



Received:  
11 September 2024  
Revised:  
10 November 2024  
Accepted:  
01 November 2024  
Published:  
22 May 2025  
P.P: 41-62

ISSN: 2008-3564  
E-ISSN: 2645-5258



## Information security risk management model in the business integration process in banks and credit institutions

Pegah Shayestehfar <sup>1\*</sup> | Elham Moghadam niya <sup>2</sup> | Amin Mohajer<sup>3</sup>

### Abstract

Business processes are considered the cornerstone of banks and financial institutions, but they are increasingly becoming the focus of attacks. In order to mitigate cyber attacks, especially those involving critical business processes, information security risks should be considered in the design of business processes. In this paper, the MARISMA-BP model (MARISMA for Business) is proposed, which is a model for assessing and managing information security risks for business process models. To demonstrate the applicability of the proposed model, the MARISMA-BP model is applied to a business process scenario in a bank. Based on the findings of the MARISMA-BP model, the intersection of these steps and strategies for managing information security risks with business processes in banks and financial institutions helps to improve information security and reduce risks, and ultimately leads to increased trust among customers and other internal and external stakeholders and business sustainability.

**Keywords:** Business process model; Information security risk assessment and management; Risk paradigm.

1. Student PHD, Department of Information Technology, Hamadan Branch, Islamic Azad University, Hamadan, IRAN
2. Assistant Professor, Department of Technology, SR.C, Islamic Azad University, Tehran, Iran  
e.moghadamnia@srbiau.ac.ir
3. Student PHD, Department of Information Technology, Islamic Azad University, Kish, IRAN

**Cite this Paper:** Shayestehfar, P & Moghadamniya, E & Mohajer, A (2025). Information security risk management model in the business integration process in banks and credit institutions. **Social Crisis Management**, 1(17), 41–62.

**Dor:** 20.1001.1.20083564.1404.17.1.5.7

**Publisher:** Imam Hussein University

© Authors



This article is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/) (CC BY 4.0).



## الگوی مدیریت مخاطرات امنیت اطلاعات در فرآیند یکپارچه‌سازی کسب‌وکار در بانک‌ها و مؤسسات اعتباری

پگاه شایسته‌فر<sup>۱</sup> || الهام مقدم‌نیا<sup>۲</sup> || امین مهاجر<sup>۳</sup>

دوره هفدهم  
بهار ۱۴۰۴

### مقاله پژوهشی

تاریخ دریافت: ۱۴۰۳/۱۱/۰۷  
تاریخ بازنگری: ۱۴۰۳/۱۲/۱۹  
تاریخ پذیرش: ۱۴۰۴/۰۲/۱۰  
تاریخ انتشار: ۱۴۰۴/۰۳/۰۱

صص: ۶۲-۴۱

شابا چاپی: ۳۵۶۴-۲۰۰۸  
الکترونیکی: ۵۲۵۸-۲۶۴۵



### چکیده

فرآیندهای کسب‌وکار سنگ بنای بانک‌ها و مؤسسات مالی در نظر گرفته می‌شوند، اما بانک‌ها و مؤسسات مالی به طور فزاینده‌ای در کانون توجه حملات دشمن قرار می‌گیرند. در جهت کاهش حملات سایبری به خصوص حملاتی که در برگیرنده فرایندهای حیاتی کسب‌وکار هستند، باید در طراحی فرآیندهای کسب‌وکار، مخاطرات امنیت اطلاعات در نظر گرفته شود. در این مقاله، الگوی ماریسما پیشنهاد شده که یک الگوی برای ارزیابی و مدیریت مخاطرات امنیت اطلاعات در فرایند مدل‌های کسب‌وکار می‌باشد. برای نشان دادن قابلیت کاربردی الگوی پیشنهادی، الگوی ماریسما ب-پ برای یک سناریوی فرآیند کسب‌وکار در بانک‌ها اعمال شده است. با توجه به یافته‌ها، الگوی ماریسما ب-پ اساس کار می‌باشد، تلاقی این مراحل و استراتژی‌های مدیریت مخاطرات امنیت اطلاعات در فرآیند کسب‌وکار در بانک‌ها و مؤسسات مالی، به ارتقاء امنیت اطلاعات و کاهش مخاطرات کمک می‌کند و در نهایت به افزایش اعتماد مشتریان و سایر ذی‌نفعان درونی و بیرونی و پایداری کسب‌وکار منجر خواهد شد.

کلیدواژه‌ها: فرآیند کسب‌وکار؛ ارزیابی و مدیریت مخاطرات، امنیت اطلاعات و الگوی ماریسما.

۱. دانشجوی دکتری گروه مدیریت فناوری اطلاعات، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران.

۲. نویسنده مسئول: استادیار گروه مدیریت فناوری، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران. e.moghadamnia@srbiau.ac.ir

۳. دانشجوی دکتری گروه مدیریت فناوری اطلاعات، واحد بین‌المللی کیش، دانشگاه آزاد اسلامی، جزیره کیش، ایران

**استناد:** شایسته‌فر، پگاه و مقدم‌نیا، الهام و مهاجر، امین (۱۴۰۴). الگوی مدیریت مخاطرات امنیت اطلاعات در فرآیند یکپارچه‌سازی کسب‌وکار در بانک‌ها و مؤسسات اعتباری، **مدیریت بحران‌های اجتماعی**، ۴(۱۷)، ۶۲-۴۱.

**Dor:** 20.1001.1.20083564.1404.17.1.5.7

ناشر: دانشگاه جامع امام حسین (ع) © نویسندگان



این مقاله تحت لیسانس آفرینندگی مردمی (Creative Commons License- CC BY) در دسترس شما قرار گرفته است.

## مقدمه و بیان مسئله

فرایندهای کسب‌وکار (BP)<sup>۱</sup> به عنوان سنگ بنای بانک‌ها و مؤسسات مالی در انتقال اهداف و اهداف راهبردی حاکمیتی به سیستم‌های اطلاعاتی که فعالیت‌های مورد نیاز را انجام می‌دهند و تصمیم‌گیری را تسهیل می‌کنند، در نظر گرفته می‌شوند (پرز-آلوارز و همکاران، ۲۰۱۸). با این حال، فرایندهای کسب‌وکار از نظر امنیتی بدون مخاطرات نیستند، (میکرو، ۲۰۲۳) یک مثال حمله به فرآیند کسب‌وکار است که از دانش عمیق رفتار این فرایندها استفاده می‌کند تا هرگونه عمل آسیب‌پذیر، سیستم‌های مستعد یا نقاط ضعف در آن‌ها را شناسایی کند. سپس مهاجم بخشی از وظایف خاص را تغییر می‌دهد و به این ترتیب به اطلاعات محرمانه دسترسی پیدا می‌کند یا فرایندهای غیرمجاز را اجرا می‌کند. این نوع حملات به طرز فزاینده‌ای متداول‌تر می‌شوند و حتی گزارش‌هایی وجود دارد که بیان می‌کند تقریباً نیمی از سازمان‌های تحلیل شده تحت تأثیر حملات مختل‌کننده فرایندهای کسب‌وکار قرار گرفته‌اند (لرد ریمورین و همکاران، ۲۰۲۳).

بنابراین، یک رویکرد جامع برای مدیریت مخاطرات باید سیستم‌های اطلاعاتی و دیدگاه سازمان و فرایندهای کسب‌وکار را در نظر بگیرد. تحلیل مخاطرات امنیتی باید عملیات و استفاده از سیستم‌های اطلاعاتی را در ارتباط با دیگر مؤلفه‌های مخاطرات سازمانی که سازمان‌ها باید به آن‌ها پردازند، مرتبط کند (روز و همکاران، ۲۰۱۹). مدیریت مخاطرات امنیت اطلاعات با این حال، فرایندهای کسب‌وکار را به عنوان مکانیزم‌هایی برای دستیابی به اهداف سازمان در نظر نمی‌گیرد. با این حال، اینکه سازمان‌ها به سیستم‌های اطلاعاتی برای دستیابی به اهدافشان و انجام عملکردهای کسب‌وکارشان وابسته هستند، از اهمیت کمتری برخوردار نیست. علاوه بر این، موفقیت مأموریت‌ها و عملکردهای کسب‌وکار به حفاظت از محرمانگی، یکپارچگی و دسترسی به اطلاعاتی که توسط سیستم‌های اطلاعاتی برای انجام مأموریت و عملکردهای کسب‌وکار پردازش، ذخیره و انتقال می‌یابد، و همچنین حفظ حریم شخصی افراد و داده‌ها بستگی دارد (NIST.SP.800-37، ۲۰۱۸)، (باختینا و همکاران، ۲۰۲۳) و (شاملی و همکاران، ۲۰۲۰).

1 Business processes (BP)

بنابراین، یک رویکرد مؤثر ارزیابی مخاطرات به مدیریت ارشد یک سازمان کمک می کند تا تصمیمات بهینه ای اتخاذ کند و از خسارات جلوگیری کند (تارکیس و همکاران، ۲۰۱۹)، که این نیازمند انتخاب و اجرای تدابیر حفاظتی است تا مخاطرات شناسایی شده را درک، پیشگیری، بازدارندگی، کاهش یا کنترل کند (سان و همکاران، ۲۰۱۹).

پیشنهادهای قبلی به مدیریت مخاطرات در فرآیندهای کسب و کار توجه کرده اند. متأسفانه، این پیشنهادات بر روی توسعه ی گسترش های مدل فرآیند کسب و کار تمرکز کرده بودند تا حمایت از تجزیه و تحلیل مخاطرات را در زمینه ی مدل دنبال کنند (سوریادی و همکاران، ۲۰۱۴)، (وارلا-واکا و همکاران، ۲۰۱۹)، (گریفور و همکاران، ۲۰۱۷). علاوه بر این، این رویکردها برخی ویژگی های جالب برای مدیریت مخاطرات را تحلیل نمی کنند، به عنوان مثال، اینکه فرآیندهای کسب و کار می توانند به عنوان سازوکاری برای یکپارچه سازی مخاطرات خاص، مانند داده های کلان (وولف و همکاران، ۲۰۱۶)، اینترنت اشیا (IoT) (جانیش و همکاران، ۲۰۲۰) یا سیستم های سایر فیزیکی (CPS)<sup>۱</sup> (بازان و همکاران، ۲۰۲۰) در اکوسیستم ها استفاده شوند. بنابراین، ممکن است فرآیند کسب و کار به وسیله تکنولوژی های زیرساختی خود مورد تهدید قرار گیرد. روش های ارزیابی مخاطرات سیستم های IT<sup>۲</sup> (فناوری اطلاعات) سنتی (پن و همکاران، ۲۰۱۶) برای اعمال به فرآیندهای کسب و کار طراحی نشده اند و بنابراین، نمی توانند به طور مستقیم اعمال شوند.

اگرچه ارزیابی مخاطرات سیستم های IT سنتی به اندازه کافی بالغ شده اند، اما رویکردهای جدیدی برای مقابله با مشکلات امنیتی رو به رشد که به دلیل تفاوت های بزرگ بین سیستم های IT و مخاطرات فرآیندهای کسب و کار به وجود می آید، لازم است (مارسینکوفسکی و همکاران، ۲۰۱۲). اگرچه پیشنهادها متعددی برای رسیدگی به ارزیابی و مدیریت مخاطرات IT به طور نظام مند وجود داشته است، این پیشنهادها معمولاً در به کارگیری عملی آن ها در محیط های بسیار پویا و به هم پیوسته با مشکلاتی مواجه شده اند (ابیویه و همکاران، ۲۰۲۱) و (الکساندروف و همکاران، ۲۰۲۱).

1 Cyber-Physical Systems (CPS)

2 Information Technology (IT)

در واقع، برای اینکه روش‌های ارزیابی و مدیریت مخاطرات واقعاً مؤثر باشند، باید قابل اجرا باشند (از نظر نیاز به منابع انسانی، فنی و اقتصادی محدود) برای کسب و کارهای کوچک و متوسط (الشوابکه و همکاران، ۲۰۱۹)، باید به اندازه کافی ساده باشند تا بتوانند به هر نوع بخشی سازگار شوند (جاوید و همکاران، ۲۰۱۷)، باید به مخاطرات نه تنها در سطح فردی در سازمان، بلکه همچنین مخاطرات ناشی از ارتباط شرکت با محیطش و سایر شرکت‌ها (مخاطرات انجمنی) (الحواری و همکاران، ۲۰۱۲) توجه کنند. علاوه بر این، باید روابطی را که ممکن است بین شرکت‌های مختلف در یک گروه وجود داشته باشد (مخاطرات سلسله‌مراتبی) در نظر بگیرند، که منجر به مفهوم مخاطرات مشترک می‌شود (پترسکو و همکاران، ۲۰۱۹).

چالش کلیدی دیگر امکان استفاده مجدد از دانش به دست آمده در تحلیل‌های مخاطرات قبلی است و داشتن ابزارهای پشتیبانی که کارها را خودکار کرده و رعایت روش‌های به کار رفته را آسان کند، امری ضروری است. نویسندگان در (آرگیروپولوس و همکاران، ۲۰۲۰) پیشنهاد می‌کنند که حوزه مهندسی الزامات امنیت و حوزه الگوهای امنیتی با هم ترکیب شوند و به همراه مدل‌سازی فرآیندهای کسب و کار، مجموعه‌ای از الگوهای امنیتی در سطح فرآیند تولید کنند که برای پیاده‌سازی امنیت در یک مدل فرآیند کسب و کار خاص استفاده شوند.

پیشرفت سریع فناوری‌های دیجیتال به طور قابل توجهی بخش بانکداری را متحول کرده است و منجر به ظهور بانکداری دیجیتال به عنوان یکی از اجزای اصلی خدمات مالی مدرن شده است. در طول دو دهه گذشته، گسترش اینترنت، تلفن‌های هوشمند و فناوری‌های ارتباطی شیوه ارائه خدمات بانکی را متحول کرده است و آنها را کاربرپسندتر، کارآمدتر و در دسترس‌تر کرده است (ایندریاساری و همکاران، ۲۰۲۲) و (بالکان و همکاران، ۲۰۲۱).

(داود و همکاران، ۲۰۲۳) مجموعه‌ای از اصول طراحی (یا حتی الگوهای) مبتنی بر مخاطرات را استخراج و تأیید کرده و می‌تواند برای جلوگیری/کاهش رویدادهای مخاطره‌آمیز در آن حوزه خاص اعمال شود.

علاوه بر این، ادغام فناوری‌های مالی نوآورانه مانند بلاک چین، هوش مصنوعی، و تجزیه و تحلیل داده‌های بزرگ، قابلیت‌های بانکداری دیجیتال را افزایش داده و خدمات شخصی و کارآمد را به مشتریان ارائه می‌دهد (تاشتیریوف و همکاران، ۲۰۲۳). این فن‌آوری‌ها بانک‌ها را قادر می‌سازند

تا عملیات خود را بهینه کنند، هزینه ها را کاهش دهند و رضایت مشتری را با ارائه راه حل های مالی در زمان واقعی و مناسب بهبود بخشند (بالکان و همکاران، ۲۰۲۱) (ویوش و همکاران، ۲۰۲۰). با این حال، دگرگونی سریع دیجیتال همچنین چالش هایی را در رابطه با امنیت داده ها، حریم خصوصی و انطباق با مقررات ایجاد می کند که باید برای اطمینان از رشد پایدار بانکداری دیجیتال مورد توجه قرار گیرد (تاشمیروف و همکاران، ۲۰۲۳) و (سبتی و همکاران، ۲۰۲۲).

