Social crisis management

1

Vol. 17
Spring 2025

Research Paper

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 *[1] | Elham Moghadam niya 2| Amin Mohajer3

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 paradig.

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.

Publisher: Imam Hussein University

مدیریت بحران های اجتماعی

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

۱

دوره هفدهم
بهار ۱٤۰٤

مقاله پژوهشی

تاریخ دریافت: ۱٤۰۳/۱۱/۰۷
تاریخ بازنگری: ۱٤۰۳/۱۲/۱۹
تاریخ پذیرش: ۱٤۰٤/۰۲/۱۰
تاریخ انتشار: ۱٤۰٤/۰۳/۰۱
صص: ۶۲-٤۱

شاپا چاپی: ۳۵٦٤-۲۰۰۸
الکترونیکی: ۵۲۵۸-۲٦٤۵

پگاه شایسته‌فر [۱] || الهام مقدم‌نیا [۲] | امین مهاجر [۳]

چکیده

فرآیندهای کسب‌وکار سنگ بنای بانک‌ها و مؤسسات مالی در نظر گرفته می‌شوند، اما بانک ها و موسسات مالی به طور فزاینده ای در کانون توجه حملات دشمن قرار می گیرند. 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 می باشد. برای نشان دادن قابلیت کاربردی الگوی پیشنهادی، الگوی ماریسما ب- پ برای یک سناریوی فرآیند کسب‌وکار در بانک ها اعمال شده است. با توجه به یافته‌ها، الگوی ماریسما ب- پ اساس کار می باشد ، 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 بحران های اجتماعی**، ۴(۱۷)، ۶۲-۴۱.
DOR: https://dorl.net/dor/20.1001.1.27173674.1403.5.1.1.3
ناشر: دانشگاه جامع امام حسین (ع)

مقدمه و بیان مسئله

فرایندهای کسب‌وکار (**BP**)[1] 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، فرآیندهای کسب‌وکار از نظر امنیتی بدون مخاطرات نیستند، (میکرو، ۲۰۲۳) یک مثال حمله به فرآیند کسب‌وکار است که از دانش عمیق رفتار این فرآیندها 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 فرآیندهای غیرمجاز را اجرا می‌کند. این نوع حملات به طرز فزاینده‌ای متداول‌تر می‌شوند و حتی گزارش‌هایی وجود دارد که بیان می‌کند تقریبا نیمی از سازمان‌های تحلیل شده تحت تأثیر حملات مختل کننده فرآیندهای کسب‌وکار قرار گرفته‌اند (لرد ریمورین و همکاران،۲۰۲۳).

بنابراین، یک رویکرد جامع برای مدیریت مخاطرات باید سیستم های 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 بپردازند، مرتبط کند (روز و همکاران، ۲۰۱۹). مدیریت مخاطرات امنیت اطلاعات با این حال، فرآیندهای کسب‌وکار را به‌عنوان 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 بهینه‌ای 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).

پیشنهادات قبلی به مدیریت مخاطرات در فرآیندهای کسب‌وکار توجه کرده‌اند. متأسفانه، این پیشنهادات بر روی توسعه‌ی گسترش‌های مدل فرآیند کسب‌وکار تمرکز کرده بودند تا حمایت از تجزیه‌وتحلیل مخاطرات را در زمینه‌ی مدل دنبال کنند (سوریادی و همکاران، ۲۰۱۴)، (وارلا–واکا و همکاران، ۲۰۱۹)، (گریفور و همکاران، ۲۰۱۷). علاوه بر این، این رویکردها برخی ویژگی‌های جالب برای مدیریت مخاطرات را تحلیل نمی کنند، به‌عنوان مثال، اینکه فرآیندهای کسب‌وکار می‌توانند به‌عنوان سازوکاری برای یکپارچه‌سازی مخاطرات خاص، مانند داده‌های کلان (وولف و همکاران، ۲۰۱۶)، اینترنت اشیا **(IoT)** (جانیش و همکاران، ۲۰۲۰) یا سیستم‌های سایبر فیزیکی **(CPS)**[1](بازان و همکاران، ۲۰۲۰) در اکوسیستم‌ها استفاده شوند. بنابراین، ممکن است فرآیند کسب‌وکار به‌وسیله تکنولوژی‌های زیرساختی خود مورد تهدید قرار گیرد. روش‌های ارزیابی مخاطرات سیستم‌های **IT** [2] (فناوری اطلاعات) سنتی (پن و همکاران، ۲۰۱۶) برای اعمال به فرآیندهای کسب‌وکار طراحی نشده‌اند و بنابراین، نمی‌توانند به‌طور مستقیم اعمال شوند.

