

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

حسابرسی فناوری اطلاعات (رویکرد کنترل و امنیت)

تألیف و اقتباس:

دکتر علیرضا فضل زاده

دکتر سجاد نقدی

سرشناسه

عنوان و نام پدید آور

: فضل زاده، علیرضا، ۱۳۴۶، گردآورنده

: حسابرسی فناوری اطلاعات (رویکرد کنترل و امنیت) / تدوین علیرضا فضل زاده ،
سجاد نقدی

مشخصات نشر

مشخصات ظاهری

فروست

شابک

وضعیت فهرست نویسی

یادداشت

موضوع

موضوع

موضوع

موضوع

شناسه افزوده

شناسه افزوده

رده بندی کنگره

رده بندی دیویی

شماره کتابشناسی ملی

Information technology - Auditing - حسابرسی فناوری اطلاعات

: سی. او. بی. آی. تی. (استاندارد مدیریت فناوری اطلاعات) COBIT

(Information technology management standard)

: Information technology - استانداردها - مدیریت - استانداردها

Management Standard

: Auditing Internal - Standards - استانداردها

: ندی، سجاد، ۱۳۶۷، - گردآورنده

: دانشگاه تبریز، انتشارات

۵۸/۵/ف ۶ ح ۵، ۱۳۹۷ TV

۵۸/۴ ۸ :

۶۰۱۷۶۱



انتشارات دانشگاه تبریز

حسابرسی فناوری اطلاعات (رویکرد کنترل و امنیت)

تدوین:

ناشر و فروست:

تاریخ و نوبت چاپ:

شمارگان:

شابک:

قیمت:

سایت:

: دکتر علیرضا فضل زاده - دکتر سجاد نقدی

: انتشارات دانشگاه تبریز؛ ۷۴۷

۱۳۹۸ - اول

۱۵۰۰ نسخه

۹۷۸-۶۰۰-۸۸۶۴-۴۷-۹

۳۹۰۰۰۰ ریال

www.publication.tabrizu.ac.ir

لیتوگرافی، چاپ و صحافی: اداره چاپ و انتشارات دانشگاه تبریز

این اثر مشمول قانون حمایت از مؤلفان و مصنفان و هنرمندان مصوب ۱۳۴۸ است. هر کس تمام یا قسمتی از این اثر را بدون اجازه ناشر، نشر یا پخش کند مورد پیگرد قانونی قرار خواهد گرفت.

نشانی: تبریز - بلوار ۲۹ بهمن - دانشگاه تبریز - تلفن: ۳۳۳۹۲۶۶۹ - نمابر: ۳۳۳۴۲۵۶۲

فهرست مطالب

۱.....	فصل اول: مقدمه‌ای بر حسابرسی فناوری اطلاعات
۲.....	مقدمه
۳.....	تأثیر IT بر حسابرسی
۶.....	حسابرس IT
۸.....	اهداف حسابرسی IT
۱۵.....	ارتباط حسابرسان IT با سایر حوزه‌های حسابرسی
۱۷.....	نهادهای حرفه‌ای و حسابرسان IT
۲۲.....	تقلب و حسابرس IT
۲۷.....	آینده حسابرسی IT
۲۸.....	خلاصه و نتیجه‌گیری
۳۱.....	فصل دوم: برنامه‌ریزی حسابرسی IT
۳۲.....	برنامه‌ریزی حسابرسی IT
۳۲.....	فرایند طراحی برنامه حسابرسی IT
۳۴.....	برنامه حسابرسان
۵۰.....	خلاصه و نتیجه‌گیری
۵۳.....	فصل سوم: حسابرسی چرخه درآمد و مخارج
۵۴.....	بخش اول: چرخه درآمد
۵۶.....	چرخه فروش - سیستم دستی
۵۸.....	چرخه فروش - سیستم مکانیزه
۶۰.....	اهداف حسابرسی چرخه فروش، کنترل‌ها و آزمون‌های کنترل و محتوا
۷۲.....	آزمون‌های محتوا در چرخه فروش
۷۲.....	بخش دوم: چرخه مخارج
۷۳.....	اهداف حسابرسی چرخه مخارج، کنترل‌ها و آزمون‌های کنترل و محتوا
۸۵.....	خلاصه و نتیجه‌گیری
۸۶.....	مطالعه موردی حسابرسی جامع IT
۸۹.....	فصل چهارم: چارچوب کوبیت

