مخاطره امنیت اطلاعات:
روش‌های ارزیابی و مدیریت

حمید رضا خدمتگزار ساناز قربانلو

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

APK
تشرکت فنی و مهندسی
امن پردازان کویر

ایرانداک در نیم‌قرنِ دوم کارِ خود، همچنان جوان و کوشا؛ همراه هر پژوهش، پژوهشگر، و سیاست‌گذار

۱۳۴۷–۱۴۰۰

مخاطره امنیت اطلاعات:

روش‌های ارزیابی و مدیریت

پدیدآوران

حمیدرضا خدمتگزار

استادیار پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)

ساناز قربانلو

پژوهشگر 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: ۴-۶۶۴۹۴۹۸۰ و ۹-۶۶۹۵۱۴۳۰ (۰۲۱)

تهران- خیابان انقلاب اسلامی. خیابان فلسطین جنوبی.

خیابان خواجه نصیر. شماره ۱۱

تقدیم به:

آنان که اهل یافتن هستند، نه اهل بافتن

کسانی که متواضعانه معترفند حقیقتی را یافته‌اند، نه کل حقیقت را

نخستین معلّمان و فرشتگان زندگی: پدر و مادر

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 گیج‌کننده 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

فهرست جدول‌ها

فهرست شکل‌ها

فصل نخست

مفاهیم پایه

مدیریت مخاطره امنیت اطلاعات

۱–۱. مقدمه

امروزه با پیشرفت سیستم‌های رایانه‌ای، رایانش ابری، خدمات شبکه‌های اجتماعی و همچنین وابستگی کسب‌وکارها به فناوری اطلاعات، خطرهای زیادی کسب‌وکارها را در معرض سرقت اطلاعات، از بین رفتن اطلاعات و یا تخریب اطلاعات قرار می‌دهند. اطلاعاتی که مهم‌ترین گنجینه سازمان‌ها و اشخاص به شمار می‌رود و از بین رفتن و حتی کوچک‌ترین آسیب به آن، نیازمند صرف زمان، هزینه و نیروی کار تصورناپذیری برای جبران است و گاهی اصول کاری و موجودیت یک سازمان را تهدید می‌کند. بیشتر سازمان‌ها برای بقاء، پیشرفت و حفاظت از دارایی‌های اطلاعاتی خود به سیستم‌های اطلاعاتی نیاز دارند. برای این منظور، مدیریت امنیت اطلاعات برای ایجاد امنیت در پیدایش و تبادل اطلاعات، به کمک نظام مدیریتی بر پایه استانداردها و راهنماهای فنی و تصمیم‌های صحیح مدیریتی، می‌تواند موجب بهبود عملکرد نظام اطلاعاتی و ارتباطی شود. در واقع، موضوع امنیت اطلاعات به عنوان مهم‌ترین عنصر فناوری اطلاعات در سازمان‌ها، بهره‌برداری از سیستم‌های امنیت اطلاعات را با چالش مخاطره مواجه کرده است. چنانچه فرآیند به‌کارگیری روش‌های مدیریت و ارزیابی مخاطره در این سیستم‌ها به درستی انجام شود، می‌تواند تأثیر شگرفی بر شیوهٔ سازماندهی فعالیت‌های سازمان‌ها در زمینه امنیت اطلاعات داشته باشد (Feng, Wang and Li 2014).

آنچه در این فصل به تفصیل بحث می‌شود، شیوهٔ پیدایش و تکامل پدیده‌ها و مفاهیم مرتبط با مدیریت امنیت اطلاعات است. برای این منظور، نخست به بررسی تاریخچه امنیت، ارکان اصلی امنیت اطلاعات، و جایگاه آن پرداخته، و در ادامه ضرورت توجه به امنیت اطلاعات بررسی می‌شود. سرانجام، چالش‌های مطرح در فرآیند مدیریت مخاطره امنیت اطلاعات شناسایی و تشریح خواهند شد.

۱–۲. نگاهی اجمالی به مفهوم امنیت

امنیت در لغت به معنای محافظت است. هدف اصلی امنیت، محافظت از داشته‌ها در مقابل دشمنان است. در این تعریف، دشمن به فردی اشاره دارد که به صورت عمدی یا غیرعمد می‌خواهد به کسی یا چیزی آسیب برساند. برای نمونه، امنیت ملّی در یک نظام امنیتی دارای چندین لایه است که به محافظت از یک کشور، دارایی‌ها، منابع و مردم آن می‌پردازد (Whitman and Mattord 2016). مفهوم امنیت در دنیای واقعی همواره برای انسان‌ها حیاتی بوده است. در آغاز تاریخ بشر، امنیت عبارت بود از:

- اصول حفظ بقا؛
- امنیت در برابر حملهٔ دیگران یا حیوانات؛

- امنیت تأمین غذا؛
- امنیت در برابر حوادث طبیعی؛ و
- امنیت در برابر بیماری‌ها.

با شکل‌گیری جوامع و برقراری ارتباطات انسانی، این مفهوم گسترش یافت و ابعاد تازه‌ای را به خود گرفت. اگرچه از دیرباز طرح مفهوم امنیت، به‌کارگیری نیروهای نظامی، و بهره‌برداری از تجهیزات نظامی را در ذهن‌ها متبادر می‌ساخت، اما با پیدایش و گسترش موضوع‌های تازه در زندگی انسان‌ها، کاربری این مفهوم هم در قالب‌های فردی و اجتماعی ابعاد تازه‌ای به خود دید که برخی از آنها عبارت بود از:

- نبود تهدید نظامی؛
- توانایی مقاومت در برابر حملات خارجی؛
- امنیت سیاسی[1]؛
- امنیت فرهنگی[2]؛
- امنیت اجتماعی[3]؛ و
- امنیت اقتصادی[4].

این روند امنیت را از قالب‌گیری صرف از تهدیدات و حملات نظامی و جنگ‌ها خارج کرد. از سوی دیگر، ابعاد اجتماعی را که در این دوران از ارزش ویژه‌ای برای انسان برخوردار شدند، در قلمرو مفهوم امنیت جای داد. آنچه در این روند تکاملی مفهوم امنیت باید به آن توجه داشت این است که این مفهوم نه تنها انسان، بلکه، موارد و موضوع‌های مرتبط با وی را نیز در بر می‌گرفت.

اگرچه از امنیت تعاریف و تعابیر گوناگونی ارائه شده است، اما با بررسی مجموعهٔ این تعریف‌ها، می‌توان مفاهیم زیر را از مفهوم امنیت برداشت کرد:

- امنیت مفهومی بین‌رشته‌ای است؛
- امنیت مفهومی نسبی است؛
- امنیت مفهومی توصیف‌گرانه است؛ و
- امنیت به یک شرایط و موقعیتی خاص اشاره دارد.

مجموعه اصول بالا موجب شده‌اند که تعریف‌های متفاوتی از امنیت ارائه شوند که هر یک برحسب حوزه تعریف، دارای اعتبار و ارزش هستند. با توجه به اصول پیش‌گفته می‌توان تعریف زیر را از امنیت ارائه کرد:

«اگر مجموعه شرایط به‌گونه‌ای باشد که داشته‌های موردنظر انسان سالم (صحیح) و از دید بیگانگان محرمانه بماند، از نظر انسان در چنین شرایطی امنیت برقرار است.»

بر پایهٔ این تعریف، مفهوم امنیت را می‌توان متشکل از دو رکن *صحت* و *محرمانگی* دانست. با بررسی کاربردهای روزمره مفهوم امنیت، می‌توان دریافت که دو رکن صحت و محرمانگی، ریشه تمام موضوع‌ها و مفاهیم در حوزه امنیت را تشکیل می‌دهند.

---

[1] Policy Security
[2] Culture Security
[3] Social Security
[4] Economic Security

۱–۳. امنیت اطلاعات و ارکان اصلی آن

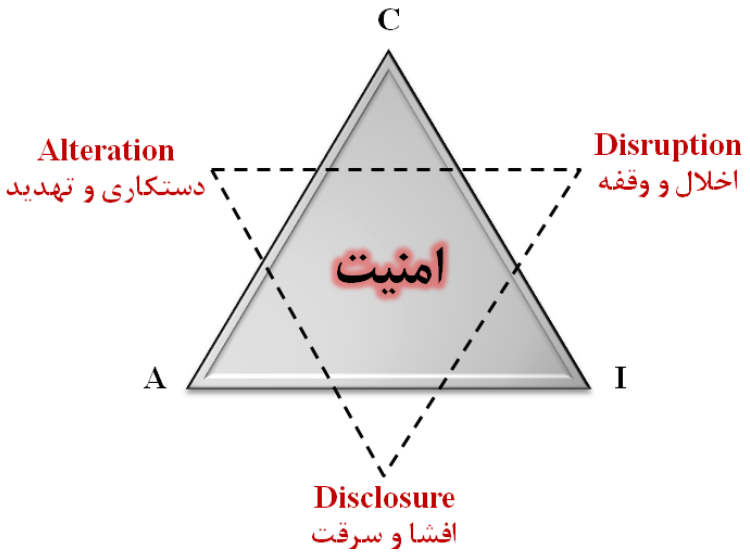
امنیت اطلاعات بر پایهٔ تعریف **انجمن سیستم‌های امنیت ملّی**[1]، به معنای حفاظت از اطلاعات و مؤلفه‌های اصلی آن است که سیستم‌ها، سخت‌افزارها، انباره‌ها و انتقال اطلاعات را در برمی‌گیرد. مؤلفه‌های امنیت اطلاعات در قالب **(شکل ۱–۱)** به تصویر کشیده شده است. همان طور که استاندارد ISO 27001 بیان می‌کند:

«امنیت اطلاعات عبارت است از حفاظت از محرمانگی، صحت و درستی و دسترس‌پذیری اطلاعات. به‌علاوه، مشخصه‌های دیگری از قبیل تأیید صحت و سندیت[2]، پاسخ‌گویی[3]، عدم انکار[4] و قابلیت اطمینان را نیز می‌توان مد نظر قرار داد.»

شکل ۱–۱. اجزای امنیت اطلاعات

امنیت اطلاعات گستره وسیعی از مفاهیم امنیتی در حوزه‌های گوناگون را دربر می‌گیرد. مدیریت امنیت اطلاعات، امنیت داده، امنیت شبکه و امنیت رایانه از عمده این موارد هستند. این اجزای امنیت اطلاعات از مدل **سازمان امنیت رایانه**[5] با نام مثلث **«سی.آی.اِی»**[6] گرفته شده که توسط **انجمن سیستم‌های امنیت ملّی**[7] ارائه شده است. این مثلث در قالب **(شکل ۱–۲)** به تصویر کشیده شده است. مثلث «سی.آی.اِی» از زمان اختراع ابررایانه‌ها به عنوان استاندارد امنیت رایانه در سطح سازمانی و دولتی استفاده می‌شود.

[1] Committee on National Security Systems (CNSS)
[2] Authenticity
[3] Accountability
[4] Non-Repudiation
[5] Computer Security Organization (CSO)
[6] Confidentiality, Integrity, Availability (CIA)
[7] Committee on National Security Systems (CNSS): http://www.cnss.gov/cnss



شکل ۱-۲. مثلث «CIA»

این استاندارد بر پایهٔ سه عامل **محرمانگی**[۱]، **صحت**[۲] و **دسترس‌پذیری**[۳] طراحی شده است. تعریف این سه عامل به شرح زیر است:

- محرمانگی: اطمینان از اینکه اطلاعات فقط در دسترس افراد و فرآیندهای مجاز قرار دارد.
- صحت: تأمین صحت و کامل بودن دارایی اطلاعاتی.
- دسترس‌پذیری: اطمینان از اینکه کاربران مجاز در صورت نیاز به اطلاعات و دارایی‌های مربوطه، به آنها دسترسی دارند.

در صورت نقص یا نبود این سه مفهوم، سه مفهوم دیگر جای دارند. محرمانگی از طریق افشاء و سرقت در معرض خطر قرار می‌گیرد، دستکاری و تهدید موجب کاهش صحت اطلاعات و دارایی‌های مربوط به آن می‌شود، و اخلال و وقفه موجب کاهش دسترس‌پذیری به اطلاعات و دارایی‌های اطلاعاتی می‌شود.

اگرچه امروزه از این سه عامل به عنوان مؤلفه‌های اصلی امنیت در سازمان‌ها یاد می‌شود، امّا باید اذعان داشت که با در نظر گرفتن ماهیت پویای محیط اطلاعاتی و سازمانی، این سه عامل برای تأمین امنیت منابع اطلاعاتی یک سازمان کافی نیستند. تهدیدهای موجود پیرامون این سه عامل دربرگیرنده گسترهٔ وسیعی از رخدادهای امنیتی هستند. این تهدیدها می‌توانند عمدی، غیرعمدی، فیزیکی و یا منطقی باشند (Whitman and Mattord 2016).

۱-۴. جایگاه امنیت اطلاعاتی سازمانی

بر پایهٔ گزارش **مؤسسه استاندارد و تحقیقات صنعتی ایران**[۴]، موضوع امنیت اطلاعات از زمانی در کانون توجه قرار گرفت که مبحث امنیت فیزیکی مطرح شد و این دو موضوع با پشتیبانی از یک‌دیگر، استخوان‌بندی کنترل امنیت شرکت‌ها را شکل می‌دهند. امنیت اطلاعات به حفاظت از اطلاعات و کمینه‌سازی خطر افشای اطلاعات در بخش‌های غیرمجاز اشاره دارد. امنیت اطلاعات به مجموعه‌ای از ابزارها اطلاق می‌شود که برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری به‌کار می‌روند. همچنین علم مطالعه روش‌های محافظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است. با توجه به تعاریفی که بیان شد، به شکل کلی، امنیت اطلاعات به مجموعه‌ای از تدابیر، روش‌ها و ابزارهایی گفته می‌شود که برای جلوگیری از دسترسی

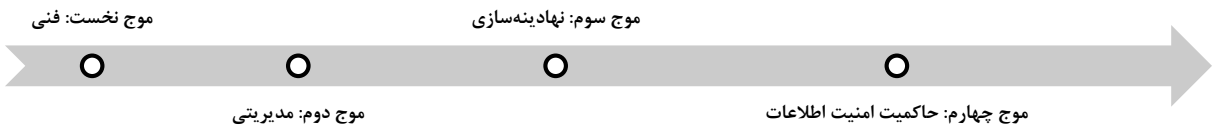
[1] Confidentiality
[2] Integrity
[3] Availability
[4] Institute of Standards & Industrial Research of Iran

و تغییرات غیرمجاز در نظام‌های رایانه‌ای و ارتباطی به‌کار می‌رود (Malekalkalami 2013). نظر به گسترش بهره‌برداری از اینترنت، تبادلات اطلاعاتی و هزینه‌های صرف‌شده به منظور یکپارچگی اطلاعاتی، امروزه مبحث کنترل و مدیریت جابه‌جایی‌های اطلاعاتی و برخورداری از سامانه‌های فراگیر برای مدیریت امنیت اطلاعات، بیش از پیش احساس می‌شود (Kwon et al. 2007).

امنیت اطلاعات مبحث بسیار مهمی است؛ زیرا هدف آن حفاظت کاربر در برابر تهدیدها و مخاطره‌ها و دسترسی به اطلاعات امن، مطمئن و محرمانه است و برای اطمینان از امنیت آن، سازمان باید سیاست‌ها و خط‌مشی‌های امنیت اطلاعات را شناسایی و تبیین کند (Xiao-yan, Yu-qing and Li-lei 2011).

۱–۵. اهمیت و ضرورت توجه به امنیت اطلاعات

با پررنگ‌تر شدن نقش اطلاعات و میزان اهمیت آن برای سازمان‌های گوناگون، رفته‌رفته موضوع امنیت اطلاعات و نیاز دستیابی به یک سیستم مدیریت امنیت اطلاعات اهمیت بیشتری یافته است. تا جایی که توسعه امنیت اطلاعات در طول ۵۰ سال گذشته، به شکل‌های گوناگونی نمود پیدا کرده است. یکی از این اشکال، بیانگر سیر تکامل و پیشرفت امنیت اطلاعات در چهار موج فنی، مدیریتی، نهادینه‌سازی و حاکمیت امنیت اطلاعات است. سیر تکاملی امنیت اطلاعات در (**شکل ۱–۳**) به تصویر کشیده شده است (Von Solms 2006; Van Niekerk and Von Solms 2010; Solms 2000).



شکل ۱–۳. سیر تکاملی امنیت اطلاعات

در ادامه، مروری گذرا بر روند تکاملی امنیت اطلاعات در طول دهه‌های گوناگون (**شکل ۱–۳**) و در قالب چهار موج فنی، مدیریتی، نهادینه‌سازی، و حاکمیت امنیت اطلاعات خواهیم داشت.

۱–۵–۱. موج نخست: فنی

این موج، به طور عمده بر ابررایانه‌ها استوار بود. در این موج، کوشش می‌شد تا امنیت اطلاعات با بهره‌برداری از امکانات موجود در رایانه‌ها (مانند سیاهه‌های کنترل دسترسی، شناسه‌های کاربر و کلمه‌های عبور) در سیستم‌های عامل پردازنده مرکزی تأمین شود. مسائلی از جمله خط‌مشی‌های امنیت اطلاعات و آگاهی از وضعیت امنیت اطلاعات کاربران در این موج در کانون توجه نبودند. با این حال حتی در همان اوایل دهه ۸۰ میلادی، افراد فنی که مسئول پیاده‌سازی/ اجرای امنیت اطلاعات بودند، به این موضوع پی بردند که در برخی از مواقع مدیریت می‌تواند نقشی چشم‌گیر در این حوزه داشته باشد. با این وجود، امنیت اطلاعات یک موضوع کاملاً فنی به شمار می‌رفت که به طور کامل به افراد فنی سپرده شده بود.

۱–۵–۲. موج دوم: مدیریتی

توسعه **رایانش توزیع‌شده**[1]، اینترنت، شبکه جهانی اطلاعات/ وب و تجارت الکترونیکی ازجمله عواملی بودند که دریچه‌ای تازه به به موضوع امنیت اطلاعات باز کردند. در این موج، مدیر ارشد/ سطح بالا درگیر مسائل امنیتی شده و مسائل مطرح در امنیت اطلاعات به شکل چشم‌گیری افزایش یافت. خط‌مشی‌های امنیت اطلاعات، مدیران امنیت اطلاعات و ساختارهای سازمانی برای امنیت

[1] Distributed Computing

اطلاعات به عنوان مسائل مهم در این موج مورد توجه قرار گرفتند. نتایج حاصل از این موج به موازات موج فنی آن بود که خواسته‌های مدیران در امنیت اطلاعات محور کلیدی قرار گرفت و در نهایت مدیران امنیت اطلاعات منصوب شدند. سپس این مدیران نسبت به تهیه پیش‌نویس خط‌مشی‌ها، رویه‌ها و ارائه گزارش به مدیران سطح بالا از طریق ساختارهای سازمان‌یافته اقدام کردند و به طور کلی، این موجب اصلاح امنیت اطلاعات شد. پس از مدتی نیازهای تازه‌ای توسط سازمان‌ها احساس شد نسبت به اینکه: ۱) امنیت اطلاعات آن‌ها چقدر خوب است؟ ۲) چگونه می‌توان امنیت سازمان را با دیگر سازمان‌ها مقایسه کرد؟ و ۳) بُعد انسانی امنیت اطلاعات همچنان می‌تواند به عنوان مشکلی بزرگ باقی ماند. این نیازها به همراه دو موج نخست و دوم، موج سوم را تشکیل دادند.

از جمله نمودهای موج دوم می‌توان به شکل‌گیری استاندارد ISO/IEC 27001 اشاره کرد که یک استاندارد معروف در حوزه مدیریت امنیت اطلاعات است. در واقع، نخستین استاندارد مدیریت امنیت اطلاعات توسط «مؤسسه استانداردهای انگلستان»[1] و با نام BS 7799 ارائه شده است. این استاندارد توسط بخش دولتی «تجارت و صنعت انگلستان» نوشته شده و دارای چندین بخش است که به‌صورت جداگانه منتشر شده‌اند:

- بخش نخست استاندارد پیش‌گفته که در رابطه با مدیریت امنیت اطلاعات است، در سال ۱۹۹۵ میلادی منتشر شد. این استاندارد در سال ۱۹۹۸ میلادی بازنویسی شده و در سال ۲۰۰۰ میلادی زیر نظر مؤسسه بین‌المللی استاندارد (ایزو) با نام ISO/IEC 17799 ارائه شد. عنوان کامل استاندارد پیش‌گفته "*فناوری اطلاعات-رهنمودهایی برای مدیریت امنیت اطلاعات*" است که در سال ۲۰۰۵ میلادی بازنگری شده و سرانجام در زیر گروه استانداردهای امنیتی ISO 27000 قرار گرفت و استاندارد ISO/IEC 27002 بر پایهٔ آن در جولای ۲۰۰۷ میلادی عرضه شد. نسخه اصلاح شده این استاندارد نیز در سال ۲۰۱۳ میلادی منتشر شده است.
- بخش دوم BS 7799 برای نخستین بار در سال ۱۹۹۹ میلادی توسط «مؤسسه استانداردهای انگلستان» با عنوان "*سیستم‌های مدیریت امنیت اطلاعات-مشخصات با راهنمایی برای استفاده*" ارائه شد و تمرکز آن بر روی پیاده‌سازی «سیستم‌های مدیریت امنیت اطلاعات»[2] بود. نسخه دوم استاندارد BS 7799 که در سال ۲۰۰۲ میلادی ارائه شد، یک مدل جدید به نام **برنامه- اجرا- کنترل- عمل** «پی.دی.سی.ای.»[3] را معرفی کرد که در رابطه با تضمین کیفیت ارائه شد. ارائه مدل «پی.دی.سی.ای.» استاندارد پیش‌گفته را به استانداردهای کیفیتی ISO 9000 نزدیک کرد. بر پایهٔ خط‌مشی‌ها و ساختارهای مدیریت امنیت اطلاعات ارائه شده در دو نسخه مذکور، استاندارد ISO/IEC 27001 در نوامبر سال ۲۰۰۵ میلادی منتشر شد و در سال ۲۰۱۳ میلادی مورد بازنگری قرار گرفت.
- بخش سوم BS 7799 در سال ۲۰۰۵ میلادی، با موضوع تحلیل و مدیریت مخاطره‌ها منتشر شد. این بخش همچنین به عنوان یک استاندارد بین‌المللی در سال ۲۰۰۵ میلادی و در قالب استاندارد ISO/IEC 27005 ارائه شد. نسخه‌های توسعه‌یافته این استاندارد نیز توسط ایزو در سال‌های ۲۰۱۳ و ۲۰۱۸ میلادی منتشر شده است. در واقع، سازمان می‌تواند با بهره‌برداری از این استاندارد مخاطره‌هایی که متوجه امنیت اطلاعات است را شناسایی و ارزیابی نموده و کنترل‌های مناسبی جهت حفظ محرمانگی، صحت و در دسترس‌بودن این سرمایه‌های مهم اتخاذ نماید.

۱-۵-۳. موج سوم- نهادینه‌سازی

نهادینه‌سازی[4] بر ایجاد یک زیرساخت امنیت اطلاعات فنی و رویه‌ای و همچنین یک فرهنگ امنیت اطلاعات شرکتی استوار است که از خط‌مشی‌های امنیت اطلاعات، رویه‌ها، روش‌ها و مسئولیت‌های شرکت پشتیبانی کند، به شکلی که تأمین امنیت اطلاعات

[1] British Standards Institution (BSI)
[2] Information Security Management Systems (ISMS)
[3] Plan-Do-Check-Act (PDCA)
[4] Institutionalization

به یک روال عادی از فعالیت‌های روزانه در بین تمامی کارکنان شرکت تبدیل شود. این زیرساخت تجاری، فنی و رویه‌ای مبتنی بر به‌روش‌های بین‌المللی است و توسط یک سیستم جامع سنجش امنیت اطلاعات در سراسر جهان پشتیبانی می‌شود که جهت مدیریت لحظه‌به‌لحظه امنیت اطلاعات، تمامی اطلاعات لازم را در اختیار مدیران قرار می‌دهد. چهار مؤلفه اصلی موج سوم عبارتند از:

- ***استانداردسازی امنیت اطلاعات، یا پیروی از به‌روش‌های بین‌المللی برای مدیریت امنیت اطلاعات***: به‌روش‌های بین‌المللی یا رهنمودهای[1] بین‌المللی جهت مدیریت امنیت اطلاعات، در واقع، جمع‌آوری تجارب ترکیبی از چندین شرکت بین‌المللی بانفوذ است که در پیوند با شیوهٔ مدیریت امنیت اطلاعات خود دچار نگرانی هستند. در واقع، این به‌روش‌ها و رهنمودها، تجربه چنین شرکت‌هایی را دربارهٔ اقدام‌های کنترلی مربوطه، رویه‌ای و همچنین فنی منعکس می‌کنند که جهت ارائه سطح مناسب یا قابل قبول امنیت اطلاعات به دست آورده‌اند. البته چنین رهنمودهایی نمی‌تواند به طور دقیق و صددرصد نشان دهد که کدام اقدام‌های کنترلی در همه موارد نیاز است، بلکه می‌توانند به عنوان یک مبنا برای امنیت اطلاعات مورد استفاده قرار گیرند. در تمامی موارد، تحلیل‌های مخاطره خاصی باید انجام شود تا تعیین کند که اگر شرکتی خاص قصد دارد از این رهنمودهای پایه استفاده کند، آیا مخاطره‌های خاص دیگری دارد که باید اقدام‌های کنترلی امنیتی خاصی برای مواجهه با آنها در نظر گرفت یا خیر؟ با این وجود، با پیروی از یک رهنمود پایه، شرکت می‌تواند به این اطمینان برسد که بیشتر جنبه‌های امنیتی که باید مورد توجه قرار گیرند، با بهره‌برداری از یک رهنمود خوب قابل شناسایی هستند.
- ***گواهینامه بین‌المللی امنیت اطلاعات، برای نشان دادن امنیت سازمان به طرف‌های بین‌المللی در تجارت الکترونیکی و بهبود وجهه تجاری***: در این مرحله، اگر شرکت از فرآیند ممیزی عبور کند، برای نمونه، سازگار با اقدام‌های کنترلی شناسایی شده در استاندارد ISO/IEC 27001 توسط تحلیلگر مخاطره، شرکت می‌تواند گواهی‌نامه بین‌المللی امنیت اطلاعات خود را با اعتبار سه ساله دریافت کند. این گواهی‌نامه، تأیید می‌کند که شرکت یا آن بخشی از شرکت که جهت دریافت گواهی‌نامه اقدام کرده، سازگار با سطح امنیت اطلاعاتی است که توسط استاندارد تعیین شده است. شرکت‌هایی که با موفقیت از این روند صدور گواهی‌نامه عبور کرده‌اند، اکنون خواستار تضمین امنیت اطلاعات از سوی شرکای تجارت الکترونیکی خود با بهره‌برداری از این گواهی‌نامه هستند. در حال حاضر، استاندارد ISO/IEC 27001 جزو محدود استانداردهای بین‌المللی برای امنیت اطلاعات است که امکان صدور چنین گواهی‌نامه‌ای را ممکن می‌سازد.
- ***فرهنگ‌سازی امنیت اطلاعات در سازمان، برای نهادینه‌سازی امنیت در کارکنان و رفع مشکلات انسانی به عنوان یکی از مهم‌ترین مشکلات در تأمین امنیت***: در بسیاری از موارد، کارکنان بزرگ‌ترین خطر برای سیستم‌های فناوری اطلاعات یک شرکت به شمار می‌روند. در اغلب موارد عدم شناخت کافی باعث شده است سازمان‌ها در سرتاسر جهان فعالیت خود را با برنامه‌های جامع آگاهی‌رسان امنیت اطلاعات شروع کنند. هر چقدر هم که اقدام‌های رویه‌ای و فنی در عمل خوب باشند، اما ابعاد انسانی امنیت اطلاعات نمی‌تواند به طور کامل با این اقدام‌ها حل شوند. لازمه این کار، فرهنگ‌سازی امنیت اطلاعات در سازمان است. این فرآیند از طریق القای جنبه‌های امنیت اطلاعات به هر کارمند و نهادینه‌سازی آن به عنوان یک روش طبیعی جهت انجام فعالیت روزانه وی صورت می‌گیرد. به همین دلیل است که دوره‌های آگاهی‌رسان امنیت در حال تغییر به برنامه‌های بهبود مستمر امنیت اطلاعات سازمانی هستند.
- ***ارزیابی دائمی و پویای امنیت اطلاعات در سازمان، سنجش و نظارت بر حسن اجرای خط‌مشی‌ها و رویه‌های امنیتی***: در بسیاری از سازمان‌ها، امنیت اطلاعات به‌صورت دوره‌ای مورد سنجش و ارزیابی قرار می‌گیرد. این اقدام معمولاً زمانی اتفاق می‌افتد که یک تیم ممیزی داخلی یا خارجی، ممیزی امنیت اطلاعات را انجام دهد. در بسیاری از موارد و با

[1] Codes of Practice

توجه به سطح بالای مخاطره، چنین ارزیابی‌هایی قابل قبول نیست. مدیریت امنیت اطلاعات به سوی مدلی از مدیریت شبکه در حال حرکت است که در آن سنجش دقیقه به دقیقه موقعیت جهت مدیریت وضعیت نیاز است.

۱-۵-۴. موج چهارم- حاکمیت امنیت اطلاعات

رابطه معناداری بین حاکمیت سازمان و امنیت اطلاعات برقرار است. حاکمیت سازمانی شامل مجموعه‌ای از خط‌مشی‌ها و کنترل‌های داخلی است که توسط سازمان، صرف‌نظر از اندازه یا شکل آن، مدیریت می‌شوند. حاکمیت امنیت اطلاعات، زیرمجموعه‌ای از برنامه کلی حاکمیت (سازمانی) است. حاکمیت امنیت اطلاعات فراتر از مدیریت امنیت اطلاعات است. حاکمیت امنیت اطلاعات به وضوح نشان‌دهنده نقش مهم مدیران ارشد و هیأت مدیره در شیوهٔ مدیریت امنیت اطلاعات در یک شرکت است. در واقع، حاکمیت امنیت اطلاعات بخشی از حاکمیت سازمانی است که دربرگیرنده موارد زیر است:

- تعهد هیأت مدیره، مدیریت و مدیران ارشد به امنیت اطلاعات خوب؛
- ساختار سازمانی مناسب برای اجرای خوب امنیت اطلاعات؛
- آگاهی‌رسانی کامل کاربران و تعهد آنها به سوی امنیت اطلاعات خوب؛ و
- خط‌مشی‌های ضروری، رویه‌ها، فرآیندها، فناوری‌ها و سازوکارهای پیروی از قوانین.

حاکمیت امنیت اطلاعات همه افراد یک سازمان، از رئیس هیأت مدیره تا کارمند ورود اطلاعات در کارگاه و راننده خودرو که محصولات را به مشتریان تحویل می‌دهد، را در برمی‌گیرد. همه افراد با یک‌دیگر همکاری می‌کنند تا از محرمانگی، صحت و دسترس‌پذیری دارایی‌های الکترونیکی سازمان (داده، اطلاعات، نرم‌افزار، سخت‌افزار، نیروی انسانی، و غیره) در هر زمان اطمینان حاصل شود.

حاکمیت امنیت اطلاعات را می‌توان به عنوان یک روش فراگیر در نظر گرفت که در آن امنیت اطلاعات به عنوان یک انتظام[1] برای کاهش مخاطرات فناوری اطلاعات مورد استفاده قرار می‌گیرد. یکی از ویژگی‌های کلیدی حاکمیت امنیت اطلاعات این است که از یک حلقه بسته تشکیل شده است. این حلقه با یک الزام مدیریتی برای امنیت اطلاعات آغاز می‌شود و آن را به عنوان یک جنبه راهبردی مهم در ماهیت وجودی سازمان و مسئول مدیریت مخاطره‌های فناوری اطلاعات سازمان در نظر می‌گیرد. این رفتار دربردارندهٔ تصویب یک خط‌مشی امنیت اطلاعات سازمانی است که توسط هیأت مدیره پذیرفته و امضاء شده است. این خط‌مشی توسط یک ساختار سازمانی مناسب برای امنیت اطلاعات، مالکیت‌ها و مسئولیت‌ها در همه سطوح پشتیبانی می‌شود. پس از آن فناوری‌های مورد نیاز به کار گرفته و مدیریت می‌شوند و در انتها ارزیابی انطباقی به منظور سنجش انطباق این فناوری‌ها با خط‌مشی‌ها و میزان کاهش سطح مخاطرات فناوری اطلاعات در سازمان انجام می‌شود. در واقع، حاکمیت امنیت اطلاعات، پیاده‌سازی کامل چرخه امن‌سازی شامل مراحل **طراحی-اجرا-کنترل-سنجش-گزارش**[2] است که لازم است طبق یک روش‌شناسی روشن به اجرا درآید.

پیشران‌های موج چهارم به شدت با توسعه و تحولات در حوزه‌های حاکمیت سازمانی و حوزه‌های قانونی ـ مقرراتی در پیوند است. از جمله پیشران‌های اصلی این موج می‌توان به خطر فرآیند تقلب و صرفه‌جویی در منابع مالی از طریق دستکاری داده‌های الکترونیکی ذخیره شده در سیستم‌های فناوری اطلاعات سازمان اشاره کرد. به نظر می‌رسد پیشگیری از تقلب از طریق دستکاری داده‌های الکترونیکی سازمان، هسته اصلی این پیشران است. در چند سال گذشته، ادغام/ ترکیب کامل فناوری اطلاعات در عملیات

[1] Discipline

[2] Plan–Do–Control–Measure–Report

راهبردی سازمان‌ها و فراگیر بودن بهره‌برداری از فناوری اطلاعات در سازمان‌ها و خدماتی که آنها ارائه می‌دهند، فرصت‌های زیادی را برای فریبکاری با بهره‌برداری از سیستم‌های فناوری اطلاعات فراهم آورده و منجر به خطرهای جدی شده است.

از جدی‌ترین این خطرها، **مهندسی اجتماعی**[1] و پیوند آن با امنیت اطلاعات است. مدیران ارشد این موضوع را فهمیده‌اند که بخشی از سیستم‌های فناوری اطلاعات که توسط نیروی انسانی، کارکنان و مشتریان استفاده می‌شود، صرف‌نظر از مقدار هزینه صرف‌شده در اقدام‌های فنی، می‌تواند سرچشمهٔ خطرهای جدی باشد. برای آنها روشن شده است که مسئله امنیت اطلاعات نمی‌تواند به تنهایی با ابزارهای فنی حل شود و نیازمند تصمیم‌های راهبردی در سطوح بالا جهت اطمینان از آگاهی همه کاربران از خطرهای احتمالی و پیامد مهندسی اجتماعی در حمله به سیستم‌های فناوری اطلاعات است. از سوی دیگر، به نظر می‌رسد کوشش برای بهره‌برداری از مهندسی اجتماعی برای انجام تقلب رو به افزایش است. لازم است این نکته را در نظر گرفت که حاکمیت خوب امنیت اطلاعات برای پاسخ این خطر ضروری است.

۱-۶. روند شکل‌گیری و توسعه امنیت اطلاعات

امنیت اطلاعات با مفهوم امنیت رایانه[2] نمود پیدا می‌کند. در جنگ جهانی دوم با بهره‌گیری از **ابررایانه‌ها**[3] -به منظور شکستن کدهای ارتباطی- موضوع امنیت رایانه اهمیت پیدا کرد. در آن برهه از زمان بیشترین سطح امنیتی که برای ابررایانه‌ها در نظر گرفته می‌شد امنیت فیزیکی آنها بود. در این شرایط از روش‌های آزمون و خطا برای حفاظت از محرمانگی داده‌ها استفاده می‌شد. برای نمونه، دسترسی به مکان‌های حساس نظامی از طریق کلیدها و روش‌های تشخیص چهره -به وسیله کارکنان قابل اعتماد- صورت می‌گرفت. در آن دوره تأمین امنیت اطلاعات یک رویه منظم و پیوسته[4] داشت که اغلب دربرگیرنده امنیت فیزیکی و دسته‌بندی ساده اطلاعات بود. دزدی فیزیکی، جعل و تغییر مستندها معرف انواع تهدیدهایی بود که حوزه امنیت اطلاعات را در معرض خطر قرار می‌داد (Whitman and Mattord 2016).

با معرفی پروژه «آرپانِت»[5]-که امروزه به عنوان اینترنت شناخته می‌شود- امنیت اطلاعات شکل دیگری به خود گرفت. در سال ۱۹۷۹ میلادی بود که وزارت دفاع آمریکا گزارشی را تحت عنوان گزارش «آر-۶۹۰»[6] منتشر کرد. در این گزارش اعلام شد که استفاده گسترده از مؤلفه‌های شبکه در سیستم‌های اطلاعاتی دفاعی منجر به بُروز مخاطره‌های جدیدی در حوزه امنیت اطلاعات شده است که با به‌کارگیری سازوکارهای موجود امکان مقابله با آنها وجود ندارد. بنابراین آسیب‌پذیری‌های زیر در سال ۱۹۷۹ میلادی برای سیستم‌های اطلاعاتی معرفی شدند (Whitman and Mattord 2016):

- آسیب‌پذیری فایل‌ها (شامل دزدی، کپی‌برداری و دسترسی غیرمجاز)؛
- آسیب‌پذیری سخت‌افزاری (شامل خرابی در مدارها، ارتباط‌های نادرست و جفت‌شدن متقابل[7])؛
- آسیب‌پذیری نرم‌افزاری (شامل کنترل دسترسی و عملکرد نادرست ویژگی‌های امنیتی)؛
- آسیب‌پذیری مربوط به منابع انسانی (شامل تعویض نوبت‌کاری، افشاء معیارهای حفاظتی، غیرفعال کردن دستگاه‌های سخت‌افزاری، غیرفعال کردن رویه‌های محافظتی، و غیره)؛
- آسیب‌پذیری دسترسی (شامل نصب رخدادنگار[8] و اِیرادهای نرم‌افزاری)؛ و
- آسیب‌پذیری کاربران راه دور (شامل شناسایی، احرازهویت و تغییر غیرمجاز).

---

[1] Social Engineering
[2] Computer
[3] Mainframe
[4] Routine
[5] The Advanced Research Projects Agency Network - ARPANet
[6] Rand Report R-690
[7] Cross Coupling
[8] Logger

با ارائه این مستند توسط وزارت دفاع آمریکا، مفهوم امنیت رایانه از محافظت مکانی و فیزیکی به موارد زیر تغییر کرد:

- امن‌سازی داده‌ها؛
- محدود کردن دسترسی‌های تصادفی و غیرمجاز به داده‌ها؛ و
- درگیر کردن کارکنان سطوح گوناگون سازمان در فرآیندهای امنیت اطلاعات.

با گسترش مفهوم امنیت رایانه، از سال ۲۰۰۰ میلادی تاکنون مفاهیم گوناگون و توسعه‌یافته‌ای برای امنیت اطلاعات بیان شده است که در ادامه به بررسی آنها پرداخته می‌شود.

۱-۷. مدیریت امنیت اطلاعات

مدیریت امنیت اطلاعات، بخشی از سیستم مدیریت کلی و سراسری در هر سازمان است که بر پایهٔ رویکرد مخاطره‌های کسب‌وکار جای دارد و هدف آن پایه‌گذاری، پیاده‌سازی، بهره‌برداری، نظارت، بازبینی، نگهداری و بهبود امنیت اطلاعات است. در صورت پیاده‌سازی صحیح این نوع مدیریت، می‌توان با کاهش مخاطره‌های پیرامونی به عنوان عامل مهم، نقش بسزایی را در تضمین سطح امنیتی تعریف‌شده ایفا کرد (Ostrowska and Mazur 2015).

مدیریت امنیت اطلاعات، بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت، بررسی موانع رسیدن به این اهداف و ارائه راهکارهای لازم را برعهده دارد (Chin et al. 2009). در نگاهی جامع به مدیریت امنیت اطلاعات، می‌توان آن را به صورت زیر تعریف کرد:

"یک چارچوب جامع، کامل و انطباق‌پذیر متشکل از برنامه‌های امنیتی و فرآیندها و رویه‌های مدیریتی که هدف نهایی آن تأمین و استمرار امنیت در فضای تبادل اطلاعات سازمان است."

با پیدایش نخستین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵ میلادی، نگرش نظام‌مند به مقوله ایمن‌سازی فضای تبادل اطلاعات شکل گرفت (Kwon et al. 2007). بر پایهٔ این نگرش، امنیت فضای تبادل اطلاعات سازمان‌ها، با تکرار تأمین نمی‌شود، بلکه باید این کار به‌صورت مداوم طی چرخه امن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح انجام گیرد. برای این منظور باید هر سازمان بر پایهٔ روش‌شناسی مشخص و برنامه‌ریزی‌شده‌ای به کنترل و نظارت بر اطلاعات و تبادلات اطلاعات در سازمان خود بپردازد (Broderick 2006). بر پایهٔ گزارش منتشر شده از سوی مؤسسه استاندارد و تحقیقات صنعتی ایران، مدیریت امنیت اطلاعات از طریق استانداردها و سامانه‌های مدیریتی امنیت اطلاعات در سازمان‌ها اجرا می‌شود. هدف مدیریت امنیت اطلاعات هر سازمان، حفظ سرمایه‌های سازمان (نرم‌افزاری، سخت‌افزاری، اطلاعاتی، ارتباطی و نیروی انسانی) در برابر هرگونه تهدید (دسترسی غیرمجاز به اطلاعات، خطرهای ناشی از محیط و سیستم و خطرهای ایجاد شده از سوی کاربران) است و برای دستیابی به این اهداف به برنامه منسجمی نیاز دارد.

بر پایهٔ گزارش مؤسسه امنیت اطلاعات، فرآیند سیستم مدیریت امنیت اطلاعات به یک دوره اقدام در نظام مدیریتی خلاصه نمی‌شود، بلکه طی فرآیندی دائمی در چرخه چهارمرحله‌ای امن‌سازی به ثمر می‌رسد. این چهار مرحله عبارتند از:

۱. *برنامه‌ریزی*: برپایی شرایط اولیه سامانه مدیریت امنیت اطلاعات؛
۲. *اجرا*: پیاده‌سازی و اجرای سامانه مدیریت امنیت اطلاعات؛
۳. *ارزیابی و کنترل*: فعالیت‌های نظارتی یا بررسی فعالیت‌های انجام‌گرفته؛ و
۴. *بهبود و اصلاح*: فعالیت‌های نگهداری و بهبود مستمر در این سامانه مدیریتی.

۱–۸. مخاطره

طبق تعریف استاندارد ISO/IEC 27005، مخاطره یا ریسک به احتمال اینکه یک تهدید بتواند از آسیب‌پذیری(های) یک یا گروهی از دارایی‌های اطلاعاتی استفاده کرده و سبب آسیب رساندن یا از دست دادن آن دارایی(ها) گردد، گفته می‌شود. به‌عبارت دیگر، مخاطره احتمال یک اثر مشخص بر روی سیستم در یک دوره زمانی مشخص است که می‌تواند ترکیبی از احتمال وقوع تهدید، پیامد و آسیب‌پذیری باشد. در این تعریف با سه مفهوم دارایی اطلاعاتی، تهدید و آسیب‌پذیری مواجه هستیم که به شرح زیر تعریف می‌شوند:

- *دارایی اطلاعاتی*: هر چیزی مرتبط با اطلاعات که برای سازمان مهم است. به شکل کلی، خود اطلاعات، دارایی است که همانند دیگر دارایی‌های سازمان دارای ارزش بوده و در نتیجه باید به طور مناسبی مورد محافظت قرار گیرد. در یک دسته‌بندی کلی دارایی‌های اطلاعاتی را می‌توان در دسته‌های گوناگونی از جمله نرم‌افزارها، سخت‌افزارها، سرویس‌ها، منابع انسانی و اسناد اطلاعات جای داد.
- *آسیب‌پذیری*: به نقاط ضعف در توصیف، طراحی، پیاده‌سازی، پیکربندی و یا اجرای اطلاعات در دارایی‌های اطلاعاتی اشاره دارد که بتوان از آنها برای نقض امنیت اطلاعات استفاده کرد. یک آسیب‌پذیری تا زمانی که مورد سوء استفاده یک تهدید قرار نگیرد، نمی‌تواند موجب آسیب شود.
- *تهدید*: یک عامل خطر است که به صورت بالقوه می‌تواند از یک یا چند آسیب‌پذیری سوء استفاده کند. این تهدیدها می‌تواند منشأ طبیعی یا انسانی داشته باشد و به شکل تصادفی و یا عمدی باشند. یک تهدید می‌تواند بر یک یا چند دارایی تأثیر بگذارد.

برای نمونه زمانی که در یک سامانه به عنوان یک دارایی اطلاعاتی، فقدان پیکربندی مناسب امنیتی وجود دارد، این آسیب‌پذیری می‌تواند توسط تهدیدی با نام دسترسی غیرمجاز مورد سوء استفاده قرار گرفته و یک رخداد امنیتی ایجاد کند. مجموع این ترکیب با عنوان یک **مخاطره** باید مورد توجه قرار گیرد. یک رخداد امنیتی می‌تواند موجب پیامدهایی شود که این پیامدها باید مورد توجه قرار گیرد. از مهمترین این پیامدها می‌توان به کاهش سطح محرمانگی، صحت و دسترس‌پذیری اطلاعات اشاره کرد.

۱–۹. مدیریت مخاطره

یکی از کلیدی‌ترین دامنه‌های مدیریت امنیت اطلاعات، مدیریت مخاطره است. مفهوم مدیریت مخاطره به فرآیند مشخص‌کردن، اندازه‌گیری و کنترل رخدادها اشاره دارد. امروزه مدیریت مخاطره را می‌توان سنگ‌بنای تصمیم‌های مدیران و متخصصان امنیتی محسوب کرد.

در اقتصاد امروز، مدیریت مخاطره مؤثر یک مؤلفه حیاتی از هر راهبرد مدیریتی موفق است. مدیریت مخاطره یکی از نُه حوزه دانشی است که توسط «**مؤسسه مدیریت پروژه**»[1] منتشر شده است و یکی از سخت‌ترین جنبه‌های مدیریت پروژه است. افزون بر این، مدیریت مخاطره در زمینه مدیریت پروژه یک روش سیستماتیک و جامع از شناسایی، تحلیل و مواجهه با مخاطره‌ها جهت دستیابی به اهداف پروژه است (Banaitiene and Banaitis 2012). مدیریت مخاطره یک فرآیند سیستماتیک است که به سازمان در درک اینکه مخاطره چیست، چه کسی در معرض مخاطره قرار دارد و کنترل‌های فعلی برای این مخاطره‌ها و قضاوت‌هایی که باید دربارهٔ اینکه آیا این کنترل‌ها مناسب هستند یا خیر، کمک می‌کند. در صورتی‌که کنترل‌های موجود مناسب و کافی نباشند، برای

[1] Project Management Institute (PMI)

کنترل/ مدیریت سطح مخاطره به یک سطح قابل قبول و معقول، نیاز است اقدام‌هایی انجام شود. امروزه پیاده‌سازی یک مدیریت مخاطره مناسب یا یک سیستم امنیتی در سازمان‌ها -به خصوص سازمان‌های بزرگ- بیش از هرگونه تعهد اخلاقی برای محافظت از کارکنان، به یک الزام قانونی تبدیل شده است (Nalik and Holt 2013).

در چند سال اخیر شاهد پیدایش **مدیریت مخاطره سازمانی**[1] بوده‌ایم که اغلب به عنوان یک روند تجاری جدید -بر پایهٔ اصول مدیریت مخاطره سنتی- مطرح می‌شود. این یک رویکرد ساختارمند و منظم است که راهبرد، فرآیندها، افراد، فناوری و دانش را با هدف سنجش و مدیریت عدم قطعیتی که سازمان به عنوان ایجاد ارزش با آن مواجه است همراستا می‌کند (KPMG 2001).

استاندارد ISO 31000 نشان‌دهنده یک خانواده از استانداردها است که به دنبال ارائه دستورالعمل‌های واحد و عمومی با بهره‌برداری از یک رویکرد مدیریت مخاطره مستقل از صنعت است (Niesen et al. 2016). استاندارد ISO 31000 یک دستورالعمل کلی را برای انواع حوزه‌های مدیریت مخاطره (برای نمونه، امور مالی، مهندسی، کسب‌وکار، و غیره) فراهم می‌کند. اگرچه اغلب سازمان‌ها ممکن است روش متداولی برای مدیریت مخاطره‌ها را در اختیار داشته باشند، اما این استاندارد مجموعه‌ای از اصول و قواعد را تعریف می‌کند که به منظور اطمینان از اثربخشی مدیریت مخاطره در کلیه بخش‌های سازمان می‌تواند مورد استفاده قرار گیرد. نکته دیگر دربارهٔ این استاندارد بهره‌برداری از چرخه «پی.دی.سی.ای.» جهت طراحی، ایجاد، پیاده‌سازی و بهبود فرآیند مدیریت مخاطره به منظور ایجاد راهبرد و برنامه‌ریزی‌های بلندمدت و سیاست‌گذاری و فرهنگ‌سازی در حوزه مدیریت مخاطره است. لذا بهره‌برداری از استاندارد ISO 31000 به منظور مدیریت راهبردی کلیه مخاطره‌های سازمان که شامل مخاطره‌های امنیت اطلاعات نیز است، مفید خواهد بود.

۱-۱۰. مدیریت مخاطره امنیت اطلاعات

مدیریت مخاطره امنیت اطلاعات که زیربنای سیستم مدیریت امنیت اطلاعات به شمار می‌رود، فرآیندی است برای درک مخاطره‌های بالقوه و برنامه‌ریزی به منظور از بین بردن، کاهش اثر یا بهره‌برداری از این مخاطره‌ها. فرآیند مدیریت مخاطره امنیت اطلاعات می‌تواند شامل گام‌های گوناگونی باشد. مدل‌ها، استانداردها و فرآیندهای گوناگونی بدین منظور طراحی و پیشنهاد شده است که در فصل آینده شرح داده خواهد شد، اما در یک برداشت اولیه و کلی از استاندارد ISO/IEC 27005:2011، فرآیند مدیریت مخاطره امنیت اطلاعات شامل سه گام اساسی شناسایی مخاطره، تحلیل مخاطره و مقابله با مخاطره است. در ادامه هر یک از مراحل فوق به تفکیک شرح داده شده است.

- **شناسایی مخاطره**[2]

هدف از شناسایی مخاطره، تعیین عواملی است که می‌توانند علت زیان بالقوه باشند و اینکه چگونه، کجا و چرا زیان ممکن است رخ دهد. گام‌های زیر در شناسایی مخاطره وجود دارند:

- شناسایی و ارزش‌گذاری دارایی‌های اطلاعاتی؛
- شناسایی تهدیدها؛
- شناسایی کنترل‌های موجود؛
- شناسایی آسیب‌پذیری‌ها؛ و
- شناسایی پیامدها.

[1] Enterprise Risk Management (ERM)

[2] Risk Identification

- **تحلیل مخاطره**[1]

تحلیل مخاطره با توجه به سطح جزئیات موردنظر، میزان حیاتی بودن دارایی‌ها، گستره آسیب‌پذیری‌های شناخته شده و نیز رخدادهای دربرگیرنده سازمان انجام می‌شود. روش تحلیل مخاطره می‌تواند کمّی و یا کیفی و یا تلفیقی از هر دو باشد. این مرحله شامل گام‌های زیر است:

- ارزیابی پیامدها؛
- سنجش احتمال رخداد؛ و
- تعیین سطح مخاطره.

- **مقابله با مخاطره**[2]

در این مرحله کنترل‌هایی جهت مقابله با مخاطره امنیت اطلاعات انتخاب می‌شوند. به منظور مقابله با مخاطره چهار رویکرد وجود دارد که عبارتند از:

- کاهش مخاطره؛
- حفظ مخاطره؛
- اجتناب از مخاطره؛ و
- انتقال (اشتراک) مخاطره.

۱-۱۱. چالش‌های مطرح در فرآیند مدیریت امنیت اطلاعات

امنیت اطلاعات همانند گذشته اهمیت دارد، اما چالش‌های تعیین عوامل مؤثر در عدم امنیت اطلاعات ماهیت پیچیده‌ای دارد. برای دستیابی به سطح مطلوبی از محافظت در برابر تهدیدها و فراهم‌کردن سازوکارهای لازم جهت محافظت از دارایی‌ها و دانش سازمان، طیف گسترده‌ای از رویکردها و روش‌های مدیریتی در دهه‌های گذشته توسعه یافته است که به تفصیل در فصل دوم و سوم مورد بررسی قرار خواهند گرفت. اما در حالت کلی مدیریت امنیت اطلاعات بر دو محور ۱) مدیریت دارایی‌های اطلاعاتی و ۲) مدیریت مخاطرات امنیت اطلاعات استوار است.

- *مدیریت دارایی‌های اطلاعاتی*[3]: برای هدایت، هماهنگی و کنترل فعالیت‌های مدیریت دارایی توسط یک سازمان استفاده می‌شود. این سیستم می‌تواند روش‌های بهتر کنترل مخاطره را فراهم کند و اطمینان دهد که اهداف مدیریت دارایی به طور منسجم حاصل خواهد شد.
- *مدیریت مخاطرت امنیت اطلاعات*: به شکل ویژه می‌تواند بخشی از فرآیند مدیریت مخاطره سازمانی باشد و یا به صورت جداگانه اجرا شود. فعالیت‌های مدیریت مخاطره امنیت اطلاعات معمولاً شامل شناسایی مخاطره‌ها، پیاده‌سازی خط‌مشی‌های مناسب و کنترل‌های مرتبط، ارتقاء، آگاهی‌رسانی، همچنین پایش و سنجش اثربخشی کنترل و خط‌مشی است.

در فرآیند مدیریت مخاطره امنیت اطلاعات چالش‌های گوناگونی ممکن است ایجاد شده که در ادامه مهم‌ترین آنها شرح داده می‌شوند:

[1] Risk analysis
[2] Risk Treatment
[3] Information Asset Management (IAM)

۱-۱۱-۱. چالش نخست: فهرست سیاهه دارایی و اقدامات متقابل

دارایی اطلاعاتی به مجموعه‌ای از اطلاعات فیزیکی (کاغذ، نامه، و غیره) و اطلاعات غیرفیزیکی (داده) گفته می‌شود که برای سازمان دارای ارزش است. دارایی‌های اطلاعاتی به سه دسته کلی تقسیم می‌شوند:

- خود اطلاعات: شامل کلیه اطلاعات فیزیکی (اسناد و مدارک) و دیجیتالی (فایل‌ها؛ پایگاه‌های‌داده، و غیره)؛
- تجهیزات مدیریت و نگهداری اطلاعات: شامل سیستم‌های‌عامل، نرم‌افزارها، سرورها و رایانه‌ها و همچنین تجهیزات زیربنایی مانند تجهیزات سرمایش، اطفاء حریق و غیره؛
- تجهیزات انتقال اطلاعات: شامل تجهیزات ارتباطی (سوئیچ‌ها، رادیوها، تجهیزات بی‌سیم، و غیره)

یکی از مهم‌ترین مباحثی که در فرآیند مدیریت امنیت اطلاعات در سازمان‌ها مطرح است، بحث مدیریت امنیت دارایی‌های اطلاعاتی است. هدف مدیریت امنیت اطلاعات در یک سازمان، حفظ سرمایه‌های (نرم‌افزاری، سخت‌افزاری، اطلاعاتی، ارتباطی و نیروی انسانی) سازمان در مقابل هرگونه تهدید (اعم از دسترسی غیرمجاز به اطلاعات، خطرات ناشی از محیط و سامانه و خطرات ایجاد شده از سوی کاربران) است که برای دستیابی به این هدف به برنامه منسجمی نیاز دارد.

مشکلات مربوط به شناسایی مناسب فهرست سیاهه دارایی‌های فناوری اطلاعات در ادبیات دانشگاهی و همچنین صنعت به عنوان یک مسئله مطرح شده است. هر چیزی که به هر نوعی به مؤلفه‌های فناوری اطلاعات متصل باشد، باید به عنوان دارایی در نظر گرفته شود، مهم نیست که یک آیتم فیزیکی مانند رایانه، سرور، یک سند، یک برنامه‌نویس باشد، یا آیتم غیرمشهود مانند فایل‌ها، کد منبع، پایگاه‌داده یا برنامه‌های نرم‌افزاری. پویایی و تغییر در محیط فناوری اطلاعات پیچیدگی این مشکل را افزایش می‌دهد. تجزیه و تحلیل همیشه به همان اندازه خوب است که داده‌های مبتنی بر آن خوب است. بنابراین بیشتر رویکردهای مدیریت مخاطره بدون فهرست قابل اعتماد سیاهه دارایی‌ها، کاربرد کمی دارند.

دو راهکار امیدوارکننده در آثار پیشین (Montesino and Fenz 2011; Fenz, Ekelhart and Weippl 2008) مورد بحث قرار گرفته است که در آنها نویسندگان پیشنهاد می‌کنند از ابزارهای خودکار برای ضبط وضعیت زیرساخت فناوری اطلاعات از طریق شبکه و تهیه کنترل و قوانینی برای شناسایی وضعیت امنیتی استفاده شود. در مدیریت مخاطره باید دو نوع دارایی برای فهرست سیاهه مد نظر قرار گیرند:

۱) دارایی‌هایی که باید محافظت شوند (مانند داده‌های مشتری، امکانات تولید)؛ و
۲) دارایی‌هایی که مأموریت یک اقدامات متقابل را انجام می‌دهند (مانند اسکنرهای بدافزار، سیستم‌های تشخیص نفوذ).

در مورد دارایی‌هایی که برای سازمان با ارزش هستند، فهرست سیاهه باید توسط مالکان داده و برنامه‌ها تهیه شود (برای مثال ذینفعان کسب‌وکار، مالکان فرآیند، راهبران فناوری اطلاعات). این فرآیند سیاهه‌نویسی باید عمدتاً به صورت دستی انجام شود، امّا رویکردهای مبتنی بر فرآیند نیز از قبل وجود دارد (برای مثال تعیین اهمیت مبتنی بر فرآیند ارائه شده توسط «فنز» و همکارانش) (Fenz, Ekelhart and Neubauer 2009). در نوع دوم دارایی‌ها، هنگامی که سخن از سیاهه اقدام متقابل می‌شود، باید سه حوزه مورد توجه قرار گیرد:

۱) اقدامات متقابل فیزیکی: قفل، درب‌های امنیتی، نگهبانان و غیره؛
۲) اقدامات متقابل فنی: فایروال‌ها، سیستم‌های نظارتی، اسکنرهای بدافزار و غیره؛ و
۳) اقدامات متقابل سازمانی: خط‌مشی‌های پشتیبان‌گیری، خط‌مشی‌های بهره‌برداری از دستگاه تلفن‌همراه، و غیره.

در حالی‌که یک درجه خودکاری پایین برای اقدامات متقابل فیزیکی و سازمانی وجود دارد، می‌توان از ابزارها و تکنیک‌های موجود برای افزایش کارایی سیاهه اقدامات متقابل فنی استفاده کرد (برای مثال ابزارهای اسکن شبکه، راهکارهای سیاهه نرم‌افزاری

یا راهکارهای مدیریت نرم‌افزار خاص مانند خدمات به‌روزرسانی سرور ویندوز[1]). برای فهرست سیاهه کارآمد، اقدامات متقابل سازمانی مانند خط‌مشی‌ها، اقدامات بیشتری به شرح زیر نیاز است:

- شناسایی الگوهای معمولی/ طرح‌بندی‌ها/ کلمه‌های کلیدی خط‌مشی‌های مربوط به امنیت؛
- توسعه ابزاری که از مشخصات خط‌مشی به منظور شناسایی خودکار خط‌مشی‌های احتمالی در مخازن داده مرکزی شرکت مانند جریان‌های شبکه استفاده می‌کند؛ و
- ارزیابی اثربخشی روش منتخب تهیه فهرست سیاهه اقدامات متقابل سازمانی.

۱-۱۱-۲. چالش دوم: تخصیص ارزش دارایی

تجزیه و تحلیل و ارزش‌گذاری صحیح دارایی‌ها نه تنها اهمیت دارایی برای سازمان را نشان می‌دهد، بلکه روابط و وابستگی‌های بین این دارایی با دیگر دارایی‌های سازمان را نیز مشخص می‌کند. در واقع، ارزش هر دارایی ترکیبی از میزان اهمیت هر یک از مؤلفه‌های (محرمانگی، صحت، دسترس‌پذیری) برای آن دارایی است که از مجموع مقادیر اختصاص‌یافته به هر سه مؤلفه محاسبه می‌شود.

افزون بر مشکلات شناسایی دارایی‌هایی که پیش‌تر نیز مورد بحث قرار گرفت، ارزیابی ارزش دارایی‌ها نیز دشوار است. تعریف یک ارزش برای آیتم‌های نسبتاً کوچک (برای نمونه، پست‌الکترونیکی) تقریباً غیرممکن است. افزون بر این، شناسایی مقادیر گوناگون جدا از ارزش‌های پولی -مانند خسارت‌های ناشی از خرابی سیستم- در ارزیابی دشوار است. خسارت و زیان ممکن است نه تنها به ضرر پولی محدود شود، بلکه می‌تواند بر تصویر سازمان (و همچنین اعتماد مشتری به سازمان) یا توانایی رقابتی تأثیر بگذارد. از بین رفتن تصویر سازمان ممکن است به حدی جدی باشد که حتی سازمان قادر به بازیابی کامل نباشد.

«فنز» و همکارانش، این مسئله را با بهره‌برداری از روش تعیین اهمیت منابع مبتنی بر فرآیند تجاری ارائه می‌دهند که مدیریت مخاطره امنیت اطلاعات را با ابزاری کارآمد و قدرتمند برای استخراج ارقام اهمیت واقعی منابع صرفاً از فرآیندهای تجاری موجود فراهم می‌کند (Fenz, Ekelhart, and Neubauer 2009). ارزیابی انجام شده نشان داده است که نتایج محاسبه روش توسعه‌یافته آنها با نتایج به‌دست‌آمده در ارزیابی‌های سنتی مبتنی بر کارگاه‌های آموزشی مطابقت دارد.

۱-۱۱-۳. چالش سوم: پیش‌بینی‌های شکست خورده از مخاطره

تغییر ماهیت مخاطره‌ها باعث شده است که دانستن اینکه کدام دارایی مورد توجه یک مهاجم قرار خواهد گرفت عملاً غیرممکن شود. یک دارایی خاص که امروزه نادیده گرفته می‌شود، ممکن است برای یک مهاجم در آینده بسیار جالب باشد. این امر مخاطره‌ها را به حوزه‌های غیرمنتظره سازمانی تبدیل می‌کند. بنابراین جدا از پیش‌بینی‌های مخاطرها، به نظر می‌رسد تعریف مخاطره نیز یک مشکل است. برخی مخاطره را عدم اطمینان نتیجه مثبت و منفی می‌دانند، و برخی دیگر تمایل دارند بیشتر به تکرار و بزرگی خسارت و ضرر فکر کنند، که تعریف بسیار رایج‌تری است. اما هنوز هم خطرِ قرار دادن مخاطرات امنیتی منفی (ضرر) در زمره مخاطرات مثبت (سود) و پذیرش ضرر/ خسارت احتمالی وجود دارد. درست همانند مدیریت امنیت اطلاعات که یک عرصه چند تخصصی است، راهکار یک مشکل نیز در زمینه‌های گوناگون نهفته است و باید به مشکلات جزئی با ریشه‌های گوناگون تقسیم شود. روش فرض مخاطره به توانایی پیش‌بینی محتمل‌ترین و ممکن‌ترین تهدید و مخاطره وابسته است. با این حال، پیش‌بینی کامل مخاطرات ناشناخته، بخشی از مجموعه ابزاری نیست که یک تحلیلگر مخاطره در دست دارد. مفروضات مخاطره می‌تواند از معرفی دیگر مدل‌های مخاطره که به طور ویژه برای فناوری اطلاعات طراحی شده‌اند، و همچنین درنظر گرفتن جنبه‌های منحصر به فرد

[1] Windows Server Update Service (WSUS)

این زمینه بسیار سود ببرد. نخستین گام‌ها در این جهت پیش‌تر توسط پژوهشگران انجام شده است (Bojanc 2012; Bojanc and Jerman-Blažič 2008; Vose 2008; Sonnenreich, Albanese and Stout 2006).

۱-۱۱-۴. چالش چهارم: اثر اطمینان بیش از حد

«آرهی» و همکارانش در پژوهش خود دربارهٔ زمینه جالب رفتارهای انسانی و فرضیه‌های مخاطره انسانی، در خصوص اینکه مدیران تمایل دارند تخمین مخاطره را خیلی خوش‌بینانه فرض کنند، بحث کردند (Rhee, Ryu and Kim 2012). در کنار اینکه تصمیم‌گیرندگان در خصوص مخاطره با منابع محدودی روبرو هستند، این اثر اطمینان بیش از حد به یک نگرش کلی مبهم نسبت به تشریفات منجر می‌شود. اثر اطمینان بیش از حد موجب انحراف نتایج ارزیابی مخاطره، احتمال، تهدید و اثری می‌شود که توسط مالکان داده‌ها و برنامه‌ها در فرآیند مدیریت مخاطره انجام می‌شود. «هوبارد» آزمون‌های درجه‌بندی (کالیبراسیون) را برای تصحیح اثر اطمینان بیش از حد در ارزیابی‌ها پیشنهاد کرده است. آزمون‌های درجه‌بندی شامل تعدادی پرسش ساده بدیهی است و مخاطب مجبور است به این پرسش‌ها پاسخ دهد و باید برای هر یک از پاسخ‌های داده شده، درصد اطمینان را ارائه دهد. تفسیر درستی پاسخ‌های داده شده و مقادیر اطمینان باعث می‌شود که مخاطب بتواند سطح اطمینان خود را در پیش‌بینی‌ها بررسی کند (Hubbard 2009).

۱-۱۱-۵. چالش پنجم: اشتراک دانش

به اشتراک‌گذاری دانش در بین سازمان‌ها موجب کاهش هزینه‌های کسب دانش، تقویت هم‌افزایی بین سازمان‌ها، بهبود توانایی نوآوری و ارتقاء رقابت‌پذیری کلی سازمان‌های شرکت‌کننده می‌شود (Fang, Liang and Jia 2011). در حوزه امنیت اطلاعات، تبادل دانش بین متخصصان از آن جهت مطلوب است که از ایجاد چندباره و تکراری برنامه‌های امنیتی یکسان توسط افراد/ سازمان‌های مستقل جلوگیری شود. چنین مبادله‌ای همچنین می‌تواند به برنامه‌های امنیتی با کیفیت بالاتر منجر شود، زیرا رویکردهای موجود می‌توانند به جای اینکه چرخ امنیتی را دوباره اختراع کنند، آن را توسعه دهند.

«فِنز» و «فِلِدی» چگونگی اشتراک دانش ماشین‌خوان امنیت اطلاعات سازمان‌های گوناگون را بر پایهٔ پورتال وب با استفاده از «وب ـ پروتژ»[1] بررسی کردند. آنها نشان داده‌اند که با بهره‌برداری از هستی‌شناسی‌ها می‌توان دامنه امنیت اطلاعات را در قالب انسانی و دستگاه‌خوان مدل‌سازی، ذخیره و ویرایش کرد (مانند محاسبات مخاطره). ارزیابی پورتال وب آنها نشان داده است که مهمترین موضوع، ایجاد انگیزه در کاربران برای مشارکت در تبادل دانش است (Feledi and Fenz 2012). رویکرد اشتراک دانش دربارهٔ موضوع‌های مشترک مربوط به امنیت و مدیریت مخاطره، همان طور که توسط (Fenz and Ekelhart 2009; Fenz 2012; Feledi and Fenz 2012) ارائه شده است، می‌تواند تبادل فعال‌تر راهکارهای ایجاد شده را فراهم کند، اما نیاز به پژوهش‌های بیشتر دربارهٔ انگیزه‌های اجتماعی و اقتصادی و موانع اشتراک دانش امنیت اطلاعات دارد. تنها با ارائه مزایای واضح برای سازمان‌ها و افراد شرکت‌کننده، می‌توان برنامه‌های اشتراک دانش را برای منافع متقابل طولانی‌مدت شرکت‌کنندگان ایجاد کرد.

۱-۱۱-۶. چالش ششم: مخاطره در مقابل هزینه‌های تجاری

پیاده‌سازی اقدامات متقابل معمولاً در وهله نخست در نتیجه مدیریت مخاطره ایجاد می‌شود و اثربخشی فنی برای به حداقل رساندن مخاطرات درک شده برای دارایی‌های سازمان ایجاد می‌شود. اما غالباً از مقرون‌به‌صرفه بودن اقدامات متقابل غفلت می‌شود. هزینه‌های اقدامات متقابل نباید بیش از ضرر مورد انتظار یک دارایی باشد. هزینه‌های اقدامات متقابل شامل هزینه‌های توسعه (برای نمونه، هزینه‌های نصب)، هزینه‌های عملیاتی (برای نمونه، هزینه‌های تعمیر و نگهداری) و هزینه‌های پاسخ (برای نمونه، پرسنل لازم

[1] Web-Protégé

برای اجرای اقدامات متقابل) است (Lee et al. 2002). از سوی دیگر تعریف هزینه‌های ناشی از حملات موفقیت‌آمیز دشوار است، زیرا آنها به ضرر مالی محدود نمی‌شوند و می‌توانند مسئول از دست دادن تصویر، اعتماد و دیگر ارزش‌های غیرفیزیکی سازمان‌ها باشند (Cavusoglu, Mishra and Raghunathan 2004).

تصمیمات مدیریتی باید مبتنی بر داده‌های یکپارچه، دانش و تجربه در زمینه مدیریت سازوکارهای امنیتی باشد. از آنجا که بیشتر مراجع مدیریتی فاقد این نوع دانش تخصصی هستند، یا یک متخصص مشاوره خارجی لازم است یا الگوی داده وضعیت امنیتی باید به گونه‌ای ساده باشد که حتی یک فرد بی‌تجربه قادر به تفسیر آن باشد. یکی از راه‌های تهیه این داده‌ها، معیارهای امنیتی است که می‌تواند به جنبه‌های گوناگون امنیت اطلاعات (اثربخشی کنترل‌های امنیتی یا کارایی عملیات) کمک کند (Jansen 2010).

با توجه به این ماهیت متنوع، معیارهای امنیتی در چندین دستهٔ فراگیر جای می‌گیرند که یک نمای کلی درباره سازگاری با الزامات امنیتی، اثربخشی کنترل‌های امنیتی و زمینه‌های بهبود ارائه می‌دهند. بیشتر رویکردهای مربوط به مدیریت مخاطره امنیت اطلاعات از این رویکرد پشتیبانی نمی‌کنند، زیرا تمایل اصلی آنها برای تبدیل به استانداردها، دستورالعمل‌ها و یا به‌روش‌های ملّی است. بنابراین، با توجه به سطوح گوناگون جزئیات، باید تمایزی بین روش‌های ارزیابی ایجاد شود. در یک طیف کلی که در یک سمت آن روش‌های عمومی و در سمت دیگر آن روش‌های دقیق هستند، سه روش مدیریتی، عملیاتی و فنی را می‌توان نام برد. در حالی که در یک روش مدیریتی دستورالعمل‌های کلی ارائه می‌شود، یک روش عملیاتی برنامه‌هایی برای اجرای کنترل معرفی می‌کند، و یک روش فنی دستورالعمل‌های ویژه‌ای را دربارهٔ جنبه‌های فنی، سازمانی، فیزیکی و انسانی ترویج می‌کند. مشکلی که دربارهٔ راهنماهای عمومی‌تر وجود دارد این است که اگر سازمان مجبور باشد برای یک مشکل نسبتاً عمومی راهکار بسیار مشخصی پیدا کند، تخمین هزینه‌های اجرای آن دشوار است. مزیت رویکردهای عمومی‌تر، توانایی آنها برای برآورد سطح بلوغ امنیتی سازمان به روش آسان و مطابقت با استانداردهای امنیتی خاص در صورت لزوم است. از طرف دیگر رویکردهای دقیق‌تر، تخمین هزینه را آسان‌تر می‌کنند، اما در آنها ارائه نمای کلی دربارهٔ میزان سازگاری با توجه به سطح بالای جزئیات می‌تواند کمرنگ شوند.

۱-۱۲. گزیدهٔ فصل

در این فصل در ابتدا در تشریح مفهوم امنیت بیان شد که اگر مجموعه شرایط به‌گونه‌ای باشد که داشته‌های موردنظر انسان سالم (صحیح) و از دید بیگانگان محرمانه بماند، از نظر انسان در چنین شرایطی امنیت برقرار است. سپس امنیت اطلاعات به معنای حفاظت از اطلاعات و مؤلفه‌های اصلی آن تعریف شد که سیستم‌ها، سخت‌افزارها، انباره‌ها و انتقال اطلاعات را در برمی‌گیرد. سپس حفاظت از محرمانگی، صحت و درستی و دسترس‌پذیری اطلاعات به عنوان ارکان امنیت اطلاعات معرفی شد. در ادامه سیر تکامل و پیشرفت امنیت اطلاعات در چهار موج فنی، مدیریتی، نهادینه‌سازی و حاکمیت امنیت اطلاعات مورد بحث قرار گرفت. در حالی که در موج نخست تمرکز بر مسائل فنی امنیت بود، در موج دوم تمرکز بر مسائل مدیریتی و استانداردسازی، در موج سوم بر ایجاد یک زیرساخت امنیت اطلاعات فنی و رویه‌ای و همچنین یک فرهنگ امنیت اطلاعات، و در موج چهارم بر حاکمیت امنیت اطلاعات به عنوان بخشی از حاکمیت سازمانی بود.

روند شکل‌گیری و توسعه امنیت اطلاعات موضوع بعدی مورد بحث در این فصل بود. بر این اساس مدیریت امنیت اطلاعات به عنوان یک چارچوب جامع، کامل و انطباق‌پذیر متشکل از برنامه‌های امنیتی و فرآیندها و رویه‌های مدیریتی معرفی شد که هدف نهایی آن تأمین و استمرار امنیت در فضای تبادل اطلاعات سازمان است. سپس مبتنی بر مفاهیم حوزه مخاطره سازمانی، مدیریت مخاطره امنیت اطلاعات به عنوان فرآیندی برای درک مخاطره‌های بالقوه حوزه امنیت اطلاعات و برنامه‌ریزی به منظور از بین بردن، کاهش اثر یا بهره‌برداری از این مخاطره‌ها معرفی شد. در انتها نیز چالش‌های موجود در فرآیند مدیریت امنیت اطلاعات در شش

حوزه ۱- فهرست سیاهه دارایی و اقدامات متقابل، ۲- تخصیص ارزش دارایی، ۳- پیش‌بینی‌های شکست خورده از مخاطره، ۴- اثر اطمینان بیش از حد، ۵- اشتراک دانش، و ۶- مخاطره در مقابل هزینه‌های تجاری معرفی و مورد تحلیل قرار گرفت.

به شکل کلی، باید گفت هر فعالیتی با مخاطره همراه است و انسان‌ها از زمان‌های بسیار دور به این مفهوم پی برده‌اند و به دنبال شناسایی عوامل و منابع آن هستند. از آنجاکه موضوع امنیت اطلاعات در سازمان‌ها بهره‌برداری از سیستم‌های امنیت اطلاعات را با چالش مخاطره مواجه کرده است، چنانچه فرآیند مدیریت مخاطره در این سیستم‌ها به درستی انجام شود، می‌توان به اجرای موفق آن دست یافت. ارزیابی و مدیریت مخاطرات وظایفی از قبیل تحلیل، ارزیابی و آگاهی‌رسانی را در بر می‌گیرد. مدیریت مخاطره، با بهره‌برداری از تشخیص و فهم تهدیدها و آسیب‌پذیری‌ها، ارزیابی، اولویت‌بندی، پیاده‌سازی کنترل‌ها و آگاهی‌رسانی در این زمینه، بهترین راه‌کار را دربارهٔ مواجهه با تهدیدهای بالقوه رایج پیرامون دارایی‌های سازمان ارائه می‌دهد. با این اوصاف، تحلیل و مدیریت مخاطره را می‌توان به عنوان هسته مرکزی از فرآیند مدیریت راهبردی امنیت سازمان محسوب کرد. در بسیاری از موارد و زمانی که سازمان با یک چالش جدی در حوزه امنیت اطلاعات مواجه است، می‌تواند با انتخاب و بکارگیری رویکرد مناسب از شرایط بحرانی خارج شده و یا نیاز امنیتی خاص خود را در آن مقطع مرتفع سازد. از این‌رو به‌کارگیری روش‌های مدیریت و ارزیابی مخاطره می‌تواند تأثیر شگرفی بر شیوهٔ سازماندهی فعالیت‌های سازمان‌ها در زمینه امنیت اطلاعات داشته باشد که در فصل دوم به معرفی روش‌های موجود برای شناسایی و ارزیابی میزان مخاطره در سازمان‌ها خواهیم پرداخت.

فصل دوم

روش‌های ارزیابی مخاطره

۲–۱. مقدمه

هنگامی که در یک سازمان و یا جامعه سخن از مخاطره به میان می‌آید، منظور احتمال از دست دادن چیز ارزشمندی مانند امنیت، سرمایه، رفاه و سلامتی است. غالباً، در روند خطر کردن، افراد خودشان انتخاب می‌کنند که با موقعیت‌هایی که هنوز قطعی نشده و امکان پیش‌بینی نتایج نهایی در آنها وجود ندارد مواجه شده و البته برای پیامدهای آن که شدت‌شان مشخص نیست آمادگی‌های لازم را پیدا کنند.

همان طور که در فصل پیش اشاره شد، مخاطره احتمال زیان یا پیامدهای ناخوشایند و ناخواسته است که انجام یک فعالیت یا گرفتن یک تصمیم را به همراه خود دارد. تقریباً همه فعالیت‌ها و تصمیم‌های انسان دارای مخاطره است. از آنجایی که هیچ‌کس از آینده خبر ندارد همه آدم‌ها کوشش می‌کنند تصمیم‌ها و فعالیت‌هایی که انجام می‌دهند مخاطره کمتر یعنی احتمال زیان کمتری داشته باشند.

ارزیابی مخاطره به معنای بررسی آسیب‌پذیری‌ها، تهدیدها و پیامدهای ناخوشایند بر سر راه یک پروژه یا سازمان است. این موانع و بحران‌ها باید قبل از بُروز شناسایی و تحلیل شوند. باید تا جایی که ممکن است از رخ دادن آن جلوگیری و یا هنگام بروز، راه‌کارهای مناسبی که از قبل طراحی شده‌اند اجرا شوند. به این شکل، مسیری کنترل شده برای عبور از بحران خواهیم داشت که در نهایت با کمترین زیان یا پیامدهای ناخوشایند روبرو خواهیم بود. البته ارزیابی مخاطره می‌تواند کار پیچیده‌ای باشد، تا جایی که گاهی نیاز است جزئیات اطلاعات مانند برنامه‌ها، اطلاعات مالی، قوانین امنیتی، پیش‌بینی فروش و بازاریابی و اطلاعات دیگر مرتبط تحلیل شود. به هر روی، بررسی مخاطره یکی از ابزارهای کلیدی یک سازمان یا پروژه است که باعث بهبود عملکرد آن می‌شود.

