# مخاطره امنیت اطلاعات:

# روش‌های ارزیابی و مدیریت



**پدید آوران**

**حمیدرضا خدمتگزار**

استادیار پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)

**ساناز قربانلو**

پژوهشگر پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)

APK
شرکت فنی و مهندسی
اصن پردازان کویر

وزارت علوم، تحقیقات و فناوری
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)

سرشناسه : خدمتگزار، حمیدرضا، ۱۳۶۳-
عنوان و نام پدیدآور : مخاطره امنیت اطلاعات: روش‌های ارزیابی و مدیریت/ پدیدآوران حمیدرضا خدمتگزار، ساناز قربانلو ؛ ویراستار بهروز رسولی.
مشخصات نشر : تهران: پژوهشگاه علوم و فناوری اطلاعات ایران، ۱۴۰۰.
مشخصات ظاهری : ۱۸۰ ص.: مصور(رنگی)، جدول (رنگی)، نمودار (رنگی).؛ ۲۹ × ۲۲ س‌م.
شابک : 978-622-98708-0-8
وضعیت فهرست‌نویسی : فیپا
یادداشت : پشت جلد به انگلیسی: Hamid Reza Khedmatgozar, Sanaz Ghorbanloo. Information Security Risk:Assessment and Management Methods.
یادداشت : کتاب حاضر با پشتیبانی شرکت فنی و مهندسی امن‌پردازان کویر منتشر شده است.
یادداشت : کتابنامه: ص. ۱۷۳-۱۸۰.
موضوع : کامپیوترها -- کنترل دستیابی
موضوع : Computers -- Access control
موضوع : کامپیوترها -- ایمنی اطلاعات
موضوع : Computer security
موضوع : تکنولوژی اطلاعات -- مدیریت
موضوع : Information technology -- Management
موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع : Computer networks -- Security measures
شناسه افزوده : قربانلو، ساناز، ۱۳۶۶-
شناسه افزوده : پژوهشگاه علوم و فناوری اطلاعات ایران
شناسه افزوده : شرکت فنی و مهندسی امن‌پردازان کویر
رده‌بندی کنگره : QA۷۶/۹
رده‌بندی دیویی : ۰۰۵/۸
شماره کتابشناسی ملی : ۸۴۶۰۴۲۰
وضعیت رکورد : فیپا



# مخاطره امنیت اطلاعات: روش‌های ارزیابی و مدیریت

**حمیدرضا خدمتگزار- استادیار پژوهشگاه علوم وفناوری اطلاعات ایران (ایرانداک)**

**ساناز قربانلو- پژوهشگر پژوهشگاه علوم وفناوری اطلاعات ایران (ایرانداک)**

ویراستار: بهروز رسولی

ویرایش فنی و صفحه‌آرایی: حمیدرضا خدمتگزار

طراح جلد: رضا عبدالحسینی

چاپ نخست ۱۴۰۰

شمارگان: ۵۰۰۰

شابک: ۸-۰-۹۸۷۰۸-۶۲۲-۹۷۸ ISBN: 978-622-98708-0-8



**قیمت: ۷۵۰۰۰ تومان**

تهران: ۶۶۴۹۴۹۸۰-۴ و ۹-۶۶۹۵۱۴۳۰ (۰۲۱)

تهران- خیابان انقلاب اسلامی. خیابان فلسطین جنوبی.

خیابان خواجه نصیر. شماره ۱۱

# پیشگفتار پدیدآوران

یکی از کارکردهای مهم حاکمیت مدیریت فناوری اطلاعات، مدیریت مخاطره (ریسک) است که هدف آن ایجاد یک محیط امن برای کسب‌وکارهای الکترونیکی و تجارت الکترونیکی است. در حمایت از این کارکرد، سازمان‌های گوناگون علاقمند به پیاده‌سازی استانداردهایی هستند که روش‌های گوناگون مدیریت مخاطره را منتشر کرده‌اند. این روش‌ها، در قالب دستورالعمل‌ها/ راهنماها، استانداردها و چارچوب‌های ملّی و بین‌المللی از خاستگاه‌های گوناگون کاربردی و پژوهشی و به منظور ارزیابی مخاطره امنیت اطلاعات طراحی، و به منظور شناسایی، تحلیل و کاهش مخاطره‌های مرتبط با فناوری اطلاعات از سوی سازمان‌ها مورد استفاده قرار می‌گیرد.