بخش بانکداری دیجیتال شیوه انجام تراکنش های مالی را متحول کرده است و راحتی و دسترسی بی سابقه ای را به کاربران در سراسر جهان ارائه می کند. با این حال، این تحول همچنین تعداد بی شماری از تهدیدات امنیت سایبری را معرفی کرده است که مخاطرات قابل توجهی هم برای مؤسسات مالی و هم برای مشتریان آنها ایجاد می کند. اتکای فزاینده به اینترنت و برنامه های تلفن همراه برای فعالیتهای بانکی، این بخش را به هدف اصلی برای مجرمان سایبری تبدیل کرده است که از تکنیک های پیچیده برای سوء استفاده از آسیب پذیری ها و سرقت اطلاعات حساس استفاده می کنند (نوتالا پاتی و همکاران، ۲۰۲۳).

در این زمینه، ضرورت اقدامات امنیت سایبری قوی در بانکداری را نمی توان اغراق کرد. امنیت سایبری نیز در زمینه مراقبت های بهداشتی مورد بررسی قرار گرفته است (آدبوکولا و همکاران، ۲۰۲۰) با این حال، تمرکز ما در اینجا بانکداری است.

حوزه پیچیده ارزیابی مخاطرات امنیت سایبری در بانکداری، با تمرکز بر روش شناسی و بهترین شیوه های ضروری برای حفاظت از مؤسسات مالی در عصر تهدیدات سایبری مداوم و پیچیده در این مطالعه بررسی می شود. از آنجایی که بخش مالی در حال حرکت در یک چشم انداز تهدید در حال تحول است که با بدافزارهای پیشرفته، حملات فیشینگ، تهدیدات داخلی و آسیب پذیری های ذاتی در سیستم های دیجیتال مشخص می شود، نیاز به یک چارچوب ارزیابی مخاطرات امنیت سایبری جامع و تطبیقی بسیار مهم می شود.

(اونیمسی و همکاران، ۲۰۲۳) به بررسی روش شناسی، به بهترین شیوه های ضروری برای مدیریت مؤثر مخاطرات امنیت سایبری در بانکداری پرداخته اند. این یکپارچه سازی اطلاعات تهدید پیشگیرانه، مکانیسم های نظارت مستمر، و برنامه ریزی واکنش به حادثه به خوبی تعریف شده به عنوان اجزای جدایی ناپذیر یک استراتژی امنیت سایبری انعطاف پذیر را بررسی می کند. علاوه بر

این، این تحقیق نقش تحول‌آفرین فناوری‌های پیشرفته مانند هوش مصنوعی و یادگیری ماشین را در افزایش کارایی و سازگاری فرآیندهای ارزیابی مخاطرات برجسته می‌کند.

با توجه به ارزیابی و مدیریت مخاطرات برای فرآیندهای کسب و کار، چندین پیشنهاد جالب در طول دهه گذشته ارائه شده است. در (وارلا و همکاران، ۲۰۱۹)، نویسندگان چندین رویکرد را که مدیریت مخاطرات را در فرآیندهای کسب و کار ادغام می‌کنند، مقایسه می‌کنند و به این نتیجه می‌رسند که کمبود جدی ابزارها و سازوکارهایی برای خودکارسازی فرآیند ارزیابی مخاطرات و مدیریت فرآیندهای کسب و کار وجود دارد.

این پیشنهادات کمک‌های جالبی می‌کنند، اما نمی‌توان آن‌ها را به‌اندازه کافی کامل و قابل اجرا در محیط‌های واقعی در نظر گرفت، زیرا شامل یک مدل اولیه است که تنها برخی از دستورالعمل‌ها را برای ساخت یک مدل کامل ارائه می‌دهد.

طراحی و اجرای فرآیندهای کسب و کار باید با مدیریت مخاطرات به منظور جلوگیری یا کاهش تأثیر حملات بر فرآیندهای کسب و کار یکپارچه شود.

چارچوب **MARISMA** (روش‌شناسی برای تحلیل مخاطرات در سیستم‌های اطلاعاتی، با استفاده از الگوهای متا و انعطاف‌پذیری) امکان مدیریت مخاطرات را به صورت جامع در این زمینه‌های مختلف فراهم می‌کند (روزادو و همکاران، ۲۰۲۱) و (روزادو و همکاران، ۲۰۲۲).

پس از تجزیه و تحلیل فرآیندها و چارچوب‌های مخاطرات فعلی، متوجه شده‌ایم که سطوح فرآیند سازمانی و کسب و کار، اغلب نادیده گرفته می‌شوند؛ به همین دلیل در این مقاله چارچوب **MARISMA** در سطحی که به چشم‌انداز فرآیند کسب و کار مربوط می‌شود، توسعه داده شده است. در واقع چارچوب **MARISMA** به طراحی مدل، پیاده‌سازی فرآیندها و اجرای عملکردهای کسب و کار که از طرح استراتژیک سازمان حمایت می‌کند و توسط سیستم‌های اطلاعاتی در سطح پایین انجام داده است. این پیشنهاد جدید شکاف پیشنهادهایی را که مخاطرات را بدون در نظر گرفتن فرآیندهای مدیریت می‌کنند، یا مخاطرات فرآیندهای کسب و کار را بدون در نظر گرفتن عنصر خارجی طراحی شده در مدل بررسی می‌کنند، پر می‌کند.

در این راستا ما در این تحقیق الگوی **(MARISMA for Business Process)** را ارائه دادیم که یک الگوی خاص به عنوان توسعه **MARISMA** است

تا ارزیابی و مدیریت مخاطرات امنیتی انعطاف پذیر، جامع و قابل اجرا را در چارچوب مدل های فرآیند کسب و کار امکان پذیر کند.

در خصوص تجزیه و تحلیل و ارزیابی مخاطرات امنیت اطلاعات، استانداردها و روش های زیر مورد بررسی قرار گرفت:

(i) روش تجزیه و تحلیل مخاطرات و مدیریت برای سیستم های اطلاعاتی (ماگرید، ۲۰۱۲)، که فرآیند مدیریت مخاطرات را در چارچوب حاکمیتی به منظور کمک به تصمیم گیری، با در نظر گرفتن مخاطرات در زمینه فناوری اطلاعات، پیاده سازی می کند.

(ii) ارزیابی تهدید، دارایی و آسیب پذیری عملیاتی حیاتی <sup>1</sup> (OCTAVE) (کارالی و همکاران، ۲۰۰۷) که یک تکنیک برنامه ریزی استراتژیک و مشاوره مبتنی بر فناوری در امنیت است.

(iii) روش تجزیه و تحلیل مخاطرات و مدیریت آژانس ارتباطات و مخابرات مرکزی (CRAMM) <sup>2</sup>، که یک روش مدیریت مخاطرات است که شامل سه مرحله است: شناسایی، ارزیابی و مدیریت مخاطرات (کلپر از سازمان ایزو، ۲۰۲۲) و (ایزو ۲۱۸۲۷، ۲۰۰۸).

(iv) اهداف کنترلی برای اطلاعات و فناوری های مرتبط <sup>3</sup> (COBIT) (دی هایس و همکاران، ۲۰۲۲)، که روشی برای کنترل کافی پروژه های فناوری، جریان های اطلاعات و مخاطرات ناشی از فقدان کنترل های کافی است. COBIT شامل فرآیند با هدف ارزیابی مخاطرات است، که عمدتاً بر معیارهای محرمانگی، یکپارچگی و دسترس پذیری متمرکز است و در مرحله دوم بر معیارهای اثربخشی، کارایی، انطباق و قابلیت اطمینان، تمرکز دارد.

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

2 Central communication and telecommunication agency Risk Analysis and Management Method (CRAMM)

3 Control Objectives for Information and Related Technologies (COBIT)

(v) چارچوب مدیریت مخاطرات عمومی پیشنهاد شده توسط سازمان ملی استاندارد و فناوری<sup>1</sup> (NIST) (روز و همکاران، ۲۰۱۷)، که برای هر سیستم اطلاعاتی قابل اجرا است (NIST، ۲۰۱۸).

با توجه به استانداردهای اصلی مدیریت امنیت، بسیاری از آنها سعی کرده‌اند ارزیابی و مدیریت مخاطرات را در فرآیندهای خود بگنجانند:

i. گروه استانداردهای ISO/IEC 27000 و به طور خاص استاندارد ISO/IEC 27005 که دستورالعمل‌هایی را برای مدیریت مخاطرات در امنیت اطلاعات ایجاد می‌کند.

ii. استاندارد ISO/IEC 21827/SSE-CMM (System Security Engineering Capability Maturity Model) (ایزو 21827، ۲۰۰۸)، که یک مدل ظرفیت و بلوغ را در مهندسی امنیت سیستم‌ها ایجاد می‌کند که ویژگی‌های اساسی فرآیندهایی را که باید در یک سازمان وجود داشته باشد، توصیف می‌کند. به منظور تضمین امنیت خوب در سیستم‌ها با گنجاندن یک فرآیند مخاطرات محور در مراحل قبلی؛

iii. استاندارد ISO/IEC 15443 (ایزو 15443، ۲۰۱۲) که روش‌های موجود را بسته به سطح امنیت و مرحله اطمینان طبقه‌بندی می‌کند (ارزیابی اطمینان به فرآیند، محصول و محیط تقسیم می‌شود، در حالی که مراحل ارزیابی مخاطرات عبارتند از طراحی/پایه‌سازی، ادغام/تأیید، همانندسازی، انتقال، و عملیات)؛

iv. کتابخانه زیرساخت فناوری اطلاعات (ITIL) (ویلارینیو و همکاران، ۲۰۱۳)، که عنصری را برای مدیریت صحیح مخاطرات فراهم می‌کند.

این استانداردها و چارچوب‌ها، دانش به روز و دقیق از کلیه دارایی‌های سازمان و روابط، وزن‌ها و وابستگی‌های بین آنها را نشان می‌دهد. با این حال، این استانداردها، در عین حال که ادغام شده‌اند، به سمت تجزیه و تحلیل مخاطرات در فرآیندهای کسب‌وکار نمی‌روند. این استانداردها دارای جهت‌گیری مخاطرات عمدتاً به سمت امنیت سایبری و سیستم‌های اطلاعاتی هستند.

1 National Institute of Standards and Technology (NIST)

طراحی فرآیند کسب و کار مبتنی بر مخاطرات یک حوزه تحقیقاتی است که هنوز به کاوش بیشتر نیاز دارد. وجود رهنمودها و/یا اصولی که به فرد اجازه می دهد فرآیند کسب و کار را بر اساس اطلاعات مرتبط با مخاطرات (مانند کشف رویدادهای مخاطرات، احتمال وقوع برخی رویدادهای «بد» و غیره) طراحی کند. از طریق تجزیه و تحلیل مخاطرات زمان طراحی یا تجزیه و تحلیل گزارش پس از اجرا یک ویژگی بسیار مطلوب است زیرا می تواند سطح مخاطرات یک فرآیند را با طراحی کاهش دهد. این به نوبه خود ممکن است هزینه های مرتبط با مدیریت مخاطرات زمان اجرا را به حداقل برساند.

به طور کلی، معمولاً نگرانی ها در خصوص مدیریت فرآیند کسب و کار (BPM)<sup>1</sup> و مدیریت مخاطرات به صورت مجزا در نظر گرفته می شوند (سوریادی و همکاران، ۲۰۱۴). با این وجود، توجه بیشتر و بیشتری به ادغام امنیت و مخاطرات در زمینه BPM معطوف شده است (گوتلمن و همکاران، ۲۰۱۴).

با توجه به اهمیت آن در این زمینه، بررسی روش مند امنیت BPM را می توان در (هاریانتي و همکاران، ۲۰۱۸) یافت، که بر انجام بررسی رویکردهای ارزیابی مخاطرات امنیتی مبتنی بر فرآیند کسب و کار متمرکز است و نویسندگان آن به این نتیجه می رسند که لازم است مدل های جدیدی با این رویکرد ایجاد شود.

این تحقیق در نهایت به سوالات زیر پاسخ خواهد داد:

- چگونه چارچوب MARISMA-BP می تواند مدیریت مخاطرات امنیتی را در فرآیندهای کسب و کار بانکی بهبود بخشد؟
- مؤلفه های کلیدی چارچوب MARISMA-BP برای کاهش مخاطرات در طراحی فرآیندهای بانکی کدامند؟
- چگونه می توان مدیریت مخاطرات را در فرآیندهای کسب و کار بانک ها و مؤسسات مالی با استفاده از چارچوب MARISMA-BP بهبود بخشید؟

## مرور ادبیات

### (أ) استاندارد ISO/IEC 27001

1 Business Process Management (BPM)

**ISO/IEC 27001** یک استاندارد بین‌المللی برای مدیریت امنیت اطلاعات (ISMS)<sup>1</sup> است. این استاندارد توسط سازمان بین‌المللی استانداردسازی (ISO) و کمیسیون الکتروتکنیکی بین‌المللی (IEC) تهیه شده است. هدف اصلی این استاندارد کمک به سازمان‌ها برای محافظت از اطلاعات حساس خود از تهدیدات احتمالی از طریق فرآیندهای مدیریتی و کنترل‌های امنیتی است.

### ب) چارچوب NIST

چارچوب NIST (National Institute of Standards and Technology)، یک موسسه استاندارد‌گذاری و تحقیقات علمی در ایالات متحده است که در حوزه‌های مختلفی از علم و فناوری فعالیت می‌کند. چارچوب امنیت سایبری NIST (CSF) مجموعه‌ای از دستورالعمل‌های داوطلبانه است که توسط موسسه ملی استاندارد و فناوری (NIST) برای کمک به سازمان‌ها در مدیریت و کاهش مخاطرات امنیت سایبری ایجاد شده است.

### ت) استاندارد ISO/IEC 27005

**ISO/IEC 27005** یک استاندارد بین‌المللی است که توسط سازمان بین‌المللی استانداردسازی (ISO) و کمیته بین‌المللی اصول الکتروتکنیکی (IEC) تنظیم شده است. این استاندارد به مدیریت مخاطرات امنیت اطلاعات می‌پردازد و راهنمایی‌هایی برای انجام فعالیت‌های ارزیابی و مدیریت مخاطرات امنیت اطلاعات ارائه می‌دهد.

### ث) محرمانگی (Confidentiality)

محافظت از اطلاعات در برابر دسترسی غیرمجاز و اطمینان از اینکه فقط افراد مجاز می‌توانند به داده‌ها دسترسی داشته باشند. مثال: استفاده از رمزنگاری برای محافظت از داده‌های حساس.

### یکپارچگی (Integrity)

اطمینان از اینکه اطلاعات دقیق و کامل هستند و در طول زمان تغییر نیافته‌اند، مگر با مجوز مناسب. مثال: استفاده از الگوریتم‌های هش برای اطمینان از صحت داده‌ها.

### دسترسی‌پذیری (Availability)

1 Information Security Management System

اطمینان از اینکه اطلاعات و سیستم های مورد نیاز در دسترس کاربران مجاز در مواقع لازم هستند. مثال: استفاده از سیستم های پشتیبان گیری و برنامه های بازیابی در شرایط بحرانی.