ارزیابی مخاطره می‌تواند در سطح جزئی ارزیابی مخاطره پروژه و در سطح کلی ارزیابی مخاطره مجموعه یک سازمان را در بر گیرد. همچنین ارزیابی مخاطره سرمایه‌گذاری به عنوان یکی از اصلی‌ترین زیرشاخه‌های مدیریت مخاطره هم در سطح جزئی و هم در سطح کلی قابل استفاده است. بررسی‌های انجام شده نشان می‌دهد در طول دهه‌های گذشته روش‌های متفاوتی به منظور ارزیابی مخاطره در مفهوم کلان آن توسعه یافته‌اند. در این فصل برجسته‌ترین این روش‌ها معرفی و مورد تحلیل قرار می‌گیرند.

۲–۲. روش‌های ارزیابی مخاطره

به شکل کلی، فنون تحلیل و ارزیابی مخاطره در شکل عمومی آن را می‌توان با توجه به ویژگی‌هایی، از جمله فرآیند استدلال (قیاسی یا استقرایی)، محدوده/ دامنه تحلیل (شناسایی یا ارزیابی)، و ماهیت فرآیند و نتایج (کیفی، کمّی و یا ترکیبی) طبقه‌بندی کرد (Abie 2012). همچنین با توجه به پژوهش صورت گرفته توسط (Xiaolin et al. 2008) می‌توان آنها را در قالب دو روش سنتی

و تازه ارزیابی مخاطره دسته‌بندی کرد: ۱) روش‌های سنتی ارزیابی مخاطره از جمله FTA، HAZOP، FMECA، COSO و غیره و ۲) روش‌های تازه از جمله CORAS، EBIOS، CRAMM، FRAAP. در این بخش مروری بر روی روش‌های ارزیابی مخاطره به شکل کلی (و نه مخاطره امنیت اطلاعات) خواهیم داشت.

۲-۲-۱. روش ارزیابی مخاطره آنالوگ (ARA)

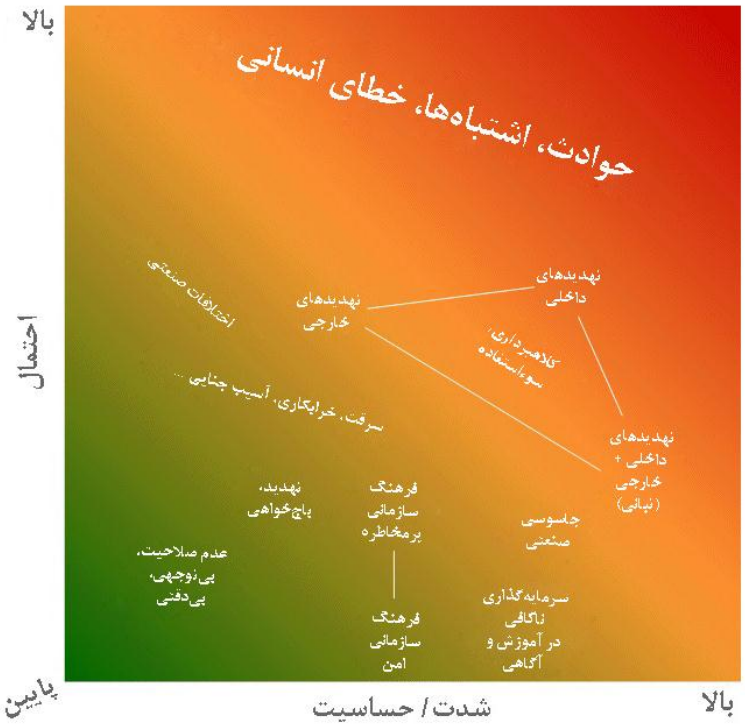
این روش ارزیابی توسط «گری هینسون»[1] ابداع شده است. **ارزیابی مخاطره آنالوگ**[2] یا به اختصار (ARA) معرف یک روش ساده برای تحلیل، گزارش‌دهی، مقایسه و بررسی مخاطره‌های سازمان بر پایهٔ احتمال وقوع و تأثیر مخاطره است. این روش ارزیابی مخاطره در قالب (**شکل ۲-۱**) به تصویر کشیده شده است. هدف اصلی این روش آن است که توجه مدیران را برای سرمایه‌گذاری امنیتی در بخش‌های قرمز رنگ (سمت راست بالای شکل) جلب کند (Hinson 2013). در حقیقت این بخش‌ها معرف حوزه‌هایی هستند که سازمان در آنها ضعف امنیتی بیشتری دارد. دستورالعمل‌های ده‌گانه ذیل، چگونگی بهره‌برداری از این روش را بیان می‌کنند:

۱. با بهره‌برداری از تجربه خود، آمار و ارقام حوادث، دیگر تجزیه و تحلیل‌های مخاطره، جلسه‌های طوفان مغزی و خیره شدن به **گوی بلورین**[3]، مجموعه‌ای از مخاطره‌ها، حوادث یا نگرانی‌های احتمالی را در حوزه مورد علاقه خود شناسایی کنید؛
۲. برای هر کدام احتمال تقریبی وقوع آن را نسبت به سایرین تخمین بزنید؛ (تعیین موقعیت بر روی محور احتمال)
۳. همچنین، اگر چنین اتفاقی رخ داد، میزان خسارت وارد شده را دوباره نسبت به دیگران تخمین بزنید؛ (تعیین موقعیت بر روی محور دقت)
۴. هر یک از موارد را در موقعیت‌های مناسب بر روی نمودار/ گراف ترسیم کنید؛
۵. نمودار/ گراف اولیه را در یک جلسه یا کارگاه آموزشی مطرح و دربارهٔ آن با مدیریت بحث کنید، موارد نشان داده شده را توصیف کنید، توضیح دهید که چرا فکر می‌کنید آنها در جای مناسب خود قرار دارند، موارد موجود بر روی نمودار/ گراف را با یک‌دیگر مقایسه کنید، در صورت وجود اجماع یا فشار از طرف گروه موارد را تغییر دهید، موارد قابل توجه جدیدی که در بحث مطرح می‌شوند، در صورتی که منطقی به نظر می‌رسند، با موارد دیگر ترکیب یا حذف کنید. موارد مرتبط را در صورتی که به این موضوع کمک می‌کنند در یک گروه قرار دهید و یا بین آنها ارتباط برقرار کنید؛
۶. پس از اینکه همه به طور منطقی نمودار/ گراف را پذیرفتند، به بحث دربارهٔ کارهایی که باید در پاسخ ارائه شود، بپردازید. بر روی هر چیزی که در بخش قرمز رنگ وجود دارد یا موارد دیگری که ممکن است به این سو گرایش داشته باشند تأکید کنید، و به دنبال راهکارهای خلاقانه باشید، مانند کنترل‌هایی که پاسخگوی چندین مورد هستند یا فرصت‌هایی برای جلوگیری یا انتقال مخاطره‌ها به اشخاص ثالث؛
۷. یک طرح/ برنامه عملی ایده‌آل همراه با اولویت‌ها، تاریخ‌های هدف و افراد به نام که مسئولیت رهبری اقدام‌های ناشی را می‌پذیرند تهیه کنید؛
۸. در مورد طرح/ برنامه عملیاتی به اتفاق نظر برسید و کار را آغاز کنید (اگر هنوز در حال انجام نیست)؛
۹. اقدام‌های لازم را ردیابی و هدایت کنید، همان طور که پیشرفت می‌کنید، موقعیت‌ها و ماهیت موارد بر روی گراف/ نمودار را تغییر دهید؛ و
۱۰. هر از چند گاهی برای بررسی پیشرفت دوباره جلسه تشکیل دهید و همین فرآیند را برای دیگر حوزه‌های مخاطره نیز اعمال کنید.

---

[1] Grey Hinson
[2] Analog Risk Assessment (ARA)
[3] Crystal-Ball-Gazing

بهره‌برداری از این روش نیازمند هیچ‌گونه برنامه یا روش‌شناسی خاص و دوره‌های آموزشی پرهزینه و گران قیمت نیست، تیم کِرَکی[1] از مشاوران وجود ندارد و حتی داشتن رایانه نیز اختیاری است. از دیگر مزیت‌های برتر روش «ARA» می‌توان به سادگی، سرعت و مقرون‌به‌صرفه بودن آن اشاره کرد. یکی از ویژگی‌های برتر روش «ARA» این است که می‌تواند برای اکثر موارد -نه همه انواع مخاطره- ازجمله مخاطره‌های مالی، سیاسی، بازار، ایمنی و سلامت، راهبردی و غیره مورد استفاده قرار گیرد.



شکل ۲-۱. روش ارزیابی امنیتی آنالوگ برای امنیت رایانامه در سازمان، (Hinson 2013)

۲-۲-۲. چارچوب اهداف کنترلی برای اطلاعات و فناوری‌های مرتبط با آن (COBIT)

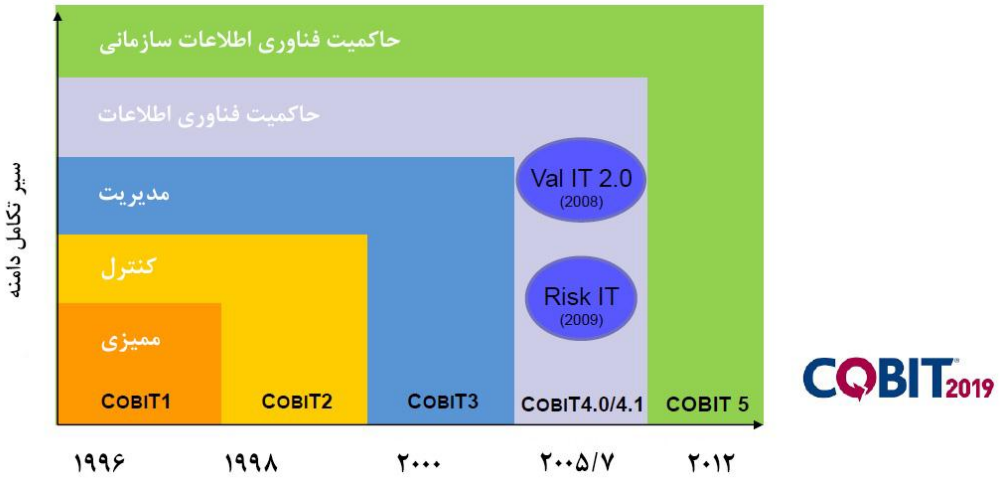
چارچوب اهداف کنترلی برای اطلاعات و فناوری‌های مرتبط با آن[2] یا به اختصار «COBIT» به عنوان کارآمدترین مدل برای پیاده‌سازی و ممیزی راهبری فناوری اطلاعات مطرح است. چارچوب «COBIT»، مجموعه‌ای از به‌روش‌ها در حوزه ارزیابی و کنترل فناوری اطلاعات است که توسط **انجمن نظارت و کنترل سیستم‌های اطلاعاتی**[3] (ایساکا) و **سازمان راهبری فناوری اطلاعات**[4] (آی.تی.آی.جی.) در سال ۱۹۹۶ میلادی ارائه شد (ISACA 2012) تا مدیران، چارچوبی برای طراحی برنامه راهبردی فناوری اطلاعات، معماری اطلاعاتی، نرم‌افزارها و سخت‌افزارهای نیاز فناوری اطلاعات، حصول از تداوم خدمات فناوری اطلاعات و کنترل عملکرد سیستم‌های فناوری اطلاعات سازمان خود در اختیار داشته و با کمک این ابزارها به تصمیم‌گیری و سرمایه‌گذاری‌های مرتبط با فناوری اطلاعات بپردازند.

«COBIT» چارچوبی برای توسعه، پیاده‌سازی، پایش و بهبود مدیریت فناوری اطلاعات بوده و هدف اساسی آن فراهم آوردن زبانی مشترک برای مدیران اجرایی در راستای اهداف و نتایج آنها است. این چارچوب، حاکمیت فناوری اطلاعات را به عنوان ساختاری از ارتباطات و فرآیندها در جهت هدایت و کنترل سازمان، به منظور دستیابی به اهداف سازمان، به وسیله افزایش ارزش در حین متوازن‌سازی مخاطره در مقابل عایدی فناوری اطلاعات و فرآیندهایش تعریف می‌کند.

---

[1] Crack Team
[2] Control Objectives for Information and Related Technology (COBIT)
[3] Information Systems Audit And Control Association (ISACA)
[4] IT Governance Institute (ITGI)

نخستین نسخه از «COBIT» توسط سازمان راهبری فناوری اطلاعات در سال ۱۹۹۶ میلادی با هدف ممیزی فناوری اطلاعات و یا نظارت بر بخش فناوری اطلاعات عرضه شد. به طور معمول ممیزی از خارج از بخش یا سازمان انجام می‌پذیرد و جهت حصول تضمین برای سرمایه‌گذاران و ذینفعان خارجی است و نتایج آن بیشتر مد نظر سرمایه‌گذاران (سهام‌داران)، مدیرعامل و هیأت رئیسه است. در واقع، این نسخه ابزاری جهت ممیزها است و فرآیند ممیزی معمولاً در بازه‌هایی خاص (برای مثال سالیانه) انجام می‌شود. در سال ۱۹۹۸ میلادی و در نسخه دوم «رهنمودهای مدیریتی» به آن افزوده شد که علاوه‌بر بحث‌های ممیزی، مباحث کنترل را نیز دربردارد و شاخص‌های کنترلی را نیز برای سازمان در بخش فناوری اطلاعات ارائه داده است. مانند شاخص‌های تعداد کاربران، میزان ذخیره‌سازی و غیره. به طور معمول کنترل به صورت درون سازمانی و جهت اطمینان مدیریت است. مباحث کنترلی معمولاً به طور لحظه‌ای و روزانه مد نظر است. در سال ۲۰۰۰ میلادی، نسخه سوم به صورت کامل‌تری ارائه شد و در سال ۲۰۰۳ میلادی، یک نسخه اینترنتی در دسترس قرار گرفت. این نسخه مدیریت و اجرای فناوری اطلاعات را در سازمان هدف‌گذاری کرد و شرح کار مدیران فناوری اطلاعات و دستورالعمل‌های مدیریتی را دربردارد. در دسامبر سال ۲۰۰۵ میلادی، نسخه اولیه چاپ چهارم با افزودن بخش نظام راهبری فناوری اطلاعات عرضه شد و در ماه مه ۲۰۰۷ میلادی نسخه تجدیدنظر شده آن، یعنی نسخه ۴/۱ چاپ شد. در واقع، از سال ۲۰۰۵ میلادی به بعد، نسخه‌های متفاوتی از (COBIT-4) ارائه گردید و به طور شفاف و کامل راهبری فناوری اطلاعات را هدف قرار داده است. این نسخه افزون بر مدیران فناوری اطلاعات مباحثی را نیز جهت مدیران ارشد دربردارد. نسخه (COBIT-5) برای ارائه در سال ۲۰۱۲ میلادی زمان‌بندی شده بود که پس از ارائه پیش‌نویس آن در سال ۲۰۱۱، در آوریل سال ۲۰۱۲ میلادی و پس از به‌روزرسانی ارائه شد. (COBIT-5) به یکپارچگی چارچوب‌های (COBIT 4.1)، چارچوب (Val IT 2.0) و چارچوب (RISK IT) می‌پردازد و همچنین، به میزان درخورتوجهی الگوی کسب‌وکار برای امنیت اطلاعات و چارچوب اطمینان‌بخشی فناوری اطلاعات را ترسیم می‌کند. در نهایت، نسخه ۲۰۱۹ چارچوب «COBIT» به عنوان آخرین نسخه این چارچوب در سال ۲۰۱۹ تحت عنوان «COBIT 2019» منتشر گردید. این نسخه تحولی در نسخه قبلی آن یعنی (COBIT-5) ایجاد کرده است و آخرین پیشرفت‌های اثرگذار مرتبط با اطلاعات و فناوری در سازمان‌ها به آن اضافه شده است. آخرین نسخه «COBIT» بسیار منعطف‌تر از نسخه قبلی شده است و اجازه می‌دهد تا بر پایهٔ نیاز سیستم حاکمیت به صورت کامل پیاده‌سازی شود و یا بر پایهٔ نیازمندی‌ها و رویکرد حل مسأله بخشی را که بیشترین اولویت را دارد، عملیاتی گردد. (**شکل ۲-۲**) تاریخچه چارچوب «COBIT» را نشان می‌دهد.



شکل ۲-۲. تاریخچه چارچوب «COBIT» (ISACA 2012)

این چارچوب معرف یک مدل فراگیر و جامع برای ارزیابی امنیتی سازمان است. این چارچوب ارائه‌گر پشتیبان برای پیاده‌سازی سیستم‌ها یا فرآیندهای صحیح حکمرانی فناوری اطلاعات است که کنترل‌های امنیتی را دربر می‌گیرد. «COBIT» به طور گسترده توسط ناظران فناوری اطلاعات و "قانون ممیزی حسابری، مسئولیت‌پذیری و شفافیت" مورد استفاده قرار می‌گیرد (ISO 2017).

این چارچوب برای مدیران، ممیزان و کاربران فناوری اطلاعات مجموعه‌ای از سنجه‌ها، معیارها، فرآیندها و به‌روش‌های قابل قبولی را ارائه می‌کند تا به آنان در افزایش سود حاصله از بکارگیری فناوری اطلاعات و توسعه کنترل و راهبری فناوری اطلاعات کمک کند. در واقع، این چارچوب به مدیران، ممیزان و کاربران این امکان را می‌دهد که سیستم‌های فناوری اطلاعات خود را بهتر درک کنند و سطح کنترل و امنیت مورد نیاز سازمان خود را شناسایی و از طریق توسعه مدل راهبری فناوری اطلاعات به آن دست یابند.

۲-۲-۳. روش تجزیه‌وتحلیل درخت خطا (FTA)

ارزیابی مخاطره احتمالی[1] یک روش نظامند و جامع به منظور ارزیابی مخاطره سامانه‌های فنی پیچیده از قبیل هواپیما (خطوط هوائی) و یا نیروگاه‌های هسته‌ای است. در ارزیابی مخاطره احتمالی، مخاطره به عنوان پیامد زیان‌آور احتمالی در نتیجه یک فعالیت یا عمل تعریف شده و توسط دو عامل شدت پیامد و احتمال پیامد مشخص می‌شود. تکنیک **تجزیه‌وتحلیل درخت خطا**[2] یا به اختصار «FTA» از فنون زیرمجموعه ارزیابی مخاطره احتمالی است. این روش برای نخستین بار سال ۱۹۶۲ میلادی در آزمایشگاه‌های تلفن «بل» به وجود آمد و سپس توسط آقای «واتسون» توسعه یافت و جهت بهبود قابلیت اطمینان سامانه کنترل موشک‌های قاره‌پیما مورد استفاده قرار گرفت. بعد از آن بازنگری و توسعه این روش توسط کارشناسان شرکت بوئینگ انجام گرفت و امروزه به طور وسیعی در تحلیل ایمنی به ویژه در سامانه‌های تولید انرژی هسته‌ای کاربرد دارد. این روش به عنوان یکی از قوی‌ترین ابزارهای تجزیه‌وتحلیل فرآیند ایمنی سیستم به‌ویژه در هنگام ارزیابی سیستم‌های بسیار پیچیده و دقیق محسوب می‌شود. به دلیل بهره‌برداری از روش قیاسی (رسیدن از کل به جزء) در این روش، بسیاری از تحلیلگرهای ایمنی سیستم، به کارگیری روش «FTA» را در بررسی حالات احتمالی گوناگون که می‌توانند منجر به بُروز رویدادهای مطلوب یا نامطلوب در سطح سیستم شوند، بسیار مفید می‌دانند.

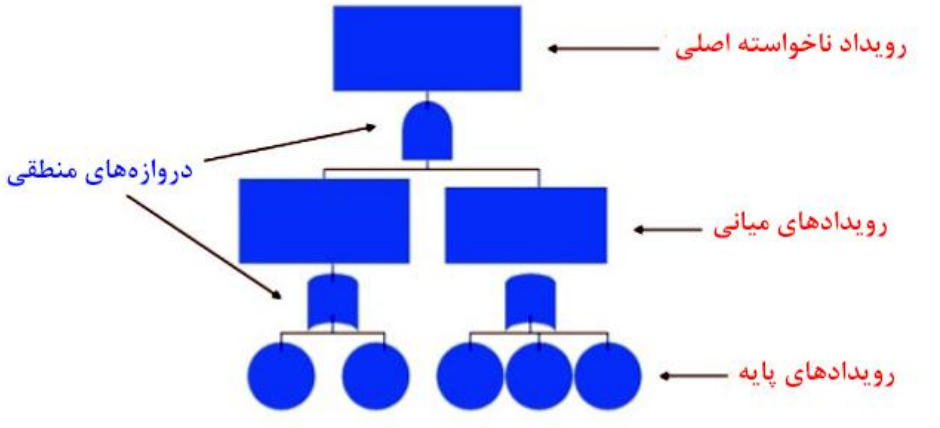
روش «FTA» یک فن ارزشیابی است که از آن می‌توان برای تعیین علل گوناگون یک رخداد خطرناک پیش‌بینی شده استفاده کرد. سپس همه راه‌هایی که می‌توانند سبب بُروز این وضعیت ناخواسته و نامطلوب شوند جستجو می‌شود. پس از آن به صورت نظام‌مند، تمامی دلایل خرابی را در یک ساختار بالا به پایین که شبیه درخت است، مرتب کرده و در نهایت از این ساختار برای محاسبه احتمال وقوع رویداد نهایی استفاده می‌شود. (**شکل ۲-۳**) اصول ترسیم روش تحلیل درخت خطا را نشان می‌دهد. این روش یک نمایش گرافیکی، دقیق و چندسونگر از شرایط یا عامل‌هایی است که باعث وقوع یک رویداد نامطلوب می‌شوند و به آن **رویداد اصلی**[3] می‌گویند. این روش به بررسی تحلیلی پرداخته و پس از بهره‌برداری از اطلاعات گوناگونی چون نقشه فرآیند، وظایف اپراتورها، روش‌های کنترلی و غیره، از نمادهای متعددی برای نشان دادن اجزای عناصر و ارتباط‌هایشان استفاده می‌کند. در نهایت نشان داده می‌شود که برای به وقوع پیوستن یک حادثه بزرگ احتمالی چه عواملی درگیر می‌شوند.

در این روش ابتدا یک حادثه بزرگ به صورت منطقی به رویدادهای بالقوه خطرناک اولیه و میانی تقسیم می‌شود و هر خطر به اجزای ریزتری می‌شکند تا به خطر پایه برسد و ارتباط میان این اجزا با نماد (and) به معنی لزوم رخ دادن همزمان و (or) یا رخ دادن مجزای این عوامل نشان داده می‌شود. سپس می‌توان نتایج را به صورت کمّی یا کیفی بررسی کرد. اما باید به خاطر داشت که

---

[1] Potential Risk Assessment
[2] Fault Tree Analysis (FTA)
[3] Top Event (TE)

تجزیه‌وتحلیل کمّی نیاز به زمان و هزینه بیشتری داشته و در عوض سه شاخص بنیادی (احتمال رخداد رویداد اصلی، احتمال و اهمیت رویدادهایی که منجر به رخداد رویداد اصلی می‌شوند و مخاطره هر یک از اجزا) را در اختیار سازمان قرار می‌دهد که برای تصمیم‌گیری‌های آینده درباره قابلیت پذیرش مخاطره‌ها و مقیاس‌های پیشگیری مفید است. در برخی از موارد، این روش را می‌توان پس از انجام روش‌های ارزیابی مخاطره «FMEA» یا «PHA» برای اجزا یا بخش‌های خاصی که دارای خطرات بالاتری هستند، انجام داد.



شکل ۲-۳. اصول ترسیم تحلیل درخت خطا، (Baklouti et al. 2017)

۲-۲-۴. چارچوب مدیریت مخاطره سازمانی کوزو (COSO ERM)

کمیته سازمان‌های حامی کمیسیون تِردوی[1] در سپتامبر سال ۲۰۰۴ میلادی چارچوب یکپارچه‌ای را تحت عنوان **چارچوب مخاطره سازمانی کوزو**[2] یا به اختصار (COSO ERM) برای کمک به اجرای فرآیند مدیریت مخاطره ارائه داد که به **مکعب کوزو**[3] شناخته می‌شود. این مکعب به روزرسانی شده چارچوب یکپارچه کنترل داخلی «COSO» اولیه ارائه شده در سال ۱۹۹۲ است. این چارچوب به عنوان ساختار یا رویکرد فراگیر مدیریت مخاطره‌های سازمانی مورد استفاده قرار می‌گیرد (ISO 2017). چارچوب مدیریت مخاطره «COSO ERM» نسخه ۲۰۰۴ از هشت جزء محیط کنترلی (داخلی)، هدف‌گذاری، شناسایی رویدادها، ارزیابی مخاطره، واکنش به مخاطره، فعالیت‌های کنترلی، اطلاعات و ارتباطات و نظارت و چهار اصل کلی (اهداف راهبردی، عملیات، گزارش‌دهی و انطباق) تشکیل شده است که در قالب (**شکل ۲-۴**) نشان داده شده است (Weller 2015).

بر پایهٔ چارچوب «COSO ERM»، ارزیابی مخاطره جزئی از وظایف روزانه مدیریت و کارکنان است. سیستم مدیریت مخاطره «کوزو» باید در فرآیندهای گوناگون، توسط مسئولان مربوطه به کار گرفته و نهادینه شود. پذیرش این موضوع توسط اعضای سازمان، نوعی تغییر سازمانی گسترده به شمار می‌رود و مستلزم اجرای عملیات فرهنگ‌سازی است.

چارچوب مدیریت مخاطره سازمانی «COSO ERM» در قالب یک ساختار سه‌بُعدی (مکعب) ارائه شده است. دلیل بهره‌برداری از مکعب در این چارچوب آن است که ارتباط بین اهداف (راهبردی، عملیاتی، گزارش‌دهی، انطباق) را با هشت مؤلفه‌ای که در جلوی مکعب دیده می‌شوند (محیط داخلی، تنظیم اهداف، شناسایی رخداد، ارزیابی مخاطره، پاسخ به مخاطره، فعالیت‌های کنترلی، امنیت و ارتباطات و پایش[4]) نشان دهد. این ارتباط بیانگر آن است که برای رسیدن به اهداف چه کارهایی را باید انجام داد.

---

[1] Committee of Sponsoring Organizations of the Treadway Commission (Treadway)
[2] The Committee Of Sponsoring Organizations Of The Tread way Commission's Enterprise Risk Management Framework (COSO ERM)
[3] COSO Cube
[4] Monitoring

در بُعد سوم نیز واحدهای سازمان (شعب سازمان، واحدهای کسب‌وکار، بخش‌های سازمان، سطح موجودیت) جای دارند. این بُعد بیانگر تمرکز چارچوب بر روی بخش خاصی از سازمان است.

شکل ۲-۴. چارچوب COSO ERM (Weller 2015)

«کمیته سازمان‌های حامی کمیسیون تردوی» همچنین در سال ۲۰۱۷ میلادی، نسخه جدید چارچوب مدیریت مخاطره سازمانی «COSO ERM» را منتشر کرده است. این نسخه نسبت به نسخه قبلی این چارچوب با تغییرات اساسی همراه است. در این نسخه ساختار و ترکیب مؤلفه‌های اصلی چارچوب تغییر یافته و پنج مؤلفه نسبتاً جدید به شرح ذیل در این چارچوب در نظر گرفته شده است.

- **راهبری و فرهنگ**: راهبری لحن سازمان را تعیین کرده و بر ضرورت تعریف مسئولیت‌ها برای مدیریت مخاطره در سازمان‌ها تأکید می‌نماید. فرهنگ نیز بر پایبندی به اصول اخلاقی، رفتارهای مطلوب و فهم مخاطره در سازمان پافشاری می‌کند.
- **راهبرد و تعیین اهداف**: مدیریت مخاطره سازمان، راهبردها و تعیین اهداف در فرآیند برنامه‌ریزی راهبردی سازمان با یک‌دیگر در ارتباط هستند. **اشتهای مخاطره**[1] در راستای راهبردها تعیین می‌شود. اهداف کسب‌وکار زمینه تحقق راهبردها را فراهم آورده و مبنایی را برای شناسایی، ارزیابی و پاسخ به مخاطره‌ها ایجاد می‌کنند.
- **عملکرد**: مخاطره‌هایی که بر تحقق راهبردها و اهداف تأثیرگذار هستند، شناسایی شده و ارزیابی می‌گردند. مخاطره‌ها بر پایهٔ شدت و در چارچوب اشتهای مخاطره سازمان اولویت‌بندی می‌شوند. سازمان سپس، پاسخ‌های مناسب به مخاطره را انتخاب کرده و سبدی از مخاطره‌ها را مورد ملاحظه قرار می‌دهد. نتایج این فرآیند به ذینفعان کلیدی مخاطره‌ها گزارش می‌گردد.

[1] Risk Appetite

- **مرور و بازنگری**: به‌واسطه مرور عملکرد سازمان، مشخص می‌شود که اجزای مدیریت مخاطره در سازمان چگونه عمل کرده‌اند و در راستای تغییرات اساسی ایجاد شده، چه به‌روزرسانی‌ها و بازنگری‌هایی ضروری است.
- **اطلاعات، ارتباطات و گزارشگری**: مدیریت مخاطره سازمان نیازمند فرآیند مستمر دریافت و به‌اشتراک‌گذاری اطلاعات از منابع درونی و بیرونی است. این اطلاعات در سطوح گوناگون سازمان از بالا به پایین، پایین به بالا و در سطوح افقی به گردش در می‌آیند.

نکته جالب توجه در این چارچوب این است که کمیته سازمان‌های حامی کمیسیون تردوی اذعان کرده است که این چارچوب جایگزین نسخه قبلی نشده است، بلکه ابعاد جدیدی در کنار نسخه قبلی مطرح شده و مکمل چارچوب قبلی مدیریت مخاطره سازمان است. (**شکل ۲-۵**) اصول و مؤلفه‌های چارچوب مدیریت مخاطره سازمانی «COSO ERM» را به تصویر کشیده است.

شکل ۲-۵. اصول و مؤلفه‌های چارچوب مدیریت مخاطره سازمانی COSO ERM (ISO 2017)

نسخه جدید چارچوب مدیریت مخاطره سازمان با تأکید بر محورهای کلیدی ذیل ارائه شده است:

- ارائه بینشی عمیق‌تر در خصوص ارزش مدیریت مخاطره سازمان در زمان تعریف و اجرای راهبردها؛
- بهبود ارتباط بین عملکرد و مدیریت مخاطره سازمان برای بهبود فرآیند تعیین اهداف عملکردی و شناخت تأثیرات مخاطره بر عملکرد؛
- ارائه روشی جدید برای نگریستن به مخاطره در زمان تعیین و تحقق اهداف در چارچوب محیط‌های کسب‌وکار پیچیده‌تر؛
- بهبود و تقویت گزارشگری نتایج مدیریت مخاطره برای افزایش شفافیت به ذینفعان؛
- ترویج بهره‌برداری از فناوری و فنون تحلیل داده در پشتیبانی از تصمیم‌گیری‌ها؛ و
- تعیین اهداف، مؤلفه‌ها و اصول برای تمامی سطوح مدیریت مرتبط با طراحی، پیاده‌سازی و هدایت فعالیت‌های مدیریت مخاطره سازمان.

۲-۲-۵. روش مطالعه مخاطرات و راهبری عملیات (Hazop)

روش مطالعه مخاطرات و راهبری عملیات[1] و یا به اختصار «Hazop» نخستین بار در اواسط دهه ۷۰ میلادی توسط مهندسین شرکت صنایع شیمیایی ICI در انگلستان بر پایهٔ فنی که بنام آزمایش بحرانی معروف بود، معرفی شد و پس از آن توسط

[1] Hazard and Operability study (Hazop)

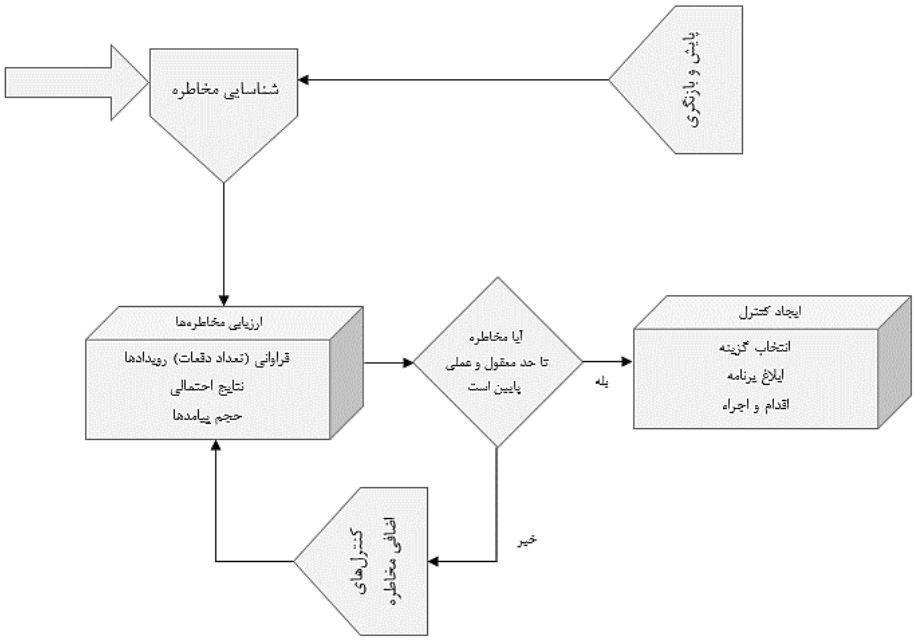
«ترور.اِی کلتز[1]»، بصورت قانونمند و امروزی در آمد. اساساً روش «Hazop» که ماهیتی آینده‌نگر و مبتنی بر پیشگیری قبل از وقوع دارد، در مقابل بهره‌برداری از چک لیست که مبتنی بر فلسفه گذشته‌نگر است، مطرح گردید. هر چند که روش «Hazop» برای نخستین بار به منظور شناسایی و ارزیابی مخاطرات فرآیندی معرفی و بکار گرفته شد، ولی با گذشت زمان و معرفی توانمندی‌های دیگر آن، به دیگر صنایع نیز گسترش یافت. کلمه «Hazop»، برگرفته از سه حرف نخست کلمه Hazard به مفهوم خطر و دو حرف اول Operability، به معنی راهبری عملیات است.

روش «Hazop»، مخاطرات و مشکلات عملیاتی را شناسایی می‌کند و مفهوم اصلی آن این است که چطور می‌شود ماشین‌آلات، تجهیزات یا سیستم، از هدف اصلی طراحی منحرف شده و انتظارات طراح را برآورده نکنند. اگر در فرآیند شناسایی مشکلات در طول انجام مطالعه «Hazop» راهکاری که واضح و معلوم باشد ارائه شود، به عنوان قسمتی از نتایج بدست آمده از «Hazop» ثبت می‌گردد. ولی باید توجه داشته باشیم که به دنبال راهکارهایی که زیاد واضح نیستند نباشیم، چرا که هدف اصلی برای انجام «Hazop» شناسایی مشکلات مربوط به فرآیند یا سیستم است. هر چند مطالعه «Hazop» به منظور تکمیل روش‌ها و شیوه‌های مبتنی بر تجربه، هنگامی که با یک طرح جدید یا یک تکنولوژی جدید سروکار داریم، توسعه داده می‌شود، علیرغم این موارد بهره‌برداری از آن تقریباً به تمام فازهای عمر یک دستگاه یا سیستم گسترش داده می‌شود. مطالعه «Hazop» بر این اصل استوار است که در آن چندین کارشناس یا متخصص با تخصص‌های گوناگون می‌توانند با هم تعامل داشته و خطرات بیشتری را نسبت به مواقعی که به طور انفرادی و مجزا کار می‌کنند، شناسایی و نتایج بدست آمده از این تعامل را با هم ترکیب و تلفیق کنند.

بهترین زمان برای انجام «هازوپ»، زمانی است که طراحی نسبتاً قطعی شده باشد (فاز طراحی). در این مرحله طراحی به نحو کاملاً خوبی مشخص و تشریح شده و این اجازه را به طراح می‌دهد که پاسخ‌های با مفهوم و معناداری را به پرسش‌های به‌وجود آمده در «هازوپ» ارائه کند. همچنین در این فاز هنوز امکان تغییر در طراحی بدون اینکه هزینه قابل توجهی در پی داشته باشد، وجود دارد. «هازوپ» می‌تواند در هر فازی بعد از طراحی نیز انجام گیرد. برای نمونه، در بسیاری از کارخانجات ماشین‌آلات و تجهیزات قدیمی از نظر کنترلی و سیستم‌های آن، تجهیز و ارتقاء یافته و بهینه‌تر شده‌اند. در «هازوپ» بین راه‌های انحراف و فلسفه طراحی سیستم کنترلی متداول برای رساندن انحرافات به صفر، یک ارتباط طبیعی وجود دارد. بنابراین خیلی مؤثر و مفید خواهد بود که به محض آنکه طراحی مجدد سیستم کنترلی قطعی گردید، ماشین آلات یا تجهیزات کارخانه را مورد مطالعه مجدد قرار دهیم.

(**شکل ۲-۶**) مراحل فرآیند «Hazop» را به تصویر می‌کشد. همان طور که در شکل نشان داده شده است، نخستین گام در راه برطرف کردن مخاطرات و حوادث موجود در واحدهای صنعتی، شناسایی مخاطرات موجود در آن است. بعد از شناسایی مخاطرات موجود، گام دوم ارزیابی مخاطرات است. بدیهی است هنگامی که تعداد خطرات شناسایی شده بیشتر از یک مورد باشد، برای پرداختن به امر کنترل آنها، پرسشی مطرح می‌شود مبنی بر اینکه کدام مخاطره را باید قبل از دیگری کنترل کرد، یا اینکه از امکانات و انرژی و بودجه موجود چند درصد را برای مخاطره شماره (۱) و چند درصد را برای مخاطره شماره (۲) و الی آخر صرف کرد. بدون ارزیابی و تعیین اولویت موجود در بین مخاطرات شناسایی شده نمی‌توان به فکر کنترل آنها بود.

[1] Trevor A. Kletz



شکل ۲-۶. چرخه فرآیند Hazop

بنابراین می‌توان گفت روش «Hazop» یک روش اصولی برای تشخیص مخاطرات و مسائل عملیاتی است و در سراسر یک پروژه بزرگ قابل کاربرد است. همچنین در افشای مخاطرات به خصوص در مراحل اولیه طراحی واحد بسیار مؤثر است. این روش زمان‌بر است، ولی انجام آن در مراحل اولیه طراحی نیاز به تغییرات اساسی در آینده را مرتفع کرده و به این ترتیب در هزینه صرفه‌جویی می‌کند. ولی از سوی دیگر مطالعه مؤثر «Hazop» بستگی زیادی به دانش فنی اعضاء تیم و همچنین تجربه و شایستگی رهبر گروه دارد. تیم «Hazop» نمی‌تواند مخاطرات یا علل احتمالی آنها را خارج از محدوده دانش خود پیش‌بینی کند. این محدودیت عامل مهمی در انتخاب اعضاء تیم است. بنابراین گرچه به نظر می‌رسد که در روش «Hazop» کلیه انحرافات فرآیندی ممکن به روشی نظام‌مند دیده می‌شوند، ولی موفقیت یا شکست این روش به چندین عامل بستگی دارد:

- تکمیل بودن و دقیق بودن نقشه‌ها و دیگر اطلاعات و داده‌هایی که به عنوان پایه و اساس مطالعه مورد استفاده قرار می‌گیرند؛
- مهارت‌های فنی و بینش و بصیرت تیم؛
- توانایی تیم برای بهره‌برداری از این روش به عنوان یک وسیله کمکی برای تحریک قوه تخیل و تصور خود نسبت به انحرافات ممکن، علل بوجود آمدن این انحرافات و پیامدهای ناشی از آن؛ و
- توانایی تیم برای تمرکز روی خطرات جدی‌تری که شناسایی شده‌اند.

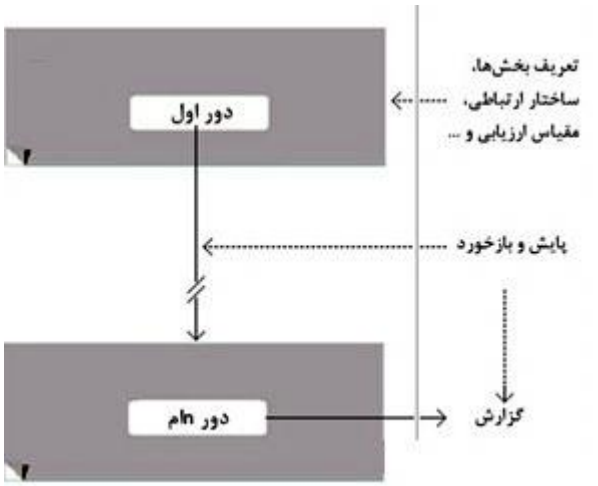
۲-۲-۶. روش ارزیابی امنیتی دلفی (Delphi)

روش ارزیابی امنیتی **دلفی**[1] یا به اختصار «Delphi» در ابتدای جنگ سرد[2] و برای پیش‌بینی تأثیر فناوری بر روی جنگ توسط مؤسسه «رَند[3]» توسعه داده شده است. در سال ۱۹۴۴ میلادی بود که «ژنرال هنری آرنولد»[4] دستور داد تا گزارشی برای نیروی هوایی ارتش آمریکا تدوین شود. بر این اساس مقرر شد تا فناوری‌های آینده که قابلیت استفاده در ارتش را دارند مشخص شوند (Wikipedia 2017). روش «Delphi» شامل گروهی از **متخصصان**[5] می‌شود که به طور ناشناس به پرسشنامه‌ها پاسخ می‌دهند و متعاقباً بازخوردهایی را به صورت بازنمایی آماری از "پاسخ گروه" دریافت می‌کنند، پس از آن روند دوباره تکرار می‌شود. نمایی از

[1] Delphi
[2] Cold War
[3] RAND
[4] General Henry H. Arnold
[5] Experts

این روش ارزیابی در قالب (**شکل ۲-۷**) به‌تصویر کشیده شده است. ازجمله ویژگی‌های بارز روش «Delphi» می‌توان به موارد ذیل اشاره کرد:

- **ناشناس بودن**[1]: مهمترین ویژگی آن گمنام بودن متخصصان در فرآیند پاسخگویی است. با توجه به خاصیت تأثیرپذیری نظرات در فرآیند پاسخگویی گروهی به صورت حضوری، این روش به گونه‌ای انجام می‌شود که این اثر کاهش یابد.
- **تکرار**[2]: به منظور رسیدن به توافق این روش چندین دور تکرار می‌شود.
- **بازخورد**[3]: نتایج دوره قبل در اختیار شرکت‌کنندگان قرار می‌گیرد و آنها نظرات خود را بر این اساس به‌روزرسانی می‌کنند.
- **بهره‌برداری از متخصصین**: پاسخ‌دهندگان در روش «Delphi» افراد خبره و متخصص می‌باشند.



شکل ۲-۷. روش ارزیابی امنیتی Delphi

در واقع، هدف این روش کاهش دامنه پاسخ‌ها و رسیدن به چیزی نزدیک به **اجماع**[4] متخصص است. امروزه روش «Delphi» به طور گسترده‌ای پذیرفته شده و مورد استفاده قرار می‌گیرد. از جمله نقاط قوت و ضعف روش «Delphi» می‌توان به موارد ذیل در قالب (**جدول ۲-۱**) اشاره کرد:

جدول ۲-۱. نقاط قوت و ضعف روش دلفی

نقاط قوت	نقاط ضعف
+ Deplphi به عنوان روشی سریع (نسبت به روش‌های دیگر)، ارزان و یک روش نسبتاً کارآمد برای ترکیب دانش و توانایی‌های گروهی از متخصصان توصیف شده است. + انعطاف‌پذیری زیاد این روش، کاربرد در برنامه‌های گوناگون، به‌کارگیری رویکردهای ارتباطی گوناگون و امکان استفاده در سطح جغرافیایی وسیع، عدم نیاز به آموزش مصاحبه‌گران، گمنامی، بهره‌برداری از پرسش‌های باز، شناسایی و فهم زیربنای موضوع از مزایای دیگر روش دلفی است. + Deplphi برای پرسش‌هایی که نیاز به توضیح و قضاوت دارد، یک روش مناسب است. با کاربرد پرسش‌نامه در روش دلفی، امکان دسترسی به تعداد بیشتری متخصص وجود دارد. در واقع، میزان	– روش Deplphi نیاز به دقت زیاد برای انتخاب شرکت‌کنندگان و تهیه پرسش‌نامه دارد و یکی از مهم‌ترین محدودیت‌های این فن، نیازمندی به کوشش و کار زیاد، سیر آهسته و وقت‌گیربودن آن است. – برخی از محققان معتقدند که روش Deplphi نسبت به روش‌های دیگر پاسخ‌های صحیح‌تری به دست نمی‌دهد و توافق به دست آمده در این روش نیز، نتیجه اعمال فشار بر شرکت‌کنندگانی است که نظریات غیرمعمول دارند. در این اجماع، خصوصیات فردی نقش مؤثری دارد. – در روش Deplphi برخی از نظرات احتمالاً تأثیرگذار و مهم افراد به دلیل اینکه نظر اکثریت اهمیت دارد، نادیده گرفته می‌شود. – Deplphi تنها مرحله آغازینی است که صرفاً برای کسب اجماع می‌کوشد و این اجماع ضرورتاً دقیق‌ترین نظر نیست. بلکه ممکن است نتیجه، شناسایی

[1] Anonymity
[2] Iteration
[3] Feedback
[4] Consensus

نقاط قوت	نقاط ضعف
محدودیت در تعداد شرکت‌کنندگان بستگی به میزان دقت و بودجه دارد. +مزیت مهم پرسش‌نامه در روش Deplphi این است که بر پایهٔ نیازهای اطلاعاتی موردنظر محققان تنظیم می‌شود. +از لحاظ روانی، اغلب افراد نمی‌توانند درباره پاسخ‌هایی که به پرسش‌نامه می‌دهند، مطمئن باشند و نیازمند تکیه‌گاهی خارجی هستند. میانگین نظرات دیگر افراد، که در مراحل بعدی در پرسش‌نامه آورده می‌شود می‌تواند نقش این تکیه‌گاه را بازی کند. +دلفی دلایل شفافی برای اجماع ارائه می‌دهد. پرسش‌نامه دلفی را می‌توان چندین بار مرور و برای مراجعات بعدی بایگانی کرد.	یک سری عبارات عمومی به جای عناوین خاص اطلاعاتی باشد. چراکه در Deplphi فرض برابری شرکت‌کنندگان از داشن و تجربه است، اما در عمل این فرض ممکن است صحیح نباشد. – پرسش‌نامه Deplphi ممکن است گمراه‌کننده و حتی نامربوط باشد. بنابراین باید با دقت زیادی طراحی شود. – پرسش‌نامه Deplphi ممکن است پاسخ‌دهندگان را محدود کند و آنها را از گفتن آنچه که فکر می‌کنند درست است، باز دارد. – طولانی بودن مدت زمان مطالعه، ریزش افراد متخصص، احتمال دریافت میزان پایین پاسخ، خستگی افراد از مراحل و موضوع، عدم وجود معیارهای کلیدی و مشخص در تعریف افراد متخصص، سطح اجماع و اندازه گروه متخصص شرکت‌کننده در مطالعه از دیگر محدودیت‌های این روش است.

۲–۲–۷. روش تجزیه‌وتحلیل حالات و اثرات شکست (FMEA)

یکی از معروف‌ترین روش‌های ارزیابی مخاطره، **روش تجزیه‌وتحلیل حالات و اثرات شکست**[1] یا به اختصار (FMEA) است (Ardeshir, Amiri and Mohajeri 2013). این روش نخستین بار در دهه ۱۹۶۰ میلادی، برای تجزیه‌وتحلیل نظام‌مند حالت‌های شکست و پیامدهای متعاقب آنها در محصولات نظامی، به ویژه در صنعت هوانوردی مورد استفاده قرار گرفت (Bowles and Peláez 1995) و پس از آن در دهه ۱۹۷۰ و ۱۹۸۰ میلادی برای مؤسسه‌های اتمی و از سال ۱۹۷۷ میلادی به بعد برای صنایع خودروسازی به کار گرفته شد. از سال ۲۰۰۰ میلادی تاکنون این روش یکی از پرکاربردترین روش‌های ارزیابی مخاطره در تمامی صنایع محسوب می‌شود. «FMEA» می‌کوشد تا حد ممکن خطرات بالقوه موجود و نیز علل و اثرات مرتبط با آن را در محدوده‌ای که ارزیابی مخاطره انجام می‌شود، شناسایی و امتیازدهی کند (Sharma, Kumar and Kumar 2005).

مهم‌ترین ویژگی این روش سادگی فهم و اجرای آن است، اما با وجود سادگی و کارایی مناسب دارای مشکلاتی از جمله درنظر گرفتن شاخص و عوامل مهمی نظیر هزینه، امتیازدهی دقیق و مستقیم عددی توسط کارشناسان و همچنین عدم توجه به اثرات متقابل بین شاخص‌ها است که در صورت برطرف کردن آنها، کارایی این روش افزایش می‌یابد (Braglia, Frosolini and Montanari 2003). مهم‌ترین هدف کاربرد این روش، شناسایی حالت‌های شکست بالقوه در اجزای سیستم، تعیین علل، ارزیابی اثرات آنها بر روی عملکرد سیستم و در نهایت تعیین راه‌هایی است که بتوان شانس وقوع و پیامدها را کاهش و قابلیت تشخیص حالت‌های شکست را افزایش داد (Stamatis 2003). روش «FMEA» سنتی بر مبنای **عدد اولویت مخاطره**[2] یا به اختصار (RPN) بوده و از حاصل‌ضرب سه عامل **شدت اثر مخاطره**[3] (S)، **احتمال وقوع مخاطره**[4] (O) و **احتمال کشف مخاطره**[5] (D) به دست می‌آید و با توجه به سطح مخاطره‌ها به ارزیابی نقض‌های بالقوه سیستم می‌پردازد (Chen and Wu 2013). بدیهی است هرچه مقدار «RPN» بالاتر باشد، میزان مخاطره مرتبط با حالت شکست مد نظر نیز بیش‌تر می‌گردد. در حالی که اگر با توجه به «FMEA» سنتی و بر مبنای «RPN» اقدام به حذف شکست‌ها شود، ممکن است برخی از شکست‌ها به دلیل کم بودن مقدار «RPN» در اولویت پایین‌تری جهت اصلاح و حذف قرار گیرند. در این صورت ممکن است وقوع این شکست‌ها در عمل منجر به تحمیل هزینه‌های بسیاری (شامل هزینه‌هایی ازجمله ضایعات تولید و نیروی کار نگهداری و تعمیرات) به سیستم گردد که این موضوع ناشی از نادیده گرفتن هزینه شکست در روش «FMEA» است. این در حالی است که یکی از اهداف این روش، افزایش کارایی و کاهش هزینه است؛ بنابراین

[1] Failure Modes and Effects Analysis (FMEA)
[2] Risk Priority Number (RPN)
[3] Severity of failure
[4] Occurrence of failure
[5] Detection of failure

درنظر گرفتن عامل هزینه افزون بر سه عامل فوق منجر به رفع این نقض موجود در روش «FMEA» می‌شود. (**شکل ۲-۸**) مراحل کار این روش را به تصویر کشیده است که در ادامه جزئیات هر یک از مراحل به تفصیل مورد بررسی قرار خواهند گرفت.

۱. **جمع‌آوری اطلاعات مربوط به فرآیند:** سایت یا مکانی که در آن ارزیابی مخاطره انجام می‌شود، باید به طور کامل شناسایی و شیوهٔ فعالیت‌ها و فرآیندها به دقت بررسی شود.

۲. **تعیین مخاطرات بالقوه:** تمام خطرات محیطی، تجهیزاتی، مواد، انسانی و غیره که ایمنی را تهدید می‌کند باید در نظر گرفته شود، همچنین حالات هر خطر نیز باید مورد تجزیه و تحلیل قرارگیرد.

۳. **بررسی پیامدهای مخاطره:** پیامدهای هر مخاطره، پیامدهای احتمالی هستند که خطر بر ایمنی افراد می‌گذارند. پیامدهای مخاطره می‌توانند مانند آتش‌سوزی، مسمومیت، شکستگی، آسیب‌های مفصلی و غیره باشد.

۴. **تعیین علل مخاطره:** شناخت کافی از محدوده مورد ارزیابی می‌تواند کمک فراوانی برای شناسایی علل بوجود آمدن خطر باشد. اطلاعات فنی، زیست محیطی و ارگونومی نیز در شناسایی بهتر علل مؤثر هستند.

۵. **بررسی کردن فرآیندهای کنترلی**: به منظور ارزیابی بهتر مخاطرات صورت می‌گیرد. بررسی برگه‌های عملیات، استانداردها، الزامات و قوانین حاکم بر محیط کار و عوامل مربوطه از جمله این کارها است.

۶. **تعیین شدت وقوع (نرخ وخامت[1])**: وخامت خطر یا میزان جدید بودن "اثر خطر بالقوه" بر افراد است. شدت یا وخامت خطر فقط دربارهٔ "اثر" آن در نظر گرفته می‌شود، کاهش در وخامت خطر فقط از طریق اعمال تغییرات در فرآیند و شیوهٔ انجام فعالیت‌ها امکان‌پذیر است. برای این وخامت خطر شاخص‌های کمّی وجود دارد که بر حسب مقیاس ۱ تا ۱۰ بیان می‌گردد.

۷. **احتمال وقوع**: مشخص می‌کند که یک علت یا مکانیزم بالقوه خطر با چه تواتری رخ می‌دهد. احتمال رخداد بر مبنای ۱ تا ۱۰ سنجیده می‌شود. بررسی سوابق و مدارک گذشته بسیار مفید است.

۸. **نرخ احتمال کشف مخاطره**: احتمال کشف نوعی ارزیابی از میزان توانایی است که به منظور شناسایی یک علت یا مکانیزم وقوع خطر وجود دارد. به عبارت دیگر احتمال کشف، توانایی پی بردن به خطر قبل از رخداد آن است.

۹. **محاسبه عدد اولویت مخاطره**: عدد اولویت مخاطره حاصل‌ضرب سه عدد شدت اثر مخاطره (S) احتمال وقوع مخاطره (O) و احتمال کشف مخاطره (D) است. برای اعداد مخاطره بالا، کارگروهی باید جهت پائین آوردن این عدد از طریق اقدام اصلاحی صورت پذیرد.

۱۰. **اصلاح نیاز است**: در این مرحله مخاطرات بر پایهٔ عدد اولویت مخاطره رتبه‌بندی می‌شوند و بر پایهٔ نظر سیستم FMEA یک حد «RPN» در نظر گرفته می‌شود.

۱۱. **اقدام‌های اصلاحی پیشنهادی**: این اقدامات باید در جهت اهداف ذیل وضع و انجام گردند:

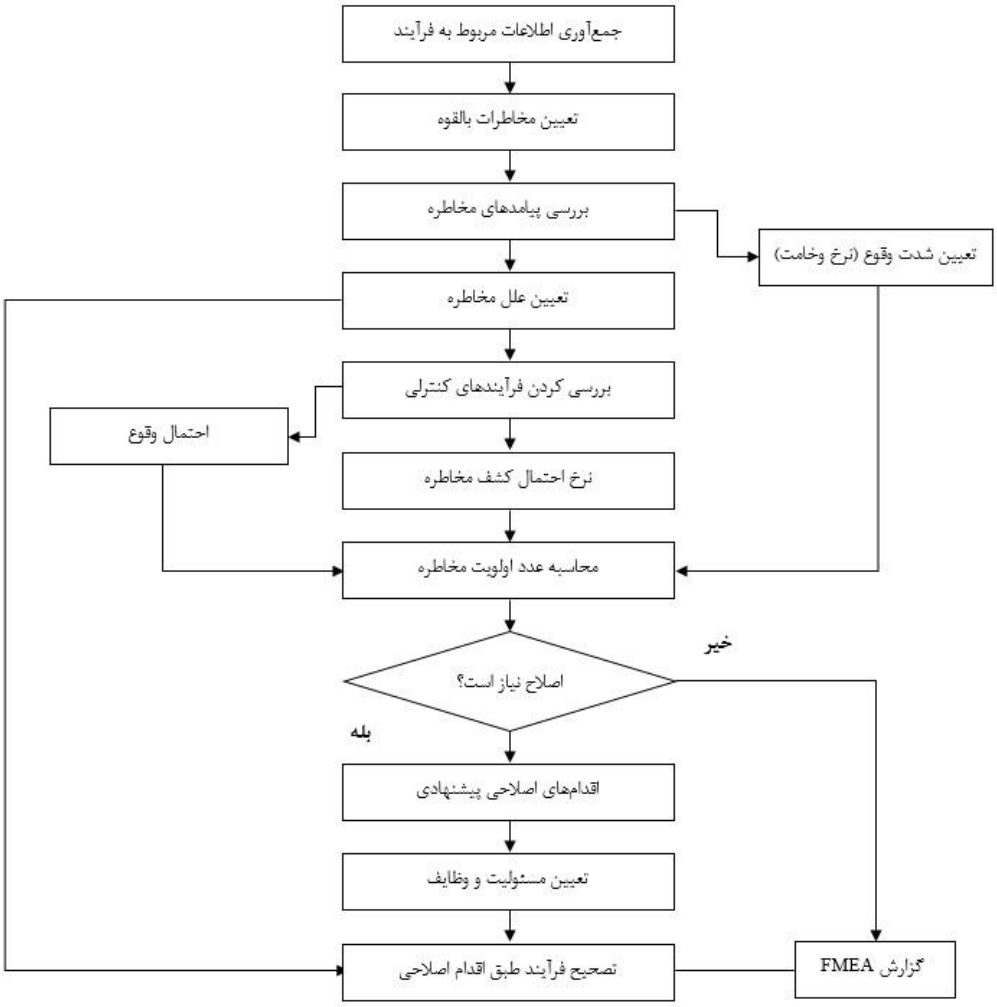
- حذف علل ریشه‌ای مخاطره؛
- کاهش وخامت پیامد مخاطره؛
- افزایش احتمال کشف مخاطره در فرآیند؛ و
- افزایش رضایت کاری کارکنان از وضعیت ایمنی.

۱۲. **تعیین مسئولیت و وظایف**: سازمان باید مسئول هر یک از اقدامات اصلاحی را مشخص و ثبت نماید. نتایج اقدامات انجام شده باید به گروه FMEA گزارش شده و صفحه‌گذاری شوند.

---

[1] Severity Rate

۱۳. **تصحیح فرآیند طبق اقدام اصلاحی:** اقدامات باید به طور مؤثر پیاده شده و این نکته درنظر گرفته شود که باید این اقدامات نیز ارزیابی شوند.



شکل ۲-۸. مراحل روش تجزیه و تحلیل حالات و اثرات شکست FMEA

علیرغم کاربرد وسیع، روش «FMEA» دارای نقص‌های عمده‌ای است که کاربرد این روش را به خصوص زمانی که این روش به منظور تحلیل بحران در محاسبه RPN استفاده شود، محدود می‌کند. از جمله محدودیت‌های روش «FMEA» سنتی می‌توان به موارد ذیل اشاره کرد:

- اهمیت نسبی پارامترهای (S)، (O) و (D) در محاسبه «RPN» منظور نشده و وزن آنها یکسان در نظر گرفته می‌شود. این در حالی است که در کاربردهای واقعی، این موضوع می‌تواند محدودیت ایجاد کند (Chanamool and Naenna 2016).
- ترکیب مخاطره عوامل گوناگون می‌تواند منجر به RPNهای یکسان شود، در حالی که ماهیت مخاطره‌های ایجاد شده متفاوت است (Zhang, Jin and Liu 2013).
- تعیین دقیق مخاطره فاکتورهای (S)، (O) و (D) اغلب مشکل است. اعضای تیم این روش ممکن است برای مخاطره فاکتورهای مشابه، ارزیابی‌های متفاوتی داشته باشند. برخی از آنها ممکن است غیردقیق، نامطمئن و ناقص باشند که به دلیل محدودیت زمانی، فقدان تجربه و داده‌های کافی ایجاد می‌شوند (Liu et al. 2012).

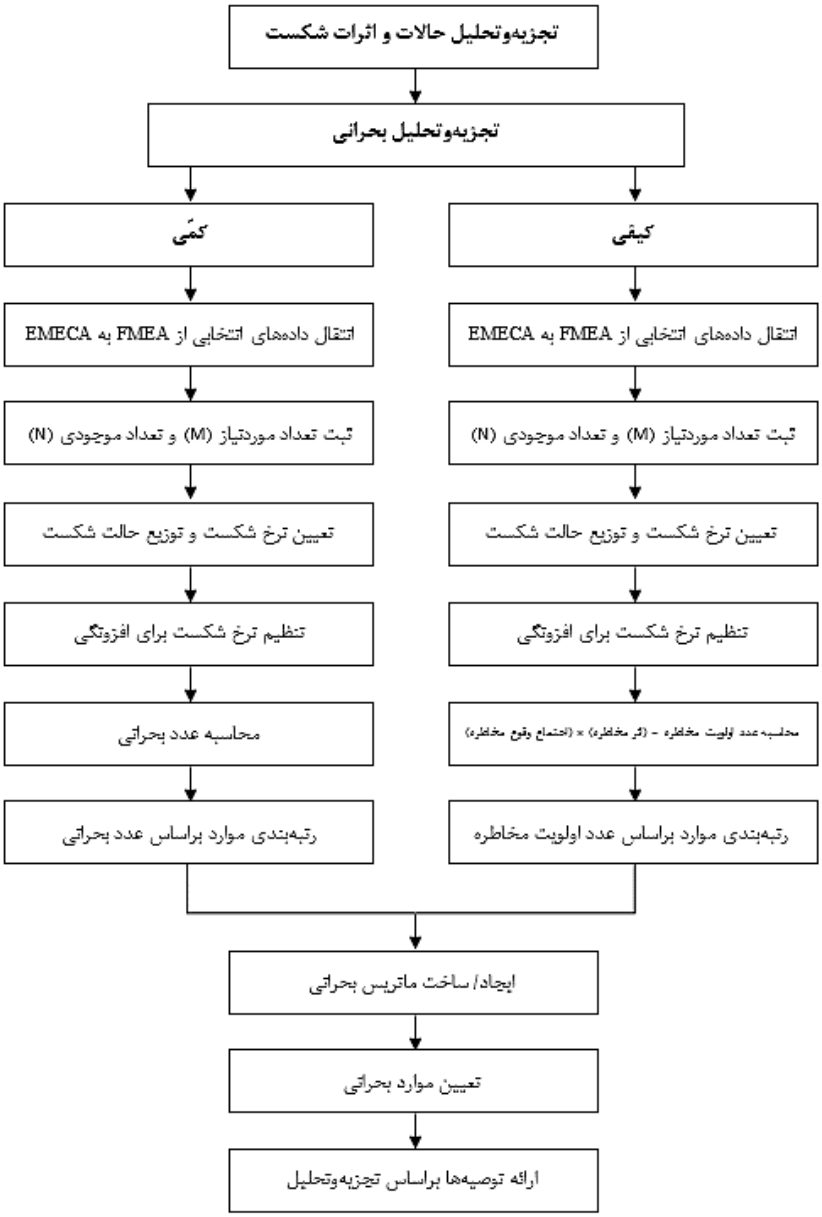
- فرمول محاسباتی «RPN» مورد تردید بوده و دارای یک بنیه علمی قوی نیست. به عبارتی دیگر منطق خاصی دربارهٔ علت ضرب کردن O، S و D برای محاسبه «RPN» وجود ندارد (Liu et al. 2012; Kutlu and Ekmekçioğlu 2012).
- مخاطره فاکتورهای S، O و D بر پایهٔ مقیاس‌های ترتیبی گسسته ارزیابی می‌شوند. این در حالی است که بهره‌برداری از عملیات ضرب برای مقیاس‌های ترتیبی بی‌معنی است. بنابراین نتایج به دست آمده نه تنها بی‌معنی، بلکه گمراه‌کننده نیز می‌باشند (Yang, et al. 2011).
- RPNهای به دست آمده پیوسته نبوده و دارای فواصل خالی زیادی در مقیاس ۱ تا ۱۰۰۰ می‌باشند. افزون بر این، میزان توزیع آنها در قسمت‌های پایینی مقیاس ۱ تا ۱۰۰۰ شدیدتر است. این موضوع می‌تواند باعث ایجاد مشکل در تفسیر اختلاف‌های بین RPNهای متفاوت گردد (Liu et al. 2012).
- «FMEA» یک روش ارزیابی مخاطره گروهی است که تنها بر پایه نظرات شخصی یک نفر ارزیابی نمی‌شود. گزارش استخراج مقدار واقعی هر یک از مخاطره فاکتورها بر پایهٔ نظر گروهی مشکل است (Wang 2009).

۲-۲-۸. روش تجزیه و تحلیل بحرانی حالات و اثرات شکست (FMECA)

روش تجزیه و تحلیل بحرانی حالات و اثرات شکست[1] یا به اختصار (FMECA)، روشی برای شناسایی و تحلیل تمام حالات شکست بالقوه قسمت‌های گوناگون سیستم، اثراتی که این شکست‌ها ممکن است روی سیستم داشته باشند، چگونگی جلوگیری از این شکست‌ها و یا کاهش اثرات آنها روی سیستم است (Becker and Flick 1996; Bertolini, Bevilacqua and Massini 2006; Rausand, Barros and Hoyland 2020). در واقع، این روش یک «FMEA» بسط‌یافته است که CA در FMECA نمایانگر بحران (یا شدت) اثرات گوناگون است (Rausand, Barros and Hoyland 2020). «FMECA» ابتدا به صورت یک روش‌شناسی طراحی در سال ۱۹۶۰ میلادی توسط صنعت هوافضای آمریکا[2] ایجاد شد، ارتش آمریکا در سال ۱۹۷۰ میلادی شروع به بهره‌برداری از آن کرد و در سال ۱۹۷۴ میلادی استاندارد نظامی MIL-STD-1629 دستورالعمل‌هایی برای انجام یک تحلیل بحرانی و اثرات حالات شکست را ارائه داد که در سال ۱۹۸۰ میلادی نسخه دوم آن ایجاد شد (Chang, Cheng and Chang 2010). در سال ۱۹۸۸ میلادی نیز شرکت خودروی فورد روش «RPN» را برای انجام روش «FMECA» پیشنهاد داده است (Bowles 1998). امروزه این روش برای بسیاری از صنایع مهم مانند صنایع نظامی، هسته‌ای، هوافضا، خودرو، صنایع الکتریکی و مکانیکی تطبیق یافته است (Bowles 1998). (**شکل ۲-۸**) مراحل کار این روش را به تصویر کشیده است. کارآمدی این روش باعث شده که از آن علاوه بر صنایع در مراکز دارویی و بهداشتی-درمانی به منظور بهبود وضعیت ایمنی و ارائه خدمات بی‌نقص به بیماران استفاده شود (Williams and Talley 1994; Hergon, Crespeau and Rouger 1994; Saizy-Callaert et al. 2002). اجرا و انجام تحلیل روش «FMECA» نیاز به کارهای آماری پیچیده ندارد، ولی از آنجایی که این تحلیل بر مبنای کار گروهی استوار است، نیاز به زمان و نیروی انسانی کافی دارد. بدون داشتن اطلاعات کافی در زمینه فرآیند و یا محصول به جای تکیه بر حقایق، به یک بازی مبتنی بر حدس و گمان تبدیل خواهد شد. به طورکلی روش «FMECA» **تک نقاط شکست**[3] -به قسمتی از یک سیستم می‌گویند که اگر خراب شود، کل سیستم دچار مشکل و توقف می‌شود- نیازمند اقدامات اصلاحی را شناسایی می‌کند، به روش‌های آزمایش و فنون عیب‌یابی کمک می‌کند، یک اساس و پایه را برای قابلیت اطمینان کیفی، نگهداشت‌پذیری و تحلیل‌های آماری و ایمنی (درخت خطا) فراهم می‌کند، یک تخمین و ارزیابی از نرخ‌های شکست سیستم را فراهم می‌کند و قسمت‌ها یا سیستم‌هایی که گرایش بیشتری به شکست دارند را شناسایی کرده و در آخر اقدام‌های اصلاحی را پیشنهاد می‌دهد (Standard 1980).

---

[1] Failure Mode & Effect Critically Analysis (FMECA)
[2] National Aeronautics and Space Administration (NASA)
[3] Single Point of Failure (SPOF)

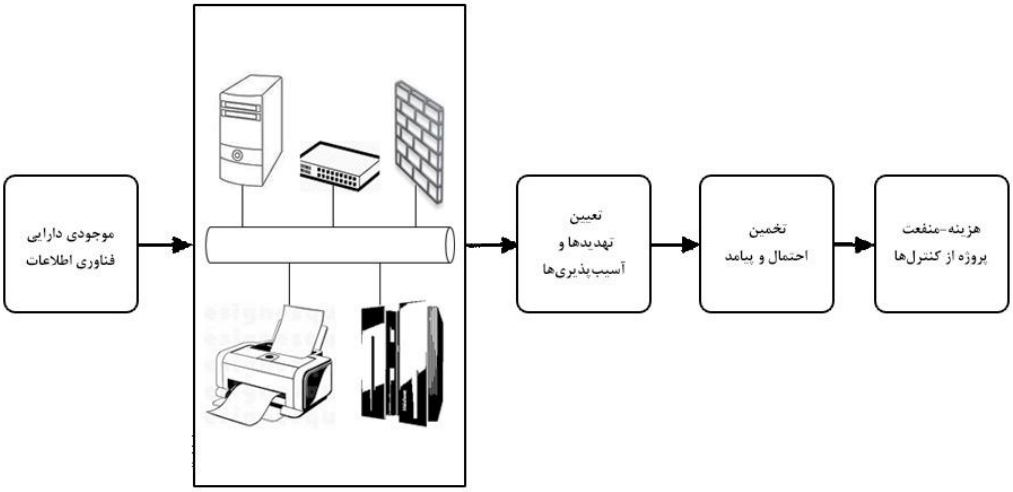


شکل ۲-۹. مراحل روش تجزیه و تحلیل بحرانی حالات و اثرات شکست FMECA، (Army 2006)

۲-۲-۹. روش سنتی تحلیل مخاطره امنیت اطلاعات

روش سنتی برای انجام تحلیل مخاطره امنیت اطلاعات[1] مبتنی بر فناوری است، زیرا در درجه نخست بر روی تهدیدهای شناخته شده انواع دارایی‌های رایانشی مورد استفاده در سازمان متمرکز است. این موضوع تا حد زیادی به دلیل منشاء تاریخی رهنمودهای امنیتی رایانه‌ای پرکاربرد (NIST, Common Criteria, RAND Corp, ISO 17799, SSE-CMM) است که در ابتدا برای امن‌سازی زیرساخت‌های رایانشی نظامی و دولتی توسعه داده شده بودند. با توجه به اینکه رهنمودهای امنیتی در ابتدا برای سیستم‌های اطلاعاتی در یک محیط تجاری درنظر گرفته نشده بودند، فاقد روش‌های شناسایی مخاطره‌های مربوط به افراد (داخلی و خارجی سازمان) و فرآیندهای کسب‌وکار هستند. گام‌های روش سنتی تحلیل مخاطره در قالب (**شکل ۲-۱۰**) خلاصه شده است (Spears 2004).

[1] Traditional Risk Analysis of Information Security



شکل ۲-۱۰. روش سنتی تحلیل مخاطره برای امنیت اطلاعات، (Spears 2004)

اولین گام در انجام فرآیند تحلیل مخاطره، شناسایی دارایی‌های فناوری اطلاعات است که باید مورد محافظت قرار گیرند. دارایی‌های فناوری اطلاعات معمولاً شامل سخت‌افزار، نرم‌افزار، داده، افراد، اسناد و امکانات قابل استفاده است. توجه داشته باشید که اگرچه افراد معمولاً به عنوان نوعی از دارایی فناوری اطلاعات درنظر گرفته می‌شوند، اما روش سنتی تحلیل مخاطره تمرکز کمی بر روی افراد دارد و به طور معمول فقط به شناسایی و احرازهویت کاربر می‌پردازد. با این وجود رویه‌هایی که مردم از آنها برای مدیریت اطلاعات استفاده می‌کنند ممکن است با خطر روبرو شود. در مرحله بعد، برای هر دارایی شناسایی شده، تهدیدها (حوادث ناخواسته‌ای که ممکن است رخ دهد) و آسیب‌پذیری‌های (نقاط ضعف موجود) مرتبط با محرمانگی، صحت و دسترس‌پذیری شناسایی می‌شوند. این امر معمولاً با بهره‌برداری از چک لیست‌های استاندارد (NIST, 2005) و تخصص تحلیلگر امنیتی تعیین می‌شود. سپس مخاطره بر پایهٔ امکان (یا احتمال) وقوع یک رویداد امنیتی کمّی (برای مثال سوءبهره‌برداری از یک آسیب‌پذیری) و در زیان مالی مورد انتظار از چنین رخدادی ضرب می‌شود (مخاطره = احتمال وقوع یک رخداد × زیان موردانتظار). این خروجی برای محاسبه تحلیل هزینه-منفعت پیاده‌سازی حفاظ‌های امنیتی استفاده می‌شود که مخاطره را تا حد قابل قبولی کاهش می‌دهد. از جمله نقاط قوت و ضعف رویکرد سنتی تحلیل مخاطره می‌توان به موارد ذیل در قالب (**جدول ۲-۲**) اشاره کرد.

جدول ۲-۲. نقاط قوت و ضعف روش سنتی تحلیل مخاطره

نقاط قوت	نقاط ضعف
+ این روش به عنوان یک استاندارد دفاکتو[1] در کتاب‌های درسی و دستورالعمل‌های امنیتی مورد پذیرش در صنعت شناخته و استفاده می‌شود؛ + تمرکز بر دیدگاه فناوری؛ + دسترس‌پذیری بسته‌های نرم‌افزاری خودکار جهت محاسبه دقیق و مدیریت داده‌های تحلیل مخاطره؛ + بهره‌برداری از معیارهای کمّی جهت پشتیبانی از تحلیل هزینه-فایده در سرمایه‌گذاری‌های محافظ‌های امنیتی؛ + داشتن ارتباط نزدیک با فنون تحلیل مخاطره در بخش‌های مالی و بیمه‌ای.	– تمرکز بیشتر بر دیدگاه فناوری و عدم توجه کافی بر افراد و فرآیندها در سیستم‌های اطلاعاتی؛ – تخمین/ برآورد اشتباه ضرر و زیان مورد انتظار بر پایهٔ ارزش دارایی‌ها (مشهود/ نامشهود)؛ – برآورد احتمال و ضرر و زیان مالی از یک نقض/ آسیب‌پذیری امنیتی با بهره‌برداری از حدس و گمان در محاسبات خود؛ – رویکرد پایین به بالا این روش به خصوص در سازمان‌های متوسط تا بزرگ بسیار پرهزینه و وقت‌گیر است؛ – انجام فرآیند تحلیل مخاطره توسط متخصصان/ کارشناسان فناوری اطلاعات و عدم آگاهی امنیتی آنها در کل سازمان با توجه به فناوری محور بودن آن و عدم دخالت کاربران.

عبارت‌دیگر، کثرت استفاده می‌تواند یک مستند یا چارچوب را به استاندارد بدل کند بی‌آنکه مؤسسات متصدی این کار، آن را تدوین کرده باشد.

[1] اگر یک مستند که توسط سازمان جهانی استاندارد یا دیگر مؤسسات بین‌المللی انتشار استانداردها تدوین نشده به قدری مورد استفاده قرار گیرد که به یک واقعیت غالب در آن موضوع خاص بدل شود به آن استاندارد دفاکتو گویند. به

در حالت کلی با توجه به اینکه بیشترین تمرکز **روش‌های سنتی تحلیل مخاطره**[1] مورد استفاده در سیستم‌های اطلاعاتی بر روی فناوری است و توجه کمتری به افراد و فرآیندها دارد، دارای کاستی‌های متعددی است که از جمله آنها می‌توان به موارد ذیل اشاره کرد:

۱. تمرکز این روش بر روی فناوری است، بدون در نظر گرفتن افراد و فرآیندها به عنوان منابع قابل توجه مخاطره امنیتی؛
۲. فرآیند تجزیه و تحلیل بر پایهٔ دارایی‌های فنی می‌تواند بیش از حد زمان‌بر و پرهزینه باشد؛ و
۳. برای برآورد احتمال و خسارت مالی ناشی از نقض امنیتی، تا حد زیادی از حدس و گمان استفاده می‌کند.

مبتنی بر این روش و با توجه به مزایا و معایب آن، روش‌های تازه مدیریت مخاطره در حوزه امنیت اطلاعات شکل پیدا کرده است که در این فصل و در ادامه، شناسایی و معرفی آنها مورد توجه قرار گرفته است.

۲-۳. گزیدهٔ فصل

برخورداری از دانش پیرامون یک موضوع و انتخاب یک روش مناسب جهت مواجهه با آن، سنگ‌بنای کلیه فعالیت‌ها و ابزار مورد استفاده در این راه خواهد بود. از این‌رو، روش‌ها با توجه به نیاز سازمان و نیز امکانات، منابع و محدودیت‌های پیش‌روی مجموعه انتخاب و بر آن مبنا، اقدامات جهت انجام یک کار مشخص طرح‌ریزی می‌شوند.

مدیران سازمانی و در کنار آنها مدیران امنیتی، همواره در جستجوی ایجاد شرایطی کم مخاطره در سطح مجموعه تحت مسئولیت خود بوده و در این راه از روش‌های گوناگون برای ارزیابی مخاطره بهره می‌برند. انتخاب روش‌های مناسب ارزیابی مخاطره می‌تواند متأثر از عوامل گوناگونی باشد که هر یک از این عوامل می‌توانند نوع نگاه و شیوهٔ تصمیم‌گیری سازمان جهت امن‌سازی فضای تبادل اطلاعات مجموعه را تحت‌تأثیر قرار دهند. از این‌رو در این فصل، مروری بر روی روش‌های ارزیابی مخاطره به شکل کلی (و نه مخاطره امنیت اطلاعات) صورت گرفت، مجموعه‌ای از روش‌های ارزیابی مخاطره مورد شناسایی قرار گرفت و در قالب روش‌های سنتی فرآیند ارزیابی مخاطره دسته‌بندی شد. در مجموع از مهمترین روش‌های سنتی ارزیابی مخاطره می‌توان به موارد زیر اشاره کرد:

- روش مطالعه مخاطرات و راهبری عملیات (Hazop): بر روی این مفهوم متمرکز است که چطور می‌شود ماشین‌آلات، تجهیزات یا سیستم، از هدف اصلی طراحی منحرف شده و انتظارات طراح را برآورده نمی‌کنند.
- روش ارزیابی امنیتی «Delphi»: بر پایه چرخه‌های تکراری اجماع‌ساز مبتنی بر نظرسنجی از متخصصانی است که به طور ناشناس به پرسشنامه‌های حوزه ارزیابی مخاطره پاسخ می‌دهند.
- روش تجزیه‌وتحلیل حالات و اثرات شکست (FMEA): برای تجزیه‌وتحلیل نظام‌مند حالت‌های شکست و پیامدهای متعاقب آنها ایجاد شده و کوشش می‌کند مخاطرات بالقوه موجود و نیز علل و اثرات مرتبط با آن را در محدوده‌ای که ارزیابی مخاطره انجام می‌شود، شناسایی و امتیازدهی کند.
- روش تجزیه و تحلیل بحرانی حالات و اثرات شکست (FMECA): روشی برای شناسایی و تحلیل تمام حالات شکست بالقوه قسمت‌های گوناگون سیستم، اثراتی که این شکست‌ها ممکن است روی سیستم داشته باشند، چگونگی جلوگیری از این شکست‌ها و یا کاهش اثرات آنها روی سیستم است.