اگرچه ارزیابی مخاطرات سیستم‌های **IT** سنتی به اندازه کافی بالغ شده‌اند، اما رویکردهای جدیدی برای مقابله با مشکلات امنیتی رو به رشد که به دلیل تفاوت‌های بزرگ بین سیستم‌های **IT**و مخاطرات فرآیندهای کسب‌وکار به وجود می‌آید، لازم است (مارسینکوفسکی و همکاران، ۲۰۱۲). اگرچه پیشنهادهای متعددی برای رسیدگی به ارزیابی و مدیریت مخاطرات **IT** به طور نظام‌مند وجود داشته است، این پیشنهادها معمولاً در به کارگیری عملی آن‌ها در محیط‌های بسیار پویا و به هم‌پیوسته با مشکلاتی مواجه شده‌اند (ابیویه و همکاران، ۲۰۲۱) و (الکساندروف و همکاران، ۲۰۲۱).

1 Cyber-Physical Systems (CPS)
2 Information Technology (IT)

در واقع، برای اینکه روش های ارزیابی و مدیریت مخاطرات واقعاً مؤثر باشند، باید قابل اجرا باشند (از نظر نیاز به منابع انسانی، فنی و اقتصادی محدود) برای کسب‌وکارهای 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 به‌دست‌آمده در تحلیل‌های مخاطرات قبلی است و داشتن ابزارهای پشتیبانی که کارها را خودکار کرده و رعایت روش های به کار رفته را آسان کند، امری ضروری است. نویسندگان در (آرگیروپولوس و همکاران، ۲۰۲۰) پیشنهاد می کنند که حوزه مهندسی الزامات امنیت و حوزه الگوهای امنیتی با هم ترکیب شوند و به همراه مدل‌سازی فرآیندهای کسب‌وکار، مجموعه‌ای از الگوهای امنیتی در سطح فرآیند تولید کنند که برای پیاده‌سازی امنیت در یک مدل فرآیند کسب‌وکار خاص استفاده شوند.

پیشرفت سریع فناوری های 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).

(داودو 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 تجزیه‌وتحلیل داده‌های بزرگ، قابلیت‌های بانکداری دیجیتال را افزایش داده و خدمات شخصی و کارآمد را به مشتریان ارائه می‌دهد (تاشتمیروف و همکاران، ۲۰۲۳) .این فن‌آوری‌ها بانک‌ها را قادر می‌سازند

تا عملیات خود را بهینه کنند، هزینه‌ها را کاهش دهند و رضایت مشتری را با ارائه راه‌حل‌های مالی در زمان واقعی و مناسب بهبود بخشند (بالکان و همکاران، ۲۰۲۱) (ویوش و همکاران، ۲۰۲۰). با این حال، دگرگونی سریع دیجیتال همچنین چالش‌هایی را در رابطه با امنیت داده‌ها، حریم خصوصی و انطباق با مقررات ایجاد می‌کند که باید برای اطمینان از رشد پایدار بانکداری دیجیتال مورد توجه قرار گیرد (تاشتمیروف و همکاران، ۲۰۲۳) و (سبتی و همکاران، ۲۰۲۲).

بخش بانکداری دیجیتال شیوه انجام تراکنش‌های مالی را متحول کرده است و راحتی و دسترسی بی‌سابقه‌ای را به کاربران در سراسر جهان ارائه می‌کند. 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 می‌کند. اتکای فزاینده به اینترنت و برنامه‌های 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 آسیب‌پذیری‌ها و سرقت اطلاعات حساس استفاده می‌کنند (نوتالاپاتی و همکاران، ۲۰۲۳).