کوبیت	۹۰
کوبیت به عنوان یک چارچوب راهنما	۹۱
معیارهای هفت گانه اطلاعاتی کوبیت	۹۴
منابع کوبیت	۹۵
کوبیت و حسابرسی IT	۹۵
ارتباط کوزو و کوبیت	۱۰۱
انواع گزارش حسابرسی IT با استفاده از کوبیت	۱۰۵
خلاصه و نتیجه گیری	۱۰۷
مطالعه موردی حسابرسی مبتنی بر کوبیت	۱۰۸
فصل پنجم: کتابخانه زیرساخت فناوری اطلاعات (ITIL)	۱۱۱
ITIL	۱۱۲
حسابرسی مدیریت زیرساخت IT	۱۳۵
خلاصه و نتیجه گیری	۱۳۶
مطالعه موردی حسابرسی مبتنی بر ITIL	۱۳۶
فصل ششم: حسابرسی فناوری اطلاعات با محاسبه ریسک کوزو	۱۳۹
اهداف و اجزای کنترل های داخلی یکپارچه	۱۴۰
قوانین و مقررات حاکم بر اجرای کوزو	۱۴۱
نقش کوزو در کنترل های IT	۱۴۳
محیط کنترلی	۱۴۶
ارزیابی ریسک	۱۴۷
فعالیت های کنترلی	۱۴۸
اطلاعات و ارتباطات	۱۴۸
فعالیت های نظارتی	۱۴۹
خلاصه و نتیجه گیری	۱۵۲
فصل هفتم: استانداردهای ایزو	۱۵۵
مقدمه ای بر استانداردهای ایزو	۱۵۶
خلاصه و نتیجه گیری	۱۶۱
مطالعه موردی حسابرسی مبتنی بر استانداردهای ایزو	۱۶۱

۱۶۵	فصل هشتم: حسابرسی زبان گزارشگری تجاری گسترش پذیر (XBRL)
۱۶۶	XBRL
۱۶۶	مفاهیم پایه‌ای XBRL
۱۶۶	واژه‌نامه
۱۶۷	سند مصداق
۱۶۷	محاسن XBRL
۱۶۹	XBRL و حسابرسی IT
۱۷۷	خلاصه و نتیجه‌گیری
۱۷۹	فصل نهم: حسابرسی امنیت فناوری اطلاعات
۱۸۰	امنیت
۱۸۰	ابعاد امنیت
۱۸۳	تهدیدهای امنیت
۱۸۷	کنترل‌های امنیتی و انواع آن
۱۹۰	راهکارهای امنیتی
۱۹۵	خلاصه و نتیجه‌گیری
۱۹۵	مطالعه موردی حسابرسی امنیت IT
۱۹۹	فصل دهم: حسابرسی کنترل‌های در سطح سازمان و شبکه
۲۰۰	حسابرسی کنترل‌های در سطح سازمان
۲۰۰	دستورالعمل حسابرسی کنترل‌های در سطح سازمان
۲۱۴	حسابرسی شبکه
۲۱۵	اجزای اصلی شبکه
۲۱۶	انواع شبکه از لحاظ وسعت
۲۱۷	منابع ریسک شبکه
۲۱۹	دستورالعمل ارزیابی شبکه
۲۲۵	خلاصه و نتیجه‌گیری
۲۲۶	مطالعه موردی حسابرسی امنیت شبکه
۲۲۹	فصل یازدهم: حسابرسی پایگاه داده و طرح بازیابی از فاجعه
۲۳۰	پایگاه داده

۲۳۱	دلایل شکست در پایگاه داده
۲۳۲	طرح بازیابی از فاجعه
۲۳۴	دستورالعمل اجرایی برای ارزیابی پایگاه داده و طرح بازیابی از فاجعه
۲۴۶	مطالعه موردی حسابرسی نرم افزارها و پایگاه داده
۲۴۹	فصل دوازدهم: حسابرسی پروژه‌های IT و برون سپاری خدمات IT
۲۵۰	حسابرسی پروژه‌های سازمان
۲۵۰	دستورالعمل حسابرسی پروژه‌های IT
۲۵۷	حسابرسی برون سپاری IT
۲۶۳	خلاصه و نتیجه گیری
۲۶۵	فصل سیزدهم: حسابرسی سیستم عامل و نرم افزارهای کاربردی
۲۶۶	سیستم عامل
۲۶۶	ارزیابی کنترل‌های امنیتی ویندوز
۲۶۸	ارزیابی کنترل‌های امنیتی لینوکس
۲۶۹	دستورالعمل حسابرسی سیستم عامل
۲۷۲	حسابرسی نرم افزارهای کاربردی
۲۷۳	دستورالعمل شناسایی نرم افزارهای غیرمجاز
۲۷۶	حسابرسی تعمیر و نگهداری سیستم
۲۸۰	دستورالعمل حسابرسی نرم افزارها و برنامه‌های کاربردی سازمان
۲۸۶	خلاصه و نتیجه گیری
۲۸۶	مطالعه موردی حسابرسی نرم افزارها و برنامه های کاربردی
۲۸۹	فصل چهاردهم: گزارش حسابرسی فناوری اطلاعات
۲۹۰	گزارش حسابرسی IT
۲۹۰	اجزای گزارش حسابرس
۲۹۳	نگرشی جامع به گزارش حسابرسی IT
۲۹۸	خلاصه و نتیجه گیری
۲۹۹	پیوست الف
۳۰۳	پیوست ب
۳۰۷	فصل پانزدهم: حسابرسی فناوری اطلاعات در ایران