[1] Traditional Risk Analysis Methods

- روش سنتی برای انجام تحلیل مخاطره امنیت اطلاعات: بر روی تهدیدهای شناخته شده انواع دارایی‌های رایانشی مورد استفاده در سازمان متمرکز است.

آنچه در ادامه و در قالب فصل سوم به آن پرداخته خواهد شد، شناسایی و معرفی انواع روش‌های تازه ارزیابی مخاطره در حوزه امنیت اطلاعات است که بر پایه روش سنتی برای انجام تحلیل مخاطره امنیت اطلاعات ایجاد شده و توسعه یافته‌اند.

فصل سوم

روش‌های ارزیابی
مخاطره امنیت اطلاعات

۳-۱. مقدمه

هر فعالیتی با مخاطره همراه است و انسان‌ها از زمان‌های بسیار دور به این مفهوم پی برده‌اند و به دنبال شناسایی عوامل و منابع آن هستند. موضوع امنیت اطلاعات از یک سو به عنوان مهم‌ترین عنصر فناوری اطلاعات در سازمان‌ها، بهره‌برداری از سیستم‌های امنیت اطلاعات را با چالش مخاطره مواجه کرده است و از سوی دیگر، به عنوان یکی از موضوع‌های چالش‌برانگیز در حوزه فناوری اطلاعات مطرح است که در سال‌های اخیر مورد توجه بسیاری از نهادها و مؤسسه‌ها قرار گرفته است.

از این‌رو پژوهش‌های زیادی به منظور شناسایی و بررسی عوامل کلیدی مؤثر بر امنیت اطلاعات برای اجرای موفق آن، انجام شده‌اند (Feng, Wang and Li 2014). مسأله مهم دیگری که در محیط‌های سازمانی و تصمیم‌گیری امروز مطرح است، پیچیدگی وضعیت و ترکیب اطلاعات است که دستیابی به تصمیم‌های بهینه را مشکل می‌کند و دیگر قوانین سرانگشتی و بهترین حدس و گمان کارساز نیست (Lo and Chen 2012). از کلیدی‌ترین مفاهیم در استقرار و ارتقای سیستم‌های مدیریت امنیت اطلاعات، مدیریت مخاطره است که در واقع، به یک فرآیند چندمرحله‌ای شامل شناسایی، تحلیل، ارزیابی، اولویت‌بندی و کاهش مخاطره در زمان و موقعیت مناسب اشاره دارد.

از اصلی‌ترین گام‌های مدیریت مخاطره امنیت اطلاعات، ارزیابی مخاطره امنیت اطلاعات[1] یا به اختصار (ISRA) است. 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 است. بر پایهٔ بررسی‌های اولیه انجام شده، برای دستیابی به سطح مطلوبی از محافظت در برابر تهدیدها و فراهم کردن سازوکارهای لازم جهت محافظت از دارایی‌ها و دانش سازمان تاکنون تعداد زیادی روش در قالب دستورالعمل‌ها/ راهنماها، استانداردها و چارچوب‌های ملّی و بین‌المللی از خاستگاه‌های گوناگون کاربردی و پژوهشی و به‌منظور ارزیابی مخاطره امنیت اطلاعات طراحی و به‌کار گرفته شده است. از این‌رو، به‌کارگیری روش‌های مدیریت و ارزیابی مخاطره می‌تواند تأثیر شگرفی بر شیوهٔ سازمان‌دهی فعالیت‌های سازمان‌ها در زمینه امنیت اطلاعات داشته باشد (Feng, Wang and Li 2014).

[1] Information Security Risk Assessment

بدین منظور آنچه در این فصل به تفصیل بحث می‌شود، شناسایی و معرفی انواع روش‌های موجود و تازه ارزیابی مخاطره در حوزه امنیت اطلاعات است. از این‌رو در بخش اول، به شناسایی اسناد پایه (کلیه استانداردها، چارچوب‌ها، روش‌ها، راهنماها، اصول، رهنمودها) مدیریت و ارزیابی مخاطره پرداخته و پارامترهای کیفی و شاخص‌های اولیه جهت تکمیل شناسنامه اسناد پایه استخراج می‌گردد. در بخش دوم نیز به معرفی استانداردهای مرجع ملّی و بین‌المللی در پیوند با حوزه مدیریت و ارزیابی مخاطره امنیت اطلاعات پرداخته، و در ادامه در بخش سوم، رویکردهای ارزیابی مخاطره در قالب چارچوب‌ها و راهنماهای عمومی مورد بررسی قرار خواهند گرفت. در نهایت نیز روش‌های فعلی و نوین منتخب حوزه مدیریت و ارزیابی مخاطره امنیت اطلاعات مورد تحلیل و بررسی قرار خواهند گرفت.

۳-۲. روش‌های ارزیابی مخاطره امنیت اطلاعات

روش‌های گفته‌شده در فصل پیش به عنوان روش‌های مدیریت و ارزیابی مخاطره در شکل کلی و عمومی آنها معرفی شدند. این روش‌ها و همچنین روش سنتی تحلیل مخاطره برای امنیت اطلاعات مبنایی برای ایجاد، شکل‌گیری و توسعه روش‌های نوین ارزیابی و مدیریت امنیت اطلاعات به شکل خاص هستند. بر این اساس در این بخش شناسایی و معرفی روش‌های مدیریت و ارزیابی مخاطره امنیت اطلاعات به طور خاص مورد توجه قرار گرفته است.

به شکل کلی، روش‌های متعددی برای ارزیابی مخاطره امنیت اطلاعات هستند و وظیفه اصلی سازمان تشخیص این مهم است که کدام روش را باید به کار گرفت. از آنجا که سازمان باید برای هر کدام از آن روش‌ها هزینه‌ای را صرف کند، لذا این امر ضروری است که روش انتخاب شده سازگار با الزامات سازمان و منطبق بر یکی از استانداردهای مدیریت مخاطره امنیت اطلاعات باشد. اگر پارامترهای مورد استفاده برای همه روش‌های ارزیابی مخاطره قابل اجرا باشند، سازمان‌ها می‌توانند تمامی پارامترهای ممکن را برای مشاهده عینی، و تصمیم به بهره‌برداری از بهترین روش، مورد ارزیابی قرار دهند. بدین منظور در ادامه این فصل شناسایی و معرفی روش‌های تازه ارزیابی و مدیریت مخاطره امنیت اطلاعات مورد توجه قرار گرفته است. مبتنی بر شناسایی و معرفی روش‌های تازه در این بخش، در فصل بعدی نیز کوشش خواهد شد با دسته‌بندی معیارهای شناسایی شده در ادبیات پژوهش، این امکان برای کاربر فراهم شود که بر پایهٔ میزان اهمیت و تخصیص وزن به هر یک از شاخص‌ها، نسبت به گزینش روش مناسب ارزیابی مخاطره در حوزه امنیت اطلاعات اقدام کند.

نکته‌ای که باید به آن توجه شود آن است که به شکل کلی، اصطلاح **روش** در این بخش، به کلیه استانداردها، چارچوب‌ها، روش‌ها، راهنماها، اصول، رهنمودهایی اشاره دارد که به منظور مدیریت و ارزیابی مخاطره امنیت اطلاعات منتشر شده‌اند. با توجه به اینکه همه این موارد در قالب یک یا چند سند پایه منتشر شده‌اند، از اصطلاح **سند پایه** به جای روش در فرآیند شناسایی، دسته‌بندی و ارزیابی استفاده شده است. در این بخش برای شناسایی اسناد پایه مدیریت و ارزیابی مخاطره و استخراج پارامترها و شاخص‌های اولیه، از منابع کتابخانه‌ای و اینترنتی شامل استانداردها، کتاب‌ها، مقالات و مطالعه‌های موردی استفاده شده است.

در **گام نخست** به منظور یکسان‌سازی ادبیات مورد استفاده در معرفی اسناد پایه، پارامترهای کیفی دسته‌بندی جهت تکمیل شناسنامه اسناد پایه در قالب (**جدول ۳-۱**) تعریف شده است. به بیان ساده این جدول می‌گوید که برای معرفی یک سند پایه، چه معیارهایی باید در کانون توجه باشند.

جدول ۳-۱. معیارهای دسته‌بندی جهت تکمیل شناسنامه اسناد پایه

ردیف	معیار	شرح معیار	منبع
۱	نام اختصاری	مخفف یا کوته‌نوشته نام/ عنوان سند پایه معرفی‌شده است.	-
۲	نام کامل	نام/ عنوان کامل سند پایه معرفی‌شده را نشان می‌دهد.	-
۳	ارائه‌دهنده	بیانگر نام سازمان یا مؤسسه پدیدآورنده/ منتشرکننده سند پایه است.	(Wangen and Snekkenes 2013; Agrawal 2017; Behnia, Abd Rashid and Chaudhry 2012)
۴	کشور ارائه‌دهنده	نشان‌دهنده کشوری است که سند پایه در آن ارائه شده است.	(Wangen and Snekkenes 2013; Agrawal 2017; Behnia, Abd Rashid and Chaudhry 2012; Ionita 2013; Macedo and Da Silva 2012; Kiran et al. 2013)
۵	وضعیت نسخه	نخستین تاریخ انتشار و آخرین نسخه ویرایش/ به‌روزسانی شده سند پایه را نشان می‌دهد.	(Behnia, Abd Rashid and Chaudhry 2012; Ionita 2013; Macedo and Da Silva 2012; Kiran et al. 2013)
۶	زبان	زبان(های) استاندارد ارائه‌شده سند پایه را پوشش می‌دهد.	(Agrawal 2017; Behnia, Abd Rashid and Chaudhry 2012; Ionita 2013)
۷	قیمت	بیانگر قیمت تمام شده جهت تهیه/ خرید/ دسترسی به سند پایه است.	(Agrawal 2017; Behnia, Abd Rashid and Chaudhry 2012; Ionita 2013; Macedo and Da Silva 2012; Zudin 2014; Kiran et al. 2013; Saleh and Alfantookh 2011; Spears 2004)
۸	دامنه کاربرد/ استفاده	بافت (زمینه‌هایی) است که سند پایه در آنها کاربرد دارد/ استفاده می‌شود.	(Shamala, Ahmad and Yusoff 2013; SESAR 2011; Dubois et al. 2010)
۹	هدف	ماهیت وجودی/ هدف اصلی سند پایه را بیان می‌کند.	(Agrawal 2017)
۱۰	چکیده	خلاصه‌ای از ساختار و محتوای سند پایه است.	(Kiran et al. 2013)
۱۱	مراحل مدیریت مخاطره	بیانگر گام‌های تشکیل‌دهنده فرآیند مدیریت مخاطره است.	(Kiran et al. 2013)
۱۲	متغیرها/ عملگرهای محاسبه مخاطره	مؤلفه‌ها و عملگرهای استفاده شده در فرمول محاسبه مخاطره را نشان می‌دهد.	(Ionita 2013)
۱۳	فرمول محاسبه مخاطره	چگونگی/ شیوهٔ محاسبه مخاطره را تشریح می‌کند.	(Agrawal 2017; Ionita 2013; Kiran et al. 2013)
۱۴	سازگاری با استانداردها	فهرستی از استانداردهای سازگار با سند پایه را فهرست می‌کند.	(Behnia, Abd Rashid and Chaudhry 2012; Ionita 2013; SESAR 2011; Saleh and Alfantookh 2011; Spears 2004)
۱۵	ابزارهای پشتیبان	بیانگر فهرستی از ابزارهای (سامانه‌ها، جعبه ابزارها، افزونه‌ها، و غیره) پشتیبان تجاری و غیرتجاری سند پایه است.	(Wangen and Snekkenes 2013; Behnia, Abd Rashid and Chaudhry 2012; Ionita 2013; Macedo and Da Silva 2012; SESAR 2011; Kiran et al. 2013)
۱۶	مزایا/ نقاط قوت	ویژگی‌ها/ خصوصیاتی است که افراد/ سازمان را به بهره‌برداری از آن سند پایه ترغیب می‌کند.	(Agrawal 2017; Behnia, Abd Rashid and Chaudhry 2012; Bornman and Labuschagne 2004; Kiran et al. 2013; Spears 2004)
۱۷	معایب/ نقاط ضعف	ویژگی‌ها/ خصوصیاتی است که بهره‌برداری از سند پایه را با محدودیت روبرو می‌کند.	(Agrawal 2017; Behnia, Abd Rashid and Chaudhry 2012; Bornman and Labuschagne 2004; Kiran et al. 2013; Spears 2004)
۱۸	وب‌سایت رسمی	پیوندی است که اطلاعات کاملی در ارتباط با سند پایه در اختیار قرار می‌دهد.	(Behnia, Abd Rashid and Chaudhry 2012)

در **گام دوم**، شناسایی اولیه اسناد پایه (در قالب استاندارد، روش، مدل، چارچوب، راهنما، رهنمود، اصول، و غیره) مدیریت و ارزیابی مخاطره امنیت اطلاعات مورد توجه قرار گرفت. امروزه بهره‌برداری از فنون مدیریت و ارزیابی مخاطره امنیت اطلاعات در حوزه‌های گوناگون رو به گسترش است، به طوری که تاکنون تعداد بسیار زیادی از فنون کیفی و کمّی گوناگون مدیریت و ارزیابی مخاطره در دنیا توسعه داده شده‌اند که تنها تعداد کمی از آنها مورد پذیرش بازار واقع شده‌اند و به روند حیات و توسعه خود ادامه

داده‌اند. بر پایهٔ بررسی صورت‌گرفته در ادبیات پژوهش در مجموع **۵۰** سند پایه شناسایی گردید که پس از بررسی‌های صورت‌گرفته، از بین آنها برخی با توجه به دلایلی از جمله عدم دسترسی یا منسوخ شدن در زمان بررسی، عدم به‌روزرسانی یا جایگزینی با نسخه به‌روز حذف گردید. جزئیات این اسناد پایه و دلایل حذف در قالب (**جدول ۳-۲**) بیان شده است.

جدول ۳-۲. اسناد پایه شناسایی شده اولیه و دلایل حذف برخی از آنها

ردیف	سند پایه		دلایل حذف
۱	The Australian and New Zealand Standard on Risk Management (AS/NZS 4360)		عدم بهره‌برداری از سال ۲۰۰۴ به بعد و جایگزین با استاندارد AS/NZS ISO 31000:2009 در ردیف ۳۸
۲	Austrian IT Security Handbook		✓
۳	ISACA Framework	COBIT-5 for Risk	✓
۴		Risk IT	✓
۵		Val IT	چارچوب جامع جهت حمایت سازمان‌ها از نظر حاکمیت فناوری اطلاعات، با تمرکز بر ارزش
۶	CORAS		✓
۷	CRAMM		✓
۸	Dutch A&K Analysis		از سال ۱۹۹۶ به بعد دیگر به‌روزرسانی نشده و منسوخ شده است.
۹	EBIOS		✓
۱۰	FAIR		✓
۱۱	FRAAP		✓
۱۲	ISAMM		از سال ۲۰۰۲ به بعد دیگر به‌روزرسانی نشده و منسوخ شده است.
۱۳	ISF Method	Standard of Good Practice	تمرکز بر ارائه دستورالعمل‌های سطح بالا برای امنیت اطلاعات
۱۴		Fundamental Information Risk Management (FIRM)	از سال ۲۰۰۵ به بعد دیگر به‌روزرسانی نشده و منسوخ شده است.
۱۵		Information Security Status Survey (ISF's)	تمرکز بر روی بررسی وضعیت امنیت اطلاعات
۱۶		IRAM	✓
۱۷		IRAM2	✓
۱۸		Simple to Apply Risk Analysis (SARA)	منسوخ شده و در روش IRAM ترکیب شده است.
۱۹		Simplified Process for Risk Identification (SPRINT)	منسوخ شده و در روش IRAM ترکیب شده است.
۲۰	Modelo de Avaliação de Risco (MAR)		عدم دسترسی به محتوا و جزئیات روش
۲۱	GAO/AIMD-00-33		عدم به روز رسانی از سال ۱۹۹۹
۲۲	IT Grundschutz		✓
۲۳	MAGERIT		✓
۲۴	Methodology of Analysis of Computer (Marion) Levels Risks Directed by		عدم بهره‌برداری از سال ۱۹۹۸ به بعد و جایگزین با روش MEHARI در ردیف ۲۵
۲۵	MEHARI		✓
۲۶	BSI Standard	BSI Standard 100-3	عدم بهره‌برداری از سال ۲۰۱۷ به بعد و جایگزین با استاندارد BSI 200-3 در ردیف ۲۷
۲۷		BSI Standard 200-3	✓
۲۸	ISO/IEC Guide 73		واژگان مورد استفاده در فرآیند مدیریت مخاطره در استانداردهای ISO
۲۹	ISO/IEC 13000	ISO/IEC 13335-1	ارائه مفاهیم و اصول امنیت فناوری اطلاعات قابل اجرا در سازمان‌های گوناگون
۳۰		ISO/IEC 13335-2	عدم بهره‌برداری از سال ۱۹۹۸ به بعد و جایگزین با استاندارد ISO/IEC 27005 در ردیف ۳۷
۳۱		ISO/IEC 13335-3	عدم دسترسی به محتوا و جزئیات استاندارد
۳۲	ISO/IEC 15000	ISO/IEC 15408	تمرکز بر سنجش امنیت محصولات یا سیستم‌ها با توجه به صدور گواهی
۳۳		ISO/IEC 15408 Common Criteria	مجموعه‌ای از الزام‌های امنیتی در سیستم‌ها و محصولات فناوری اطلاعات
۳۴	ISO/IEC 17799		عدم بهره‌برداری از سال ۲۰۰۷ به بعد و جایگزین با استاندارد ISO/IEC 27001 در ردیف ۳۵
۳۵	ISO/IEC 27000	ISO/IEC 27001	تمرکز بر سیستم مدیریت امنیت اطلاعات و فرآیند ممیزی و صدورگواهی (فرآیند و محتوای مدیریت مخاطره آن در استاندارد ISO/IEC 27005 آمده است)

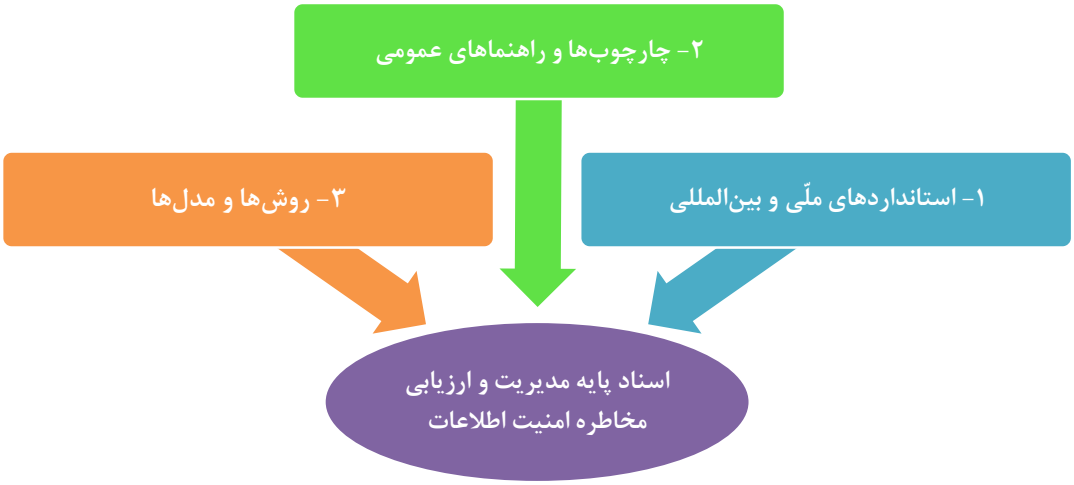
ردیف	سند پایه		دلایل حذف
۳۶	ISO/IEC 27002		تمرکز بر دستورالعمل‌های پیشنهادی برای کنترل‌های امنیت اطلاعات
۳۷	ISO/IEC 27005		✓
۳۸	ISO/IEC 31000	ISO/IEC 31000	✓
۳۹	ISO/IEC 31010		✓
۴۰	NIST SP 800-30	NIST SP 800	✓
۴۱	NIST SP 800-37		✓
۴۲	NIST SP 800-39		✓
۴۳	OCTAVE		✓
۴۴	ETSI TVRA		✓
۴۵	HB 231		عدم دسترسی به محتوا و جزئیات استاندارد
۴۶	Information Technology Infrastructure Library (ITIL)		تمرکز بر مجموعه‌ای از مفاهیم و فنون برای مدیریت زیرساخت فناوری اطلاعات و عدم تمرکز بر مدیریت
۴۷	Microsoft Security Risk Management		✓✓
۴۸	MG-2 and MG-3		عدم دسترسی به محتوا و جزئیات راهنما
۴۹	IT System Security Assessment		عدم دسترسی به محتوا و جزئیات راهنما
۵۰	Los Alamos Vulnerability and Risk Assessment (LAVA)		از سال ۱۹۸۶ به بعد دیگر به‌روزرسانی نشده و منسوخ شده است.

در **گام سوم**، از بین اسناد شناسایی شده، فهرست نهایی اسناد منتخب به منظور معرفی و ارزیابی مقایسه‌ای انتخاب شد. این اسناد در قالب (**جدول ۳-۳**) معرفی شده‌اند.

جدول ۳-۳. اسناد پایه شناسایی شده منتخب

ردیف	نام کامل سند پایه		مخفف
۱	ISO/IEC 27000	ISO/IEC 27005	ISO 27005
۲	ISO/IEC 31000	ISO/IEC 31000	ISO 31000
		ISO/IEC 31010	ISO 31010
۳	NIST SP 800	NIST SP800-30	NIST SP800-30
		NIST SP800-37	NIST SP800-37
		NIST SP800-39	NIST SP800-39
۴	BSI Series	BSI STANDARD 200-3	BSI 200-3
		IT-GRUNDSCHUTZ	IT-GRUNDSCHUTZ
۵	The European Telecommunication Standards Institute Threat Vulnerability and Risk Analysis (TVRA) Method		ETSI TVRA
۶	Austrian IT Security Handbook		Austrian IT Security Handbook
۷	Information Systems Risk Analysis and Management Methodology for		MAGERIT
۸	Microsoft's Security Risk Management Guide		Microsoft’s Security Risk Management Guide
۹	Control Objectives for Information and Related Technology for Risk		COBIT-5 for Risk
۱۰	RISK IT		RISK IT
۱۱	Consultative Objective Risk Analysis System		CORAS
۱۲	CCTA Risk Analysis and Management Method		CRAMM
۱۳	Expression des Besoins et Identification des Objectifs de Sécurité		EBIOS
۱۴	Factor Analysis of Information Risk		FAIR
۱۵	Facilitated Risk Analysis and Assessment Process		FRAAP
۱۶	Method For Harmonized Analysis Of Risk		MEHARI
۱۷	Operationally Critical Threat, Asset, And Vulnerability Evaluation		OCTAVE
۱۸	Information Risk Analysis Methodologies		IRAM/ IRAM2

سرانجام، در **گام چهارم**، به شکل کلی، و بر پایهٔ بررسی انجام شده اسناد پایه شناسایی شده از دیدگاه نوع و سطح قالب اسناد منتشر شده در سه گروه به شرح (**شکل ۳-۱**) دسته‌بندی شدند. گروه نخست اسنادی هستند که در قالب **استاندارد**[1] در سطح بین‌المللی یا ملّی منتشر شده‌اند، گروه دوم اسنادی هستند که در قالب **راهنما و چارچوب**[2] ارزیابی مخاطره امنیت اطلاعات منتشر شده‌اند، و گروه سوم نیز **روش‌ها و مدل‌هایی**[3] هستند که در سطوح اجرایی به منظور ارزیابی و مدیریت امنیت اطلاعات منتشر شده‌اند. در ادامه و در بخش‌های بعد هر کدام از این سه گروه و اسناد پایه زیر مجموعه آنها به تفکیک معرفی خواهند شد.



شکل ۳-۱. قالب‌های مدیریت و ارزیابی مخاطره

۳-۲-۱. استانداردهای ملّی و بین‌المللی مدیریت و ارزیابی مخاطره امنیت اطلاعات

بسیاری از سازمان‌ها ترجیح می‌دهند زمان زیادی صرف این بحث‌ها کنند که آیا باید «مدیریت مخاطره جامع‌نگر» در پیش گیرند یا «مدیریت مخاطره کسب‌وکار» و یا حتی «مدیریت مخاطره تمام کسب‌وکار»؟ ولی دیگر سازمان‌ها در پی آن هستند تا برنامه‌ای مرحله‌ای و تدریجی تدوین و اجرا کنند که نهادهای نظارتی و تدوین‌کننده مقررات را راضی کند. سازمان‌های موفق سازمان‌هایی هستند که مخاطره‌های موجود در مسیر تحقق اهداف سازمانی را شناسایی می‌کنند و برای دستیابی به موفقیت، آنها (مخاطره‌ها) را مدیریت می‌کنند. سازمان‌هایی که به مدیریت مخاطره اهتمام دارند، بر این نکته آگاهی دارند که اجرای استانداردهای بین‌المللی به صورت کامل یا بخشی از آنها، سازمان‌ها را قادر خواهد ساخت مخاطره‌ها را به صورت مؤثرتری مدیریت کنند و به این ترتیب در فرآیند تحقق اهداف سازمانی فرصت‌ها را به حداکثر رسانده و خسارات را به حداقل برسانند.

از این‌رو با توجه به اهمیت موضوع امنیت اطلاعات به ویژه نگاه نظام‌مند به آن و همچنین ایجاد چارچوب‌ها و سازوکارهای قابل قبول برای این حوزه، تهیه و تدوین استانداردهای گوناگون از سال‌های گذشته در دستور کار مجامع بین‌المللی و سازمان‌های ذیربط قرار گرفته است. به صورت خاص در حوزه مدیریت مخاطره امنیت اطلاعات استانداردهای خانواده ۲۷۰۰۰ و ۳۱۰۰۰ **سازمان جهانی استاندارد** (ISO) و استانداردهای خانواده ۸۰۰ **مؤسسه ملّی استانداردها و فناوری** (NIST) در حال حاضر به عنوان معتبرترین استانداردها در دنیا شناخته می‌شوند که بسیاری از شرکت‌ها و سازمان‌ها در سراسر جهان از آنها استفاده می‌کنند.

---

[1] Standard
[2] Handbook and Framework
[3] Methods and Models

همچنین در سطوح منطقه‌ای و ملّی نیز برخی استانداردها بدین منظور ایجاد شده و توسعه یافته‌اند که از آن جمله می‌توان به استانداردهای منطقه‌ای اروپا و کشور آلمان اشاره کرد.

در این بخش کوشش می‌شود ضمن معرفی استانداردهای شناسایی شده بین‌المللی و ملّی مدیریت و ارزیابی مخاطره امنیت اطلاعات، ویژگی‌ها، هدف از انتشار و آخرین وضعیت هر یک از این استانداردها بیان شود. در **(شکل ۳-۲)** درختواره استانداردهای مرجع ملّی و بین‌المللی حوزه مخاطرات امنیت اطلاعات به تصویر کشیده شده است. در ادامه معرفی مختصر و شناسنامه هر کدام از این استانداردها نیز ارائه می‌شود.

شکل ۳-۲. استانداردهای ملّی و بین‌المللی حوزه ارزیابی مخاطرات امنیت اطلاعات

۳-۲-۱-۱. استاندارد سری ISO 27000

استانداردهای خانواده ۲۷۰۰۰ نخستین دسته استاندارد در زمینه امنیت اطلاعات هستند که توسط سازمان جهانی استاندارد (ISO) و کمیسیون بین‌المللی الکتروتکنیک (IEC) منتشر شده و یا در حال تدوین می‌باشند. به شکل کلی، این خانواده دارای سه استاندارد الزام‌آوار است که سازمان‌ها می‌توانند در صورت اجرای بندها و الزامات موجود در آنها و طی مراحل ممیزی شخص ثالث، گواهینامه آن استاندارد را دریافت کنند. باید توجه داشت که سازمان‌ها به منظور پیاده‌سازی الزامات استاندارد پیش‌گفته می‌توانند از رویکردهای گوناگونی بهره‌گیری کنند، حتی ممکن است در این خصوص با بهره‌برداری از روش‌ها و مدل‌های گوناگون، اقدام به اولویت‌بندی الزامات استانداردی در مجموعه خود کرده و از این طریق فرآیند پیاده‌سازی و استقرار را مدیریت نمایند. نخستین و معروف‌ترین استاندارد الزام‌آور ISO/IEC 27001 است که به بیان الزامات سیستم مدیریت امنیت اطلاعات اختصاص دارد، ISO/IEC 27006 الزامات مربوط به شرکت‌های ممیزی‌کننده یا ارائه‌دهنده گواهی (CB) را تبیین می‌کند و ISO/IEC 27009 که الزامات پیاده‌سازی «سیستم‌های مدیریت امنیت اطلاعات» برای حوزه‌های کسب‌وکاری خاص را تدوین کرده است. دیگر استانداردهای این خانواده به عنوان مکمل و راهنمایی برای جنبه‌های گوناگون پیاده‌سازی یک سیستم مدیریت امنیت اطلاعات به صورت عمومی و اختصاصی کسب‌وکارها موجود هستند. بنابراین ذکر این نکته ضروری است که به غیر از سه استاندارد مذکور، دیگر استانداردها نظیر ISO/IEC 27002یا ISO/IEC 27005 قابلیت دریافت گواهینامه از سوی سازمان‌ها و شرکت‌های گوناگون را ندارند.

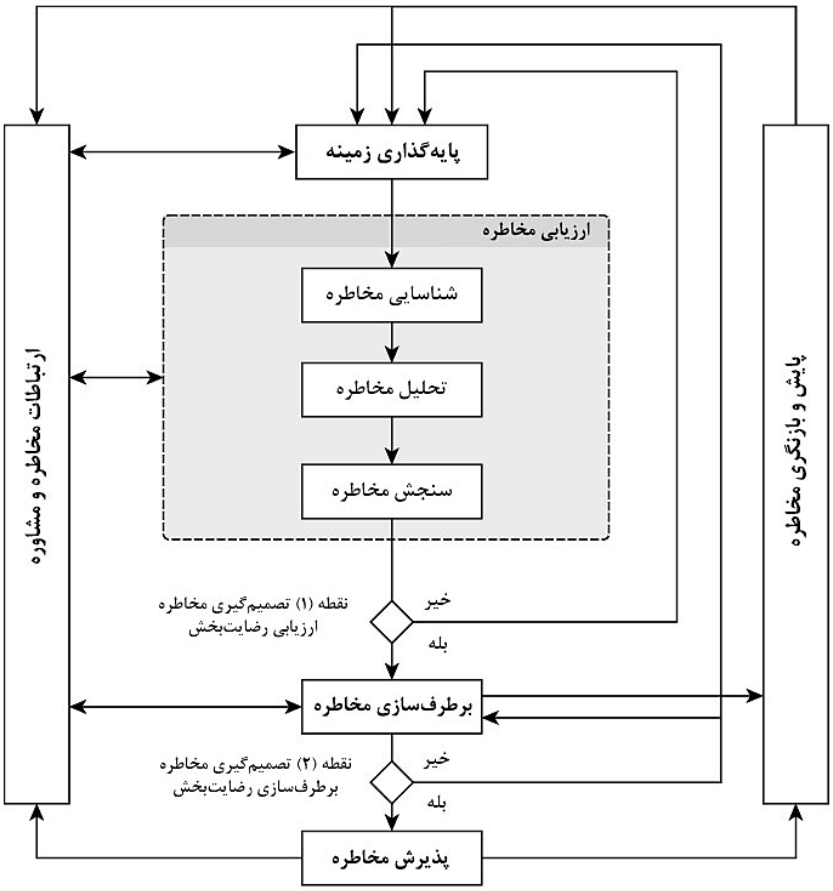
اما اصلی‌ترین استاندارد سری ۲۷۰۰۰ که به بیان الزامات سیستم مدیریت امنیت اطلاعات اختصاص دارد، استاندارد ISO/IEC 27001 است که نخستین نسخه آن بر پایه استاندارد انگلیسی BS 7799 و سپس ISO/IEC 17799، در سال ۲۰۰۵ میلادی منتشر شد. در ۲۵ سپتامبر سال (۲۰۱۳) نیز نسخه جدید این استاندارد با نام ISO 27001:2013 منتشر و جایگزین استاندارد قبلی گردید. هدف از تدوین این استاندارد بین‌المللی، مشخص کردن الزامی برای ایجاد، اجرا، بهره‌برداری، پایش، بازنگری، نگهداری، بهبود و ارتقاء یک سیستم مدیریت امنیت اطلاعات مستند شده، با درنظر گرفتن مفهوم مخاطره‌های کلان کسب‌وکار سازمان است. الزام‌های بیان شده در این استاندارد عمومی بوده و قصد آن است که در کلیه سازمان‌ها، صرف‌نظر از نوع، اندازه و

ماهیت قابل اعمال باشند. از ویژگی‌های این استاندارد وجود ۱۱۳ کنترل امنیتی در قالب ۳۵ هدف کنترلی و ۱۴ حوزه شامل خط‌مشی امنیتی، سازمان، مدیریت دارایی، امنیت منابع انسانی، امنیت فیزیکی و محیطی، امنیت عملیات، امنیت ارتباطات، کنترل‌دسترسی، رمزنگاری، ارتباط با تأمین‌کنندگان، اکتساب، توسعه و نگهداری سیستم‌های اطلاعاتی، مدیریت حوادث امنیت اطلاعات، مدیریت تداوم کسب‌وکار و انطباق است که جنبه‌های گوناگون مدیریتی، عملیاتی و فنی را در یک سازمان پوشش می‌دهد. استاندارد ISO/IEC 27001 تمامی نیازمندی‌های ضروری را جهت ایجاد و عملیات یک سیستم مدیریت امنیت اطلاعات ایجاد می‌کند که شامل مجموعه‌ای از اقدامات برای کنترل و کاهش مخاطره‌های مرتبط با دارایی‌های اطلاعاتی است. این مخاطره‌های امنیتی مواردی هستند که مورد قبول مجموعه نمی‌باشند و سازمان می‌خواهد از طریق سیستم مدیریت امنیت اطلاعات از آنها اجتناب کند. سازمان‌هایی که سیستم مدیریت امنیت اطلاعات را اجرا می‌کنند می‌توانند بر پایهٔ این استاندارد ممیزی شده و گواهینامه آن را دریافت کنند.

اما استانداردی از خانواده ۲۷۰۰۰ که بر ارزیابی و مدیریت مخاطره امنیت اطلاعات متمرکز است و در این کتاب مد نظر است، استاندارد ISO/IEC 27005 است. این استاندارد به عنوان یک استاندارد پرکاربرد در زمینه انجام مدیریت مخاطره در سازمان‌ها و شرکت‌های دارای سیستم مدیریت امنیت اطلاعات شناخته می‌شود. نسخه اولیه این استاندارد مربوط به سال ۲۰۰۸ میلادی است که پس از یک اصلاح در سال ۲۰۱۱، نسخه جدید آن در سال ۲۰۱۸ میلادی منتشر شده است. شرکت‌هایی که تمایل به پیاده‌سازی سیستم مدیریت امنیت اطلاعات دارند، معمولاً علاقه زیادی در خصوص انطباق فرآیند ارزیابی مخاطره خود سازگار با استاندارد ISO/IEC 27005 دارند و در اکثر موارد این استاندارد را به عنوان یک الزام در پیاده‌سازی سیستم مدیریت امنیت اطلاعات در نظر می‌گیرند. این استاندارد روش خاصی برای مدیریت مخاطره امنیت اطلاعات ارائه نمی‌دهد. در واقع، استاندارد شماره ISO 27005 سازمان بین‌المللی استاندارد معرف یک روش ارزیابی یا مدیریت مخاطره خاص نیست. قالب ارائه شده در این استاندارد را می‌توان یک **فرا-روش**[1] نامید. این استاندارد ارائه‌گر رویکردی است که برای انتخاب روشی مناسب برای ارزیابی و مدیریت مخاطره در سازمان کاربرد دارد (ISO 2011). رویکرد مطرح شده در این استاندارد مفاهیم عمومی مشخص شده در استاندارد ISO/IEC 27001 را پشتیبانی می‌کند. استاندارد ISO/IEC 27005 راهنمای دستیابی به رویکرد مدیریت مخاطره فرآیندگرا را برای کمک به اجرای رضایت‌بخش و سازگار با الزام‌های مدیریت مخاطره امنیت اطلاعات در استاندارد ISO/IEC 27001 فراهم می‌کند.

این استاندارد به شکل مرحله‌ای و فارغ از روش ارزیابی و مدیریت مخاطره، فرآیند مدیریت مخاطره را در قالب (**شکل ۳-۳**) تعریف کرده است (ISO 2011). در حالی‌که مراحل اصلی مشابه استاندارد NIST SP 800-30 است، تفاوت‌های آن در این است که در این روش جنبه‌های سازمانی، مانند مرحله پذیرش مخاطره و ارتباط با مخاطره، بخش‌هایی صریح و آشکار از کل روش‌شناسی مدیریت مخاطره هستند. همچنین ISO 27005 به شکل کلی، قصد دارد تا جایگاه راهنما بودن (به جای الزام بودن) استاندارد را بیش از پیش برای مخاطبین تبیین کند.

[1] Meta-Method



شکل ۳-۳. فرآیند مدیریت مخاطره امنیت اطلاعات بر پایهٔ استاندارد ISO 27005، (ISO 2011)

در این استاندارد مدیریت مخاطره امنیت اطلاعات، شامل مراحل زیر است:

۱. **پایه‌گذاری زمینه**: در این مرحله زمینه داخلی و خارجی مدیریت مخاطره امنیت اطلاعات پایه‌گذاری می‌شود که شامل تنظیم معیارهای بنیادی برای مدیریت مخاطره امنیت اطلاعات است. موارد زیر در این مرحله مد نظر قرار می‌گیرد:

- تعیین رویکرد و روش مدیریت مخاطره؛
- تعیین معیارهای ارزیابی مخاطره؛
- تعیین معیارهای پیامد؛
- تعیین معیارهای پذیرش مخاطره؛
- تعریف محدوده و قلمرو مدیریت مخاطره امنیت اطلاعات؛ و
- سازماندهی.

۲. **شناسایی مخاطره**: هدف از شناسایی مخاطره، تعیین عواملی است که می‌توانند علت زیان بالقوه باشند و اینکه چگونه، کجا و چرا زیان ممکن است رخ دهد. گام‌های زیر در شناسایی مخاطره وجود دارند:

- شناسایی و ارزش‌گذاری دارایی‌ها؛
- شناسایی تهدیدها؛
- شناسایی کنترل‌های موجود؛
- شناسایی آسیب‌پذیری‌ها؛ و
- شناسایی پیامدها.

۳. **تحلیل مخاطره**: تحلیل مخاطره با توجه به سطح جزئیات موردنظر، میزان حیاتی بودن دارایی‌ها، گستره آسیب‌پذیری‌های شناخته شده و نیز رخدادهای دربرگیرنده سازمان انجام می‌شود. روش تحلیل مخاطره می‌تواند کمّی و یا کیفی و یا تلفیقی از هر دو باشد. این مرحله شامل گام‌های زیر است:
   - ارزیابی پیامدها؛
   - سنجش احتمال رخداد؛ و
   - تعیین سطح مخاطره.

۴. **سنجش مخاطره**: در این گام سطوح مخاطره با معیار ارزیابی مخاطره و معیار پذیرش آن، مقایسه می‌شود.

۵. **برطرف‌سازی مخاطره**: در این گام کنترل‌هایی جهت مقابله با مخاطره امنیت اطلاعات انتخاب می‌شوند. به منظور مقابله با مخاطره چهار رویکرد وجود دارد که عبارتند از:
   - اصلاح (کاهش) مخاطره؛
   - حفظ مخاطره؛
   - اجتناب از مخاطره؛ و
   - انتقال مخاطره.

۶. **پذیرش مخاطره**: در این گام تصمیم‌گیری در خصوص پذیرش مخاطره امنیت اطلاعات صورت می‌گیرد. باید توجه داشت که تصمیم‌های مرتبط با پذیرش مخاطره و نیز مسئولیت تصمیم‌گیری باید به طور رسمی ثبت شود.

۷. **ارتباطات مخاطره و مشاوره**: اطلاعات مرتبط با مخاطره باید بر پایهٔ سطوح مناسب دسترسی در سازمان مبادله و یا مابین تصمیم‌گیران و دیگر ذی‌نفعان به اشتراک گذاشته شود.

۸. **پایش و بازنگری مخاطره**: مخاطره و دیگر مؤلفه‌های درگیر در فرآیند مدیریت مخاطره امنیت اطلاعات (مانند ارزش دارایی‌ها، پیامدها، تهدیدها، آسیب‌پذیری‌ها، احتمال وقوع) به منظور شناسایی تغییرات محتمل در سازمان و برای حفظ صحت و دقت ارزیابی‌های صورت گرفته در طول زمان باید مورد پایش و بازنگری قرار گیرند.

همان طور که نشان داده شد، فرآیند مدیریت مخاطرات امنیت اطلاعات می‌تواند برای فعالیت‌های ارزیابی مخاطره و یا مقابله با مخاطره به صورت تکرارپذیر انجام گیرد. رویکرد تکرارپذیر به منظور هدایت ارزیابی مخاطره می‌تواند عمق و جزئیات ارزیابی را در هر تکرار افزایش دهد. این رویکرد تکراری، هنگامی که این اطمینان به وجود آمد که مخاطره سطح بالا به صورت مناسبی ارزیابی شده‌اند، تعادل مناسبی میان حداقل زمان ممکن و تلاش‌های مربوط به شناسایی کنترل‌ها فراهم می‌آورد.

جدول ۳-۴. شناسنامه (۱): استاندارد ISO 27000 Series

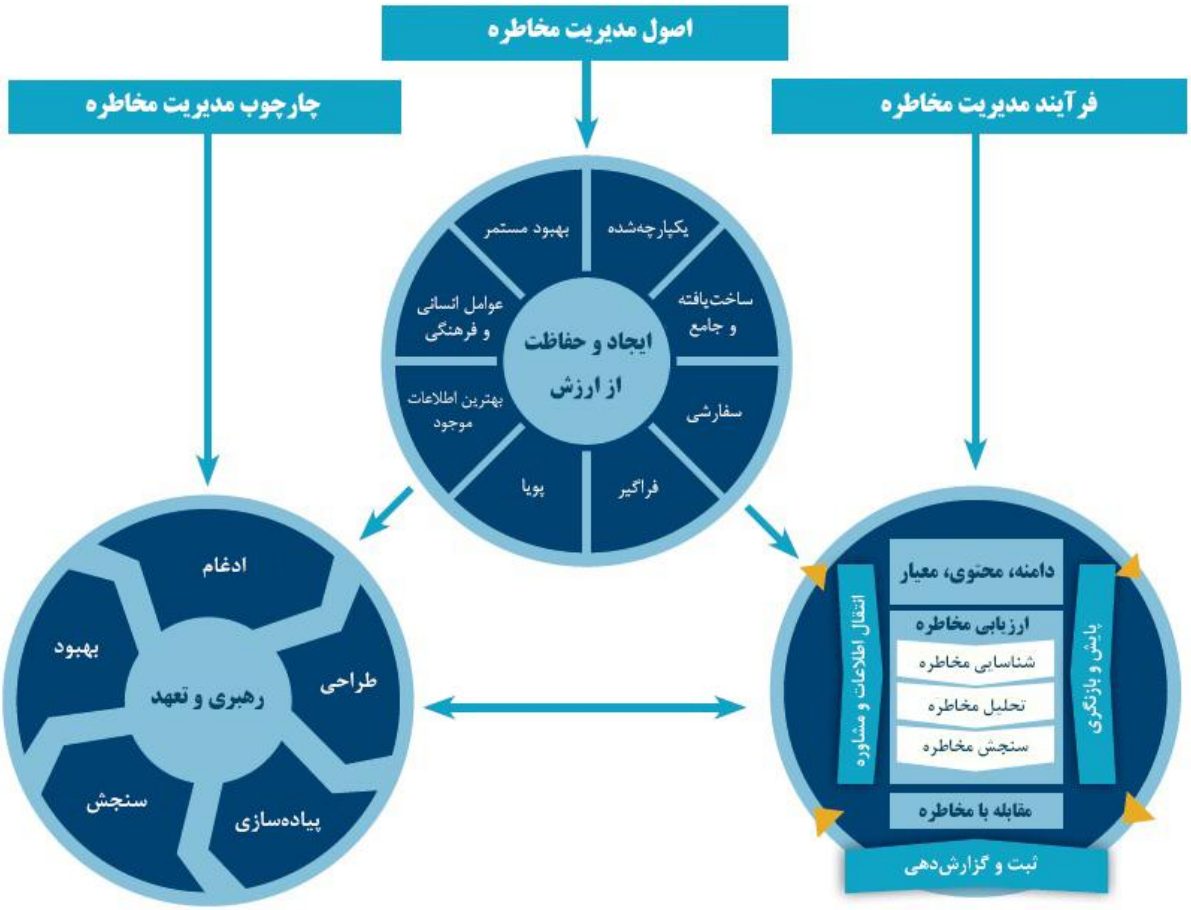
شناسنامه استاندارد ISO 27000 Series	
نام اختصاری	ایزو ۲۷۰۰۰- ISO 27000 Series (شناسنامه با تمرکز بر ISO 27005 تدوین شده است)
نام کامل	فناوری اطلاعات- فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات
ارائه‌دهنده	سازمان بین‌المللی استاندارد و کمیسیون بین‌المللی الکترونیک
کشور ارائه‌دهنده	سوئیس
وضعیت نسخه	نخستین نسخه این استاندارد در سال ۲۰۰۸ میلادی منتشر شد، نسخه دوم در سال ۲۰۱۱ میلادی به چاپ رسید و در حال حاضر نسخه ۲۰۱۸ این استاندارد در ۵۶ صفحه به عنوان آخرین نسخه معتبر محسوب می‌شود.
زبان	انگلیسی، فرانسوی
قیمت	با پرداخت هزینه در دسترس است.
دامنه کاربرد/ استفاده	* یک فرآیند منطقی، نظام‌مند، ساختاریافته از تحلیل مخاطره تا ایجاد طرح مقابله با مخاطره را مشخص می‌کند. * یک استاندارد پرکاربرد در زمینه انجام مدیریت مخاطره در سازمان‌ها و شرکت‌های دارای سیستم مدیریت امنیت اطلاعات است.
هدف	* ارائه دستورالعمل‌هایی برای مدیریت مخاطره امنیت اطلاعات. * برقراری تعادل مناسب میان حداقل زمان ممکن و تلاش‌های مربوط به شناسایی کنترل‌ها جهت کاهش مخاطره‌های سطح بالا. * این روش با هدف کمک به اجرای رضایت‌بخش امنیت اطلاعات بر پایهٔ رویکرد مدیریت مخاطره طراحی شده است.
مراحل مدیریت مخاطره	فرآیند مدیریت مخاطره در این استاندارد شامل پایه‌گذاری زمینه، ارزیابی مخاطره (شناسایی مخاطره، تحلیل مخاطره، سنجش مخاطره)، برطرف‌سازی مخاطره، پذیرش مخاطره، ارتباطات مخاطره و مشاوره و در نهایت پایش و بازنگری مخاطره است.
فرمول محاسبه مخاطره	پیشنهادهایی در خصوص محاسبه مخاطره در قالب ساختارهای (مخاطرات سطح بالا، ارزیابی جزئی، ماتریس با ارزش‌های از پیش تعیین شده، رتبه‌بندی تهدیدها توسط اندازه‌گیری مخاطره، ارزیابی ارزش برای احتمال و پیامدهای مخاطره) ارائه می‌دهد که در تمامی این روش‌ها، متغیرهای احتمال وقوع تهدید، شدت آسیب‌پذیری، پیامد حادثه (ارزش دارایی اطلاعاتی) به عنوان متغیرهای اصلی معرفی شده است، اما فرمول مشخصی ارائه نداده است.
سازگاری با استانداردها	این استاندارد با استانداردهای ISO 27001، سری ISO 31000 و Risk Assessment سازگار است.
ابزارهای پشتیبان	مبتنی بر این استاندارد ابزارهای پشتیبان پولی Manager CCS Risk، Countermeasures، Manager Modulo Risk، Proteus Enterprise، Resolver، Ballot و ابزار پشتیبان رایگان EBIOS ایجاد شده است.
مزایا/ نقاط قوت	+ رویکردی جامع؛ + بسیار ساده و نظام‌مند؛ + پشتیبانی شده توسط دسته‌بندی گسترده و استانداردشده، مدل مفهومی و چارچوب مدیریت مخاطره (سری ISO 31000، ISO 13335) + از رویکرد مبتنی بر تکرار برای ارزیابی مخاطره پشتیبانی می‌کند؛ + بر پایهٔ چرخه «پی.دی.سی.ای.» عمل می‌کند؛ + تشریح فرآیند ارزیابی مخاطره در یک سطح بسیار جزئی؛ + شرح مفصل رویکرد؛ + ساختاریافته؛ + امکان استفاده آسان به عنوان یک استاندارد مرجع و جامع؛
معایب/ نقاط ضعف	- روش خاصی را تشریح نمی‌کند، ولی توصیه‌های عمومی جهت انتخاب و بهره‌برداری از چنین روش‌هایی را ارائه می‌دهد؛ - فرمول مشخصی ارائه نمی‌کند؛ - فراوانی اطلاعات بی‌ربط برای یک پروژه ارزیابی مخاطره امنیت اطلاعات؛ - درک روش برای تازه‌کارها به دلیل استفاده گسترده از عبارات، نفسیرها و اصطلاحات فنی بسیار سخت است؛ - یافتن اطلاعات مرتبط و یادگیری آنها با توجه به جامعیت روش دشوار است؛ - همانند روش OCTAVE، تیم‌ها با توضیحات فنی که به زبان مادری آنها بیان نشده است، با مشکل روبرو هستند؛
وب‌سایت‌رسمی	https://www.iso.org/standard/75281.html

۳-۲-۱-۲. استاندارد سری ISO 31000

استاندارد سری ISO 31000 یک استاندارد بین‌المللی برای مدیریت مخاطره است. این استاندارد مجموعه‌ای از اصول، چارچوب و فرآیندهای مدیریت مخاطره را فراهم می‌کند که به سازمان‌ها کمک می‌کند تا نسبت به مخاطره‌های پیش‌روی خود رویکردی پیشگیرانه داشته باشند. نخستین نسخه استاندارد ISO 31000 در تاریخ ۱۳ نوامبر سال ۲۰۰۹ میلادی منتشر شد. هدف این استاندارد در آن زمان، تهیه اصول و دستورالعمل‌های عمومی دربارهٔ مدیریت مخاطره با ارائه یک رویکرد مشترک برای فرآیندهای مدیریت مخاطره در حمایت از استانداردهای مقابله با مخاطره‌های خاص (بدون جایگزینی این استانداردها) بود. با این حال نسخه ISO 31000 در سال ۲۰۰۹ میلادی قصد ارتقاء یکپارچگی مدیریت مخاطره در سازمان‌ها را نداشت.

ویرایش جدید استاندارد ISO 31000 در فوریه سال ۲۰۱۸ میلادی با نام "مدیریت مخاطره-رهنمودها" منتشر و جایگزین نسخه قبلی آن گردید. استاندارد اصلاح شده، راهنمایی واضح‌تر و مختصرتری ارائه می‌دهد که به سازمان‌ها کمک می‌کند تصمیم‌گیری بهتری داشته باشند. این استاندارد بر یکپارچگی مدیریت مخاطره در سازمان و نقش و مسئولیت رهبری تأکید دارد. با توجه به اینکه ISO 31000:2018 از زبانی ساده‌تر استفاده می‌کند بنابراین برای همه ذینفعان در دسترس است.

چارچوب کلی، اصول و فرآیندهای این استاندارد در قالب (**شکل ۳-۴**) به تصویر کشیده شده است. این استاندارد ممکن است برای طیف گسترده‌ای از فعالیت‌ها و یا عملیات شرکت‌های دولتی، خصوصی، جامعه و یا گروه‌ها اعمال شود. این استاندارد به سازمان‌ها کمک می‌کند تا چارچوبی را که هدف از آن ادغام راهبردهای مدیریت مخاطره در کلیه فرآیندهای سازمانی ازجمله تصمیم‌گیری است، ایجاد، پیاده‌سازی و به طور مداوم بهبود دهند.



شکل ۳-۴. چارچوب، اصول و فرآیندهای استاندارد ISO 31000، (ISO 2018)

استاندارد ISO 31000 علاوه بر رهنمودهایی که برای شناسایی زمینه‌های داخلی و خارجی در نظر گرفته است، بزرگ‌ترین ارزش آن در ارائه یک چارچوب برای مدیریت انواع مخاطره‌های موجود در سطح شرکت و فراتر از امنیت اطلاعات است؛ این استاندارد می‌تواند کمک کند مدیریت مخاطره در برخی از مسائل سازمانی درک شود. از آنجایی‌که استاندارد ISO 31000 در خصوص شیوهٔ مدیریت مخاطره به صورت راهبردی و جامع است، می‌تواند به عنوان یک چارچوب عالی برای **مدیریت مخاطره سازمانی** در نظر گرفته شود. این استاندارد بر روی مدیریت مخاطره به شکل کلی، متمرکز بوده و راهبردها و توصیه‌های آن می‌تواند در حوزه مدیریت مخاطره امنیت اطلاعات مورد استفاده قرار گیرد.

این استاندارد بین‌المللی در صورتی که سازمان علاقه‌مند به فراهم آوردن رهنمودهای جامع در جهت کمک به تقویت فرآیند تصمیم‌گیری و مدیریت کلی خود باشد، دارای اهمیت است. ISO 31000 برای ساده‌کردن اداره شرایط پیچیده در نظر گرفته شده است که به تصمیم‌هایی مهم برای دستیابی به یک رویکرد ساختاری شناسایی و ارزیابی مخاطره‌ها نیاز دارد.

اما استانداردی از سری ۳۱۰۰۰ که فنون ارزیابی مخاطره را مورد توجه ویژه قرار داده است، استاندارد ISO 31010 (مدیریت مخاطره-تکنیک‌های ارزیابی مخاطره) است که توسط کمیته فنی کمیسیون بین‌المللی الکتروتکنیک[1] و با همکاری کمیته فنی سازمان جهانی استاندارد تدوین شده است. ویرایش جدید استاندارد ISO 31010 در سال ۲۰۱۹ با یک بازنگری فنی نسبت به نسخه پیشین منتشر و جایگزین ISO 31010:2009 گردید، این استاندارد دامنه‌ای از فنون را برای تشخیص و فهم مخاطره‌ها در برمی‌گیرد. این استاندارد برای گسترش کاربردها و افزایش جزئیات به‌روزرسانی شده است و مکمل استاندارد ISO 31000 است. این استاندارد بین‌المللی راهنمایی در ارتباط با انتخاب و بهره‌برداری از فنون ارزیابی مخاطره در طیف گسترده‌ای از موقعیت‌ها ارائه می‌دهد. این فنون با ارائه اطلاعاتی در ارتباط با مخاطره‌های خاص و در مواردی که عدم اطمینان وجود دارد، به عنوان بخشی از یک فرآیند مدیریت مخاطره برای کمک به فرآیند تصمیم‌گیری استفاده می‌شوند. این فنون در موارد ذیل مورد استفاده قرار می‌گیرند:

- زمانی‌که به درک بهتری از مخاطره‌های موجود و یا یک مخاطره خاص نیاز باشد؛
- در فرآیند تصمیم‌گیری، جایی که طیف وسیعی از گزینه‌ها -که هر کدام شامل مخاطره هستند- نیاز به مقایسه یا بهینه‌سازی دارند؛
- در فرآیند مدیریت مخاطره که منجر به اقدام‌هایی جهت مقابله/ مواجهه با مخاطره می‌شود.

این فنون در مراحل ارزیابی مخاطره (شامل شناسایی، تحلیل و سنجش مخاطره) همان طور که در استاندارد ISO 31000 شرح داده شده است، و به شکل کلی، هر زمان که به درک عدم اطمینان و پیامدهای آن نیاز باشد، استفاده می‌شوند. فنون معرفی شده در این استاندارد را می‌توان در طیف وسیعی از زمینه‌ها استفاده کرد، هرچند اکثر آنها از حوزه و دیدگاه فنی نشأت گرفته‌اند. برخی از فنون از نظر مفهوم مشابه هستند، اما اسامی و روش‌های گوناگونی دارند که روند توسعه آنها در بخش‌های گوناگون را نشان می‌دهد. فنون با گذشت زمان تکامل یافته و همچنان در حال تکامل هستند و بسیاری از آنها می‌توانند در طیف وسیعی از موقعیت‌های خارج از کاربری اصلی خود مورد استفاده قرار گیرند. این فنون می‌توانند برای تأمین نیازهای فعلی و آینده توسعه داده شده و یا با روش‌های جدید سازگار، ترکیب و به کار برده شوند.

این استاندارد ماهیتی کلی دارد تا بتواند برای تمامی صنایع و انواع سیستم‌ها رهنمودهایی را ارائه کند. همچنین این استاندارد به معرفی فنون ارزیابی مخاطره می‌پردازد و آنها را از لحاظ کاربرد، مزایا و محدودیت‌هایی که با خود به همراه دارند، مورد مقایسه قرار می‌دهد. در واقع، هدف از این استاندارد منعکس ساختن رویه‌های خوب فعلی در انتخاب و به‌کارگیری فنون ارزیابی مخاطره است. هر فن برای مراحل گوناگون فرآیند ارزیابی مخاطره (شامل شناسایی مخاطره، تحلیل مخاطره-تحلیل عواقب، تحلیل مخاطره-

[1] The International Electrotechnical Commission (IEC)

برآورد کیفی، نیمه کمّی یا کمّی احتمال، تحلیل مخاطره-ارزیابی اثربخشی هر کنترل موجود، تحلیل مخاطره-برآورد سطح مخاطره، سنجش مخاطره) قابل استفاده است. برخی از فنون در مراحل دیگر فرآیند نیز مورد استفاده قرار می‌گیرند. به عنوان نمونه، در (**شکل ۳-۵**) یک نمای کلی از فنون مورد استفاده در فرآیند مدیریت مخاطره استاندارد ISO 31000 نشان داده شده است. این فهرستی جامع از فنون قابل استفاده در هر مرحله نیست و فقط به عنوان نمونه به آن اشاره شده است.

شکل ۳-۵. کاربرد فنون در فرآیند مدیریت مخاطره استاندارد ISO 31000، (Peace 2017)

جدول ۳-۵. شناسنامه (۲): استاندارد سری ISO 31000

شناسنامه استاندارد سری ISO 31000	
نام اختصاری	ایزو ۳۱۰۰۰- ISO 31000 Series (شناسنامه با تمرکز بر ISO 31000 تدوین شده است).
نام کامل	مدیریت مخاطره، اصول، خط‌مشی‌ها، رهنمودها و فنون ارزیابی مخاطره
ارائه‌دهنده	سازمان بین‌المللی استاندارد، کمیسیون بین‌المللی الکتروتکنیک
کشور ارائه‌دهنده	سوئیس
وضعیت نسخه	نسخه اولیه استاندارد ISO 31000 تحت عنوان اصول و رهنمودهای مدیریت مخاطره در سال ۲۰۰۹ میلادی منتشر شد. در حال حاضر آخرین ویرایش این استاندارد تحت عنوان ISO 31000:2018 معتبر و مورد استفاده سازمان‌ها است. نخستین نسخه استاندارد ISO 31010 در سال ۲۰۰۹ میلادی منتشر شد و در حال حاضر نسخه ۲۰۱۹ این استاندارد در ۲۶۴ صفحه به عنوان آخرین نسخه معتبر محسوب می‌شود.
زبان	انگلیسی، فرانسوی، اسپانیایی
قیمت	با پرداخت هزینه در دسترس است.
دامنه کاربرد/ استفاده	این استاندارد می‌تواند مورد استفاده هر بنگاه عمومی، خصوصی یا اجتماعی، انجمن، گروه یا فرد قرار گیرد. بنابراین این استاندارد، خاص هیچ صنعت یا بخشی نیست. این استاندارد را می‌توان در کل عمر یک سازمان و به عنوان راهنمایی جهت انتخاب و بهره‌برداری از روش‌های ارزیابی مخاطره در گستره‌ای وسیع از فعالیت‌ها و موقعیت‌ها به کار برد، ازجمله راهبردها و تصمیم‌ها، عملیات، فرآیندها ، وظایف، پروژه‌ها، محصولات، خدمات و دارایی‌ها. این استاندارد را می‌توان دربارهٔ هر نوع مخاطره با هر ماهیتی به کار برد، چه دارای پیامد مثبت باشد و چه منفی (مانند ایمنی، محیط زیست، امنیت، مالی، و غیره).
هدف	هدف از تدوین این استاندارد ارائه اصول و رهنمودهای عام دربارهٔ مدیریت مخاطره است. در واقع، از این استاندارد برای هماهنگ‌سازی فرآیندهای مدیریت مخاطره در استانداردهای موجود و استانداردهای آتی استفاده می‌شود. این استاندارد رویکردی مشترک در پشتیبانی از استانداردهایی ارائه می‌دهد که به مخاطره‌ها و یا بخش‌های خاصی می‌پردازند و جایگزینی برای آن استانداردها نیست. همچنین، راهنمایی دربارهٔ انتخاب و به کارگیری فنون نظام‌مند برای ارزیابی مخاطره ارائه می‌دهد.
مراحل مدیریت مخاطره	فرآیند مدیریت مخاطره شامل پنج مرحله تشخیص شرایط، شناسایی خطرات مرتبط با ریسک، ارزیابی و تعیین مخاطره، کنترل مخاطره‌های ارزیابی شده و بررسی پیامد مخاطره‌ها است.
فرمول محاسبه مخاطره	پیشنهادهایی در خصوص محاسبه مخاطره ارائه می‌دهد، اما فرمول مشخصی ارائه نداده است. ازجمله فنون مورد استفاده در فرآیند مدیریت مخاطره می‌توان به فنونی برای تحلیل کنترل‌ها، فنونی برای درک احتمال و نتیجه، فنونی برای تحلیل وابستگی‌ها و تعاملات، فنون ارائه‌دهنده معیار مخاطره، فنونی برای استخراج دیدگاه‌ها، فنونی برای شناسایی مخاطره، فنونی برای تعیین منابع، دلایل و محرک‌های مخاطره، فنونی برای سنجش اهمیت مخاطره و فنونی برای انتخاب از این گزینه‌ها اشاره نمود.
سازگاری با استانداردها	فرآیند ارزیابی و مقابله با مخاطره امنیت اطلاعات در استاندارد ISO 27001:2013 با اصول و راهنمایی‌های کلان موجود در استاندارد ISO 31000 منطبق است. این استاندارد با استانداردهای ISO Guide 73، ISO/IEC 31010 و ISO 27005 سازگار است.
ابزارهای پشتیبان	هر یک از فنون از ابزارهای مخصوص به خود پشتیبانی می‌کند.
مزایا/ نقاط قوت	+ افزایش احتمال دستیابی به اهداف و بهبود کنترل‌ها؛ + ترغیب به مدیریت پیشگیرانه و بهبود شناسایی فرصت‌ها و تهدیدها؛ + ایجاد آگاهی از لزوم شناسایی، کاهش و مقابله با مخاطره در کل سازمان؛ + انطباق با الزام‌های قانونی و مقرراتی و نُرم‌های بین‌المللی مربوطه و بهبود حاکمیت؛ + ایجاد پایه و اساس ثابت برای تصمیم‌گیری و برنامه‌ریزی؛ + تخصیص و استفاده مؤثر از منابع جهت مقابله با مخاطره و توانایی سازمان در هدایت منابع بر روی مخاطره‌های مهم‌تر و اثرگذارتر؛ + بهبود پیشگیری از خسارت و مدیریت حادثه و حداقل‌سازی خسارات؛ + بهبود یادگیری و تاب‌آوری سازمانی؛ + مدیریت و کنترل تأثیر پیامدهای منفی و یا مثبت بر روی اهداف سازمانی؛ + قابلیت اتخاذ تصمیم آگاهانه با توجه به مدیریت اثرات منفی بالقوه مخاطره‌ها و سود جستن از فرصت‌ها؛ + ارتقاء عملکرد سلامت و ایمنی سازمان و جلوگیری از غافلگیر شدن و افزایش کارایی سازمان و اثربخشی عملیات؛ + یکپارچه‌سازی فرآیندهای مدیریت مخاطره با دیگر فرآیندهای مدیریتی سازمان؛ + کاهش هزینه‌ها از طریق مدیریت مخاطره مناسب و بهبود گزارش‌دهی مالی؛ + واکنش مؤثر به تغییرات و یافتن راهکارهای مناسب؛ + ایجاد و حفظ ارزش، به دست آوردن برتری رقابتی و اطمینان و اعتماد ذی‌نفعان؛ + این استاندارد بر روی مدیریت مخاطره به شکل کلی، متمرکز بوده و راهبردها و توصیه‌های آن می‌تواند در حوزه مدیریت مخاطره امنیت اطلاعات مورد استفاده قرار گیرد.
معایب/ نقاط ضعف	- عدم پیشنهاد فرمول خاص محاسبه مخاطره و ارائه پیشنهادهای کلی؛ - عدم ارائه تحلیل مقایسه‌ای برای فنون گوناگون.
وب‌سایت‌رسمی	https://www.iso.org/standard/65694.html

۳-۲-۱-۳. استاندارد سری NIST 800

مستندات سری ۸۰۰ سازمان NIST مجموعه‌ای از نشریاتی هستند که توسط مؤسسه ملّی استانداردها و فناوری -یک آژانس غیرنظارتی از وزارت بازرگانی ایالات متحده آمریکا- ارائه شده است. سری ۸۰۰ در سال ۱۹۹۰ میلادی ایجاد و از آن زمان رشد کمی داشته است و شامل مجموعه‌ای کامل، عمیق و همیشه در حال رشد از مستندات امنیتی رایانه است که توسط بسیاری از افراد پیشرو در صنعت دیده می‌شود. علاوه‌براین مستندات سری ۸۰۰ برای بسیاری از متخصصان فناوری اطلاعات -به ویژه از نظر امنیت اطلاعات- شناخته شده است، همان طور که آنها در سال ۲۰۰۲ میلادی با قانون مدیریت امنیت اطلاعات فدرال -معروف به **قانون مدیریت امنیت اطلاعات فدرال**[1] یا به اختصار (FISMA)- آشنا شدند. «FISMA» اساساً مجموعه‌ای منسجم از دستورالعمل‌های امنیت اطلاعات را برای آژانس‌های فدرال و دیگر اشخاص وابسته ایجاد کرد که در آن از سری انتشارات ۸۰۰ به عنوان بخشی از انطباق با «FISMA» مورد استفاده قرار گرفت (و هنوز هم وجود دارد). از آنجا که بسیاری از آژانس‌های فدرال به بخش خصوصی برون‌سپاری می‌کنند، این امر به نوبه خود مستلزم آن است که بسیاری از پیمانکاران، پیمانکاران فرعی و دیگر شرکت‌های وابسته با همان استانداردهای «FISMA» که این آژانس‌ها دارند، مطابقت کنند. در حال حاضر بسیاری از شرکت‌های خصوصی از مجموعه نشریات سری ۸۰۰ سازمان NIST -مانند بسیاری از آژانس‌های فدرال- برای ایجاد و حفظ به‌روش‌ها دربارهٔ امنیت اطلاعات استفاده می‌کنند.

در واقع نشریات سری ۸۰۰ سازمان NIST گزارش‌هایی از تحقیقات، دستورالعمل‌ها و تلاش‌های چارچوب **کتابخانه زیرساخت فناوری اطلاعات**[2] یا به اختصار (ITIL) در زمینه امنیت سیستم‌های اطلاعاتی هستند و همکاری‌های این آزمایشگاه با سازمان‌های علمی، دولتی و صنعتی را گزارش می‌کنند.

تمامی نشریات سری ۸۰۰ این سازمان بسیار جامع و دقیق هستند و اطلاعات به روز و مرتبطی را دربارهٔ یک موضوع خاص ارائه می‌دهند. از جمله مشهورترین و شناخته‌شده‌ترین نشریات سری ۸۰۰ در حوزه مخاطرات امنیت اطلاعات می‌توان به استاندارد NIST 800-30، NIST 800-37 و NIST 800-39 اشاره کرد که در ادامه هر یک به تفصیل مورد بررسی قرار خواهند گرفت.

۳-۲-۱-۳-۱. استاندارد NIST 800-30

مستند بهترین تجربیات شماره ۳۰-۸۰۰ مؤسسه ملّی استانداردها و فناوری تحت عنوان «**راهنمای مدیریت مخاطرات سیستم‌های فناوری اطلاعات**»[3] منتشر شده است (NIST 2002). این مستند، روش به‌روزرسانی شده مدیریت مخاطره امنیت اطلاعات، ارائه شده «گالاگر» و «بلنک» در سال (۲۰۱۲) است که نسخه ابتدایی آن در سال (۲۰۰۲) میلادی منتشر شد. این مستند از ارزیابی مخاطره به عنوان نخستین قدم در مدیریت مخاطره یاد می‌کند. این روش شامل مؤلفه‌های ۱- قالب‌بندی مخاطرات، ۳- ارزیابی مخاطرات، ۳-پاسخ به مخاطرات و ۴- پایش مخاطرات است. **مؤلفه نخست** یعنی قالب‌بندی مخاطره، به تعریف مخاطره اشاره دارد، یعنی تولید یک راهبرد مدیریت مخاطره که شیوهٔ ارزیابی مخاطره، پاسخ به مخاطره و پایش مخاطره را تعریف می‌کند. **مؤلفه دوم** یعنی ارزیابی مخاطره، ویژگی‌های اصلی مخاطرات، یعنی تهدیدها برای سازمان‌ها، آسیب‌پذیری‌های داخلی و خارجی سازمان‌ها، تأثیر یا آسیب‌هایی را که ممکن است در هنگام تهدیدها از سوء بهره‌برداری از آسیب‌پذیری‌ها و احتمال وقوع چنین حادثه‌ای ایجاد کند، شناسایی می‌کند. در **مؤلفه سوم** یعنی پاسخ به مخاطرات، این راهبرد تدوین شده است که پس از تعریف مخاطره در مرحله ارزیابی، به یک مخاطره پاسخ دهد تا بتواند یک واکنش گسترده و سازمانی در چارچوب مخاطره سازمانی ایجاد کند و بتواند با اثرات منفی مخاطرات مقابله کند. سرانجام، **مؤلفه چهارم** یعنی پایش مخاطره، چگونگی نظارت بر مخاطرات را با

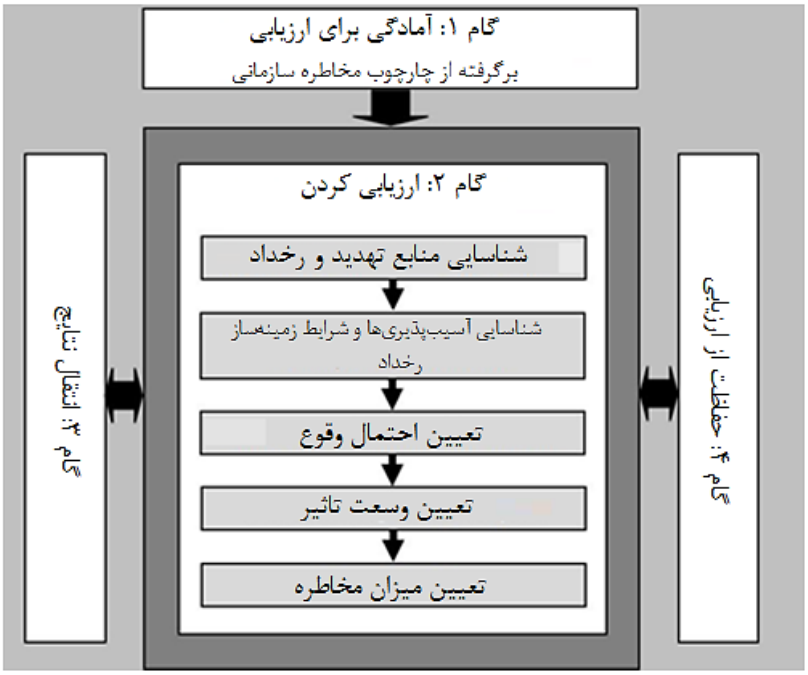
1 The Federal Information Security Management Act (FISMA)

2 Information Technology Infrastructure Library (ITIL)

3 Special Publications Risk management Guide for Information Technology Systems

گذشت زمان تعیین می‌کند، به گونه‌ای که اثربخشی مداوم راهبردهای کاهش مخاطره به صورت مکرر ارزیابی شده و هرگونه تغییر مخاطره‌پذیر در سیستم‌ها و محیط‌های اطلاعاتی سازمانی مشخص می‌شود. در واقع، این سند بر چگونگی آماده‌سازی برای ارزیابی مخاطره، چگونگی انجام ارزیابی، چگونگی اشتراک‌گذاری نتایج مخاطره با کارمندان کلیدی و نیز چگونگی حفظ این ارزیابی در دوره‌های گوناگون تمرکز دارد.

ارزیابی مخاطره، مؤلفه اصلی در کل این روش است و از چهار مرحله اصلی تشکیل شده است. مراحل ارزیابی مخاطره بر پایهٔ این سند در قالب (**شکل ۳-۶**) به‌تصویر کشیده شده است.



شکل ۳-۶. مراحل ارزیابی مخاطره بر پایهٔ روش NIST 800-30، (NIST 2002)

در مرحله اول، آماده‌سازی برای ارزیابی، زمینه ارزیابی مخاطره ایجاد و از قالب‌بندی مخاطره استفاده می‌شود. وظایف اصلی تهیه آمادگی برای ارزیابی مخاطره شامل شناسایی هدف ارزیابی، دامنه ارزیابی، فرضیات و محدودیت‌های مرتبط با ارزیابی و منابع اطلاعاتی است که باید به عنوان ورودی برای ارزیابی و مدل مخاطره و رویکردهای تحلیلی مورد استفاده قرار گیرند.

در مرحله دوم، ارزیابی واقعی انجام می‌شود. نتیجه این مرحله سیاهه‌ای از مخاطرات امنیتی است که توسط تهدیدها، آسیب‌پذیری‌ها، پیامدها و احتمال وقوع، و همچنین عدم اطمینان در ارتباط با فرآیند ارزیابی برای اطلاع‌رسانی به تصمیم‌گیرندگان در پاسخ به مخاطره تعیین می‌شود. ارزیابی باید کل فضای تهدید را همان طور که در مرحله آماده‌سازی تعریف شده است، پوشش دهد. این مرحله به طور خاص، شامل کارهای مشخصی به شرح موارد زیر است:

- شناسایی منابع تهدید مرتبط با سازمان‌ها؛
- شناسایی رویدادهایی که می‌تواند توسط این منابع تولید شود؛
- شناسایی آسیب‌پذیری‌هایی که می‌تواند مورد سوء استفاده قرار گیرد؛
- تعیین احتمال وقوع تهدیدها و میزان موفقیت آنها؛
- تعیین اثرات منفی که سازمان‌ها باید با آن روبرو شوند؛ و

- تعیین مخاطرات امنیتی اطلاعات به عنوان ترکیبی از احتمال سوء بهره‌برداری از تهدیدها، آسیب‌پذیری‌ها، تأثیر و هرگونه عدم اطمینان در رابطه با تعیین مخاطره.

این فعالیت‌ها احتمالاً برای پوشش کل فضای تهدید به روشی تکراری اجرا می‌شوند. اطلاعات جمع‌آوری شده در مرحله ارزیابی و سپس در مرحله سوم باید به اشتراک گذاشته شود. نتایج ارتباط، نه تنها به اطلاع تصمیم‌گیرندگان در سراسر سازمان از نتایج ارزیابی می‌رسد، بلکه همچنین برای حمایت از دیگر فعالیت‌های مدیریت مخاطره مطرح می‌شود.

سرانجام، آخرین و چهارمین مرحله حفظ ارزیابی است. این مرحله شامل تعیین اثربخشی پاسخ‌های مخاطره به عنوان پاسخ مستقیم برای ارزیابی مخاطره، شناسایی هرگونه تغییر در اثر مخاطره در سیستم‌های اطلاعات سازمانی و همچنین تأیید انطباق است.

۳-۲-۱-۳-۲. استاندارد NIST 800-37

انجمن ملّی استانداردها و فناوری با همکاری وزارت دفاع -دفتر مدیریت اطلاعات ملّی- و کمیته سیستم‌های امنیت ملّی در سال (۲۰۰۴) یک چارچوبی تحت عنوان «**چارچوب مدیریت مخاطره**» [1] جهت بهبود امنیت اطلاعات، تقویب فرآیندهای مدیریت مخاطره و ایجاد توافق میان سازمان‌ها با هدف به اشتراک‌گذاری اطلاعات توسعه داده است. نسخه دوم این چارچوب در سال (۲۰۱۰) به چاپ رسید و ویرایش دوم این استاندارد در دسامبر سال (۲۰۱۸) میلادی، به عنوان آخرین نسخه معتبر از این چارچوب شناخته می‌شود.

این استاندارد چارچوب مدیریت مخاطره را توصیف می‌کند و دستورالعمل‌هایی را برای استفاده این چارچوب در سازمان‌ها و سیستم‌های اطلاعاتی ارائه می‌دهد. چارچوب مدیریت مخاطره یک فرآیند منظم، ساختاریافته و انعطاف‌پذیر برای مدیریت مخاطره امنیت و حریم خصوصی فراهم می‌کند که شامل طبقه‌بندی امنیت اطلاعات؛ انتخاب، پیاده‌سازی و ارزیابی کنترل؛ مجوزهای کنترل مشترک و سیستمی؛ و نظارت مستمر است. چارچوب مدیریت مخاطره دربردارندهٔ فعالیت‌هایی برای آماده‌سازی سازمان جهت اجرای چارچوب در سطوح مناسب مدیریت مخاطره است. این چارچوب همچنین مدیریت مخاطره در زمان واقعی، سیستم اطلاعاتی در حال اجرا و مجوز کنترل مشترک را از طریق اجرای فرآیندهای نظارت مستمر بهبود می‌بخشد؛ اطلاعات لازم را برای تصمیم‌های مدیریت مخاطره کارآمد و مقرون‌به‌صرفه دربارهٔ سیستم‌های پشتیبان از مأموریت‌ها و عملکردهای کسب‌وکار در اختیار رهبران و مدیران ارشد قرار می‌دهد؛ و امنیت و حریم خصوصی را در چرخه عمر توسعه سیستم در نظر می‌گیرد. اجرا و پیاده‌سازی وظایف چارچوب مدیریت مخاطره، فرآیندهای اساسی مدیریت مخاطره در سطح سیستم را به فرآیندهای مدیریت مخاطره در سطح سازمان پیوند می‌دهد. افزون بر این، مسئولیت و پاسخگویی دربارهٔ کنترل‌های اجرا شده در سیستم‌های اطلاعاتی سازمان و کنترل‌های به ارث برده شده توسط سیستم‌ها را تعیین می‌کند.