### مدیریت مخاطرات امنیت اطلاعات

مدیریت مخاطرات امنیت اطلاعات (ISO/IEC27001:2022) فرآیندی است که به شناسایی، ارزیابی و کنترل مخاطرات مرتبط با امنیت اطلاعات در یک سازمان می پردازد. این فرآیند به سازمان ها کمک می کند تا تهدیدات امنیتی را شناسایی کنند، تأثیرات بالقوه آنها را ارزیابی کنند و اقدامات لازم برای کاهش این مخاطرات را اجرا کنند.

### روش تحقیق

این پژوهش از نوع توصیفی-تحلیلی است که با هدف بررسی و تحلیل مدیریت مخاطرات در فرآیندهای کسب و کار انجام شده است. روش پژوهش به صورت کمی-کیفی طراحی شده است، به طوری که از تحلیل محتوای متون علمی و استانداردهای مرتبط (روش کیفی) و همچنین استفاده از ماتریس ها و چارچوب های تحلیلی مانند MARISMA-BP (روش کمی) بهره گرفته شده است. این پژوهش همچنین از نظر هدف، کاربردی است، زیرا به دنبال ارائه راهکارهای عملی برای بهبود مدیریت مخاطرات در سازمان هاست.

جامعه این پژوهش شامل متون علمی، استانداردهای بین المللی (مانند ISO/IEC 27001، ISO/IEC 27005، NIST 800-53)، و همچنین خبرگان حوزه مدیریت مخاطرات و فرآیندهای کسب و کار است. همچنین نمونه گیری به صورت هدفمند انجام شده و شامل اسناد معتبر، استانداردهای منتخب، و نظرات خبرگان (متخصصان امنیت سایبری، تحلیل گران مخاطرات، و متخصصان فرآیندهای کسب و کار) بوده است.

### ا) روش جمع آوری داده ها

در این روش، داده های مورد تحقیق به صورت کیفی و کمی جمع آوری شده است:

- داده های کیفی: از طریق مرور سیستماتیک متون علمی، استانداردها، و

چارچوب های موجود (مانند MARISMA، BPMN و SecBPMN2)

جمع آوری شده است.

- داده‌های کمی: با استفاده از ماتریس‌های تحلیلی (مانند ماتریس کنترل-تهدید و ماتریس تهدید-دارایی-ابعاد) و نظرسنجی از خبرگان، داده‌ها کمیت‌بخشی شده‌اند.

### ب) ابزارهای پژوهش

ابزارهای مورد استفاده در این تحقیق به سه دسته زیر تقسیم می‌شود:

- مصاحبه نیمه‌ساختاریافته با خبرگان.
- پرسشنامه‌های تخصصی برای ارزیابی روابط بین عناصر مخاطرات.
- نرم‌افزار تحلیل داده Excel برای پردازش ماتریس‌ها.

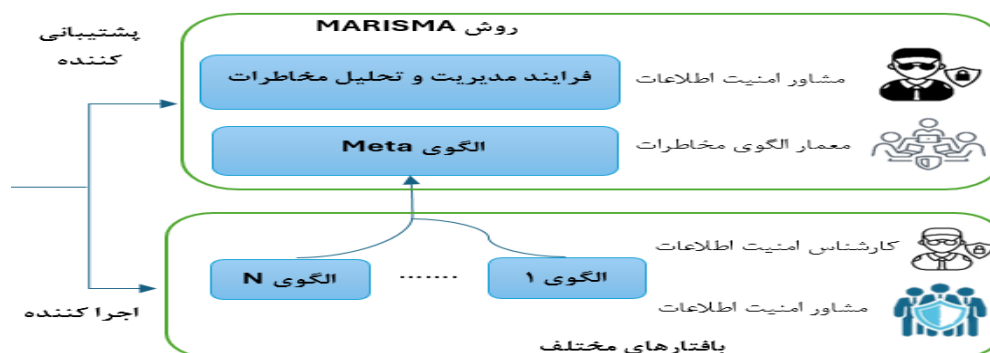
### ت) روش تحلیل داده‌ها

تحلیل داده‌ها در این پژوهش به صورت ترکیبی مورد ارزیابی قرار گرفتند:

- **تحلیل کیفی:** از روش تحلیل محتوا برای استخراج مفاهیم کلیدی از متون و استانداردها استفاده شده است.
- **تحلیل کمی:** با استفاده از ماتریس‌ها و مدل‌سازی روابط بین تهدیدها، دارایی‌ها، و ابعاد امنیتی، داده‌ها تحلیل شده‌اند.
- **روش دلفی:** برای رسیدن به اجماع میان خبرگان در مورد روابط و وزن‌های ماتریس‌ها به کار گرفته شده است.
- **تحلیل SWOT:** برای شناسایی نقاط قوت، ضعف، فرصت‌ها، و تهدیدهای چارچوب پیشنهادی استفاده شده است.

### ث) چارچوب MARISMA

یک محیط فناوری مبتنی بر ابر که به عنوان یک پلتفرم کاربرپسند عمل می‌کند تا پروژه‌های ارزیابی و مدیریت مخاطرات را انجام دهد. MARISMA چارچوبی است که به سمت پیاده‌سازی سیستم‌های ارزیابی و مدیریت مخاطرات، که از جمله ویژگی‌های دیگر، ظرفیت انطباق با محیط‌های مختلف تکنولوژیکی را دارند، جهت‌گیری می‌کند (سانتوس اولمو و همکاران، ۲۰۱۶).



### شکل ۱ معماری چارچوب MARISMA

همانطور که در شکل ۱ نشان داده شده است، چارچوب از سه بخش تشکیل شده است. یک روش پشتیبانی شده توسط یک ساختار ابر داده (متا الگوی مخاطرات ما)، یک سازوکار توسعه پذیری (در قالب الگوهای خاص که نمونه هایی از متا الگوی مخاطرات هستند) است.

عنصر اصلی چارچوب MARISMA روشی است که یک فرآیند جامع و دقیق را تعریف می کند که با آن می توان کل ارزیابی مخاطرات و چرخه عمر مدیریت را برای یک شرکت یا بخشی از آن، از جمله فعالیت های مورد نیاز برای پیکربندی ساختارهای داده قابل استفاده مجدد مناسب انجام داد.

این روش توسط مجموعه ای از شاخص های مخاطرات کلیدی (KRI)<sup>۱</sup> و توسط یک طرح ابر داده پشتیبانی می شود، که عناصر و روابط آنها را مشخص می کند که حداکثر سفارشی سازی و اتوماسیون فرآیند ارزیابی و مدیریت مخاطرات را امکان پذیر می سازد.

الگوی متای مخاطرات ما شامل اجزای کلیدی ارزیابی مخاطرات (تهدیدها، انواع دارایی ها و ابعاد)، سلسله مراتب عناصر و ماتریس های لازم برای محاسبه و استنباط دانش است. با این حال، از آنجایی که ما می دانیم که بخش های خاص یا محیط های فناوری خاص ممکن است به یک استراتژی ارزیابی و مدیریت مخاطرات متفاوت نیاز داشته باشند (به عنوان مثال، آن هایی که تحت تأثیر انواع مختلف تهدیدات قرار دارند یا دارای دارایی هایی با ماهیت متفاوت هستند)، یا حتی اینکه مخاطرات ممکن است در سطوح انتزاعی متفاوتی در نظر گرفته شود (به عنوان مثال،

1 Key Risk Indicators (KRI)

مخاطرات سیستم‌های اطلاعاتی، مخاطرات فرآیندهای کسب‌وکار یا حتی مخاطرات سازمانی)، ما همچنین احتمال پیاده‌سازی طرح متاداده خود را در زمینه‌های خاص نیز مدنظر قرار داده‌ایم (نکته‌گذاری الگوهای خاص در شکل ۱)، مانند **ISO/IEC 27001**، سیستم‌های مبتنی بر داده‌های کلان، **CPS**<sup>۱</sup> و **BP** و غیره.

در واقع این چارچوب از دانش به دست آمده از پیاده‌سازی‌های قبلی و حوادث امنیتی گزارش شده در سیستم استفاده می‌کند تا با استفاده از روش‌های تجزیه و تحلیل داده‌ها، پیشنهاداتی برای بهبود تحلیل مخاطرات و خود الگوها ایجاد کند.

فرآیند ایجاد الگو در بخش زیر توضیح داده شده و در شکل ۴ نشان داده شده است. به عنوان مثال، در سازمانی با سیستم اطلاعات عمومی، **ISO/IEC 27001** چارچوبی فراگیر برای مدیریت امنیت اطلاعات فراهم می‌کند.

استاندارد **ISO/IEC 27005** به طور خاص از فعالیت‌های مدیریت مخاطرات پشتیبانی می‌کند و در نتیجه انطباق با هر دو استاندارد را تضمین می‌کند. از طرف دیگر، باید الزامات و چارچوب‌هایی که از نهادهای بالادستی به بانک‌ها و مؤسسات مالی ابلاغ می‌شود نیز باید مورد توجه قرار گیرد و در فرایندها اعمال گردد.

این استانداردها ممکن است دامنه‌های متفاوتی داشته باشند، اما می‌توانند در دسته دارایی‌های اطلاعاتی مشترک باشند. در این حالت، این دو الگو دارای کنترل‌های متفاوت، طبقه‌بندی تهدیدات مختلف، انواع و ابعاد مختلف دارایی‌ها هستند و همه روابط بین همه این عناصر به هدفی که روی آن متمرکز شده‌اند بستگی دارد. برای اینکه شرکت بتواند دارایی‌های خود را از منظرهای مختلف مخاطرات تجزیه و تحلیل کند، باید بتواند بر استانداردهای خاص، در این مورد **ISO27001** و زیرساخت بحرانی تکیه کند.

این چارچوب به طور گسترده در انواع مختلف شرکت‌ها (برق، هیدروکربن، دولت، بهداشت، کشتی‌سازی، صنایع شیمیایی و غیره) در بیش از هشت کشور اروپایی و آمریکای لاتین اعمال شده و می‌شود که در یک چرخه بهبود جهانی به وضوح مثبت است. هر شرکتی که از یک الگو استفاده می‌کند، دانش را از طریق حوادث خود تولید می‌کند، که برای غنی‌سازی الگو استفاده

1 Cyber-Physical Systems (CPS)

می شود، بنابراین دقت عناصر خود را افزایش می دهد و به سازمان های دیگر اجازه می دهد از این اصلاح جدید بهره مند شوند (روزادو و همکاران، ۲۰۲۱) و (روزادو و همکاران، ۲۰۲۲).

### الگوی MARISMA-BP

یکی از اجزای اصلی چارچوب MARISMA، متا الگوی مخاطرات است که جزء کلیدی برای انجام تجزیه و تحلیل مخاطرات برای هر سیستم یا محیط فناوری اطلاعات می باشد. این ساختار عمومی است و بنابراین قابل استفاده مجدد بوده و هر دو هنجارها یا استانداردهای امنیتی را می توان برای تعریف دامنه ها و کنترل ها، همراه با طبقه بندی تهدیدها و انواع دارایی های امنیتی رایج ترین در هر محیط فناوری اطلاعات در نظر گرفت.

بنابراین، هدف MARISMA-BP ارائه مدل های فرآیند کسب و کار با ارزیابی و مدیریت مخاطرات کامل، انعطاف پذیر، سازگار و قابل اجرا است. مدیریت مخاطرات فرآیندهای کسب و کار شامل عناصری مانند گردش کار، وظایف، داده های خارجی و سازوکارهایی برای رخدادهای و رویدادها است.

فرآیند الگوی MARISMA-BP، عناصر عمومی مشترک برای هر تحلیل و مدیریت مخاطرات، مانند دارایی ها، تهدیدها و ابعاد را تعریف می کند، علاوه بر این شامل کنترل های امنیتی بوده که امکان مدیریت مخاطرات را با توصیه به بهبودها و اقدامات متقابل مناسب فراهم می کند.

الگوی متا مجموعه ای از روابط را بین این عناصر تعریف می کند و مشخص می کند که چه نوع حملاتی می توانند بر سیستم بانک و مؤسسات مالی تأثیر بگذارند. چه تأثیری بر انواع دارایی ها بر اساس ابعاد آن ها دارند و چه مجموعه ای از کنترل ها برای حفاظت از آن دارایی ها در برابر تهدیدها مناسب تر است.

فرآیند الگوی MARISMA از یک سو شامل دارایی ها (خانواده و انواع دارایی ها) به عنوان دسته بندی دارایی های سیستم در نظر گرفته می شود و از سوی دیگر، تهدیدات (خانواده، انواع تهدیدها) که می تواند به عنوان دسته بندی یا گروه بندی تهدیدهایی که به سیستم حمله می کنند، در نظر گرفته شود.

شاخه سوم به کنترل‌های امنیتی (دامنه‌ها، قابلیت‌ها و کنترل‌ها) مربوط می‌شود و شامل کنترل‌ها یا پادمان‌هایی است که با آن سیستم را در برابر حملات احتمالی محافظت می‌کند. در نهایت، روابط بین این عناصر و ابعاد ایجاد می‌شود.

بنابراین، این رابطه سه تایی است (ATD: نوع دارایی - نوع تهدید - ابعاد)<sup>1</sup> بین انواع دارایی‌ها، انواع تهدیدها و ابعادی که با آن تأثیر تهدیدها و آسیبی که ممکن است از طریق آنها به ارزش دارایی وارد شوند را نشان می‌دهد. ابعاد رابطه یکی دیگر از روابط موجود بین انواع تهدیدها و کنترل‌های موجود است که می‌تواند برای کاهش چنین تهدیداتی مورد استفاده قرار گیرد و چارچوب MARISMA برای محافظت از سیستم با ارائه مناسب‌ترین توصیه‌ها در نظر گرفته می‌شود.

این فرآیند به عنوان مبنایی برای تعریف و مشخص کردن عناصر خاصی که در تحلیل مخاطرات سازمان خواهند کرد، بسته به محیط یا سیستم مورد تجزیه و تحلیل، عمل خواهد کرد. در این کار، ما قصد داریم یک تحلیل مخاطرات برای مدل‌های فرآیند کسب‌وکار در زمان طراحی انجام دهیم و در نتیجه، می‌خواهیم محاسبه کنیم که کدام عناصر مدل در معرض تهدیدات هستند، چه نوع تهدیداتی مدل را تهدید می‌کند و کدام کنترل‌ها مناسب‌ترین هستند تا از دارایی‌های مدل محافظت کنیم و یک مدل فرآیند کسب‌وکار بهبود یافته و ایمن‌تر در زمان طراحی به دست آوریم. بنابراین، شکل ۲ عناصر خاص مدل‌های فرآیند کسب‌وکار را نشان می‌دهد که باید با استفاده از عناصر و روابط فرآیند به عنوان پایه تعریف شوند.

1 ATD: Asset type - Threat type- Dimension



## کنترل‌های امنیتی

همانطور که شکل ۳ نشان می‌دهد، کنترل‌های امنیتی انواع تهدید را کاهش می‌دهند (مثال الگوی ماریسما، کادر پایین سمت چپ، خط قرمز)، اما این انواع تهدید، انواع تهدیدهای خاص فرآیندهای کسب‌وکار هستند (کادر بالا سمت چپ). بنابراین، تعیین اینکه کدام کنترل‌های امنیتی برای کاهش انواع تهدیدات موجود در فرآیندهای کسب‌وکار مناسب هستند، ضروری است. همانطور که شکل ۳ نشان می‌دهد، با شروع از فرآیند الگوی ماریسما (به کادر فرآیند، پایین سمت چپ، خط قرمز مراجعه کنید)، اگر بخواهیم الگوی ماریسما ب-پ را تعریف کنیم، باید الگوی متا را با عناصر مرتبط با فرآیندهای کسب‌وکار گسترش دهیم.