در این زمینه، ضرورت اقدامات امنیت سایبری قوی در بانکداری را نمی‌توان اغراق کرد. امنیت سایبری نیز در زمینه مراقبت‌های 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 روش‌شناسی و بهترین شیوه‌های ضروری برای حفاظت از موسسات مالی در عصر تهدیدات سایبری مداوم و پیچیده در این مطالعه بررسی می‌شود. از آنجایی که بخش مالی در حال حرکت در یک چشم‌انداز تهدید در حال تحول است که با بدافزارهای پیشرفته، حملات فیشینگ، تهدیدات داخلی و آسیب‌پذیری‌های ذاتی در سیستم‌های دیجیتال مشخص می‌شود، نیاز به یک چارچوب ارزیابی مخاطرات امنیت سایبری جامع و تطبیقی بسیار مهم می‌شود.

(اونیمسی و همکاران،۲۰۲۳) به بررسی روش‌شناسی، به بهترین شیوه‌های ضروری برای مدیریت مؤثر مخاطرات امنیت سایبری در بانکداری پرداخته‌اند. 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 می‌کند. 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 کسب‌وکار، 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 کسب‌وکار ادغام می‌کنند، مقایسه می‌کنند و به این نتیجه می رسند که کمبود جدی ابزارها و سازوکارهایی برای خودکارسازی فرآیند ارزیابی مخاطرات و مدیریت فرآیندهای کسب‌وکار 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 کسب‌وکار باید با مدیریت مخاطرات به منظور جلوگیری یا کاهش تأثیر حملات بر فرآیندهای کسب‌وکار یکپارچه شود.

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

پس از تجزیه‌وتحلیل فرآیندها و چارچوب‌های مخاطرات فعلی، متوجه شده‌ایم که سطوح فرآیند سازمانی و کسب‌وکار، اغلب نادیده گرفته می‌شوند؛ به همین دلیل در این مقاله چارچوب **MARISMA**در سطحی که به چشم‌انداز فرآیند کسب‌وکار مربوط می‌شود، توسعه داده شده است. در واقع چارچوب **MARISMA** به طراحی مدل، پیاده‌سازی فرآیندها و اجرای عملکردهای کسب‌وکار 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 کسب‌وکار را بدون در نظر گرفتن عنصر خارجی طراحی‌شده در مدل بررسی می‌کنند، پر می‌کند.

در این راستا ما در این تحقیق الگوی **(MARISMA for Business Process) MARISMA-BP** 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 کسب‌وکار امکان پذیر کند.

در خصوص تجزیه‌وتحلیل و ارزیابی مخاطرات امنیت اطلاعات، استانداردها و روش‌های زیر مورد بررسی قرار گرفت:

(**i**) روش تجزیه‌وتحلیل مخاطرات و مدیریت برای سیستم‌های اطلاعاتی (ماگرید، ۲۰۱۲)، که فرآیند مدیریت مخاطرات را در چارچوب حاکمیتی به منظور کمک به تصمیم‌گیری، با در نظر گرفتن مخاطرات در زمینه فناوری اطلاعات، پیاده‌سازی می‌کند.

(**ii**) ارزیابی تهدید، دارایی و آسیب پذیری عملیاتی حیاتی **(OCTAVE)**[1] (کارالی و همکاران، ۲۰۰۷) که یک تکنیک برنامه‌ریزی استراتژیک و مشاوره مبتنی بر فناوری در امنیت است.

(**iii**) روش تجزیه‌وتحلیل مخاطرات و مدیریت آژانس ارتباطات و مخابرات مرکزی (**CRAMM**)[2]، که یک روش مدیریت مخاطرات است که شامل سه مرحله است: شناسایی، ارزیابی و مدیریت مخاطرات (کلیپر از سازمان ایزو، ۲۰۲۲) و (ایزو ۲۱۸۲۷، ۲۰۰۸).

(**iv**) اهداف کنترلی برای اطلاعات و فناوری‌های مرتبط **(COBIT)**[3] (دی هایس و همکاران، ۲۰۲۲)، که روشی برای کنترل کافی پروژه‌های فناوری، جریان‌های اطلاعات و مخاطرات ناشی از فقدان کنترل‌های کافی است. **COBIT** شامل فرآیند با هدف ارزیابی مخاطرات است، که عمدتاً بر معیارهای محرمانگی، یکپارچگی و دسترس‌پذیری 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 [1] **(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 کرده اند ارزیابی و مدیریت مخاطرات را در فرآیندهای خود بگنجانند:

i. گروه استانداردهای **ISO/IEC 27000** و به طور خاص استاندارد **ISO/IEC 27005** که دستورالعمل هایی را برای مدیریت مخاطرات در امنیت اطلاعات ایجاد می کند.

