-۱۴ دسترسی منطقی حسابرسی.....
۴۳۲.....	۵-۴-۱۵ نشت داده.....
۴۳۴.....	۵-۵ امنیت شبکه و نقطه پایانی.....
۴۳۵.....	۵-۵-۱ زیرساخت شبکه سیستم اطلاعاتی.....
۴۳۶.....	۵-۵-۲ معماری شبکه‌های سازمانی.....
۴۳۶.....	۵-۵-۳ انواع شبکه‌ها.....
۴۳۷.....	۵-۵-۴ خدمات شبکه.....
۴۳۸.....	۵-۵-۵ استانداردها و پروتکل‌های شبکه.....
۴۳۸.....	۵-۵-۶ معماری اتصال داخلی سیستم‌های باز (OSI).....
۴۴۱.....	۵-۵-۷ کاربرد مدل OSI در معماری شبکه.....
۴۶۴.....	۵-۵-۸ امنیت زیرساخت شبکه.....
۴۷۲.....	۵-۵-۹ Shadow IT.....
۴۷۳.....	۵-۶ طبقه‌بندی داده‌ها.....
۴۷۴.....	۵-۷ رمزگذاری داده‌ها و تکنیک‌های مربوط به رمزگذاری.....
۴۷۴.....	۵-۷-۱ عناصر کلیدی سیستم‌های رمزگذاری.....
۴۷۶.....	۵-۷-۲ سیستم‌های رمزنگاری کلید متقارن.....
۴۷۷.....	۵-۷-۳ سیستم‌های رمزنگاری کلید عمومی (نامتقارن).....
۴۸۰.....	۵-۷-۴ کاربردهای سیستم‌های رمزنگاری.....
۴۸۱.....	۵-۸ زیرساخت کلید عمومی.....
۴۸۳.....	۵-۹ فناوری‌های ارتباطی تحت‌وب.....
۴۸۳.....	۵-۹-۱ صدا روی IP.....
۴۸۵.....	۵-۹-۲ تبادل شعبه خصوصی.....
۴۸۶.....	۵-۹-۳ مسائل امنیتی پست الکترونیکی.....
۴۸۸.....	۵-۹-۴ رایانش هم‌تا به هم‌تا.....
۴۸۹.....	۵-۹-۵ پیامرسانی فوری.....
۴۹۰.....	۵-۹-۶ رسانه‌های اجتماعی.....
۴۹۲.....	۵-۹-۷ رایانش ابری.....
۴۹۹.....	۵-۱۰ محیط‌های مجازی.....
۵۰۲.....	۵-۱۰-۱ حوزه‌های ریسک کلیدی.....
۵۰۲.....	۵-۱۰-۲ کنترل‌های معمولی.....
۵۰۳.....	۵-۱۱ دستگاه‌های سیار، بی‌سیم و اینترنت اشیا.....
۵۰۳.....	۵-۱۱-۱ رایانش سیار.....
۵۰۷.....	۵-۱۱-۲ شبکه‌های بی‌سیم.....

۵۱۲.....	۵-۱۱-۳ اینترنت اشیا.....
۵۱۳.....	بخش ب: مدیریت رویداد امنیتی.....
۵۱۳.....	۵-۱۲ آموزش و برنامه‌های آگاهی امنیتی.....
۵۱۴.....	۵-۱۳ روش‌ها و تکنیک‌های حمله به سیستم اطلاعاتی.....
۵۱۵.....	۵-۱۳-۱ عوامل ریسک کلاهبرداری.....
۵۱۵.....	۵-۱۳-۲ معضلات مربوط به جرایم کامپیوتری و افشا.....
۵۲۵.....	۵-۱۳-۳ تهدیدات اینترنتی و امنیت.....
۵۲۷.....	۵-۱۳-۴ بدافزار.....
۵۳۰.....	۵-۱۴ ابزارها و تکنیک‌های آزمون امنیت.....
۵۳۱.....	۵-۱۴-۱ تکنیک‌های آزمون برای کنترل‌های امنیتی رایج.....
۵۳۳.....	۵-۱۴-۲ آزمون‌های نفوذ در شبکه.....
۵۳۷.....	۵-۱۴-۳ هوش تهدید.....
۵۳۷.....	۵-۱۵ ابزارهای نظارت امنیتی و تکنیک‌ها.....
۵۳۷.....	۵-۱۵-۱ سیستم‌های تشخیص نفوذ.....
۵۳۹.....	۵-۱۵-۲ سیستم‌های پیشگیری از نفوذ.....
۵۴۱.....	۵-۱۵-۳ اطلاعات امنیتی و مدیریت رویداد.....
۵۴۱.....	۵-۱۶ مدیریت واکنش به حادثه.....
۵۴۳.....	۵-۱۷ جرایم و جمع‌آوری شواهد.....
۵۴۳.....	۵-۱۷-۱ جرایم کامپیوتری.....
۵۴۶.....	۵-۱۷-۲ حفاظت از شواهد و زنجیره نگهداری.....
۵۴۶.....	مطالعه موردی.....
۵۴۸.....	پاسخ به سؤالات مطالعه موردی.....

پیوست الف: اطلاعات عمومی آزمون CISA..... ۵۵۱

پیوست ب: شیوه شغلی CISA 2019..... ۵۵۵

۵۵۵.....	حوزه ۱- فرایند حسابرسی سیستم‌های اطلاعاتی (۲۱ درصد).....
۵۵۵.....	حوزه ۲- حاکمیت و مدیریت فناوری اطلاعات (۱۷ درصد).....
۵۵۶.....	حوزه ۳: اکتساب، توسعه و پیاده‌سازی سیستم‌های اطلاعاتی (۱۲ درصد).....
۵۵۶.....	حوزه ۴- عملیات‌های سیستم‌های اطلاعاتی و انعطاف‌پذیری کسب‌وکار (۲۳ درصد).....
۵۵۷.....	حوزه ۵- حفاظت از دارایی‌های اطلاعاتی (۲۷ درصد).....
۵۵۷.....	وظایف پشتیبانی.....

واژه‌نامه..... ۵۵۹