این کار با نشان دادن اینکه کدام نوع از دارایی‌ها در فرآیندهای کسب‌وکار وجود دارد انجام می‌شود، چه نوع تهدیدهایی می‌توانند به این نوع زمینه‌ها (به کادر انواع تهدیدها، بالا سمت چپ رجوع کنید) حمله کنند، و کدام ابعاد دارایی تحت تأثیر تهدیدها (به کادر ابعاد امنیتی، بالا سمت راست مراجعه کنید) قرار می‌گیرد.

به عنوان مثال، اگر در یک فرآیند کسب‌وکار وظیفه‌ای داشته باشیم که اطلاعات را به یک دیتا استور ارسال می‌کند، الگو باید وظیفه، پیام ارسال شده و انبار داده‌ای را که اطلاعات در آن به عنوان دارایی ذخیره می‌شود را مشخص کند تا محافظت شود. به عنوان یک تهدید، سرقت داده به عنوان یک حمله عمدی شناسایی می‌شود و ما می‌خواهیم از محرمانگی و یکپارچگی آن اطلاعات (به عنوان ابعاد) اطمینان حاصل کنیم.

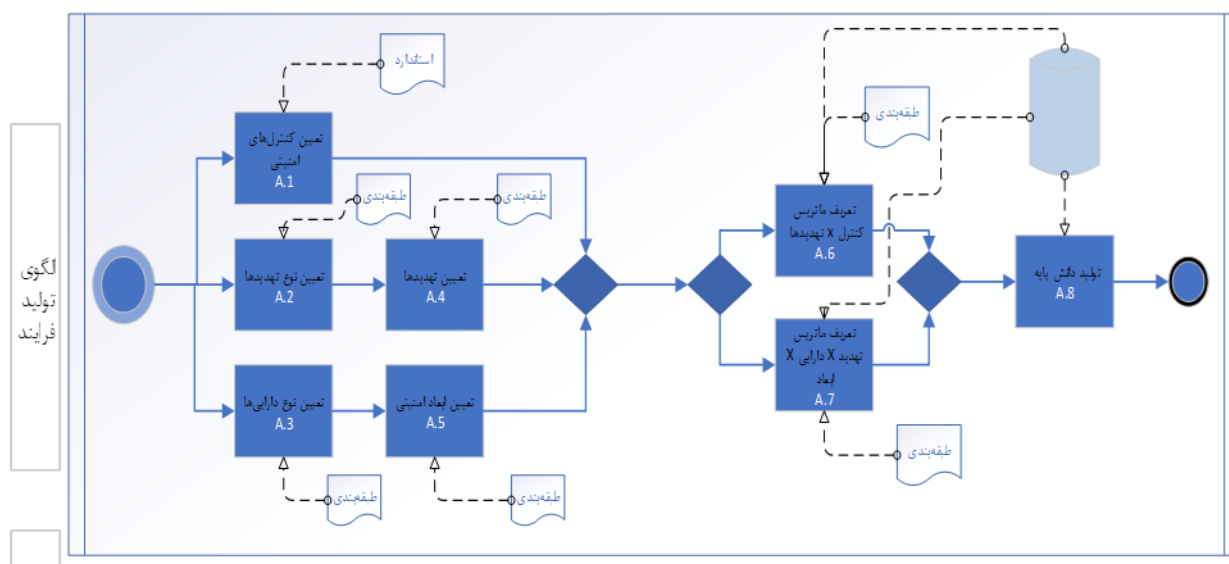
بنابراین ما از این عناصر (دارایی‌ها، حملات و ابعاد) جهت محاسبه مخاطرات موجود با این عناصر، برای اطلاعات ارسال شده، داده‌های ذخیره‌شده و مدیریت داده‌ها قبل از ارسال، استفاده می‌کنیم. هنگامی که یک الگو ایجاد می‌شود، عناصر فرآیند با تطبیق آنها با زمینه خاص (با در نظر گرفتن سیستم بانک) نمونه‌سازی می‌شوند. فرآیند به کار گرفته شده برای تعریف الگو (نشان داده شده در شکل ۴) به شرح زیر است:

۱- ابتدا عناصر اصلی الگو تعریف می‌شوند. همکاری بین کارشناس امنیت سایبری (که از استانداردها و الزامات امنیتی لازم برخوردار است) و کارشناس فرآیند کسب‌وکار برای این منظور مهم است؛ کنترل‌های امنیتی را انتخاب کنید یا تطبیق دهید که برای زمینه، در مورد سیستم بانک و

- مدل های فرآیند کسب و کار مناسب تر هستند. این کنترل ها معمولاً با استفاده از تجزیه و تحلیل استانداردهای اصلی امنیت و فرآیندهای کسب و کار انتخاب می شوند (فعالیت A.1).
- ۲- انواع تهدیدات مربوط به فرآیندهای کسب و کار را با مطالعه و تجزیه و تحلیل طبقه بندی های مختلف تهدیدات مناسب برای این زمینه تعریف و انتخاب کنید (فعالیت A.2).
- ۳- شناسایی و تعریف انواع دارایی های اطلاعاتی که لازم است محافظت شود. این دارایی ها با مطالعه و ۳ تجزیه و تحلیل طبقه بندی های اصلی دارایی برای فرآیندهای کسب و کار موجود انتخاب می شوند (فعالیت A.3).
- ۳- شناسایی تهدیدهای بالقوه ای که ممکن است در حوزه فرآیند کسب و کار مرتبط باشند. این تهدیدها با مطالعه و تجزیه و تحلیل طبقه بندی تهدیدات اصلی برای فرآیندهای کسب و کار موجود (فعالیت A.4) انتخاب می شوند.
- ۴- مجموعه ابعادی را که بخشی از انواع دارایی ها را تشکیل می دهند و به آن مربوط می شوند، تعریف کنید، زیرا آنها عناصری هستند که نشان دهنده آسیب وارد شده به یک دارایی در اثر ظاهر شدن یک تهدید هستند (فعالیت A.5).
- ۵- هنگامی که عناصر اصلی الگو تعریف شدند، لازم است معیارهایی به کار گرفته شود که با آن روابط موجود بین این عناصر مشخص شود. بنابراین، گام بعدی، پیکربندی و پارامترسازی ماتریس های رابطه است، بنابراین اجازه می دهد ماتریسی تولید شود که تهدیدات را به کنترل ها مرتبط می کند، و یک مقدار اولیه برای درصد وقوع یک تهدید برای یک کنترل خاص تعریف می کند (فعالیت A. 6).
- ۶- ماتریسی که با آن تهدیدها را به انواع دارایی مرتبط می کند نیز ایجاد می شود که ابعاد امنیتی را نشان می دهد که توسط عمل تهدید برای هر نوع دارایی به خطر می افتد (فعالیت A.7).
- این ماتریس ها از اهمیت عمده ای برخوردارند، زیرا به عنوان مخزن دانشی که الگو را ارائه می کند، این امکان را می دهند که ویژگی های پویایی خود را در انطباق با تغییرات و سرعت در تولید تحلیل مخاطرات داشته باشیم. دانش ترکیبی متخصص امنیت سایبری و کارشناس فرآیند کسب و کار نیز یک جنبه کلیدی در این مرحله خواهد بود، زیرا بازخورد به وظایف A.1-A.5 با پیکربندی ماتریس ها مکرر است.

بنابراین، هنگام ایجاد روابط، می‌توان عناصری را یافت که در ابتدا در نظر گرفته نشده بودند و باید اضافه شوند. به طور مشابه، ممکن است عناصر جدا شده ای نیز وجود داشته باشد (مثلا تهدیداتی که بر هیچ یک از انواع دارایی‌های تعریف شده تأثیر نمی گذارد) که باید از الگو حذف شوند. هنگامی که تمام عناصر الگو و روابط آنها برقرار شد، وظیفه A.8 به طور خودکار پایگاه دانش حاصل را تولید می‌کند، تمام اطلاعات جمع آوری شده در کارهای قبلی را ذخیره و نمایه می‌کند.

شکل ۴- فرآیند ایجاد یک الگوی جدید در چارچوب ماریسما



جدول ۱ خلاصه‌ای از مراجع استفاده شده در هر یک از منابع را نشان می‌دهد:

جدول ۱: چارچوب‌ها، طبقه‌بندی‌ها و استانداردهای مرجع استفاده شده در الگو

| خلاصه منابع مورد استفاده برای الگوی MARISMA-BP |                                                                                         |
|------------------------------------------------|-----------------------------------------------------------------------------------------|
| عناصر الگو                                     | مراجع استفاده شده                                                                       |
| کنترل‌های امنیت                                | ISO27002:2022 (2022), NIST 800-53 (2020)                                                |
| انواع دارایی‌ها                                | Business Process Model and Notation (BPMN) (2021)                                       |
| ابعاد امنیتی                                   | IAS-Octave of RMIAS (2013) , SecBPMN2 (2017)                                            |
| انواع تهدیدها                                  | Taxonomy of operational security risks (SEI) (2014)<br>ENISA taxonomy of threats (2016) |

موسسه مهندسی نرم افزار (SEI)<sup>۱</sup> طبقه‌بندی مخاطرات امنیت اطلاعات را توسعه داد (سبولا و همکاران، ۲۰۱۴). این طبقه‌بندی به چهار کلاس تقسیم شده و با طبقه‌بندی مخاطرات ریسک قانون مدیریت امنیت اطلاعات فدرال (FISMA)، انتشارات ویژه NIST، و روش OCTAVE® همسو شده است.

ENISA طبقه‌بندی تهدیدات خود را بر اساس استانداردهای اصلی مخاطرات موجود توسعه داد (مارینوس و همکاران، ۲۰۱۶) و (مارینوس و همکاران، ۲۰۱۹). در نهایت، CAPEC<sup>۲</sup> طبقه‌بندی خود را براساس فهرست‌بندی الگوهای حمله مورد استفاده برای بهره‌برداری از آسیب‌پذیری‌های سیستم، توسعه داد (بارنوم، ۲۰۰۸).

علاوه بر این، BPMN<sup>۳</sup> استاندارد است که برای نمایش گرافیکی فرآیندهایی که تقریباً در هر نوع سازمانی رخ می‌دهد، استفاده می‌شود (چینوسی و همکاران، ۲۰۱۲). BPMN یک زبان عمومی است که محققان اغلب آن را گسترش می‌دهند با فرآیندهایی در حوزه‌های خاص یا بهبود خود زبان (زارور و همکاران، ۲۰۱۹).

امنیت در فرآیندهای کسب‌وکار یک ویژگی مهم است، همانطور که اجازه می‌دهد مفاهیم امنیتی برای افزودن به مدل‌های فرآیند کسب‌وکار با ارائه زبان و درک مشترک، بنابراین هماهنگی بین فعالیت‌ها و همکاری بین کارشناسان موضوع را ممکن می‌سازد (لایتنر و همکاران، ۲۰۱۳) و (آرژیروپولوس و همکاران، ۲۰۲۰).

بنابراین، بسیار مهم است که الزامات امنیتی در سطح مفهومی به منظور شناسایی نیازهای امنیتی را درک کنید. وجود یک ابزار و روش یکپارچه که اجازه دهد مشخصات و اجرای الزامات انطباق و امنیتی برای سیستم‌های سازمانی که توسط فرآیندهای کسب‌وکار هدایت شوند، لازم است (چرگی و همکاران، ۲۰۱۸).

با توجه به بخش کنترل، استاندارد ISO27002:2022 راهنمای خوبی در جهت اقدامات است و این استاندارد شامل لیستی از کنترل‌های امنیتی می‌باشد که بانک‌ها و مؤسسات اعتباری باید به منظور مدیریت صحیح امنیت اطلاعات سیستم‌های خود انجام دهد.

1 The Software Engineering Institute (SEI)

2 Common attack pattern enumeration and classification (CAPEC)

3 Business Process Model and Notation (BPMN)

## عناصر الگوی MARISMA-BP

همانطور که قبلاً ذکر شد، فرآیند الگوی چارچوب MARISMA (کادر متاالگوی MARISMA در شکل ۳) شامل تمام موجودیت‌ها است. برای انجام تجزیه و تحلیل مخاطرات، مانند کنترل‌های امنیتی، تهدیدات، دارایی‌ها و ابعاد امنیتی، همراه با روابط بین این عناصر انواع دارایی‌ها برای فرآیندهای کسب و کار (جدول ۲) از استاندارد BPMN انتخاب شده است و دارایی‌هایی هستند که ممکن است در برابر حملات امنیتی آسیب پذیرتر باشند این سطح از فرآیندهای کسب و کار ابعاد امنیتی که تحت تأثیر قرار خواهند گرفت توسط دارایی‌ها در صورت وقوع تهدید، در نتیجه باعث می‌شود ارزش آن دارایی در یک یا برخی از ابعاد مربوط به آن کاهش یابد، تعریف شده اند (به کادر ابعاد امنیتی در جدول ۳ مراجعه کنید). در نهایت انواع تهدیدهایی که ممکن است بر فرآیندهای کسب و کار در سطح سازمانی تأثیر بگذارد تعریف شده اند (به انواع تهدید در شکل ۵ (شرح تفصیلی انواع تهدیدات الگوی MARISMA-BP)). این MARISMA-BP عناصر به طور مفصل در زیر بخش‌های زیر ارائه شده است.

این مجموعه از کنترل‌ها باید به الگو اضافه شود تا پاسخ امنیتی به تهدیدات احتمالی ارائه شود. با تجزیه و تحلیل استاندارد جدید ISO/IEC 27002:2022 که در آن جنبه‌های زیادی نسبت به نسخه قبلی آن اصلاح شده است، متذکر می‌شویم که مجموعه‌ای از کنترل‌ها (۳۸ کنترل) که در سطح سازمانی وجود دارد، ابزار مناسبی برای محافظت از مدل‌های فرآیند کسب و کار در یک سازمان است.

علاوه بر این، از آنجایی که افراد در این فرآیندهای کسب و کار درگیر هستند، کنترل‌های فردی (۸ کنترل) تعریف شده در استاندارد نیز در نظر گرفته شده است، و دسته‌بندی‌های دیگر مانند فیزیکی و فنی را کنار می‌گذاریم، زیرا در این تکرار اول در نظر گرفته نشده‌اند. لیست کنترل‌های امنیتی در نظر گرفته شده در ستون‌های اول جدول ۷ نشان داده شده است.