در واقع، سازمان‌ها می‌توانند با بهره‌برداری از چارچوب مدیریت مخاطرات که در این استاندارد تشریح شده است، اطمینان حاصل کنند که سطح ضمانت مناسبی وجود دارد و سیستم‌های اطلاعاتی و مؤلفه‌های آنها می‌توانند فرآیندهای کسب‌وکار و مأموریت‌های سازمان را به خوبی انجام دهند.

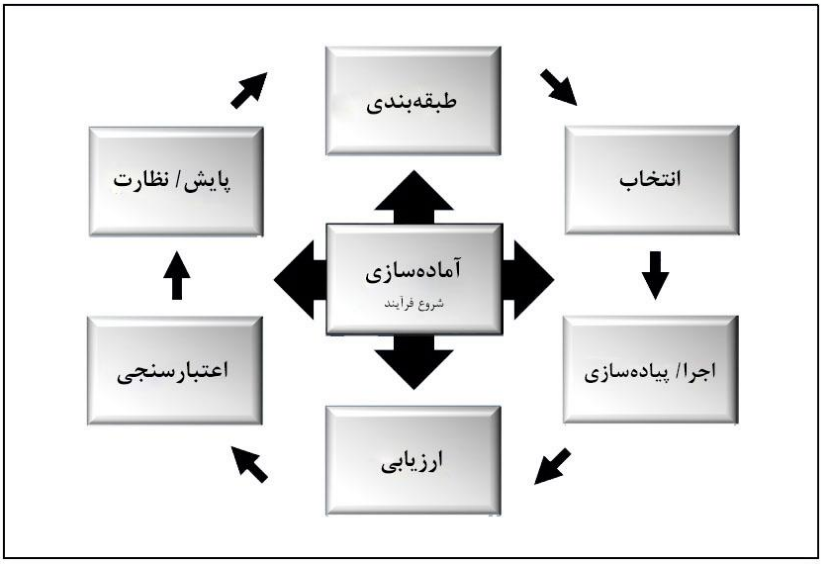
در چارچوب مدیریت مخاطره هفت مرحله وجود دارد. یک گام مقدماتی برای اطمینان از آمادگی سازمان‌ها جهت اجرای فرآیند و شش مرحله اصلی. تمامی هفت مرحله برای اجرای موفقیت‌آمیز چارچوب مدیریت مخاطره ضروری است. این مراحل شامل:

- **آماده‌سازی**، جهت اجرای چارچوب مدیریت مخاطره از یک سازمان و از چشم‌انداز سطح سیستمی از طریق ایجاد زمینه و تعیین اولویت‌هایی برای مدیریت مخاطره امنیتی و حفظ حریم خصوصی؛

[1] Risk Management Framework

- **طبقه‌بندی** سیستم و اطلاعات پردازش شده، ذخیره شده و منتقل شده توسط سیستم بر پایهٔ تجزیه‌وتحلیل پیامد خسارت؛
- **انتخاب** یک مجموعه از کنترل‌های اولیه برای سیستم و متناسب‌سازی کنترل‌ها در صورت لزوم جهت کاهش مخاطره به یک سطح قابل قبول بر پایهٔ ارزیابی مخاطره؛
- **اجرا/ پیاده‌سازی** کنترل‌ها و تشریح چگونگی بهره‌برداری از کنترل‌ها در سیستم و محیط عملیاتی آن؛
- **ارزیابی** کنترل‌ها جهت تعیین اینکه کنترل‌ها به درستی پیاده‌سازی شده‌اند، سازگار با هدف عمل می‌کنند و نتایج مطلوبی را در ارتباط با تأمین امنیت و حفظ حریم خصوصی تولید می‌کنند؛
- **اعتبارسنجی** سیستم یا کنترل‌های مشترک بر پایهٔ تشخیص قابل قبول بودن مخاطره برای دارایی‌ها، عملیات سازمانی، افراد و سازمان‌های دیگر؛
- **پایش/ نظارت** سیستم و کنترل‌های مربوطه به طور مستمر که شامل ارزیابی اثربخشی کنترل، مستندسازی تغییرات در سیستم و محیط کار، انجام ارزیابی‌های مخاطره و تجزیه و تحلیل پیامد، و گزارش وضعیت امنیت و حریم خصوصی سیستم است.

(**شکل ۳-۷**) مراحل چارچوب مدیریت مخاطره استاندارد ۳۷-۸۰۰ را نشان می‌دهد. این چارچوب در تمامی مراحل سلسله‌مراتب مدیریت مخاطره (سطح سازمانی، سطح فرآیند کسب‌وکار، سطح سیستم اطلاعاتی) اجرا می‌شود.



شکل ۳-۷. چارچوب مدیریت مخاطره استاندارد NIST 800-37، (Force 2018)

۳-۲-۱-۳-۳. استاندارد NIST 800-39

مستند بهترین تجربه شماره ۳۹-۸۰۰ مؤسسه ملّی استانداردها و فناوری، تحت عنوان «**مدیریت مخاطره‌های سیستم‌های اطلاعاتی-دید سازمانی**»[1] در سال ۲۰۱۱ میلادی منتشر شده است که می‌تواند به سازمان‌ها کمک کند تا به شکل مؤثرتری برنامه مخاطره امنیت اطلاعات را در عملیات حیاتی مأموریت و اهداف کلی خود ادغام کنند.

[1] Information Systems Risk Management-Organizational Perspective

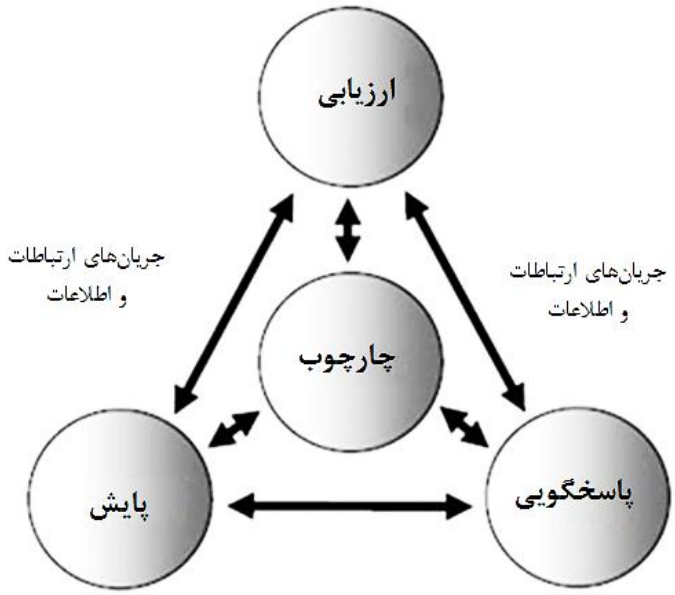
استاندارد NIST 800-39 دستورالعملی را برای مدیریت مخاطرات در سه لایه (**شکل ۳-۸**) ارائه می‌دهد: سطح سازمانی، سطح مأموریت‌ها و فرآیندهای کسب‌وکار و سطح سیستم اطلاعات. سازمان‌ها باید فرآیند مشخصی برای مخاطرات تعریف کنند و کنترل‌های امنیتی ذکر شده در این سند را به عنوان بخشی از آن فرآیند مورد استفاده قرار دهند.

شکل ۳-۸. رویکرد سه لایه مدیریت مخاطره امنیت اطلاعات استاندارد NIST 800-39، (Force 2018)

دستیابی به سطح بالایی از ضمانت می‌تواند برای سازمان‌ها دشوار و پرهزینه باشد، اما گاهی اوقات این امر برای حصول اطمینان از انجام صحیح مأموریت‌ها، فرآیندهای کسب‌وکار و عملیات اصلی سازمان ضرورت دارد. تعیین اینکه در کدام بخش‌های زیرساخت فناوری اطلاعات سازمان به ضمانت بالاتری نیاز است، بخشی از مرحله نخست و مرحله دوم فرآیند مدیریت مخاطرات سازمان به شمار می‌آید. این فعالیت‌ها هنگامی رخ می‌دهند که سازمان، الزامات امنیتی نیاز برای حفاظت از عملیات سازمان (یعنی مأموریت، عملکردها، تصویر سازمان، شهرت و اعتبار سازمان)، سرمایه‌های سازمان، افراد سازمان، دیگر سازمان‌ها و مردم را تعیین می‌کند. تعیین الزام‌های امنیتی و قابلیت‌های امنیتی مربوطه، بخشی از فرآیند مدیریت مخاطرات سازمان است که در شماره ویژه استاندارد NIST 800-39 تشریح شده است. این امر به شکل ویژه در توسعه راهبرد واکنش به مخاطرات اهمیت دارد که پس از بررسی مخاطرات انجام می‌شود (هنگامی که سازمان اقدام به تعیین اولویت‌ها، فرض‌ها، محدودیت‌ها و سطح تحمل مخاطرات، بررسی تهدیدات، آسیب‌پذیری‌ها، مأموریت‌ها و فرآیندهای کسب‌وکار، و احتمال وقوع مخاطرات می‌کند).

پس از اینکه الزام‌های امنیتی و قابلیت‌های امنیتی در مراحل نخست و دوم مشخص شدند (شامل الزامات ضمانتی برای فراهم آوردن شاخص‌های اعتماد به قابلیت‌های مطلوب)، الزامات و قابلیت‌های پیش‌گفته در طراحی معماری سازمان، مأموریت‌ها و فرآیندهای کسب‌وکار و سیستم‌های اطلاعاتی نیاز برای پشتیبانی از این فرآیندها به کار گرفته می‌شوند. رهنمودهای مدیریت مخاطره امنیت اطلاعات که در این استاندارد شرح داده شده است به عنوان مکمل هستند و می‌توانند به عنوان بخشی از یک برنامه جامع مدیریت مخاطره سازمانی مورد استفاده قرار گیرند.

بر پایهٔ این مستند، فرآیند مدیریت مخاطره از چهار مؤلفه چارچوب مخاطره، ارزیابی مخاطره، پاسخ‌گویی به مخاطره و پایش مخاطره تشکیل می‌شود. ارتباط مابین این چهار مؤلفه در قالب (**شکل ۳-۹**) به تصویر کشیده شده است.



شکل ۳-۹. ارتباط مؤلفه‌های مدیریت مخاطره در مراحل ارزیابی مخاطره در استاندارد NIST 800-39، (Ross 2011)

جدول ۳-۶. شناسنامه (۳): استاندارد سری NIST 800

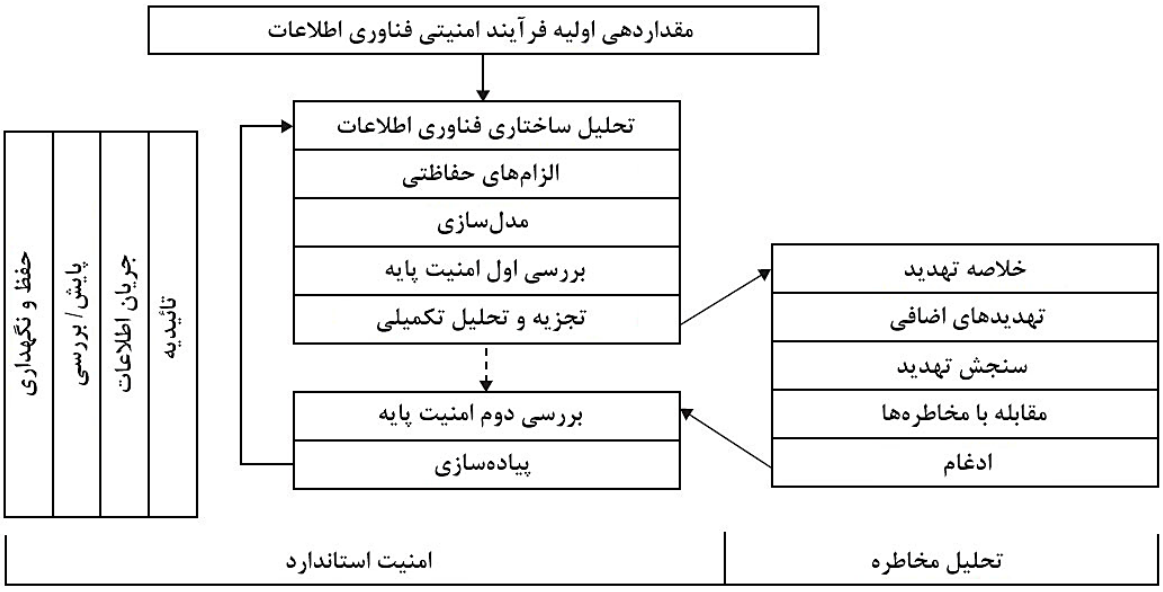
شناسنامه استاندارد سری NIST 800	
نام اختصاری	اِن.آی.اِس.تی ۸۰۰- NIST 800 Series (شناسنامه با تمرکز بر NIST 800-30 تدوین شده است)
نام کامل	چارچوب و راهنمای مدیریت مخاطره‌های سیستم‌های فناوری اطلاعات
ارائه‌دهنده	انجمن ملّی استانداردها و فناوری
کشور ارائه‌دهنده	ایالات متحده آمریکا
وضعیت نسخه	نخستین نسخه استاندارد ۳۰-۸۰۰ در سال ۲۰۰۲ میلادی منتشر شد و در حال حاضر نسخه ۲۰۱۲ این استاندارد به عنوان آخرین نسخه معتبر محسوب می‌شود. نخستین نسخه استاندارد ۳۷-۸۰۰ در سال ۲۰۰۴ میلادی منتشر شد، نسخه دوم در سال ۲۰۱۰ میلادی به چاپ رسید و در حال حاضر ویرایش دوم این استاندارد در ۱۸۳ صفحه در دسامبر ۲۰۱۸ به عنوان آخرین نسخه معتبر محسوب می‌شود.
زبان	انگلیسی
قیمت	به صورت رایگان در دسترس است.
دامنه کاربرد/ استفاده	نسخه ۳۰-۸۰۰ راهنمایی برای مدیریت و ارزیابی مخاطره در امنیت رایانه ارائه می‌کند. نسخه ۳۷-۸۰۰ دستورالعمل‌هایی جهت مدیریت مخاطره‌های امنیتی و حریم خصوصی و بهره‌برداری از چارچوب مدیریت مخاطره در سازمان‌ها و سیستم‌های اطلاعاتی ارائه می‌دهد. نسخه ۳۹-۸۰۰ این استاندارد مختص کاربران فنی تدوین شده است.
هدف	نسخه ۳۰-۸۰۰: - ارائه راهنمایی برای مدیریت مخاطره سیستم‌ها و سازمان‌های اطلاعاتی فدرال نسخه ۳۷-۸۰۰: - پشتیبانی از یک فرآیند تکرارپذیر جهت حفاظت از اطلاعات و سیستم‌های اطلاعاتی متناسب با مخاطره؛ - تمرکز بر آماده‌سازی سازمان جهت مدیریت مخاطرات امنیتی و حفظ حریم خصوصی؛ - تسهیل طبقه‌بندی اطلاعات و سیستم‌ها، انتخاب، پیاده‌سازی، ارزیابی و پایش کنترل‌ها و مجوزدهی سیستم‌های اطلاعاتی و کنترل‌های مشترک؛ - ترویج بهره‌برداری از خودکارسازی برای مدیریت مخاطره بلادرنگ و مداوم سیستم و مجوز کنترل از طریق اجرای فرآیندهای پایش مستمر؛ - تشویق به بهره‌برداری از معیارهای صحیح و به موقع و ارائه اطلاعات لازم به رهبران و مدیران ارشد جهت تصمیم‌گیری‌های مقرون‌به‌صرفه و مبتنی بر مخاطره برای سیستم‌های اطلاعاتی پشتیبانی‌کننده از مأموریت‌ها و عملکردهای کسب‌وکار؛ - تسهیل ادغام الزام‌های امنیتی و حریم خصوصی و کنترل‌ها در معماری سازمانی، چرخه SDLC، فرآیندهای مالکیت و فرآیندهای مهندسی سیستم‌ها؛ - اتصال فرآیندهای مدیریت مخاطره در سازمان و سطوح فرآیند کسب‌وکار به فرآیندهای مدیریت مخاطره در سطح سیستم اطلاعاتی از طریق یک مقام مسئول ارشد برای مدیریت و اجرای مخاطره؛

شناسنامه استاندارد سری NIST 800	
	- تعیین مسئولیت و پاسخگویی دربارهٔ کنترل‌های اجرا شده در سیستم‌های اطلاعاتی سازمان و به ارث برده شده توسط سیستم‌ها؛ نسخه ۳۹-۸۰۰: - ارائه راهنمایی برای یک برنامه سازمان یافته یکپارچه جهت مدیریت مخاطره امنیت اطلاعات در عملیات سازمانی (مانند مأموریت، عملکردها، تصویر سازمان، شهرت و اعتبار سازمان)، دارایی‌های سازمانی، افراد، دیگر سازمان‌ها و نتایج حاصل از عملیات و بهره‌برداری از سیستم‌های اطلاعاتی فدرال.
مراحل مدیریت مخاطره	مراحل چارچوب مدیریت مخاطره مبتنی بر استاندارد ۳۰-۸۰۰: ۱) آمادگی برای ارزیابی، ۲) ارزیابی کردن، ۳) انتقال نتایج، ۴) حفاظت از ارزیابی. مراحل چارچوب مدیریت مخاطره مبتنی بر استاندارد ۳۷-۸۰۰: ۱) آماده‌سازی، ۲) طبقه‌بندی، ۳) انتخاب، ۴) اجرا/ پیاده‌سازی، ۵) ارزیابی، ۶) اعتبارسنجی، ۷) پایش/ نظارت. مراحل چارچوب مدیریت مخاطره مبتنی بر استاندارد ۳۹-۸۰۰: ۱) چارچوب مخاطره، ۲) ارزیابی مخاطره، ۳) پاسخگویی به مخاطره، ۴) پایش مخاطره.
فرمول محاسبه مخاطره	مخاطره (تهدید، دارایی) = احتمال (تهدید)×آسیب‌پذیری (تهدید، دارایی)×پیامد (تهدید، دارایی) مبتنی بر استاندارد ۳۰-۸۰۰
سازگاری با استانداردها	مفاهیم و اصول این استاندارد با استانداردهای سری ISO و IEC بسیار مشابه و سازگار است. پشتیبانی از دیگر دستورالعمل‌ها و استانداردهای امنیتی سری NIST
ابزارهای پشتیبان	پشتیبانی از ابزارهای مستندسازی، گزارش‌نویسی و پایش
مزایا/ نقاط قوت	+ ارائه دستورالعمل‌های خاص در انجام فرآیند ارزیابی مخاطره اطلاعات؛ + امکان استفاده در سازمان‌ها و صنایع گوناگون؛ + امکان استفاده آسان از راهنما همراه با الگوها، نمونه پرسش‌های مصاحبه و یک طرح کلی از گزارش ارزیابی مخاطره؛ + کاربر را در طول فرآیند ارزیابی مخاطره با بهره‌برداری از جداول و نمودارها راهنمایی می‌کند؛ + بسیار ساختارمند و انعطاف‌پذیر (امکان انجام فرآیند تحلیل در سازمان‌های با اندازه‌های گوناگون)؛ + پرداختن به مؤلفه‌های ارزیابی مخاطره از فرآیند مدیریت مخاطره؛ (استاندارد ۳۹-۸۰۰) + ارائه رهنمودهایی دربارهٔ بهره‌برداری از مفاهیم ارزیابی مخاطره در هر سه لایه سلسله مراتب مدیریت مخاطره و هر مرحله از چارچوب مدیریت مخاطره؛ + ارائه تحلیل و توضیحات دقیق از دارایی‌های اطلاعاتی موضوع پژوهش. + رویکرد مدیریت مخاطره چندلایه؛ + ارائه جزئیات خاص از فرآیند ارزیابی، پاسخگویی و پایش مخاطره به طور مداوم؛ + تمرکز بر چرخه حیات توسعه سیستم و معماری سازمانی؛ + یک فرآیند جامع مدیریت مخاطره؛ + تعیین فرآیندها (وظایف) برای هر یک از شش مرحله چارچوب مدیریت مخاطره در سطح سیستمی؛ + یک رویکرد پویا و انعطاف‌پذیر جهت مدیریت مؤثر مخاطرات امنیتی و حفظ حریم خصوصی در محیط های گوناگون با تهدیدهای پیچیده، مأموریت‌های در حال تکامل و عملکردهای کسب‌وکار و تغییر آسیب‌پذیری‌های سازمانی و سیستمی؛ + اطمینان از سازگاری سیستم مدیریت مخاطره امنیتی و حفظ حریم خصوصی با مأموریت و اهداف تجاری سازمان و راهبرد مدیریت مخاطره ایجاد شده توسط مدیریت ارشد از طریق اجرای مخاطره؛ + حفاظت از حریم خصوصی افراد و حفاظت‌های امنیتی برای اطلاعات و سیستم‌های اطلاعاتی از طریق اجرای راهبردهای مناسب پاسخگویی به مخاطره؛ + پشتیبانی از تصمیم‌های سازگار، آگاهانه و مجاز در حال انجام، توافقات طرفین، شفافیت و ردیابی امنیت و حریم خصوصی اطلاعات؛ + تسهیل ادغام الزام‌های امنیتی و حریم خصوصی و کنترل‌ها در معماری سازمانی، فرآیندهای SDLC، فرآیندهای مالکیت و فرآیندهای مهندسی سیستم‌ها؛ + تسهیل اجرای چارچوب جهت بهبود امنیت سایبری زیرساخت‌های حیاتی.
معایب/ نقاط ضعف	- تأثیر عامل انسانی در نتیجه نهایی؛ - بیشتر به عنوان یک راهنما مورد استفاده قرار می‌گیرد تا یک روش؛ - با توجه به استفاده الکترونیکی از الگوها و تهیه خودکار گزارش‌ها از داده‌های جمع‌آوری شده در طول فرآیند ارزیابی مخاطره اطلاعات، امکان پشتیبانی از طریق رایانه برای این راهنما در دسترس نیست؛
وب‌سایت‌رسمی	https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

۳-۲-۱-۴. استاندارد سری BSI

استانداردهای سری «مؤسسه استانداردهای انگلستان»[1] یا به اختصار «BSI» به ویژه استاندارد BSI 200-3 روشی آسان جهت شناسایی و اجرای رویه‌هایی است که به سازمان‌ها این امکان را می‌دهد که به شکلی هدفمند مخاطره‌های امنیت اطلاعات سازمان خود را کنترل کنند. در واقع، استانداردهای سری «BSI» بخشی جداناپذیر از روش IT-Grundschutz هستند. روش‌شناسی IT-Grundschutz یا **کتابچه راهنمای محافظت از اطلاعات پایه فناوری اطلاعات**[2] در سال ۱۹۹۴ میلادی توسط **اداره فدرال امنیت اطلاعات**[3] آلمان برای مقامات دولتی تدوین شد. این روش به سازمان این امکان را می‌دهد که بتواند سیستم مدیریت امنیت اطلاعات خود را بر پایهٔ به‌روش‌ها پیاده‌سازی کند و تأمین امنیت سیستم‌های اطلاعاتی و محافظت از اطلاعات سازمان را تضمین کند. این روش در درجه نخست بر امنیت اطلاعات و محافظت از سازمان‌هایی که داده‌ها را پردازش می‌کنند، تمرکز دارد. این روش نه تنها جنبه‌های فنی بلکه جنبه‌های ساختاری، انسانی و سازمانی را نیز در نظر می‌گیرد. روش IT-Grundshutz یک رویکرد نظام‌مند برای امنیت اطلاعات ارائه می‌دهد که با استاندارد ISO/IEC 27001 سازگار است. این روش برای سازمان‌هایی که سازگار با IT-Grundshutz فعالیت می‌کنند، یک روش مناسب برای تحلیل مخاطره در اختیار آنها قرار می‌دهد و در صورتی که سازمانی در عملیات و فرآیندهای روزانه خود از IT-Grundshutz استفاده نکند، در عملکرد خود با پیچیدگی روبرو می‌شود.

این روش نه تنها شامل توصیه‌های عمومی امنیت فناوری اطلاعات برای ایجاد یک فرآیند امنیتی فناوری اطلاعات کاربردی است، بلکه توصیه‌های فنی دقیق برای دستیابی به یک سطح از امنیت برای یک دامنه خاص را نیز دربرمی‌گیرد. رویکرد اصلی در روش IT-Grundshutz ارائه چارچوبی برای مدیریت امنیت فناوری اطلاعات و ارائه اطلاعاتی برای استفاده رایج از مؤلفه‌های (ماژول‌های) فناوری اطلاعات است. ماژول‌های IT-Grundshutz شامل فهرستی از تهدیدهای مرتبط و اقدام‌های متقابل نیاز در سطح نسبتاً فنی است. این عناصر می‌توانند با توجه به نیازهای یک سازمان گسترش یافته یا سازگار شوند. (**شکل ۳-۱۰**) رویکرد کلی روش IT-Grundschutz را نشان می‌دهد.



شکل ۳-۱۰. راهنمای محافظت از اطلاعات پایه فناوری اطلاعات بر پایهٔ **روش IT-Grundschutz، (BSI 2008)**

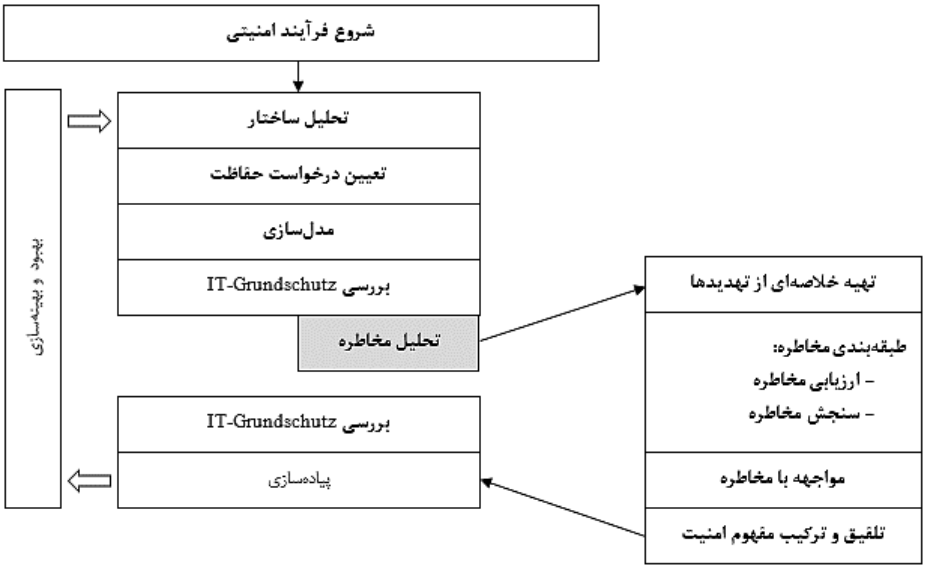
[1] British Standards Institution (BSI)
[2] IT Baseline Protection Manual (IT-Grundschutz)
[3] The Federal Office for Information Security (BSI)

به شکل کلی، استانداردهای سری «BSI» توصیه‌هایی دربارهٔ روش‌ها، فرآیندها و رویه‌ها و همچنین رویکردها و اقدامات در ارتباط با جنبه‌های گوناگون امنیت اطلاعات ارائه می‌دهند. کاربران نهادها و شرکت‌های دولتی و همچنین تولیدکنندگان یا ارائه‌دهندگان خدمات می‌توانند از استانداردهای «BSI» برای امن‌سازی داده‌ها و فرآیندهای کسب‌وکار خود استفاده کنند. این استاندارد شامل سه سند زیرمجموعه برای امنیت فناوری اطلاعات به شرح ذیل است:

- (۱۰۰-۱) سیستم مدیریت امنیت اطلاعات
- (۱۰۰-۲) روش IT-Grundschutz (شامل یک روش کیفی برای ارزیابی مخاطره)
- (۱۰۰-۳) تحلیل مخاطره بر پایهٔ IT-Grundschutz (نمایش چگونگی قرارگرفتن تهدیدها در کاتالوگ IT-Grundschutz که می‌تواند برای انجام یک تحلیل ساده از مخاطره‌های فناوری اطلاعات مورد استفاده قرار گیرد. این روش یک روش مکمل است و نمی‌تواند به طور جداگانه انجام شود. این روش یک تحلیل امنیتی مکمل است)

از اکتبر سال ۲۰۱۷، استانداردهای BSI 200-1، 200-2 و 200-3 جایگزین استانداردهای BSI سری 100-x شده است. استاندارد BSI 200-1 الزام‌های کلی «سیستم مدیریت امنیت اطلاعات» را تعریف می‌کند. این استاندارد همچنین با استاندارد ISO 27001 سازگار است و توصیه‌های دیگر استانداردهای ISO مانند ISO 27002 را نیز در نظر می‌گیرد. استاندارد BSI 200-2 پایه و اساس روش اثبات شده «مؤسسه استانداردهای انگلستان» را برای ایجاد سیستم مدیریت جامع امنیت اطلاعات تشکیل می‌دهد. با توجه به ساختار مشابه دو استاندارد 200-1 و 200-2 کاربران می‌توانند به راحتی با هر دو سند کار کنند.

استاندارد BSI 200-3 شامل تمامی مراحل کاری مرتبط با مخاطره مشابه روش IT-Grundschutz است. در این کتاب، بر روی این استاندارد از این سری استانداردها تمرکز شده است. مزیت این استاندارد برای کاربر، کاهش قابل توجه کوشش وی برای دستیابی به یک سطح موردنظر از امنیت است. اگر در حال حاضر شرکت‌ها و یا مقامات دولتی به شکل موفقیت‌آمیز با روش IT-Grundschutz کار می‌کنند و بخواهند به شکل مستقیم فرآیند تحلیل مخاطره را به تحلیل IT-Grundschutz اضافه کنند، این استاندارد بسیار ایده‌آل است. مراحل چهارگانه تحلیل مخاطره در این استاندارد به شرح ذیل است که در قالب (**شکل ۳-۱۱**) نیز به تصویر کشیده شده است.



شکل ۳-۱۱. مراحل چهارگانه تحلیل مخاطره در استاندارد BSI 200-3، (BSI 2008)

در ادامه به صورت خلاصه به تشریح هر یک از مراحل چهارگانه تحلیل مخاطره پرداخته شده است:

- **مرحله نخست – تهیه خلاصه‌ای از تهدیدها**
  - تهیه فهرستی از تهدیدهای احتمالی ابتدایی
  - مشخص‌کردن تهدیدهای اضافی که فراتر از تهدیدهای ابتدایی هستند و از سناریوهای عملیاتی خاص ناشی می‌شوند.
- **مرحله دوم – طبقه‌بندی مخاطره**
  - ارزیابی مخاطره (تخمین فراوانی وقوع و میزان آسیب/ خسارت)
  - سنجش مخاطره (تعیین طبقه مخاطره)
- **مرحله سوم – مواجهه با مخاطره**
  - اجتناب از مخاطره
  - کاهش مخاطره (تعیین حفاظ‌های امنیتی)
  - انتقال مخاطره
  - پذیرش مخاطره
- **مرحله چهارم – تلفیق و ترکیب مفهوم امنیت**
  - ادغام/ ترکیب حفاظ‌های امنیتی اضافی شناسایی شده بر پایهٔ تحلیل مخاطره در مفهوم امنیتی

جدول ۳-۷. شناسنامه (۴): استاندارد سری BSI

شناسنامه استاندارد سری BSI	
نام اختصاری	بی‌اِس.آی- BSI Series (شناسنامه با تمرکز بر روش IT-Grundschutz تدوین شده است)
نام کامل	تحلیل مخاطره بر پایهٔ IT-Grundschutz
ارائه‌دهنده	اداره فدرال امنیت اطلاعات آلمان
کشور ارائه‌دهنده	آلمان
وضعیت نسخه	نخستین نسخه روش IT-Grundschutz در سال ۱۹۹۴ میلادی منتشر شد، نسخه دوم در سال ۲۰۰۵ میلادی به چاپ رسید، نسخه سوم در سال ۲۰۱۳ میلادی و نسخه (۱,۰) در اکتبر سال ۲۰۱۶ میلادی در قالب CD منتشر شد و در حال حاضر نسخه ۲۰۱۷ این روش به زبان انگلیسی و نسخه ۲۰۱۹ به زبان آلمانی عنوان آخرین نسخه معتبر محسوب می‌شود. نخستین نسخه استاندارد BSI 200-3 در قالب CD در اکتبر سال ۲۰۱۶ میلادی منتشر شد و در حال حاضر نسخه ۲۰۱۷ این روش به عنوان آخرین نسخه معتبر محسوب می‌شود.
زبان	انگیسی، آلمانی
قیمت	به صورت رایگان در دسترس است.
دامنه کاربرد/ استفاده	این استاندارد زمانی می‌تواند مورد استفاده قرار گیرد که شرکت‌ها یا آژانس‌های دولتی با روش IT-Grundschutz سازگار با استاندارد BSI 200-2 با موفقیت کار می‌کنند و تمایل دارند تحلیل مخاطره را به صورت مستقیم به IT-Grundschutz اضافه کنند.
هدف	ارائه یک روش کیفی برای شناسایی، تحلیل و سنجش رویدادهای امنیتی که ممکن است به کسب‌وکارها خسارت وارد کند. استانداردها یک ارزیابی مخاطره دو مرحله‌ای را تشریح می‌کنند: ۱) طراحی شده برای دستیابی به سطح استاندارد از امنیت، ۲) تحلیل مخاطره مکمل که توسط سازمان‌ها و با هدف سفارشی‌سازی روش متناسب با نیازهای امنیتی مورد استفاده قرار می‌گیرد. در واقع، هدف از این استاندارد ارائه یک روش آسان و شناخته‌شده که به سازمان‌ها امکان کنترل کافی و هدفمند مخاطره‌های امنیت اطلاعات را می‌دهد.
مراحل مدیریت مخاطره	**مراحل ارزیابی مخاطره:** - شناسایی مخاطره: هر ماژول IT-Grundschutz شامل فهرستی از تهدیدهای رایج است. تهدیدها همچنین در پنج کاتالوگ تهدید طبقه‌بندی می‌شوند. شناسایی تهدیدهای اضافی/ بیشتر در طول فرآیند تحلیل مخاطره تکمیلی انجام می‌شود. توصیف ویژگی‌های مخاطره نتیجه ارزیابی الزام‌های حفاظتی است. به همین منظور، دسته‌های الزام حفاظتی تعریف و سناریوهای احتمالی خسارت/ آسیب به دسته‌های الزام حفاظتی اختصاص داده می‌شوند. توصیف بیشتر از ویژگی‌های مخاطره

شناسنامه استاندارد سری BSI	
	در تحلیل مخاطره تکمیلی ارائه شده است، جایی که مخاطره‌ها با کمک تصمیمِ گرفته شده در ارتباط با چگونگی کنترل آنها مشخص می‌شوند. - تحلیل مخاطره: به ازای هر تهدید -موجود در یک ماژول- شرح مفصلی از موضوع ارائه شده است. - سنجش مخاطره: ارزیابی از طریق ارزیابی الزام‌های حفاظتی با کمک سناریوهای خسارت انجام می‌شود. برای تهدیدهای شناسایی شده در محدوده تحلیل مخاطره تکمیلی، ارزیابی در طول فرآیند مراحل ارزیابی تهدیدها انجام می‌شود. **مراحل مدیریت مخاطره:** - ارزیابی مخاطره: به مراحل روش ارزیابی مخاطره رجوع شود. - مقابله/ مواجهه با مخاطره: کاتالوگ‌هایی از حفاظ‌های امنیتی پیشنهاد شده است. شرح مفصلی از حفاظ‌های امنیتی به هر ماژول IT-Grundschutz اختصاص داده شده است. اختصاص حفاظ‌های امنیتی به تهدیدها درنظر گرفته شده است (جدول‌های ارجاع متقابل). - پذیرش مخاطره: تحلیل مخاطره بر پایهٔ IT-Grundschutz. - ارتباط با مخاطره: بخشی از ماژول "مدیریت امنیت فناوری اطلاعات" و به ویژه در حفاظ‌های امنیتی S 2.191 تحت عنوان "تنظیم پیش‌نویسی از خط‌مشی امنیت اطلاعات" و S 2.200 "تهیه گزارش‌های مدیریتی در ارتباط با امنیت فناوری اطلاعات" به کار گرفته می‌شود.
فرمول محاسبه مخاطره	مخاطره (رخداد، دارایی) = احتمال (حادثه) × پیامد (حادثه، دارایی)
سازگاری با استانداردها	این روش با استانداردهای ISO/IEC 177799، ISO/IEC 27001، ISO 27005 و ISO 31000 سازگار است.
ابزارهای پشتیبان	ابزار غیرتجاری GSTOOL برای استفاده رایگان مقامات دولتی. ابزارهای تجاری به شرح ذیل: BSI - GSTOOL HiSolutions AG HiScout SME INFODAS GmbH - SAVe inovationtec - IGSDoku Kronsoft e.K. - Secu-Max Baseline-Tool - Swiss Infosec AG WCK - PC-Checkheft
مزایا/ نقاط قوت	+ تضمین کسب‌وکار و افزایش شهرت و اعتبار در بازار؛ + مبتنی بر رویکرد سنتی تحلیل مخاطره؛ + یک مدل با جزئیات مفصل؛ + ساده‌ترشدن فرآیند پس از تکمیل کار؛ + محاسبه و ارزیابی سطح امنیت فناوری اطلاعات سازمان و ارائه توصیه‌های فنی بسیار دقیق؛ + رویکردی دومرحله‌ای که اجازه می‌دهد روش به طور پیوسته در سیستم‌هایی با الزام‌های امنیتی و پیچیدگی‌های گوناگون استفاده شود؛ + پشتیبانی توسط اسناد، دستورالعمل‌ها و استانداردهای مدیریت مخاطره؛ + سازگار با استانداردهای امنیت اطلاعات سری ISO/IEC 27000؛ + تعداد زیادی از ابزارهای شخص ثالث سازگار با روش‌های دسترس‌پذیر. + کاهش قابل توجه کوشش کاربر جهت دستیابی به یک سطح موردنظر از ایمنی؛ + یک استاندارد ایده‌آل جهت انجام فرآیند تحلیل مخاطره؛ + سازگار با روش IT-Grundschutz؛ + کاربران IT-Grundschutz برای بخش عمده‌ای از سیستم اطلاعاتی مجبور به انجام تجزیه و تحلیل تهدید و آسیب‌پذیری به صورت مستقل و فردی نیستند، زیرا این ارزیابی بیشتر توسط «مؤسسه استانداردهای انگلستان» انجام شده است؛ + مورد استفاده در بسیاری از کشورهای عضو اتحادیه اروپا؛ + ارائه فهرستی از تهدیدهای مرتبط و اقدام‌های لازم در سطح نسبتاً فنی؛
معایب/ نقاط ضعف	- نیازمند منابع و زمان بیشتر جهت انجام فرآیند ارزیابی مخاطره؛ - نیازمند تجربه و دانش بیشتر نسبت به دو مدل IRAM و OCTAVE؛ - نیازمند اطلاعات بیشتر برای شروع فرآیند نسبت به دو مدل IRAM و OCTAVE؛ - نیازمند تخصص امنیتی و فنی جهت استفاده و بهره‌برداری از برخی توصیفات. - در سطح بالایی از پیچیدگی جای دارد؛
وب‌سایت‌رسمی	https://www.bsi.bund.de/DE/Home/home_node.html

۳-۲-۱-۵. استاندارد ETSI TVRA

برای تحلیل تهدیدها، مخاطره‌ها و آسیب‌پذیری‌های یک سیستم ارتباطی، روش طراحی سیستمی تحت عنوان «**روش مدل‌سازی امنیتی TVRA**»[1] یا به اختصار «TVRA» توسط استاندارد TISPAN **مؤسسه استانداردهای مخابراتی اروپا**[2] معرفی و به صورت رسمی ارائه شده است. این روش به ویژه برای برنامه‌های کاربردی شبکه بسیار مناسب است و یک فرآیند نظام‌مند برای شناسایی و تحلیل مخاطره‌های مرتبط با حمله‌ها علیه دارایی‌های حیاتی شناسایی شده در یک سازمان محسوب می‌شود. این روش یک جدول نقشه‌برداری از ارزش دارایی و رتبه آسیب‌پذیری است که می‌تواند برای فرموله کردن هر نوع از مخاطره مورد استفاده قرار گیرد. این روش مدلی تعریف شده از سیستم را به همراه تحلیل آن ارائه می‌کند که بیانگر آسیب‌پذیری‌ها، ضعف‌ها، و تهدیدهای آن سیستم است. اطلاعات حاصل از این روش تحلیل و مدل‌سازی، با **اقدام‌های متقابل**[3] در مقابل آسیب‌پذیری‌ها، در پیاده‌سازی یک سیستم تعریف شده کارا بسیار مفید خواهد بود (ETSI 2006:2008:2010).

روش «TVRA» بر پایهٔ تجزیه‌وتحلیل آسیب‌پذیری‌ها، تهدیدها و تحلیل مخاطره انجام می‌شود. اصول مدل کردن در «TVRA» شامل موضوع‌های زیر است که در شبکه مدل شونده، تعیین و مشخص خواهند شد (deMeer and Rennoch 2011).

- **اهداف امنیتی**[4]: مشخص کردن اهداف امنیتی (ابعاد امنیتی)، اساس بررسی آسیب‌پذیری‌های یک سیستم است. اهداف امنیتی شامل تشخیص هویت، محرمانگی، یکپارچگی/ صحت، حسابرسی، دسترس‌پذیری، کنترل دسترسی، خصوصی‌سازی و امنیت ارتباطی است. این اهداف در سیستم ثابت هستند.
- **دارایی**[5]: هر چیزی که برای سیستم ارزشمند باشد در این بخش قرار می‌گیرد، مانند دارایی فیزیکی (تجهیزات) و دارایی منطقی (اطلاعات موجود در درون تجهیزات).
- **ضعف**[6]: سیستم‌ها ضعف‌هایی دارند که توسط مهاجمان مورد سوءاستفاده قرار می‌گیرند. این ضعف‌ها می‌توانند به عنوان یک تهدید برای سیستم محسوب شوند.
- **حادثه ناخواسته**[7]: حادثه ناخواسته (اتفاق پیش‌بینی نشده) نظیر از دست دادن محرمانگی، یکپارچگی/ صحت و یا دسترس‌پذیری است. به محرمانگی، یکپارچگی/ صحت و تشخیص هویت مثلث امنیتی (CIA) گفته می‌شود، چرا که امنیت مبتنی بر این سه عنصر است.
- **تهدید**[8]: تهدیدهایی مثل شنودی که سیستم با آن مواجه است می‌تواند موجب زیان به سیستم یا شبکه شوند.
- **آسیب‌پذیری**[9]: مجموعه‌ای از ضعف‌های درون سیستم که می‌تواند توسط مهاجم مورد تهدید قرار گیرد آسیب‌پذیری نامیده می‌شود. در روش «TVRA»، گام به گام مشخصه‌های گوناگون یک سیستم بررسی می‌شوند تا مخاطره‌ها، حمله‌ها و آسیب‌پذیری‌های آن سیستم به دست آمده و احتمال حوادث مخرب در آن مشخص شوند و اقدام‌های پیشگیرانه از آنها تعیین شود (Collier 2005).

روش «TVRA» به طور نظام‌مند دارایی‌ها و روابط بین دارایی‌ها (جایی که رابطه ممکن است به عنوان یک دارایی نامشهود در نظر گرفته شود) را شناسایی می‌کند، سپس برای هر دارایی نقاط ضعفی که این دارایی دارد مشخص می‌کند و در نهایت، چگونگی مواجهه با این ضعف و مخاطره حاصل از آن را ارزیابی می‌کند. به ازای هر مرحله در این روش، تعدادی معیار برای کمک به کاربر

---

[1] ETSI Threat Vulnerability & Risk Analysis (TVRA) Method
[2] European Telecommunications Standards Institute (ETSI)
[3] Counter Measure
[4] Security Objective
[5] Asset
[6] Weakness
[7] Unwanted Incident
[8] Threat
[9] Vulnerability

روش معرفی شده است. مراحل ده‌گانه روش «TVRA» که شامل مراحل گوناگون جمع‌آوری، تحلیل و پردازش است، در قالب (**شکل ۳-۱۲**) نشان داده شده است.

شکل ۳-۱۲. مراحل مدل‌سازی TVRA

- **مرحله نخست – شناسایی هدف از سنجش:** یک «TVRA» موفق به تعریف روشنی از محدوده، هدف و هدف از تحلیل بستگی دارد. باید توصیف جامعی از **هدف سنجش**[1] (TOE) و محیط آن تهیه شود. یک TOE باید با هدف نشان دادن سیستم تحت استانداردسازی در نظر گرفته شود. در این مرحله اولیه، تعیین مرز بین سیستم (هدف از استانداردسازی) و محیط آن ضروری است. بدون این تعریف، احتمال دستیابی به برخی از اهداف امنیتی (مرحله دوم) مشخص شده غیرممکن خواهد بود.
- **مرحله دوم – شناسایی اهداف:** اهداف امنیتی، اهداف گسترده یک استاندارد یا سیستم را از نظر محافظت از کاربران و اطلاعات در چارچوبی از ویژگی‌های **محرمانگی، صحت، دسترس‌پذیری، احرازهویت** و **پاسخگویی**[2] (CIAAA) مشخص می‌کند. بدون چنین اهدافی، توسعه مجموعه‌ای منسجم از الزام‌های امنیتی و همچنین انجام معنادار فرآیند «TVRA» دشوار است. اهداف امنیتی باید مختص سیستم هدف باشند و ویژگی‌های CIAAA تحت تأثیر را به شکل روشنی مشخص کنند. ETSI TR 187 011 رهنمودهایی دربارهٔ شیوهٔ نوشتن اهداف امنیتی و ETSI TR 187 002 نمونه‌هایی از اهداف امنیتی را ارائه می‌دهد.

[1] Target Of Evaluation (TOE)

[2] Confidentiality, Integrity, Availability, Authenticity and Accountability (CIAAA)

- **مرحله سوم – شناسایی الزام‌های امنیتی کاربردی:** الزام‌ها/ نیازمندی‌های سیستم به اهداف شناسایی شده سیستم در مرحله نخست وابسته است و دارای دو ویژگی خاص ۱) **الزام‌های امنیتی**[1] و ۲) **الزام‌های اطمینان**[2] است.
- **مرحله چهارم – موجودی نظام‌مند از دارایی‌ها:** ثبت ماهیت هر دارایی سیستم و پیچیدگی فناوری استفاده شده در ساخت دارایی و هرگونه اطلاعات مربوط به فناوری بکار رفته در دارایی که به صورت عمومی در دسترس است، از اهمیت بالایی برخوردار است. بین آنها، این سه جنبه سطح درک از دارایی را تا حد زیادی تعیین می‌کنند. امید به زندگی دارایی با درنظر گرفتن زمان لازم جهت توسعه و اجرای حمله (توسعه عامل تهدید برای یک نوع خاص از حمله) مورد استفاده قرار می‌گیرد. این امر ممکن است تحت تأثیر جنبه‌هایی از جمله دفعات به‌روزرسانی کلید یا کلمه عبور، مدت زمانی که انتظار می‌رود دارایی به شکل عملیاتی استفاده شود، قرار گیرد.
- **مرحله پنجم – شناسایی نظام‌مند سطح تهدید و آسیب‌پذیری‌ها:** برای شناسایی آسیب‌پذیری‌های احتمالی، ابتدا لازم است مشخص شود که نقاط ضعف در کجا وجود دارد، -در صورت وجود- تهدیدهای قابل اجرا می‌توانند از این نقاط ضعف استفاده کنند و چه آسیب‌هایی که می‌توانند در اثر حمله به یک نقطه ضعف ایجاد شود. این فقط یک نقطه ضعف است که چنین تهدیدی برای آن وجود دارد که می‌تواند به عنوان یک آسیب‌پذیری در سیستم در نظر گرفته شود.
- **مرحله ششم – تخمین احتمال حمله و پیامد آن:** هر یک از فاکتورهای حمله باید جمع شود (برای نمونه، زمان + تخصص + دانش + فرصت + تجهیزات) تا یک رتبه/ امتیاز کلی از احتمال حمله بدست آید. سپس ارزش احتمال حمله باید به یک رتبه آسیب‌پذیری نگاشت شود. در نهایت، میزان آسیب‌پذیری با سطح تهدید ترکیب می‌شود تا احتمال وقوع بدست آید.
- **مرحله هفتم – تعیین مخاطره‌ها:** برای هر یک از دارایی‌های سیستم مورد بررسی می‌توان نقاط ضعف، تهدیدها و آسیب‌پذیری‌های مربوط به آنها را شناسایی کرد. برای هر آسیب‌پذیری، احتمال باید همان‌طور که در مرحله ششم توضیح داده شده است محاسبه شود. برای هر دارایی باید مخاطره مرتبط با هر آسیب‌پذیری محاسبه شود.
- **مرحله هشتم – شناسایی اقدام‌های متقابل امنیتی:** اقدام‌های متقابل امنیتی، دارایی‌هایی هستند که به منظور کاهش مخاطره به یک سیستم اضافه می‌شوند. هدف از اقدام‌های متقابل کاهش احتمال حمله یا پیامد حمله است. اقدام‌های متقابل امنیتی به عنوان نمونه‌ای از دارایی‌ها مدل‌سازی می‌شوند و در حالی که در درجه نخست منطقی هستند، ولی ممکن است انسانی یا فیزیکی نیز باشند. چندین اقدام متقابل جایگزین ممکن است وجود داشته باشد که ابتدا باید شناسایی، سپس سنجش و در نهایت مقایسه شوند تا هزینه‌ها و مزایای هر یک مشخص گردد تا بتوان برای انتخاب اقدام‌های متقابل تصمیم آگاهانه‌ای گرفته شود.
- **مرحله نهم – تحلیل هزینه-منفعت اقدام متقابل:** بیش از یک اقدام متقابل ممکن است در کاهش مخاطره‌های خاص یا مجموعه‌ای کلی از مخاطره‌ها مؤثر باشد. از این‌رو، روش «TVRA» یک تحلیل هزینه-منفعت متقابل را تعیین می‌کند. هدف از تحلیل، شناسایی مقرون به‌صرفه‌ترین اقدام متقابل از بین گزینه‌های پیشنهادی است. مزیت اصلی هر اقدام متقابل، کاهش اقدام‌های حمله است که هم منجر به امنیت بیشتر می‌شود و هم محافظت صریح و آشکار از حمله را به همراه خواهد داشت. افزایش پذیرش از سوی بازار و بهبود انطباق و سازگاری با مقررات می‌تواند از دیگر مزایای آن باشد. هزینه‌ها صرفاً جنبه اقتصادی ندارند، بلکه بر استانداردسازی، اجرا/ پیاده‌سازی و بهره‌برداری تأثیر می‌گذارند.
- **مرحله دهم – مشخصات دقیق الزام‌ها/ نیازمندی‌ها:** الزام‌های امنیتی باید هم برای دارایی و هم در صورت لزوم برای محیط آن شناسایی شوند. الزام‌های دقیق از الزام‌های امنیتی کاربردی مرحله سوم و خدمات امنیتی و توانایی اقدام‌های متقابل و الزام‌های امنیتی شناسایی شده در مرحله هشتم و تحلیل شده در مرحله نهم حاصل می‌شود.

---

[1] Security Requirement

[2] Assurance Requirement

جدول ۳-۸. شناسنامه (۵): استاندارد ETSI TVRA

شناسنامه استاندارد ETSI TVRA	
نام اختصاری	تی.وی.آر.ای - TVRA
نام کامل	ETSI Threat Vulnerability & Risk Analysis (TVRA) Method روش تحلیل مخاطره، آسیب‌پذیری، تهدید
ارائه‌دهنده	مؤسسه استانداردسازی مخابراتی/ ارتباطاتی اروپا
کشور ارائه‌دهنده	فرانسه
وضعیت نسخه	نسخه ۴،۱،۱ این روش در فوریه سال ۲۰۰۳ میلادی، نسخه ۴،۲،۱ در دسامبر ۲۰۰۶ میلادی و نسخه ۲،۳ این روش در سال ۲۰۱۱ میلادی منتشر گردید. در حال حاضر نسخه ۵ این روش در سال ۲۰۱۷ میلادی به عنوان آخرین نسخه معتبر شناخته می‌شود.
زبان	انگلیسی
قیمت	به صورت رایگان در دسترس است.
دامنه کاربرد/ استفاده	این روش برای برنامه‌های کاربردی شبکه مناسب است.
هدف	شناسایی مخاطره سیستم بر پایهٔ احتمال حمله و پیامدی که چنین حمله‌ای بر روی سیستم خواهد گذاشت.
مراحل مدیریت مخاطره	فرآیند روش TVRA شامل مراحل زیر است: ۱) شناسایی هدف از سنجش ۲) شناسایی اهداف ۳) شناسایی الزام‌های امنیتی کاربردی ۴) موجودی نظام‌مند از دارایی‌ها ۵) شناسایی نظام‌مند سطح تهدید و آسیب‌پذیری‌ها ۶) تخمین احتمال حمله و پیامد آن ۷) تعیین مخاطرات ۸) شناسایی اقدام‌های متقابل امنیتی ۹) تحلیل هزینه-منفعت اقدام متقابل ۱۰) مشخصات دقیق الزام‌ها/ نیازمندی‌ها
فرمول محاسبه مخاطره	پیشنهادهایی در خصوص محاسبه مخاطره ارائه می‌دهد، اما فرمول مشخصی ارائه نداده است. از جمله اجزای پیشنهادی این روش برای محاسبه مخاطره می‌توان به موارد ذیل اشاره نمود: شناسایی نقاط ضعف، تهدیدها و آسیب‌پذیری‌های مربوط به دارایی‌های سیستم و محاسبه رتبه/ امتیاز کلی احتمال حمله بر پایهٔ مجموع فاکتورهای حمله (برای نمونه، زمان + تخصص + دانش + فرصت + تجهیزات)، نگاشت ارزش احتمال حمله به یک رتبه آسیب‌پذیری و در نهایت، ترکیب میزان آسیب‌پذیری با سطح تهدید جهت تخمین احتمال وقوع.
سازگاری با استانداردها	این روش با استانداردهای ISO/IEC 15408، ISO/IEC 17799، ISO 31000 سازگار است.
ابزارهای پشتیبان	این روش از نرم‌افزار اکسل و پایگاه‌داده SQL بهره می‌برد.
مزایا/ نقاط قوت	+ توانایی در برقراری ارتباط بین اجزای گوناگون سامانه و نیازمندی‌ها و اثر متقابل این دو بخش بر روی یک‌دیگر؛ + این روش از قابلیت تکرارپذیری برخوردار است؛ + ارزیابی درستی از عملکرد سیستم در زمان وقوع حمله‌ها ارائه می‌کند؛ + کاهش هرچه بیشتر حوادث ناخواسته در زمان پیاده‌سازی؛ + ارزیابی نقاط قوت و ضعف در طیف گسترده‌ای از حالات/ سناریوها؛ + امکان ارزیابی حفاظ‌های امنیتی موجود در برابر مخاطره‌های امنیتی شناخته شده؛ + سنجش تهدیدهای شناسایی شده و تعیین سطح مخاطره، احتمال وقوع یک رویداد ناخواسته و پیامد حاصل از آن؛ + توصیه راهبردهای کنترل مخاطره جهت کاهش مخاطره‌های امنیتی شناسایی شده در یک سطح قابل قبول با هزینه مقرون‌به‌صرفه.
معایب/ نقاط ضعف	- مخاطره‌های امنیتی را مشخص می‌کند، اما نمی‌تواند به صورت خودکار اقدام‌های امنیتی را تعیین کند؛ - بهره‌برداری از این روش آسان نیست؛
وب‌سایت‌رسمی	https://www.etsi.org

۳-۲-۲. چارچوب‌ها و راهنماهای عمومی مدیریت و ارزیابی مخاطره امنیت اطلاعات

گاهی سازمان‌ها برای مدیریت فرآیند ارزیابی و مدیریت مخاطرات از محصولاتی استفاده می‌کنند که به جای دیکته کردن آنچه که باید -در قالب یک استاندارد- پیاده‌سازی و به کار برده شود، مجموعه را با هدایت و ارائه رهنمود عملی در این زمینه، آماده می‌کنند. این محصولات عموماً با نام رهنمودها شناخته می‌شوند. از آنجایی که یک رهنمود نتیجه تجارب مستندشده یک یا مجموعه‌ای از سازمان‌ها در یک حوزه تخصصی امنیت است، آنها را در زمره بهترین تجربیات لحاظ می‌نمایند.

در هر سازمانی به دلیل عوامل داخلی و خارجی متعدد به منظور حفظ جایگاه رقابتی در بازار و رسیدن به اهداف، پیاده‌سازی فرآیند مدیریت مخاطره سازمانی امری ضروری محسوب می‌شود. افزون بر این، به دلیل الزام در اعمال پیوسته و مداوم نظرات ذینفعان دربارهٔ وضعیت مخاطره در کل سازمان و نهادینه‌سازی فرهنگ مخاطره، اجرایی کردن این فرآیند اهمیت می‌یابد. فاصله میان تصمیم‌گیری در این زمینه و اجرایی کردن آن از اصلی‌ترین مسائل در پیاده‌سازی مدیریت مخاطره است، چرا که اکثر مدیران در انتخاب چارچوب و روش مناسب مدیریت مخاطره مشکلات اساسی دارند.

هیأت مدیره، مدیران عامل، مدیران کسب‌وکار و فناوری اطلاعات و متخصصین مخاطره در کل سازمان نیازمند راهنماهایی هستند تا بتوانند فرآیند مدیریت مخاطره را با توجه به شرایط داخلی و خارجی سازمان خود، به‌صورت گام‌به‌گام و مؤثر اجرا کنند. بنابراین لازم است تا با بهره‌برداری از به‌روش‌ها و چارچوب‌های رایج این فاصله را به حداقل رساند و راهنمایی برای مدیران و دیگر مخاطبان فراهم کرد.

رهنمودها برای هر عمل و یا فرآیندی که در جهت رسیدن به یک هدف اصلی نیاز است، راهنمایی لازم را ارائه می‌کنند. رهنمودها می‌توانند برای یک فرآیند کامل و یا زیرمجموعه‌ای از یک فرآیند مشخص ارزیابی و مدیریت مخاطرات تعریف شوند. رهنمودهایی که در این بخش معرفی می‌شوند برای ارائه رهنمودهایی طرح‌ریزی شده‌اند که چگونگی شناسایی، تعریف، ارزیابی و مدیریت مخاطرات در حوزه امنیت اطلاعات را بازگو می‌کنند.

در این بخش، ضمن معرفی چارچوب‌ها و رهنمودهای موجود، به بیان ویژگی‌ها، هدف از انتشار و آخرین وضعیت هر یک از این چارچوب‌ها پرداخته خواهد شد. (**شکل ۳-۱۳**) درختواره چارچوب‌ها و رهنمودهای عمومی حوزه مخاطرات امنیت اطلاعات را به تصویر کشیده است. در ادامه معرفی مختصر و شناسنامه هر یک از این چارچوب، اصول و رهنمودهای عمومی نیز ارائه خواهد شد.

شکل ۳-۱۳. چارچوب و رهنمودهای حوزه مخاطرات امنیت اطلاعات

۳-۲-۲-۱. راهنمای Austrian IT Security Handbook

کتابچه راهنمای امنیت فناوری اطلاعات اتریش[1] در سال ۱۹۹۸ میلادی و از سوی **شورای فدرال اتریش**[2] برای سازمان‌های دولتی توسعه داده شد. این کتابچه شامل یک شرح کلی از چگونگی انجام فرآیند ارزیابی مخاطره امنیت اطلاعات است. این سند در دو بخش تدوین شده است:

[1] Austrian IT Security Handbook

[2] Austrian Federal Chancellery

- بخش اول) توضیحات مفصل از فرآیند مدیریت امنیت فناوری اطلاعات، ازجمله توسعه خط‌مشی‌های امنیتی، تحلیل مخاطره، طراحی مفاهیم امنیتی، اجرای برنامه امنیتی و فعالیت‌های پیگیری را ارائه می‌دهد.
- بخش دوم) مجموعه‌ای از ۲۳۰ اقدام امنیتی اولیه/ پایه است. ابزاری که از فرآیند اجرا و پیاده‌سازی پشتیبانی می‌کند نیز به عنوان نمونه اولیه[1] در دسترس است.

کتابچه راهنمای امنیت فناوری اطلاعات اتریش در ابتدا برای سازمان‌های دولتی تدوین شده بود، ولی هم‌اکنون برای انواع کسب‌وکارها در دسترس است. این کتابچه راهنما، با استاندارد ISO/IEC 13335، روش IT-Grundschutz و تا حدودی با استاندارد ISO/IEC IS 17799 سازگار است. این کتابچه/ راهنما شامل توضیحات عمومی دربارهٔ ارزیابی مخاطره است، اما روش خاصی را مشخص نمی‌کند.

پیش‌شرط اساسی برای مدیریت موفقیت‌آمیز امنیت اطلاعات، ارزیابی مخاطره‌های امنیتی موجود است. از این‌رو، در فرآیند تحلیل مخاطره سعی در شناسایی و ارزیابی مخاطره‌ها و در نتیجه تعیین مخاطره کلی است. در واقع، هدف اصلی کاهش مخاطره‌ها تا حدی است که مخاطره باقی‌مانده قابل اندازه‌گیری و قابل پذیرش باشد. تحلیل مخاطره برای یک سیستم فناوری اطلاعات شامل شناسایی مخاطره‌های موجود و تخمین میزان آنها است. برای همین منظور، مقادیر (دارایی‌ها)، تهدیدها و آسیب‌پذیری‌های سیستم شناسایی شده و مخاطره‌های ناشی از آن نیز تعیین می‌شود. فرآیند تحلیل مخاطره بیان شده در این راهنما شامل مراحل ذیل است:

- **مرحله نخست – تعیین محدود تحلیل:** در این مرحله سیستم‌های فناوری اطلاعات مورد تحلیل باید مشخص شوند و باید به این موضوع پرداخته شود که آیا دیگر اشیاء (برای مثال، ساختمان‌ها و زیرساخت‌ها) نیز باید در فرآیند تحلیل درنظر گرفته شوند یا خیر.
- **مرحله دوم – شناسایی اشیاء در معرض خطر (ارزش‌ها، دارایی‌ها):** هدف این مرحله ثبت کلیه اشیاء در معرض خطر است که در محدوده فرآیند تحلیل- مرحله قبل- جای دارند.
- **مرحله سوم – تحلیل ارزش (تحلیل پیامد):** در این مرحله، ارزش اشیاء در معرض خطر تعیین می‌شود. فرآیند تحلیل ارزش شامل موارد ذیل است:
  - تعیین مبنای ارزیابی برای دارایی‌های مادی؛
  - تعیین مبنای ارزیابی برای دارایی‌های نامشهود؛
  - تعینی وابستگی بین اشیاء؛ و
  - ارزیابی اشیاء در معرض خطر و آسیب احتمالی (تجزیه و تحلیل پیامد).
- **مرحله چهارم – تحلیل تهدید:** اشیاء در معرض تهدیدهای متعددی قرار می‌گیرند که می‌تواند ناشی از سهل‌انگاری و یا از روی عمد باشد. فرآیند تحلیل تهدید شامل موارد ذیل است:
  - شناسایی تهدیدهای احتمالی (بلایا، خطاهای عملیاتی، حمله‌های عمدی) و مهاجمان احتمالی (کارمندان، افراد خارجی و غیره)
  - تعیین احتماع وقوع
- **مرحله پنجم – تحلیل آسیب‌پذیری:** تهدید فقط با سوءبهره‌برداری از آسیب‌پذیری‌های موجود می‌تواند مؤثر واقع شود. به همین منظور به طور خاص زمینه فعالیت، زمان، سخت‌افزار، نرم‌افزار، پرسنل و زیرساخت‌ها مورد بررسی قرار می‌گیرند.

[1] Prototype

- **مرحله ششم – شناسایی اقدام‌های امنیتی موجود:** جهت جلوگیری از تلاش‌ها و هزینه‌های غیرضروری، اقدام‌های امنیت موجود باید ثبت و از لحاظ پیامدهای آنها بر امنیت کل سیستم و عملکرد صحیح، بررسی شوند. اقدام‌های امنیتی جدید برنامه‌ریزی شده باید با اقدام‌های موجود سازگار باشند و از نظر اقتصادی و فنی منطقی باشند.
- **مرحله هفتم – ارزیابی مخاطره:** در این مرحله، مخاطره‌ها به صورت جزئی و کلی تعیین و ارزیابی می‌شوند.
- **مرحله هشتم – ارزیابی و تهیه نتایج:** ارزیابی و پردازش نتیجه منجر به تحلیل مخاطره می‌شود.

همچنین در یک برداشت کلی، این راهنما بیان می‌کند که در زمان اجرای فرآیند تحلیل مخاطره باید اصول زیر مد نظر قرار گیرد:

- کل فرآیند باید شفاف باشد؛
- هیچ فرضیه پنهانی وجود ندارد که منجر به نادیده‌گرفتن تهدیدها شود.
- تمامی ارزیابی‌ها باید توجیه‌پذیر باشند تا پیامدهای ذهنی را شناسایی کند و تا حد امکان از آنها دوری کند.
- تمامی مراحل باید به گونه‌ای مستند شوند که در آینده برای سایرین قابل درک باشد. این اقدام پردازش بعدی مفهوم امنیت اطلاعات را تسهیل می‌کند.
- تلاش لازم برای اجرای این روش باید منعکس‌کننده ارزش کاربردهای فناوری اطلاعات و ارزش‌های سازمان باشد.

جدول ۳-۹. شناسنامه (۶): راهنمای Austrian IT Security Handbook

شناسنامه راهنمای Austrian IT Security Handbook		
نام اختصاری	کتابچه راهنمای امنیتی فناوری اطلاعات – IT Security Handbook	
نام کامل	کتابچه راهنمای امنیت فناوری اطلاعات اتریش	Austrian IT Security Handbook
ارائه‌دهنده	شورا فدرال اتریش	
کشور ارائه‌دهنده	اتریش	
وضعیت نسخه	نخستین نسخه این کتابچه در سال ۱۹۹۸ میلادی منتشر شد، نسخه (۲,۲) این سند در نوامبر سال ۲۰۰۴ میلادی و در حال حاضر نسخه (۴,۲,۲.) این راهنما در سال ۲۰۲۰ میلادی به عنوان آخرین نسخه معتبر محسوب می‌شود.	
زبان	آلمانی	
قیمت	به صورت رایگان در دسترس است.	
دامنه کاربرد/ استفاده	در اصل برای سازمان‌های دولتی توسعه یافته بود ولی در حال حاضر برای انواع کسب‌وکارها در دسترس است.	
هدف	این کتابچه شامل یک توضیحات عمومی دربارهٔ فرآیند ارزیابی مخاطره است، اما روش خاصی را مشخص نمی‌کند.	
مراحل مدیریت مخاطره	پشتیبانی از مراحل روش ارزیابی مخاطره: - شناسایی مخاطره - تحلیل مخاطره - سنجش مخاطره	پشتیبانی از مراحل روش مدیریت مخاطره: - ارزیابی مخاطره - مواجهه با مخاطره - پذیرش مخاطره - ارتباط با مخاطره
فرمول محاسبه مخاطره	پیشنهادهایی در خصوص محاسبه مخاطره ارائه می‌دهد اما فرمول مشخصی ارائه نداده است.	
سازگاری با استانداردها	این کتابچه/ سند با استانداردهای ISO/IEC 27001، ISO/IEC IS 13335، روش IT-Grundschutz و تا حدودی نیز با استاندارد ISO/IEC IS 17799 سازگار است.	
ابزارهای پشتیبان	ابزارهای غیرتجاری در وضعیت نمونه اولیه (به صورت رایگان) از آن پشتیبانی می‌کنند.	
مزایا/ نقاط قوت	+ یک رویکرد ترکیبی؛ + مناسب در هر نوع و سطحی از سازمان؛ + بسیار مقرون‌به‌صرفه است؛ + از سرعت به نسبت مناسبی برخوردار است؛	
معایب/ نقاط ضعف	- عدم پشتیبانی از زبان‌های رایج دنیا؛ (فقط زبان آلمانی) - این کتابچه راهنما شامل توضیح عمومی در ارتباط با ارزیابی مخاطره است، اما روش خاصی را مشخص نمی‌کند؛ - فرآیند تحلیل مخاطره آن از دقت پایینی برخوردار است؛	
وب‌سایت‌رسمی	http://www.cio.gv.at/securenetworks/sihb/	

۳-۲-۲-۲. راهنمای MAGERIT

روش **تحلیل و مدیریت مخاطره سیستم‌های اطلاعاتی**[1] یا به اختصار «MAGERIT»، یک روش متن‌باز است که توسط **وزارت امورخارجه اسپانیا**[2] توسعه یافته است و به عنوان یک چارچوب و راهنمای مدیریت دولتی جهت امنیت شبکه‌ها و سیستم‌های اطلاعاتی و با اهداف ذیل ارائه شده است:

- آگاه ساختن مسئولان سیستم‌های اطلاعاتی از وجود مخاطره‌ها و لزوم مقابله به موقع با آنها؛
- ارائه یک روش نظام‌مند برای تحلیل مخاطره‌ها؛
- کمک در توصیف و برنامه‌ریزی اقدام‌های مناسب برای تحت کنترل نگه داشتن مخاطره‌ها؛
- به صورت غیرمستقیم، آماده‌سازی سازمان برای سنجش، ممیزی، صدور گواهی‌نامه یا فرآیندهای اعتبارسنجی مرتبط در هر مورد.
- طراحی متن‌باز جهت استفاده در خارج از سازمان.

در ادامه، به چهار بخش اصلی فرآیند تحلیل مخاطره راهنمای «MAGERIT» همراه با فرآیندهای موجود در هر بخش در قالب (**شکل ۳-۱۴**) اشاره شده است.

شکل ۳-۱۴. مراحل تحلیل مخاطره راهنمای MAGERIT

هر فرآیند شامل تعدادی فعالیت به شرح ذیل است:

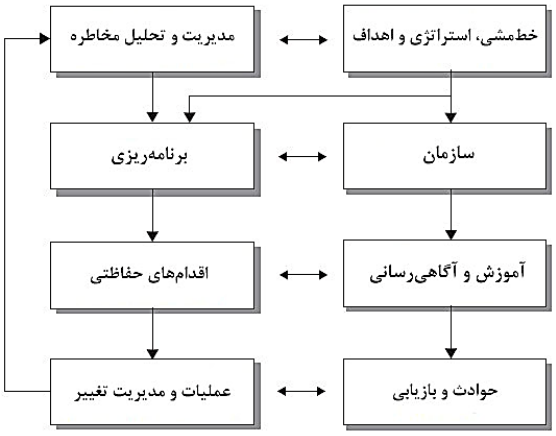
- **بخش نخست – تعیین ویژگی دارایی‌ها**: این بخش دارایی‌های مربوط به سیستم مورد تحلیل را شناسایی می‌کند و آنها را با توجه به نوع دارایی‌ها مشخص می‌کند، روابط بین دارایی‌های گوناگون را شناسایی می‌کند، تعیین می‌کند کدام ابعاد امنیتی مهم هستند و این اهمیت را ارزیابی می‌کند. خروجی این بخش، گزارشی تحت عنوان «**مدل ارزش**[3]» است. این بخش بر پایهٔ فرآیندهای زیر است:
  - شناسایی دارایی‌ها؛
  - وابستگی/ ارتباط بین دارایی‌ها؛
  - ارزش دارایی‌ها.

[1] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)
[2] Spanish Ministerio de Administraciones Públicas
[3] Value Model

- **بخش دوم – تعیین ویژگی تهدیدها**: این بخش تهدیدهای مربوط به سیستم مورد تحلیل را شناسایی می‌کند و آنها را با توجه به برآورد وقوع (احتمال) و خسارت وارده (تخریب) مشخص می‌کند. خروجی این بخش، گزارشی تحت عنوان «**نقشه مخاطره**[1]» است. این بخش بر پایهٔ فرآیندهای زیر است:
  - شناسایی تهدیدها؛
  - ارزش تهدیدها.
- **بخش سوم – تعیین ویژگی حفاظ‌های امنیتی**: این بخش حفاظ‌های امنیتی مستقر در سیستم مورد تحلیل را شناسایی می‌کند و آنها را با توجه به اثربخشی آنها در برابر تهدیدهایی که قصد کاهش آنها را دارند، مشخص می‌کند. خروجی این بخش، مجموعه‌ای از گزارش‌ها در قالب شرح کاربردپذیری/ قابلیت اجراء، سنجش حفاظ‌های امنیتی، کمبودها[2] (یا آسیب‌پذیری‌های سیستم حفاظتی) است. این بخش بر پایهٔ فرآیندهای زیر است:
  - شناسایی حفاظ‌های امنیتی مرتبط؛
  - سنجش حفاظ‌های امنیتی.
- **بخش چهارم – تخمین وضعیت مخاطره**: این بخش داده‌های جمع‌آوری شده در بخش قبلی را با هدف:
  - تهیه گزارش وضعیت مخاطره: تخمین مخاطره و پیامد؛
  - تهیه گزارش کمبودها (آسیب‌پذیری‌ها): نقص یا ضعف سیستم حفاظ‌های امنیتی.

  پردازش می‌کند. این بخش بر پایهٔ فرآیندهای زیر است:
  - تخمین پیامد؛
  - تخمین مخاطره.

این روش فرآیند مدیریت مخاطره را در یک چارچوب کاری پیاده‌سازی می‌کند تا نهادهای حاکمیتی با درنظر گرفتن مخاطره‌های ناشی از بهره‌برداری از فناوری‌های اطلاعاتی تصمیم‌گیری کنند. نقشه‌راه روش پیش‌گفته در قالب (**شکل ۳-۱۵**) نشان داده شده است.



شکل ۳-۱۵. نقشه راه روش MAGERIT

[1] Risk Map

[2] Deficiencies

جدول ۳-۱۰. شناسنامه (۷): روش MAGERIT

شناسنامه روش MAGERIT	
نام اختصاری	ماگِریت - MAGERIT
نام کامل	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) روشی برای مدیریت و تحلیل مخاطره‌های سیستم‌های اطلاعاتی
ارائه‌دهنده	وزارت امور خارجه اسپانیا
کشور ارائه‌دهنده	اسپانیا
وضعیت نسخه	نخستین نسخه این چارچوب در سال ۱۹۹۷ میلادی منتشر شد، نسخه دوم در سال ۲۰۰۵ میلادی به چاپ رسید و در حال حاضر نسخه سوم در سال ۲۰۱۴ میلادی این روش به عنوان آخرین نسخه معتبر محسوب می‌شود.
زبان	اسپانیایی، انگلیسی، ایتالیایی
قیمت	به صورت رایگان در دسترس است.
دامنه کاربرد/ استفاده	موردعلاقه افرادی است که با اطلاعات مکانیزم شده کار می‌کنند و سیستم‌های رایانه‌ای که آن را مدیریت می‌کنند.
هدف	**اهداف مستقیم:** - آگاه‌ساختن مسئولان سیستم‌های اطلاعاتی از وجود مخاطره‌ها و لزوم مقابله به موقع با آنها؛ - ارائه یک روش سیستماتیک برای تحلیل مخاطرات؛ - کمک به تشریح و برنامه‌ریزی اقدام‌های مناسب برای به حداقل رساندن مخاطره‌ها. **اهداف غیرمستقیم:** - آماده‌سازی سازمان جهت فرآیندهای سنجش، ممیزی، تأیید اعتبار یا اعتبارسنجی؛ - دستیابی به یکنواختی در گزارش‌های حاوی یافته‌ها و نتایج حاصل از پروژه مدیریت و تحلیل مخاطره.
مراحل مدیریت مخاطره	۱. تعیین دارایی‌های مرتبط با سازمان، روابط بین آنها و ارزش آنها؛ ۲. تعیین تهدیدهایی که این دارایی‌ها را در معرض خطر قرار می‌دهد؛ ۳. تعیین حفاظ‌های امنیتی در دسترس و چگونگی مواجهه مؤثر با مخاطره؛ و ۴. تخمین/ برآورد وضعیت مخاطره. پیشنهاد می‌شود پس از اتمام فرآیند ارزیابی مخاطره، مرحله (۴) مجدد تکرار و مورد استفاده قرار گیرد.
فرمول محاسبه مخاطره	بیش از یک فن برای محاسبه مخاطره ارائه داده است. یکی از فرمول‌های پیشنهادی: مخاطره (تهدید، دارایی) = احتمال (تهدید) × آسیب‌پذیری (تهدید، دارایی) × پیامد (تهدید، دارایی)
سازگاری با استانداردها	این روش با استانداردهای ISO/IEC 27001، ISO/IEC 15408، ISO/IEC 1779، ISO/IEC 13335، ISO/IEC 27005 و ISO 31000 سازگار است.
ابزارهای پشتیبان	ابزارهای غیرتجاری: PILAR : http://www.ar-tools.com/pilar/ ابزارهای تجاری: EAR : http://www.ar-tools.com/
مزایا/ نقاط قوت	+ ارائه فرآیند ارزیابی مخاطره در سطوح گوناگون و مورد استفاده به صورت کمّی و کیفی؛ + پشتیبانی توسط اسناد فنی که دارایی‌های مشترک، تهدیدها، حفاظ‌های امنیتی، معیارها، قالب‌ها و فنون رسمی را تشریح می‌کند؛ + می‌تواند به صورت یک روش ارزیابی مخاطره جداگانه/ مستقل و همچنین به عنوان یک سیستم مدیریت امنیت اطلاعات کامل مورد استفاده قرار گیرد. + بسیار انعطاف‌پذیر (امکان انجام فرآیند تحلیل در سازمان‌هایی با اندازه گوناگون)؛ + مورد استفاده در بسیاری از کشورهای عضو و کشورهای غیرعضو اتحادیه اروپا؛ + از سطح متوسطی از پیچیدگی برخوردار است.
معایب/ نقاط ضعف	- نسخه سوم از این روش تنها به زبان اسپانیایی در دسترس است. - تأثیر عامل انسانی در نتیجه نهایی.
وب‌سایت‌رسمی	https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en

۳-۲-۲-۳. راهنمای Microsoft's Security Risk Management

راهنمای **مدیریت مخاطره امنیت مایکروسافت**[1] یا به اختصار «Microsoft» یک رویکرد ترکیبی است که بهترین عناصر از دو رویکرد سنتی و رویکردهای کیفی و کمّی را با یک‌دیگر تلفیق کرده است. این راهنما یک رویکرد منحصربه‌فرد جهت مدیریت مخاطره امنیت ارائه می‌دهد که به طور قابل توجهی سریع‌تر از یک رویکرد کمّی سنتی است. این راهنمای توصیفی به تمامی مشتریان در برنامه‌ریزی، ساخت و نگهداری یک برنامه مدیریت مخاطره امنیت موفق کمک می‌کند. این راهنما در واقع، یک فرآیند چهار مرحله‌ای مدیریت مخاطره است که به ذینفعان کمک می‌کند تا مخاطره‌های امنیتی حوزه فناوری اطلاعات را شناسایی و کاهش دهند. فرآیند مدیریت مخاطره امنیتی مایکروسافت از چهار مرحله تشکیل شده است. این چرخه مدیریت مخاطره چهاربخشی، خلاصه فرآیند مدیریت مخاطره امنیت مایکروسافت است که برای ساختاردهی مطالب در سراسر این راهنما نیز استفاده می‌شود.