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 می کند که ویژگی های اساسی فرآیندهایی را که باید در یک سازمان وجود داشته باشد، توصیف می کند. 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 روش های موجود را بسته به سطح امنیت و مرحله اطمینان طبقه بندی می کند (ارزیابی اطمینان به فرآیند، محصول و محیط تقسیم می شود، در حالی که مراحل ارزیابی مخاطرات عبارتند از طراحی/پیاده‌سازی، ادغام/تأیید، همانندسازی، انتقال، و عملیات)؛

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

این استانداردها و چارچوب‌ها، دانش به روز و دقیق از کلیه دارایی‌های سازمان و روابط، وزن ها و وابستگی های بین آنها را نشان می‌دهد. با این حال، این استانداردها، در عین حال که ادغام شده‌اند، به سمت تجزیه‌وتحلیل مخاطرات در فرآیندهای کسب‌وکار نمی‌روند. این استانداردها دارای جهت گیری مخاطرات عمدتاً به سمت امنیت سایبری و سیستم‌های اطلاعاتی هستند.

1 National Institute of Standards and Technology (NIST)

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

به طور کلی، معمولاً نگرانی‌ها در خصوص مدیریت فرآیند کسب‌وکار (**BPM**)[1] و مدیریت مخاطرات به‌صورت مجزا در نظر گرفته می‌شوند (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 روش‌مند امنیت **BPM** را می‌توان در (هاریانتی و همکاران، ۲۰۱۸) یافت، که بر انجام بررسی رویکردهای ارزیابی مخاطرات امنیتی مبتنی بر فرآیند کسب‌وکار متمرکز است و نویسندگان آن به این نتیجه می رسند که لازم است مدل‌های جدیدی با این رویکرد ایجاد شود.

این تحقیق در نهایت به سوالات زیر پاسخ خواهد داد:

- چگونه چارچوب **MARISMA-BP** می‌تواند مدیریت مخاطرات امنیتی را در فرآیندهای کسب‌وکار بانکی بهبود بخشد؟
- مؤلفه‌های کلیدی چارچوب **MARISMA-BP** برای کاهش مخاطرات در طراحی فرآیندهای بانکی کدامند؟
- چگونه می‌توان مدیریت مخاطرات را در فرآیندهای کسب‌وکار بانک‌ها 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**[1]) 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)** مجموعه ای از دستورالعمل های داوطلبانه است که توسط موسسه ملی استاندارد و فناوری (**NIST**) برای کمک به سازمان ها در مدیریت و کاهش مخاطرات امنیت سایبری ایجاد شده است.

ت) استاندارد ISO/IEC 27005

ISO/IEC 27005یک 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.

دسترس‌پذیری (Availability)

1 Information Security Management System

اطمینان از اینکه اطلاعات و سیستم‌های مورد نیاز در دسترس کاربران مجاز در مواقع لازم هستند.
مثال: استفاده از سیستم‌های پشتیبان‌گیری و برنامه‌های 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 می‌پردازد. این فرآیند به سازمان‌ها کمک می‌کند 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 کسب‌وکار 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 ماتریس‌ها و چارچوب‌های 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 سازمان‌هاست.

جامعه این پژوهش شامل متون علمی، استانداردهای بین‌المللی (مانند **ISO/IEC 27001**، **ISO/IEC 27005**، **NIST 800-53**)، و همچنین خبرگان حوزه مدیریت مخاطرات و فرآیندهای کسبوکار است. همچنین نمونه‌گیری به صورت هدفمند انجام شده و شامل اسناد معتبر، استانداردهای منتخب، و نظرات خبرگان (متخصصان امنیت سایبری، تحلیل‌گران مخاطرات، و متخصصان فرآیندهای کسب‌وکار) بوده است.

أ) روش جمع‌آوری داده‌ها

در این روش، داده‌های مورد تحقیق به صورت کیفی و کمی جمع‌آوری شده است:

- داده‌های کیفی: از طریق مرور سیستماتیک متون علمی، استانداردها، و چارچوب‌های موجود (مانند **MARISMA**، **BPMN** و **SecBPMN2**) جمع‌آوری 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.