## انواع دارایی‌ها

انواع گروه‌های دارایی‌های اطلاعاتی تعریف شده برای مدل‌های فرآیند کسب و کار در جدول زیر، بیان شده است:

جدول ۲: تعریف نوع و گروه دارایی‌ها

| نوع                   | گروه                            | توضیحات                                                                                                                                 |
|-----------------------|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| اسناد و سوابق سازمانی | سند کاغذی                       | مستندات سیستمی، نامه‌ها، دستورالعمل‌ها، فرم‌های خالی و تکمیل شده، آیین‌نامه‌ها، خط‌مشی‌ها، قوانین و مقررات ایمنی، روش‌های اجرایی و غیره |
|                       | سند الکترونیکی                  | انواع فایل‌های ذخیره شده بر روی رایانه‌ها با فرمت‌های مختلف که حاوی اطلاعات هستند.                                                      |
| شبکه و تجهیزات مرتبط  | سرویس‌های پایه شبکه             | DNS, DHCP, NTP, LDAP, File Sharing, WEB Service, WSUS, Domain Controller, WEB Server, VoIP                                              |
|                       | تجهیزات اکتیو شبکه              | Switch, Router, Firewall, ADSL Modem                                                                                                    |
| سخت‌افزارها           | میزبان‌ها و سرورها              | سرورهای فیزیکی، ایستگاه‌های کاری کاربران و تین‌کلاینت‌ها                                                                                |
|                       | تجهیزات دسترسی به اطلاعات       | کارت هوشمند و توکن                                                                                                                      |
| ذخیره‌سازها           | تجهیزات اداری (بدون مراقبت)     | پرینتر، فکس، دیش ماهواره و تجهیزات ارتباط رادیویی                                                                                       |
|                       | ذخیره‌سازها                     | SAN Storage<br>انواع HDD, External, UFD, لپ‌تاپ، تبلت، Tape, ODD <sup>۱</sup>                                                           |
| منابع انسانی          | کارکنان سازمان                  | کارکنان بخش‌های مختلف سازمان                                                                                                            |
|                       | پیمانکاران                      | نیروهای شرکت‌های طرف قرارداد، شرکای کسب و کار و مشاوران                                                                                 |
| دارایی‌های زیرساختی   | تجهیزات تأمین برق               | ، برق شهری، UPS ژنراتور و تابلو برق،                                                                                                    |
|                       | لینک‌های سرویس دیتا و ارتباطی   | MPLS, Leased Line(E1), xDSL, PSTN, WiMax, WiFi خطوط مخابرات                                                                             |
| فرایند                | تجهیزات تهویه مطبوع             | تجهیزات خنک‌کننده سایت‌ها و رک‌ها                                                                                                       |
|                       | تجهیزات اعلان و اطفای حریق      | حسگرهای دود، سامانه‌های اعلان و اطفای حریق                                                                                              |
| سامانه/نرم‌افزار      | تجهیزات کنترل دسترسی            | دزدگیر، دوربین‌ها و دستگاه‌های کنترل تردد                                                                                               |
|                       | فرایند مدیریت پروژه             | پروژه‌های اجرایی مرتبط با امنیت اطلاعات                                                                                                 |
| فرایند                | فرایند توسعه سیستم‌های اطلاعاتی | کلیه فرایندهای توسعه سیستم‌های اطلاعاتی برون‌سپاری شده و داخلی                                                                          |
|                       | سرورهای مجازی                   | VMware                                                                                                                                  |
| فرایند                | برنامه‌های کاربردی و            | برنامه‌های اتوماسیون اداری، مالی، اداری، پورتال داخلی،                                                                                  |

1 USB Flash Drive  
2 Optical Disk Drive

| نوع | گروه                          | توضیحات                                         |
|-----|-------------------------------|-------------------------------------------------|
|     | سرویس‌های کسب‌وکار            | کارتابل الکترونیکی، آرشیو مرکزی، ضدویروس، انواع |
|     | پایگاه‌های داده               | برنامه‌های خاص منظوره کسب‌وکار شرکت             |
|     | سیستم‌های عامل و میان‌افزارها | Oracle, MS SQL, MySQL                           |
|     |                               | لینوکس و ویندوز                                 |

لازم به ذکر است، دسته‌های دارایی اطلاعاتی در جدول بالا با توجه به نوع و ماهیت کسب‌وکار می‌تواند متغیر باشد.

### ابعاد امنیتی

ابعاد انتخاب شده به عنوان مبنای الگوی MARISMA-BP بر اساس نتایج تجزیه و تحلیل برخی از آثار در رابطه با اهداف امنیتی تعریف شده در [82] IAS-Octave RMIAS (هاکس و همکاران، ۲۰۲۱) و همچنین حاشیه‌نویسی‌های مربوط به جنبه‌های امنیتی استفاده‌شده در SecBPMN2 (سالنتری و همکاران، ۲۰۱۷) بوده است. شرح ابعاد در جدول ۳ نشان داده شده است:

جدول ۳: شرح تفصیلی ابعاد امنیتی الگوی MARISMA-BP

| ابعاد امنیتی                    | توضیح                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------|
| مسئولیت پذیری (AC) <sup>۱</sup> | توانایی یک سیستم برای مسئول دانستن کاربران برای اعمالشان (مانند سوء استفاده از اطلاعات).                               |
| قابلیت ممیزی (AD) <sup>۲</sup>  | توانایی یک سیستم برای نظارت دائمی و غیرقابل عبور از تمام اقدامات انجام شده توسط انسان یا ماشین در مدل فرآیند کسب‌وکار. |
| اصالت (AT) <sup>۳</sup>         | توانایی یک سیستم برای تأیید هویت در اطلاعاتی که ارائه می‌دهد.                                                          |
| دسترس پذیری (AV) <sup>۴</sup>   | یک سیستم باید اطمینان حاصل کند که تمام اجزای مدل زمانی که توسط کاربران مجاز مورد نیاز است در دسترس و عملیاتی هستند.    |
| محرمانگی (CO) <sup>۵</sup>      | یک سیستم باید اطمینان حاصل کند که فقط کاربران مجاز به اطلاعات و فرآیندها دسترسی دارند.                                 |
| یکپارچگی (IN) <sup>۶</sup>      | یک سیستم باید از کامل بودن، دقت و عدم وجود تغییرات غیرمجاز در تمام اجزای آن اطمینان حاصل کند.                          |

1 AC: Accountability

2 AD: Auditability

3 AT: Authenticity

4 AV: Availability

5 CO: Confidentiality

6 IN: Integrity

|                                    |                                                                                                                                                               |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| عدم انکار <sup>۱</sup> (NR)        | توانایی یک سیستم برای اثبات (با اعتبار قانونی) وقوع/عدم وقوع یک رویداد یا شرکت/عدم مشارکت یک طرف در یک رویداد.                                                |
| عدم تفویض اختیار <sup>۲</sup> (ND) | توانایی سیستم برای نیاز به این که مجموعه ای از اقدامات فقط توسط کاربران اختصاص داده شده اجرا شود.                                                             |
| تفکیک وظایف <sup>۳</sup> (SD)      | توانایی سیستم برای وادار کردن دو یا چند فرد مختلف برای انجام یک کار یا مجموعه ای از وظایف مرتبط.                                                              |
| تعهد به فرایند <sup>۴</sup> (BD)   | توانایی فرآیند کسب و کار برای الزام همان فرد به مسئولیت تکمیل مجموعه ای از وظایف مرتبط.                                                                       |
| تاب آوری <sup>۵</sup> (RE)         | توانایی پیش بینی، مقاومت، بازیابی و انطباق با شرایط نامطلوب، استرس ها، حملات یا سازش های سیستمی که از منابع سایبری استفاده می کنند یا توسط آنها فعال می شوند. |

در این مدل ما مبحث «تاب آوری» را نیز به الگوی خود اضافه کردیم، زیرا جهت تداوم فرآیندهای کسب و کار باید سازمان توانایی مدیریت رخدادهای امنیت اطلاعات را داشته باشد و جهت کاهش این رخدادهایی که ممکن است مستقیم کسب و کار بانک را تحت تأثیر قرار دهد نیز در گرفت (آنتونس و همکاران، ۲۰۱۰)، (چردانتسوا و همکاران، ۲۰۱۳).

### خانواده تهدیدها و انواع تهدیدها

مجموعه انواع تهدیدات برای الگوی MARISMA-BP بوده است با تجزیه و تحلیل و مطالعه طبقه بندی امنیت عملیاتی تعریف شده است مخاطرات (سبولا و همکاران، ۲۰۱۴) که سعی در شناسایی و سازماندهی منابع عملیاتی دارد مخاطرات امنیتی، همانطور که در طبقه بندی تهدیدات ENISA<sup>۱</sup> می دهد (مارینوس و همکاران، ۲۰۱۶). درواقع مجموعه ای از انواع تهدیدها در نظر گرفته شده که سعی شده است تهدیدهایی که مرتبط با مدل های فرایند کسب و کار است استفاده شود. نزدیک ترین آنها هستند مربوط به مدل های فرآیند کسب و کار شرح انواع تهدید در جدول ۴ نشان داده شده است.

جدول ۴: شرح تفصیلی انواع تهدیدات الگوی MARISMA-BP

| انواع تهدید | تشریح                                                                                                                                                                                                                        |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| افراد       | اقدام یا عدم اقدامی که توسط افراد به طور عمدی یا غیرعمدی انجام می شود و بر مخاطرات امنیتی تأثیر می گذارد. این کلاس اقدامات خودی و غیرخودی را پوشش می دهد. زیرگروه های پشتیبانی کننده آن عبارتند از اقدامات غیر عمدی، اقدامات |

- 1 NR: Non-repudiation  
2 ND: Non-Delegation  
3 SD: Separation of Duty  
4 BD: Bind of Duty  
5 RE: Resilience

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| عمدی و عدم فعالیت.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |        |
| انواع تهدیدات مرتبط با شکست های مشکل ساز فرآیندهای داخلی برای انجام آن گونه که مورد نیاز یا مورد انتظار است. زیرگروه های پشتیبانی کننده آن شامل طراحی یا اجرای فرآیند، کنترل‌های فرآیند و فرآیندهای پشتیبانی می‌شود.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | فرایند |
| حقوقی: انواع تهدیدها با مخاطراتی سروکار دارند که به دلیل رعایت مقررات، قوانین و دعوی حقوقی عناصر، ممکن است بر سازمان تأثیر بگذارند.<br>مخاطرات: انواع تهدیدات مربوط به مخاطرات ناشی از رویدادها، اعم از طبیعی و انسانی، که سازمان هیچ کنترلی بر آنها ندارد و می‌تواند بدون اطلاع قبلی رخ دهد (رویداد آب و هوا، آتش سوزی، سیل، زلزله، ناآرامی و بیماری همه گیر).<br>کسب‌وکار: انواع تهدیدات مربوط به عوامل شکست تامین کننده، شرایط بازار و شرایط اقتصادی. با مخاطرات های عملیاتی ناشی از تغییرات در محیط کسب‌وکار سازمان سر و کار دارد.<br>خدمات: با مخاطرات ناشی از وابستگی سازمان با طرف‌های خارجی برای ادامه عملیات (ثبات احوال، خدمات اضطراری، شاپرک، اداره برق و غیره) سروکار دارد. | بیرونی |

### ماتریس کنترل-تهدید

برای کشف تأثیری که یک تهدید بر نوع دارایی دارد، لازم است آسیب‌هایی که این نوع تهدید به برخی از ابعاد آن وارد می‌کند، مورد بررسی قرار گیرد. این بدان معنی است که ابعاد باید به نوع دارایی‌ها مرتبط باشند تا بدانیم کدام ابعاد می‌توانند تحت تأثیر تهدیدات قرار بگیرند. این رابطه در جدول ۵ نشان داده شده است. این جدول روابط تعریف شده بین انواع دارایی‌ها و ابعاد آن‌ها را نشان می‌دهد.

با استفاده از BPMN روابط بین ابعاد و انواع دارایی‌ها و معیارهای ارائه شده توسط تیم کارشناسان درگیر در ایجاد الگو (یک کارشناس امنیت سایبری، یک متخصص تجزیه و تحلیل مخاطرات و یک متخصص فرآیند کسب‌وکار) به طور رضایت بخشی تکمیل شده است.

جدول ۵: ابعاد و انواع دارایی‌های BPMN

ابعاد

| انواع دارایی ها       | مسئولیت پذیری | قابلیت ممیزی | صالت | دسترسی پذیری | مهر مانگی | پیکار چگی | عدم انکار | عدم تفویض اختیار | تفکیک وظایف | تعهد به فرایند | تاب آوری |
|-----------------------|---------------|--------------|------|--------------|-----------|-----------|-----------|------------------|-------------|----------------|----------|
| اسناد و سوابق سازمانی | X             | X            |      | X            | X         | X         | X         | X                | X           | X              |          |
| شبکه و تجهیزات مرتبط  |               |              |      | X            |           |           |           |                  |             |                | X        |
| سخت افزارها           |               |              |      |              |           |           |           |                  |             |                | X        |
| منابع انسانی          | X             |              |      |              |           |           | X         | X                | X           | X              |          |
| دارایی های زیر ساختی  |               |              |      |              |           |           |           |                  |             |                |          |
| فرایند                | X             | X            | X    | X            | X         | X         | X         | X                | X           | X              | X        |
| سامانه/نرم افزار      |               |              |      |              |           |           |           |                  |             |                | X        |

به عنوان مثال، نگاشت ابعاد با اسناد و سوابق سازمانی به دلایل زیر است:

۱. مسئولیت پذیری یکی از اصول مهم در مدیریت اسناد و سوابق سازمانی است که اطمینان می دهد هر فعالیت، تصمیم و اقدام در سازمان به درستی ثبت شده و افرادی که مسئول آن ها هستند به درستی شناسایی شده اند. این اصل کمک می کند تا شفافیت و اعتماد در سازمان حفظ شود و اقدامات انجام شده به راحتی قابل پیگیری باشد. با پیاده سازی این راهکارها، سازمان ها می توانند اطمینان حاصل کنند که مسئولیت پذیری به درستی در تمامی فعالیت ها و فرآیندها به اجرا درآمده و سوابق سازمانی به طور کامل و دقیق ثبت شده است. جنبه های مسئولیت پذیری شامل و موارد زیر است:

- تعیین وظایف و واگذاری مسئولیت ها
- ثبت و مستندسازی
- پایش و ارزیابی
- پیشگیری از تخلفات
- بهبود فرآیندها

۲. قابلیت ممیزی یکی از ویژگی‌های اساسی در مدیریت اسناد و سوابق سازمانی است که به سازمان‌ها امکان می‌دهد تا به طور مستقل و مؤثر اقدامات، فرآیندها و عملکرد خود را ارزیابی کنند. این قابلیت به شفافیت و اعتماد در سازمان کمک می‌کند و از نظر قانونی و مالی اهمیت بالایی دارد: قابلیت ممیزی شامل و نه محدود به موارد زیر است:

- ثبت دقیق و کامل اطلاعات
- دسترسی کنترل شده به اسناد

۳. عدم انکار یکی از اصول اساسی امنیت اطلاعات است که اطمینان می‌دهد یک فرستنده یا گیرنده نمی‌تواند انکار کند که عملی خاص مانند ارسال یا دریافت یک پیام یا انجام یک تراکنش صورت گرفته است. این اصل در اسناد و سوابق سازمانی نقش مهمی ایفا می‌کند و از جنبه‌های مختلفی حائز اهمیت است. با پیاده‌سازی عدم انکار در بانک‌ها و مؤسسات اعتباری، می‌توان اطمینان حاصل کرد که تمامی عملیات و تراکنش‌ها به درستی ثبت شده و نمی‌توانند انکار شوند. جنبه‌های عدم انکار شامل و نه محدود به شرایط زیر است:

- احراز هویت فرستنده و گیرنده
- حفاظت از اطلاعات و سلامت داده‌ها
- اعتبار قانونی
- ثبت و نگهداری سوابق
- پیشگیری از تخلفات

۴. عدم تفویض اختیار به معنای عدم واگذاری مسئولیت‌ها و اختیارات به دیگران است. با پیاده‌سازی این راهکارها، بانک‌ها و مؤسسات اعتباری می‌توانند فرهنگ تفویض اختیار را تقویت کرده و از مزایای آن بهره‌مند شوند. نمونه‌هایی از عدم تفویض اختیار در اسناد و سوابق می‌تواند شامل موارد زیر باشد:

- تمرکز بیش از حد وظایف در دست مدیران ارشد
- نبود اسناد رسمی واگذاری مسئولیت‌ها
- دستورالعمل‌های محدود کننده

- کاهش انگیزه کارکنان
  - کندی در فرآیند تصمیم گیری
  - بار کاری افزایش یافته
۵. محرمانگی در اسناد و سوابق سازمانی به معنای حفظ و حفاظت از اطلاعات حساس و مهم سازمانی از دسترسی غیرمجاز و افشای اطلاعات به افراد غیرمجاز است. این امر به ویژه در سازمان هایی که با داده ها و اطلاعات حساس کار می کنند، اهمیت بسیاری دارد. حفظ محرمانگی در اسناد و سوابق سازمانی نیازمند توجه مستمر و پیاده سازی سیاست ها و روش های امنیتی مناسب است.
۶. یکپارچگی در اسناد و سوابق سازمانی به معنای اطمینان از صحت، دقت و کامل بودن اطلاعات در طول چرخه عمر آنها است. حفظ یکپارچگی اطلاعات از تغییرات غیرمجاز، تحریف یا نابودی محافظت می کند. این امر در سازمان ها از اهمیت بالایی برخوردار است، زیرا اطلاعات نادرست یا ناقص می تواند منجر به تصمیمات نادرست و مشکلات جدی شود. یکپارچگی اسناد و سوابق به سازمان ها کمک می کند تا اطلاعات دقیق و قابل اعتمادی داشته باشند که می توانند بر اساس آن تصمیمات استراتژیک و عملیاتی خود را اتخاذ کنند.
۷. دسترسی پذیری در اسناد و مدارک سازمانی به معنای اطمینان از این است که اطلاعات و داده ها برای کاربران مجاز به موقع و به صورت مطمئن در دسترس باشند. این امر در مدیریت اطلاعات سازمانی بسیار حیاتی است زیرا دسترسی پذیری ناکافی می تواند منجر به اختلال در عملیات، کاهش بهره وری و حتی از دست رفتن فرصت های کسب و کار شود. اطمینان از دسترسی پذیری اطلاعات می تواند بهره وری سازمان را افزایش داده و از تلفات داده ها جلوگیری کند.
۸. تعهد به فرآیند در اسناد و مدارک سازمانی به معنای پایبندی به رویه ها و استانداردهای تعیین شده برای مدیریت، نگهداری و به روزرسانی این اسناد و مدارک است. این تعهد به اطمینان از اجرای صحیح و بهینه فرآیندهای مرتبط با اسناد و مدارک، و همچنین

بهبود مداوم آنها کمک می‌کند. تعهد به فرآیند در مدیریت اسناد و مدارک سازمانی نقش بسیار مهمی در حفظ نظم، دقت و کارایی اطلاعات دارد.

به منظور ایجاد رابطه بین انواع تهدیدها و کنترل‌های امنیتی نشان داده شده در جدول ۶، ما یک سری نگاشت بین عناصر بر اساس طبقه بندی‌های مختلف انجام داده ایم. اول، ما تهدیدات (تعریف شده در طبقه بندی SEI و ENISA) را با کنترل‌های تعریف شده توسط NIST 80053 ترسیم کرده ایم، که نشان می‌دهد کدام کنترل‌ها می‌توانند تهدیدات را کاهش دهند (براساس یادداشت فنی CMU/SEI-2014-TN006)، و دوم، ما کنترل‌های ISO27002:2022 را با کنترل‌های NIST برای مدل خود نگاشت کرده ایم.

مجموعه‌ای از کنترل‌های امنیتی که امکان تهدیدات احتمالی را فراهم می‌کند و حمله به سیستمی که باید با آن مواجه شود از استاندارد نسخه جدید ISO/IEC گرفته شده است. استاندارد ۲۷۰۰۲:۲۰۲۲ که ۴ گروه از کنترل‌ها را تعریف می‌کند تنها گروه «کنترل سازمانی» و «کنترل فردی» در سطح فرآیندهای کسب‌وکار حفظ و نگهداری می‌شود. رابطه بین کنترل‌ها و انواع تهدیداتی که می‌توان با این کنترل‌ها کاهش داد را می‌توان در جدول ۶ مشاهده کرد که لیستی از کنترل‌های انتخاب شده، الگو و اینکه چگونه هر یک از این کنترل‌ها می‌توانند یک یا بسیاری از آنها را کاهش دهند و انواع تهدیدهایی که می‌تواند در سطح فرآیند کسب‌وکار رخ دهد را نشان می‌دهد.

به عنوان مثال، برای کنترل ۵,۲۸ «مجموعه شواهد»، ما انواع تهدیدات مرتبط با «طراحی فرآیند» و «کنترل‌های فرآیند» به دلیل حملاتی که ممکن است ایجاد شکست در مسئولیت‌ها، اعلان‌ها، نظارت یا ممیزی فرآیندها و رابطه دیگری با «مسائل حقوقی» به دلیل حملات مربوط به قوانین و انطباق را ارتباط دادیم. کنترل‌ها برای محافظت از دارایی‌هایی که احتمالاً توسط تهدیدها، مورد حمله قرار می‌گیرند، می‌باشد.

جدول ۶- ماتریس کنترل‌ها در مقابل نوع تهدیدات برای الگوی MARISMA-BP

| کنترل‌ها | انواع تهدیدها    |                        |
|----------|------------------|------------------------|
|          | اقدام‌های انسانی | فرآیندهای داخلی ناموفق |
|          | رویدادهای بیرونی |                        |

مدیریت بحران های اجتماعی

| مقیاس ارزیابی آمادگی سازمان برای پاسخگویی به حوادث امنیتی |       |           |             |         |          |                  |              |          |      |          |      |      |                                                      |
|-----------------------------------------------------------|-------|-----------|-------------|---------|----------|------------------|--------------|----------|------|----------|------|------|------------------------------------------------------|
| خدمات                                                     | مسئله | کسب و کار | مسائل حقوقی | مخاطرات | پشتیبانی | کنترل‌های فرآیند | طراحی فرآیند | بدون عمل | عملی | غیر عملی | ردیف | نمره | توضیحات                                              |
|                                                           | X     | X         | X           | X       | X        | X                | X            | X        |      | X        | X    | 1.5  | سیاست‌های امنیت اطلاعات                              |
|                                                           | X     |           |             |         | X        | X                | X            |          |      | X        | X    | 2.5  | نقش‌ها و مسئولیت‌های امنیت اطلاعات                   |
|                                                           |       |           |             |         |          | X                | X            |          |      | X        | X    | 3.5  | مکانیک وظایف                                         |
|                                                           |       |           |             |         |          | X                | X            | X        |      | X        | X    | 4.5  | مسئولیت‌های مدیریت                                   |
|                                                           |       |           | X           |         |          |                  | X            | X        |      | X        | X    | 5.5  | ماس با نهادهای بالادستی                              |
|                                                           |       |           | X           |         |          |                  | X            |          |      | X        | X    | 6.5  | ماس با گروه‌های ذینفع خاص                            |
|                                                           |       |           |             |         |          |                  |              | X        |      | X        | X    | 7.5  | روش تهدید                                            |
|                                                           | X     | X         | X           |         | X        |                  | X            |          |      |          |      | 8.5  | نیت اطلاعات در مدیریت پروژه                          |
|                                                           |       |           | X           |         |          |                  |              | X        |      |          |      | 9.5  | وجودی اطلاعات و سایر دارایی‌های مرتبط                |
|                                                           |       |           | X           |         |          |                  |              |          |      |          |      | 10.5 | استفاده قابل قبول از اطلاعات و سایر دارایی‌های مرتبط |
|                                                           |       |           | X           |         |          |                  |              | X        |      |          |      | 11.5 | زگشت دارایی‌ها                                       |
|                                                           |       | X         | X           |         | X        |                  | X            |          |      |          |      | 12.5 | بهبودبندی اطلاعات                                    |
|                                                           |       |           | X           |         |          |                  |              | X        |      | X        | X    | 13.5 | چسب گذاری اطلاعات                                    |
|                                                           | X     | X         | X           | X       | X        | X                |              | X        |      | X        | X    | 14.5 | انتقال اطلاعات                                       |
|                                                           |       |           |             |         |          |                  |              |          |      |          |      | 15.5 | کنترل دسترسی                                         |
|                                                           |       | X         | X           |         |          |                  |              |          |      | X        | X    | 16.5 | مدیریت هویت                                          |
|                                                           |       |           |             |         |          |                  |              |          |      | X        | X    | 17.5 | اطلاعات احراز هویت                                   |
|                                                           |       |           |             |         |          |                  |              |          |      | X        | X    | 18.5 | حقوق دسترسی                                          |
|                                                           | X     | X         |             |         |          | X                |              |          |      |          |      | 19.5 | نیت اطلاعات در روابط                                 |

| انواع تهدیدها             |      |          |              |                  |                        |         |             |           |       | شماره کنترل‌ها |                  |  |  |  |  |
|---------------------------|------|----------|--------------|------------------|------------------------|---------|-------------|-----------|-------|----------------|------------------|--|--|--|--|
| اقدام‌های انسانی          |      |          |              |                  | فرآیندهای داخلی ناموفق |         |             |           |       |                | رویدادهای بیرونی |  |  |  |  |
| برنامه‌ریزی عملی          | عملی | بدون عمل | طراحی فرآیند | کنترل‌های فرآیند | پشتیبانی               | مخاطرات | مسائل حقوقی | کسب و کار | خدمات |                |                  |  |  |  |  |
| تأمین کننده               |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| رداختن به امنیت اطلاعات   |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| در قراردادهای تأمین       |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| کننده                     |      |          |              |                  |                        |         |             |           |       |                | 20.5             |  |  |  |  |
| مدیریت امنیت اطلاعات در   |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| زنجیره تأمین ICT          |      |          |              |                  |                        |         |             |           |       |                | 21.5             |  |  |  |  |
| ظارت، بررسی و مدیریت      |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| تغییر خدمات تأمین         |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| کننده                     |      |          |              |                  |                        |         |             |           |       |                | 22.5             |  |  |  |  |
| نیست اطلاعات برای استفاده |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| از خدمات ابری             |      |          |              |                  |                        |         |             |           |       |                | 23.5             |  |  |  |  |
| نامه ریزی و آماده سازی    |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| مدیریت حوادث امنیت        |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| اطلاعات                   |      |          |              |                  |                        |         |             |           |       |                | 24.5             |  |  |  |  |
| زیایی و تصمیم‌گیری در     |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| مورد رویدادهای امنیت      |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| اطلاعات                   |      |          |              |                  |                        |         |             |           |       |                | 25.5             |  |  |  |  |
| اسخ به حوادث امنیت        |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| اطلاعات                   |      |          |              |                  |                        |         |             |           |       |                | 26.5             |  |  |  |  |
| سادگیری از حوادث امنیت    |      |          |              |                  |                        |         |             |           |       |                |                  |  |  |  |  |
| اطلاعات                   |      |          |              |                  |                        |         |             |           |       |                | 27.5             |  |  |  |  |
| مجموعه شواهد              |      |          |              |                  |                        |         |             |           |       |                | 28.5             |  |  |  |  |
| نیست اطلاعات در هنگام     |      |          |              |                  |                        |         |             |           |       |                | 29.5             |  |  |  |  |

| انواع تهدیدها    |      |          |              |                  |          |         |             |                        |       |                                                    | کنترل ها |
|------------------|------|----------|--------------|------------------|----------|---------|-------------|------------------------|-------|----------------------------------------------------|----------|
| اقدام های انسانی |      |          |              |                  |          |         |             | فرآیندهای داخلی ناموفق |       |                                                    |          |
| پیش عملی         | عملی | بدون عمل | طراحی فرآیند | کنترل های فرآیند | پشتیبانی | مخاطرات | مسائل حقوقی | کسب و کار              | خدمات |                                                    |          |
| اختلال           |      |          |              |                  |          |         |             |                        |       |                                                    |          |
|                  |      |          |              |                  |          |         |             |                        |       | مسادگی ICT برای تداوم کسب و کار                    |          |
|                  |      |          |              |                  |          |         |             |                        |       | 30.5                                               |          |
|                  |      |          |              |                  |          |         |             |                        |       | مناسایی الزامات قانونی، قانونی، مقرراتی و قراردادی |          |
|                  |      |          |              |                  |          |         |             |                        |       | 31.5                                               |          |
|                  |      |          |              |                  |          |         |             |                        |       | حقوق مالکیت معنوی                                  |          |
|                  |      |          |              |                  |          |         |             |                        |       | 32.5                                               |          |
|                  |      |          |              |                  |          |         |             |                        |       | حفاظت از سوابق                                     |          |
|                  |      |          |              |                  |          |         |             |                        |       | 33.5                                               |          |
|                  |      |          |              |                  |          |         |             |                        |       | تمریم خصوصی و حفاظت از PII                         |          |
|                  |      |          |              |                  |          |         |             |                        |       | 34.5                                               |          |
|                  |      |          |              |                  |          |         |             |                        |       | ورسی مستقل امنیت                                   |          |
|                  |      |          |              |                  |          |         |             |                        |       | 35.5                                               |          |
|                  |      |          |              |                  |          |         |             |                        |       | اطلاعات                                            |          |
|                  |      |          |              |                  |          |         |             |                        |       | عایت سیاست ها و استانداردهای امنیت                 |          |
|                  |      |          |              |                  |          |         |             |                        |       | 36.5                                               |          |
|                  |      |          |              |                  |          |         |             |                        |       | اطلاعات                                            |          |
|                  |      |          |              |                  |          |         |             |                        |       | 37.5                                               |          |
|                  |      |          |              |                  |          |         |             |                        |       | رویه های عملیاتی مستند                             |          |
|                  |      |          |              |                  |          |         |             |                        |       | 1.6                                                |          |
|                  |      |          |              |                  |          |         |             |                        |       | ربالگری                                            |          |
|                  |      |          |              |                  |          |         |             |                        |       | 2.6                                                |          |
|                  |      |          |              |                  |          |         |             |                        |       | رابط و ضوابط استخدام                               |          |
|                  |      |          |              |                  |          |         |             |                        |       | گاهی، آموزش و آموزش امنیت اطلاعات                  |          |
|                  |      |          |              |                  |          |         |             |                        |       | 3.6                                                |          |
|                  |      |          |              |                  |          |         |             |                        |       | رآیند انضباطی                                      |          |
|                  |      |          |              |                  |          |         |             |                        |       | 4.6                                                |          |
|                  |      |          |              |                  |          |         |             |                        |       | سئولیت های پس از خاتمه یا تغییر شغل                |          |
|                  |      |          |              |                  |          |         |             |                        |       | 5.6                                                |          |

| انواع تهدیدها                 |                  |          |           |        |                  |                        |         |             |          |       |
|-------------------------------|------------------|----------|-----------|--------|------------------|------------------------|---------|-------------|----------|-------|
|                               | اقدام‌های انسانی |          |           |        |                  | فرآیندهای داخلی ناموفق |         |             |          |       |
|                               | پذیرش عملی       | عدم عملی | تغییر عمل | فرآیند | کنترل‌های فرآیند | پیش‌بینی               | مخاطرات | مسائل حقوقی | کسب‌وکار | خدمات |
| ترازادهای محرمانه یا عدم افشا |                  | X        |           |        |                  | X                      |         | X           |          |       |
| ساز راه دور                   |                  | X        |           | X      | X                |                        | X       |             | X        |       |
| سزارش رویداد امنیت اطلاعات    |                  |          | X         |        | X                |                        |         | X           |          |       |
|                               |                  |          |           |        |                  |                        |         |             |          |       |

### ماتریس T-دارایی-T/تهدید/ابعاد

فراالگوی (ماتالگو) شامل یک رابطه س تعریف شده است (به کادر متالگوی MARISMA در شکل ۲ مراجعه کنید). این فراالگو برای تکمیل این ماتریس، معیارهای کمیته کارشناسانی که بر روی ایجاد الگو کار می‌کنند (یک کارشناس امنیت سایبری، یک کارشناس تحلیل ریسک و یک متخصص فرآیند کسب‌وکار) ضروری بود تا مشخص شود که کدام نوع تهدید می‌تواند به کدام نوع دارایی حمله کند. هنگامی که این رابطه برقرار شد، و با دانستن رابطه بین نوع دارایی‌ها و ابعاد (در جدول ۵)، و انواع تهدیدها (از قبل آگاهی از کنترل‌هایی که آنها را کاهش می‌دهند)، توانستیم جدول ۷ را تکمیل کنیم.