با این وجود، قبل از تعریف روش‌های خاص در فرآیند مدیریت مخاطره امنیت مایکروسافت، درک فرآیند مدیریت مخاطره و مؤلفه‌های آن بسیار مهم است. هر بخش از چرخه شامل چندین مرحله است. فهرست زیر با تشریح هر مرحله کمک می‌کند تا اهمیت هر یک از مراحل به طورکلی در راهنما درک شود:

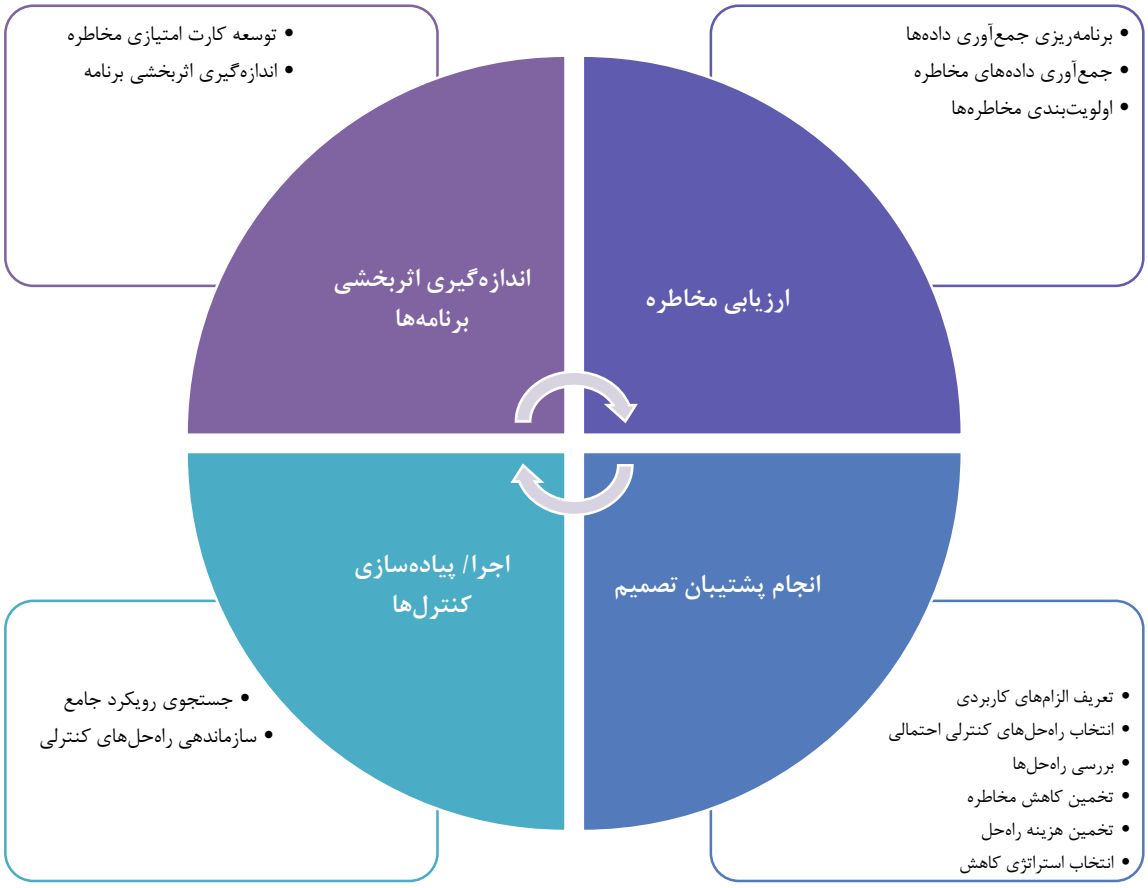
- **مرحله نخست – ارزیابی مخاطره**: شناسایی و اولویت‌بندی مخاطره‌های مربوط به کسب‌کار با ترکیب جنبه‌هایی از روش‌های کیفی و کمّی ارزیابی مخاطره؛
  - برنامه‌ریزی جمع‌آوری داده‌ها: بحث درباره کلیدهای موفقیت و راهنمای آماده‌سازی؛
  - جمع‌آوری داده‌های مخاطره: نمای کلی تحلیل و فرآیند جمع‌آوری داده‌ها؛
  - اولویت‌بندی مخاطره‌ها: نمای کلی مراحل پیشنهادی جهت تعیین کیفیت و کمّی‌سازی مخاطره‌ها.
- **مرحله دوم – فرآیند اجرای تصمیم‌یار**[2]: شناسایی و سنجش راهکارهای کنترلی بر پایهٔ فرآیند مشخص تحلیل هزینه-منفعت؛
  - تعریف الزام‌های کاربردی: تعریف الزام‌های کاربردی جهت کاهش مخاطره‌ها؛
  - انتخاب راهکارهای کنترلی احتمالی: نمای کلی رویکرد جهت شناسایی راهکارهای کاهش؛
  - بررسی راهکارها: سنجش کنترل‌های پیشنهادی در برابر الزام‌های کاربردی؛
  - تخمین کاهش مخاطره: کوشش جهت کاهش میزان مواجهه یا احتمال مخاطره‌ها؛
  - تخمین هزینه راهکار: سنجش هزینه‌های مستقیم و غیرمستقیم مربوط به راهکارهای کاهش؛
  - انتخاب راهبرد کاهش: تکمیل تحلیل هزینه-منفعت جهت شناسایی کارآمدترین راهکار کاهش هزینه.
- **مرحله سوم – اجرا/ پیاده‌سازی کنترل‌ها**: استقرار و راه‌اندازی راهکارهای کنترلی جهت کاهش مخاطره در کسب‌وکارها؛
  - جستجوی رویکرد جامع: ادغام/ ترکیب افراد، فرآیندها و فناوری در راهکار کاهش؛
  - سازماندهی از طریق **دفاع در عمق**[3]: سازماندهی راهکارهای کاهش در کل کسب‌وکار؛
- **مرحله چهارم – اندازه‌گیری اثربخشی برنامه:** تجزیه و تحلیل فرآیند مدیریت مخاطره جهت اثربخشی و اطمینان از ارائه میزان حفاظت موردانتظار از سوی کنترل‌ها.
  - توسعه **کارت امتیازی مخاطره**[4]: درک وضعیت و پیشرفت مخاطره؛
  - اندازه‌گیری اثربخشی برنامه: سنجش برنامه مدیریت مخاطره جهت فرصت‌های بهبود.

---

[1] The Microsoft's Security Risk Management Guide
[2] Decision Support
[3] Defense-in-depth
[4] Risk Scorecard

در این فرآیند چهار مرحله‌ای، (**شکل ۳-۱۶**) راهنمای چگونگی ایجاد یک فرآیند مستمر برای اندازه‌گیری و هدایت مخاطره‌های امنیتی به یک سطح قابل قبول را شرح می‌دهد. فرآیند مدیریت مخاطره امنیتی مایکروسافت ترکیبی از رویکردهای گوناگون از جمله تحلیل کمّی خالص، بازگشت تحلیل سرمایه‌گذاری امنیتی[1] (مقدار پولی که انتظار می‌رود یک سازمان در طی یک سال با اجرای کنترل امنیتی پس‌انداز کند)، تحلیل کیفی و رویکردهای به‌روش‌ها را ارائه می‌دهد. باید به این نکته مهم اشاره کرد که این راهنما به یک فرآیند می‌پردازد و به فناوری خاصی نیازی ندارد.

با توجه به اینکه فرآیند مدیریت مخاطره امنیتی مایکروسافت یک فرآیند مداوم/ مستمر و در حال اجرا است، سازمان‌ها می‌توانند با هدف پیشگیری از مخاطره نسبت به شناسایی و پایش دارایی‌ها، تهدیدها و آسیب‌پذیری‌های جدید اقدام کنند.



شکل ۳-۱۶. فرآیند چهارمرحله‌ای مدیریت مخاطره Microsoft

[1] Return on Security Investment (ROSI)

جدول ۳-۱۱. شناسنامه (۸): روش Microsoft

شناسنامه روش «Microsoft»	
نام اختصاری	مایکروسافت – Microsoft
نام کامل	Microsoft's Security Risk Management Guide راهنمای مدیریت مخاطره امنیت مایکروسافت
ارائه‌دهنده	مایکروسافت
کشور ارائه‌دهنده	ایالات متحده آمریکا
وضعیت نسخه	اولین نسخه این راهنما در سال ۲۰۰۶ میلادی منتشر گردید و در حال حاضر نسخه به‌روزرسانی شده این راهنما در سال ۲۰۲۰ میلادی به عنوان آخرین نسخه معتبر محسوب می‌شود.
زبان	انگلیسی
قیمت	به صورت رایگان در دسترس است.
دامنه کاربرد/ استفاده	بر چگونگی برنامه‌ریزی، استقرار و حفظ و نگهداری فرآیند موفقیت‌آمیز مدیریت مخاطره امنیتی در هر نوع و اندازه از سازمان متمرکز است.
هدف	به ذینفعان کمک می‌کند تا مخاطره‌های امنیتی حوزه فناوری اطلاعات را شناسایی و کاهش دهند.
مراحل مدیریت مخاطره	شامل چهار مرحله: - مرحله نخست: شناسایی و اولویت‌بندی مخاطره‌ها با توجه به کسب‌وکار؛ - مرحله دوم: شناسایی و سنجش کنترل‌ها بر پایهٔ فرآیند تحلیل هزینه-منفعت جهت انتخاب راهکارهای کنترلی ممکن؛ - مرحله سوم: اجرای کنترل‌ها با درنظر گرفتن افراد، فرآیندها و فناوری؛ - مرحله چهارم: تمرکز بر اندازه‌گیری اثربخشی برنامه مدیریت مخاطره اطلاعات از طریق پایش و نظارت مواجهه با مخاطره؛
فرمول محاسبه مخاطره	پیشنهادهایی در خصوص محاسبه مخاطره ارائه می‌دهد اما فرمول مشخصی ارائه نداده است.
سازگاری با استانداردها	با استانداردهای سری ISO 27000 و NIST 800 سازگار است.
ابزارهای پشتیبان	مجموعه‌ای از ابزارها و قالب‌های مدیریت مخاطره امنیتی جهت استفاده آسان سازمان‌ها از این راهنما در فرمت وُرد و اکسل.
مزایا/ نقاط قوت	+ نه تنها شامل فرآیند ارزیابی مخاطره است بلکه با اجرای فرآیند تصمیم‌یار، پیاده‌سازی کنترل‌ها و اندازه‌گیری اثربخشی برنامه مدیریت مخاطره را نیز پوشش می‌دهد؛ + از نظر تکرارپذیری قوی است؛ + امکان اجرای فرآیند ارزیابی مخاطره اطلاعات در فواصل منظم با توجه به داده‌های جدید در هر مرحله؛ + پشتیبانی از مراحل کیفی و کمّی فرآیند ارزیابی مخاطره؛ + توانمندسازی سازمان‌ها جهت اجرا و نگهداری فرآیندهای شناسایی و اولویت‌بندی مخاطره‌ها در محیط فناوری اطلاعات؛ + مناسب جهت هر نوع و اندازه‌ای از سازمان؛ + راهنمایی بسیار دقیق جهت درک کامل از مخاطره‌های با اهمیت بالا؛ + ارائه اسناد پشتیبان و تکمیلی جهت کمک به فرآیند ارزیابی مخاطره؛ + ساده‌تر از مدیریت مخاطره کمّی سنتی است؛ + به حداقل رساندن مقاومت در برابر نتایج تحلیل مخاطره و مراحل پشتیبان تصمیم؛ + امکان دستیابی سریع‌تر به نتایج و نگهداری آن در طول فرآیند؛ + بسیار مقرون‌به‌مصرفه.
معایب/ نقاط ضعف	- عدم قابلیت جمع‌آوری داده‌ها به صورت خودکار؛ - عدم امکان نمایش گرافیکی گزارش‌ها؛ - علی‌رغم عمومیت راهنما، در سازمان‌های فناوری مانند خود مایکروسافت به شکل مؤثرتری عمل می‌کند.
وب‌سایت‌رسمی	https://www.microsoft.com/en-us/

۳-۲-۲-۴. چارچوب‌های ISACA

انجمن نظارت و کنترل سیستم‌های اطلاعاتی که به اختصار «ایساکا» نامیده می‌شود یکی از تأثیرگذارترین تشکل‌های حرفه‌ای و استانداردگذار در زمینه نظارت و کنترل سامانه‌های اطلاعاتی و راهبری فناوری اطلاعات در آمریکا و جهان است؛ که بیش از ۴۵ سال از تشکیل آن می‌گذرد. «ایساکا» یکی از اعضای وابسته **فدراسیون بین‌المللی حسابداران**[1] (IFAC) نیز است. «ایساکا»، هم‌اکنون بیش از صدهزار عضو دارد که در ۱۸۰ کشور جهان زندگی و کار می‌کنند. پیشه اعضای «ایساکا» طیف گوناگونی از پیشه‌های مربوط به فناوری اطلاعات را در بر می‌گیرد، از جمله نظارت سامانه‌های اطلاعاتی، مشاور سامانه‌های اطلاعاتی، آموزگار سامانه‌های اطلاعاتی، کارشناس امنیت سامانه‌های اطلاعاتی، مقررات‌گذار، حسابرس داخلی، و غیره. دامنه تجربه این اعضاء نیز از تازه‌کاران تا متخصصان زبردست را شامل می‌شود. این اعضاء در صنایع گوناگونی همچون مالی، بانکداری، حسابرسی، تولیدی، و غیره در دو بخش دولتی و خصوصی کار می‌کنند. این گوناگونی پیشه‌ها، تجارب، و صنایع موجب شده است تا اعضای «ایساکا» همواره در حال فراگیری از یک‌دیگر باشند و دانسته‌های خود را با هم به اشتراک بگذارند. این ویژگی یگانه یکی از توانمندی‌های قابل توجه «ایساکا» به‌شمار می‌رود.

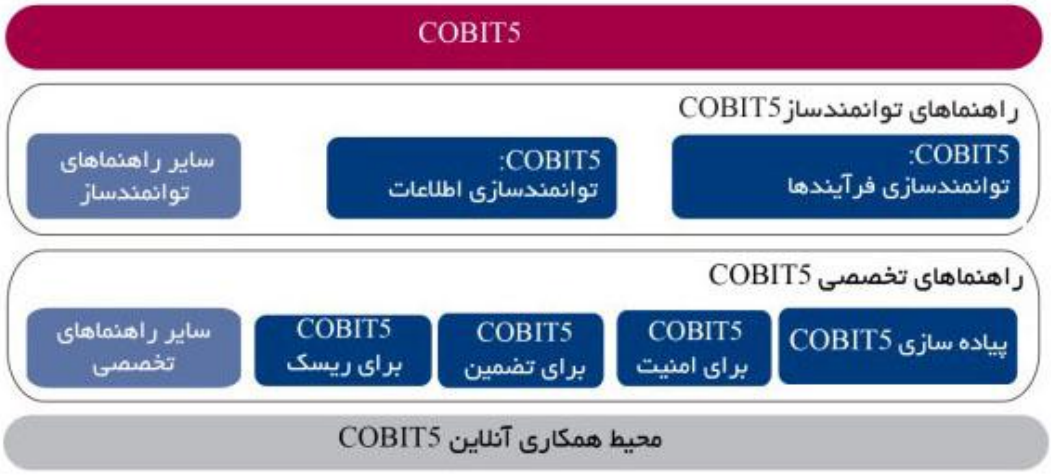
مؤسسه «ایساکا» چارچوب‌هایی مانند COBIT، **ارزش فناوری اطلاعات**[2] (Val IT)، **مخاطره فناوری اطلاعات**[3] (Risk IT)، **مدل کسب‌وکار برای امنیت اطلاعات**[4] (BMIS) و **چارچوب تضمین فناوری اطلاعات**[5] (ITAF) را برای کمک به سازمان‌ها در اجرای حاکمیت فناوری اطلاعات ارائه کرده و چارچوب COBIT-5 با ایجاد یک معماری یکپارچه برای حاکمیت فناوری اطلاعات، تمام این چارچوب‌ها را در کنار یکدیگر بکار می‌برد و مبتنی بر مجموعه‌ای از توانمندسازها، تدوین یک پایگاه دانش و در نهایت با بهره‌برداری از یک مدل مرجع فرآیندی استقرار حاکمیت فناوری اطلاعات را در سازمان‌ها به وجود خواهد آورد.

چارچوب «COBIT-5» مدل مرجع فرآیند حاکمیت و مدیریت فرآیندهای سازمانی فناوری اطلاعات به دو حوزه اصلی «فرآیندهای حاکمیت» و «فرآیندهای مدیریت» می‌پردازد. فرآیندهای حاکمیت، حاوی پنج فرآیند حاکمیتی شامل حاکمیت‌های اطمینان از تنظیم چارچوب و نگهداری، اطمینان از تحویل سود، اطمینان از بهینه‌سازی سود، اطمینان از بهینه‌سازی منابع و اطمینان از شفافیت ذینفعان است که برای هر یک از پنج فرآیند یاد شده کارهای ارزیابی، هدایت و پایش تعریف شده است. فرآیندهای مدیریت «COBIT-5» شامل ۳۲ فرآیند در چهار حوزه فرآیندی است که ۱۳ فرآیند برنامه‌ریزی، ۱۰ فرآیند در ساخت، شش فرآیند در اجرا و سه فرآیند در نظارت تمامی محدوده فناوری اطلاعات را پوشش می‌دهد.

محصولات «COBIT-5» دو بخش اصلی دارد. در بخش نخست راهنماهای توانمندسازی شامل: فرآیندهای توانمندسازی، اطلاعات توانمندسازی و دیگر راهنماهای توانمندساز است. توانمندسازها دستیابی به اهداف حاکمیتی سازمان را آسان می‌سازد و هدف از طراحی آنها پیاده‌سازی مؤثر سیستم حاکمیت و مدیریت فناوری اطلاعات سازمان است. بخش دوم محصولات «COBIT-5» راهنماهای حرفه‌ای است که شامل، راهنمای پیاده‌سازی، «COBIT-5» برای امنیت اطلاعات، «COBIT-5» برای تضمین، «COBIT-5» برای مخاطره و دیگر راهنماهای حرفه‌ای دیگر است (**شکل ۳-۱۷**).

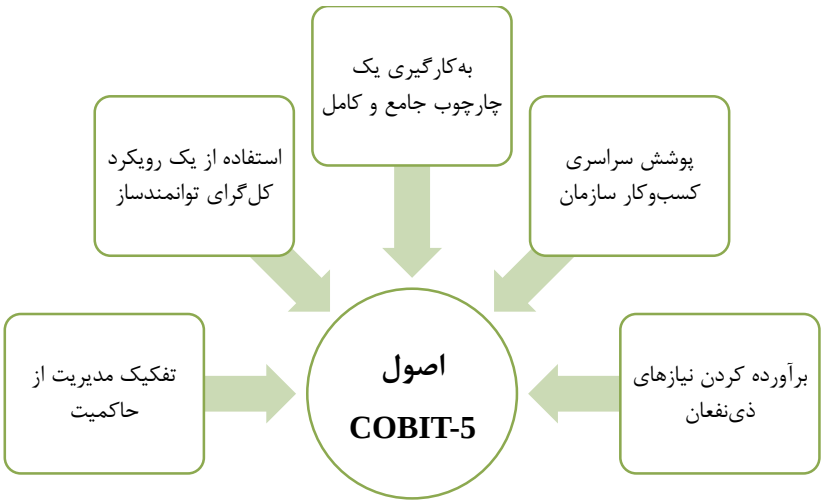
---

[1] International Federation of Accountants (IFAC)
[2] Val IT
[3] Risk IT
[4] Business Model for Information Security (BMIS)
[5] The Information Technology Assurance Framework (ITAF)



شکل ۳-۱۷. خانواده محصولات COBIT-5، (ISACA 2019)

این چارچوب برای رسیدن به حاکمیت فناوری اطلاعات در سازمان دارای پنج اصل بنیادی است که شامل، "برآورده کردن نیازهای ذی‌نفعان"، "پوشش سراسری کسب‌وکار سازمان"، "به‌کارگیری یک چارچوب جامع و کامل"، "بهره‌برداری از یک رویکرد کل‌گرای توانمندساز" و "تفکیک مدیریت از حاکمیت" است **(شکل ۳-۱۸)**.

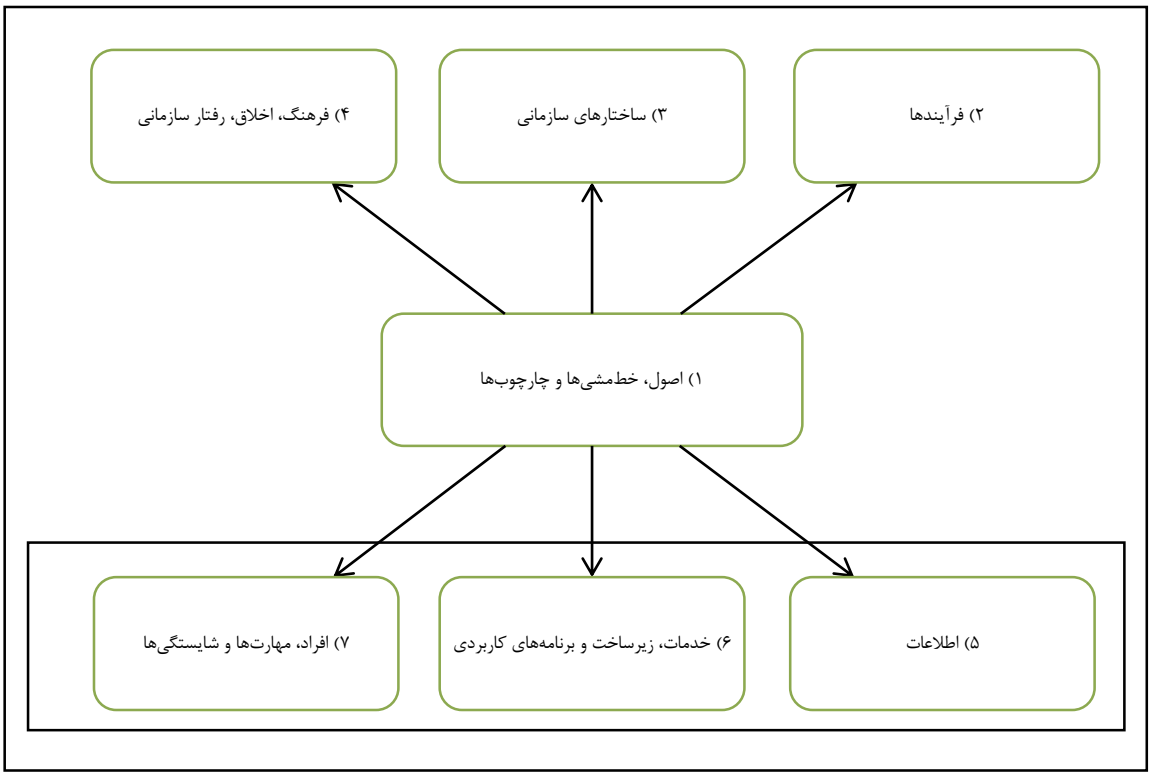


شکل ۳-۱۸. اصول چارچوب COBIT-5

«COBIT-5» تنها چارچوب کسب‌وکار برای مدیریت سازمان و حاکمیت فناوری اطلاعات است که به افزایش ارزش اطلاعات به وسیله سازمان‌دهی به آخرین تفکرات در حاکمیت فناوری اطلاعات و فنون مدیریتی آن می‌پردازد و اصول، تجارب، ابزارهای تحلیلی و مدل‌هایی ارائه می‌کند که اصل حاکمیت فناوری اطلاعات در سازمان‌ها را تثبیت می‌کند. طراحی و تدوین این چارچوب نشان می‌دهد که جهان به نقش فناوری اطلاعات به عنوان یک ابزار در سازمان‌ها اکتفا نمی‌کند و در پی آن است که با گسترش این دانش عظیم، آن را تا سطح حاکمیتی ارتقاء دهد و در تمامی فرآیندهای تصمیم‌گیری و راهبرد از آن بهره بگیرد.

در واقع، چارچوب «COBIT-5» یک راهنمای جامع و گام‌به‌گام در فرآیند مدیریت مخاطره برای خلق ارزش در سازمان و روش‌شناسی لازم برای ارزیابی و پاسخگویی به مخاطره را ارائه می‌دهد. «COBIT-5» به ایجاد دید دقیق‌تر نسبت به مخاطره‌های کنونی و آینده در سازمان و مشخص کردن مسئولیت‌های مربوط به مخاطره در کل سازمان کمک می‌کند. همچنین نمونه‌های عملی از سناریوهای رایج را درحوزه فناوری اطلاعات در قالب پروفایل‌های مخاطره معرفی کرده است. این چارچوب تمامی ۱۱ اصل مدیریت مخاطره در استاندارد ISO 31000 را با پنج اصل و هفت توانمندساز **(شکل ۳-۱۹)**، پوشش می‌دهد. همچنین تمامی جنبه‌های

موجود در چارچوب و فرآیند مدیریت مخاطره تعریف شده در استاندارد ISO 31000، در مدل فرآیندی «COBIT-5» نیز وجود دارد.



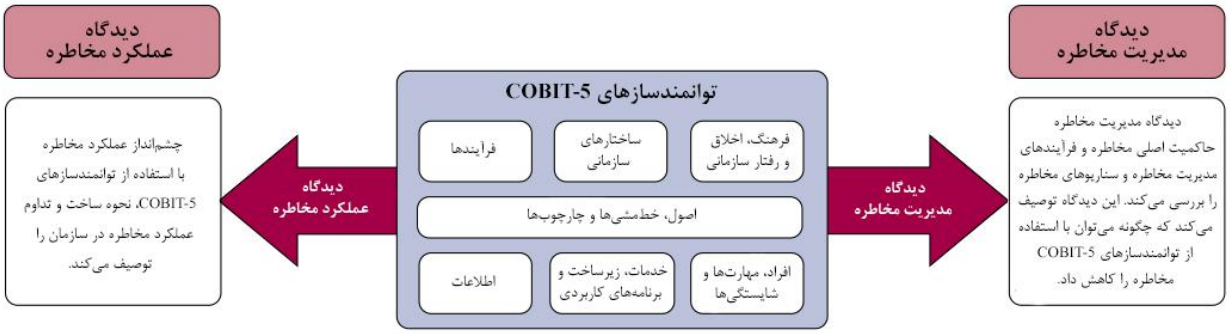
شکل ۳-۱۹. توانمندسازهای چارچوب COBIT-5، (ISACA 2012)

تمامی این توانمندسازها در هر دو لایه حاکمیت و مدیریت مخاطره کاربرد دارند. هدف اصلی از پیاده‌سازی چارچوب «COBIT-5» بهره‌برداری از این هفت توانمندساز برای تصحیح، تسهیل و تسریع فرآیند مدیریت مخاطره است. در واقع، توانمندسازهای چارچوب «COBIT-5» به پیاده‌سازی فعالیت‌های کلیدی راهبری و مدیریت مخاطره کمک می‌کنند و اجرا نمودن این فرآیند را تسهیل و ممکن می‌سازند.

۳-۲-۲-۴-۱. چارچوب COBIT-5 for Risk

«COBIT-5 برای مخاطره» -همان طور که در (**شکل ۳-۱۷**) نشان داده شده است- بر پایهٔ چارچوب «COBIT-5» و با تمرکز بر مخاطره و ارائه راهنمایی دقیق‌تر و عملی‌تر برای مختصصان مخاطره و دیگر افراد علاقه‌مند در تمامی سطوح سازمان ایجاد شده است. «COBIT-5 برای مخاطره» در ارتباط با مخاطره‌های مربوط به فناوری اطلاعات صحبت می‌کند. «COBIT-5 برای مخاطره» دربارهٔ شیوهٔ بهره‌برداری از «COBIT-5» در زمینه مخاطره دو دیدگاه ارائه می‌دهد که در قالب (**شکل ۳-۲۰**) نشان داده شده است.

- **دیدگاه عملکرد مخاطره**: توصیف آنچه در یک سازمان برای ایجاد و تداوم فعالیت‌های مدیریت و حاکمیت پایدار و مؤثر مخاطره نیاز است. در واقع، این دیدگاه بر نیازمندی‌های ایجاد و حفظ عملکرد مخاطره در یک سازمان متمرکز است.
- **دیدگاه مدیریت مخاطره**: توصیف اینکه چگونه فرآیند اصلی مدیریت مخاطره شامل شناسایی، تحلیل، پاسخگویی و گزارش‌دهی می‌تواند توسط توانمندسازهای «COBIT-5» هدایت و مورد استفاده قرار گیرند. در واقع، این دیدگاه بر فرآیندهای اصلی حاکمیت و مدیریت مخاطره در ارتباط با چگونگی بهینه‌سازی مخاطره و شیوهٔ شناسایی، تحلیل، پاسخگویی و گزارش مخاطره به صورت روزانه متمرکز است.



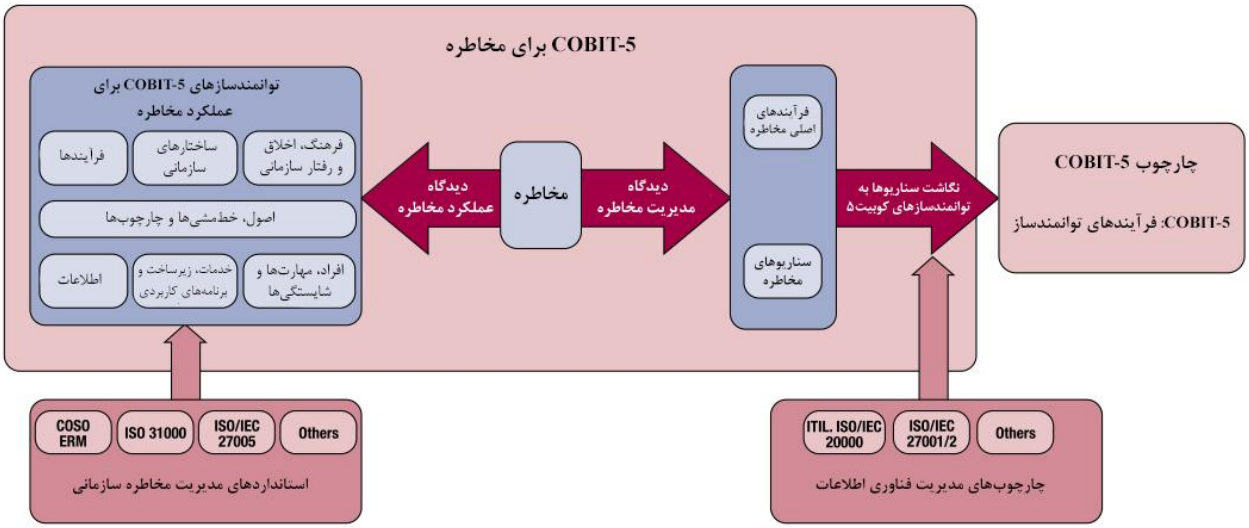
شکل ۳-۲۰. دیدگاه مطرح در ارتباط با مخاطره، (ISACA 2013)

بهره‌برداری از «COBIT-5 برای مخاطره»، توانمندی‌های مربوط به مخاطره سازمانی را افزایش می‌دهد که از جمله مزایایی که برای سازمان به همراه دارد می‌توان به موارد ذیل اشاره کرد:

- شناسایی دقیق‌تر مخاطره و تخمین موفقیت در مواجهه با مخاطره؛
- درک بهتر پیامد مخاطره بر سازمان؛
- راهنمای نظیربه‌نظیر در ارتباط با شیوهٔ مدیریت مخاطره، شامل مجموعه‌ای گسترده از اقدام‌ها؛
- دانش و آگاهی از شیوهٔ سرمایه‌گذاری در سرمایه‌گذاری‌های مربوط به روش‌های مدیریت مخاطره فناوری اطلاعات؛
- درک درست از شیوهٔ مؤثر مدیریت مخاطره فناوری اطلاعات با اثربخشی و کارآیی فرآیند کسب‌وکار، بهبود کیفیت و کاهش زمان و هزینه‌ها، در بهینه‌سازی ارزش؛
- فرصت‌های ادغام مدیریت مخاطره فناوری اطلاعات با مخاطره سازمانی و ساختارهای انطباق‌پذیر؛
- درک و ارتباطات بهبودیافته میان تمام ذی‌نفعان داخلی و خارجی با توجه به چارچوب و زبان مشترک و پایدار پذیرفته شده در سطح جهانی جهت ارزیابی و پاسخگویی به مخاطره؛
- ارتقاء مسئولیت و پذیرش مخاطره در کل سازمان؛
- یک پروفایل کامل از مخاطره، شناسایی کامل سازمان در معرض مخاطره و امکان استفاده بهتر از منابع سازمانی؛ و
- بهبود و افزایش آگاهی از مخاطره در کل سازمان.

(**شکل ۳-۲۱**) دامنه چارچوب «COBIT-5 برای مخاطره» و چگونگی ارتباط آن با دیگر چارچوب‌های «ایساکا» را نشان می‌دهد که همراه با «COBIT-5 برای مخاطره»، راهنمایی جامع در ارتباط با مدیریت و حاکمیت مخاطره در حوزه فناوری اطلاعات سازمان ارائه می‌کند.

- بر بهره‌برداری از توانمندسازهای «COBIT-5 برای مخاطره» از دیدگاه عملکرد مخاطره متمرکز است (برای نمونه، چگونگی بهره‌برداری از COBIT-5)؛
- عملکرد مؤثر و کارآمد مدیریت و حاکمیت مخاطره را ممکن می‌سازد؛
- با بهره‌برداری از فرآیندهای اصلی مدیریت مخاطره در «COBIT-5» و سناریوهای مخاطره، رهنمودهایی سطح بالا در ارتباط با چگونگی شناسایی، تحلیل و پاسخگویی به مخاطره ارائه می‌دهد؛
- با منابع مرجع بازار مدیریت مخاطره سازمانی (استانداردها، چارچوب‌ها و رهنمودهای عملیاتی) و طرح‌های مدیریت مخاطره سازمانی همراستا و در ارتباط است؛
- بین سناریوهای مخاطره و توانمندسازهای «COBIT-5» پیوند/ ارتباط برقرار می‌کند که می‌تواند برای کاهش مخاطره مورد استفاده قرار گیرد.



شکل ۳-۲۱. دامنه COBIT-5 برای مخاطره، (ISACA 2013)

جنبه مهم و ویژگی متمایز «COBIT-5 برای مخاطره» این است که **۲۰** دسته مخاطره تعریف می‌کند (**جدول ۳-۱۲**) که در مجموع **۱۱۲** سناریوی مخاطره را برای کمک به سازمان‌ها برای کاهش بهتر مخاطره شامل می‌شود. از این سناریوهای مخاطره می‌توان برای راهنمایی و هدایت مستقیم فعالیت مدیریت مخاطره استفاده کرد.

برخلاف استانداردها و چارچوب‌های دیگر، سناریوهای «COBIT-5 برای مخاطره» بیش از ۱۰۰ نوع مخاطره را پوشش می‌دهد، مانند سرقت و خرابکاری کارمندان، نقض داده‌ها، جاسوسی صنعتی و پشتیبانی از نوآوری.

جدول ۳-۱۲. دسته‌بندی تعریف شده سناریو مخاطره در COBIT

شماره	سناریو	شماره	سناریو
۱	استقرار و نگهداری نمونه کارها	۱۱	تأمین‌کننده
۲	مدیریت چرخه حیات برنامه/ پروژه	۱۲	پیروی از مقررات
۳	تصمیم‌گیری دربارهٔ سرمایه‌گذاری فناوری اطلاعات	۱۳	ژئوپلیتیک
۴	تخصص و مهارت‌های فناوری اطلاعات	۱۴	تخریب یا سرقت زیرساخت
۵	عملیات کارکنان	۱۵	بدافزار
۶	اطلاعات	۱۶	حمله‌های منطقی
۷	معماری	۱۷	اقدام صنعتی
۸	زیرساخت	۱۸	محیطی
۹	نرم‌افزار	۱۹	بلایای طبیعی
۱۰	مالکیت کسب‌وکار فناوری اطلاعات	۲۰	نوآوری

ایجاد کتابخانه‌ای از سناریوهای مخاطره، به سازمان کمک می‌کند تا مخاطره بالقوه را پیش‌بینی کرده و پاسخ‌های مناسب مخاطره را جهت کاهش پیامد در اشتهای مخاطره و تحمل مخاطره انتخاب کند. نشریات «ایساکا» (برای نمونه، COBIT-5 برای مخاطره، سناریوهای مخاطره برای COBIT-5) ابزارهای بسیار مفیدی را در اختیار متخصصان مخاطره قرار می‌دهند.

ابزار اصلی در فرآیند مدیریت مخاطره، بهره‌برداری از سناریوهای مخاطره است. «COBIT-5 برای مخاطره» که بر روی توانمندسازهای فرآیند مدیریت و فرآیند حاکمیت گسترش می‌یابد- دارای بخش کوچکی است که برخی از سناریوهای عمومی مخاطره را ارائه می‌دهد. با این وجود، متخصص مخاطره باید خود را با سناریوهای مخاطره مسلح کند و از COBIT-5 به عنوان یک کتابخانه جامع از سناریوهای مخاطره استفاده کند.

در واقع، سناریوی مخاطره توصیف یک رویداد احتمالی است که در صورت وقوع، پیامد نامشخصی بر سازمان خواهد داشت. این پیامد می‌تواند مثبت یا منفی باشد. برای توصیف سناریوی مخاطره می‌توان یک ساختار در «چارچوب COBIT» یافت که می‌تواند برای توصیف سناریوها مخاطره خاص سازمان مورد استفاده قرار گیرد. هسته اصلی فرآیند مدیریت مخاطره نیازمند شناسایی و ارزیابی مخاطره و پیاده‌سازی یک پاسخ مناسب جهت مواجهه با مخاطره است. سناریوهای مخاطره‌ای که به خوبی توسعه یافته‌اند از این فعالیت‌ها پشتیبانی کرده و آنها را به شکلی واقع‌بینانه و مرتبط با سازمان جلوه می‌دهند. سپس سناریو مخاطره رهنمودهایی در ارتباط با پاسخ مناسب با مخاطره ارائه می‌دهد. زمانی که فرآیند ارزیابی مخاطره مشخص می‌کند که مخاطره در تحمل و اشتهای مخاطره سازمان نیست، یکی از حالت‌های چهارگانه پاسخ به مخاطره در قالب موارد ذیل نیاز است:

- **اجتناب**: انجام آن فعالیت را متوقف کنید؛
- **کاهش**: اقدام‌های کاهشی را جهت کاهش مخاطره اجرا کنید؛
- **اشتراک/ انتقال**: انتقال مخاطره، مانند بهره‌برداری از بیمه؛
- **پذیرش**: هیچ کاری انجام ندهید و با مخاطره زندگی کنید.

اگر پاسخ به مخاطره انتخاب شده کاهش یابد، در این صورت سناریو مخاطره برخی از نشانگرها را به توانمندسازهای فرآیند COBIT-5 می‌دهد که می‌تواند جهت مدیریت مناسب مخاطره اجرا و پیاده‌سازی شود. در واقع، سناریوی مخاطره زمانی قابل کنترل و مدیریت است که کنترل‌ها/ تدابیر کافی در نظر گرفته شده باشند، به طوری که پیامدهای منفی یک حادثه بالقوه/ احتمالی را برای اهداف سازمانی به میزان مناسب کاهش دهد.

جدول ۳-۱۳. شناسنامه (۹): چارچوب COBIT-5 for Risk

شناسنامه چارچوب COBIT-5 for Risk	
نام اختصاری	کوبیت۵ برای مخاطره – COBIT-5 for Risk
نام کامل	COBIT-5 for Risk IT کوبیت۵ برای مخاطره فناوری اطلاعات
ارائه‌دهنده	انجمن نظارت و کنترل سیستم‌های اطلاعاتی (ایساکا)
کشور ارائه‌دهنده	ایالات متحده
وضعیت نسخه	نخستین نسخه این چارچوب در سال ۱۹۹۶ میلادی منتشر شد، نسخه COBIT-5 در سال ۲۰۱۲ میلادی به چاپ رسید و در حال حاضر نسخه ۲۰۱۹ این چارچوب به عنوان آخرین نسخه معتبر محسوب می‌شود.
زبان	انگلیسی
قیمت	به صورت رایگان برای اعضاء در دسترس است.
دامنه کاربرد/ استفاده	کنترل و مدیریت راهکارها و خدمات مبتنی بر فناوری اطلاعات کسب‌وکار در تمامی سطوح سازمان.
هدف	با تمرکز بر مخاطره و ارائه راهنمایی دقیق‌تر و عملی‌تر برای مختصصان مخاطره و دیگر افراد علاقه‌مند در تمامی سطوح سازمان ایجاد شده است.
مراحل مدیریت مخاطره	۱) جمع‌آوری داده ▪ ایجاد و نگهداری مدلی برای جمع‌آوری داده‌ها؛ ▪ جمع‌آوری داده در محیط عملیاتی؛ ▪ جمع‌آوری داده در ارتباط با رویدادهای مخاطره؛ ▪ شناسایی فاکتورهای مخاطره. ۲) تحلیل مخاطره ▪ تعیین حوزه تحلیل مخاطره فناوری اطلاعات؛ ▪ سنجش مخاطره فناوری اطلاعات؛ ▪ شناسایی گزینه‌های پاسخ به مخاطره؛ ▪ انجام یک بررسی دقیق از تحلیل مخاطره فناوری اطلاعات. ۳) نگهداری پروفایل مخاطره ▪ نگاشت منابع فناوری اطلاعات به فرآیندهای کسب‌وکار؛

شناسنامه چارچوب COBIT-5 for Risk	
	▪ تعیین اهمیت کسب‌وکار از منابع فناوری اطلاعات؛ ▪ درک قابلیت‌های فناوری اطلاعات؛ ▪ به‌روزرسانی مؤلفه‌های سناریو مخاطره فناوری اطلاعات. ۴) تشریح و تبیین مخاطره ۵) تعریف مجموعه اقدام‌های مدیریت مخاطره ۶) پاسخ به مخاطره
فرمول محاسبه مخاطره	مخاطره (تهدید، دارایی) = احتمال (تهدید) × آسیب‌پذیری (تهدید، دارایی) × پیامد (تهدید، دارایی)
سازگاری با استانداردها	این چارچوب با استانداردهای سری ISO 27000، ISO 31000 و چارچوب‌های COSO، Risk IT و Val IT نیز سازگار است.
ابزارهای پشتیبان	ابزار COBIT از این روش پشتیبانی می‌کند.
مزایا/ نقاط قوت	+ کار بر روی سطحی بالا از حاکمیت فناوری اطلاعات و طراحی برای مدیریت مخاطره؛ + صرف‌نظر از اندازه، صنعت و ماهیت برای کلیه سازمان‌ها قابل استفاده است؛ + بهره‌برداری از این چارچوب، توانمندی‌های مربوط به مخاطره سازمانی را افزایش می‌دهد؛ + ۲۰ دسته سناریوی مخاطره برای کمک به سازمان‌ها برای کاهش بهتر مخاطره فراهم می‌کند؛ + برخلاف استانداردها و چارچوب‌های دیگر، سناریوهای این چارچوب بیش از ۱۰۰ نوع مخاطره را پوشش می‌دهد، مانند سرقت و خرابکاری کارمندان، نقض داده‌ها، جاسوسی صنعتی و پشتیبانی از نوآوری؛ + چارچوبی جامع برای کنترل و مدیریت راهکارها و خدمات مبتنی بر فناوری اطلاعات کسب‌وکار؛ + با ارائه مجموعه‌ای از کنترل‌ها جهت کاهش مخاطره فناوری اطلاعات، روش‌های مناسبی را برای ابزارهای مدیریت مخاطره تعیین می‌کند؛ + کلیه فعالیت‌های مربوط به فناوری اطلاعات را در سازمان مدیریت می‌کند؛
معایب/ نقاط ضعف	- ضعف در هر یک از توانمندسازها در سازمان، باعث عدم قطعیت در تحقق اهداف سازمانی و به نعبیری مخاطره سازمانی می‌شود؛ - جهت درک چارچوب، مهارت و دانش زیادی لازم است؛ - پیچیدگی چارچوب؛ - بسیار پر هزینه است و مقرون‌به‌صرفه نیست؛
وب‌سایت‌رسمی	https://www.isaca.org/resources/cobit

۳-۲-۲-۴-۲. چارچوب Risk IT

چارچوب «مخاطره فناوری اطلاعات» یا به اختصار (Risk IT) در سال (۲۰۰۹) میلادی توسط انجمن نظارت و کنترل سیستم‌های اطلاعاتی بر پایه اصول استانداردها/ چارچوب‌های مدیریت مخاطره سازمان مانند «COSO» و AS/NZS 4360 و با هدف مقابله با انواع گوناگونی از مخاطره‌های مرتبط با فناوری اطلاعات -عمدتاً مخاطره‌های مربوط به امنیت- بنا شده است و نگرشی را بر مبنای چگونگی به‌کارگیری رهنمودها در فناوری اطلاعات مطرح می‌کند. چارچوب «Risk IT» در واقع، بخشی از مخاطره کسب‌وکار محسوب می‌شود که با بهره‌برداری از مالکیت، بهره‌برداری، مشارکت، نفوذ و پذیرش فناوری اطلاعات در یک سازمان - شامل رویدادهای مرتبط با فناوری اطلاعات- در ارتباط است و می‌تواند به طور بالقوه بر روی کسب‌وکار تأثیرگذار باشد. مدیریت مخاطره کسب‌وکار یکی از مؤلفه‌های اساسی در هر سازمان محسوب می‌شود. از این‌رو با توجه به اهمیت و ضرورت فناوری اطلاعات در تمامی کسب‌وکارها، باید با چارچوب «Risk IT» مانند دیگر مخاطره‌های کسب‌وکار رفتار شود. چارچوب «Risk IT» مخاطره‌های فناوری اطلاعات را تشریح می‌کند و کاربران را قادر می‌سازد:

- مدیریت مخاطره فناوری اطلاعات را با برنامه‌ریزی منابع سازمانی ادغام کنند؛
- مخاطره ارزیابی شده فناوری اطلاعات را با اشتهای مخاطره و تحمل مخاطره سازمان مقایسه کنند؛
- شیوهٔ مدیریت مخاطره را درک کنند.

چارچوب «Risk IT» باید توسط کلیه رهبران اصلی کسب‌وکار در داخل سازمان مدیریت می‌شود؛ و این فقط یک مسئله فنی مربوط به بخش فناوری اطلاعات نیست. چارچوب «Risk IT» را می‌توان به روش‌های گوناگونی دسته‌بندی کرد:

- توانمندساز ارزش/ سود فناوری اطلاعات: مخاطره‌های مربوط به فرصت‌های ازدست‌رفته جهت افزایش ارزش کسب‌وکار توسط فرآیندهای بهبودیافته یا توانمندشده فناوری اطلاعات؛
- تحویل پروژه/ برنامه فناوری اطلاعات: مخاطره‌های مربوط به مدیریت پروژه‌های فناوری اطلاعات‌محور جهت ایجاد یا بهبود کسب‌وکار؛ برای مثال مخاطره بیش از حد بودجه یا تحویل با تأخیر (یا اصلاً تحویل ندادن) این پروژه‌ها؛
- ارائه خدمات و عملیات فناوری اطلاعات: مخاطره‌های مربوط به عملیات روزمره و ارائه خدمات فناوری اطلاعات که می‌تواند مسائلی را به همراه داشته باشد، ناکارآمدی در عملیات کسب‌وکار یک سازمان.

چارچوب «Risk IT» بر پایهٔ اصول زیر تدوین شده است:

- همراستایی همیشگی با اهداف کسب‌وکار؛
- همراستایی مدیریت مخاطره فناوری اطلاعات با برنامه‌ریزی منابع سازمانی؛
- متعادل‌سازی هزینه‌ها و مزایای مدیریت مخاطره فناوری اطلاعات؛
- ارتقاء ارتباطات آزاد و منصفانه مخاطره‌های فناوری اطلاعات؛
- اولویت قراردادن و بهره‌مندی از لحن مناسب هنگام تعریف و تفویض مسئولیت‌ها؛ و
- یک فرآیند مداوم و مستمر و بخشی از فعالیت‌های روزمره.

در ادامه، به سه حوزه اصلی چارچوب «Risk IT» همراه با فرآیندهای موجود در هر دامنه در قالب (**شکل ۳-۲۲**) اشاره شده است.

شکل ۳-۲۲. مدل فرآیند Risk IT، (ISACA 2009)

هر فرآیند شامل تعدادی فعالیت به شرح ذیل است:

- **دامنه – حاکمیت مخاطره:** اطمینان حاصل کنید که شیوه‌های مدیریت «Risk IT» در سازمان تعبیه شده است و آن را توانمند می‌سازد تا بازدهی بهینه با مخاطره را تأمین کند. این دامنه بر پایهٔ فرآیندهای زیر است:
  - **ایجاد و حفظ یک دیدگاه مشترک/ رایج از مخاطره:** اطمینان حاصل کنید که فعالیت‌های مدیریت مخاطره با ظرفیت اهداف سازمان همراستا است.
    - انجام ارزیابی مخاطره فناوری اطلاعات سازمان؛
    - بیان آستانه تحمل مخاطره فناوری اطلاعات؛
    - تأیید تحمل مخاطره فناوری اطلاعات؛
    - همراستایی خط‌مشی مخاطره فناوری اطلاعات؛
    - ارتقاء فرهنگ آگاهی مخاطره فناوری اطلاعات؛ و
    - ترغیب و تشویق ارتباطات مؤثر در مخاطره فناوری اطلاعات.
  - **ادغام با برنامه‌ریزی منابع سازمانی:** عملیات و راهبرد «Risk IT» را با تصمیم‌های راهبردی مخاطره کسب‌وکار که در سطح سازمان اتخاذ شده، ادغام کنید.
    - تعیین و حفظ مسئولیت/ پاسخگویی برای مدیریت مخاطره فناوری اطلاعات؛
    - هماهنگی راهبرد مخاطره کسب‌وکار و راهبرد مخاطره فناوری اطلاعات؛
    - تطبیق روش‌های مخاطره فناوری اطلاعات با روش‌های مخاطره سازمانی؛
    - ارائه منابع کافی برای مدیریت مخاطره فناوری اطلاعات؛ و
    - ارائه اطمینان کافی از مدیریت مخاطره فناوری اطلاعات.
  - **اتخاذ تصمیم‌های کسب‌وکار آگاه از مخاطره:** اطمینان حاصل کنید که تصمیم‌های سازمان طیف وسیعی از فرصت‌ها و پیامدهای ناشی از اتکا به فناوری اطلاعات را برای دستیابی به موفقیت در نظر می‌گیرند.
    - دستیابی مدیریت جهت رویکرد تحلیل مخاطره فناوری اطلاعات؛
    - تأیید تحلیل مخاطره فناوری اطلاعات؛
    - تعبیه مفروضات مخاطره فناوری اطلاعات در تصمیم‌گیری‌های راهبردی کسب‌وکار؛
    - پذیرش مخاطره فناوری اطلاعات؛ و
    - اولویت‌بندی فعالیت‌های پاسخگویی به مخاطره فناوری اطلاعات.
- **دامنه – سنجش مخاطره:** اطمینان حاصل کنید که فرصت‌ها و مخاطره‌های مرتبط با فناوری اطلاعات شناسایی و تحلیل شده و بر پایهٔ اصطلاح‌های کسب‌وکار ارائه می‌شوند. این دامنه بر پایهٔ فرآیندهای زیر است:
  - **جمع‌آوری داده:** داده‌های مربوطه را شناسایی کنید تا فرآیند شناسایی، تحلیل و گزارش‌دهی مخاطره مربوط به فناوری اطلاعات به شکل مؤثری شکل گیرد.
    - ساخت و نگهداری مدلی برای جمع‌آوری داده‌ها؛
    - جمع‌آوری داده‌های مربوط به محیط عملیاتی؛
    - جمع‌آوری داده‌ها مربوط به رویدادهای مخاطره؛ و
    - شناسایی عامل‌ها/ فاکتورهای مخاطره.
  - **تحلیل مخاطره:** برای پشتیبانی از تصمیم‌های مخاطره، اطلاعات مفیدی از عامل‌های مخاطره مربوط به کسب‌وکار تهیه کنید.
    - تعیین محدوده تحلیل مخاطره فناوری اطلاعات؛

- تخمین مخاطره فناوری اطلاعات؛
- شناسایی گزینه‌های پاسخگویی به مخاطره؛ و
- انجام یک بررسی دقیق از تحلیل مخاطره فناوری اطلاعات.

○ **حفظ و نگهداری پروفایل مخاطره:** یک موجودی به‌روز و کامل از مخاطره‌ها و ویژگی‌های شناخته شده (برای مثال تواتر موردانتظار، پیامد بالقوه، وضع موجود)، منابع فناوری اطلاعات، توانایی‌ها و کنترل‌ها نگه دارید. همان‌طور که در زمینه فرآیندها، خدمات و محصولات کسب‌وکار قابل درک است.

- نگاشت منابع فناوری اطلاعات به فرآیندهای کسب‌وکار؛
- تعیین اهمیت و ضرورت کسب‌وکار از منابع فناوری اطلاعات؛
- درک قابلیت‌ها/ توانایی‌های فناوری اطلاعات؛
- به‌روزرسانی مؤلفه‌های سناریو مخاطره؛
- حفظ و نگهداری نقشه و ثبت مخاطره فناوری اطلاعات؛ و
- توسعه شاخص‌های مخاطره فناوری اطلاعات.

– **دامنه – پاسخ به مخاطره:** اطمینان حاصل کنید که مسائل، فرصت‌ها و رویدادهای مربوط به «Risk IT» به روش مقرون‌به‌صرفه و سازگار با اولویت‌های کسب‌وکار پاسخ داده شده‌اند. این دامنه بر پایهٔ فرآیندهای زیر است:

○ **بیان مخاطره:** اطمینان حاصل کنید که اطلاعات مربوط به فرصت‌ها و راه‌های مواجهه مرتبط با فناوری اطلاعات به موقع و در دسترس افراد مناسب جهت پاسخگویی قرار گرفته است.

- ارتباط نتایج تحلیل مخاطره فناوری اطلاعات؛
- گزارش فعالیت‌های مدیریت مخاطره فناوری اطلاعات و وضعیت انطباق؛
- تفسیر مستقل یافته‌های ارزیابی فناوری اطلاعات؛ و
- شناسایی فرصت‌های مربوط به فناوری اطلاعات.

○ **مدیریت مخاطره:** اطمینان حاصل کنید که جهت دستیابی به فرصت‌های راهبردی و کاهش مخاطره تا یک سطح قابل قبول، اقدام‌ها به عنوان یک پروتفولیو مدیریت می‌شوند.

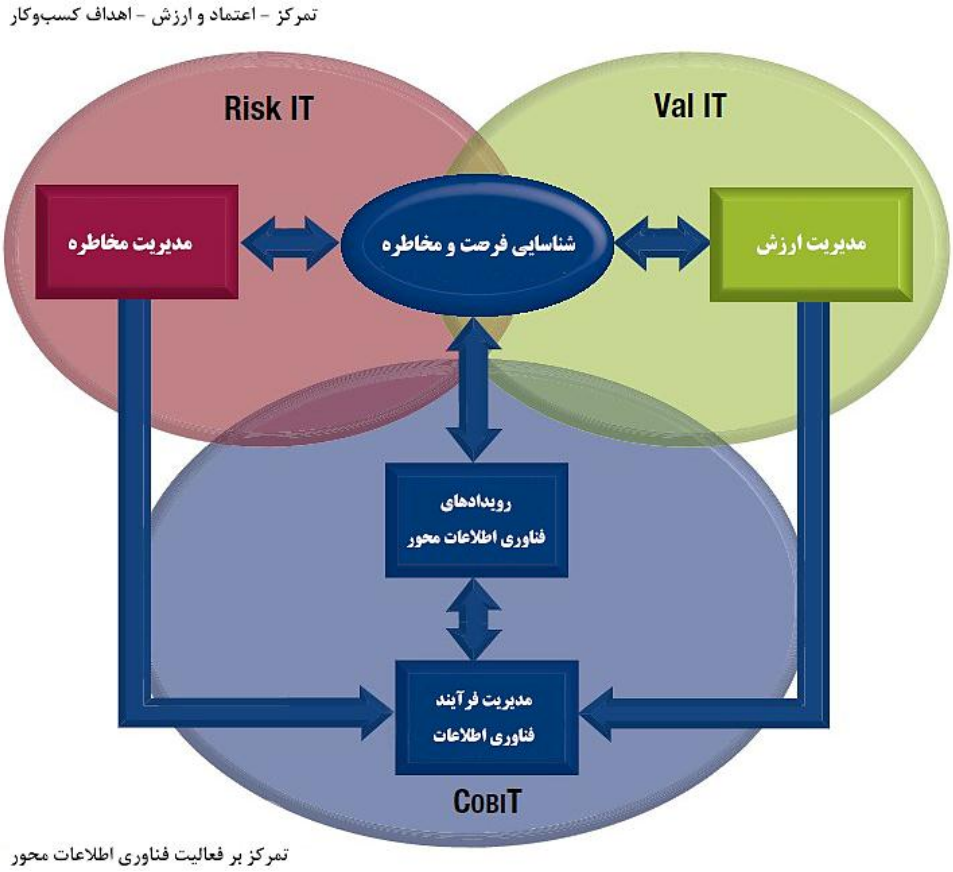
- کنترل‌های موجودی؛
- پایش همراستایی عملیاتی با آستانه تحمل مخاطره؛
- پاسخ به فرصت و مواجهه با مخاطره کشف شده؛
- اجرای کنترل‌ها؛ و
- گزارش پیشرفت برنامه عملیاتی مخاطره فناوری اطلاعات.

○ **واکنش به رویدادها:** اطمینان حاصل کنید که جهت بهره‌برداری از فرصت‌های لحظه‌ای یا محدودکردن میزان ضرر و زیان ناشی از رویدادهای مربوط به فناوری اطلاعات، اقدام‌ها به موقع فعال شده و مؤثر واقع شوند.

- حفظ و نگهداری برنامه‌های پاسخ به حادثه؛
- پایش مخاطره فناوری اطلاعات؛
- آغاز پاسخ/ واکنش به حادثه؛ و
- ارتباط درس‌های آموخته شده از رویدادهای مخاطره.

چارچوب «Risk IT» مکمل چارچوب COBIT است که چارچوبی جامع برای کنترل و مدیریت راهکارها و خدمات مبتنی بر فناوری اطلاعات کسب‌وکار ارائه می‌کند. چارچوب «Risk IT» با فراهم آوردن چارچوبی برای سازمان‌ها جهت شناسایی، کنترل و مدیریت مخاطره فناوری اطلاعات، اقدام‌های مناسبی را برای اهداف تعیین می‌کند. در حالی که COBIT با ارائه مجموعه‌ای از

کنترل‌ها جهت کاهش مخاطره فناوری اطلاعات، روش‌های مناسبی را برای ابزارهای مدیریت مخاطره تعیین می‌کند. چارچوب «ارزش فناوری اطلاعات» یا به اختصار (Val IT)، به مدیران کسب‌وکار این امکان را می‌دهد تا با ارائه یک چارچوب حاکمیتی، ارزش کسب‌وکار خود را از طریق سرمایه‌گذاری‌های فناوری اطلاعات بدست آورند. می‌توان از چارچوب «Val IT» جهت سنجش واکنش‌های تعیین شده توسط فرآیند مدیریت مخاطره استفاده کرد. سند چارچوب «Risk IT» بیان می‌کند که اگرچه Risk IT یک چارچوب مستقل برای مدیریت مخاطره است، اما می‌تواند همراه با «چارچوب COBIT» و چارچوب «Val IT» نیز مورد استفاده قرار گیرد. (**شکل ۳-۲۳**) شیوهٔ ارتباط این سه چارچوب با یک‌دیگر را در زمینه حاکمیت فناوری اطلاعات نشان می‌دهد. فرآیندهای COBIT کلیه فعالیت‌های مربوط به فناوری اطلاعات را در سازمان مدیریت می‌کند. این فرآیندها با رویدادهای داخلی یا خارجی سازمانی سروکار دارند. رویدادهای داخلی می‌توانند شامل حوادث عملیاتی فناوری اطلاعات، شکست‌های پروژه، سوئیچ‌های کامل راهبرد (فناوری اطلاعات) و ادغام‌ها باشند. رویدادهای خارجی می‌توانند شامل تغییرات در شرایط بازار، رقبای جدید، در دسترس بودن فناوری جدید و قوانین و مقررات مؤثر بر فناوری اطلاعات باشند.



شکل ۳-۲۳. موقعیت قرارگیری چارچوب COBIT، Val IT و Risk IT نسبت به یک‌دیگر، (ISACA 2009)

این رویدادها در معرض مخاطره‌ها و یا فرصت‌هایی جای دارند که نیازمند ارزیابی و پاسخگویی هستند. ابعاد مخاطره و شیوهٔ مدیریت آن موضوع اصلی چارچوب «Risk IT» است. زمانی که فرصت‌های تغییر فناوری اطلاعات کسب‌وکار شناسایی می‌شوند، چارچوب «Val IT» به بهترین شکل شیوهٔ پیشرفت و به حداکثر رساندن بازده سرمایه‌گذاری را توصیف می‌کند. نتیجه ارزیابی به احتمال زیاد در برخی از فرآیندهای فناوری اطلاعات و یا بر ورودی فرآیندهای فناوری اطلاعات تأثیر خواهد داشت. از این‌رو، پیکان‌ها از "مدیریت مخاطره" و "مدیریت ارزش" به حوزه "مدیریت فرآیند فناوری اطلاعات" متصل می‌شوند.

در واقع، چارچوب «Risk IT» با هدف پرکردن شکاف بین چارچوب‌های مدیریت مخاطره سطح بالا (مانند ISO 31000، AS/NZS 4360) و چارچوب‌های حوزه خاص (در ارتباط با امنیت یا مدیریت پروژه) معرفی شده است.

جدول ۳-۱۴. شناسنامه (۱۰): چارچوب Risk IT

شناسنامه چارچوب Risk IT		
نام اختصاری	چارچوب مخاطره فناوری اطلاعات – Risk IT	
نام کامل	چارچوب مخاطره فناوری اطلاعات	Risk IT
ارائه‌دهنده	انجمن نظارت و کنترل سیستم‌های اطلاعاتی (ایساکا)	
کشور ارائه‌دهنده	ایالات متحده	
وضعیت نسخه	نخستین نسخه این چارچوب در سال ۲۰۰۹ میلادی منتشر شد و در حال حاضر نسخه ۲۰۲۰ به عنوان آخرین نسخه معتبر محسوب می‌شود.	
زبان	انگلیسی	
قیمت	به صورت رایگان برای اعضاء در دسترس است.	
دامنه کاربرد/ استفاده	آدرس‌دهی انواع گوناگون مخاطره‌های مرتبط با فناوری اطلاعات، به ویژه مخاطرات مربوط به امنیت.	
هدف	برای پرکردن شکاف بین چارچوب‌های مدیریت مخاطره سطح بالا (مانند ISO 31000، AS/NZS 4360) و چارچوب‌های حوزه خاص (در ارتباط با امنیت یا مدیریت پروژه) معرفی شده است. در واقع، این چارچوب با هدف مقابله با انواع گوناگونی از مخاطره‌های مرتبط با فناوری اطلاعات -عمدتاً مخاطره‌های مربوط به امنیت- بنا شده است و نگرشی را بر مبنای چگونگی به‌کارگیری رهنمودها در فناوری اطلاعات مطرح می‌کند.	
مراحل مدیریت مخاطره	بخش اول) دامنه حاکمیت مخاطره - ایجاد و حفظ یک دیدگاه مشترک/ رایج از مخاطره - ادغام با برنامه‌ریزی منابع سازمانی - اتخاذ تصمیم‌های کسب‌وکار آگاه از مخاطره بخش دوم) دامنه سنجش مخاطره - جمع‌آوری داده	- تحلیل مخاطره - حفظ و نگهداری پروفایل مخاطره بخش سوم) پاسخ به مخاطره - بیان مخاطره - مدیریت مخاطره – واکنش به رویدادها
فرمول محاسبه مخاطره	مخاطره (تهدید، دارایی) = احتمال (تهدید) × آسیب‌پذیری (تهدید، دارایی) × پیامد (تهدید، دارایی)	
سازگاری با استانداردها	این چارچوب با استانداردهای سری ISO 27000، ISO 31000 و چارچوب‌های COSO، Val IT و COBIT-5 نیز سازگار است.	
ابزارهای پشتیبان	ابزار مدل‌سازی بلوغ جهت ارزیابی سطح بلوغ سازمان، ابزارهای گردش کار جهت افزایش مسائل مخاطره و پیگیری تصمیم‌ها، ابزارهای نقشه و ثبت مخاطره، ابزار گرافیکی جهت رتبه‌بندی و نمایش مخاطره‌ها	
مزایا/ نقاط قوت	+ از طیف گسترده‌ای از اسناد مربوط به فناوری اطلاعات و مدیریت مخاطره پشتیبانی می‌کند؛ + بر پایه چارچوب شناخته‌شده جهانی COBIT جهت حاکمیت فناوری اطلاعات استوار است. + امکان ادغام آسان یا روش‌های مدیریت مخاطره در سراسر سازمان را فراهم می‌کند؛ + صرف‌نظر از اندازه، صنعت و ماهیت برای کلیه سازمان‌ها قابل استفاده است؛ + مکمل چارچوب COBIT است؛ + ارائه چارچوبی برای سازمان‌ها جهت شناسایی، کنترل و مدیریت مخاطره فناوری اطلاعات؛ + می‌تواند همراه با چارچوب COBIT و چارچوب VaL IT مورد استفاده قرار گیرد؛ + یک زبان مشترک جهت کمک به برقراری ارتباط بین فناوری اطلاعات کسب‌وکار، مخاطره و مدیریت ممیزی؛ + راهنمای نظیربه‌نظیر در ارتباط با شیوهٔ مدیریت مخاطره‌های مربوط به فناوری اطلاعات؛ + یک پروفایل کامل از مخاطره جهت درک بهتر مخاطره به منظور استفاده بهتر از منابع سازمانی؛ + درک بهتری از نقش‌ها و مسئولیت‌ها در ارتباط با مدیریت مخاطره فناوری اطلاعات؛ + همراستا با برنامه‌ریزی منابع سازمانی؛ + ارائه یک دیدگاه بهتر از مخاطره مرتبط با فناوری اطلاعات و پیامدهای مالی آن؛ + شکست‌ها و رویدادهای غیرمنتظره عملیاتی کمتر؛ + افزایش کیفیت اطلاعات؛ + افزایش اعتماد و اطمینان ذینفعان و کاهش نگرانی‌های نظارتی؛	
معایب/ نقاط ضعف	- ارزیابی مخاطره را با جزئیات فنی تشریح نمی‌کند و فقط راهنمایی در ارتباط با چگونگی استفاده و ادغام آن با فرآیندهای مدیریت مخاطره در سطح سازمانی ارائه می‌دهد؛ - ارزیابی مخاطره نمی‌تواند مستقل از بقیه چارچوب استفاده شود. - با توجه به توسعه اخیر چارچوب، دستیابی به مزایای این چارچوب برای طولانی مدت امکان‌پذیر نیست؛ - با توجه به قابلیت انعطاف‌پذیری این چارچوب، اجرای نادرست آن ممکن است مزایایی به همراه نداشته باشد و مخاطره‌های ناشناخته و شناسایی نشده در سازمان فناوری اطلاعات را با خود به همراه داشته باشد؛ - با توجه به اینکه این چارچوب بر پایهٔ به‌روش‌ها بنا شده است، ممکن از مقبولیت و استقبال گسترده‌ای برخوردار نباشد؛ - این چارچوب به اجرای مناسب COBIT و Val IT وابسته است -که ممکن است در همه سازمان‌ها وجود نداشته باشد- بنابراین ممکن است مانعی برای پذیرش آن در بسیاری از سازمان‌ها باشد؛ - علی‌رغم بهره‌برداری از کنترل‌های موجود فناوری اطلاعات، ماهیت جامع این چارچوب می‌تواند به سرعت هزینه‌های بالای مدیریت مخاطره فناوری اطلاعات را به همراه داشته باشد؛	
وب‌سایت‌رسمی	https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2	

۳-۲-۳. روش‌های مدیریت و ارزیابی مخاطره امنیت اطلاعات

گاهی سازمان‌ها از روش‌های ساخت‌یافته‌ای جهت ارزیابی و مدیریت مخاطرات استفاده می‌کنند. با توجه به اینکه چارچوب‌ها، رویکردها و روش‌های گوناگونی برای شناسایی و ارزیابی میزان مخاطره در سازمان وجود دارد. انتخاب روش ارزیابی مخاطره در سازمان به **ریزدانگی**[1] و عمق تحلیل مخاطره وابسته است. روش‌های گوناگون ارزیابی و مدیریت مخاطرات امنیت اطلاعات شامل مجموعه‌ای از روش‌ها، رویه‌ها و فنون عملیاتی یکپارچه می‌باشند که برای پشتیبانی از فرآیند مدیریت مخاطرات در سازمان طرح‌ریزی شده‌اند. غالب این روش‌ها بر مبنای استانداردها و به‌روش‌ها و نیز رویکردهای گوناگون امنیتی و مدیریتی حاکم بر سازمان‌های گوناگون توسعه داده شده‌اند. در حالت کلی این روش‌ها بسیار شبیه به هم عمل می‌کنند. بنابراین هیچ روش برتری وجود ندارد و انتخاب روش کاملاً به خود سازمان و ویژگی‌های گوناگون ارزیابی بستگی دارد. بیشتر روش‌ها، ارائه‌گر یک رتبه‌بندی عددی ساده برای درجه‌بندی مخاطرهای امنیتی هستند. خروجی این معیارها کمک شایانی به مدیران در راستای تخصیص بودجه، مدیریت مخاطره و مقابله با مخاطره‌ها می‌کند (Brotby and Hinson 2013). اکثر روش‌های ارائه شده در زمینه مدیریت امنیت اطلاعات به صورت عام و ارزیابی و مدیریت مخاطرات به صورت خاص، از یک چرخه «پی.دی.سی.ای.» برخوردار بوده و روش نظامند معینی را برای ارزیابی و مدیریت مخاطرات عرضه می‌نمایند. بدیهی است که روش‌های گوناگونی در این زمینه تدوین و منتشر شده است با این وجود در این بخش بر روی روش‌هایی متمرکز خواهیم شد که هرکدام از آنها دارای یک رویه و فناوری مشخصی در شناسایی، اندازه‌گیری، کنترل و پایش مخاطرات می‌باشند. با توجه به اینکه، هر روش رویکرد متفاوتی را برای جمع‌آوری اطلاعات پیرامون مخاطرات ارائه داده و معیارهای متفاوتی را برای تحلیل و ارزیابی به خدمت می‌گیرد، در ادامه روش‌های نوین ارزیابی مخاطره شناسایی و مورد تحلیل و بررسی قرار خواهد گرفت.

۳-۲-۳-۱. روش CORAS

سیستم تحلیل مخاطره عینی-مشاوره‌ای[2] یا به اختصار «CORAS» یک رویکرد مدل‌محور برای تحلیل مخاطره امنیتی است که مبتنی بر استاندارد مدیریت مخاطره «ISO 31000» ارائه شده است. این روش بر پایهٔ پژوهش‌های تجربی و یک سری مطالعات صورت گرفته در حوزه صنعت -پروژه‌هایی که توسط شورای تحقیقاتی نروژ و اتحادیه اروپا تأمین مالی می‌شوند- توسعه یافته است. «CORAS» یک زبان سفارشی برای مدل‌سازی مخاطره و تهدید ارائه می‌دهد، و دارای دستورالعمل‌ها و رهنمودهای دقیقی است که بیان می‌کند که چگونه باید این زبان جهت ضبط و مدل‌سازی اطلاعات مربوطه در طول مراحل گوناگون تحلیل امنیتی مورد استفاده قرار گیرد.

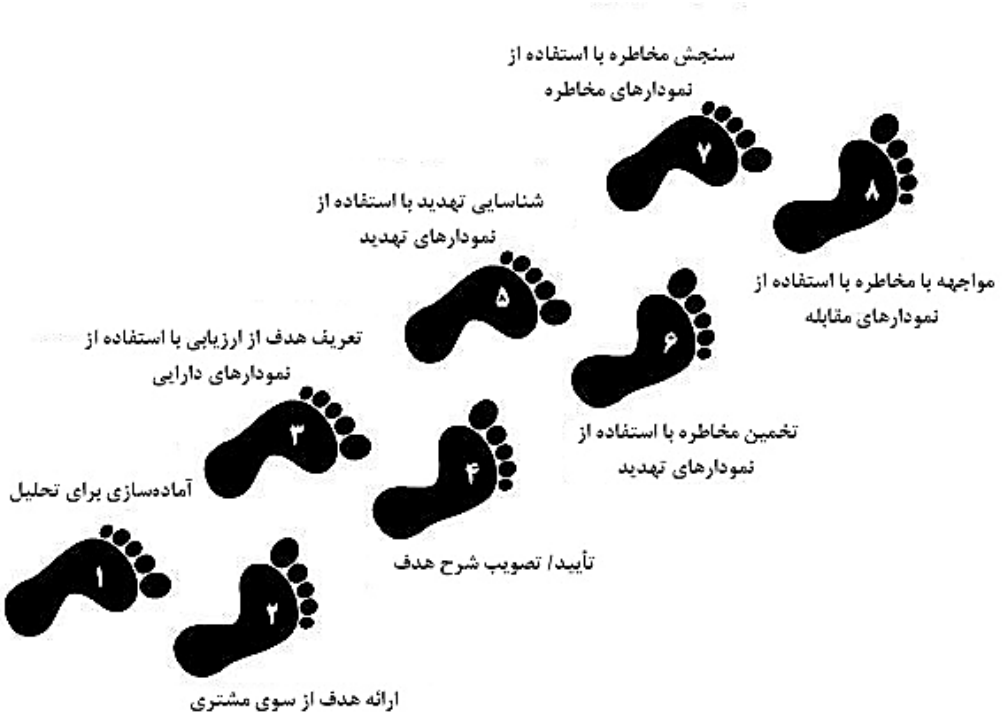
این روش از سه بخش ۱) روش CORAS (دارایی‌محور است، بدین معنا که دارایی‌هایی که در معرض ارزیابی مخاطره قرار دارند در مراحل اولیه فرآیند شناسایی و ثبت می‌شوند)، ۲) زبان CORAS (یک نماد گرافیکی با انواع گوناگونی از نمودارها است که در طول فرآیند -از شروع تا انتها- مورد استفاده قرار می‌گیرد) و ۳) ابزار CORAS (یک ویرایشگر نمودار است که انواع گوناگون نمودارها را ایجاد می‌کند) تشکیل شده است. در واقع، این روش یک بستر یکپارچه برای ارزیابی مخاطره است که برای ایجاد مدل‌های مخاطره اطلاعات از زبان UML پشتیبانی می‌کند. زبان مدل‌سازی یکپارچه به طور معمول برای مدل‌سازی هدف تجزیه و تحلیل مورد استفاده قرار می‌گیرد. برای مستندسازی نتایج میانی و ارائه نتایج کلی از نمودارهای مخصوص «CORAS» -که الهام گرفته از زبان UML است- استفاده می‌شود. روش «CORAS» یک ابزار رایانه‌ای در اختیار قرار می‌دهد که به منظور پشتیبانی از فرآیند مستندسازی، حفظ و نگهداری و گزارش نتایج تحلیل از طریق مدل‌سازی مخاطره طراحی شده است. «CORAS» بر فنون سنتی تحلیل امنیت مانند فن طوفان مغزی ساختاریافته «Hazop»، «FTA»، «FMECA»، «Markov» و «CRAMM» استوار است.

---

[1] Granularity

[2] Consultative Objective Risk Analysis System (CORAS)

این روش به استاندارد «ISO 31000» بسیار نزدیک و شبیه است و از استانداردهای بین‌المللی ازجمله AS/NZS 4360:1999 و ISO/IEC 17799-1:2000 پیروی می‌کند. (**شکل ۳-۲۴**) گام‌های هشت‌گانه تحلیل مخاطره امنیتی در روش «CORAS» را به تصویر کشیده است.



شکل ۳-۲۴. گام‌های هشت‌گانه روش ارزیابی مخاطره CORAS، (Sourceforge 2015)

در ادامه هر یک از این گام‌های هشت‌گانه به تفکیک مورد بررسی قرار خواهد گرفت:

۱. **گام نخست – آماده‌سازی اولیه برای تحلیل مخاطره**: هدف اصلی دستیابی به یک ایده اولیه در ارتباط با هدف و عمق تجزیه و تحلیل است به گونه‌ای که بتوان مقدمات لازم برای انجام واقعی کارهای تحلیل را فراهم کرد.

۲. **گام دوم – جلسه معارفه با مشتری:** موضوع اصلی جلسه ارائه اهداف کلی از فرآیند تحلیل از سوی نمایندگان مشتری است. هدف دستیابی به یک درک مشترک از اهداف تحلیل و آنچه که طرفین تحلیل بیشتر از همه نگران آن هستند. در این گام، اهداف کلی تحلیل بیان می‌گردد، میزان تمرکز و دامنه/ محدوده تحلیل تعیین می‌شود و مابقی فرآیند تحلیل برنامه‌ریزی می‌شود.

۳. **گام سوم – اطمینان از دستیابی به یک درک مشترک از اهداف تحلیل (ازجمله تمرکز، محدوده و دارایی‌های اصلی):** تیم تحلیلگر درک خود را از آنچه که در نخستین جلسه‌ای که با مشتری داشتند و از مطالعه مستنداتی که از سوی مشتری در اختیار و دسترس آنها قرار گرفته است، بیان می‌کنند. تیم تحلیگر بر پایهٔ داشتن تعامل با مشتری، دارایی‌های اصلی که باید حفظ و نگهداری شوند، شناسایی می‌کند. افزون بر این، تیم تحلیلگر به منظور شناسایی سناریوهای اصلی تهدید، آسیب‌پذیری‌ها و مخاطره‌های سطح سازمانی که باید مورد بررسی بیشتر قرار گیرند، یک تحلیل سطح بالا انجام می‌دهد. خروجی این گام دستیابی به یک درک صحیح و دقیق از توصیف هدف و اهداف تحلیل است که تا به اینجا توسط تحلیلگران مستند شده است.