در حوزه امنیت اطلاعات، ارزیابی مخاطره امنیت اطلاعات به شکل کلی، یک روش نظام‌مند به منظور دستیابی به یک دید جامع در خصوص شناسایی (یافتن، تشخیص و تشریح)، تحلیل (درک ماهیت و تعیین سطح) و سنجش (مقایسه سطح با معیارها) مخاطره‌های امنیت اطلاعات در یک سازمان را فراهم می‌آورد. در حال حاضر تعداد زیادی از انواع روش‌های ارزیابی مخاطره امنیت اطلاعات وجود دارد که توسط نهادهای ملّی و بین‌المللی، سازمان‌های حرفه‌ای و طرح‌های پژوهشی منتشر شده است. هر یک از این روش‌ها برای برآورده ساختن نیازهای خاصی طراحی شده‌اند و از این‌رو اهداف، مراحل، ساختار و سطح کاربرد متفاوتی دارند. هدف مشترک این روش‌ها برآورد و اولویت‌بندی ارزش مخاطره و پیشنهاد بهترین برنامه کاهش مخاطره برای رفع یا به حداقل رساندن این مخاطره‌ها به یک سطح قابل قبول است.

به رغم تعداد روزافزون روش‌های ارزیابی و مدیریت مخاطره، گزارش‌های گوناگون، نظرسنجی‌ها و ادبیات این حوزه نشان می‌دهد که گسترش کاربرد این روش‌ها در حال حاضر در سازمان‌ها به دلیل کمبود آگاهی، هزینه‌های بالا، نیاز به تخصص و فرآیند طولانی بسیار محدود است. افزون بر این، اعتماد به این روش‌ها به علت نتایج ضعیف، گزارش‌های اشتباه و محدوده فناورانه بسیار کم است. افزون بر این، تعداد بسیار زیاد و گیج کننده روش‌های مدیریت و ارزیابی مخاطره امنیت اطلاعات مشکلی را برای سازمان‌هایی که تمایل به پذیرش و بهره‌برداری از این روش‌ها دارند ایجاد کرده است و کمبود و عدم توافق در معیارهای مرجع توافق شده یا چارچوبی برای مقایسه این روش‌ها، کاربرد علمی آن را در ارزیابی مخاطره‌های امنیتی اطلاعات سازمان‌ها محدود می‌کند. در این حوزه علی‌رغم اینکه تعدادی مطالعه در مقایسه این روش‌ها انجام شده است، اما هم از نظر جامعیت روش‌های مورد بررسی و هم معیارهای طراحی شده در چارچوب پایه مقایسه محدودیت‌های فراوانی دارند. ضمن آنکه پیچیدگی موجود این ارزیابی‌ها در شکل ارائه نیز استفاده گسترده و سریع از آنها را در حوزه کاربرد دچار خدشه کرده است. از سوی دیگر در حوزه کاربرد در ایران شاهد آن هستیم که علی‌رغم وجود تنوع زیاد روش‌های ارزیابی مخاطره امنیت اطلاعات، هم از سوی مشاوران و هم از سوی بهره‌برداران دانش و آگاهی کافی در خصوص این روش‌ها وجود ندارد و تنها تعداد محدودی از آنها مورد استفاده قرار می‌گیرد. همچنین چارچوبی که بتوان مبتنی بر آن نسبت به شناخت و مقایسه این روش‌ها در موقعیت‌های گوناگون کاربردی اقدام کرد، یافت نشد.

در مجموع این محدودیت‌های پژوهشی و کاربردی، لزوم طراحی چارچوب مقایسه روش‌های ارزیابی و مدیریت مخاطره امنیت اطلاعات و سپس مصورسازی آنها را به منظور ایجاد امکان استفاده گسترده در حوزه کاربرد بیشتر نمایان می‌کند. با این توضیحات، هدف این کتاب را می‌توان مقایسه جامع و مصورسازی روش‌های ارزیابی و مدیریت مخاطره امنیت اطلاعات معرفی کرد.

این کتاب با توجه به رویکرد خود می‌تواند برای استفاده کاربردی، پژوهشی و دانشگاهی در حوزه‌های تخصصی مرتبط با مدیریت و مهندسی امنیت اطلاعات مد نظر قرار گیرد. از همه صاحب‌نظرانی که انتقاد و پیشنهادی برای ارتقاء اثر حاضر دارند، تقاضا داریم هرگونه نظر خود را درباره کتاب حاضر با پست الکترونیکی به آدرس khedmatgozar@irandoc.ac.ir ارائه فرمایند.