جدول ۷ این رابطه پیچیده تجزیه و تحلیل مخاطرات با MARISMA که نیاز به اجرا دارد را نشان می‌دهد. بنابراین، این جدول نشان می‌دهد که سلول‌ها برای هر نوع تهدید (ردیف‌های جدول) ابعاد را نشان می‌دهند که تحت تأثیر تهدید برای هر نوع دارایی قرار می‌گیرند (ستون‌های موجود در جدول). برای مثال، «تهدید عمدی» می‌تواند نوعی دارایی «تجهیزات اکتیو شبکه» در مدل فرآیند کسب‌وکار را تهدید کند و باعث آسیب به این گروه دارایی شود، اما این تهدید فقط در ابعاد "AD AT AV CO IN" که نمایانگر به ترتیب قابلیت ممیزی، دسترس‌پذیری، محرمانگی و یکپارچگی است، تأثیر گذار است.

[illegible]

1 T-Assets/T-Threats/Dimensions (ATD)

1000

## بررسی ماتریس

جدول ۷ روابط پیچیده بین انواع دارایی‌های اطلاعاتی، انواع تهدیدها و ابعاد امنیت اطلاعات را نشان می‌دهد. برخی از تلاقی‌های موجود در ماتریس شامل تمامی ابعاد امنیتی می‌شود که با All نشان داده شده است.

با توجه به جدول ۷ در طراحی فرایندهای کسب‌وکار در بانک‌ها و مؤسسات مالی باید ابعاد امنیتی لحاظ گردد. به عنوان مثال در طراحی فرایند سامانه اینترنت بانک (در دسته دارایی برنامه‌های کاربردی و سرویس‌های کسب‌وکار) باید طراحی فرایندهای داخلی این سامانه به گونه‌ای باشد که تمامی ابعاد امنیتی را پوشش دهد.

نکته حائز اهمیت این است که دارایی‌های اطلاعاتی به هم وابسته هستند و رفتار آنها بر روی یکدیگر تأثیر می‌گذارد. به عنوان مثال یک سرور فیزیکی دارای سیستم عامل است و بر روی آن برنامه کاربردی نصب شده و کارمندان (حتی پیمانکاران) می‌توانند به آن در سطوح مختلف دسترسی داشته باشند. در صورتی که کارمندی چه به صورت عمدی/غیرعمدی اختلالی در سرور فیزیکی بوجود آورد که سبب عدم دسترسی پذیری به آن شود، می‌تواند کل دارایی‌های اطلاعاتی وابسته را با اختلال عدم دسترسی پذیری مواجه کند.

در فرایند مدیریت مخاطرات باید وابستگی بین انواع دارایی‌های اطلاعاتی، انواع تهدیدها و ابعاد امنیت اطلاعات در نظر گرفته شود و نکته مهم‌تر تلاقی مدیریت مخاطرات امنیت اطلاعات در کل کسب‌وکار بانک است که باید در کلیه فرایندهای کسب‌وکار (حتی بجز فرایندهای امنیت اطلاعات)، باید لحاظ گردد.

### یافته‌های تحقیق

در پاسخ به سوالات مطرح شده در مقدمه و بیان مسئله، پس از انجام تحقیقات و بررسی‌های جامع بر روی مدل پیشنهادی، به نتایج و یافته‌های زیر دست یافتیم:

سوال تحقیق ۱: چگونه چارچوب MARISMA-BP می‌تواند مدیریت مخاطرات امنیتی را در فرایندهای کسب‌وکار بانکی بهبود بخشد؟

فرایند پاسخ به سوال ۱ و یافته‌ها:

- نتایج حاصل از مصاحبه با خبرگان نشان داد که ادغام شاخص‌های KRI در مدل، شناسایی تهدیدات را تا ۴۰٪ افزایش داده است.

- تحلیل پرسشنامه ها تأیید کرد که کنترل های پیشنهادی چارچوب، انطباق با استاندارد ISO/IEC 27005 را تسهیل می کند.
- سوال تحقیق ۲: مؤلفه های کلیدی چارچوب MARISMA-BP برای کاهش مخاطرات در طراحی فرآیندهای بانکی کدامند؟  
فرایند پاسخ به سوال ۲ و یافته ها:
- فراالگوی ATD (دارایی-تهدید-بُعد) به عنوان هسته اصلی چارچوب شناسایی شد.
- ۸۵٪ پاسخ دهندگان تأثیر مثبت سازوکارهای خودکار شناسایی تهدیدات را تأیید کردند.
- سوال تحقیق ۳: چگونه میتوان مدیریت مخاطرات را در فرآیندهای کسبوکار بانکها و مؤسسات مالی با استفاده از چارچوب MARISMA-BP بهبود بخشید؟  
فرایند پاسخ به سوال ۳ و یافته ها:

#### مبانی نظری:

- ادغام مفاهیم مدیریت مخاطرات (Risk Management) و مدیریت فرآیندهای کسبوکار (BPM) بر اساس استانداردهای ISO/IEC 27001 و NIST.
- معرفی چارچوب MARISMA-BP به عنوان یک راهکار یکپارچه برای تحلیل مخاطرات در فرآیندها.
- شناسایی انواع داراییهای اطلاعاتی (مانند اسناد سازمانی، سختافزارها، منابع انسانی) و تهدیدهای مرتبط (عمدی، غیرعمدی، بیرونی).
- تعیین ابعاد امنیتی (مانند محرمانگی، یکپارچگی، دسترس پذیری) و روابط آنها با دارایی ها و تهدیدها.
- تأیید روابط ماتریس ها و اولویت بندی کنترل های امنیتی بر اساس تجربیات عملی.
- پیشنهاد بهبودها برای افزایش تاب آوری فرآیندها در برابر مخاطرات.

- ارائه ماتریس‌های تحلیلی مانند ماتریس (ATD) برای شناسایی مخاطرات و کنترل‌های مؤثر.
- طراحی فرآیندهای کسب‌وکار ایمن با در نظر گرفتن ابعاد امنیتی و وابستگی‌های دارایی‌ها.

### بحث و نتیجه گیری

بانک‌ها و مؤسسات اعتباری باید به طور مستمر اقدامات امنیتی خود را ارزیابی کرده و تطبیق دهند تا از تهدیدات در حال تحول جلوتر بمانند.

الگوی پیشنهادی با ترکیب فناوری، آموزش و انطباق، نه تنها از جرمه‌های مالی و آسیب به شهرت جلوگیری می‌کند، بلکه به بانک‌ها و مؤسسات اعتباری کمک می‌کند به عنوان پیشگامان امنیت سایبری در صنعت مالی مطرح شوند. اجرای این الگو نیازمند تعهد مدیریت ارشد و تخصیص منابع کافی است، اما نتایج آن در بلندمدت، پایداری کسب‌وکار و جلب اعتماد مشتریان را تضمین می‌کند.

ویژگی‌های الگوی پیشنهادی شامل موارد زیر است:

- الگوی پیشنهادی در این تحقیق بر پایه ادغام چارچوب‌های بین‌المللی (مانند NIST CSF, ISO 27001) و الزامات نظارتی داخلی طراحی شده است. ویژگی‌های کلیدی آن عبارتند از:
- پویایی و انعطاف‌پذیری: توانایی تطبیق با تهدیدات سایبری در حال تحول و تغییرات مقرراتی.
- یکپارچه‌سازی با فرآیندهای کسب‌وکار: پیوند مستقیم مدیریت ریسک با عملیات روزمره بانک‌ها (مانند پردازش تراکنش‌ها، مدیریت داده‌های مشتریان).
- تمرکز بر پیشگیری و پاسخ سریع: استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی برای شناسایی تهدیدات و کاهش زمان پاسخگویی.

دلایل انتخاب الگوی پیشنهادی به شرح زیر است:

- ۱ پوشش شکاف‌های موجود در نظام بانکی

- ۱ بسیاری از بانک ها از چارچوب های ناهمگون و پراکنده استفاده می کنند که انطباق کافی با الزامات نظارتی داخلی ندارند. الگوی حاضر با تلفیق استانداردهای بین المللی و مقررات بومی، این خلأ را مرتفع می سازد.
- ۲ مزایای رقابتی نسبت به سایر الگوهای متداول
  - کاهش هزینه های انطباق: از طریق مکانیزه سازی فرآیندهای نظارت بر مخاطرات و گزارش دهی به مراجع ناظر.
  - جلب اعتماد ذی نفعان: با افزایش شفافیت در فرآیندهای امنیتی و ارتقای کارایی در صیانت از داده های حساس.

### پیشنهادهای

با استناد به یافته های این مطالعه، پیاده سازی الگوی ارائه شده می تواند به بانک ها و مؤسسات مالی کمک کند تا ضمن ارتقا امنیت اطلاعات و هماهنگی با فرایندهای کسب و کار، مزیت رقابتی قابل توجهی در مقایسه با سایر نهادهای هم صنف خود ایجاد نمایند. موارد زیر حاصل استخراج نتایج الگوی ارائه شده و پیشنهاد برای بانک ها و مؤسسات اعتباری می باشد:

- ۱ استقرار چارچوب های پویا
  - ایجاد واحدهای ارزیابی مستمر امنیتی برای نظارت بر تهدیدات نوظهور.
  - استفاده از تست های نفوذ و شبیه سازی حملات به صورت دوره ای.
- ۲ آموزش و فرهنگ سازی
  - توسعه برنامه های آموزشی اختصاصی برای کارکنان در سطوح مختلف (از مدیران ارشد تا اپراتورها).
  - برگزاری کارگاه های آگاهی بخشی درباره فیشینگ، مهندسی اجتماعی و حفاظت از داده ها.
- ۳ همکاری صنعتی و فناوری:
  - مشارکت در پلتفرم های اشتراک اطلاعات تهدیدات سایبری (مانند CERT های مالی).

- سرمایه‌گذاری بر راه‌حل‌های هوش مصنوعی و یادگیری ماشین برای تشخیص الگوهای حملات.
- ۴ انطباق نظارتی
- طراحی سیستم‌های گزارش‌دهی خودکار برای اثبات رعایت مقررات به نهادهای نظارتی.
- تعیین مسئول انطباق (Compliance Officer) برای پیگیری تغییرات قانونی.

### تحقیقات آینده

در راستای توسعه و ارتقای چارچوب‌های امنیت اطلاعات در حوزه بانکداری، پژوهش‌های آتی می‌توانند بر یکپارچه‌سازی مؤلفه‌های پویای مدیریت مخاطرات با تمرکز بر سازوکارهای خودکار شناسایی تهدیدات سایبری متمرکز شوند. همچنین، بررسی نقش تعدیل‌گر الزامات نظارتی و حریم خصوصی در چارچوب‌های امنیتی پیشرفته، از جمله مدل **IAS-Octave**، می‌تواند به درک عمیق‌تری از تعامل میان انطباق‌پذیری مقرراتی و کارایی عملیاتی منجر گردد.

علاوه بر این، ارزیابی اثربخشی چارچوب‌های ترکیبی مانند **MARISMA** در محیط‌های بانکی با استفاده از روش‌های شبیه‌سازی و تحلیل داده‌های بلادرنگ، می‌تواند گامی مؤثر در جهت بهینه‌سازی سیستم‌های مدیریت امنیت اطلاعات (**ISMS**) باشد. مطالعات طولی نیز می‌توانند تأثیر این چارچوب‌ها را بر پایداری امنیتی و تحول دیجیتال سازمانی در بلندمدت مورد سنجش قرار دهند.

در نهایت، توسعه الگوریتم‌های هوشمند مبتنی بر یادگیری ماشین برای پیش‌بینی تهدیدات نوظهور و سازوکارهای انطباق پویا با مقررات بانک مرکزی و سایر نهادهای نظارتی، می‌تواند به عنوان جهتی نوین در تحقیقات آینده مورد بررسی قرار گیرد.