۴. **گام چهارم – اطمینان از صحت و کامل بودن مستندات پس‌زمینه برای مابقی فرآیند تحلیل (ازجمله، هدف، تمرکز و محدوده) همان‌گونه که در نگاه مشتری دیده می‌شود:** این گام شامل ارائه توضیحات دقیق‌تر از هدف تحلیل از جمله پیش‌فرض‌ها و پیش‌شرط‌های مطرح شده است. به طور معمول، تحلیلگران با بهره‌برداری از یک نشان/ نماد رسمی یا نیمه‌رسمی -مانند زبان UML- هدف را تشریح می‌کنند. پیش از شروع تحلیل واقعی مخاطره در گام بعدی از فرآیند تحلیل، شرح هدف باید از سوی مشتری مورد تأیید قرار بگیرد. افزون بر این،، گام چهارم شامل تصمیم‌گیری در ارتباط با معیارهای سنجش مخاطره برای هر دارایی است. این گام از تحلیل شامل ایجاد/ استقرار زمینه است.

۵. **گام پنجم – شناسایی مخاطره با بهره‌برداری از نمودارهای تهدید**: برای شناسایی مخاطره‌ها، «CORAS» از طوفان فکری ساختاریافته استفاده می‌کند. طوفان فکری ساختاریافته یک فرآیند گام‌به‌گام دستیابی به اهداف تحلیل است و به عنوان یک کارگاه آموزشی با راهبری و هدایت تحلیلگران برگزار می‌شود. ایده اصلی طوفان فکری ساختاریافته این است که از آنجا که شرکت‌کنندگان در کارگاه آموزشی از شایستگی‌ها/ مهارت‌ها، زمینه‌ها و علائق گوناگونی برخوردار هستند، از دیدگاه‌ها/ چشم‌اندازهای گوناگونی هدف را مشاهده می‌کنند و در نتیجه مخاطره‌های بیشتری را شناسایی کرده و نسبت به افراد یا یک گروه همگن مدیریت خواهند کرد. شناسایی مخاطره شامل شناسایی نظام‌مند تهدیدها، حوادث ناخواسته، سناریوهای تهدید و آسیب‌پذیری‌های مرتبط با دارایی‌های شناسایی شده است. فعالیت‌ها توسط زبان «CORAS» پشتیبانی می‌شوند و نتایج با بهره‌برداری از نمودارهای تهدید «CORAS» مستند می‌شوند.

۶. **گام ششم – تخمین سطح مخاطره با بهره‌برداری از نمودارهای تهدید**: هدف این گام تعیین سطح مخاطره از مخاطره‌های نشأت گرفته از حوادث ناخواسته شناسایی شده است. در طول گام پنجم، حوادث ناخواسته در قالب نمودارهای تهدید مستند می‌شوند و این نمودارها به عنوان مبنایی برای تخمین مخاطره عمل می‌کنند. این گام به عنوان یک طوفان فکری متشکل از کارکنانی با پس‌زمینه‌های گوناگون برگزار می‌شود، و به طور اساسی شامل تخمین احتمالات و پیامدهای حوادث ناخواسته است. این ارزش‌ها/ مقادیر به صورت ترکیبی سطح مخاطره را برای هر یک از مخاطره‌های شناسایی شده به همراه دارند. نمودارهای تهدید «CORAS» با پشتیبانی از تخمین احتمال تهدیدها و سناریوهای تهدید که موجب حوادث ناخواسته می‌شوند، احتمال تخمین را تسهیل می‌کنند.

۷. **گام هفتم – سنجش مخاطره با بهره‌برداری از نمودارهای مخاطره**: این مرحله، در ارتباط با اینکه کدامیک از مخاطره‌های شناسایی شده قابل قبول، و کدامیک از مخاطره‌ها باید برای برخورد احتمالی بیشتر مورد سنجش قرار گیرند، تصمیم‌گیری می‌کند. قابل قبول بودن یا نبودن مخاطره‌ها با بهره‌برداری از معیارهای سنجش مخاطره که پیش‌تر تعریف شده و نتایج تخمین مخاطره تعیین می‌شود. افزون بر این، این گام شامل تخمین و سنجش مخاطره‌ها با توجه به دارایی‌های غیرمستقیم است.

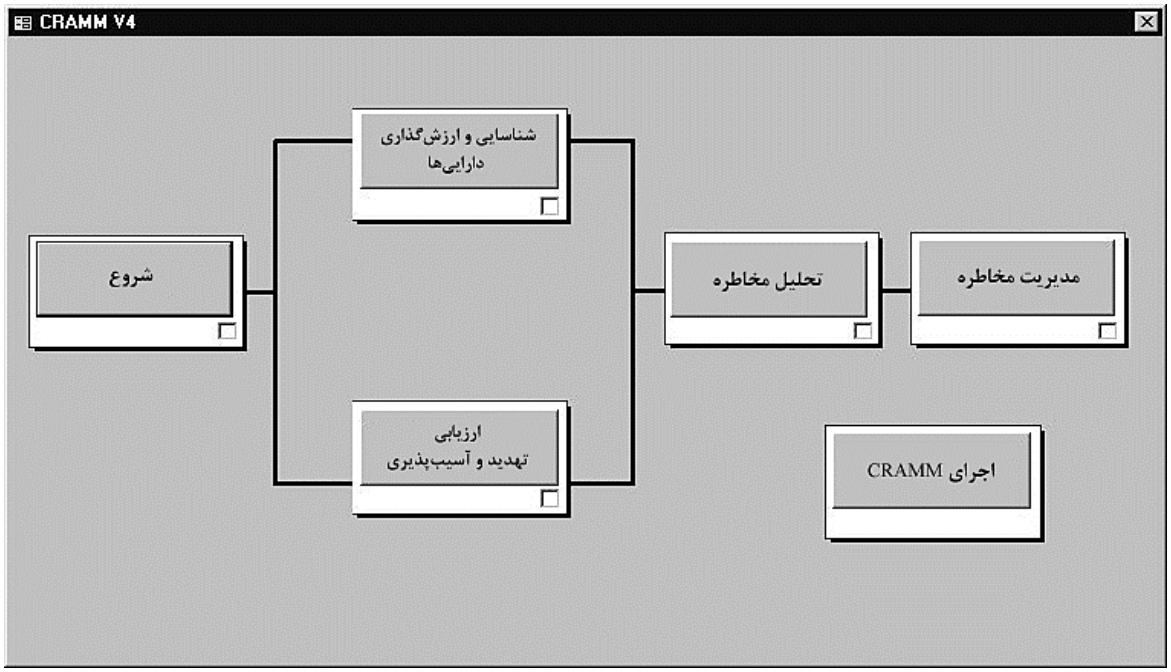
۸. **گام هشتم – مواجهه با مخاطره با بهره‌برداری از نمودارهای مقابله**: این گام مربوط به شناسایی و تحلیل راهکارهای مواجهه است. مخاطره‌هایی که غیرقابل قبول شناخته می‌شوند، برای اینکه راهی برای کاهش آنها پیدا شود، مورد سنجش قرار می‌گیرند. راه مواجهه باید به کاهش احتمال و یا نتیجه یک حادثه ناخواسته کمک کند. با توجه به اینکه راه‌های مواجهه با مخاطره می‌توانند بسیار پرهزینه باشند -پیش از تهیه یک برنامه نهایی درمان- بادرنظر گرفتن هزینه-منفعتی که دارند، مورد ارزیابی قرار می‌گیرند.

جدول ۳-۱۵. شناسنامه (۱۱): روش CORAS

شناسنامه روش CORAS	
نام اختصاری	کُراس - CORAS
نام کامل	Consultative Objective Risk Analysis System سیستم تحلیل مخاطره عینی-مشاوره‌ای
ارائه‌دهنده	نتیجه حاصل از پروژه EU-Dunded که در سال ۲۰۰۳ میلادی تکمیل شد.
کشور ارائه‌دهنده	چهار کشور اتحادیه اروپا (یونان، آلمان، نروژ، انگلستان) سه شرکت (Telenor ،Solinet ،Intracom) هفت مؤسسه (CTI، FORTH، IFE، NCT، NR، RAL، Sintef) و دانشگاه QMUL در انگلستان
وضعیت نسخه	نخستین نسخه این روش در سال ۲۰۰۱ میلادی منتشر شد، نسخه پلت‌فرم ارزیابی اطلاعات بین سال‌های ۲۰۰۱ تا ۲۰۰۳ میلادی و نسخه مربوط به افزایش ویژگی‌ها/ کارکردهای روش بین سال‌های ۲۰۰۴ تا ۲۰۰۷ میلادی توسعه یافت و در حال حاضر نسخه ۲۰۱۵ این روش به عنوان آخرین نسخه معتبر محسوب می‌شود.
زبان	انگلیسی
قیمت	به صورت رایگان در دسترس است.
دامنه کاربرد/ استفاده	حوزه امنیت، ایمنی، قانون، حفاظت مدنی، برنامه‌ریزی اضطراری، دفاع، بهداشت و سلامت، پزشکی از راه‌دور، تجارت الکترونیکی، و غیره.
هدف	هدف اصلی این روش بهبود روش سنتی ارزیابی مخاطره جهت دستیابی به نتایج بهتر است. همچنین، توسعه چارچوبی است که از روش‌هایی برای تحلیل مخاطره، از روش‌های نیمه-رسمی برای مدلسازی شی‌گرا و از ابزارهای رایانه‌ای برای ارزیابی دقیق و کارآمد مخاطره سیستم‌های حیاتی-امنیتی استفاده می‌کند.
مراحل مدیریت مخاطره	گام نخست: آمادگی برای تحلیل؛ (شناسایی هدف از ارزیابی و عمق تحلیل) گام دوم: ملاقات با مشتری؛ (دستیابی به یک درک مشترک از اهداف کلی و برنامه‌ریزی) گام سوم: تعریف هدف از ارزیابی با بهره‌برداری از نمودارهای دارایی؛ (بررسی برخی از سناریوهای تهدید؛ آسیب‌پذیری‌ها و مخاطره‌ها در سطوح بالا) گام چهارم: مرحله قبل از تحلیل واقعی مخاطره با تمرکز بر استخراج معیارهای سنجش مخاطره که بایستی بیشتر مورد استفاده قرار گیرد. گام پنجم: شناسایی مخاطره با بهره‌برداری از نمودارهای تهدید گام ششم: تخمین مخاطره با بهره‌برداری از نمودارهای تهدید گام هفتم: سنجش مخاطره با بهره‌برداری از نمودارهای مخاطره گام هشتم: مواجهه با مخاطره با بهره‌برداری از نمودارهای مقابله/ رفتاری
فرمول محاسبه مخاطره	مخاطره (رخداد، دارایی) = احتمال (حادثه) × پیامد (حادثه، دارایی)
سازگاری با استانداردها	این روش با استانداردهای The Australian/New Zealand Standard، AS/NZS 4360:2004، ISO/IEC 17799، ISO/IEC 13335 و ISO 31000 سازگار است.
ابزارهای پشتیبان	CORAS tools - ابزار نشانه‌گذاری XML برای تبادل داده‌های ارزیابی مخاطره - یک زبان توصیفی مبتنی بر UML که ارزیابی امنیتی را هدف قرار می‌دهد.
مزایا/ نقاط قوت	+ ارائه توضیحات دقیق از سیستم هدف، مفهوم آن و تمام ویژگی‌های امنیتی مرتبط در یک فرمت به راحتی قابل دسترس؛ + ارائه گرافیکی اطلاعات، بهبود ارتباطات و تعاملات بین طرف‌های درگیر در تحلیل را به همراه دارد؛ + تسهیل مستندسازی نتایج ارزیابی مخاطره و فرضیاتی که این نتایج به آنها بستگی دارد؛ + ابزار پشتیبان رایگان؛ + تسهیل ارتباطات تکراری و همکاری بین ذینفعان گوناگون؛ + دارای ویرایشگر نمودار؛ + مبتنی بر زبان UML، زبانی که از نمودارها برای نشان دادن روابط و وابستگی بین کاربران و محیطی که در آن کار می‌کنند استفاده می‌کند؛ + بهره‌برداری از فن طوفان فکری جهت جمع‌آوری اطلاعات مربوط به شناسایی مخاطره؛ + شامل تعداد زیادی نمودار و اشکال گرافیکی است که درک روش را برای کاربر آسان می‌کند؛ + بسیار کامل، مناسب برای سیستم‌های حیاتی-امنیتی و سازمان‌های بزرگ؛ + دارای یک زبان گرافیکی سفارشی‌سازی شده جهت مدل‌سازی مخاطره و تهدید؛ + یک رویکرد ساده نسبت به روش ISRAM است.
معایب/ نقاط ضعف	- نیازمند دانش متخصصین در زمینه‌های گوناگون؛ - نیازمند کوشش مضاعف؛ - زمان‌بر بودن؛ - روند تقریباً طولانی؛ - نیازمند زمان لازم جهت آمادگی و یادگیری روش توسط تیم تحلیل؛ - از دقت کمتری نسبت به روش ISRAM برخوردار است؛ - عدم توسعه؛
وب‌سایت‌رسمی	http://coras.sourceforge.net/index.html

۳-۲-۳-۲. روش CRAMM

روش تحلیل و مدیریت مخاطره آژانس مرکزی ارتباطات و مخابرات[1] یا به اختصار «CRAMM» یک روش تحلیل مخاطره توسعه‌یافته توسط سازمان دولتی بریتانیا (آژانس مرکزی ارتباطات و مخابرات انگلستان[2]) در سال (۱۹۸۵) میلادی است که در حال حاضر به نام دفتر بازرگانی دولتی[3] تغییر نام داده است. این روش دربرگیرنده طیف گسترده‌ای از ابزارهای ارزیابی مخاطره است که شامل یک کتابخانه اقدام‌های متقابل متشکل از بیش از ۳۰۰۰ اقدام متقابل دقیق است که در بیش از ۷۰ گروه‌بندی منطقی سازمان‌یافته است. ابزار پشتیبان این روش نیز به همین نام «CRAMM» است که نمایی از این ابزار در (**شکل ۳-۲۵**) به تصویر کشیده شده است.



شکل ۳-۲۵. ابزار CRAMM، (Yazar 2002)

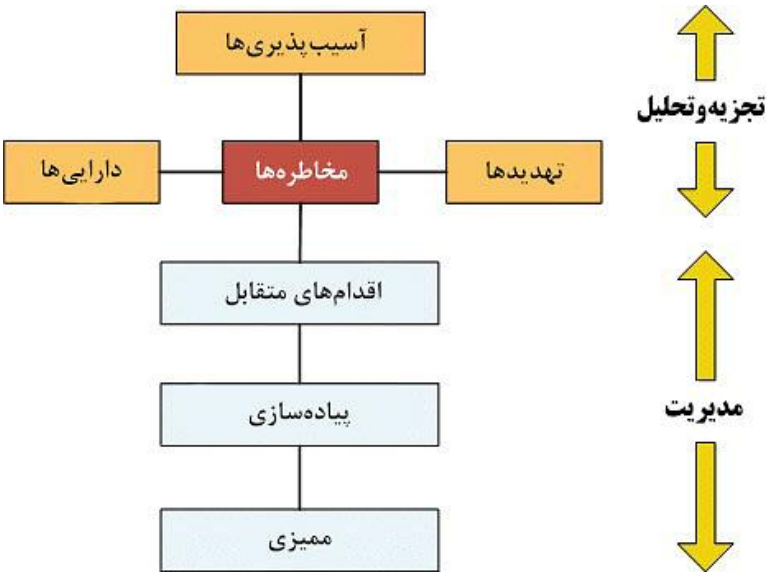
امکان بهره‌برداری از این روش بدون ابزار «CRAMM» بسیار مشکل و دشوار است. نخستین نسخه از روش/ ابزار «CRAMM» بر پایهٔ به‌روش‌های سازمان‌های دولتی بریتانیا تدوین شده بود. در حال حاضر، «CRAMM» روشی است که دولت انگلستان ترجیح می‌دهد جهت فرآیند تحلیل مخاطره از آن استفاده کند. این روش در بسیاری از کشورهای خارج از انگلستان نیز استفاده می‌شود. این روش به شکل ویژه برای سازمان‌های بزرگ همانند سازمان‌های دولتی و صنعتی مناسب است. این روش بر جنبه‌های فنی امنیت تمرکز دارد و مراحل زیر را شامل می‌شود:

- شناسایی و ارزیابی دارایی؛
- ارزیابی تهدید و آسیب‌پذیری؛ و
- انتخاب و توصیه اقدام‌های متقابل.

در مرحله شناسایی و ارزیابی، دارایی‌های فیزیکی برحسب هزینه جایگزینی‌شان ارزش‌گذاری می‌شوند، در حالی‌که دارایی‌های نامشهود (برای مثال داده‌ها و نرم‌افزار) با توجه به هزینه‌هایی که در صورت خراب شدن، افشاء یا اصلاح شدن اطلاعات رخ می‌دهد، رتبه‌بندی می‌شوند. بر پایهٔ دارایی‌های شناسایی شده، تهدیدها و آسیب‌پذیری‌های شناسایی شده و فراوانی آنها به صورت کیفی

[1] Central Computing and Telecommunications Agency Risk Analysis and Management Method (CRAMM)
[2] Central Computer and Telecommunications Agency (UK)
[3] The Office of Government Commerce (OGC)

ارزیابی می‌شود. یک ماتریس مخاطره برای ترکیب اطلاعات مربوط به تهدید و آسیب‌پذیری خاص یک دارایی برای محاسبه مقدار مخاطره نهایی استفاده می‌شود. یکی از مزایای روش «CRAMM» پشتیبانی از ابزار قدرتمند آن است. در مرحله کاهش مخاطره، «CRAMM» به طور خودکار اقدامات متقابل مناسبی را برای ترکیب دارایی/ تهدید/ آسیب‌پذیری/ مخاطره توصیه می‌کند. با این حال «CRAMM» با تمرکز بر سازمان‌های بزرگ توسعه‌یافته است، و دانش تخصصی قابل توجهی برای انجام کل فرآیند مدیریت مخاطره امنیت اطلاعات لازم دارد. این روش یک رویکرد مرحله‌ای و منظم است که هم جنبه‌های فنی (برای مثال سخت‌افزار و نرم‌افزار) و هم جنبه‌های غیرفنی امنیت (مانند فیزیکی و انسانی) را دربرمی‌گیرد. مراحل این روش در (**شکل ۳-۲۶**) ارائه شده است.



شکل ۳-۲۶. مراحل فرآیند روش CRAMM

جدول ۳-۱۶. شناسنامه (۱۲): روش CRAMM

شناسنامه روش CRAMM	
نام اختصاری	کرام - CRAMM
نام کامل	Central Computing and Telecommunications Agency Risk Analysis and Management Method (CRAMM) روش مدیریت و تحلیل مخاطره آژانس مرکزی ارتباطات و مخابرات
ارائه‌دهنده	آژانس مرکزی ارتباطات و مخابرات، دولت انگلستان
کشور ارائه‌دهنده	انگلستان
وضعیت نسخه	نخستین نسخه این روش در سال ۱۹۸۵ میلادی منتشر شد، نسخه (۱,۰) در سال ۱۹۸۷ میلادی، نسخه (۲,۰) در سال ۱۹۹۱ میلادی، نسخه (۳,۲) در سال ۱۹۹۸ میلادی، نسخه (۴,۰) در سال ۲۰۰۱ میلادی، نسخه (۵,۰) در سال ۲۰۰۳ میلادی به چاپ رسید و در حال حاضر نسخه (۵,۶) سال ۲۰۰۵ میلادی این روش به عنوان آخرین نسخه معتبر محسوب می‌شود.
زبان	انگلیسی، هلندی، چک
قیمت	با پرداخت هزینه (رایگان نیست/ روشی پرهزینه است)
دامنه کاربرد/ استفاده	برای سازمان‌های بزرگ مانند نهادهای دولتی و صنعتی در نظر گرفته شده است.
هدف	می‌تواند جهت توجیه سرمایه‌گذاری‌های امنیتی از طریق نشان دادن نیاز به اقدام در سطح مدیریتی مورد استفاده قرار گیرد.
مراحل مدیریت مخاطره	این روش شامل سه مرحله: - مرحله نخست: شناسایی و ارزیابی دارایی؛ - مرحله دوم: ارزیابی تهدید و آسیب‌پذیری؛ و - مرحله سوم: انتخاب و توصیه اقدام‌های متقابل.
فرمول محاسبه مخاطره	مخاطره (تهدید، دارایی) = احتمال (تهدید) × آسیب‌پذیری (تهدید، دارایی) × پیامد (تهدید، دارایی)
سازگاری با استانداردها	فرآیندی مشابه استاندارد ISO/IEC 27005 دارد و سازمان‌ها را برای دریافت گواهی ISO/IEC 27001 حمایت می‌کند. با استانداردهای ISO/IEC 27001، ISO/IEC 17799 و ISO/IEC 27005 سازگار است.

شناسنامه روش CRAMM	
ابزارهای پشتیبان	ابزارهای تجاری CRAMM expert (Insight) و CRAMM express (Insight) از این روش پشتیبانی می‌کنند.
مزایا/ نقاط قوت	+ رویکرد ساختاریافته برای مدیریت و تحلیل مخاطره بر پایهٔ روش ایجادشده؛ + کمک در برنامه‌ریزی احتمالی، ممیزی‌ها و صدور گواهینامه BS7799؛ + ارتقاء آگاهی امنیتی و پذیرش؛ + امکان بررسی‌های کامل و سریع (همچنین بررسی‌های سطح بالا که از بیانیه‌های خط‌مشی پشتیبانی می‌کند)؛ + به‌روزرسانی مرتب پایگاه‌داده و همچنین پوشش‌دهی حوزه‌های غیرفنی؛ + اولویت‌بندی نسبی اقدامات متقابل، ازجمله معیارهای اثربخشی و هزینه‌های پیاده‌سازی؛ + ثبات ناشی از راهکارهای مشابه برای پروفایل‌های مشابه مخاطره. + روش ردیابی سریع با هدف دسته‌بندی منطقی دارایی‌ها؛ + پیچیدگی ارزیابی می‌تواند با نیازها در ارتباط باشد؛ + بسیار مناسب برای سازمان‌ها و شرکت‌های بزرگ؛ + فرآیند معمولاً به صورت خودکار انجام می‌شود. + تمامی معیارهای مربوط به دسته‌بندی مخاطره را پوشش می‌دهد؛ + دسته‌های گوناگون مخاطره را در نظرمی‌گیرد؛ + اجرا و پیاده‌سازی کنترل‌ها بایستی مبتنی بر ایجاد ارزش برای سازمان باشد؛ + دارای یک رابطه علی و معلولی از طریق رابطه مبتنی بر تهدید و دارایی است؛ + از تخمین و اندازه‌گیری کمّی و کیفی استفاده می‌کند؛ + فرآیند کنترلی آن نسبت به دو روش OCTAVE و CORAS از عملکردی بهتری برخوردار است؛
معایب/ نقاط ضعف	- نیاز به افراد متخصص و مجرب برای بهره‌برداری از ابزار؛ - بهره‌برداری از ابزار پشتیبان همراه با هزینه مجوز و زمان لازم جهت آموزش نرم‌افزار؛ - بررسی‌های کامل، که ممکن است طولانی شدن فرآیند تحلیل و خروجی‌های بسیار زیاد به‌صورت هارد-کپی را به همراه داشته باشد؛ - اهمیت ناچیز برخی نتایج در یک بررسی کامل به دلیل تاخیر بین تحلیل و پیاده‌سازی پس از تغییرات سریع در سیستم یا شبکه مورد بررسی؛ - نیاز به دانش متخصص؛ - ارزیابی کامل می‌تواند طولانی و پیچیده باشد؛ - تنها در ارتباط با ابزارهای اختصاصی استفاده می‌شود؛ - بهره‌برداری از این روش بیشتر محدود به اروپا می‌شود؛ - برای سازمان‌های با اندازه کوچک-متوسط مناسب نیست؛ - روش کندی است؛ (تحلیل کامل ممکن است به جای چندین روز، ماه‌ها به طول انجامد) - با توجه به حجم زیاد اطلاعاتی که تولید می‌کند، از انعطاف لازم برخوردار نیست.
وب‌سایت‌رسمی	https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83

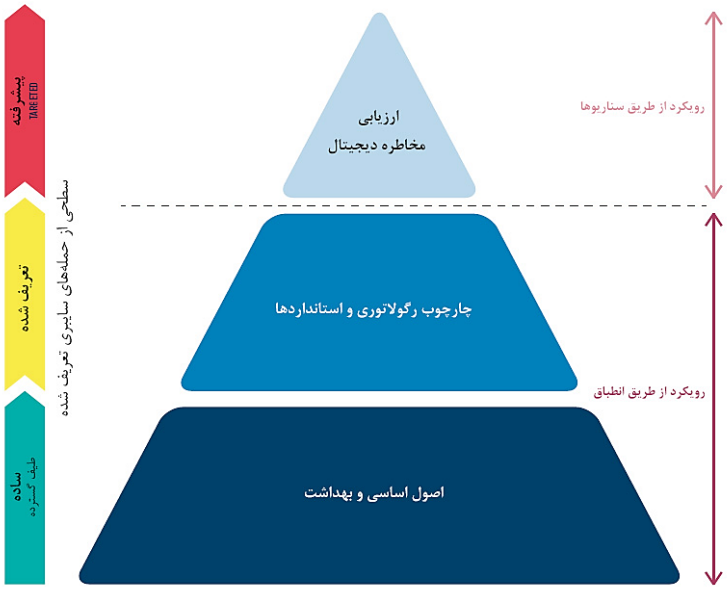
۳-۲-۳-۳. روش EBIOS

بیان نیازها و شناسایی اهداف امنیتی[1] یا به اختصار «EBIOS» روشی برای ارزیابی و مواجهه با مخاطره‌های دیجیتال است که توسط آژانس امنیت سایبری ملّی فرانسه[2] و با حمایت باشگاه «EBIOS» منتشر گردید. این روش جعبه ابزاری را در اختیار قرار می‌دهد که می‌تواند با توجه به اهداف پروژه خود را سازگار کند و به شکل‌های متفاوتی مورد استفاده قرار گیرد. مدیریت مخاطره «EBIOS» در اثرگذاری با استانداردهای مرجع موجود -از لحاظ مدیریت مخاطره و همچنین امنیت سایبری- سازگار است. مدیریت مخاطره «EBIOS» ارزیابی مخاطره‌های دیجیتال و شناسایی اقدام‌های امنیتی جهت کنترل آنها، همچنین امکان اعتبارسنجی سطح قابل قبول مخاطره را در یک رویکرد بهبود مستمر در بلندمدت فراهم می‌سازد. سرانجام، این روش امکان ایجاد منابع و استدلال‌هایی را فراهم می‌آورد که برای برقراری ارتباط و تصمیم‌گیری در داخل سازمان و با توجه به شرکای آن مفید است. از روش مدیریت مخاطره «EBIOS» می‌توان برای اهداف گوناگونی استفاده کرد:

- استقرار یا تقویت فرآیند مدیریت مخاطره دیجیتال در یک سازمان؛
- ارزیابی و مواجهه با مخاطره‌های مرتبط با یک پروژه دیجیتال، به ویژه با هدف اعتبارسنجی امنیتی؛
- تعیین سطح امنیتی لازم برای یک محصول یا خدمت، با توجه به موارد استفاده و مخاطره‌های قابل مواجهه؛

این روش هم در سازمان‌های دولتی و هم سازمان‌های خصوصی -صرف‌نظر از اندازه سازمان- که بخش فعالیت آنها و اینکه سیستم‌های اطلاعاتی آنها در حال توسعه هستند یا از قبل وجود دارند، قابل اجرا است.

روش مدیریت مخاطره «EBIOS» رویکردی را برای مدیریت مخاطره دیجیتال اتخاذ می‌کند که از بالاترین سطح (مأموریت‌های اصلی هدف مورد مطالعه) آغاز می‌شود تا با مطالعه سناریوهای احتمالی، به تدریج به کارکردهای تجاری و فنی برسد. هدف این است که با قراردادن این دو رویکرد مکمل در جایی که بالاترین ارزش افزوده را دارند، تلفیقی بین «انطباق» و «سناریوها» حاصل شود. این رویکرد توسط هرم مدیریت مخاطره دیجیتال در (**شکل ۳-۲۷**) نشان داده شده است.



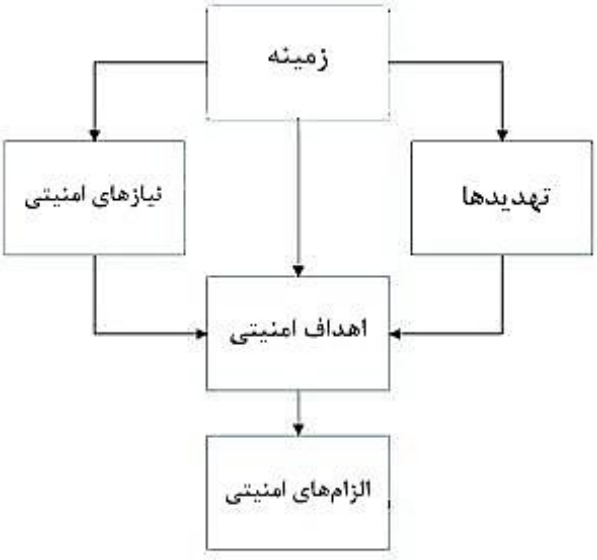
شکل ۳-۲۷. هرم مدیریت مخاطره دیجیتال، (ANSSI 2019)

[1] Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives (EBIOS)

[2] Direction Centrale de la Sécurité des Systémes d'Information (DCSSI)

این روش اطلاعاتی برای پشتیبانی از فرآیند تصمیم‌گیری (توضیحات دقیق، سهام راهبردی، جزئیات مخاطره‌ها با پیامد آنها بر سازمان، الزام‌ها و اهداف صریح امنیتی) فراهم می‌کند. این روش مجموعه‌ای جامع از راهنماها را (به‌همراه یک ابزار نرم‌افزاری متن‌باز رایگان) در اختیار مدیران مخاطره سیستم اطلاعاتی قرار می‌دهد. این روش یک رویکرد برای ارزیابی و مواجهه با مخاطره‌ها در حوزه امنیت سیستم‌های اطلاعاتی تدوین می‌کند و تمام موجودیت‌های فنی (نرم‌افزار، سخت‌افزار، شبکه‌ها) و موجودیت‌های غیرفنی (سازمان، جنبه‌های فردی، امنیت فیزیکی) را در نظر می‌گیرد. این روش مدیریت مخاطره امنیت اطلاعات فرانسوی، از پنج مرحله در قالب (**شکل ۳-۲۸**) تشکیل شده است:

۱. یک مطالعه زمینه‌ای برای شناسایی محیط، هدف و عملکرد سیستم هدف.
۲. بیان نیازهای امنیتی (ارزیابی مخاطره) با ارزیابی دارایی‌های اساسی از نظر دسترس‌پذیری، صحت و محرمانگی.
۳. یک مطالعه تهدید (ارزیابی مخاطره) برای شناسایی تهدیدهای مؤثر بر سیستم و آسیب‌پذیری‌های مربوطه که می‌تواند توسط این تهدیدها مورد سوء استفاده قرار گیرد.
۴. شناسایی اهداف امنیتی (ارزیابی مخاطره) برای رسمی‌سازی مخاطرات با مقایسه تأثیر تهدیدهای احتمالی بر نیازهای امنیتی سازمان؛ و
۵. تعیین الزامات امنیتی (مقابله با مخاطره) برای تعیین الزامات عملکردی که امکان تحقق اهداف امنیتی تعریف شده را می‌دهد.



شکل ۳-۲۸. نقشه‌راه روش EBIOS

مراحل اصلی روش «EBIOS» مشابه استاندارد NIST SP 800-30 است، اما تفاوت‌های زیادی نیز وجود دارد: «EBIOS» یک روش مدیریت مخاطره امنیت اطلاعات در سطح بالا را ارائه می‌دهد و این روش هیچ تکراری را تعریف نمی‌کند.

این روش هم در بخش عمومی (کلیه وزارتخانه‌ها و ارگان‌های تحت مدیریت و اداره آنها) و هم در بخش خصوصی (شرکت‌های مشاوره‌ای، شرکت‌های کوچک و بزرگ) فرانسه و خارج از کشور (اتحادیه اروپا، کبک، بلژیک، تونس، لوکزامبورگ، و غیره) مورد استفاده قرار می‌گیرد.

جدول ۳-۱۷. شناسنامه (۱۳): روش EBIOS

شناسنامه روش EBIOS	
نام اختصاری	اِبیوس - EBIOS
نام کامل	Identification of Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Security Objectives بیان نیازها و شناسایی اهداف امنیتی
ارائه‌دهنده	اداره مرکزی امنیت سیستم‌های اطلاعاتی (آژانس امنیت ملّی فرانسه)
کشور ارائه‌دهنده	فرانسه
وضعیت نسخه	نخستین نسخه این روش در سال ۱۹۹۵ میلادی منتشر شد، نسخه دوم در ژوئن سال ۲۰۰۴ میلادی، نسخه سوم در ژانویه سال ۲۰۱۰ میلادی به چاپ رسید و در حال حاضر نسخه ۲۰۱۸ این روش به عنوان نسخه چهارم معتبر محسوب می‌شود.
زبان	فرانسوی، انگلیسی، آلمانی، اسپانیایی
قیمت	به صورت رایگان در دسترس است.
دامنه کاربرد/ استفاده	سنجش مخاطره‌های مرتبط با سیستم‌های اطلاعاتی در درجه نخست برای سازمان‌های دولتی و تجاری که با وزارت دفاع کار می‌کنند و اطلاعات طبقه‌بندی شده محرمانه یا پنهانی را کنترل می‌کنند، درنظر گرفته شده است.
هدف	روشی برای تحلیل، سنجش و مقابله با مخاطرات مرتبط با سیستم‌های اطلاعاتی هدف اصلی روش، ارزیابی و آمادگی برای موقعیت‌های احتمالی آینده (در مورد یک سیستم اطلاعاتی به تازگی ایجاد شده)، و شناسایی و پاسخ به نواقص (زمانی که سیستم کار می‌کند) به منظور اصلاح ترتیبات امنیتی. ارزیابی و مواجهه با مخاطره‌های مرتبط با سیستم اطلاعاتی (چه در سطح سازمانی و چه در سطح خصوصی) جهت پشتیبانی از تصمیم‌گیری در سطح مدیریت و ایجاد زمینه مشترک برای بحث‌های امنیتی بین ذی‌نفعان گوناگون.
مراحل مدیریت مخاطره	این روش شامل پنج مرحله: - مرحله نخست: ساخت/ تولید محتوا (ارتباط بین محتوای کسب‌وکار و سیستم اطلاعاتی)؛ - مرحله دوم: تعیین الزام‌های امنیتی بر پایهٔ رویدادهای امنیتی؛ - مرحله سوم: شناسایی و تحلیل سناریوهای تهدید؛ - مرحله چهارم: بهره‌برداری از اطلاعات قبلی جهت شناسایی مخاطره‌ها و شرح اهداف امنیتی مناسب و مورد نیاز در ارتباط با مخاطره‌ها؛و - مرحله پنجم: تعیین کنترل‌های امنیتی لازم و تصریح مخاطره‌های باقی‌مانده.
فرمول محاسبه مخاطره	مخاطره (تهدید، دارایی، نیازها) = پیامد (تهدید، نیازها) × آسیب‌پذیری (تهدید، دارایی)
سازگاری با استانداردها	این روش با بسیاری از استانداردهای امنیتی فناوری اطلاعات ازجمله با استانداردهای ISO/IEC 27001، ISO/IEC 15408، ISO/IEC 17799، ISO/IEC 13335، ISO/IEC 21827، ISO/IEC 27005 و ISO/IEC 31000 سازگار است.
ابزارهای پشتیبان	ابزار رایگان EBIOS
مزایا/ نقاط قوت	+ روشی عمومی جهت انطباق با استانداردهای محلی، روش‌ها، محتوا + می‌تواند متناسب با اهداف ارزیابی در اندازه‌ها و پیچیدگی‌های گوناگون مورد استفاده قرار گیرد. + تسهیل افزایش آگاهی توسط ذینفعان درگیر در یک پروژه (مدیران عالی، مالی، حقوقی یا بخش‌های منابع انسانی، مقامات عقد قرارداد، پیمانکاران اصلی، کاربران) + افزایش درگیری بازیگران سیستم اطلاعاتی و استانداردسازی واژگان؛ + می‌تواند در طول طراحی فاز یا یک سیستم موجود مورد استفاده قرار گیرد؛ + منطبق با اهداف راهبردی سازمان؛ + اعتبارسنجی گام‌به‌گام روش؛ + ارزیابی مخاطره در فرآیند توسعه سیستم؛ + بهینه‌سازی منابع؛ + مورد استفاده در بسیاری از کشورهای عضو و کشورهای غیرعضو اتحادیه اروپا؛ + نسبت به دیگر روش‌های از پیچیدگی متوسطی برخوردار است؛ + یک روش تکرارپذیر؛
معایب/ نقاط ضعف	– بسیاری از اسناد پشتیبان فقط به زبان فرانسوی در دسترس است.
وب‌سایت رسمی	https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/

۳-۲-۳-۴. روش FAIR

تحلیل عاملی مخاطره اطلاعات[1] یا به اختصار «FAIR»، مدلی مبتنی بر عامل‌های مؤثر در ایجاد مخاطره و چگونگی تأثیر هر یک از آنها بر یک‌دیگر است که در سال ۲۰۰۵ میلادی توسط «جک جونز[2]» رئیس هیأت مدیره فعلی شرکت «اُپن‌گروپ»[3] -مجموعه‌ای از سازمان‌های بین‌المللی که به کسب‌وکارها کمک می‌کنند علاوه‌بر اندازه‌گیری و مدیریت مخاطره‌های اطلاعاتی، مخاطره‌های امنیت سایبری خود را نیز شناسایی کنند- ارائه شد. به طور معمول، چارچوب «FAIR» برای تحلیل و شناسایی میزان احتمال اینکه یک کسب‌وکار یک نقض داده یا از دست دادن داده را تجربه کند، مورد استفاده قرار می‌گیرد. پس از شناسایی مخاطره‌ها، سازمان‌ها می‌توانند در جهت بهبود پروتکل‌های امنیت سایبری خود گام بردارند. مدل ارزیابی مخاطره این روش نسبت به دیگر چارچوب‌های امنیت سایبری متفاوت است. این روش برای ارزیابی مخاطره از نمودارها یا امتیازدهی عددی استفاده نمی‌کند، بلکه بر روی داده‌های علمی جمع‌آوری شده در طول فرآیند تحلیل متمرکز است و آسیب‌پذیری‌ها را در قالب اصطلاح‌های مالی فهرست می‌کند. «FAIR» یک چارچوب مدیریت مخاطره است که با استانداردهای بین‌المللی سازگار است و اهداف آن کمک به سازمان‌ها در درک، تحلیل و اندازه‌گیری مخاطره اطلاعات است. «FAIR» یک **چارچوب ارزش در معرض مخاطره استاندارد**[4] است که مخاطره عملیاتی و امنیت سایبری را هدف قرار می‌دهد. «FAIR» استانداردها و به‌روش‌هایی را در اختیار سازمان‌ها قرار می‌دهد که آنها را قادر می‌سازد مخاطره اطلاعات را از دیدگاه/ منظر کسب‌وکار تا ذینفعان- ازجمله مخاطره اطلاعات، امنیت سایبری و مدیران کسب‌وکار- اندازه‌گیری، مدیریت و گزارش کنند.

«FAIR»، به عنوان روشی برای تعیین کمیت و مدیریت مخاطره در هر نوع و سطح از سازمانی استفاده می‌شود. این روش تنها مدل کمّی استاندارد بین‌المللی برای مخاطره امنیت سایبری است. این روش:

- مدلی برای درک، تحلیل و کمّی‌سازی مخاطره سایبری در اصطلاح‌های مالی ارائه می‌کند؛
- برخلاف چارچوب‌های ارزیابی مخاطره است که خروجی خود را بر روی نمودارهای رنگی کیفی یا مقیاس‌های وزنی عددی متمرکز می‌کنند؛
- پایه و اساسی برای توسعه رویکرد علمی در مدیریت مخاطره اطلاعات ایجاد می‌کند؛
- استاندارد OpenFAIR توسط Open Group به عنوان یک کنسرسیوم جهانی که دستیابی به اهداف کسب‌وکار را از طریق استانداردهای فناوری اطلاعات امکان‌پذیر می‌کند، حفظ و نگهداری می‌شود.

چارچوب «FAIR» شامل چهار مؤلفه اصلی -تهدیدها، دارایی‌ها، خود سازمان و محیط خارجی- است. تمامی موارد درون یک سناریو در یکی از این طبقه‌بندی‌ها جای می‌گیرند، و هر یک دارای ویژگی‌ها یا عامل‌هایی هستند که به شکلی مثبت یا منفی در بُروز مخاطره نقش دارند.

روش «FAIR» احتمال وقوع حمله‌های سایبری را اندازه‌گیری می‌کند. این روش از سناریوها برای اندازه‌گیری احتماع وقوع نقض امنیتی استفاده می‌کند و زمانی که مخاطره‌ها شناسایی می‌شوند، کسب‌وکارها می‌توانند اقدام‌های لازم جهت جلوگیری از دست دادن اطلاعات را انجام دهند. پنج مؤلفه به شرح زیر برای این مدل مقیاس‌پذیر وجود دارد که سازمان‌ها را قادر می‌سازد تا مخاطره‌های اطلاعاتی خود را اندازه‌گیری و پس از شناسایی، آنها را به شکل مؤثری مدیریت کنند:

۱. شناسایی رابطه بین حوزه‌های گوناگون و پروتکل‌های امنیت سایبری موجود؛
۲. کمک به ایجاد چارچوبی برای پروتکل‌های جمع‌آوری داده؛

---

[1] Factor analysis of information risk (FAIR)
[2] Jack Jones
[3] Open Group
[4] A Standard Value at Risk (VaR) Framework

۳. اندازه‌گیری عامل‌های مخاطره گذشته و جاری همراه با عوامل احتمالی آینده؛

۴. محاسبه مخاطره؛

۵. تحلیل سناریوهای پیچیده مخاطره.

این چارچوب به کسب‌وکارها کمک می‌کند تا یک پایه و اساس محکم برای اندازه‌گیری و مدیریت مخاطره‌های اطلاعاتی ایجاد کنند. مراحل ده‌گانه روش تحلیل عاملی مخاطره اطلاعات در چهار بخش به شرح ذیل تدوین شده است:

- **بخش اول) شناسایی اجزاء/ مؤلفه‌های سناریو**
  - مرحله اول) شناسایی دارایی در معرض مخاطره
  - مرحله دوم: شناسایی جامعه تهدید تحت بررسی
- **بخش دوم) سنجش شدت/ میزان رویداد از دست رفته** [1]
  - مرحله سوم: تخمین نرخ احتمال رویداد تهدید[2]
  - مرحله چهارم: تخمین قابلیت تهدید[3]
  - مرحله پنجم: تخمین قدرت کنترل[4]
  - مرحله ششم: به دست آوردن آسیب‌پذیری
  - مرحله هفتم: به دست آوردن میزان رویداد از دست رفته
- **بخش سوم) سنجش شدت/ مقدار خسارت احتمالی**[5]
  - مرحله هشتم: تخمین بدترین حالت خسارت
  - مرحله نهم: تخمین ضرر/ خسارت احتمالی
- **بخش چهارم) نتیجه و محاسبه مخاطره**
  - مرحله دهم: نتیجه و محاسبه مخاطره

روش «FAIR»، مکمل روش‌های دیگر مانند «COSO»، «ITIL»، «ISO 27002:2005»، «COBIT»، «OCTAVE» و غیره است. این روش اسبابی را فراهم می‌کند که می‌تواند در دیگر مدل‌های مخاطره استفاده شود.

[1] Loss Event Frequency (LEF)
[2] Threat Event Frequency (TEF)
[3] Threat Capability (TCap)
[4] Control strength (CS)
[5] Probable Loss Magnitude (PLM)

جدول ۳-۱۸. شناسنامه (۱۴): روش FAIR

شناسنامه روش FAIR	
نام اختصاری	فِیر - FAIR
نام کامل	Factor analysis of information risk تحلیل عاملی مخاطره اطلاعات
ارائه‌دهنده	کنسرسیوم استاندارد صنعتی Open Group
کشور ارائه‌دهنده	ایالات متحده آمریکا
وضعیت نسخه	نخستین نسخه این روش در سال ۲۰۰۱ میلادی منتشر شد، نسخه دوم در سال ۲۰۰۵ میلادی و نسخه سوم در سال ۲۰۰۹ میلادی توسعه یافت و در حال حاضر نسخه ۲۰۱۷ این روش به عنوان آخرین نسخه معتبر محسوب می‌شود.
زبان	انگلیسی
قیمت	به صورت رایگان در دسترس است.
دامنه کاربرد/ استفاده	سازمان‌های با ارزش بالای دارایی و آسیب‌پذیری‌های تهدید شدید. محافظت از اطلاعات شخصی خصوصی شامل داده‌های مالی، بهداشت و سلامت، کارت‌های اعتباری، و غیره.
هدف	هدف از این روش، ارائه چارچوبی جهت اجرای اثربخش تحلیل مخاطره برای تقویت و تکمیل فرآیندهای موجود است. در واقع، جهت مدیریت آسیب‌پذیری‌ها و حوادث در داخل سازمان، شبکه یا سیستم با بهره‌برداری از رویکرد مبتنی بر مخاطره طراحی شده است.
مراحل مدیریت مخاطره	بخش اول) شناسایی اجزاء/ مؤلفه‌های سناریو - مرحله نخست: شناسایی دارایی در معرض مخاطره - مرحله دوم: شناسایی جامعه تهدید موردنظر بخش دوم) سنجش شدت/ میزان خسارت احتمالی - مرحله سوم: تخمین احتمال رویداد تهدید - مرحله چهارم: تخمین قابلیت تهدید - مرحله پنجم: تخمین قدرت کنترل - مرحله ششم: به دست آوردن آسیب‌پذیری - مرحله هفتم: به دست آوردن میزان رویداد از دست رفته بخش سوم) سنجش شدت/ مقدار خسارت احتمالی - مرحله هشتم: تخمین بدترین حالت خسارت - مرحله نهم: تخمین ضرر/ خسارت احتمالی بخش چهارم) نتیجه و بیان مخاطره - مرحله دهم: بیان نتیجه مخاطره
فرمول محاسبه مخاطره	مخاطره = میزان رویداد از دست‌رفته (آسیب‌پذیری (مشکل آسیب‌پذیری، قابلیت تهدید) + نرخ احتمال رویداد تهدید (نرخ تماس، احتمال اقدام)) × میزان خسارت احتمالی (خسارت اولیه + مخاطره ثانویه (میزان خسارت ثانویه، نرخ رویداد خسارت ثانویه))
سازگاری با استانداردها	با استانداردهای ISO 27001, 27005, 31000 سازگار است.
ابزارهای پشتیبان	نرم‌افزار اکسل و ابزار اختصاصی FAIRLite
مزایا/ نقاط قوت	+ طبقه‌بندی پایه‌ای برای معیارهای جمع‌آوری داده‌ها ایجاد می‌کند، زمینه‌ای را برای طبقه‌بندی داده‌ها و همچنین چارچوبی برای تحلیل داده‌ها فراهم می‌کند. + درنظر گرفتن فاکتورهای جزئی جهت دستیابی به نتایج کلان توسط شکست مخاطره به المان‌ها؛ + پشتیبانی توسط دسته‌بندی گسترده، مدل مفهومی و چارچوب مدیریت مخاطره؛ + فرآیند پایه‌ای و سریع ارزیابی مخاطره و نیاز به ابزارهای اختصاصی و یا آموزش ندارد؛ + مناسب برای مدیریت مخاطره در هر نوع سازمانی؛ + شناسایی راحت مخاطره‌ها با توجه به سادگی روش؛ + بهره‌برداری از مقادیر عددی، ریاضیات و کمّی‌سازی جهت دستیابی به نتایج و پاسخ‌های دقیق و صحیح؛ + اطمینان از آمادگی کسب‌وکارها در مواجهه با تهدیدهای داده جاری و آینده؛ + مناسب برای تمامی سطوح سازمان‌ها؛ + مدیریت مخاطره مقرون‌به‌صرفه؛
معایب/ نقاط ضعف	- اسناد موجود فقط ارزیابی مخاطره بر دارایی‌های مستقل را پشتیبانی می‌کند؛ - برای انجام تحلیل در سیستم‌های گسترده نیاز به آموزش ویژه و خاص دارد؛ - بسیار زمان‌بر است؛
وب‌سایت رسمی	https://www.fairinstitute.org/what-is-fair

۳-۲-۳-۵. روش FRAAP

فرآیند تسهیل‌شده ارزیابی مخاطره[1] یا به اختصار «FRAAP» یک ارائه از «توماس پلتیر[2]» است. این روش مبتنی بر پیاده‌سازی فنون مدیریت مخاطره به‌صورت مقرون‌به‌صرفه است و از یک روش تحلیل مخاطره کیفی استفاده می‌کند که شامل تحلیل آسیب‌پذیری، تحلیل پیامد، تحلیل تهدید و نظرسنجی‌ها است. این روش افزون بر این، بر یک سیستم پیش آزمایش تأکید دارد و به عنوان یک ارزیابی رسمی مخاطره بر روی سیستم مناسب اجرا می‌شود. سرانجام، این رابطه با بهره‌برداری از تحلیل پیامد تجاری/ کسب‌وکار به عنوان مبنایی برای تعیین میزان پیامد بر مخاطره «FRAAP» تأثیر می‌گذارد. این روش بر جنبه‌های امنیت فرآیندهای کسب‌وکار یا سیستم متمرکز است. تیم ارزیابی این روش بیانگر مهارت‌ها و جنبه‌های فنی، جنبه‌های تجاری و ویژگی‌های مدیریت است. این روش بر تهدیدها، آسیب‌پذیری‌ها و نتایج حاصل از محرمانگی، صحت و دسترس‌پذیری متمرکز است. این روش شامل سه گام به شرح ذیل است:

- جلسه پیش از «FRAAP»: تصمیم‌گیری دربارهٔ به تصویرکشیدن سیستم و حوزه/ منطقه ارزیابی و همچنین تشکیل و تنظیم تیم سنجش.
- جلسه «FRAAP»: این گام از ۳ اقدام تشکیل شده است:
  - تعیین مسئولیت‌های هر یک از شرکت‌کنندگان در جلسه طوفان فکری؛
  - شناسایی مخاطره‌های احتمالی در محدوده ارزیابی؛
  - اولویت‌بندی مخاطره‌های شناسایی شده؛
- جلسه پس از «FRAAP»: تحلیل بیشتر اطلاعات جمع‌آوری شده از جلسه «FRAAP» است. نتایج حاصل از این روش، نشان‌دهنده مخاطره‌ها و چگونگی کاهش آنها با کنترل‌های موجود یا جدید است. گزارش نهایی شامل اطلاعاتی جامع دربارهٔ این فرآیند، استقبال از یک ایده عملی برای اقدام‌های مورد نیاز پیشنهاد شده است.

در واقع، این روش به سازمان اجازه می‌دهد تا از منابع خود جهت ارزیابی مخاطره در کنار دیگر رویکردها تا حد توان استفاده کند. رویکردی برای شناسایی ذینفعان و درنظر گرفتن دارایی‌های اطلاعاتی تحت مالکیت آنها است. این روش به واحدهای تجاری/ کسب‌وکار اجازه می‌دهد که کنترل منابع خود را در دست بگیرند. همچنین نسبت به تعیین حفاظ‌های امنیتی مورد نیاز و اینکه چه کسی مسئول اجرا/ پیاده‌سازی این حفاظ‌های امنیتی باشد، کمک می‌کند.

---

[1] Facilitated Risk Analysis and Assessment Process (FRAAP)

[2] Thomas Peltier

جدول ۳-۱۹. شناسنامه (۱۵): روش FRAAP

شناسنامه روش FRAAP	
نام اختصاری	فِرآپ - FRAAP
نام کامل	Facilitated Risk Analysis and Assessment Process فرآیند ارزیابی و تحلیل مخاطره تسهیل‌شده
ارائه‌دهنده	توماس پلتیر
کشور ارائه‌دهنده	ایالات متحده آمریکا (واشنگتن دی.سی)
وضعیت نسخه	نخستین نسخه این روش در سال ۲۰۰۱ میلادی منتشر شد، نسخه دوم در سال ۲۰۰۵ میلادی به چاپ رسید و در حال حاضر نسخه ۲۰۱۰ این روش به عنوان آخرین نسخه معتبر محسوب می‌شود.
زبان	انگلیسی
قیمت	به صورت رایگان در دسترس است.
دامنه کاربرد/ استفاده	تحلیل سیستم، برنامه‌کاربردی، پلت‌فرم، فرآیند کسب‌وکار و یا بخشی از عملیات تجاری/ کسب‌وکار در یک زمان
هدف	به عنوان یک روش کارآمد و منظم برای اطمینان از شناسایی، بررسی و مستندسازی تهدیدهای مربوط به فعالیت‌های تجاری/ کسب‌وکارها توسعه یافته است. طراحی چگونگی بهره‌برداری از یک "راهنمای تسهیل‌گر" ارزیابی و تحلیل مخاطره کیفی جهت تولید یافته‌های قابل‌فهم توسط غیرکارشناسان.
مراحل مدیریت مخاطره	**مراحل پیش از رویکرد:** - پیش نمایش نتایج: یک نسخه از این نتایج باید در طرح فرآیند ارزیابی مخاطره ذخیره شود. - تعیین دامنه: تعیین محدودیت‌هایی که باید بررسی گردد و در طول فرآیند پیش از ورود به روش FRAAP بارها مورد بازبینی و اصلاح قرار گیرد. - نمودار بصری (مدل تصویری): مروری بر فرآیند تحلیل مخاطره -با بهره‌برداری از نمودار فویل- در واقع، فرآیندی که قرار است بررسی شود، توصیف می‌کند. - ایجاد تیم FRAAP: معمولاً شامل تعدادی از اعضای نماینده کسب‌وکارها در حوزه‌های گوناگون است. - مکانیک جلسه: جلسه مدیر واحد کسب‌وکار با فرد برنامه‌ریزی کننده است که مسئولیت تدارکات، هماهنگی مکان و زمان ارزیابی مخاطره و دعوت از اعضای تیم را به عهده دارد. - توافق بر سر تعاریف واژگان و اصطلاحات - جلسه کوتاه طوفان فکری: شناسایی چهار الی پنج تهدید برای هر یک از ویژگی‌های کسب‌وکار (صحت، محرمانگی، دسترس‌پذیری) توسط اعضای تیم. (فرآیند شناسایی سریع تهدید) **مراحل رویکرد:** ۱- شناسایی مخاطره، ۲- اولویت‌بندی مخاطره، ۳- کنترل‌های شناسایی شده **مراحل پس از رویکرد:** - جدول مرجع متقابل: برگه‌ای کاری است که بر پایهٔ جدول مخاطره‌ها و کنترل‌ها برای شناسایی جداول کنترلی سازگار با مخاطره‌ها شناسایی شده است. - برنامه عملیاتی/ طرح اقدام: برگه‌ای کاری است که برای تعیین نوع مناسب کاهش مخاطره متناسب با وضعیت سیستم ساخته شده است، همچنین مشخص می‌کند فرآیند کاهش توسط چه کسی و در چه زمانی انجام خواهد شد.
فرمول محاسبه مخاطره	مخاطره = دارایی (ارزش) × تهدید (احتمال) × آسیب‌پذیری
سازگاری با استانداردها	این روش با استانداردهای BS7799-3 و ISO/IEC TR 13335-3 سازگار است.
ابزارهای پشتیبان	در بهره‌برداری از این ابزار، هر سازمان باید جعبه ابزار مخصوص به خود را تهیه کند.
مزایا/ نقاط قوت	+ قابلیت اجرا/ پیاده‌سازی توسط صاحبان کسب‌وکار؛ + مدت زمان کوتاه/ صرف زمان کوتاه جهت انجام فرآیند تحلیل مخاطره (چند روز به جای هفته‌ها و ماه‌ها) + مقرون‌به‌صرفه بودن؛ + امکان بهره‌برداری از قابلیت‌ها/ توانمندی‌های متخصصان درون سازمانی؛ + سازگار و انعطاف‌پذیر با نیازهای سازمان؛ + عدم نیاز به سخت‌افزار اضافی یا نرم‌افزار گران قیمت؛ + رویکرد کسب‌وکار-محور، تولید خروجی مرتبط با ذینفعان؛ + نیاز به کمی کمک خارجی، اکثر مراحل این روش را می‌توان با کارکنان سازمان پیاده‌سازی کرد (حتی اگر آنها کارشناسان امنیتی نباشند)؛ + بسیار سریع.
معایب/ نقاط ضعف	– دستیابی به موفقیت بسیار وابسته به "تسهیل‌گر[1]" است که باید یک مذاکره‌کننده خوب باشد و در ارتباط با امنیت اطلاعات و کسب‌وکار دانش لازم را داشته باشد؛ – تنها در ارتباط با روش فنی مناسب به خوبی کار می‌کند.
وب‌سایت‌رسمی	http://www.peltierassociates.com/frap.htm

[1] Facilitator

۳-۲-۳-۶. روش MEHARI

روش «MEHARI» معرف **روشی برای تحلیل هماهنگ مخاطره**[1] است که توسط **سازمان امنیت اطلاعات فرانسه**[2] در سال ۱۹۹۶ و با هدف کمک به مدیران اجرایی در مدیریت امنیت اطلاعات، منابع فناوری اطلاعات و در نتیجه کاهش مخاطره‌های مرتبط توسعه‌یافته است. این روش همچنین برای کمک به اجرا و پیاده‌سازی استاندارد مدیریت مخاطره امنیت اطلاعات « ISO 27005» طراحی شده است. علاوه براینکه «MEHARI» به عنوان یک روش شناخته می‌شود، «MEHARI» مجموعه‌ای از ابزارهایی است که تضمین می‌کند یک راهکار مناسب مدیریت امنیت را می‌توان -بدون توجه به رویکرد مورد استفاده- طراحی کرد. «MEHARI» سازگار با استاندارد مدیریت مخاطره «ISO 13335» طراحی شده است و برای فرآیند **سیستم مدیریت امنیت اطلاعات**[3] که در استاندارد «ISO 27001» شرح داده شده، مناسب است. افزون بر این، این روش به ذی‌نفع اجازه می‌دهد تا برنامه‌های امنیتی را بر پایهٔ فهرستی از نقاط کنترلی آسیب‌پذیر و فرآیند پایش دقیق جهت دستیابی به چرخه بهبود مستمر توسعه دهد. این روش جایگزین **"روش تحلیل مخاطرات رایانه‌ای بر پایهٔ سطوح**[4]**"** یا به اختصار (MARION) گردید. این روش در سال ۲۰۰۴ میلادی به‌روزرسانی شد و از زمانی که دیگر سازمان امنیت اطلاعات فرانسه از آن حمایت نکرد، روش «MEHARI» جایگزین آن شد. «MEHARI» یک روش مدیریت، ارزیابی و تحلیل مخاطره **متن‌باز**[5] است که توسط متخصصین امنیت اطلاعات در سازمان‌های گوناگون استفاده می‌شود. این روش -به شکل مستقیم در پایگاه‌های دانش خود- شامل بسیاری از فرمول‌ها جهت ارزیابی مستقیم مخاطره و انتخاب راهی جهت کاهش آنها است. این روش، به مدیران سازمان و متخصصین حوزه امنیت اجازه می‌دهد تا مخاطره‌های سازمانی مرتبط با اطلاعات، سیستم‌های اطلاعاتی و فرآیندهای اطلاعاتی را ارزیابی و مدیریت کنند. روش «MEHARI» در راستای استانداردهای «ISO 27001» و «ISO 27005» سازمان بین‌المللی استانداردسازی توسعه داده شده است. برخی از اهداف اصلی این روش عبارتند از:

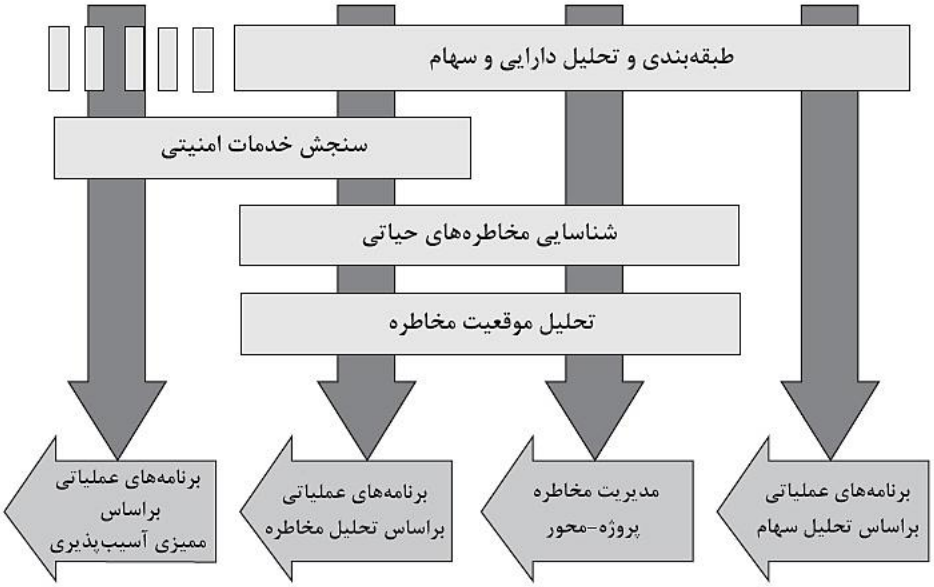
- ارائه یک روش مدیریت و ارزیابی مخاطره به ویژه در حوزه امنیت اطلاعات؛
- ارائه مجموعه‌ای از عناصر و ابزارهای مورد نیاز جهت اجرای موفقیت‌آمیز آن؛
- امکان تحلیل مستقیم و فردی از موقعیت‌های مخاطره توصیف شده در موارد گوناگون؛ و
- ارائه مجموعه‌ای کامل از ابزارها به ویژه برای مدیریت کوتاه‌مدت، میان‌مدت و بلندمدت امنیت که با بسیاری از اقدام‌ها و سطوح بلوغ سازگار است.

علاوه‌براین تصمیم به اجرای اقدام‌های امنیتی در یک سازمان بسته به وضعیت فعلی آن سازمان خاص ممکن است در بعضی مواقع بسیار دشوار باشد. با این وجود چنین تصمیم‌هایی باید با بهره‌برداری از یک رویکرد ساختاریافته و کاملاً متفکرانه -برای نمونه، MEHARI- اتخاذ شود، به طوری که با مخاطره‌های درگیر در سازمان مقابله و اطمینان دهد که سطوح آنها قابل قبول است. به طور کلی، «MEHARI» برای مدیران عملیاتی، مدیران مخاطره، **مدیران ارشد امنیت اطلاعات**[6] و **مدیران ارشد اطلاعات**[7] مفید است. «MEHARI» یک روش کارآمد برای مدیریت امنیت اطلاعات در تمامی سازمان‌ها -از طریق ارائه یک چارچوب روش‌شناختی (**شکل ۳-۲۹**)- محسوب می‌شود که شامل مراحل ذیل است:

- تحلیل و طبقه‌بندی دارایی و سهام؛
- تحلیل مخاطره و؛
- سنجش خدمات امنیتی؛
- تعریف برنامه‌های امنیتی.

---

[1] Me´thode Harmonise´e d'Analyse de Risques — Harmonised Risk Analysis Method (MEHARI)
[2] Club de la sécurité de l'information français (CLUSIF)
[3] Information Security Management System- ISMS
[4] Methodology of Analysis of Computer Risks Directed by Levels (MARION)
[5] Open Source
[6] Chief Information Security Officers (CISO)
[7] Chief Information Officers (CIO)



شکل ۳-۲۹. نقشه‌راه روش MEHARI (CLUSIF 2015)

- **مرحله نخست – طبقه‌بندی و تحلیل دارایی و سهام:** هدف از تحلیل سهام شناسایی پیامدهای مستقیم و غیرمستقیمی است که ممکن است منجر به عدم دسترسی، یکپارچگی و محرمانگی شود. تحلیل سهام بسیار مهم و حیاتی است، زیرا در انتخاب اقدام‌های انجام شده کمک می‌کند و از هزینه‌هایی که اهمیت سهام کمتر است، جلوگیری می‌کند. از محدودیت‌های غیرضروری جلوگیری کرده و اولویت‌ها را تعیین می‌کند. تحلیل سهام دو پیامد/ خروجی اصلی دارد:
  - مقیاس ارزش عملکرد نادرست - سند مرجعی که بر روی پیامدهای کسب‌وکار تمرکز دارد.
  - طبقه‌بندی دارایی‌ها - طبقه‌بندی دارایی‌های سیستم اطلاعاتی.
- **مرحله دوم – سنجش/ ممیزی خدمات امنیتی:** هدف از سنجش خدمات امنیتی، اطمینان از وجود نقاط ضعف و نقص در اقدام‌های امنیتی شناسایی شده است. عناصر اصلی سنجش خدمات امنیتی عبارتند از:
  - اثربخشی خدمات امنیتی؛
  - ثبات/ استحکام آنها؛ و
  - پایداری آنها در طول زمان.

  افزون بر این، ازجمله اهداف این مرحله می‌توان به موارد ذیل اشاره کرد:
  - تأیید اینکه هیچ نقطه ضعف غیرقابل قبولی وجود ندارد، در غیراینصورت برنامه‌های اقدام فوری ایجاد می‌شود؛
  - سنجش کارایی و اثربخشی اقدام‌های امنیتی با بهره‌برداری از چک‌لیست حرفه‌ای؛ و
  - مقایسه سازمان با به‌روش‌ها، جهت سنجش انطباق/ سازگاری با استاندارد و اهمیت آن در سطح تخصص پایگاه ممیزی مورد استفاده.
- **مرحله سوم – شناسایی مخاطره‌های حیاتی: تحلیل مخاطره روش MEHARI شامل فرآیندهای ذیل است:**
  - شناسایی موقعیت‌هایی که ممکن است نتایج موردانتظار را با تأخیر روبرو کند؛
  - تخمین احتمال چنین موقعیت‌هایی، پیامدهای احتمالی و معیارهای کاهش، انتقال یا نگهداری مخاطره؛ و
  - فراهم‌سازی مقدمات اقدام‌های امنیتی مربوطه.
- **مرحله چهارم – تحلیل موقعیت مخاطره:** واضح است که تعریف موقعیت‌های مخاطره مرحله مهمی است که ابزارها مهم‌ترین منابع حیاتی هستند. دو روش اصلی برای تعریف و شناسایی مخاطره‌ها وجود دارد که عبارتند از:
  - یک رویکرد مستقیم، از طریق مقیاس ارزش عملکرد نادرست، و
  - یک رویکرد سازمان‌یافته و نظام‌مند، از طریق سنجش خودکار با بهره‌برداری از سناریو ارائه شده توسط MEHARI.

جدول ۳-۲۰. شناسنامه (۱۶): روش MEHARI

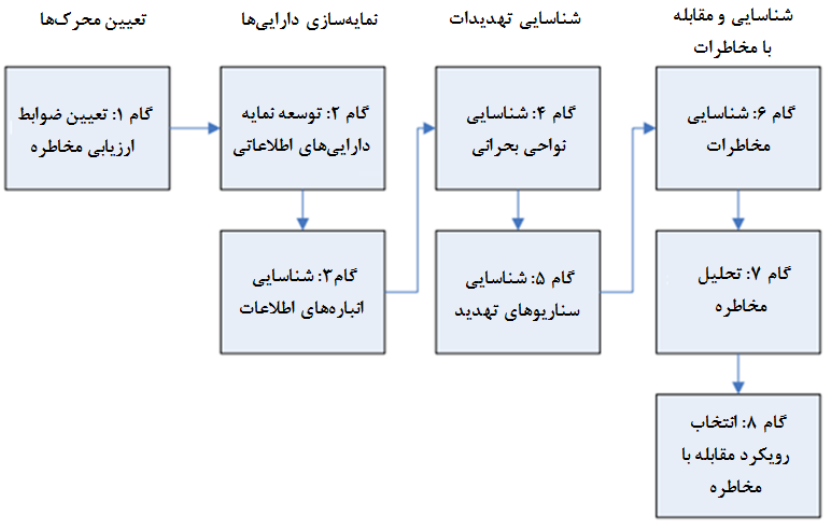
شناسنامه روش MEHARI	
نام اختصاری	مِهاری - MEHARI
نام کامل	Me´thode Harmonise´e d'Analyse de Risques — Harmonised Risk Analysis Method (MEHARI) روشی برای تحلیل هماهنگ مخاطره
ارائه‌دهنده	سازمان امنیت اطلاعات غیرانتفاعی و شرکت خصوصی Risicare
کشور ارائه‌دهنده	فرانسه
وضعیت نسخه	در ابتدا (۱۹۹۸) برای اعضای Clusif توسعه داده شد و از سال ۲۰۰۷ میلادی به بعد به‌صورت متن-باز، رایگان و عمومی در دسترس قرار گرفت. MEHARI Expert (2010) 2Q 2016 نسخه Mehari Pro (از سال ۲۰۱۴ میلادی) برای سازمان‌های با اندازه کوچک و متوسط نسخه Mehari Manager (از سال ۲۰۱۳ میلادی) برای پروژه‌های جدید یا فعالیت‌هایی خارج از محدوده اجرای قبلی روش نسخه Mehari Standard (از سال ۲۰۱۷ میلادی) برای سازمان‌های با اندازه کوچک و متوسط.
زبان	انگلیسی - فرانسوی
قیمت	یک روش متن-باز و به صورت رایگان در دسترس است.
دامنه کاربرد/ استفاده	توسعه طرح‌های امنیتی توسط ذینفعان بر پایهٔ فهرستی از نقاط کنترلی آسیب‌پذیر و یک فرآیند پایش دقیق جهت دستیابی به یک چرخه بهبود مستمر.
هدف	ارزیابی و مدیریت مخاطرات مرتبط با اطلاعات و مقابله با آنها هدف این روش کمک به مجریان (مدیران عملیاتی، CISO، CIO مدیر مخاطره، ممیزی/ حسابرسان) جهت مدیریت امنیت اطلاعات و منابع فناوری اطلاعات و کاهش مخاطره‌های مرتبط است. هدف این روش تهیه ابزارها و روش‌هایی است که می‌تواند برای انتخاب مناسب‌ترین اقدام‌های امنیتی برای یک سازمان مشخص و سنجش مخاطره‌های باقیمانده پس از عملیاتی‌شدن این اقدام‌ها مورد استفاده قرار گیرد. عمدتاً پرسنل اجرایی را موردهدف قرار می‌دهد (به ویژه CISOs) و برای کمک به اجرای استانداردهای ISO/IEC 27005 طراحی شده است. هدف از این روش، اجازه تحلیل چشم‌اندازهای مخاطره مبتنی بر سناریو توسط فرآیند ممیزی تصدیق‌پذیری و ارائه ابزارهایی برای مدیریت کوتاه‌مدت و بلندمدت امنیت است.
مراحل مدیریت مخاطره	۱. شناسایی موقعیت مخاطره؛ (با بهره‌برداری از پایگاه دانش یا به صورت مستقیم، دستی و غیره) ۲. سنجش قرارگرفتن در محیط طبیعی؛ ۳. سنجش فاکتورهای بازدارنده و پیشگیرانه؛ ۴. سنجش فاکتورهای بهبودبخش، تسکین‌دهنده و حفاظتی؛ ۵. سنجش توانمندی؛ ۶. سنجش پیامدهای درونی (نتایج) با پرکردن در یک جدول؛ ۷. سنجش پیامد و کاهش پیامد از طریق رایانش خودکار؛ ۸. سنجش جهانی مخاطره با توجه به فاکتورهای پیشین؛ ۹. تصمیم‌گیری در ارتباط با اینکه مخاطره قابل پذیرش است یا خیر.
فرمول محاسبه مخاطره	مخاطره (تهدید، دارایی) = احتمال (تهدید) × آسیب‌پذیری (تهدید، دارایی) × پیامد (تهدید، دارایی)
سازگاری با استانداردها	این روش با استانداردهای ISO/IEC 31000; ISO/IEC IS 13335-1; ISO/IEC 27005:2011; ISO/IEC 27001:2013; ISO 27002:2013 سازگار است.
ابزارهای پشتیبان	در حال حاضر ۴ ابزار مرتبط به عنوان پایگاه دانش روش، با بهره‌برداری از اکسل و برنامه آفیس در دسترس است. کتابچه راهنمایی که شیوهٔ بهره‌برداری از این ابزارها را شرح می‌دهد به صورت رایگان است. - Mehari Expert، برای تمامی انواع سازمان‌ها در اندازه‌های متوسط و بزرگ - Mehari Pro، برای موجودیت‌های کوچک - Mehari Manager، قابل استفاده برای پروژه‌های جدید، آماده‌سازی برای فعالیت‌های جدید، و غیره. - Mehari Standard، برای موجودیت‌های متوسط تا بزرگ
مزایا/ نقاط قوت	+ قابلیت تحلیل مخاطره‌ها به صورت مستقیم و مستقل؛ + کاملاً سازگار با استانداردهای امنیت اطلاعات مجموعه ISO؛ + دارای پایگاه دانش گسترده در قالب و فرمت اکسل؛ + بسیار انعطاف‌پذیر و مناسب برای سازمان‌های کوچک و بزرگ؛ + مورد استفاده در بسیاری از کشورهای عضو و کشورهای غیرعضو اتحادیه اروپا؛
معایب/ نقاط ضعف	- فقط می‌تواند در ارتباط با نرم‌افزار اختصاصی یا صفحه‌های گسترده مورد استفاده قرار گیرد؛ - نخستین نمونه از تحلیل تاحدودی نیازمند سازگاری با پایگاه دانش است. - عدم وجود پایگاه داده‌ای از اقدام‌های متقابل که مخاطرات سیستم‌های امنیت اطلاعات را کاهش دهد؛ - پایگاه دانش آسیب‌پذیری‌ها و تهدیدهای این روش باعث شده است این روش تاحدودی پیچیده و زمان‌بر باشد؛ - محدودیت در استفاده خارج از مناطق فرانسوی زبان؛ - تأثیر عامل انسانی در نتیجه نهایی؛ - پیچیدگی بالایی دارد؛
وب‌سایت‌رسمی	http://meharipedia.org/home

۳-۲-۳-۷. روش OCTAVE

«آلبرتز» و همکارانش (۲۰۰۳) روشی را برای مدیریت مخاطره امنیت اطلاعات شرح دادند که با نام «**ارزیابی عملیاتی تهدیدها، دارایی‌ها و آسیب‌پذیری‌های حیاتی**[1]» یا به اختصار «OCTAVE» شناخته می‌شود. این چارچوب معرف یک روش ارزیابی راهبردی مخاطره‌محور و برنامه‌ریزی امنیت است که توسط **انجمن پاسخ به رخدادهای امنیتی**[2] (CERT) ارائه شده است. «OCTAVE» یک رویکرد خودگردان است، به این معنی که افراد یک سازمان مسئولیت ایجاد راهبرد امنیت سازمان خود را بر عهده می‌گیرند. همچنین این روش به عنوان یک استاندارد دفاکتو شناخته می‌شود. این روش به بررسی مخاطره‌های امنیتی در قالب کسب‌وکار -و نه در قالب مخاطره‌های فنی- می‌پردازد. «OCTAVE» روشی برای شناسایی و سنجش مخاطرات امنیت اطلاعات است. این روش شامل سه مرحله به شرح زیر است:

۱) تعیین دارایی‌های حیاتی، کنترل‌های امنیتی که در حال حاضر اجرا شده و مهمترین دارایی‌ها، و همچنین ایجاد پروفایل‌های تهدید برای این دارایی‌ها؛
۲) شناسایی آسیب‌پذیری‌های زیرساختی؛ و
۳) شناسایی مخاطرات مربوط به دارایی‌های حیاتی و کنترل‌های بالقوه برای کاهش مخاطرات در حد قابل قبول و همچنین ایجاد راهبرد محافظت.

مراحل اصلی این روش شبیه استاندارد «NIST 800-30» مؤسسه ملّی استانداردها و فناوری است، اما «OCTAVE» در نکات زیر متفاوت است: «OCTAVE» خود مدیریتی است و نیازی به رهبری متخصص ندارد، و بر روی شیوه‌های امنیتی و نه بر فناوری تمرکز دارد. (**شکل ۳-۳۰**) نقشه‌راه و مراحل گام‌به‌گام روش «OCTAVE» را نشان می‌دهد (Caralli et al. 2007).



شکل ۳-۳۰. نقشه‌راه روش OCTAVE، (Caralli et al. 2007)

نسخه مربوط به سازمان‌های کوچک-متوسط این روش تحت عنوان «**روش ارزیابی عملیاتی تهدیدها، دارایی‌ها و آسیب‌پذیری حیاتی سازمان‌های کوچک-متوسط**[3]» یک نوع رویکرد متناسب با ابزارهای محدود و محدویت‌های منحصربه‌فردی است که به طور معمول در سازمان‌های کوچک (کمتر از ۱۰۰ نفر) یافت می‌شود. «OCTAVE-S» توسط یک تیم کوچک و متشکل از تخصص‌های گوناگون (۳ تا ۵ نفر) از پرسنل سازمان -کسانی که اطلاعات را جمع‌آوری و تحلیل می‌کنند، یک راهبرد حفاظتی و

[1] Operationally Critical Threat, Asset, and Vulnerability Evaluation (OVTAVE)
[2] Community Emergency Response Team
[3] **O**perationally **C**ritical **T**hreat ,**A**sset ,and **V**ulnerability **E**valuation **S**MEs (OCTAVE-S)

برنامه‌های کاهش خطر بر پایهٔ مخاطره‌های امنیتی منحصربه‌فرد عملیات سازمان ایجاد می‌کنند- هدایت می‌شود. برای اجرای کارآمد و مؤثر «OCTAVE-S» تیم باید اطلاعات گسترده‌ای از فرآیندهای امنیتی وکسب‌وکار داشته باشد تا بتواند تمام فعالیت‌ها را به تنهایی انجام دهد.

دیگر نسخه بهبودیافته روش «OCTAVE» تحت عنوان «**روش بهبود فرآیند ارزیابی عملیاتی تهدیدها، دارایی‌ها و آسیب‌پذیری‌های حیاتی**[1]» یا به اختصار «OCTAVE ALLEGRO» یک روش برای ساده‌سازی و بهینه‌سازی فرآیند ارزیابی مخاطرات امنیت اطلاعات است تا یک سازمان بتواند با سرمایه‌گذاری کوچک/ اندک در زمان، افراد و دیگر منابع محدود به نتایج کافی دست یابد. این روش سازمان را در انتخاب افراد، فن‌آوری و امکانات مرتبط با اطلاعات، فرآیندهای کسب‌وکار و خدماتی که آنها پشتیبانی می‌کنند، هدایت می‌کند.