۳۰۸.....	وضعیت حسابرسی IT در ایران
۳۰۹.....	نگرشی تطبیقی بر وضعیت حسابرسی IT در کشور
۳۱۱.....	مشکلات و چالش‌های استقرار حسابرسی IT در ایران
۳۱۴.....	خلاصه و نتیجه‌گیری
۳۱۷.....	منابع

www.ketab.ir

پیشگفتار

در عصر حاضر فناوری اطلاعات و ارتباطات آن قدر با زندگی مردم آمیخته شده است که کمتر کسی در ضرورت و جایگاه آن تردید دارد. شعاع فناوری اطلاعات روبه‌روز گسترش پیدا کرده و وارد حوزه‌های تخصصی دیگری از قبیل حسابرسی شده است. این فرایند منجر به ظهور حرفه نوینی با عنوان حسابرسی فناوری اطلاعات گردیده است. به‌رغم توجه کافی به موضوع حسابرسی فناوری اطلاعات در کشورهای مختلف، این امر در کشور ایران غافل مانده است. افزون بر آن، واکاوی موشکافانه فرایند حسابرسی مؤسسات حسابرسی کشور حاکی از این است که رست‌های حسابرسان عمدتاً با استفاده از روش‌ها و تکنیک‌های سنتی و دستی انجام شده و کمتر فرآیندهای فناوری اطلاعات بررسی و رسیدگی می‌شوند. در نتیجه با یک بررسی تطبیقی ساده می‌توان نتیجه‌گیری کرد که رویکرد حسابرسی حال حاضر کشور از تنوع چندانی برخوردار نبوده و دستی‌تار را گشای حل معضلات کنونی حسابرسی کشور باشد. به همین دلیل مؤسسات حسابرسی در صورتی که قصد داشته باشند تا در بلندمدت به حیات خود ادامه دهند، ناگزیرند تا از مسیر فناوری اطلاعات عبور کنند. سازمان حسابرسی، جامعه حسابداران رسمی ایران، انجمن حسابرسی فناوری اطلاعات ایران و سایر نهادهای حرفه‌ای در کنار حمایت مالی و پشتیبانی دولت، این مسئولیت را دارا تا جدی‌تر از همیشه به حوزه حسابرسی فناوری اطلاعات بنگرند.

به‌منظور ارائه تصویر کاملی از مسئله و به دلیل فقدان کتاب به‌گشا و جامع به زبان فارسی در خصوص حسابرسی فناوری اطلاعات با رویکردی کاربردی، تصمیم بر آن شد تا با تألیف کتابی در این زمینه، توضیحات بیشتری ارائه گردد. در این مجموعه درس به این بوده است تا در یک فضای کاربردی به‌ضرورت و چگونگی توسعه و اجرای حسابرسی فناوری اطلاعات در سازمان‌ها پرداخته شود. از ویژگی‌های منحصربه‌فرد نوشتار حاضر این است که علاوه بر الزام و تأکید بر نقش حسابرسی فناوری اطلاعات، سعی بر آن داشته است تا با نگاهی تحلیلی-تطبیقی به متون پژوهشی این حوزه، دستورالعمل جامع و کاربردی در راستای اجرای حسابرسی فناوری اطلاعات معرفی و به طریق مقتضی ارائه گردد.

سخن پایانی:

از کلیه اساتید و همکارانی که به نحوی ما را در پدید آوردن این مجموعه یاری رسانده‌اند، خصوصا اداره چاپ و انتشارات دانشگاه تبریز به خاطر همکاری در نشر این اثر سپاسگزاریم.

نگارندگان به هیچ وجه ادعا ندارند که این نوشتار عاری از کاستی است. آنچه اهمیت دارد، جلب توجه جامعه دانشگاهی و انجمن‌های حرفه‌ای حسابرسی به موضوع حسابرسی فناوری اطلاعات است تا فضای جدیدی برای چالش و هم‌فکری در حوزه حسابرسی فناوری اطلاعات فراهم گردد. ما از تمام دانش‌پژوهان محترم تقاضا می‌شود، با ارائه پیشنهادات هوشمندانه و نقادانه خود، نگارندگان را در تکمیل این حوزه جدید از حسابرسی یاری نمایند.

دکتر علیرضا فضل زاده

دکتر سجاد نقدی

Fazlzadeh_Acc@yahoo.com

Sajad Nagdi@yahoo.com