**با سپاس**

**حمیدرضا خدمتگزار**

**ساناز قربانلو**

# پیشگفتار پشتیبان کتاب

توسعه روزافزون به‌کارگیری فناوری اطلاعات در فرآیندهای کسب‌وکار موجب شده است که اطلاعات و دارایی‌های اطلاعاتی به یکی از منابع حیاتی سازمان‌ها تبدیل شود. استفاده مناسب از این اطلاعات و دارایی‌های اطلاعاتی به یکی از نیازهای اساسی برای دستیابی به اهداف سازمانی تبدیل شده است و حفظ محرمانگی، صحت و دسترس‌پذیری اطلاعات از مشخصه‌های مهم برای حفظ حیات و تداوم کسب‌وکار تلقی می‌شود.

پیشرفت سیستم‌های رایانه‌ای، رایانش ابری، خدمات شبکه‌های اجتماعی و وابستگی کسب‌وکارها به فناوری اطلاعات، آنها را در معرض خطرات زیادی از جمله سرقت، از بین رفتن و یا تخریب اطلاعات قرار داده است. از این منظر باید گفت تأمین امنیت اطلاعات مهمترین دغدغه و چالش این دوران است. از مهمترین موضوع‌ها در حوزه امنیت اطلاعات، شناسایی و مدیریت مخاطرات است که می‌توان آن را به عنوان سنگ‌بنای تصمیم‌های مدیران و متخصصان امنیتی دانست. مدیریت مخاطره یک فرآیند نظام‌مند است که به سازمان‌ها در درک اینکه مخاطره چیست، چه کسانی در معرض مخاطره قرار دارند و اینکه کنترل‌های فعلی برای این مخاطره‌ها و قضاوت‌های موجود در خصوص کفایت این کنترل‌ها مناسب هستند یا خیر، کمک می‌کند. در صورتی که این کنترل‌های موجود مناسب و کافی نباشند، برای ارتقای کنترل و مدیریت سطح مخاطره به یک سطح قابل قبول و معقول، بایستی اقدام‌هایی انجام شود. امروزه پیاده‌سازی یک سیستم مدیریت امنیت اطلاعات مبتنی بر مدیریت مخاطره مناسب در سازمان‌ها، به خصوص سازمان‌های بزرگ، بیش از هرگونه تعهد اخلاقی برای محافظت از کارکنان، به یک الزام قانونی تبدیل شده است که توصیه می‌شود قبل از هرگونه اقدامی از تجارب شرکت‌های دارای سابقه در این حوزه بهره جست.

تجربیات گسترده «شرکت فنی‌ومهندسی امن‌پردازان کویر» یا به اختصار (APK) در زمینه خدمات و محصولات مدیریت مخاطرات امنیت اطلاعات، طی سالیان متمادی، آن را به شرکتی قابل اعتماد و پیشرو تبدیل کرده که می‌تواند همراه مطمئنی برای سازمان‌ها در مسیر مشاوره، پیاده‌سازی، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات باشد.



ما معتقدیم "ارزیابی مخاطره امنیت اطلاعات" و راهکارهای فنی مبتنی بر آن، باید همواره به عنوان سنگ‌بنای پیاده‌سازی استانداردهای "سیستم مدیریت امنیت اطلاعات" مورد توجه سازمان‌ها و کسب‌وکارها قرار گیرد؛ اگرچه، هم‌اکنون تنوع روش‌های ارزیابی و مدیریت مخاطره امنیت اطلاعات، همچنین عدم توافق در معیارهای مرجع مورد تأیید و نبود چارچوب مقایسه‌ای برای ارزیابی آنها، سازمان‌ها را در فرآیند انتخاب و بهره‌برداری از این روش‌ها با چالش‌هایی جدی مواجه کرده است.

در همین راستا امیدواریم این اثر برای مدیران اجرایی، ممیزان، مشاوران و سران تیم‌های امنیتی در استفاده بهینه از یک چارچوب ارزیابی مقایسه‌ای، با هدف به‌کارگیری مناسب روش‌های ارزیابی و مدیریت مخاطره امنیت اطلاعات مفید بوده و با کاهش چالش‌های سازمان‌ها در این حوزه، به ذینفعان این اطمینان خاطر را دهد که مخاطره‌ها به صورت بهینه مدیریت می‌شوند.

با سپاس

شرکت فنی و مهندسی

امن‌پردازان کویر

www.apk-group.net

# فهرست نوشته‌ها