روش «OCTAVE ALLEGRO» بر موقعیت‌یابی ارزیابی مخاطره در زمینه سازمانی مناسب متمرکز است، اما این یک رویکرد جایگزین است که به شکل ویژه در ارتباط با دارایی‌های اطلاعاتی و تاب‌آوری آنها ارائه شده است. این رویکرد جایگزین می‌تواند توانایی سازمان در موقعیت و اجرای ارزیابی مخاطره را بهبود بخشد، به طوری که منجر به ارائه نتایج معنادار به‌شیوه‌ای کارآمد و مؤثر می‌شود.

جدول ۳-۲۱. شناسنامه (۱۷): روش OCTAVE V2.0

شناسنامه روش OCTAVE V2.0	
نام اختصاری	اُکتاو - OCTAVE
نام کامل	Operationally Critical Threat, Asset, and Vulnerability Evaluation (OVTAVE) ارزیابی عملیاتی تهدیدها، دارایی‌ها و آسیب‌پذیری‌های حیاتی
ارائه‌دهنده	مؤسسه مهندسی نرم‌افزار و دانشگاه کارنگی ملون
کشور ارائه‌دهنده	ایالات متحده آمریکا
وضعیت نسخه	نخستین نسخه این روش در سپتامبر سال ۱۹۹۱ میلادی و نسخه ۲,۰ در سپتامبر سال ۲۰۰۱ میلادی تحت عنوان چارچوب و نسخه (۲,۰) در دسامبر سال ۲۰۰۱ میلادی تحت عنوان معیار OCTAVE منتشر گردید. همچنین، نسخه (۹,۰) در سپتامبر سال ۲۰۰۳ میلادی و نسخه (۱,۰) در مارچ سال ۲۰۰۵ میلادی تحت عنوان OCTAVE-S منتشر گردید و سرانجام، نسخه (۱,۰) این روش در ژوئن سال ۲۰۰۷ میلادی تحت عنوان OCTAVE ALLEGRO توسعه داده شد.
زبان	انگلیسی
قیمت	برای استفاده اعضای سازمان به صورت رایگان ولی برای استفاده سازمان‌های غیرعضو با خرید مجوز در دسترس است.
دامنه کاربرد/ استفاده	قانون انتقال و پاسخ‌گویی الکترونیک بیمه سلامت برای حریم‌خصوصی و امنیت سلامت پرسنل بهبود فرآیند ارزیابی مخاطره امنیت اطلاعات این روش نسبت به رویکردهای قبلی به شکل متفاوت‌تری عمل می‌کند و بیشتر بر روی دارایی‌های اطلاعاتی متمرکز است از چگونگی بهره‌برداری از آنها، محل ذخیره آن‌ها، شیوهٔ انتقال آنها، پردازش و چگونگی قرارگرفتن در معرض تهدیدها، آسیب‌پذیری‌ها و اختلالات به عنوان نتیجه.
هدف	این روش با هدف کمک به سازمان‌ها در اجرای فرآیند ارزیابی مخاطره امنیت اطلاعات در ارتباط با پیشران‌های راهبردی/ راهبردی و عملیاتی -جهت دستیابی به مأموریت سازمانی- طراحی شده است. هدف این روش کمک به سازمان‌ها در: - توسعه معیارهای سنجش مخاطره کیفی است که میزان تحمل مخاطره عملیاتی سازمان را تشریح می‌کند؛ - شناسایی دارایی‌هایی که برای مأموریت سازمان مهم هستند؛ - شناسایی تهدیدها و آسیب‌پذیری‌های مرتبط با دارایی‌ها؛ - تعیین و سنجش پیامدهای بالقوه برای سازمان در صورت بروز تهدیدها.
مراحل مدیریت مخاطره	این روش شامل ۸ گام است که در ۴ مرحله تدوین شده است: ۱) مرحله نخست، تعیین محرک‌ها: توسعه معیارهای تخمین مخاطره با محرک‌های سازمانی؛ - گام اول) تعیین ضوابط ارزیابی مخاطره

[1] Operationally Critical Threat, Asset, and Vulnerability Evaluation Allegro (OCTAVE Allegro)

شناسنامه روش OCTAVE V2.0		
	۲) مرحله دوم، نمایه‌سازی دارایی‌ها: ایجاد پروفایلی از دارایی‌های اطلاعاتی حیاتی تعیین شده؛ (فرآیند ایجاد پروفایل، مرزهای مشخصی را برای دارایی، شناسایی الزام‌های امنیتی و شناسایی تمام موقعیت‌هایی که دارایی در آن مکان‌ها ذخیره شده، اتقال داده شده و یا پردازش شده است) - گام دوم) توسعه نمایه دارایی‌های اطلاعاتی - گام سوم) شناسایی انباره‌های اطلاعات ۳) مرحله سوم، شناسایی تهدیدها: شناسایی تهدیدهای مرتبط با دارایی‌های اطلاعاتی در مکان‌هایی که دارایی ذخیره‌شده، انتقال داده شده یا پردازش شده است؛ - گام چهارم) شناسایی نواحی بحرانی - گام پنجم) شناسایی سناریوهای تهدید ۴) مرحله چهارم، شناسایی و مقابله با مخاطره‌ها: شناسایی مخاطره‌های مرتبط با دارایی‌های اطلاعاتی، تحلیل و شروع توسعه رویکردهای کاهش. - گام ششم) شناسایی مخاطره‌ها - گام هفتم) تحلیل مخاطره - گام هشتم) انتخاب رویکرد مقابله با مخاطره	
فرمول محاسبه مخاطره	مخاطره (تهدید، دارایی حیاتی) = پیامد (تهدید و دارایی حیاتی) × آسیب‌پذیری (دارایی حیاتی) تهدید (موقعیت) + پیامد (نتیجه) = مخاطره امتیاز مخاطره = ارزش پیامد * رتبه و جایگاه (محل پیامد)	
سازگاری با استانداردها	این روش با استانداردهای ISO 27005، ISO 31000 و NIST 800-30 سازگار است.	
ابزارهای پشتیبان	ابزارهای تجاری؛ ابزارهای آموزشی (با دسترس‌پذیری آزاد: پشتیبان آموزشی، آموزش‌های آگاهی‌رسانی)	
مزایا/ نقاط قوت	+ توانایی پیوند/ اتصال اهداف سازمانی به اهداف امنیت اطلاعات؛ + این روش مناسب افرادی است که می خواهند فرآیند ارزیابی مخاطره را بدون ورودی، تخصص و یا مشارکت گسترده سازمان انجام دهند. + منا سب برای سازمان‌هایی که به سادگی بی شتر از دقت تمرکز دارند؛ + خودآموز/ راهبر: می‌تواند تو سط تیم‌های کوچک از کارکنان خود سازمان انجام شود؛ + انعطاف پذیر: شامل چندین روش مناسب برای سازمان‌ها و زمینه‌های خاص است؛ + روشی که به طور گسترده مورد استفاده قرار می‌گیرد با مقدار زیادی از اسناد پشتیبان و ابزارهای سازگار شخص ثالث؛ + به آمادگی کمتری نسبت به مدل های IRAM و IT-GRUNDSCHUTZ نیاز دارد؛ + امکان تکمیل با تیم‌های کوچکی از افراد و مهارت‌های فنی جزئی در یک دوره زمانی کوتاه؛ + عدم نیاز به جزئیات فنی؛ + یک رویکرد بصری و سریع برای ارزیابی مخاطره که تنها اطلاعات ضروری را تولید می‌کند؛ + معیارها و اقدام های سازگار که می تواند متناسب با نیازهای سازمان سفارشی شود؛ + مناسب برای تیم‌های کوچک؛ + از پیچیدگی کمی برخوردار است؛ + عدم نیاز به دخالت گسترده سازمانی؛ + در سطوح گوناگون سازمان قابل استفاده است؛	+ نسخه OCTAVE آن برای سازمان های بزرگ و نسخه OCTAVE-S آن مخصوص سازمان‌های کوچک درنظر گرفته شده است؛ + تمامی معیارهای مربوط به دسته‌بندی مخاطره را پوشش می‌دهد؛ + توسعه برنامه زمانی ارزیابی مجدد را تسهیل می‌کند؛ + ارزیابی مخاطره بدون درنظر گرفتن احتمال وقوع تهدید؛ + قابلیت انطباق‌پذیری متناسب با نیازمندی‌های یک سازمان؛ + بر روی دو فاکتور سادگی و دقت متمرکز است؛ + در پیشگیری از ضرر و زیان بسیار مفید است؛ + توانایی تصمیم گیری در ارتباط با محافظت از اطلاعات را برای شرکت فراهم می‌کند؛ + جزئیات و سازوکارهای لازم برای ارزیابی مخاطره امنیت داده‌های مبتنی بر محتوا، سیستماتیک و گسترده را شفاف می‌کند؛ + فرآیندی جامع، سیستماتیک و سازگار؛ + تمرکز بر محرک های سازمانی با هدف درک بهتر از نیازهای سازمان؛ + استفاده آسان از کاربرگ‌ها پس از یادگیری؛ + اطمینان از دقت فرآیند ارزیابی توسط چک‌لیست‌های روش؛ + تخمین نتایج؛ + سهولت در استفاده و یادگیری راحت روش؛
معایب/ نقاط ضعف	- یک روش سنگین شامل بسیاری از فرآیندها، برگه‌های کاری و غیره است؛ - دسترسی به ویژگی‌های دیگر توسط چارچوب ارائه نشده است؛ - اطلاعاتی در ارتباط با هزینه تحلیل مخاطره ارائه نکرده است؛ - تأثیر عامل انسانی در نتیجه نهایی؛	- برای موارد اضطراری استفاده نمی‌شود؛ - جهت اصلاح و رفع آسیب پذیری های به وجود آمده مناسب نیست؛ - عدم اولویت‌بندی احتمال‌ها؛
وب‌سایت‌رسمی	http://www.cert.org/octave/osig.html	

۳-۲-۳-۸. روش IRAM

روش‌های انجمن امنیت اطلاعات[1] یک انجمن بین‌المللی از شرکت‌های خصوصی و سازمان‌های بخش دولتی است. این انجمن شامل چندین محصول و ابزار مکمل برای انجام فرآیند ارزیابی مخاطره است که ازجمله آنها می‌توان به موارد ذیل اشاره کرد:

- **استاندارد تجارب خوب**[2]، هر ساله توسط «مجمع امنیت اطلاعات» منتشر می‌شود و دستورالعمل‌های سطح بالایی را برای امنیت اطلاعات ارائه می‌کند. این راهنما طیف گسترده‌ای از ترتیبات مربوط به امنیت اطلاعات را پوشش می‌دهد که برای حفظ مخاطرات کسب‌وکار در سطوح قابل قبول نیاز است.
- **مدیریت مخاطره اطلاعات پایه**[3] «FIRM» *و نسخه اصلاح شده کارت امتیازی* «FIRM»، یک رویکرد دقیق برای پایش و کنترل مخاطره اطلاعات در سطح سازمانی است. این روش شامل راهنمایی برای برقراری ارتباط، کسب حمایت و پشتیبانی ذینفعان و پیاده‌سازی آن است. **"کارت امتیازی مخاطره اطلاعات**[4]**"** به عنوان بخشی از روش «FIRM» برای جمع‌آوری اطلاعات مربوط به یک دارایی خاص مورد استفاده قرار می‌گیرد.
- **بررسی وضعیت امنیت اطلاعات**[5]، ابزاری جامع برای مدیریت مخاطره است که طیف وسیعی از کنترل‌های امنیتی که توسط سازمان‌ها جهت کنترل مخاطره‌های کسب‌وکار مرتبط با سیستم‌های اطلاعاتی مبتنی بر فناوری اطلاعات مورد استفاده قرار می‌گیرد، مورد ارزیابی قرار می‌دهد.
- **فرآیند ساده برای تحلیل مخاطره**[6] یا به اختصار «SARA»، یک روش دقیق برای تحلیل مخاطره اطلاعات در سیستم‌های اطلاعات حیاتی است و با روش «SPRINT» ترکیب شده است و در قالب یک روش جدید تحت عنوان «IRAM» به روزرسانی شده است.
- **فرآیند ساده‌سازی شده برای شناسایی مخاطره**[7] یا به اختصار «SPRINT»، یک روش نسبتاً سریع و آسان برای استفاده و جهت ارزیابی پیامدهای کسب‌وکار و تحلیل مخاطره اطلاعات در سیستم‌های اطلاعاتی مهم و نه حیاتی محسوب می‌شود. این روش به عنوان مکمل/ تکمیل‌کننده روش «SARA» شناخته می‌شود و گزینه مناسب‌تری برای تحلیل مخاطره مرتبط با سیستم‌های حیاتی کسب‌وکار محسوب می‌شود؛ و در نهایت
- **متدولوژی‌های تحلیل مخاطره اطلاعات**[8] یا به اختصار «IRAM»، یک روش مدیریت مخاطره نظیربه‌نظیر است که توسط انجمن امنیت اطلاعات و به عنوان جایگزین روش‌های «SARA» و «SPRINT» توسعه یافته است. از این‌رو، در این کتاب بر روی این روش از این سری روش‌های ارائه شده توسط انجمن امنیت اطلاعات تمرکز شده است.

«IRAM» روشی است با چشم‌انداز کسب‌وکار که جنبه‌های گوناگونی را نیز شامل می‌شود. این روش ساختارمند و دقیق در عین حال عملیاتی، انعطاف‌پذیر و فراتر از همه برای استفاده آسان است، این روش به منظور پاسخگویی به نیازهای مطرح شده تحلیلگران مخاطره اطلاعات در سازمان‌های مدرن مخاطره‌محور توسعه داده شده است. این روش با انجام یک تحلیل مخاطره کامل

---

[1] Information Security Forum (ISF) Methods
[2] Standard of Good Practice
[3] Fundamental Information Risk Management (Firm)
[4] Information Risk Scorecard
[5] Information Security Status Survey
[6] Simple to Apply Risk Analysis (Sara)
[7] Simplified Process for Risk Identification (Sprint)
[8] Information Risk Analysis Methodologies (IRAM)

بر روی سیستم‌ها، به سازمان‌ها جهت تعیین میزان حیاتی بودن/ اهمیت سیستم‌های اطلاعاتی کمک می‌کند. (**شکل ۳-۳۱**) فرآیند سه مرحله‌ای روش تحلیل مخاطره اطلاعات را نشان می‌دهد.

مرحله	هدف مرحله	خروجی اصلی
مرحله اول **ارزیابی پیامد کسب‌وکار**	ارزیابی پیامد احتمالی کسب‌وکار و تعیین الزام‌های امنیتی کسب‌وکار جهت محافظت از اطلاعات در یک سیستم	- فرم‌های ارزیابی پیامد کسب‌وکار - فرم خلاصه ارزیابی پیامد کسب‌وکار
مرحله دوم **ارزیابی تهدید و آسیب‌پذیری**	تعیین تهدیدها و آسیب‌پذیری‌هایی که احتمال وقوع حوادث جدی در یک سیستم را افزایش می‌دهد	- گزارش ارزیابی تهدید - گزارش ارزیابی آسیب‌پذیری - گزارش دقیق الزام‌های امنیتی
مرحله سوم **انتخاب کنترل**	سنجش و انتخاب کنترل‌ها جهت کاهش احتمال وقوع حوادث جدی	- گزارش سنجش کنترل - گزارش انتخاب کنترل

شکل ۳-۳۱. روش تحلیل مخاطره اطلاعات (IRAM)، (Creasey and Marvell 2013)

۳-۲-۳-۸-۱. روش IRAM2

روش تحلیل مخاطره اطلاعات نسخه شماره (۲)[1] یا به اختصار «IRAM2» آخرین روش ارزیابی و مواجهه با مخاطره اطلاعات است که در سال ۲۰۱۶ میلادی توسط انجمن امنیت اطلاعات (ISF) توسعه یافته است. «IRAM2» روشی است که دیدگاهی/ چشم‌اندازی تجاری دارد و جنبه‌های گوناگونی را شامل می‌شود. این روش با هدف پاسخگویی به چالش‌های جدید در مدیریت مخاطره توسعه و تجدید شده است. این روش دارای شش هدف اصلی است که بیان می‌کند چگونه این روش می‌تواند برای سازمان‌ها مفید باشد:

- *بکارگیری رویکردی ساده، عملی و در عین حال دقیق*: بر سادگی در طول اجرا تمرکز دارد، یک روش دقیق در تمام مراحل ارزیابی که امکان تجزیه‌وتحلیل عمیق را فراهم می‌کند، به طوری‌که در تصمیم‌گیری‌های راهبردی کسب‌وکار مفید باشد؛
- *درک واحد/ زبان مشترک*: ارائه یک چارچوب و فرهنگ لغت مشترک، این امکان را برای فعالان و مدیران مخاطره اطلاعات فراهم می‌سازد تا به یک درک یکسان از مخاطره اطلاعات در حوزه‌های گوناگون کسب‌وکار دست یابند و در مدیریت مخاطره سازمانی ادغام شوند؛
- *تمرکز بر چشم‌انداز تجاری*: مخاطره‌ها از منظر تجاری ارزیابی می‌شوند و نتیجه نهایی که یک پروفایل مخاطره است نمایانگر مخاطره اطلاعات و در قالب اصطلاحات تجاری بیان می‌شود؛
- *پوشش بیشتری از مخاطره‌ها*: پوشش گسترده‌تر و جامع‌تر مخاطره، در نتیجه احتمال نادیده گرفته شدن یک مخاطره قابل توجه کاهش پیدا می‌کند؛
- *تمرکز بر روی مخاطره‌های قابل توجه*: این روش شناسایی مهم‌ترین مخاطره‌ها را امکان‌پذیر می‌سازد تا مدیریت بتواند تصمیم بگیرد که منابع را کجا متمرکز کند؛
- *تعامل با ذی‌نفعان اصلی*: این روش راهی سازمان‌یافته برای تعامل بین فعالان مخاطره با دیگر ذی‌نفعان اصلی کسب‌وکار، مخاطره و فناوری فراهم می‌کند.

در بسیاری از سازمان‌ها، اطلاعات دیجیتال از اهمیت گسترده‌ای برخوردار هستند، به طوری که هسته اصلی کسب‌وکار آنها محسوب می‌شود. بهره‌برداری از اطلاعات دیجیتال به روشی ارزشمند و مؤثر در داشتن یک کسب‌وکار موفق بسیار مهم و کلیدی است. از سوی دیگر، فناوری‌های جدید دیجیتال منجر به مخاطره‌های جدید می‌شوند و پیامد این مخاطره‌ها در حال رشد است. از این‌رو، سازمان‌ها نیازمند تمرکز بیشتری بر فرآیند مدیریت مخاطره‌ها هستند. روش تحلیل مخاطره اطلاعات (دو) یک رویکرد

[1] Information Risk Analysis Methodologies 2 (IRAM2)

نظیربه‌نظیر است که با هدف پاسخگویی به چالش‌ها با دیدگاه تجاری در مدیریت مخاطره طراحی شده است. این روش شامل راهنمایی برای فعالان مخاطره جهت اجرای فرآیند شش مرحله‌ای متشکل از تعیین محدوده، ارزیابی پیامد کسب‌وکار، پروفایل تهدید، ارزیابی آسیب‌پذیری، سنجش مخاطره و مقابله با مخاطره است که در (**شکل ۳-۳۲**) به تصویر کشیده شده است.

شکل ۳-۳۲. مراحل روش تحلیل مخاطره اطلاعات نسخه شماره دو (IRAM2)، (ISF 2016)

در ادامه، هر یک از این مراحل به تفکیک مورد بررسی قرار خواهد گرفت:

- **مرحله نخست – تعیین محدوده: ارائه یک دیدگاه کسب‌وکار محور از مخاطره:** راهنمایی برای محدوده ارزیابی‌های مخاطره اطلاعات در هر دو بخش فناوری و کسب‌وکار ارائه می‌دهد. متخصصان مخاطره از این مرحله برای ارائه یک نگاه یکپارچه از مخاطره -از لایه خدمات کسب‌وکار تا زیرساخت فناوری- استفاده می‌کنند.
- **مرحله دوم – ارزیابی پیامد کسب‌وکار: ارزیابی سناریوهای واقع‌بینانه و بدترین پیامدهای کسب‌وکار:** راهنمایی برای شناسایی و ارزیابی پیامدهای کسب‌وکار ارائه می‌دهد. متخصصان مخاطره از این مرحله برای تعیین پیامد احتمالی کسب‌وکار استفاده می‌کنند جایی که باید محرمانگی، صحت و دسترس‌پذیری سیستم‌ها یا دارایی‌های اطلاعاتی حفظ شود.
- **مرحله سوم – پروفایل تهدید: درک و الگو قراردادن تهدیدها:** راهنمایی برای انجام یک ارزیابی عملی/ واقع‌گرایانه از چشم‌انداز تهدید اطلاعات ارائه می‌دهد. متخصصان مخاطره از این مرحله برای شناسایی و نمایه‌سازی تهدیدهای اصلی در گروه‌های گوناگون از طریق تعیین رویدادهای تهدید استفاده می‌کنند.
- **مرحله چهارم – ارزیابی آسیب‌پذیری: درک چگونگی مقاومت محیط/ سیستم‌ها در برابر تهدیدها:** راهنمایی برای انجام یک ارزیابی از آسیب‌پذیری‌هایی که احتمال موفقیت یک رویداد تهدید را تحت‌تأثیر قرار می‌دهد، ارائه می‌دهد. متخصصان مخاطره از این مرحله برای بررسی میزان ارتباط و اجرای کنترل‌های اصلی که به تعیین قدرت کنترل کمک می‌کند، استفاده می‌کنند.
- **مرحله پنجم: سنجش مخاطره: سنجش مخاطره در برابر اشتهای مخاطره سازمان:** راهنمایی عملی برای کمک به سنجش مخاطره‌ها پس از ارزیابی پیامد کسب‌وکار، نمایه‌سازی تهدید و مراحل ارزیابی آسیب‌پذیری ارائه می‌دهد. متخصصان خاطره از این مرحله برای نگاشت/ ترسیم احتمال رویدادهای موفقیت‌آمیز تهدید به مناسب‌ترین سناریوهای پیامد کسب‌وکار استفاده می‌کنند و آن را به چارچوب مخاطره سازمانی پیوند می‌دهند.

- **مرحله ششم – مقابله با مخاطره: تدوین برنامه‌های واقع‌گرایانه مقابله با مخاطره**: راهنمایی واقع‌گرایانه جهت مقابله با مخاطره‌های اطلاعاتی شناسایی شده ارائه می‌دهد. متخصصان مخاطره از این مرحله برای کشف رویکردهای گوناگون جهت مقابله و درمان مخاطره اطلاعات (برای نمونه، کاهش، اجتناب، انتقال و پذیرش) استفاده می‌کنند.

جدول ۳-۲۲. شناسنامه (۱۸): روش IRAM

شناسنامه روش IRAM	
نام اختصاری	آی‌رَم. – IRAM
نام کامل	روش‌های تحلیل مخاطره اطلاعات — Information Risk Analysis Methodologies (IRAM)
ارائه‌دهنده	انجمن امنیت اطلاعات
کشور ارائه‌دهنده	اعضای انجمن بین‌المللی امنیت اطلاعات
وضعیت نسخه	در حال حاضر نسخه (۲۰۱۶) این روش به عنوان آخرین نسخه معتبر محسوب می‌شود.
زبان	انگلیسی
قیمت	غیر رایگان، نیازمند ثبت عضویت است.
دامنه کاربرد/ استفاده	یک رویکرد طراحی شده نظیربه‌نظیر کسب‌وکار محور جهت پاسخگویی به چالش‌های جدید در مدیریت مخاطره و یک روش آسان برای استفاده جهت ارزیابی پیامد کسب‌وکار و تحلیل مخاطره اطلاعات در سیستم‌های اطلاعاتی مهم و نه حیاتی.
هدف	روشی برای تحلیل مخاطره اطلاعات در سیستم‌های اطلاعاتی حیاتی شامل برنامه‌ریزی، شناسایی الزام‌های کسب‌وکار برای امنیت، ارزیابی آسیب‌پذیری‌ها و الزام‌های کنترلی، و گزارش‌دهی. ازجمله اهداف این روش می‌توان به موارد ذیل اشاره نمود: ▪ ایجاد زمینه‌ای برای بالا بردن سطح امنیت اطلاعات سازمان‌ها در سرتاسر جهان از طریق تجربه‌ای برتر ▪ کمک به سازمان‌ها و شرکت‌هایی که عضو ISF نیستند، برای بهبود وضعیت امنیتی خود و کاهش خطرات امنیتی در سطح قابل قبول ▪ کمک عملی به تولیدکنندگان استانداردها برای مشخص کردن نواحی و کاهش مخاطره‌های اطلاعاتی
مراحل مدیریت مخاطره	مراحل تحلیل مخاطره روش IRAM شامل: ۱) ارزیابی پیامد کسب‌وکار، ۲) ارزیابی تهدید و آسیب‌پذیری، ۳) انتخاب کنترل است. مراحل تحلیل مخاطره روش IRAM2 شامل: ۱) تعیین محدوده، ۲) ارزیابی پیامد کسب‌وکار، ۳) پروفایل تهدید، ۴) ارزیابی آسیب‌پذیری، ۵) سنجش مخاطره، ۶) مقابله با مخاطره است.
فرمول محاسبه مخاطره	مخاطره = پیامد (پیامد کسب‌وکار) × احتمال (تهدید، رویداد تهدید، آسیب‌پذیری)
سازگاری با استانداردها	با استاندارد ISO/IEC 17799 سازگار است.
ابزارهای پشتیبان	ابزارهای غیرتجاری مانند فرم‌ها، لیست‌ها و جدول‌های اکسل برای انواع محصولات انجمن امنیت اطلاعات که تنها برای اعضای انجمن قابل دسترس است. ابزارهای الکترونیکی که از این روش پشتیبانی می‌کنند عبارتند از: – IRAM2 Assessment Tool – BIA Assistant – Threat and Vulnerability Assessment Assistant – Control Selection Assistant
مزایا/ نقاط قوت	+ با وجود پیچیدگی از سرعت بالایی برخوردار است؛ + سطح گسترده‌ای از جزئیات را پوشش می‌دهد؛ + ارائه گزارش‌های دقیق از تهدیدها، آسیب‌پذیری‌ها و الزام‌های امنیتی؛ + بسیار ساده، کاربردی و دقیق است؛ + جمع‌آوری اطلاعات از طریق مصاحبه‌های رودرو و پرسش‌نامه؛ + رویکرد فرآیندگرا، ارائه اسناد و ابزارهای پشتیبان، ساده‌سازی و عملیاتی‌کردن کل فرآیند؛ + مشابه روش OCTAVE یک مدل انعطاف‌پذیر و سازگار با سازمان‌های گوناگون؛ + نسبت به روش OCTAVE فنی‌تر است؛ + روشی اقتصادی و بسیار مقرون‌به‌صرفه است؛ + مورد استفاده در صنعت به‌شکل گسترده؛ + شناسایی آسیب‌پذیری‌های سیستم‌های موجود و نیاز به حفاظ‌های ایمنی جهت محافظت در برابر آنها؛ + تعیین الزام‌های امنیتی برای سیستم‌های در حال توسعه و تعیین کنترل‌های نیاز برای برآورده ساختن آنها؛ + مورد استفاده در بسیاری از کشورهای عضو اتحادیه اروپا؛ + از لحاظ پیچیدگی در سطح متوسطی جای دارد؛
معایب/ نقاط ضعف	– نیازمند سطح بالایی از تخصص؛ – نسبت به روش OCTAVE از پیچیدگی بیشتری برخوردار است؛ – ابزارهای الکترونیکی قابلیت گزارش‌دهی خودکار را ندارند؛ – بسیار زمان‌بر است؛ – نیاز به آمادگی بیشتر نسبت به روش OCTAVE؛
وب‌سایت رسمی	https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/

۳-۳. گزیدهٔ فصل

امن‌سازی فضای تبادل اطلاعات سازمان از طریق ارزیابی و مدیریت مخاطرات امنیتی محقق می‌شود. به این معنا که طرح‌ریزی برنامه‌ها و اقدام‌های امنیتی بر پایهٔ نتایج حاصل از فرآیند تحلیل مخاطرات انجام می‌شود. اگرچه بین امنیت اطلاعات و مدیریت مخاطرات رابطه‌ای برقرار است، ولی با این وجود موجودیتی ثابت شده نیست. در طی سال‌های اخیر غالب توجهات به سوی فناوری‌ها، روش‌ها و فنونی معطوف شده که می‌توانند به صورت ملموسی جهت کاهش مخاطرات در فضای تبادل اطلاعات سازمان مورد استفاده قرار گیرند. روش‌های ارزیابی مخاطره در مفهوم کلی آن به ویژه روش سنتی تحلیل مخاطره برای امنیت اطلاعات، مبنایی برای ایجاد، شکل‌گیری و توسعه روش‌های نوین ارزیابی و مدیریت امنیت اطلاعات به شکل خاص ایجاد کرده و موجب شکل‌گیری روش‌های نوین مدیریت مخاطره امنیت اطلاعات شده‌اند.

بر این اساس در این فصل بر پایهٔ فرآیندی شامل چهار گام، شناسایی و معرفی روش‌های مدیریت و ارزیابی مخاطره امنیت اطلاعات به طور خاص مورد توجه قرار گرفت. در گام نخست تعریف پارامترهای کیفی دسته‌بندی جهت تکمیل شناسنامه اسناد پایه، در گام دوم شناسایی اولیه ۵۰ سند پایه (در قالب استاندارد، روش، مدل، چارچوب، راهنما، رهنمود، اصول، و غیره) مدیریت و ارزیابی مخاطره امنیت اطلاعات، در گام سوم ارزیابی و انتخاب ۱۸ سند پایه به‌منظور به منظور معرفی و ارزیابی مقایسه‌ای، و در گام چهارم دسته‌بندی اسناد پایه منتخب در سه گروه به شرح زیر انجام شد:

۱- استانداردهای ملّی و بین‌المللی: شامل ISO/IEC 27000 series، ISO/IEC 31000 series، NIST 800 series، ETSI TVRA، و BSI Standard series؛

۲- چارچوب‌ها و راهنماهای عمومی: شامل Austrian IT Security Handbook، Magerit، Microsoft Security Risk Management، COBIT، و Risk IT؛ و

۳- روش‌ها و مدل‌ها: شامل CORAS، CRAMM، EBIOS، FAIR، FRAAP، MEHARI، OCTAVE، IRAM، و IRAM2.

آنچه در ادامه و در قالب فصل چهارم به آن پرداخته خواهد شد، مقایسه روش‌های مدیریت و ارزیابی مخاطره امنیت اطلاعات است که با مصورسازی روش‌های موجود در قالب ارائه یک چارچوب مقایسه‌ای، میزان سازگاری روش‌ها بر پایهٔ یک سری از معیارهای کیفی و کمّی به تصویر کشیده خواهد شد.

فصل چهارم

مقایسه روش‌های
مدیریت و ارزیابی مخاطره امنیت اطلاعات

۴-۱. مقدمه

مدیریت مخاطره امنیت اطلاعات، تمرین مداوم شناسایی، مرور و رصد مخاطره‌ها جهت دستیابی و نگهداری سطح قابل قبولی از مخاطره است. به شکل کلی، مدیریت مخاطره به عنوان سنگ بنای امنیت اطلاعات مورد توجه است. مدیریت مخاطره به منظور تعیین اینکه چه چیزی و چگونه باید مورد محافظت قرار گیرد، استفاده می‌شود. شیوهٔ برخورد با مدیریت مخاطره در امنیت اطلاعات، موضوع بحثی است که سالهاست توجه محققان را به خود مشغول کرده است. رویکردهای گوناگون موجود در مدیریت مخاطره نشان‌دهنده نگاه‌های گوناگون به این موضوع هستند.

همان طور که در فصل سوم مشاهده شد، تعداد زیادی از انواع اسناد پایه ارزیابی مخاطره امنیت اطلاعات وجود دارد که توسط نهادهای ملّی و بین‌المللی، سازمان‌های حرفه‌ای و طرح‌های پژوهشی منتشر شده است. هر یک از این اسناد برای برآوردن نیازهای خاصی طراحی شده‌اند و اهداف، مراحل، ساختار و سطح کاربرد متفاوتی دارند. هدف مشترک این اسناد 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.

گزارش‌ها، نظرسنجی‌ها و ادبیات گوناگون منتشر شده در این حوزه حاکی از آن است که گسترش روش‌های مدیریت مخاطره در سازمان‌ها به دلیل کمبود آگاهی، هزینه‌های بالا، فرآیند طولانی و میزان تخصص مورد نیاز با محدودیت مواجه است. از یک سو، تنوع در تعداد روش‌های مدیریت مخاطره امنیت اطلاعات سازمان‌ها را در فرآیند انتخاب و بهره‌برداری از این روش‌ها با چالش‌هایی مواجه کرده است. از سوی دیگر نیز، نبود و عدم توافق در معیارهای مرجع مورد تأیید یا چارچوب مقایسه‌ای برای ارزیابی این روش‌ها، کاربرد علمی آنها را در ارزیابی مخاطره‌های امنیت اطلاعات سازمان‌ها محدود کرده است.

از این‌رو در این فصل کوشش شده است نخست با ارائه یک چارچوب مفهومی مبتنی بر معیارهای ارزیابی (مانند ماهیت روش، سازمان هدف، سطح تخصص، پشتیبانی ابزارها، کارایی روش‌ها) اسناد پایه مدیریت و ارزیابی مخاطره امنیت اطلاعات مورد مقایسه قرار گیرند و در ادامه، با مصورسازی روش‌های موجود در قالب ارائه یک چارچوب پیشنهادی، میزان سازگاری روش‌ها بر پایهٔ یک سری از معیارها در قالب طراحی مفهومی و مصورسازی چارچوب مقایسه‌ای به تصویر کشیده خواهد شد. در واقع، هدف از این چارچوب مقایسه‌ای کمک به متخصصان در انتخاب یک روش مناسب جهت مدیریت و ارزیابی مخاطره در حوزه امنیت اطلاعات برای سازمان است.

۴-۲. روش پژوهش

با توجه به اینکه بیشتر سازمان‌ها درصدد اجرای تنها یک و یا ترکیبی از اسناد پایه مدیریت و ارزیابی مخاطره امنیتی هستند که به طور گسترده پذیرفته شده باشد، بدین منظور در ادامه این فصل مقایسه و ارزیابی اسناد پایه مدیریت و ارزیابی مخاطره امنیت اطلاعات مورد توجه قرار گرفته است. مبتنی بر شناسایی و معرفی اسناد پایه در فصل سوم، در این فصل کوشش خواهد شد با دسته‌بندی معیارهای ارزیابی شناسایی شده در ادبیات پژوهش، این امکان برای کاربر فراهم شود که بر پایهٔ میزان اهمیت و تخصیص وزن به هر یک از شاخص‌ها نسبت به انتخاب روش مناسب ارزیابی مخاطره در حوزه امنیت اطلاعات اقدام کند.

در این بخش برای مقایسه اسناد پایه مدیریت و ارزیابی مخاطره و استخراج معیارها و شاخص‌های اولیه، از منابع کتابخانه‌ای و اینترنتی شامل استانداردها، کتاب‌ها، مقاله‌ها، و موردکاوی‌ها استفاده شده است. از این‌رو به منظور یکسان‌سازی ادبیات مورد استفاده در مقایسه اسناد پایه، معیارهای ارزیابی اسناد پایه در قالب (**جدول ۴-۱**) تعریف شده است. به بیان ساده، این جدول بیان می‌کند که برای مقایسه و ارزیابی اسناد پایه، چه معیارهای باید مد نظر قرار گیرد. تعریف آیتم‌های این جدول به شرح زیر است:

- **معیار ارزیابی:** بیانگر این است که هر یک از اسناد پایه بر پایهٔ چه معیارهایی (برای نمونه، سطح کاربری، سطح تخصص، سازمان هدف، و غیره) مورد ارزیابی قرار خواهند گرفت.
- **شاخص ارزیابی:** بیانگر این است که در زمان مقایسه، فرآیند ارزیابی بر چه اساس صورت خواهد گرفت که می‌تواند در قالب هر یک از حالت‌های (تک انتخابی، چندانتخابی و طیف لیکرت) باشد.
- **گزینه‌های ارزیابی:** بیانگر این است که هر یک از معیارهای ارزیابی از چه گزینه‌هایی برای انتخاب (برای نمونه، معیار رویکرد تخمین مخاطره شامل گزینه‌های کمّی، کیفی و ترکیبی) تشکیل شده است.

جدول ۴-۱. معیارهای ارزیابی جهت مقایسه اسناد پایه مدیریت و ارزیابی مخاطره

ردیف	معیار ارزیابی	شاخص ارزیابی	گزینه‌های ارزیابی	شرح معیار	لینک مرجع
۱	نوع	چندانتخابی	استاندارد، راهنما/ دستورالعمل، مدل، روش	تعیین‌کننده یک یا ترکیبی از گونه‌های (استاندارد، راهنما/ دستورالعمل، مدل، روش) است.	(Kiran et al. 2013; Macedo and Da Silva 2012; Behnia, Abd Rashid and Chaudhry 2012)
۲	ماهیت	چندانتخابی	فناوری-محور، کسب‌وکار-محور، دارایی-محور، خدمت-محور، دانش-محور، مدل-محور، نرم‌افزار-محور	تعیین‌کننده فلسفه وجودی روش بر پایهٔ یک یا ترکیبی از حالت‌های (فناوری-محور، کسب‌وکار-محور، دارایی-محور، خدمت-محور، دانش-محور، مدل-محور، نرم‌افزار-محور) است.	(Spears 2004; Wangen and Snekkenes 2013; Shameli-Sendi, Aghababaei-Barzegar and Cheriet 2016; Pan and Tomlinson 2016; Agrawal 2017; Ionita 2013)
۳	سازمان ارائه‌دهنده	تک انتخابی	نهاد(های) بین‌المللی، نهادهای دولتی (ملّی)، نهاد(های) خصوصی، نهاد(های) دانشگاهی	نوع نهاد ارائه‌دهنده روش را بر پایهٔ یکی از انواع (بین‌المللی، دولتی/ ملّی، خصوصی، دانشگاهی) نشان می‌دهد.	(Saleh and Alfantookh 2011; Kiran et al. 2013; Macedo and Da Silva 2012; (Shamala, Ahmad and Yusoff 2013)
۴	اندازه سازمان هدف	چندانتخابی	سازمان‌های بزرگ، SMEs	تعیین‌کننده نوع سازمان هدف (از لحاظ اندازه یا بزرگی سازمان) بر پایهٔ یک یا ترکیبی از حالت‌های (سازمان‌های بزرگ، SMEs) است.	(Ionita 2013)
۵	سطح کاربری	چندانتخابی	مدیریتی، عملیاتی، فنی	تعیین‌کننده نوع کاربری روش بر پایهٔ یک یا ترکیبی از حالت‌های (مدیریتی، عملیاتی، فنی) است.	(Wangen and Snekkenes 2013; Wangen and Snekkenes 2013; Ionita 2013)
۶	سطح تخصص/ مهارت مورد نیاز	چندانتخابی	تخصص بالا (متخصص)، تخصص متوسط (استاندارد)، تخصص کم (پایه)	سطح تخصص/ مهارت موردنیاز برای انجام هر یک از اسناد پایه را نشان می‌دهد.	(Wangen and Snekkenes 2013; Kiran et al. 2013; Agrawal 2017; Ionita 2013; Behnia, Abd Rashid and Chaudhry 2012)
۷	پشتیبانی از مراحل مدیریت مخاطره	چندانتخابی	پایه‌گذاری محتوا، ارزیابی مخاطره، مقابله با مخاطره، پذیرش مخاطره، ارتباطات مخاطره، پایش و بازبینی مخاطره	تعیین‌کننده مراحلی است که اسناد پایه در فرآیند مدیریت مخاطره از آنها پشتیبانی می‌کند.	(Wangen and Snekkenes 2013; Sulaman, Weyns and Höst 2013; Kiran et al. 2013; Agrawal 2017; Zudin 2014; Macedo and Da Silva 2012; (Shamala, Ahmad and Yusoff 2013)
۸	پشتیبانی از مراحل ارزیابی مخاطره	چندانتخابی	شناسایی مخاطره، تحلیل مخاطره، سنجش مخاطره	تعیین‌کننده مراحلی است که اسناد پایه در فرآیند ارزیابی مخاطره از آنها پشتیبانی می‌کند.	(Kiran et al. 2013; Macedo and Da Silva 2012; Macedo and Da Silva 2012; Shamala, Ahmad and Yusoff 2013; Ionita 2013)
۹	رویکرد تخمین مخاطره	تک انتخابی	کمّی، کیفی، ترکیبی	تعیین‌کننده روش تخمین/ برآورد مخاطره بر پایهٔ یکی از حالت‌های (کمّی، کیفی و یا ترکیبی) است.	(Spears 2004; Wangen and Snekkenes 2013; Shameli-Sendi, Aghababaei-Barzegar and Cheriet 2016; (Sulaman, Weyns and Höst 2013; Macedo and Da Silva 2012; Bornman and Labuschagne 2004; Kiran et al. 2013; Pan and Tomlinson

					2016; Agrawal 2017; Nosworthy 2000; Zudin 2014; Shamala, Ahmad and Yusoff 2013; Ionita 2013; Behnia, Abd Rashid and Chaudhry 2012; Wangen 2017; SESAR 2011)
۱۰	شیوه ارزیابی	چندانتخابی	خودارزیابی، مصاحبه، کارگاه آموزشی	تعیین‌کننده روش ارزیابی بر پایهٔ یک یا ترکیبی از حالت‌های (خودارزیابی، مصاحبه و یا کارگاه آموزشی) است.	(Kiran et al. 2013; Macedo and Da Silva 2012)
۱۱	پشتیبانی ابزارها	چندانتخابی	رایگان، ابزار پولی به‌همراه نسخه آزمایشی، ابزار پولی بدون نسخه آزمایشی، نداشتن ابزار نرم‌افزاری، نداشتن ابزار و اسناد پشتیبان	تعیین‌کننده پشتیبانی ابزارها از اسناد پایه است.	(Wangen and Snekkenes 2013; Agrawal 2017; Macedo and Da Silva 2012; Ionita 2013; (Behnia, Abd Rashid and Chaudhry 2012; SESAR 2011)
۱۲	پشتیبانی از زبان‌های رایج	طبف لیکرت پنج ارزشی	بسیار زیاد، زیاد، متوسط، کم، خیلی کم	تعیین‌کننده تعداد زبان‌هایی است که روش از آنها پشتیبانی می‌کند.	(Agrawal 2017; Ionita 2013; Behnia, Abd Rashid and Chaudhry 2012; Agrawal 2017)
۱۳	میزان سازگاری با استانداردها و مستندات پایه	طبف لیکرت پنج ارزشی	بسیار زیاد، زیاد، متوسط، کم، خیلی کم	میزان تطابق با قوانین، مقررات، استانداردها، دستورالعمل‌ها و غیره را نشان می‌دهد.	(Saleh and Alfantookh 2011; Spears 2004; (Ionita 2013; Agrawal 2017; Behnia, Abd Rashid and Chaudhry 2012; SESAR 2011)
۱۴	پوشش تعاریف و اصطلاحات (واژه‌نامه)	طبف لیکرت پنج ارزشی	بسیار زیاد، زیاد، متوسط، کم، خیلی کم	تعیین‌کننده میزان پوشش‌دهی تعاریف و اصطلاحات مورد استفاده در روش است به طوری که کاربر بدون نیاز به دانستن اصطلاحات خاص بتواند از آن استفاده کند.	(Macedo and Da Silva 2012; Spears 2004; Zudin 2014; Ionita 2013; SESAR 2011)
۱۵	نوع دسترسی	تک انتخابی	آزاد، باهزینه	نوع دسترسی به اسناد پایه را بر پایهٔ یکی از حالت‌های (دسترسی با هزینه و دسترسی آزاد) نشان می‌دهد.	(Zudin 2014; Macedo and Da Silva 2012; Ionita 2013; Spears 2004; Agrawal 2017; SESAR 2011; Kiran et al. 2013)
۱۶	کارایی: سرعت	طبف لیکرت پنج ارزشی	بسیار زیاد، زیاد، متوسط، کم، خیلی کم	زمان درنظر گرفته شده جهت انجام فرآیند تحلیل و ارزیابی مخاطره را نشان می‌دهد.	(Spears 2004; Zudin 2014; Macedo and Da Silva 2012; SESAR 2011; Ionita 2013; Kiran et al. 2013; Agrawal 2017)
۱۷	کارایی: سهولت استفاده/ کاربری آسان	طبف لیکرت پنج ارزشی	بسیار زیاد، زیاد، متوسط، کم، خیلی کم	میزان سادگی، آسانی و راحتی درک و استفاده را نشان می‌دهد.	
۱۸	کارایی: فرآیند روشن و شفاف مراحل	طبف لیکرت پنج ارزشی	بسیار زیاد، زیاد، متوسط، کم، خیلی کم	میزان شفافیت مراحل و چگونگی اجرای هر مرحله را نشان می‌دهد.	
۱۹	کارایی: تکرارپذیری	طبف لیکرت پنج ارزشی	بسیار زیاد، زیاد، متوسط، کم، خیلی کم	میزان قابلیت تکرارپذیری و مقایسه نتایج ارزیابی با دیگر روش‌ها (اسناد پایه) را نشان می‌دهد.	

۴-۳. مقایسه اسناد پایه مدیریت و ارزیابی مخاطره

در این بخش، اسناد پایه مدیریت و ارزیابی مخاطره تعریف شده در فصل سوم بر پایهٔ معیارهای ارزیابی -نوع، ماهیت، سازمان ارائه‌دهنده، اندازه سازمان هدف، سطح کاربری، سطح تخصص، فرآیند تطبیق مراحل مدیریت و ارزیابی مخاطره، رویکردهای تخمین مخاطره، شیوه ارزیابی مخاطره، پشتیبانی ابزارها، پشتیبانی از زبان‌های رایج، میزان سازگاری با استانداردها و مستندات، پوشش تعاریف و اصطلاحات، کارایی رویکردهای ارزیابی- ارائه شده در (**جدول ۴-۱**) مورد مقایسه قرار خواهند گرفت. به منظور برداشت یکسان از گزینه‌های سنجش، پیش از مقایسه اسناد منتخب، هر یک از آنها معرفی و تعریف شده است. شایان ذکر است در این چارچوب ارزیابی، در بسیاری از معیارها، اسناد پایه می‌توانند در چند گزینه ارزیابی جای گیرند و لزوم بر قرارگیری آنها در یک گزینه ارزیابی نیست. برای نمونه، می‌توان به ISO 27005 اشاره کرد که هم استاندارد است و هم راهنما/ دستورالعمل.

۴-۳-۱. نوع سند پایه ارزیابی مخاطره

همان طور که در فصل سوم بیان شد، از اصطلاح **سند پایه** به جای روش در فرآیند شناسایی، دسته‌بندی و ارزیابی استفاده شده است. هر یک از اسناد پایه مدیریت و ارزیابی مخاطره نشان‌دهنده یک یا ترکیبی از گونه‌های استاندارد، چارچوب، روش، راهنما/ دستورالعمل، اصول و رهنمودهایی هستند (**جدول ۴-۲**) که در ادامه توضیح مختصری در ارتباط با هر یک از این گونه‌ها ارائه شده است.

- **استاندارد**: مجموعه‌ای از قوانین شناخته‌شده که چگونگی توسعه و مدیریت مواد، محصولات، خدمات، فناوری‌ها، وظایف، فرآیندها و سیستم‌ها توسط افراد را کنترل می‌کند.
- **راهنما/ دستورالعمل**: توصیه یا دستورالعمل داده‌شده به‌منظور هدایت یا راهنمایی یک عملیات است.
- **روش/ مدل**، به عنوان یک ترتیب منظم و نظام‌مند از مراحل انجام کار برای رسیدن به نقطه پایان تعریف می‌شود و الگوهایی هستند برای نمایش کنترل شده یک پدیده واقعی و با ساختار تعریف شده (شناسایی، تحلیل، ارزیابی) که در زیرمجموعه روش‌شناسی یک طرح قابل استفاده می‌باشند تا از طریق آنها نتایج نزدیک‌تر به واقعیت قابل استنباط باشند.

جدول ۴-۲. نوع سند پایه مدیریت و ارزیابی مخاطره

ردیف	نام سند	معیار نوع		
		استاندارد	راهنما/دستورالعمل	روش/ مدل
۱	ISO 27005	✓	✓	
۲	ISO 31000	✓	✓	
۳	NIST 800-30	✓	✓	
۴	BSI Standard 200-3	✓		
۵	TVRA	✓		✓
۶	Austrian IT		✓	
۷	MAGERIT		✓	✓
۸	Microsoft		✓	
۹	COBIT-5 for Risk		✓	
۱۰	Risk IT		✓	✓
۱۱	CORAS			✓
۱۲	CRAMM			✓
۱۳	EBIOUS			✓
۱۴	FAIR			✓
۱۵	FRAAP			✓

ردیف	نام سند	معیار نوع		
		استاندارد	راهنما/دستورالعمل	روش/ مدل
۱۶	MEHARI			✓
۱۷	OCTAVE (S) , (ALLEGRO)			✓
۱۸	IRAM			✓

۴-۳-۲. ماهیت سند پایه ارزیابی مخاطره

فلسفه وجودی اسناد پایه مدیریت و ارزیابی مخاطره بر پایهٔ یک یا ترکیبی از حالت‌های (فناوری‌محور، کسب‌وکارمحور، دارایی‌محور، خدمت‌محور، دانش‌محور، مدل‌محور، نرم‌افزارمحور) است که در قالب **(شکل ۴-۱)** نشان داده شده است. سازمان‌ها می‌توانند در سطوح گوناگونی مخاطرات امنیت اطلاعات را مورد بررسی و ارزیابی قرار دهند.

شکل ۴-۱. ماهیت اسناد پایه ارزیابی مخاطره

هر یک از این سطوح به تفکیک در ادامه توضیح داده شده‌اند:

- **دارایی‌محور**: در این سطح، ابتدا تهدیدها و آسیب‌پذیری‌های هر دارایی شناسایی می‌شود و سپس سناریوهای مخاطره شکل می‌گیرد. نقطه ضعف اصلی این سطح، ایجاد خستگی و احتمال بُروز خطا با توجه به تعدد سناریوهای مخاطره است که به ازای هر دارایی اطلاعاتی شکل می‌گیرد. مزیت اصلی این سطح فهم و درک آسان آن است و با توجه به کاربرد گسترده این سطح، اکثر ابزارهای موجود در بازار مبتنی بر این دیدگاه طراحی شده است.
- **خدمت‌محور**: در این دیدگاه مخاطره‌ها شناسایی و بر پایهٔ میزان پیامد/ تأثیر بر روی خدمات مورد ارزیابی قرار می‌گیرند. در این دیدگاه، تمامی خدمات مهم سازمان شناسایی می‌شود و برخلاف دیدگاه دارایی‌محور تهدیدها و آسیب‌پذیری‌ها به ازای هر خدمت و نه به ازای یک دارایی مستقل شناسایی می‌شوند. معمولاً زمانی که تعداد خدمات در یک سازمان از تعداد دارایی‌ها کمتر است، رویکرد خدمت‌محور برای بکارگیری و مدیریت گزینه مناسب و آسان‌تری است.
- **کسب‌وکارمحور**: این دیدگاه مبتنی بر اهداف کسب‌وکار و فرآیندهای پشتیبان این اهداف عمل می‌کند. تمرکز اصلی این دیدگاه بر شناسایی و تحلیل فرآیندهای کسب‌وکار و ارتباط آنها با آسیب‌پذیری‌ها و تهدیدها است. با توجه به ارتباط مستقیم این دیدگاه با اهداف سازمان، امکان تشریح آن به مدیریت ارشد بسیار ساده‌تر است.
- **فناوری‌محور**: این دیدگاه بر روی تهدیدهای شناخته شده انواع دارایی‌های رایانشی مورد استفاده در سازمان متمرکز است. تمرکز اصلی این دیدگاه بر فناوری و عدم دخالت کاربران است و به افراد و فرآیندها توجه کمتری دارد. از این دیدگاه بیشتر در روش‌های سنتی مدیریت و ارزیابی مخاطره استفاده می‌شود.
- **دانش‌محور**: این دیدگاه دارایی‌ها، تهدیدها و آسیب‌پذیری‌های سیستم‌های اطلاعاتی را بر پایهٔ دانش ارزیابی می‌کند. پایگاه دانش این رویکرد شامل قوانین اساسی و قوانین خاص است. قوانین اساسی به عنوان قوانین بی‌تأثیر بر روابط خارجی تعریف می‌شوند، در حالی‌که قوانین خاص به قوانینی گفته می‌شود که مخصوص یک سازمان است. این دیدگاه باعث افزایش کارایی می‌شود و اطمینان از ارزیابی مخاطره را به همراه دارد.

- **مدل‌محور:** از یک مدل معماری اطلاعات -روشی برای تخصیص ارزش‌ها به دارایی‌های اطلاعاتی و مؤلفه‌های فناوری اطلاعات- و روشی برای محاسبه مخاطره‌ها استفاده می‌کند. روش مدل‌محور یا معماری‌محور، امکانات بیشتر و با ارزش‌تری را برای تحلیل سیستم‌های پیچیده فراهم می‌کند.
- **نرم‌افزارمحور:** روش‌های مبتنی بر نرم‌افزار شامل یک قالب/ چارچوب غیرقابل انعطاف است. با توجه به اینکه چارچوب اصلی فرآیند تحلیل مخاطره توسط نرم‌افزار ترسیم می‌شود، به همین دلیل در طول فرآیند تحلیل مخاطره که در آن از نرم‌افزار استفاده می‌شود ممکن است تغییرات لازم اعمال و حاصل نشود. ازجمله معایب این رویکرد می‌توان به هزینه بالا آن اشاره کرد.

امروزه، بسیاری از ابزارها و روش‌های نوین ارزیابی مخاطره "مبتنی بر دارایی" هستند، بدین معنی که آنها از طریق ارزش دارایی‌ها (داده‌ها، اطلاعات یا منابع) یک سازمان کل فرآیند ارزیابی مخاطره را انجام می‌دهند، ولی در مطالعات جدید این تغییر حاصل شده است که کار بر روی سطح خدمات و یا سطح فرآیند کسب‌وکار بسیار آسان‌تر و دقیق‌تر است. در واقع اسناد پایه می‌توانند رویکردهای چندگانه‌ای داشته باشند و لزوم بر قرارگیری آنها در یک رویکرد ارزیابی نیست. (**جدول ۴-۳**) ماهیت وجودی هر یک از اسناد پایه را در قالب انتخاب یک یا چند حالت از سطوح (فناوری‌محور، کسب‌وکارمحور، دارایی‌محور، خدمت‌محور، دانش‌محور، مدل‌محور، نرم‌افزارمحور) نشان می‌دهد.

جدول ۴-۳. ماهیت سند پایه مدیریت و ارزیابی مخاطره

ردیف	نام سند	معیار ماهیت						
		فناوری‌محور	کسب‌وکارمحور	دارایی‌محور	خدمت‌محور	دانش‌محور	مدل‌محور	نرم‌افزارمحور
۱	ISO 27005		✓	✓				
۲	ISO 31000	✓	✓					
۳	NIST 800-30		✓	✓				
۴	BSI Standard 200-3	✓	✓	✓				
۵	TVRA		✓	✓			✓	
۶	Austrian IT	✓	✓	✓				✓
۷	MAGERIT	✓	✓	✓				
۸	Microsoft	✓	✓	✓				
۹	COBIT-5 for Risk	✓	✓	✓	✓	✓		✓
۱۰	RISK IT		✓		✓			
۱۱	CORAS			✓			✓	
۱۲	CRAMM			✓			✓	✓
۱۳	EBIOUS		✓		✓			
۱۴	FAIR		✓	✓			✓	
۱۵	FRAAP		✓	✓				✓
۱۶	MEHARI		✓	✓		✓		
۱۷	OCTAVE (S) , (ALLEGRO)		✓	✓				
۱۸	IRAM	✓	✓	✓				

۴-۳-۳. سازمان ارائه‌دهنده سند پایه ارزیابی مخاطره

هریک از اسناد پایه تحت نظارت یک نهاد بین‌المللی، ملّی-دولتی، خصوصی و یا دانشگاهی تدوین شده است. منظور از هر یک از این نهادها عبارت است از:

- **نهاد بین‌المللی**: سازمان بین‌المللی، از نظر حقوق بین‌الملل، سازمانی است که عضوهای آن دولت‌ها هستند.

- **نهاد ملّی-دولتی**: نهاد ملّی، به معنای نهادی است که در قالب یک نهاد عمومی فعالیت می‌کند و به طور خاص توسط دفتر مرکزی ملّی آن کشور به رسمیت شناخته شده است. در واقع، تحت مالکیت یا کنترل از سوی دولت یک کشور یا ملت است.
- **نهاد خصوصی**: نهاد خصوصی، به معنای هر نهادی غیر از نهاد عمومی است که می‌تواند شامل یک مشارکت/ همکاری، یک شرکت سهامی عام، یک سازمان غیرانتفاعی، یک شرکت یا هر گروه سازمان‌یافته دیگری باشد که وابسته به دولت نیست.
- **نهاد دانشگاهی**: نهاد دانشگاهی -برای نمونه، دانشگاه، پژوهشگاه یا کالج- نهادی است که به طور مستقل و جدا از دیگر نهادهای مشابه اداره می‌شود و قوانین و فرآیندهای کسب‌وکار مخصوص به خود را دارد.

(**جدول ۴-۴**) سازمان ارائه‌دهنده هر یک از اسناد پایه را در قالب یک یا چند حالت انتخابی (نهاد بین‌المللی، نهاد ملّی-دولتی، نهاد خصوصی، نهاد دانشگاهی) نشان می‌دهد.

جدول ۴-۴. سازمان ارائه‌دهنده سند پایه مدیریت و ارزیابی مخاطره

ردیف	نام سند	معیار سازمان ارائه‌دهنده			
		نهاد(های) بین‌المللی	نهاد(های) دولتی/ ملّی	نهاد(های) خصوصی	نهاد(های) دانشگاهی
۱	ISO 27005	✓			
۲	ISO 31000	✓			
۳	NIST 800-30	✓			
۴	BSI Standard 200-3		✓		
۵	TVRA	✓			
۶	Austrian IT		✓		
۷	MAGERIT		✓		
۸	Microsoft		✓		
۹	COBIT-5 for Risk	✓			
۱۰	IT RISK	✓			
۱۱	CORAS	✓	✓	✓	✓
۱۲	CRAMM	✓			
۱۳	EBIOUS		✓		
۱۴	FAIR	✓			
۱۵	FRAAP			✓	✓
۱۶	MEHARI		✓		
۱۷	OCTAVE (S) , (ALLEGRO)	✓			
۱۸	IRAM	✓			

۴-۳-۴. اندازه سازمان هدف سند پایه ارزیابی مخاطره

معیارهای متفاوتی برای تعریف اندازه سازمان به کار گرفته شده است. برخی از معیارها از تعداد کارکنان بهره می‌گیرند و برخی دیگر معیارهایی همچون ابعاد مالی و عملکردی را به کار می‌گیرند. هرچند بیشتر تعریف‌ها بر پایهٔ تعداد کارکنان بیان می‌شوند، در ایران بر پایهٔ تعریف بانک مرکزی، واحدهایی که تعداد کارکنان آن کمتر از ۵۰ نفر باشد صنایع کوچک، با ۵۰ نفر تا ۲۵۰ نفر کارمند، صنایع متوسط و بیش از آن صنایع بزرگ نامیده می‌شوند (Central Bank 2014). در این پژوهش، با بهره‌برداری از تعریف بانک مرکزی جمهوری اسلامی ایران شرکت‌های صنعتی زیر ۵۰ نفر، کوچک و بیشتر از آن بزرگ فرض می‌شوند.

- **سازمان‌ها/ شرکت‌های بزرگ**: برای شرکت‌هایی با بیش از ۲۵۰ کارمند مفید و قابل استفاده است.

- **سازمان‌ها/ شرکت‌های کوچک و متوسط**[1] (SMEs): برای کلیه بنگاه‌های کوچک و متوسط که توانایی پرداخت هزینه مربوط به پرسنل مدیریت مخاطره و یا تفکیک کامل وظایف و مسئولیت‌ها را ندارد، مناسب است.

هر یک از اسناد پایه با سطح و اندازه خاصی از سازمان (سازمان بزرگ، سازمان کوچک-متوسط) سازگاری دارند. (**جدول ۴-۵**) اندازه سازمان متناسب با هر یک از اسناد پایه را نشان می‌دهد.

جدول ۴-۵. سازمان هدف سند پایه مدیریت و ارزیابی مخاطره

ردیف	نام سند	معیار سازمان هدف	
		سازمان‌ها/ شرکت‌های بزرگ	SMEs
۱	ISO 27005	✓	✓
۲	ISO 31000	✓	✓
۳	NIST 800-30	✓	✓
۴	BSI Standard 200-3	✓	✓
۵	TVRA	✓	
۶	Austrian IT		✓
۷	MAGERIT	✓	✓
۸	Microsoft	✓	✓
۹	COBIT-5 for Risk	✓	✓
۱۰	RISK IT	✓	✓
۱۱	CORAS	✓	✓
۱۲	CRAMM	✓	
۱۳	EBIOUS	✓	✓
۱۴	FAIR	✓	✓
۱۵	FRAAP		✓
۱۶	MEHARI	✓	✓
۱۷	OCTAVE (S) , (ALLEGRO)	✓	✓
۱۸	IRAM	✓	✓

۴-۳-۵. سطح کاربری سند پایه ارزیابی مخاطره

هر یک از اسناد پایه ارزیابی مخاطره بر پایهٔ یک و یا ترکیبی از سطوح مدیریتی، عملیاتی و فنی تدوین شده است.

- **سطح مدیریتی**: دستورالعمل‌ها/ رهنمودهای عمومی را در اختیار قرار می‌دهد.
- **سطح عملیاتی**: دستورالعمل‌ها/ رهنمودهایی را برای برنامه‌ریزی و پیاده‌سازی با جزئیات کم ارائه می‌دهد.
- **سطح فنی**: دستورالعمل‌ها/ رهنمودهای خاص مربوط به جنبه‌های فنی، سازمانی، فیزیکی و انسانی امنیت فناوری اطلاعات را با جزئیات زیاد ارائه می‌دهد.

سطح کاربری هر یک از اسناد پایه بر پایهٔ یک یا چند حالت از گزینه‌های ارزیابی (سطح مدیریتی، سطح عملیاتی، سطح فنی) در قالب (**جدول ۴-۶**) نشان داده شده است.

[1] Small and mid-size enterprises (SMEs)

جدول ۴-۶. سطح کاربری سند پایه مدیریت و ارزیابی مخاطره

ردیف	نام سند	معیار سطح کاربری		
		مدیریتی	عملیاتی	فنی
۱	ISO 27005	✓	✓	
۲	ISO 31000	✓	✓	✓
۳	NIST 800-30		✓	✓
۴	BSI Standard 200-3	✓	✓	✓
۵	TVRA	✓	✓	✓
۶	Austrian IT	✓	✓	
۷	MAGERIT	✓	✓	✓
۸	Microsoft	✓	✓	✓
۹	COBIT-5 for Risk	✓	✓	✓
۱۰	RISK IT	✓	✓	
۱۱	CORAS	✓	✓	✓
۱۲	CRAMM	✓	✓	✓
۱۳	EBIOUS	✓	✓	
۱۴	FAIR	✓	✓	
۱۵	FRAAP	✓	✓	
۱۶	MEHARI	✓	✓	✓
۱۷	OCTAVE (S) , (ALLEGRO)	✓	✓	
۱۸	IRAM	✓	✓	✓

۴-۳-۶. سطح تخصص/ مهارت مورد نیاز سند پایه ارزیابی مخاطره

سه گونه مهارت در اسناد پایه مدیریت و ارزیابی مخاطره در نظر گرفته شده‌اند که عبارتند از:

- **معرفی:** به مهارت‌های مورد نیاز جهت درک وابستگی بین جزئیات خاص از محصول اشاره دارد. برای نمونه، مفاهیم گوناگون پشتیبانی شده، مراحل، فعالیت‌ها، و غیره.
- **استفاده:** به تخصص‌ها و مهارت‌های خاصی اشاره می‌کند که جهت انجام کارهای جاری نیاز است. برای نمونه، اسناد قابل فهم و کاربری آسان.
- **نگهداری:** به تخصص‌ها و مهارت‌های خاصی جهت حفظ و نگهداری چرخه عمر محصول اشاره می‌کند. برای نمونه، سفارشی‌سازی، متناسب‌سازی یا انجام منظم به‌روزرسانی‌ها.

برای هر گونه، سطح مهارت‌ها بر پایهٔ مقیاس زیر دسته‌بندی می‌شوند:

- **تخصص کم (پایه)**: بیانگر تجربه و حس مشترک است.
- **تخصص متوسط (استاندارد)**: بیانگر این است که چند روز یا هفته برای آموزش کافی و مناسب است.
- **تخصص بالا (متخصص)**: بیانگر تجربه و دانش کامل مورد نیاز است.

سطح تخصص/ مهارت نیاز هر یک از اسناد پایه در قالب (**جدول ۴-۷**) بر پایهٔ یکی از گزینه‌های ارزیابی (سطح پایه، سطح استاندارد، سطح متخصص) نشان داده شده است.

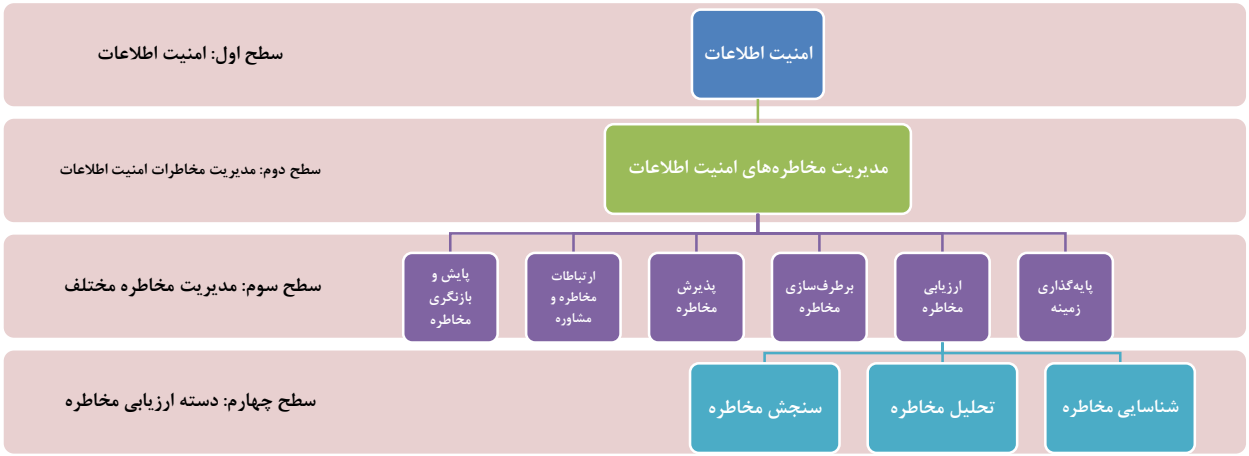
جدول ۴-۷. سطح تخصص/ مهارت روش مدیریت و ارزیابی مخاطره

ردیف	نام سند	معیار سطح تخصص/ مهارت		
		تخصص بالا (متخصص)	تخصص متوسط (استاندارد)	تخصص کم (پایه)
۱	ISO 27005		✓	
۲	ISO 31000		✓	
۳	NIST 800-30		✓	
۴	BSI Standard 200-3		✓	
۵	TVRA	✓		
۶	Austrian IT		✓	
۷	MAGERIT	✓	✓	✓
۸	Microsoft		✓	
۹	COBIT-5 for Risk	✓	✓	✓
۱۰	IT RISK		✓	
۱۱	CORAS	✓	✓	
۱۲	CRAMM	✓		
۱۳	EBIOUS		✓	
۱۴	FAIR			✓
۱۵	FRAAP	✓	✓	✓
۱۶	MEHARI		✓	
۱۷	OCTAVE (S) , (ALLEGRO)	✓	✓	✓
۱۸	IRAM	✓	✓	

۴-۳-۷. فرآیند تطبیق مراحل مدیریت و ارزیابی مخاطره امنیت اطلاعات بر اساس استاندارد ISO/IEC 27005

در این بخش، از استاندارد ISO/IEC 27005 برای به دست آوردن یک روش کلی مدیریت و ارزیابی مخاطره امنیت اطلاعات استفاده شده است. با بررسی فعالیت‌های پژوهشی و شناسایی مشکلات و راهکارهای بالقوه در مدیریت مخاطره در این روش کلی، این بخش به دنبال پشتیبانی از بیشتر روش‌های مدیریت مخاطره امنیت اطلاعات است. یکی از مهم‌ترین اجزای سازنده سیستم مدیریت امنیت اطلاعات، فرآیند مدیریت و ارزیابی مخاطره است. در فرآیند مدیریت مخاطره امنیت اطلاعات، پس از اجرای مراحلی چون شناسایی، تحلیل و سنجش مخاطره که به شکل کلی، در یک دسته کلان‌تر با عنوان ارزیابی مخاطره جای می‌گیرند، باید چگونگی و راهبرد برخورد با مخاطره‌های کشف شده، تعیین شود. خروجی حاصل از مرحله ارزیابی مخاطره، سناریوهای مخاطره‌ای هستند که در محدوده‌های متفاوتی نظیر قابل قبول و یا غیرقابل قبول برای سازمان دسته‌بندی می‌شوند.

دربارهٔ فرآیند مدیریت مخاطره یا مخاطرات امنیت اطلاعات، روش‌های بسیاری وجود دارد که هر یک با توجه به رویکرد مد نظر خود، گام‌هایی را برای انجام روند ارزیابی و مقابله با مخاطره تعریف می‌کنند. اما در عمده این روش‌ها برخی اصول و مفاهیم پایه یکسان در نظر گرفته می‌شود. (**شکل ۴-۲**) مراحل گوناگون این فرآیند که اغلب به شکل مشترک در روش‌های معتبر مدیریت مخاطره امنیت اطلاعات دیده می‌شوند را نشان می‌دهد.



شکل ۴-۲. مراحل مدیریت و ارزیابی مخاطره

مدیریت مخاطره به سازمان‌ها این امکان را می‌دهد که نقاط ضعف و تهدیدهای امنیتی خود را شناسایی و متناسب با مخاطره‌های تعیین شده، روش مناسب جهت مقابله با آنها را اتخاذ کنند. اما چگونه می‌توان برنامه‌ریزی کاملی جهت پیاده‌سازی فرآیند مدیریت مخاطره انجام داد و چه راهکارهایی برای انجام صحیح این فرآیند وجود دارد؟ جهت پاسخ به این پرسش و سنجش مراحل مدیریت و ارزیابی مخاطره دیگر روش‌های شناسایی شده ارزیابی مخاطره، از استاندارد ISO/IEC 27005 استفاده شده است.

۴-۳-۷-۱. پشتیبانی از مراحل مدیریت مخاطره

یکی از اصلی‌ترین و کلیدی‌ترین مفاهیم در استقرار و ارتقای سیستم‌های مدیریت امنیت اطلاعات، مدیریت مخاطره است که در واقع، به یک فرآیند چندمرحله‌ای شامل شناسایی، تحلیل، ارزیابی، اولویت‌بندی و کاهش مخاطره در زمان و موقعیت مناسب اشاره دارد.

هر یک از رویکردهای شناسایی شده ترکیبی از چند مرحله از فرآیند مدیریت مخاطره را پشتیبانی می‌کنند. فرآیند مدیریت مخاطره از شش مرحله پایه‌گذاری محتوا، ارزیابی مخاطره، مقابله با مخاطره، پذیرش مخاطره، تبادل اطلاعات و رایزنی مخاطره و در نهایت پایش و بازنگری مخاطره تشکیل شده است که در ادامه به هر یک از زیرفرآیندهای این مراحل به صورت خلاصه‌ای اشاره‌ای شده است.

- **پایه‌گذاری زمینه:** در این مرحله زمینه داخلی و خارجی مدیریت مخاطره امنیت اطلاعات پایه‌گذاری می‌شود که شامل تنظیم معیارهای بنیادی برای مدیریت مخاطره امنیت اطلاعات است. موارد زیر در این مرحله مد نظر قرار می‌گیرد:
  - تعیین رویکرد و روش مدیریت مخاطره؛
  - تعیین معیارهای ارزیابی مخاطره؛
  - تعیین معیارهای پیامد؛
  - تعیین معیارهای پذیرش مخاطره؛
  - تعریف محدوده و قلمرو مدیریت مخاطره امنیت اطلاعات؛ و
  - سازماندهی.
- **ارزیابی مخاطره:** به شکل کلی، فعالیت‌های مربوط با مدیریت مخاطره با ارزیابی مخاطره آغاز می‌گردد. در واقع، این مرحله، خود شامل سه زیربخش با نام‌های شناسایی مخاطره، تحلیل مخاطره و سنجش مخاطره است که در بخش (۴-۳-۷-۲) به تفصیل به آن پرداخته شده است.
- **برطرف‌سازی مخاطره**: در این مرحله سازمان باید راهبرد و برنامه خود برای برخورد و مقابله با مخاطره‌های پذیرش نشده را تعیین کند. مهمترین خروجی این بخش طرح مقابله با مخاطره[1] (RTP) است که در آن سازمان ضمن اولویت‌بندی

[1] Risk Treatment Plan (RTP)

مخاطره‌ها، هر یک از اقدامات مد نظر خود را به منظور مقابله با آنها تشریح می‌کند. به منظور مقابله با مخاطره چهار رویکرد وجود دارد که عبارتند از:

- اصلاح مخاطره؛
- حفظ مخاطره؛
- اجتناب از مخاطره؛ و
- انتقال (اشتراک) مخاطره.

- **پذیرش مخاطره**: در این مرحله تصمیم‌گیری در خصوص پذیرش مخاطره امنیت اطلاعات صورت می‌گیرد. باید توجه داشت که تصمیمات مرتبط با پذیرش مخاطره و نیز مسئولیت تصمیم‌گیری باید به طور رسمی ثبت شود.
- **ارتباطات مخاطره و مشاوره**: اطلاعات مرتبط با مخاطره باید بر پایهٔ سطوح مناسب دسترسی در سازمان مبادله و یا مابین تصمیم‌گیران و دیگر ذی‌نفعان به اشتراک گذاشته شود.
- **پایش و بازنگری مخاطره**: مخاطره و دیگر مؤلفه‌های درگیر در فرآیند مدیریت مخاطره امنیت اطلاعات (مانند ارزش دارایی‌ها، پیامدها، تهدیدها، آسیب‌پذیری‌ها، احتمال وقوع) به منظور شناسایی تغییرات محتمل در سازمان و برای حفظ صحت و دقت ارزیابی‌های صورت گرفته در طول زمان باید مورد پایش و بازنگری قرار گیرند.

(**جدول ۴-۸**) پشتیبانی اسناد پایه از هر یک از مراحل مدیریت مخاطره (پایه‌گذاری زمینه، ارزیابی مخاطره، برطرف‌سازی مخاطره، پذیرش مخاطره، ارتباطات مخاطره و مشاوره، پایش و بازنگری مخاطره) را بر پایهٔ استاندارد ISO/IEC 27005 نشان می‌دهد.

جدول ۴-۸. پشتیبانی از مراحل مدیریت مخاطره

ردیف	نام سند	معیار پشتیبانی از مراحل مدیریت مخاطره					
		پایه‌گذاری زمینه	ارزیابی مخاطره	برطرف‌سازی مخاطره	پذیرش مخاطره	ارتباطات مخاطره و مشاوره	پایش و بازنگری مخاطره
۱	ISO 27005	✓	✓	✓	✓	✓	✓
۲	ISO 31000	✓	✓	✓	✓	✓	✓
۳	NIST 800-30	✓	✓	✓	✓		
۴	BSI Standard 200-3		✓	✓	✓	✓	
۵	TVRA	✓	✓	✓			
۶	Austrian IT		✓	✓	✓	✓	
۷	MAGERIT	✓	✓	✓	✓	✓	
۸	Microsoft		✓	✓	✓		✓
۹	COBIT-5 for Risk		✓	✓	✓		
۱۰	RISK IT	✓	✓	✓			
۱۱	CORAS	✓	✓	✓	✓	✓	✓
۱۲	CRAMM		✓				
۱۳	EBIOUS	✓	✓	✓	✓	✓	✓
۱۴	FAIR		✓				
۱۵	FRAAP	✓	✓	✓	✓		✓
۱۶	MEHARI	✓	✓	✓	✓	✓	✓
۱۷	OCTAVE (S) , (ALLEGRO)	✓	✓	✓	✓	✓	✓
۱۸	IRAM	✓	✓	✓			

۴-۳-۷-۲. پشتیبانی از مراحل ارزیابی مخاطره

یکی از اصلی‌ترین گام‌های مدیریت مخاطره امنیت اطلاعات، ارزیابی مخاطره امنیت اطلاعات (ISRA) است. ارزیابی مخاطره امنیت اطلاعات به شکل کلی، یک روش نظام‌مند به‌منظور 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 را فراهم می‌آورد.

ارزیابی مخاطره شامل فرآیندهایی مانند شناسایی فعالیت‌ها و دارایی‌ها، ارزش‌گذاری دارایی‌ها، ارزیابی تهدیدها و ارزیابی آسیب‌پذیری‌ها و تضمین آنها است. هر یک از روش‌های شناسایی شده، ترکیبی از یک یا چند مرحله از فرآیند ارزیابی مخاطره (شامل شناسایی مخاطره، تحلیل مخاطره و سنجش مخاطره) را پشتیبانی می‌کنند که در ادامه به تفصیل زیرفرآیندهای هر یک از این مراحل شرح داده شده است.

- **شناسایی مخاطره**: هدف از شناسایی مخاطره، تعیین عواملی است که می‌توانند علت زیان بالقوه باشند و اینکه چگونه، کجا و چرا زیان ممکن است رخ دهد. گام‌های زیر در شناسایی مخاطره وجود دارند:
  - شناسایی و ارزش گذاری دارایی‌ها؛
  - شناسایی تهدیدها؛
  - شناسایی کنترل‌های موجود؛
  - شناسایی آسیب‌پذیری‌ها؛ و
  - شناسایی پیامدها.
- **تحلیل مخاطره**: تحلیل مخاطره با توجه به سطح جزئیات موردنظر، میزان حیاتی بودن دارایی‌ها، گستره آسیب‌پذیری‌های شناخته شده و نیز رخدادهای دربرگیرنده سازمان انجام می‌شود. در واقع، تمامی فعالیت‌های مربوط به شناسایی، دسته‌بندی و ارزش‌گذاری دارایی‌های اطلاعاتی از یک سو و همچنین شناسایی سناریوهای مخاطره‌ای که معمولاً از نگاشت میان آسیب‌پذیری‌ها و تهدیدها حاصل می‌شوند از سوی دیگر را می‌توان در این مرحله درنظر گرفت. روش تحلیل مخاطره می‌تواند کمّی و یا کیفی و یا تلفیقی از هر دو باشد. این مرحله شامل گام‌های زیر است:
  - ارزیابی پیامدها؛
  - سنجش احتمال رخداد؛ و
  - تعیین سطح مخاطره.
- **سنجش مخاطره**: فرآیند مقایسه مخاطره تخمین زده شده به عنوان خروجی مرحله قبل با معیارهای مخاطره سازمان، به منظور تعیین میزان اهمیت مخاطره را سنجش مخاطره می‌نامند. در این مرحله سطوح مخاطره با معیار ارزیابی مخاطره و معیار پذیرش آن، مقایسه می‌شود.