## فهرست منابع

- Pérez-Álvarez JM, Maté A, Gómez-López MT, Trujillo J. Tactical business process- - decision support based on KPIs monitoring and validation. Comput Ind 2018;102:23–39. <http://dx.doi.org/10.1016/j.compind.2018.08.001>
- Micro T. Business process compromise (BPC). Tech. Rep., California, USA: Trend Micro - Forward-Looking Threat Research (FTR) Team; 2017, Accessed: 2023-25-07
- Lord Remorin RF, Matsukawa B. Tracking trends in business email compromise (BEC) - schemes. Tech. Rep., California, USA: Trend Micro Forward-Looking Threat Research (FTR) Team; 2018, Accessed: 2023-25-07
- Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R. Developing cyber resilient - systems: a systems security engineering approach. Tech. Rep., Maryland, USA: National Institute of Standards and Technology; 2019, <http://dx.doi.org/10.6028/NIST.SP.800-160v2r1>
- NIST Special Publication 800-37. Risk management framework for information systems - and organizations: A system life cycle approach for security and privacy. Tech. Rep., Gaithersburg, MD: National Institute of Standards and Technology; 2018, <http://dx.doi.org/10.6028/NIST.SP.800-37r2>
- Bakhtina M, Matulevičius R, Seeba M. Tool-supported method for privacy analysis of a - business process model. J Inf Secur Appl 2023;76:103525. <http://dx.doi.org/10.1016/j.jisa.2023.103525>, URL <https://www.sciencedirect.com/science/article/pii/S2214212623001096>
- Shameli-Sendi A. An efficient security data-driven approach for implementing risk - assessment. J Inf Secur Appl 2020;54:102593. <http://dx.doi.org/10.1016/j.jisa.2020.102593>, URL <https://www.sciencedirect.com/science/article/pii/S2214212620307614>
- Turskis Z, Goranin N, Nurusheva A, Boranbayev S. Information security risk assessment - in critical infrastructure: A hybrid MCDM approach. Informatica (Ljublj) 2019;30(1):187-211. <http://dx.doi.org/10.15388/Informatica.2019.203>
- Sun H, Xie X. Threat evaluation method of warships formation air defense based on - AR(p)-DITOPSIS. J Syst Eng Electron 2019;30(2):297. <http://dx.doi.org/10.21629/JSEE.2019.02.09>
- Suriadi S, Weiss B, Winkelmann A, ter Hofstede A, Adams M, Conforti R, Fidge C, Rosa - ML, Ouyang C, Pika A, Rosemann M, Wynn M. Current research in risk-aware business

- process management - overview, comparison, and gap analysis. *Communications of the Association for Information Systems* 2014;34:933–84. <http://dx.doi.org/10.17705/1CAIS.03452>, URL <http://eprints.qut.edu.au/50606>
- Varela-Vaca AJ, Parody L, Gasca RM, Gomez-Lopez MT. Automatic verification and diagnosis of security risk assessments in business process models. *IEEE Access* 2019;7:26448–65. <http://dx.doi.org/10.1109/ACCESS.2019.2901408>
- Griffor E, Wollman D, Greer C. Framework for cyber-physical systems: Volume 1, overview. Tech. Rep., Gaithersburg, MD: National Institute of Standards and Technology; 2017, <http://dx.doi.org/10.6028/NIST.SP.1500-201>
- Wulff A, Wunck C. Integration of business process management and big data technologies. In: *International conference on industrial engineering and operations management*. 2016, p. 8–10. <http://dx.doi.org/10.46254/AN06.20160061>
- Janiesch C, Koschmider A, Mecella M, Weber B, Burattin A, Di Ciccio C, et al. The internet of things meets business process management: A manifesto. *IEEE Syst Man Cybern Mag* 2020;6(4):34–44. <http://dx.doi.org/10.1109/MSMC.2020.3003135>
- Bazan P, Estevez E. Industry 4.0 and business process management: state of the art and new challenges. *Bus Process Manag J* 2021;28(1):62–80. <http://dx.doi.org/10.1108/bpmj-04-2020-0163>
- Pan L, Tomlinson A. A systematic review of information security risk assessment. *Int J Saf Secur Eng* 2016;6(2):270–81. <http://dx.doi.org/10.2495/SAFE-V6-N2-270-281>
- Marcinkowski B, Kuciapski M. A business process modeling notation extension for risk handling. In: Cortesi A, Chaki N, Saeed K, Wierchoń S, editors. *Computer information systems and industrial management*. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012, p. 374–81. [http://dx.doi.org/10.1007/978-3-642-33260-9\\_32](http://dx.doi.org/10.1007/978-3-642-33260-9_32)
- Abioye TE, Arogundade OT, Misra S, Adesemowo K, Damasevicius R. Cloud-based business process security risk management: A systematic review, taxonomy, and future directions. *Computers* 2021;10(12). <http://dx.doi.org/10.3390/computers10120160>
- Aleksandrov MN, Vasiliev VA, Aleksandrova SV. Implementation of the riskbased approach methodology in information security management systems. In: *2021 international conference on quality management, transport and information security, information technologies (IT QM IS)*. 2021, p. 137–9. <http://dx.doi.org/10.1109/ITQMIS53292.2021.9642767>
- Alshawabkeh M, Li X, Sullabi M. New information security risk management framework as an integral part of project life cycle. In: *Proceedings of the 2019 5th international*

- conference on humanities and social science research (ICHSSR 2019). Paris, France: Atlantis Press; 2019, p. 133–9. <http://dx.doi.org/10.2991/ichssr-19.2019.24>
- Javaid MI, Iqbal MMW. A comprehensive people, process and technology (PPT) application model for information systems (IS) risk management in small/medium enterprises (SME). In: 2017 international conference on communication technologies (ComTech). 2017, p. 78–90. <http://dx.doi.org/10.1109/COMTECH.2017.8065754>
- Alhawari S, Karadsheh L, Nehari Talet A, Mansour E. Knowledge-Based Risk Management framework for Information Technology project. *Int J Inf Manage* 2012;32(1):50–65. <http://dx.doi.org/10.1016/j.ijinfomgt.2011.07.002>
- Zambon E, Etalle S, Wieringa RJ, Hartel P. Model-based qualitative risk assessment for availability of IT infrastructures. *Softw Syst Model* 2011;10(4):553–80. <http://dx.doi.org/10.1007/s10270-010-0166-8>
- Argyropoulos N, Mouratidis H, Fish A. Enhancing secure business process design with security process patterns. *Softw Syst Model* 2020;19(3):555–77. <http://dx.doi.org/10.1007/S10270-019-00743-Y/FIGURES/16>, URL <https://link.springer.com/article/10.1007/s10270-019-00743-y>
- Adebukola, A. A., Navya, A. N., Jordan, F. J., Jenifer, N. J., & Begley, R. D. (2020). Cyber security as a threat to health care. *Journal of Technology and Systems*, 4(1), 32-64
- Samuel O,D, Adedolapo Omotosho, Odunayo Josephine Akindote, Abimbola Oluwatoyin Adegbite4, & Sarah Kuzankah Ewuga ,CYBERSECURITY RISK ASSESSMENT IN BANKING: METHODOLOGIES AND BEST PRACTICES, *Computer Science & IT Research Journal*, Volume 4, Issue 3, December 2023 ,DOI: 10.51594/csitrj.v659
- Rosado DG, Moreno J, Sánchez LE, Santos-Olmo A, Serrano MA, Fernández- Medina E. MARISMA-BiDa pattern: Integrated risk analysis for big data. *Comput Secur* 2021;102:102155. <http://dx.doi.org/10.1016/j.cose.2020.102155>
- Rosado DG, Santos-Olmo A, Sánchez LE, Serrano MA, Blanco C, Mouratidis H, et al. Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. *Comput Ind* 2022;142:103715. <http://dx.doi.org/10.1016/j.compind.2022.103715>
- E. Indriasari, H. Prabowo, F. Gaol, and B. Purwandari, "Digital Banking: Challenges, Emerging Technology Trends, and Future Research Agenda," *Int. J. E Bus. Res.*, vol. 18, pp. 1-20, 2022, doi: 10.4018/ijebr.309398
- B. Balkan, "Impacts of Digitalization on Banks and Banking," in *Digital Transformation in Industry*, pp. 33-50, 2021, doi: 10.1007/978-981-33-6811-8\_3

- M. Tashtamirov, "Financial Innovation and Digital Technology in the Banking System: An Institutional Perspective," SHS Web of Conferences, 2023, doi: 10.1051/shsconf/202317202004.
- L. Wewege, J. Lee, and M. Thomsett, "Disruptions and Digital Banking Trends," Journal of Applied Finance and Banking, vol. 10, pp. 1-2, 2020.
- R. Sebti, "BANKING IN THE DIGITAL AGE: ISSUES AND CHALLENGES," RIMAK International Journal of Humanities and Social Sciences, 2022, doi: 10.47832/2717-8293.18.12.
- S.B Nuthalapati, "AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking", 2023, Doi: 10.53555/kuey.v29i1.6908
- S.O. Dawodu, A.Omotosho, O. J. Akindote ,A.O.Adegbite, S.K.Ewuga, "Current Research in Risk-aware Business Process Management—Overview, Comparison, and Gap Analysis", Volume 4, Issue 3, P.220-243, December 2023,DOI: 10.51594/csitrj.v659
- Magerit. Magerit\_v3: Methodology for information systems risk analysis and management. Tech. Rep., Ministry of Public Administration; 2012, URL [https://administracionelectronica.gob.es/pae\\_Home/pae\\_Documentacion/pae\\_Metodolog/pae\\_Magerit.html](https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html)
- Caralli RA, Stevens JF, Young LR, Wilson WR. Introducing octave allegro: Improving the information security risk assessment process. Tech. Rep., Pittsburgh PA, USA: Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst; 2007,<http://dx.doi.org/10.1184/R1/6574790.v1>
- Klipper S. ISO/IEC 27005. In: Information security risk management: risikomanagement mit ISO/IEC 27001, 27005 und 31010. Wiesbaden: Vieweg+Teubner; 2022, p. 63–97. [http://dx.doi.org/10.1007/978-3-8348-9870-8\\_3](http://dx.doi.org/10.1007/978-3-8348-9870-8_3)
- ISO/IEC 21827:2008. Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®). Tech. Rep., International Organization for Standardization & International Electrotechnical Commission; 2008, <https://www.iso.org/standard/44716.html>
- De Haes S, Van Grembergen W, Joshi A, Huygh T. COBIT as a framework for enterprise governance of IT. In: Enterprise governance of information technology: achieving alignment and value in digital organizations. Cham: Springer International Publishing; 2020, p. 125–62. [http://dx.doi.org/10.1007/978-3-030-25918-1\\_5](http://dx.doi.org/10.1007/978-3-030-25918-1_5)
- Ross M, Jara AJ, Cosenza A. Baseline security recommendations for IoT in the context of critical information infrastructures. Tech. Rep., (November). European Union Agency For Network And Information Security; 2017, <http://dx.doi.org/10.2824/03228>

- NIST Special Publication 800-37. Risk management framework for information systems and organizations: A system life cycle approach for security and privacy. Tech. Rep., Gaithersburg, MD: National Institute of Standards and Technology; 2018, <http://dx.doi.org/10.6028/NIST.SP.800-37r2>
- ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Tech. Rep., <https://www.iso.org/standard/75652.html>: International Organization for Standardization & International Electrotechnical Commission; 2022
- ISO/IEC 27002:2022 - "Information security, CyberSecurity and Privacy Protection- Information Security Control", <https://www.iso.org/standard/75652.html>
- NIST Special Publication 800-53rev5. Security and privacy controls for information systems and organizations. Tech. Rep., National Institute of Standards and Technology; 2020, <http://dx.doi.org/10.6028/NIST.SP.800-53r5>
- Goettelmann E, Dahman K, Gateau B, Dubois E, Godart C. A security risk assessment model for business process deployment in the cloud. In: 2014 IEEE international conference on services computing. 2014, p. 307–14. <http://dx.doi.org/10.1109/SCC.2014.48>
- Hariyanti E, Djunaidy A, Siahaan DO. A conceptual model for information security risk considering business process perspective. In: 2018 4th international conference on science and technology. ICST, 2018, p. 1–6. <http://dx.doi.org/10.1109/ICSTC.2018.8528678>
- Santos-Olmo A, Sánchez L, Rosado D, Fernández-Medina E, Piattini M. Applying the action-research method to develop a methodology to reduce the installation and maintenance times of information security management systems. Future Internet 2016;8(3):36. <http://dx.doi.org/10.3390/fi8030036>, URL <http://www.mdpi.com/1999-5903/8/3/36>
- ISO/IEC TR 15443-1:2012. Information technology – Security techniques – A framework for IT security assurance – Part 1: Overview and framework. 2012, URL <https://www.iso.org/standard/59138.html>
- Vilarinho S, Mira da Silva M. Risk management model in ITIL. In: Cruz-Cunha MM, Varajão Ja, Trigo A, editors. Sociotechnical enterprise information systems design and integration. Hershey, PA, USA: IGI Global; 2013, p. 207–14. <http://dx.doi.org/10.4018/978-1-4666-3664-4.ch013>
- Cebula J, Popeck M, Young L. A taxonomy of operational cyber security risks version 2. Tech. Rep. CMU/SEI-2014-TN-006, Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University; 2014, <http://dx.doi.org/10.1184/R1/6571784.v1>

- Marinos L. ENISA threat taxonomy: A tool for structuring threat information. Initial report. Tech. Rep., (January):European Union Agency For Network And Information Security; 2016, p. 1–24, URL <https://www.enisa.europa.eu/topics/threat-risk-management/threats-andtrends/enisa-threat-landscape/threat-taxonomy/view>
- Marinos L, Lourenço M. ENISA threat landscape report 2018: 15 top cyberthreats and trends. European Union Agency for Network and Information Security (ENISA); 2019, URL [https://www.enisa.europa.eu/publications/enisathreat-landscape-report-2018/at\\_download/fullReport](https://www.enisa.europa.eu/publications/enisathreat-landscape-report-2018/at_download/fullReport)
- Barnum MS. Common attack pattern enumeration and classification (CAPEC) schema. Tech. Rep., Dulles, VA: Department of Homeland Security; 2008, URL [https://capec.mitre.org/documents/documentation/CAPEC\\_Schema\\_Description\\_v1.3.pdf](https://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1.3.pdf)
- Hacks S, Lagerström R, Ritter D. Towards automated attack simulations of BPMN-based processes. In: 2021 IEEE 25th international enterprise distributed object computing conference. EDOC, 2021, p. 182–91. <http://dx.doi.org/10.1109/EDOC52215.2021.00029>
- Cherdantseva Y, Hilton J. A reference model of information assurance amp; security. In: 2013 international conference on availability, reliability and security. 2013, p. 546–55. <http://dx.doi.org/10.1109/ARES.2013.72>
- Salnitri M, Dalpiaz F, Giorgini P. Designing secure business processes with SecBPMN. Softw Syst Model 2017;16(3):737–57. <http://dx.doi.org/10.1007/s10270-015-0499-4>
- Chinosi M, Trombetta A. BPMN: An introduction to the standard. Comput Stand Interfaces 2012;34(1):124–34. <http://dx.doi.org/10.1016/j.csi.2011.06.002>
- Aagesen G, Krogstie J. BPMN 2.0 for modeling business processes. In: vom Brocke J, Rosemann M, editors. Handbook on business process management 1: introduction, methods, and information systems. Berlin, Heidelberg: Springer Berlin Heidelberg; 2015, p. 219–50. [http://dx.doi.org/10.1007/978-3-642-45100-3\\_10](http://dx.doi.org/10.1007/978-3-642-45100-3_10)
- Zarour K, Benmerzoug D, Guermouche N, Drira K. A systematic literature review on BPMN extensions. Bus Process Manag J 2019;26(6):1473–503. <http://dx.doi.org/10.1108/BPMJ-01-2019-0040>
- Salnitri M, Dalpiaz F, Giorgini P. Designing secure business processes with SecBPMN. Softw Syst Model 2017;16(3):737–57. <http://dx.doi.org/10.1007/s10270-015-0499-4>
- Antunes P, Mourão H. Resilient Business Process Management: Framework and services. Expert Syst Appl 2011;38(2):1241–54. <http://dx.doi.org/10.1016/j.eswa.2010.05.017>, URL <https://linkinghub.elsevier.com/retrieve/pii/S0957417410004288>

Zahoransky RM, Koslowski T, Accorsi R. Toward resilience assessment in business – process architectures. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8696 LNCS, Springer Verlag; 2014, p. 360–70. [http://dx.doi.org/10.1007/978-3-319-10557-4\\_39](http://dx.doi.org/10.1007/978-3-319-10557-4_39)/COVER, URL [https://link.springer.com/chapter/10.1007/978-3-319-10557-4\\_39](https://link.springer.com/chapter/10.1007/978-3-319-10557-4_39)