(جدول ۴-۹) پشتیبانی اسناد پایه از هر یک از مراحل ارزیابی مخاطره (شناسایی مخاطره، تحلیل مخاطره و سنجش مخاطره) را بر پایهٔ استاندارد ISO/IEC 27005 نشان می‌دهد.

جدول ۴-۹. پشتیبانی از مراحل ارزیابی مخاطره

ردیف	نام سند	معیار پشتیبانی از مراحل ارزیابی مخاطره		
		شناسایی مخاطره	تحلیل مخاطره	سنجش مخاطره
۱	ISO 27005	✓	✓	✓
۲	ISO 31000	✓	✓	✓
۳	NIST 800-30	✓	✓	
۴	BSI Standard 200-3	✓	✓	✓
۵	TVRA	✓	✓	
۶	Austrian IT	✓	✓	✓
۷	MAGERIT	✓	✓	✓
۸	Microsoft	✓	✓	
۹	COBIT-5 for Risk	✓	✓	✓
۱۰	RISK IT	✓	✓	✓
۱۱	CORAS	✓	✓	✓
۱۲	CRAMM	✓	✓	✓
۱۳	EBIOUS	✓	✓	✓
۱۴	FAIR	✓	✓	✓
۱۵	FRAAP	✓	✓	✓
۱۶	MEHARI	✓	✓	✓
۱۷	OCTAVE (S) , (ALLEGRO)	✓	✓	✓
۱۸	IRAM	✓	✓	✓

۴-۳-۸. رویکردهای تخمین مخاطره

چندین نوع گوناگون و متفاوت از رویکردهای تخمین مخاطره وجود دارد که می‌توان آنها را به سه نوع اساسی (**شکل ۴-۳**) تقسیم کرد: ارزیابی کمّی، ارزیابی کیفی و ارزیابی ترکیبی

شکل ۴-۳. رویکردهای تخمین مخاطره

هر یک از اسناد پایه مدیریت و ارزیابی مخاطره ممکن است از یکی از رویکردهای کیفی، کمّی و یا ترکیبی استفاده کنند که هر یک از این رویکردها به تفکیک در ادامه توضیح داده شده است:

- **ارزیابی کمّی (قابل اندازه‌گیری)**: یک رویکرد مبتنی بر محاسبات ریاضی است که برای انجام تحلیل مخاطره، به حجم بالایی از داده‌ها نیازمند است. از داده‌های عینی و قابل اندازه‌گیری برای تعیین ارزش دارایی، احتمال از دست دادن و مخاطره همراه با آن استفاده می‌کند. در واقع، هدف کوشش برای محاسبه ارزش عددی هر یک از مؤلفه‌های حاصل در طول فرآیند ارزیابی مخاطره و فرآیند تحلیل هزینه-منفعت است. این رویکرد، با مشکل عدم اطمینان و عدم صحت اطلاعات مواجه است، مراحل کنترلی و اقدامی اغلب با تعدادی از رویدادهای بالقوه مواجه است، به‌طوری که این رویدادها خود باهم در ارتباط هستند. بهره‌برداری از این رویکرد، نیازمند زمان، منابع و هزینه زیادی است، از این‌رو برای محیط پیچیده سیستم‌های اطلاعاتی مناسب نیست.

- **ارزیابی کیفی (توصیفی):** رایج‌ترین رویکرد تخمین پیامد مخاطره است و از چندین المان (احتمال وقوع تهدیدها، شدت آسیب‌پذیری‌ها، میزان پیامد حوادث و کنترل‌ها) که با یک‌دیگر در ارتباط هستند، استفاده می‌کند. در حقیقت، یک رویکرد ذهنی است که تهدیدها بر پایهٔ دانش و نظر تحلیلگران در یکی از سطوح پایین، متوسط، بالا و یا بر پایهٔ طیف‌های کیفی مانند طیف لیکرت مورد ارزیابی قرار می‌گیرند. در واقع، این رویکرد، پیامد و احتمال مخاطره‌های شناسایی شده را به شیوه‌ای سریع و مقرون‌به‌صرفه مورد سنجش قرار می‌دهد. یکی از ضعف‌های این روش، عدم ثبات نتایج حاصل از معیارهای مخاطره است.
- **ارزیابی ترکیبی:** یک تکنیک واسطه‌ای است که احتمال و پیامد ناشی از مخاطره را با بهره‌برداری از دسته‌های کمّی طبقه‌بندی می‌کند. در رویکرد نیمه‌کمّی برآورد مخاطره با مقیاس‌های آماری و برخی ابزارهای ریاضی صورت می‌گیرد. به عبارتی دیگر، پس از شناسایی مخاطره با روش‌های کیفی، مخاطره موردنظر با معیارهای کمّی برآورد می‌شود. روش‌های تجزیه‌وتحلیل حالات و اثرات شکست، درخت رویداد، درخت خطا و درخت تصمیم از رویکردهای نیمه‌کمّی هستند. در حقیقت با توجه به نقاط ضعف و قوت هر دو روش کمّی و کیفی، از روش ارزیابی ترکیبی با هدف بهره‌برداری از سرعت و سادگی فرآیند ارزیابی کیفی و مزایای ارزیابی کمّی برای دارایی‌های حیاتی استفاده می‌شود.

پس از تعریف هر یک از رویکردهای کمّی، کیفی و ترکیبی تخمین مخاطره، به بیان مزایا و معایبی که هر یک از دو رویکرد کمی و کیفی به همراه خواهد داشت در قالب (**شکل ۴-۴**) می‌پردازیم.

شکل ۴-۴. مزایا و معایب رویکردهای کمّی و کیفی

رویکرد تخمین مخاطره هر یک از اسناد پایه در یکی از حالات (کمّی، کیفی و ترکیبی) در قالب (**جدول ۴-۱۰**) نشان داده شده است.

جدول ۴-۱۰. رویکردهای تخمین مخاطره

ردیف	نام روش	معیار رویکردهای تخمین مخاطره		
		کمّی	کیفی	ترکیبی
۱	ISO 27005			✓
۲	ISO 31000			✓
۳	NIST 800-30			✓
۴	BSI Standard 200-3		✓	
۵	TVRA	✓		
۶	Austrian IT			✓
۷	MAGERIT			✓
۸	Microsoft			✓
۹	COBIT-5 for Risk			✓
۱۰	RISK IT		✓	
۱۱	CORAS			✓
۱۲	CRAMM			✓
۱۳	EBIOUS		✓	
۱۴	FAIR	✓		
۱۵	FRAAP		✓	
۱۶	MEHARI			✓
۱۷	OCTAVE (S) , (ALLEGRO)			✓
۱۸	IRAM		✓	

۴-۳-۹. شیوه ارزیابی مخاطره

ارزیابی مخاطره بخشی از مدیریت مخاطره است که فرآیندی ساختاریافته را فراهم می‌آورد تا چگونگی تحت تأثیر قرارگرفتن اهداف را شناسایی کند و مخاطره را پیش از تصمیم‌گیری در این مورد که آیا به برخورد بیشتر نیاز است، از جنبه پیامدها و احتمال آن تحلیل کند. ارزیابی مخاطره دریافت تصمیم‌گیران و طرف‌های مسئول از مخاطره‌ها را بهبود می‌بخشد که می‌تواند بر دستیابی به اهداف و شایستگی و اثربخشی کنترل‌هایی که از قبل در کارند، تأثیر بگذارد. این امر مبنایی برای تصمیم‌گیری دربارهٔ مناسب‌ترین رویکردی که باید به منظور برخورد با مخاطره‌ها استفاده شود را فراهم می‌سازد. خروجی ارزیابی مخاطره، ورودی به فرآیندهای تصمیم‌گیری سازمان است. فرآیند ارزیابی مخاطره شامل شناسایی مخاطره، تحلیل/ تخمین مخاطره و سنجش مخاطره است. مخاطره‌ها را می‌توان در سطح سازمانی، در سطح شعبه‌ای، برای پروژه‌ها، فعالیت‌های منفرد یا مخاطره‌های خاص ارزیابی کرد. شیوه‌های متفاوتی ممکن است در فضاهای گوناگون مناسب باشند که شیوهٔ به‌کارگیری این فرآیند به فضای مدیریت مخاطره و همچنین شیوه‌های مورد استفاده برای انجام ارزیابی مخاطره بستگی دارد. مهم‌ترین شیوه‌های ارزیابی مخاطره که تاکنون مورد استفاده قرار گرفته، بدین شرح است:

- **خودارزیابی**[1]: یکی از شیوه‌های ارزیابی است که در آن، مسئولیت ارزیابی و گزارش کردن یک یا چند پارامتر به خود فرد/ سازمان واگذار می‌شود.
- **مصاحبه**: شیوه ارزیابی مبتنی بر مصاحبه، شامل تعاملی است که در آن مصاحبه‌گر از طریق فرآیند پرسش-پاسخ نسبت به جمع‌آوری اطلاعات موردنیاز جهت ارزیابی مخاطره اقدام می‌کند.

[1] Self-Assessment

- **کارگاه آموزشی**: در این شیوه فرآیند ارزیابی مخاطره از طریق برگزاری جلسه‌هایی در قالب کارگاه‌های آموزشی که تمامی ذینفعان در آن شرکت دارند، صورت می‌گیرد.

هر یک از اسناد پایه مدیریت و ارزیابی مخاطره از شیوه خاصی (خودارزیابی، مصاحبه، کارگاه آموزشی) جهت سنجش و ارزیابی مخاطره در سازمان بهره‌مند هستند که در (**جدول ۴-۱۱**) مورد مقایسه قرار گرفته‌اند.

جدول ۴-۱۱. شیوه ارزیابی مخاطره

ردیف	نام سند	معیار شیوه ارزیابی مخاطره		
		خودارزیابی	مصاحبه	کارگاه آموزشی
۱	ISO 27005	✓	✓	
۲	ISO 31000		✓	✓
۳	NIST 800-30	✓	✓	
۴	BSI Standard 200-3	✓		
۵	TVRA	✓		
۶	Austrian IT	✓		
۷	MAGERIT	✓		
۸	Microsoft	✓	✓	✓
۹	COBIT-5 for Risk	✓	✓	
۱۰	IT RISK	✓		
۱۱	CORAS			✓
۱۲	CRAMM	✓	✓	✓
۱۳	EBIOUS	✓		
۱۴	FAIR	✓		
۱۵	FRAAP	✓		
۱۶	MEHARI	✓	✓	
۱۷	OCTAVE (S) , (ALLEGRO)	✓	✓	✓
۱۸	IRAM	✓	✓	✓

۴-۳-۱۰. پشتیبانی ابزارها

بسیاری از اسناد پایه ارزیابی مخاطره بدون ابزار قابلیت استفاده ندارد، و یا ممکن است بهره‌برداری از رویکرد را با سختی همراه سازد. این معیار بیان‌کننده فهرست ابزارهایی است که از اسناد پایه پشتیبانی می‌کنند. امکان بهره‌برداری از ابزارها را در هر یک از اسناد پایه در یکی از حالات (ابزار رایگان، ابزار پولی به همراه نسخه آزمایشی، ابزار پولی بدون نسخه آزمایشی، عدم وجود ابزار نرم‌افزاری، عدم وجود ابزار و اسناد پشتیبان) نشان می‌دهد.

- **ابزار رایگان**: ابزاری که به صورت رایگان و بدون پرداخت هزینه جهت پشتیبانی از اسناد پایه در دسترس است.
- **ابزار پولی (به همراه نسخه آزمایشی)**: بیانگر این است که برای دسترسی و بهره‌برداری از ابزار باید پول پرداخت کرد، ولی نسخه آزمایشی از آن برای مشتریان بالقوه در اختیار است.
- **ابزار پولی (بدون نسخه آزمایشی)**: بیانگر این است که برای دسترسی و بهره‌برداری از ابزار باید پول پرداخت کرد، ولی نسخه آزمایشی از آن در اختیار مشتریان بالقوه قرار نمی‌گیرد.
- **عدم وجود ابزار نرم‌افزاری (همراه با اسناد پشتیبان)**: بیانگر این است که از هیچ‌گونه ابزار نرم‌افزاری پشتیبانی نمی‌کند ولی اسناد پشتیبان (برای نمونه، پرسش‌نامه، فرم‌ها، و غیره) را پوشش می‌دهد.
- **عدم وجود ابزار و اسناد پشتیبان**: بیانگر این است که شامل هیچ‌گونه ابزار و اسناد پشتیبانی نمی‌شود.

(**جدول ۴-۱۲**) پشتیبانی اسناد پایه از ابزارها را در یک یا چند حالت (ابزار رایگان، ابزار پولی به همراه نسخه آزمایشی، ابزار پولی بدون نسخه آزمایشی، عدم وجود ابزار نرم‌افزاری، عدم وجود ابزار و اسناد پشتیبان) نشان می‌دهد.

جدول ۴-۱۲. پشتیبانی ابزارها

ردیف	نام سند	معیار پشتیبانی ابزارها				
		ابزار رایگان	ابزار پولی به‌همراه نسخه آزمایشی	ابزار پولی بدون نسخه آزمایشی	عدم وجود ابزار نرم‌افزاری	عدم وجود ابزار و اسناد پشتیبان
۱	ISO 27005	✓	✓	✓		
۲	ISO 31000	✓	✓	✓		
۳	NIST 800-30	✓				✓
۴	BSI Standard 200-3	✓	✓			✓
۵	TVRA	✓				
۶	Austrian IT	✓	✓			
۷	MAGERIT	✓	✓			
۸	Microsoft	✓				
۹	COBIT-5 for Risk		✓			
۱۰	RISK IT		✓			
۱۱	CORAS	✓				
۱۲	CRAMM	✓	✓			
۱۳	EBIOUS	✓				
۱۴	FAIR	✓	✓			
۱۵	FRAAP	✓				
۱۶	MEHARI	✓	✓			
۱۷	OCTAVE (S) , (ALLEGRO)	✓	✓		✓	
۱۸	IRAM	✓	✓			

۴-۳-۱۱. پشتیبانی از زبان‌های رایج

یکی دیگر از معیارهای مطرح در انتخاب و ارزیابی اسناد پایه ارزیابی، پشتیبانی از زبان‌های رایج است. هر چقدر یک سند پایه از تعداد زبان‌های بین‌المللی بیشتری پشتیبانی کند، قاعدتاً جامعه کاربری آن نیز افزایش می‌یابد. (**جدول ۴- ۱۳**) پشتیبانی اسناد پایه از زبان‌های رایج در جهان را بر پایهٔ طیف لیکرت پنج ارزشی (از بسیار کم تا بسیار زیاد) نشان می‌دهد.

جدول ۴- ۱۳. پشتیبانی از زبان‌های رایج

ردیف	نام سند	معیار پشتیبانی از زبان‌های رایج				
		بسیار کم	کم	متوسط	زیاد	بسیار زیاد
۱	ISO 27005		✓			
۲	ISO 31000			✓		
۳	NIST 800-30	✓				
۴	BSI Standard 200-3		✓			
۵	TVRA	✓				
۶	Austrian IT	✓				
۷	MAGERIT			✓		
۸	Microsoft	✓				
۹	COBIT-5 for Risk	✓				
۱۰	RISK IT	✓				

ردیف	نام سند	معیار پشتیبانی از زبان‌های رایج				
		بسیار کم	کم	متوسط	زیاد	بسیار زیاد
۱۱	CORAS			✓		
۱۲	CRAMM			✓		
۱۳	EBIOUS				✓	
۱۴	FAIR	✓				
۱۵	FRAAP	✓				
۱۶	MEHARI		✓			
۱۷	OCTAVE (S) , (ALLEGRO)	✓				
۱۸	IRAM	✓				

۴-۳-۱۲. میزان سازگاری با استانداردها و مستندات پایه

بسیاری از اسناد پایه مدیریت و ارزیابی مخاطره با یک یا چندین استاندارد ملّی یا بین‌المللی (برای نمونه ISO/IEC 13335-1، ISO/IEC 15408) و همچنین دیگر مستندات پایه (برای مثال MAGERIT، RISK IT) سازگاری دارند. از این‌رو میزان کمّیت سازگاری به عنوان یکی از معیارهای ارزیابی در انتخاب سند پایه در سازمان‌ها از اهمیت قابل توجهی برخوردار است. (**جدول ۴-۱۴**) میزان سازگاری هر یک از اسناد پایه با استانداردها و مستندات پایه را در قالب طیف لیکرت (بسیار کم تا بسیار زیاد) نشان می‌دهد.

جدول ۴-۱۴. قابلیت سازگاری با استانداردها و مستندات پایه

ردیف	نام سند	معیار قابلیت سازگاری با استانداردها و مستندات پایه				
		بسیار کم	کم	متوسط	زیاد	بسیار زیاد
۱	ISO 27005					✓
۲	ISO 31000				✓	
۳	NIST 800-30			✓		
۴	BSI Standard 200-3			✓		
۵	TVRA		✓			
۶	Austrian IT			✓		
۷	MAGERIT				✓	
۸	Microsoft		✓			
۹	COBIT-5 for Risk					✓
۱۰	RISK IT					✓
۱۱	CORAS				✓	
۱۲	CRAMM			✓		
۱۳	EBIOUS					✓
۱۴	FAIR			✓		
۱۵	FRAAP				✓	
۱۶	MEHARI			✓		
۱۷	OCTAVE (S) , (ALLEGRO)			✓		
۱۸	IRAM	✓				

۴-۳-۱۳. پوشش تعاریف و اصطلاحات (واژه‌نامه)

هرچه دامنه تعاریف و اصلاحات مورد استفاده در اسناد پایه ارزیابی مخاطره گسترده‌تر باشد، سهولت و کاربری آسان‌تری نیز به همراه خواهد داشت. (**جدول ۴-۱۵**) میزان پوشش‌دهی تعاریف پایه و اصطلاحات کلیدی در هر یک از اسناد پایه را بر پایهٔ طیف لیکرت پنج ارزشی (از بسیار کم تا بسیار زیاد) نشان می‌دهد.

جدول ۴-۱۵. پوشش تعاریف و اصطلاحات (واژه‌نامه)

ردیف	نام سند	معیار پوشش تعاریف و اصطلاحات (واژه‌نامه)				
		بسیار کم	کم	متوسط	زیاد	بسیار زیاد
۱	ISO 27005					✓
۲	ISO 31000				✓	
۳	NIST 800-30					✓
۴	BSI Standard 200-3			✓		
۵	TVRA			✓		
۶	Austrian IT				✓	
۷	MAGERIT					✓
۸	Microsoft		✓			
۹	COBIT-5 for Risk				✓	
۱۰	RISK IT				✓	
۱۱	CORAS			✓		
۱۲	CRAMM		✓			
۱۳	EBIOUS				✓	
۱۴	FAIR				✓	
۱۵	FRAAP					✓
۱۶	MEHARI				✓	
۱۷	OCTAVE (S) , (ALLEGRO)		✓			
۱۸	IRAM				✓	

۴-۳-۱۴. نوع دسترسی سند پایه ارزیابی مخاطره

سازمان‌ها جهت به‌کارگیری روش‌های مدیریت و ارزیابی مخاطره، در وهله نخست نیازمند دسترسی به مستندات و اسناد پایه آنها هستند. از این‌رو سازمان‌ها می‌توانند بر پایهٔ یکی از حالت‌های (دسترسی با هزینه و دسترسی آزاد) به هر یک از اسناد پایه مدیریت و ارزیابی مخاطره دسترسی داشته باشند. (**جدول ۴-۱۶**) شیوهٔ دسترسی به اسناد پایه را نشان می‌دهد.

- دسترسی باهزینه: سندی که جهت دسترسی و بهره‌برداری از آن باید پول پرداخت کرد.
- دسترسی آزاد: سندی که به صورت رایگان و بدون پرداخت هزینه در دسترس است.

جدول ۴-۱۶. نوع دسترسی سند پایه ارزیابی مخاطره

ردیف	نام سند	نوع دسترسی	
		آزاد	باهزینه
۱	ISO 27005		✓
۲	ISO 31000		✓
۳	NIST 800-30	✓	
۴	BSI Standard 200-3	✓	
۵	TVRA	✓	
۶	Austrian IT	✓	
۷	MAGERIT	✓	
۸	Microsoft	✓	
۹	COBIT-5 for Risk		✓
۱۰	RISK IT	✓	
۱۱	CORAS	✓	
۱۲	CRAMM		✓

ردیف	نام سند	نوع دسترسی	
		آزاد	باهزینه
۱۳	EBIOUS	✓	
۱۴	FAIR	✓	
۱۵	FRAAP	✓	
۱۶	MEHARI	✓	
۱۷	OCTAVE (S) , (ALLEGRO)		✓
۱۸	IRAM		✓

۴-۳-۱۵. کارایی سند پایه ارزیابی مخاطره

از عوامل مؤثر در کارایی اسناد پایه شناسایی شده ارزیابی مخاطره می‌توان به شاخص‌های سرعت، سهولت استفاده/ کاربری آسان، فرآیند روشن و شفاف مراحل و تکرارپذیری اشاره کرد. در ادامه هر یک از این شاخص‌ها به تفکیک شرح داده شده است.

- **سرعت**: زمان درنظر گرفته شده جهت انجام فرآیند تحلیل و ارزیابی مخاطره را نشان می‌دهد.
- **استفاده/ کاربری آسان**: میزان سادگی، آسانی و راحتی درک و استفاده را نشان می‌دهد.
- **فرآیند روشن و شفاف مراحل**: میزان شفافیت مراحل و چگونگی اجرای هر مرحله را نشان می‌دهد.
- **تکرارپذیری**: میزان قابلیت تکرارپذیری و مقایسه نتایج ارزیابی با دیگر روش‌ها (اسناد پایه) را نشان می‌دهد.

میزان کارایی هر یک از اسناد پایه بر پایهٔ شاخص‌های تعریف شده در قالب طیف لیکرت پنج ارزشی (از بسیار کم تا بسیار زیاد) در (**جدول ۴-۱۷**) نشان داده شده است.

جدول ۴-۱۷. کارایی سند پایه مدیریت و ارزیابی مخاطره

ردیف	نام روش	معیار کارایی																			
		سرعت					سهولت استفاده					فرآیند روشن و شفاف مراحل					تکرارپذیری				
		بسیار کم	کم	متوسط	زیاد	بسیار زیاد	بسیار کم	کم	متوسط	زیاد	بسیار زیاد	بسیار کم	کم	متوسط	زیاد	بسیار زیاد	بسیار کم	کم	متوسط	زیاد	بسیار زیاد
۱	ISO 27005					✓					✓					✓					✓
۲	ISO 31000				✓					✓					✓					✓	
۳	NIST 800-30				✓						✓					✓				✓	
۴	BSI Standard 200-3		✓					✓					✓				✓				
۵	TVRA			✓				✓					✓							✓	
۶	Austrian IT			✓				✓					✓						✓		
۷	MAGERIT			✓						✓						✓				✓	
۸	Microsoft			✓					✓					✓						✓	
۹	COBIT-5 for Risk		✓					✓					✓						✓		
۱۰	RISK IT			✓					✓					✓					✓		
۱۱	CORAS		✓					✓					✓						✓		
۱۲	CRAMM		✓					✓					✓					✓			
۱۳	EBIOUS				✓				✓						✓					✓	
۱۴	FAIR	✓						✓					✓						✓		
۱۵	FRAAP					✓					✓					✓					✓
۱۶	MEHARI				✓			✓					✓							✓	
۱۷	OCTAVE (S) , (ALLEGRO)			✓						✓					✓						✓
۱۸	IRAM				✓				✓						✓				✓		

۴-۴. مصورسازی روش‌های مدیریت و ارزیابی مخاطره

اصطلاح مصورسازی در طیف گسترده‌ای از تعاریف و موارد به‌کار رفته است. تا همین اواخر، فرهنگ‌های لغت معمولاً مصورسازی را فعالیتی تعریف می‌کردند که انسان‌ها طی آن چیزی را در ذهن خود مجسم می‌کنند (Mazza 2009). «مازا» این تعریف را معنی اصلی مصورسازی می‌داند و بر این عقیده است که مصورسازی، فعالیتی شناختی است، به طوری که افراد یک بازنمایی ذهنی و داخلی از جهان می‌سازند و بر پایهٔ آن می‌توانند این داده‌ها را گسترش داده و درک کنند و این فرآیند با بازنمایی‌های دیداری تسهیل می‌شود. وی بیان می‌کند که این تعاریف مستقل از رایانه‌ها بیان شده است و با اینکه رایانه‌ها می‌توانند مصورسازی را تسهیل کنند، اما باز هم مصورسازی فعالیتی است که در ذهن صورت می‌گیرد. وی بین خلق یک بازنمایی تصویری از داده‌ها و فرآیند شناختی که در زمان تفسیر بازنمایی تصویر روی می‌دهد تفاوت قائل شده است و برای مورد نخست از اصطلاح بازنمایی دیداری و برای مورد دوم از اصطلاح مصورسازی استفاده کرده است.

از طرف دیگر در حال حاضر اصطلاح مصورسازی بیشتر به معنی بازنمایی گرافیکی داده‌ها و مفاهیم و به عنوان مصنوع خارجی برای حمایت از تصمیم‌گیری و ابزاری شناختی به‌کار می‌رود (Ware 2019). چنان که «ترگان» و «کلر» در سال ۲۰۰۵ میلادی، مصورسازی را ابزاری شناختی می‌دانند که نظام شناختی کاربر را حمایت می‌کند. به گفته «بورنر»، «چن»، و «بویاک» در سال ۲۰۰۳ میلادی منظور از مصورسازی، طراحی نمایش تصویری اشیاء داده‌ای و روابط بین آن‌ها است. تعریفی دیگر، مصورسازی را روشی از محاسبه می‌داند که موارد نمادین را به شکل هندسی تبدیل می‌کند و بدین ترتیب پژوهشگران را قادر می‌سازد که شبیه‌سازی‌ها و محاسبات خود را مشاهده کنند، روشی برای مشاهده نادیدنی‌ها پیشنهاد می‌کند، به فرآیند کشف علمی می‌رسد و آگاهی‌های عمیق و غیرمنتظره را می‌پروراند (McCormick, Thomas and Maxine 1987). تمامی این تعاریف مصورسازی را به عنوان بازنمایی بیرونی از داده‌ها و اطلاعات و ابزاری برای کمک به فرآیند شناختی انسان معرفی کرده‌اند.

با توجه به دو رویکرد کلی بالا دربارهٔ مفهوم مصورسازی، آنچه در این فصل بر روی آن تمرکز شده است مفهوم دوم مصورسازی، یعنی بازنمایی بیرونی داده‌ها است. بر این اساس و بر پایه تعاریف و مفاهیم ارائه شده می‌توان مصورسازی را بدین‌گونه تعریف نمود: *بازنمایی گرافیکی داده‌ها، اطلاعات و دانش و روابط آشکار و نهان بین آنها، به عنوان ابزاری شناختی برای انتقال بهتر اطلاعات به کاربر.*

در حقیقت، یکی از ابزارهایی که در انتخاب مناسب روش مدیریت و ارزیابی مخاطره در بین دیگر اسناد پایه به سازمان‌ها کمک می‌کند، بهره‌برداری از روش‌های گرافیکی برای نمایش ارتباط داده‌های کمّی و کیفی است. به همین منظور، در این بخش از نمودارهای دایره‌ای -روش نمایش اطلاعات- با هدف مصورسازی نتایج حاصل از مقایسه اسناد پایه مدیریت و ارزیابی مخاطره بر پایهٔ معیارهای ارزیابی استفاده شده است. مصورسازی چارچوب ارزیابی مقایسه‌ای روش‌های مدیریت و ارزیابی مخاطره در قالب (**شکل ۴-۵**) قابل مشاهده است.

۴-۵. گزیدهٔ فصل

مدیریت و ارزیابی مخاطره امنیت اطلاعات یک فرآیند ثابت و محدود به یک زمان خاص نیست، بلکه یک فرآیند مداوم و مستمر است. به‌طوری که باید به صورت دوره‌ای تکرار شود و در هر تکرار، چالش‌های تکرارهای قبلی، تغییرات فناوری و سناریوهای جدید مخاطره در نظر گرفته شود. ازاین‌رو، انتخاب روشی مناسب و کارا از بین اسناد پایه معرفی شده به پارامترهای گوناگونی ازجمله اندازه سازمان هدف، سطح مهارت مورد نیاز، میزان سازگاری با استانداردها، نوع دسترسی، شیوه ارزیابی مخاطره، سطح کاربری سند

پایه و دیگر عوامل بستگی دارد. در این فصل، اسناد پایه مدیریت و ارزیابی مخاطره بر پایهٔ معیارهای ارزیابی پیش‌گفته مورد مقایسه و ارزیابی قرار گرفتند. سرانجام، نتایج حاصل از مطالعات و بررسی‌های صورت‌گرفته در قالب یک چارچوب ارزیابی مقایسه‌ای مبتنی بر میزان پوشش‌دهی معیارهای ارزیابی به تصویر کشیده شده است تا بتواند در انتخاب بهینه سند پایه به سازمان‌ها کمک کند.

چارچوب مقایسه روش‌های مدیریت و ارزیابی مخاطره امنیت اطلاعات

تعریف معیارهای ارزیابی:

- **نوع:** تعیین‌کننده یک یا ترکیبی از گونه‌های (استاندارد، راهنما/ دستورالعمل، مدل، روش) است.
- **ماهیت:** تعیین‌کننده فلسفه وجودی روش براساس یک یا ترکیبی از حالت‌های (فناوری محور، کسب وکارمحور، دارایی‌محور، خدمت‌محور، دانش‌محور، مدل محور، نرم افزارمحور،) است.
- **سازمان ارائه‌دهنده:** نوع نهاد ارائه‌دهنده روش را براساس یکی از انواع (بین‌المللی، دولتی/ ملّی، خصوصی، دانشگاهی) نشان می‌دهد.
- **اندازه سازمان هدف:** روش برای چه نوع سازمانی (اندازه یا بزرگی سازمان) طراحی و استفاده شده است.
- **سطح کاربری:** تعیین‌کننده نوع کاربری روش براساس یکی یا ترکیبی از حالت‌های (مدیریتی، عملیاتی، فنی) است.
- **سطح تخصص/ مهارت موردنیاز:** برای انجام هریک از روش‌ها به چه سطحی از تخصص/ مهارت نیاز است.
- **پشتیبانی از مراحل مدیریت مخاطره:** روش موردنظر از کدامیک از مراحل مدیریت مخاطره پشتیبانی می‌کند
- **پشتیبانی از مراحل ارزیابی مخاطره:** روش موردنظر ازکدامیک از مراحل ارزیابی مخاطره پشتیبانی می‌کند.
- **رویکرد تخمین مخاطره:** تعیین‌کننده روش تخمین/ برآورد مخاطره براساس یکی از حالت‌های (کمّی، کیفی و یا ترکیبی) است.

- **رویکرد ارزیابی:** تعیین‌کننده روش ارزیابی براساس یک یا ترکیبی از حالت‌های (خودارزیابی، مصاحبه و یا کارگاه آموزشی) است.
- **قابلیت پشتیبانی از ابزارها:** تعیین‌کننده پشتیبانی از ابزارهای تجاری/غیرتجاری و چگونگی دسترسی به آن‌ها است.
- **قابلیت پشتیبانی از زبان‌های رایج:** تعیین‌کننده تعداد زبان‌هایی است که روش از آنها پشتیبانی می‌کند.
- **قابلیت سازگاری با استانداردها و مستندات پایه:** میزان تطابق با قوانین، مقررات، استانداردها، دستورالعمل‌ها وغیره را نشان می‌دهد.
- **پوشش تعاریف و اصطلاحات (واژه‌نامه):** تعیین‌کننده میزان پوشش‌دهی تعاریف و اصطلاحات مورد استفاده در روش است به طوریکه کاربر بدون نیاز به دانستن اصطلاحات خاص بتواند از آن استفاده کند.
- **نوع دسترسی:** نحوه دسترسی عموم به اطلاعات جهت سنجش و مقایسه مدل با دیگر مدلها را فراهم می‌کند.
- **سرعت:** حداقل و حداکثر زمان درنظرگرفته شده جهت انجام فرآیند تحلیل و ارزیابی مخاطره را نشان می‌دهد.
- **سهولت استفاده/ کاربری آسان:** به شکل ساده، آسان و راحت در تمامی مراحل درک و استفاده شود.
- **فرآیند روشن و شفاف:** مراحل به‌طور روشن و شفاف تعریف شده باشند و چگونگی اجرای هر مرحله از قبل مشخص باشد.
- **تکرارپذیری:** به راحتی قابل تکرار باشد و نتایج را بتوان با ارزیابی‌های قبلی و سایر ارزیابی‌ها مقایسه کرد.

نام کامل و آدرس دسترسی روش‌ها:

- **Austrian IT:** Austrian IT Security Handbook (http://www.cio.gv.at/securenetworks/sihb/)
- **BSI 200-3:** BSI Standard 200-3 (https://www.bsi.bund.de/DE/Home/home_node.html)
- **COBIT:** Control Objectives for Information and Related Technology for Risk (https://www.isaca.org/resources/cobit)
- **CORAS:** Consultative Objective Risk Analysis System (http://coras.sourceforge.net/index.html)
- **CRAMM:** CCTA Risk Analysis and Management Method (https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83)
- **EBIOUS:** Expression des Besoins et Identification des Objectifs de Sécurité (https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/)
- **ETSI TVRA:** The European Telecommunication Standards Institute Threat Vulnerability and Risk Analysis (TVRA) Method (https://www.etsi.org)
- **FAIR:** Factor Analysis of Information Risk (https://www.fairinstitute.org/what-is-fair)
- **FRAAP:** Facilitated Risk Analysis and Assessment Process (http://www.peltierassociates.com/frap.htm)
- **IRAM:** Information Risk Analysis Methodologies (https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/)
- **ISO 27005:** ISO/IEC 27005 (https://www.iso.org/standard/75281.html)
- **ISO 31000:** ISO/IEC 31000 (https://www.iso.org/standard/65694.html)
- **MAGERIT:** Risk Analysis and Management Methodology for Information Systems (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en)
- **MEHARI:** Method For Harmonized Analysis of Risk (http://meharipedia.org/home)
- **Microsoft:** Microsoft's Security Risk Management Guide (https://www.microsoft.com/en-us/)
- **NIST 800-30:** NIST SP800-30 (https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final)
- **OCTAVE:** Operationally Critical Threat, Asset, And Vulnerability Evaluation (http://www.cert.org/octave/osig.html)
- **Risk IT:** Risk IT (https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2)

راهنما :

۱	۲	۳	۴	۵
بسیار کم	کم	متوسط	زیاد	بسیار زیاد

تدوین:
حمیدرضا خدمتگزار
ساناز قربانلو

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

شرکت فنی و مهندسی
امن پردازان کویر
APK

فهرست واژگان و علائم اختصاری انگلیسی به فارسی

واژه انگلیسی	برگردان فارسی
A	
A Standard Value at Risk (VaR) Framework	چارچوب ارزش در معرض مخاطره استاندارد
Accountability	پاسخ‌گویی
Analog Risk Assessment (ARA)	ارزیابی مخاطره آنالوگ
Analysis	تحلیل
Anonymity	ناشناس بودن
Asset	دارایی
Assurance Requirement	الزام‌های اطمینان
Austrian Federal Chancellery	شورای فدرال اتریش
Austrian IT Security Handbook	کتابچه راهنمای امنیت فناوری اطلاعات اتریش
Authenticity	صحت و سندیت
Availability	دسترس‌پذیری
B	
Business Model for Information Security (BMIS)	مدل کسب‌وکار برای امنیت اطلاعات
C	
Central Computer and Telecommunications Agency (UK)	آژانس مرکزی ارتباطات و مخابرات انگلستان
Central Computing and Telecommunications Agency Risk Analysis and Management Method (CRAMM)	روش تحلیل و مدیریت مخاطره آژانس مرکزی ارتباطات و مخابرات
Chief Information Officers (CIO)	مدیران ارشد اطلاعات
Chief Information Security Officers (CISO)	مدیران ارشد امنیت اطلاعات
Club de la sécurité de l'information français (CLUSIF)	سازمان امنیت اطلاعات فرانسه
Codes of practice	به‌روش‌های یا رهنمودهای بین‌المللی
Cold War	جنگ سرد
Committee of Sponsoring Organizations of the Treadway Commission (Treadway)	کمیته سازمان‌های حامی کمیسیون تِرِدوی
Committee on National Security Systems (CNSS)	انجمن سیستم‌های امنیت ملّی
Community Emergency Response Team	انجمن پاسخ به رخدادهای امنیتی
Computer	رایانه
Computer Security Organization (CSO)	سازمان امنیت رایانه
Confidentiality	محرمانگی
Confidentiality, Integrity, Availability, Authenticity and Accountability (CIAAA)	محرمانگی، صحت، دسترس‌پذیری، احرازهویت و پاسخگویی
Confidentiality,Integrity, Availability (CIA)	مثلث سی.آی.اِی (محرمانگی، صحت، دسترس‌پذیری)
Consensus	اجماع
Consultative Objective Risk Analysis System (CORAS)	سیستم تحلیل مخاطره عینی-مشاوره‌ای
Control Objectives for Information and Related Technology (COBIT)	چارچوب اهداف کنترلی برای اطلاعات و فناوری‌های مرتبط با آن
Control strength (CS)	تخمین قدرت کنترل
COSO Cube	مکعب کوزو
Counter Measure	اقدام متقابل
Crack Team	تیم کرک
Cross Coupling	جفت‌شدن متقابل

واژه انگلیسی	برگردان فارسی
Crystal-Ball-Gazing	گوی بلورین
Culture Security	امنیت فرهنگی
D	
Decision Support	تصمیم‌یار
Defense-in-depth	دفاع در عمق
Deficiencies	کمبودها
Delphi	دلفی
Detection of failure	احتمال کشف مخاطره
Direction Centrale de la Sécurité des Systémes d'Information (DCSSI)	آژانس امنیت سایبری ملّی فرانسه
Discipline	انتظام
Distributed Computing	رایانش توزیع‌شده
E	
Economic Security	امنیت اقتصادی
Enterprise Risk Management (ERM)	مدیریت مخاطره سازمانی
ETSI Threat Vulnerability & Risk Analysis (TVRA) Method	تحلیل تهدیدها، مخاطره‌ها و آسیب‌پذیری‌های یک سیستم ارتباطی، روش طراحی سیستمی تحت عنوان "روش مدل‌سازی امنیتی TVRA
European Telecommunications Standards Institute (ETSI)	مؤسسه استانداردهای مخابراتی اروپا
Evaluation	سنجش
Experts	متخصصان
Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives (EBIOS)	بیان نیازها و شناسایی اهداف امنیتی
F	
Facilitated Risk Analysis and Assessment Process (FRAAP)	فرآیند تسهیل‌شده ارزیابی مخاطره
Facilitator	تسهیل‌گر
Factor analysis of information risk (FAIR)	تحلیل عاملی مخاطره اطلاعات
Failure Mode & Effect Critically Analysis (FMECA)	تجزیه و تحلیل بحرانی حالات و اثرات شکست
Failure Modes and Effects Analysis (FMEA)	تجزیه‌وتحلیل حالات و اثرات شکست
Fault Tree Analysis (FTA)	تجزیه‌وتحلیل درخت خطا
Feedback	بازخورد
Fundamental Information Risk Management (FIRM)	مدیریت مخاطره اطلاعات پایه
G	
Granularity	ریزدانگی
H	
Handbook and Framework	راهنما و چارچوب
Hazard and Operability study (HAZOP)	مطالعه مخاطرات و راهبری عملیات
I	
Identification	شناسایی
Information Asset Management (IAM)	مدیریت دارایی‌های اطلاعاتی
Information Risk Analysis Methodologies (IRAM)	متدولوژی‌های تحلیل مخاطره اطلاعات
Information Risk Analysis Methodologies 2 (IRAM2)	متدولوژی‌های تحلیل مخاطره اطلاعات نسخه شماره (۲)
Information Risk Scorecard	کارت امتیازی مخاطره اطلاعات
Information Security Forum (ISF) Methods	انجمن امنیت اطلاعات
Information Security Management System- ISMS	سیستم مدیریت امنیت اطلاعات

واژه انگلیسی	برگردان فارسی
Information Security Risk Assessment	ارزیابی مخاطره امنیت اطلاعات
Information Security Status Survey	بررسی وضعیت امنیت اطلاعات
Information Systems Audit And Control Association (ISACA)	انجمن نظارت و کنترل سیستم‌های اطلاعاتی
Information Systems Risk Management-Organizational Perspective	مدیریت مخاطره‌های سیستم‌های اطلاعاتی-دید سازمانی
Information Technology Infrastructure Library (ITIL)	کتابخانه زیرساخت فناوری اطلاعات
Institute of Standards & Industrial Research of Iran	مؤسسه استاندارد و تحقیقات صنعتی ایران (ماتصا)
Institutionalization	نهادینه‌سازی
Integrity	صحت
International Federation of Accountants (IFAC)	فدراسیون بین‌المللی حسابداران
International Organization for Standardization (ISO)	سازمان جهانی استاندارد
IT Baseline Protection Manual (IT-Grundschutz)	کتابچه راهنمای محافظت از اطلاعات پایه فناوری اطلاعات
IT Governance Institute (ITGI)	سازمان راهبری فناوری اطلاعات
Iteration	تکرار
L	
Logger	رخدادنگار
Loss Event Frequency (LEF)	شدت/ میزان رویداد از دست رفته
M	
Mainframe	ابررایانه‌ها
Me´thode Harmonise´e d'Analyse de Risques — Harmonised Risk Analysis Method (MEHARI)	روشی برای تحلیل هماهنگ مخاطره
Meta-Method	فرا-روش
Methodology of Analysis of Computer Risks Directed by Levels (MARION)	روش تحلیل مخاطرات رایانه‌ای بر پایهٔ سطوح
Methods and Models	روش‌ها و مدل‌ها
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)	تحلیل و مدیریت مخاطره سیستم‌های اطلاعاتی
Monitoring	پایش
N	
National Aeronautics and Space Administration (NASA)	صنعت هوافضای آمریکا
National Institute of Standards and Technology (NIST)	مؤسسه ملّی استانداردها و فناوری
Non-Repudiation	عدم انکار
O	
Occurrence of failure	احتمال وقوع مخاطره
Open Source	متن‌باز
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OVTAVE)	ارزیابی عملیاتی تهدیدها، دارایی‌ها و آسیب‌پذیری حیاتی
Operationally Critical Threat ,Asset ,and Vulnerability Evaluation SMEs (OCTAVE-S)	ارزیابی عملیاتی تهدیدها، دارایی‌ها و آسیب‌پذیری حیاتی سازمان‌های کوچک-متوسط
Operationally Critical Threat, Asset, and Vulnerability Evaluation Allegro (OCTAVE Allegro)	بهبود فرآیند ارزیابی عملیاتی تهدیدها، دارایی‌ها و آسیب‌پذیری‌های حیاتی
P	
Plan-Do-Check-Act (PDCA)	برنامه- اجرا- کنترل- عمل
Plan–Do–Control–Measure–Report	طراحی-اجرا-کنترل-سنجش-گزارش
Policy Security	امنیت سیاسی
Potential Risk Assessment	ارزیابی مخاطره احتمالی
Probable Loss Magnitude (PLM)	شدت/ مقدار خسارت احتمالی

واژه انگلیسی	برگردان فارسی
Project Management Institute (PMI)	مؤسسه مدیریت پروژه
Prototype	نمونه اولیه
R	
Return on Security Investment (ROSI)	بازگشت تحلیل سرمایه‌گذاری امنیتی
Risk analysis	تحلیل مخاطره
Risk Appetite	اشتهای مخاطره
Risk Evaluation	سنجش مخاطره
Risk IT	مخاطره فناوری اطلاعات
Risk Management Framework	چارچوب مدیریت مخاطره
Risk Map	نقشه مخاطره
Risk Priority Number (RPN)	عدد اولویت مخاطره
Risk Scorecard	کارت امتیازی مخاطره
Risk Treatment Plan (RTP)	طرح مقابله با مخاطره
Routine	منظم و پیوسته
S	
Security Objective	اهداف امنیتی
Security Requirement	الزام‌های امنیتی
Self-Assessment	خودارزیابی
Severity of failure	شدت اثر مخاطره
Simple to Apply Risk Analysis (Sara)	فرآیند ساده برای تحلیل مخاطره
Simplified Process for Risk Identification (Sprint)	فرآیند ساده‌سازی شده برای شناسایی مخاطره
Single Point of Failure (SPOF)	تک نقاط شکست
Small and mid-size enterprises (SMEs)	سازمان‌ها/ شرکت‌های کوچک و متوسط
Social Engineering	مهندسی اجتماعی
Social Security	امنیت اجتماعی
Spanish Ministerio de Administraciones Públicas	وزارت امورخارجه اسپانیا
Special Publications Risk management Guide for Information Technology Systems	راهنمای مدیریت مخاطره‌های سیستم‌های فناوری اطلاعات
Standard	استاندارد
Standard of Good Practice	استاندارد تجارب خوب
T	
Target Of Evaluation (TOE)	هدف سنجش
The Advanced Research Projects Agency Network - ARPANet	شبکه آژانس پروژه‌های تحقیقاتی پیشرفته (آرپانِت)
The Committee Of Sponsoring Organizations Of The Tread way Commission’s Enterprise Risk Management Framework (COSO ERM)	چارچوب مخاطره سازمانی کوزو
The Federal Information Security Management Act (FISMA)	قانون مدیریت امنیت اطلاعات فدرال
The Federal Office for Information Security (BSI)	اداره فدرال امنیت اطلاعات
The Information Technology Assurance Framework (ITAF)	چارچوب تضمین فناوری اطلاعات
The International Electrotechnical Commission (IEC)	کمیته فنی کمیسیون بین‌المللی الکتروتکنیک
The Microsoft’s Security Risk Management Guide	راهنمای مدیریت مخاطره امنیت مایکروسافت
The Office of Government Commerce (OGC)	دفتر بازرگانی دولتی
Threat	تهدید
Threat Capability (TCap)	قابلیت تهدید
Threat Event Frequency (TEF)	نرخ احتمال رویداد تهدید

واژه انگلیسی	برگردان فارسی
Top Event (TE)	رویداد اصلی
Traditional Risk Analysis Methods	روش‌های سنتی تحلیل مخاطره
Traditional Risk Analysis of Information Security	روش سنتی برای انجام تحلیل مخاطره امنیت اطلاعات
U	
Unwanted Incident	حادثه ناخواسته
V	
Val IT	ارزش فناوری اطلاعات
Value Model	مدل ارزش
Vulnerability	آسیب‌پذیری
W	
Weakness	ضعف
Windows Server Update Service (WSUS)	خدمات به‌روزرسانی ویندوز سرور

فهرست واژگان و علائم اختصاری فارسی به انگلیسی

واژه فارسی	برگردان انگلیسی
الف	
ابرایانه‌ها	Mainframe
اجماع	Consensus
احتمال کشف مخاطره	Detection of failure
احتمال وقوع مخاطره	Occurrence of failure
اداره فدرال امنیت اطلاعات	The Federal Office for Information Security (BSI)
ارزش فناوری اطلاعات	Val IT
ارزیابی عملیاتی تهدیدها، دارایی‌ها و آسیب‌پذیری حیاتی	Operationally Critical Threat, Asset, and Vulnerability Evaluation (OVTAVE)
ارزیابی عملیاتی تهدیدها، دارایی‌ها و آسیب‌پذیری حیاتی سازمان‌های کوچک-متوسط	Operationally Critical Threat ,Asset ,and Vulnerability Evaluation SMEs (OCTAVE-S)
ارزیابی مخاطره احتمالی	Potential Risk Assessment
ارزیابی مخاطره امنیت اطلاعات	Information Security Risk Assessment
ارزیابی مخاطره آنالوگ	Analog Risk Assessment (ARA)
آژانس امنیت سایبری ملّی فرانسه	Direction Centrale de la Sécurité des Systémes d'Information (DCSSI)
آژانس مرکزی ارتباطات و مخابرات انگلستان	Central Computer and Telecommunications Agency (UK)
استاندارد	Standard
استاندارد تجارب خوب	Standard of Good Practice
آسیب‌پذیری	Vulnerability
اشتهای مخاطره	Risk Appetite
اقدام متقابل	Counter Measure
الزام‌های اطمینان	Assurance Requirement
الزام‌های امنیتی	Security Requirement
امنیت اجتماعی	Social Security
امنیت اقتصادی	Economic Security
امنیت سیاسی	Policy Security
امنیت فرهنگی	Culture Security
انتظام	Discipline
انجمن امنیت اطلاعات	Information Security Forum (ISF) Methods
انجمن پاسخ به رخدادهای امنیتی	Community Emergency Response Team
انجمن سیستم‌های امنیت ملّی	Committee on National Security Systems (CNSS)
انجمن نظارت و کنترل سیستم‌های اطلاعاتی	Information Systems Audit And Control Association (ISACA)
اهداف امنیتی	Security Objective
ب	
بازخورد	Feedback
بازگشت تحلیل سرمایه‌گذاری امنیتی	Return on Security Investment (ROSI)
بررسی وضعیت امنیت اطلاعات	Information Security Status Survey
برنامه- اجرا- کنترل- عمل	Plan-Do-Check-Act (PDCA)
بهبود فرآیند ارزیابی عملیاتی تهدیدها، دارایی‌ها و آسیب‌پذیری‌های حیاتی	Operationally Critical Threat, Asset, and Vulnerability Evaluation Allegro (OCTAVE Allegro)

واژه فارسی	برگردان انگلیسی
به روش‌های یا رهنمودهای بین‌المللی	Codes of practice
بیان نیازها و شناسایی اهداف امنیتی	Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives (EBIOS)

پ

پاسخ‌گویی	Accountability
پایش	Monitoring

ت

تجزیه و تحلیل بحرانی حالات و اثرات شکست	Failure Mode & Effect Critically Analysis (FMECA)
تجزیه‌وتحلیل حالات و اثرات شکست	Failure Modes and Effects Analysis (FMEA)
تجزیه‌وتحلیل درخت خطا	Fault Tree Analysis (FTA)
تحلیل	Analysis
تحلیل تهدیدها، مخاطره‌ها و آسیب‌پذیری‌های یک سیستم ارتباطی، روش طراحی سیستمی تحت عنوان "روش مدل‌سازی امنیتی TVRA	ETSI Threat Vulnerability & Risk Analysis (TVRA) Method
تحلیل عاملی مخاطره اطلاعات	Factor analysis of information risk (FAIR)
تحلیل مخاطره	Risk analysis
تحلیل و مدیریت مخاطره سیستم‌های اطلاعاتی	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)
تخمین قدرت کنترل	Control strength (CS)
تسهیل‌گر	Facilitator
تصمیم‌یار	Decision Support
تک نقاط شکست	Single Point of Failure (SPOF)
تکرار	Iteration
تهدید	Threat
تیم کِرَک	Crack Team

ج

جفت‌شدن متقابل	Cross Coupling
جنگ سرد	Cold War

چ

چارچوب ارزش در معرض مخاطره استاندارد	A Standard Value at Risk (VaR) Framework
چارچوب اهداف کنترلی برای اطلاعات و فناوری‌های مرتبط با آن	Control Objectives for Information and Related Technology (COBIT)
چارچوب تضمین فناوری اطلاعات	The Information Technology Assurance Framework (ITAF)
چارچوب مخاطره سازمانی کوزو	The Committee Of Sponsoring Organizations Of The Tread way Commission’s Enterprise Risk Management Framework (COSO ERM)
چارچوب مدیریت مخاطره	Risk Management Framework

ح

حادثه ناخواسته	Unwanted Incident

خ

خدمات به‌روزرسانی ویندوز سرور	Windows Server Update Service (WSUS)
خودارزیابی	Self-Assessment

د

واژه فارسی	برگردان انگلیسی
دارایی	Asset
دسترس‌پذیری	Availability
دفاع در عمق	Defense-in-depth
دفتر بازرگانی دولتی	The Office of Government Commerce (OGC)
دلفی	Delphi

ر

راهنما و چارچوب	Handbook and Framework
راهنمای مدیریت مخاطره امنیت مایکروسافت	The Microsoft’s Security Risk Management Guide
راهنمای مدیریت مخاطره‌های سیستم‌های فناوری اطلاعات	Special Publications Risk management Guide for Information Technology Systems
رایانش توزیع‌شده	Distributed Computing
رایانه	Computer
رخدادنگار	Logger
روش تحلیل مخاطرات **رایانه‌ای** بر **پایهٔ** سطوح	Methodology of Analysis of Computer Risks Directed by Levels (MARION)
روش تحلیل و مدیریت مخاطره آژانس مرکزی ارتباطات و مخابرات	Central Computing and Telecommunications Agency Risk Analysis and Management Method (CRAMM)
روش سنتی برای انجام تحلیل مخاطره امنیت اطلاعات	Traditional Risk Analysis of Information Security
روش‌ها و مدل‌ها	Methods and Models
روش‌های سنتی تحلیل مخاطره	Traditional Risk Analysis Methods
روشی برای تحلیل هماهنگ مخاطره	Me´thode Harmonise´e d’Analyse de Risques — Harmonised Risk Analysis Method (MEHARI)
رویداد اصلی	Top Event (TE)
ریزدانگی	Granularity

س

سازمان امنیت اطلاعات فرانسه	Club de la sécurité de l'information français (CLUSIF)
سازمان امنیت رایانه	Computer Security Organization (CSO)
سازمان جهانی استاندارد	International Organization for Standardization (ISO)
سازمان راهبری فناوری اطلاعات	IT Governance Institute (ITGI)
سازمان‌ها/ شرکت‌های کوچک و متوسط	Small and mid-size enterprises (SMEs)
سنجش	Evaluation
سنجش مخاطره	Risk Evaluation
سیستم تحلیل مخاطره عینی-مشاوره‌ای	Consultative Objective Risk Analysis System (CORAS)
سیستم مدیریت امنیت اطلاعات	Information Security Management System- ISMS

ش

شبکه آژانس پروژه‌های تحقیقاتی پیشرفته (آرپانِت)	The Advanced Research Projects Agency Network – ARPANet
شدت اثر مخاطره	Severity of failure
شدت/ مقدار خسارت احتمالی	Probable Loss Magnitude (PLM)
شدت/ میزان رویداد از دست رفته	Loss Event Frequency (LEF)
شناسایی	Identification
شورای فدرال اتریش	Austrian Federal Chancellery

ص

صحت	Integrity
صحت و سندیت	Authenticity

واژه فارسی	برگردان انگلیسی
صنعت هوافضای آمریکا	National Aeronautics and Space Administration (NASA)
ض	
ضعف	Weakness
ط	
طراحی-اجرا-کنترل-سنجش-گزارش	Plan–Do–Control–Measure–Report
طرح مقابله با مخاطره	Risk Treatment Plan (RTP)
ع	
عدد اولویت مخاطره	Risk Priority Number (RPN)
عدم انکار	Non-Repudiation
ف	
فدراسیون بین‌المللی حسابداران	International Federation of Accountants (IFAC)
فرا-روش	Meta-Method
فرآیند تسهیل‌شده ارزیابی مخاطره	Facilitated Risk Analysis and Assessment Process (FRAAP)
فرآیند ساده برای تحلیل مخاطره	Simple to Apply Risk Analysis (Sara)
فرآیند ساده‌سازی شده برای شناسایی مخاطره	Simplified Process for Risk Identification (Sprint)
ق	
قابلیت تهدید	Threat Capability (TCap)
قانون مدیریت امنیت اطلاعات فدرال	The Federal Information Security Management Act (FISMA)
ک	
کارت امتیازی مخاطره	RISK SCORECARD
کارت امتیازی مخاطره اطلاعات	Information Risk Scorecard
کتابچه راهنمای امنیت فناوری اطلاعات اتریش	Austrian IT Security Handbook
کتابچه راهنمای محافظت از اطلاعات پایه فناوری اطلاعات	IT Baseline Protection Manual (IT-Grundschutz)
کتابخانه زیرساخت فناوری اطلاعات	Information Technology Infrastructure Library (ITIL)
کمبودها	Deficiencies
کمیته سازمان‌های حامی کمیسیون تِردوی	Committee of Sponsoring Organizations of the Treadway Commission (Treadway)
کمیته فنی کمیسیون بین‌المللی الکتروتکنیک	The International Electrotechnical Commission (IEC)
گ	
گوی بلورین	Crystal-Ball-Gazing
م	
متخصصان	Experts
متدولوژی‌های تحلیل مخاطره اطلاعات	Information Risk Analysis Methodologies (IRAM)
متدولوژی‌های تحلیل مخاطره اطلاعات نسخه شماره (۲)	Information Risk Analysis Methodologies 2 (IRAM2)
متن‌باز	Open Source
مثلث سی.آی.اِی (محرمانگی، صحت، دسترس‌پذیری)	Confidentiality,Integrity, Availability (CIA)
محرمانگی	Confidentiality
محرمانگی، صحت، دسترس‌پذیری، احرازهویت و پاسخگویی	Confidentiality, Integrity, Availability, Authenticity and Accountability (CIAAA)
مخاطره فناوری اطلاعات	Risk IT

واژه فارسی	برگردان انگلیسی
مدل ارزش	Value Model
مدل کسب‌وکار برای امنیت اطلاعات	Business Model for Information Security (BMIS)
مدیران ارشد اطلاعات	Chief Information Officers (CIO)
مدیران ارشد امنیت اطلاعات	Chief Information Security Officers (CISO)
مدیریت دارایی‌های اطلاعاتی	Information Asset Management (IAM)
مدیریت مخاطره اطلاعات پایه	Fundamental Information Risk Management (FIRM)
مدیریت مخاطره سازمانی	Enterprise Risk Management (ERM)
مدیریت مخاطره‌های سیستم‌های اطلاعاتی-دید سازمانی	Information Systems Risk Management-Organizational Perspective
مطالعه مخاطرات و راهبری عملیات	Hazard and Operability study (HAZOP)
مکعب کوزو	COSO Cube
منظم و پیوسته	Routine
مهندسی اجتماعی	Social Engineering
مؤسسه استاندارد و تحقیقات صنعتی ایران	Institute of Standards & Industrial Research of Iran (MATSA)
مؤسسه استانداردهای مخابراتی اروپا	European Telecommunications Standards Institute (ETSI)
مؤسسه مدیریت پروژه	Project Management Institute (PMI)
مؤسسه ملّی استانداردها و فناوری	National Institute of Standards and Technology (NIST)

ن

ناشناس بودن	Anonymity
نرخ احتمال رویداد تهدید	Threat Event Frequency (TEF)
نقشه مخاطره	Risk Map
نمونه اولیه	Prototype
نهادینه‌سازی	Institutionalization

ه

هدف سنجش	Target Of Evaluation (TOE)

و

وزارت امورخارجه اسپانیا	Spanish Ministerio de Administraciones Públicas

فهرست منابع

- Abie, H. 2010, revised July 2012. "State of the Art Privacy Risk Analysis: Survey and Classification."
- Agrawal, V. 2017. "A Comparative Study on Information Security Risk Analysis Methods." *JCP* 12 (1): 57-67.
- ANSSI. 2019. *EBIOS Risk Manager – The Method Guide.* ANSSI.
- Ardeshir, A, M Amiri, and M Mohajeri. 2013. "Safety risk assessment in mass housing projects using combination of fuzzy FMEA, fuzzy FTA and AHP-DEA." *Iran Occupational Health* 10 (6).
- Army, U.S. 2006. "Failure Modes, Effects and Criticality Analysis (FMECA) for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities." Department of the Army, TM 5-698-4, Washington, DC.
- Baklouti, A, N Nguyen, J Choley, F Mhenni, and A Mlika. 2017. "Free and open source fault tree analysis tools survey." *2017 Annual IEEE International Systems Conference (SysCon).* 1-8. doi:10.1109/SYSCON.2017.7934794.
- Banaitiene, N, and A Banaitis. 2012. "Risk Management in Construction Projects." *in Risk Management - Current Issues and Challenges, InTech.*
- Becker, J.C, and G Flick. 1996. "A practical approach to failure mode, effects and criticality analysis (FMECA) for computing systems." *In Proceedings. IEEE High-Assurance Systems Engineering Workshop (Cat. No. 96TB100076).* IEEE. 228-236.
- Behnia, A, R Abd Rashid, and J.A Chaudhry. 2012. "A survey of information security risk analysis methods." *SmartCR* 2 (1): 79-94.
- Bertolini, M, M Bevilacqua, and R Massini. 2006. "FMECA approach to product traceability in the food industry." *Food control* 17 (2): 137-145.
- Bojanc, R. 2012. "Quantitative Model for Information Security Risk Management." *International School for Social and Business Studies, Celie.*
- Bojanc, R, and B Jerman-Blažicˇ. 2008. "An economic modelling approach to information security risk management." *International Journal of Information Management* 28 (5): 413-422.
- Bornman, W.G, and L Labuschagne. 2004. "A comparative framework for evaluating information security risk management methods." *In Information Security South Africa Conference.* 13-23.
- Bowles, J.B. 1998. "The new SAE FMECA standard." *In Annual Reliability and Maintainability Symposium. 1998 Proceedings. International Symposium on Product Quality and Integrity.* IEEE. 48-53.
- Bowles, J.B, and C.E Peláez. 1995. "Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis." *Reliability Engineering & System Safety* 50 (2): 203-213.

- Bozdag, E, U Asan, A Soyer, and S Serdarasan. 2015. "Risk prioritization in Failure Mode and Effects Analysis using interval type-2 fuzzy sets." *Expert Systems with Applications* 42 (8): 4000-4015.

- Braglia, M, M Frosolini, and R Montanari. 2003. "Fuzzy criticality assessment model for failure modes and effects analysis." *International Journal of Quality & Reliability Management.*

- Broderick, J.S. 2006. "ISMS, security standards and security regulations." *information security technical report* 11 (1): 26-31.

- Brotby, Krag W, and Gary Hinson. 2013. *PRAGMATIC Security Metrics: Applying Metametrics to Information Security.* Taylor & Francis Group.

- Caralli, Richard, James Stevens, Lisa Young, and William Wilson. 2007. "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process." Software Engineering.

- Cavusoglu, H, B Mishra, and S Raghunathan. 2004. "The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers." *International Journal of Electronic Commerce* 9 (1): 70-104.

- Central Bank. 2014. *Central Bank of The Islamic Republic of Iran.* August 11. https://www.cbi.ir/.

- Chanamool, N, and T Naenna. 2016. "Fuzzy FMEA application to improve decision-making process in an emergency department." *Applied Soft Computing* 43: 441-453.

- Chang, K.H, C.H Cheng, and Y.C Chang. 2010. "Reprioritization of failures in a silane supply system using an intuitionistic fuzzy set ranking technique." *Soft Computing* 14 (3): 285.

- Chen, P.S, and M.T Wu. 2013. "A modified failure mode and effects analysis method for supplier selection problems in the supply chain risk environment: A case study." *Computers & Industrial Engineering* 66 (4): 634-642.

- Chen, P.S, and M.T Wu. 2013. "A modified failure mode and effects analysis method for supplier selection problems in the supply chain risk environment: A case study." *Computers & Industrial Engineering* 66 (4): 634-642.

- Chin, K.S, D.W Tang, J.B Yang, S.Y Wong, and H Wang. 2009. "Assessing new product development project risk by Bayesian network with a systematic probability generation methodology." *Expert Systems with Applications* 36 (6): 9879-9890.

- CLUSIF. 2015. *MEHARI: Risk Assessment with MEHARI Method.* Paris, France: Club de la sécurité de l'information français (CLUSIF).

- Colli, A. 2015. "Failure mode and effect analysis for photovoltaic systems." *Renewable and Sustainable Energy Reviews* 50: 804-809.

- Collier, M. 2005. "Basic Vulnerability Issuse for SIP Security." *SecureLogix Corporation.*

- Creasey, Jason, and Simon Marvell. 2013. *A complete Information Risk Management solution For ISF Members using IRAM and STREAM.* Information Security Forum (ISF), Stream.

- deMeer, J, and A Rennoch. 2011. "The ETSI TVRA Security-Measurement Methodology by Means of TTCN-3 Notation." *In 10th TTCN-3 User Conference.*

- Dubois, É, P Heymans, N Mayer, and R Matulevičius. 2010. "A systematic approach to define the domain of information system security risk management." *In Intentional Perspectives on Information Systems Engineering* (Springer) 289-306.

- Fang, Y, Q Liang, and Z Jia. 2011. "Knowledge sharing risk warning of industry cluster: an engineering perspective." *Systems Engineering Procedia* 2 (1): 412-421.

- Feledi, D, and S Fenz. 2012. "Challenges of web-based information security knowledge sharing." *In 2012 Seventh international conference on availability, reliability and security.* IEEE. 514-521.

- Feng, N, H.J Wang, and M Li. 2014. "A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis." *Information sciences* 256: 57-73.

- Fenz, S. 2012. "Increasing knowledge capturing efficiency by enterprise portals." *VINE.*

- Fenz, S, A Ekelhart, and E Weippl. 2008. "Fortification of IT security by automatic security advisory processing." *In 22nd International Conference on Advanced Information Networking and Applications (aina 2008).* IEEE. 575-582.

- Fenz, S, A Ekelhart, and T Neubauer. 2009. "Business process-based resource importance determination." *In International Conference on Business Process Management.* Berlin, Heidelberg: Springer. 113-127.

- Fenz, S, and A Ekelhart. 2009. "Formalizing information security knowledge." *In Proceedings of the 4th international Symposium on information, Computer, and Communications Security.* 183-194.

- Force, J.T. 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (No. NIST Special Publication (SP) 800-37 Rev. 2).* National Institute of Standards and Technology.

- Hergon, E, H Crespeau, and P Rouger. 1994. "Failure mechanisms in the transfusion process. Importance of anticipatory operational safety analysis." *Transfusion clinique et biologique: journal de la Societe francaise de transfusion sanguine* 1 (5): 379-386.

- Hinson, Gray. 2013. *Analog Risk Assessment method, ARA [UPDATED x2]*. 8 29. http://blog.noticebored.com/2013/08/analog-risk-assessment-method-ara.html.

- Hubbard, D.W. 2009. "The failure of risk management: Why it's broken and how to fix it." *John Wiley & Sons.*

- n.d. *Information Risk Management.* «ایزو ۲۷۰۰۱». Accessed 4 22, 2017. http://www.iso27001security.com/html/risk_mgmt.html#RAmethods.

- Information Security Forum. 2016. *Information Risk Assessment Methodology 2 (IRAM2) - Information Security Forum.* Accessed Nov 23, 2016. https://www.securityforum.org/tool/information-risk-assessmentmethodology-iram2/.
- Institute of Standards & Industrial Research of IR. 2008. "IT- security technologiesand information security management procedures."
- Institute, Information Security. 2005. *Information Security*.
- Ionita, D. 2013. "Current established risk assessment methodologies and tools." *Master's thesis, University of Twente.*
- ISACA. 2012. *COBIT 5.* USA: Information Systems Audit and Control Association (ISACA).
- ISACA. 2013. *COBIT 5 for Risk.* USA: Information Systems Audit and Control Association (ISACA).
- ISACA. 2013. *COBIT 5 for Risk.* USA: Information Systems Audit and Control Association (ISACA).
- ISACA. 2019. *COBIT® 5 for Risk (An ISACA Framework).* Information Systems Audit and Control Association (ISACA). www.isaca.org/cobit5.
- ISACA. 2009. *Risk IT Framework (Based on COBIT).* USA: Information Systems Audit and Control Association (ISACA).
- Jansen, W. 2010. "Directions in Security Metrics Research." *Diane Publishing.*
- Jong, C.H, K.M Tay, and C.P Lim. 2013. "Application of the fuzzy failure mode and effect analysis methodology to edible bird nest processing." *Computers and electronics in agriculture* 96: 90-108.
- Kiran, K, S Mukkamala, A Katragadda, and D Reddy. 2013. "Performance and analysis of risk assessment methodologies in information security." *International Journal of Computer Trends and Technology (IJCTT)* 4 (10): 3685-3692.
- KPMG, LLP. 2001. "Enterprise Risk Management, An emerging model for building shareholder value."
- Kutlu, A.C, and M Ekmekçioğlu. 2012. "Fuzzy failure modes and effects analysis by using fuzzy TOPSIS-based fuzzy AHP." *Expert Systems with Applications* 39 (1): 61-67.
- Kwon, S, S Jang, J Lee, and S Kim. 2007. "Common defects in information security management system of Korean companies." *Journal of Systems and Software* 80 (10): 1631-1638.
- Lee, W, W Fan, M Miller, S.J Stolfo, and E Zadok. 2002. "Toward cost-sensitive modeling for intrusion detection and response." *Journal of Computer Security* 10 (1): 5-22.
- Liu, H.C, J.X You, X.J Fan, and Q.L Lin. 2014. "Failure mode and effects analysis using D numbers and grey relational projection method." *Expert Systems with Applications* 41 (10): 4670-4679.

- Liu, H.C, J.X You, X.Y You, and M.M Shan. 2015. "A novel approach for failure mode and effects analysis using combination weighting and fuzzy VIKOR method." *Applied soft computing* 28: 579-588.

- Liu, H.C, L Liu, and N Liu. 2013. "Risk evaluation approaches in failure mode and effects analysis: A literature review." *Expert systems with applications* 40 (2): 828-838.

- Liu, H.C, L Liu, N Liu, and L.X Mao. 2012. "Risk evaluation in failure mode and effects analysis with extended VIKOR method under fuzzy environment." *Expert Systems with Applications* 39 (17): 1926-12934.

- Lo, C.C, and W.J Chen. 2012. "A hybrid information security risk assessment procedure considering interdependences between controls." *Expert Systems with Applications* 39 (1): 247-257.

- Macedo, F, and M.M Da Silva. 2012. "Comparative study of information security risk assessment models." *Universidad Técnica de Lisboa, Lisboa*.

- Malekalkalami, M. 2013. "Evaluating the performance of information security management at the central libraries of public universities in Tehran, according to the international standard-ISO/IEC." *Journal of Information Processing and Management* 28 (4): 895-916.

- Mazza, R. 2009. "Introduction to information visualization." *Springer Science & Business Media.*

- McCormick, B.H, A.D Thomas, and D.B Maxine. 1987. "Visualization in scientific computing." *Computer graphics* 21 (6).

- Montesino, R, and S Fenz. 2011. "Information security automation: how far can we go?" *In 2011 Sixth International Conference on Availability, Reliability and Security.* IEEE. 280-285.

- Nalik, S.A, and B Holt. 2013. "Factors that affect the adoption of Enterprise Risk Management (ERM)." *OR Insight* 24 (4): 253-269.

- Niesen, C, P Houy, P Fettke, and P Loos. 2016. "Towards an Integrative Big Data Analysis Framework for Data-Driven Risk Management in Industry 4.0." *in 2016 49th Hawaii International Conference on System Sciences (HICSS).* 5065-5074.

- Nosworthy, J. 2000. "A practical risk analysis approach: managing BCM risk." *Computers & security* 19 (7): 596-596.

- Ostrowska, M, and S Mazur. 2015. "Risk in crisis situation." *procedia economics and finance Elsevier* 23 (10): 615-621.

- Pan, L, and A Tomlinson. 2016. "A systematic review of information security risk assessment." *International Journal of Safety and Security Engineering* 6 (2): 720-281.

- Peace, C. 2017. "The reasonably practicable test and work health and safety-related risk assessments." *Journal of Employment Relations* 42 (2): 61-78.

- Rausand, M, A Barros, and A Hoyland. 2020. "System reliability theory: models, statistical methods, and applications." *John Wiley & Sons.*

- Rhee, H.S, Y.U Ryu, and C.T Kim. 2012. "Unrealistic optimism on information security management." *Computers & Security* 31 (2): 221-232.

- Rosenquist, M. 2009. *Prioritizing information security risks with threat agent risk assessment.* Intel Corporation.

- Ross, R.S. 2011. "Managing information security risk: Organization, mission, and information system view."

- Saizy-Callaert, S, R Causse, A Thébault, and C Chouaïd. 2002. "Failure mode, effects and criticality analysis (FMECA) as a means of improving the hospital drug prescribing process." *International Journal of Risk & Safety in Medicine* 15 (3-4): 193-202.

- Saleh, M.S, and A Alfantookh. 2011. "A new comprehensive framework for enterprise information security risk management." *Applied computing and informatics* 9 (2): 107-118.

- SESAR. 2011. *Selection of Risk Assessment Methods Object of Study.* University of Trento, SESAR JOINT UNDERTAKING.

- Shafiee, M Shafiee, and F Dinmohammadi. 2014. "An FMEA-based risk assessment approach for wind turbine systems: a comparative study of onshore and offshore." *Energies* 7 (2): 619+642.

- Shamala, P, R Ahmad, and M Yusoff. 2013. "A conceptual framework of info structure for information security risk assessment (ISRA)." *Journal of Information Security and Applications* 18 (1): 45-52.

- Shameli-Sendi, A, R Aghababaei-Barzegar, and M Cheriet. 2016. "Taxonomy of information security risk assessment (ISRA)." *Computers & security* 57: 14-30.

- Sharma, R.K, D Kumar, and P Kumar. 2005. "Systematic failure mode effect analysis (FMEA) using fuzzy linguistic modelling." *Systematic failure mode effect analysis (FMEA) using fuzzy linguistic modelling.*

- Solms, B.V. 2000. "Information Security — The Third Wave?" *Computers & Security* 19 (7): 615-620.

- Song, W, X Ming, Z Wu, and B Zhu. 2014. "A rough TOPSIS approach for failure mode and effects analysis in uncertain environments." *Quality and Reliability Engineering International* 30 (4): 473-486.

- Sonnenreich, W, J Albanese, and B Stout. 2006. "Return on security investment (ROSI)-a practical quantitative model." *Journal of Research and Practice in Information Technology* 38 (1): 45-56.

- Sourceforge. 2015. *The CORAS Method.* Sourceforge. http://coras.sourceforge.net/index.html.

- Spears, J.L. 2004. "A HOLISTIC RISK ANALYSIS METHOD FOR IDENTIFYING INFORMATION SECURITY RISKS." *In: Dowland P., Furnell S., Thuraisingham B., Wang X.S. (eds) Security Management, Integrity, and Internal Control in Information Systems.* Springer, Boston, MA. 185-202. doi:https://doi.org/10.1007/0-387-31167-X_12.

- Stamatis, D.H. 2003. "Failure mode and effect analysis: FMEA from theory to execution." *Quality Press.*

- Standard, M. 1980. "Procedures for performing a failure mode, effects and criticality analysis." (Department of Defense, Washington, DC, Standard No. MIL-STD-1629A).

- Sulaman, S.M, K Weyns, and M Höst. 2013. "A review of research on risk analysis methods for IT systems." *In Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering.* 86-96.

- TR187002, ETSI. 2010. " Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) Threat and Risk Analysis."

- TR187011, ETSI. 2008. "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; ." *Application of ISO-15408-2 requirements to ETSI standards –guide, method and application with examples.*

- TS102165-1, ETSI. 2006. "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat Vulnerability and Risk Analysis." *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat Risk Vulnerability Analysis* 12.

- Van Niekerk, J.F, and R Von Solms. 2010. "Information Security Culture: A Management Perspective." *Computers & Security* 29 (4): 476-486.

- Von Solms, B. 2006. "Information Security-The Fourh Wave." *Computers & Security* 25 (3): 165-168.

- Vose, D. 2008. "Risk Analysis: A Quantitative Guide." *John Wiley and Sons.*

- Wang, Y.M, K.S Chin, G.K Poon, and J.B Yang. 2009. "Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean." *Expert systems with applications* 36 (2): 1195-1207.

- Wangen, G, and E Snekkenes. 2013. "A taxonomy of challenges in information security risk management." *In Proceeding of Norwegian Information Security Conference/Norsk informasjonssikkerhetskonferanse-NISK 2013-Stavanger, 18th-20th November 2013.* Akademika Forlag.

- Wangen, G.B. 2017. "Cyber Security Risk Assessment Practices: Core Unified Risk Framework." *Thesis for the degree of Philosophiae Doctor* (Norwegian University of Science and Technology).

- Ware, C. 2019. "Information visualization: perception for design." *Morgan Kaufmann.*

- Weller, Nick. 2015. *COSO.* http://www.accaglobal.com/uk/en/student/exam-support-resources/professional-exams-study-resources/p1/technical-articles/coso-enterprise-risk-management-framework-part-1.html.

- Whitman, Michael E, and Herbert J Mattord. 2016. *Principles of Information Security*. Boston. USA: CENGAGE Learning.

- Williams, E, and R Talley. 1994. "The use of failure mode effect and criticality analysis in a medication error subcommittee." *Hospital pharmacy* 29 (4): 331-2.

- Xiao, N, H.Z Huang, Y Li, L He, and T Jin. 2011. "Multiple failure modes analysis and weighted risk priority number evaluation in FMEA." *Engineering Failure Analysis* 18 (4): 1162-1170.

- Xiaolin, C, T Xiaobin, Z Yong, and X Hongsheng. 2008. "A markov game theory-based risk assessment model for network information system." *In 2008 International Conference on Computer Science and Software Engineering.* IEEE. 1057-1061.

- Xiao-yan, G, Y Yu-qing, and L Li-lei. 2011. "An information security maturity evaluation mode." *Procedia Engineering.* 335-339.

- Yang, J, H.Z Huang, L.P He, S.P Zhu, and D Wen. 2011. "Risk evaluation in failure mode and effects analysis of aircraft turbine rotor blades using Dempster–Shafer evidence theory under uncertainty." *Engineering Failure Analysis* 18 (8): 2084-2092.

- Yari, S. 2017. "Assessment of potential risk by the failure mode and effects analysis in an air conditioning equipment manufacturing company." *Journal of Safety Promotion and Injury Prevention* 5 (2): 89-96.

- Yazar, Z. 2002. *A qualitative risk analysis and management tool–CRAMM.* SANS Institute InfoSec Reading Room, 12-32.

- Zhang, X, F Jin, and P Liu. 2013. "A grey relational projection method for multi-attribute decision making based on intuitionistic trapezoidal fuzzy number." *Applied Mathematical Modelling* 37 (5): 3467-3477.

- Zudin, R. 2014. "Analysis of information risk management methods."

Information Security Risk: Assessment and Management Methods

Hamid Reza Khedmatgozar

Assistant professor - Iranian Research Institute for Information Science and Technology (IranDoc)

Sanaz Ghorbanloo

Researcher - Iranian Research Institute for Information Science and Technology (IranDoc)

2021

شرکت فنی و مهندسی امن پردازان کویر

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

Information Security Risk: Assessment and Management Methods

Hamid Reza Khedmatgozar
Sanaz Ghorbanloo

Iranian Research Institute
for Information Science and Technology
(IranDoc)

APK
Engineering and Technical Company
Amn Pardazan Kavir

ISBN:978-622-98708-0-8
9 786229 870808