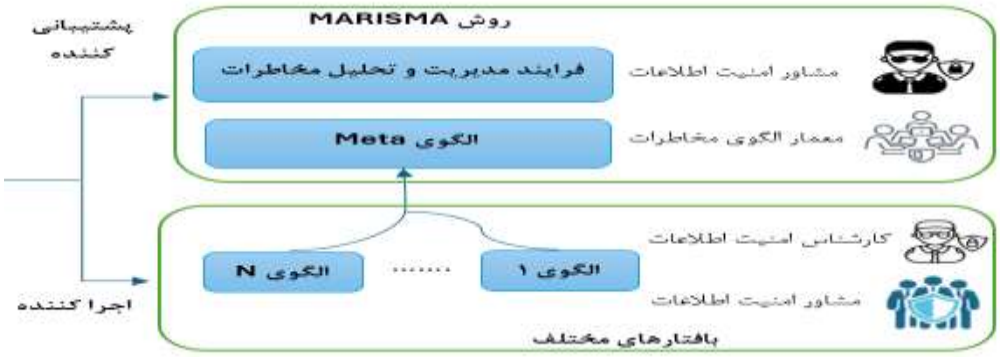
ت) روش تحلیل داده‌ها

تحلیل داده‌ها در این پژوهش به‌صورت 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 ۱معماری 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 ابرداده (متا الگوی مخاطرات ما)، یک سازوکار توسعه پذیری (در قالب الگوهای خاص که نمونه هایی از متاالگوی 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 مجموعه‌ای از شاخص‌های مخاطرات کلیدی (**KRI**)[1] و توسط یک طرح ابرداده پشتیبانی می‌شود، که عناصر و روابط آنها را مشخص می کند که حداکثر سفارشی‌سازی و اتوماسیون فرآیند ارزیابی و مدیریت مخاطرات را امکان‌پذیر می‌سازد.

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 می‌دانیم که بخش‌های خاص یا محیط‌های 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**[1] 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 تجزیه‌وتحلیل 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 تجزیه‌وتحلیل کند، باید بتواند بر استانداردهای خاص، در این مورد **ISO27001** و زیرساخت بحرانی تکیه کند.

این چارچوب به طور گسترده در انواع مختلف شرکت ها (برق، هیدروکربن، دولت، بهداشت، کشتی سازی، صنایع شیمیایی و غیره) در بیش از هشت کشور اروپایی و آمریکای لاتین اعمال شده و می شود 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 غنی سازی الگو استفاده

1 Cyber-Physical Systems (CPS)

می‌شود، بنابراین دقت عناصر خود را افزایش می‌دهد و به سازمان‌های دیگر اجازه می‌دهد از این اصلاح جدید بهره‌مند 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 وتحلیل 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 کنترل‌ها، همراه با طبقه‌بندی تهدیدها و انواع دارایی‌های امنیتی رایج ترین در هر محیط فناوری اطلاعات در نظر گرفت.

بنابراین، هدف **MARISMA-BP** ارائه مدل‌های فرآیند کسب‌وکار با ارزیابی و مدیریت مخاطرات کامل، انعطاف‌پذیر، سازگار و قابل اجرا است. مدیریت مخاطرات فرآیندهای کسب وکار شامل عناصری مانند گردش کار، وظایف، داده های خارجی و سازوکارهایی برای رخدادها و رویدادها است.

فراالگوی[1] **MARISMA-BP** ، عناصر عمومی مشترک برای هر تحلیل و مدیریت مخاطرات، مانند دارایی‌ها، تهدیدها و ابعاد را تعریف می کند، علاوه بر این شامل کنترل‌های 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 دارایی‌ها بر اساس ابعاد آن‌ها دارند و چه مجموعه‌ای از کنترل‌ها برای حفاظت از آن دارایی‌ها در برابر تهدیدها مناسب‌تر است .

فراالگوی **MARISMA** از یک سو شامل دارایی‌ها (خانواده و انواع دارایی‌ها) به عنوان دسته‌بندی دارایی های سیستم درنظر گرفته می‌شود 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، درنظر گرفت.

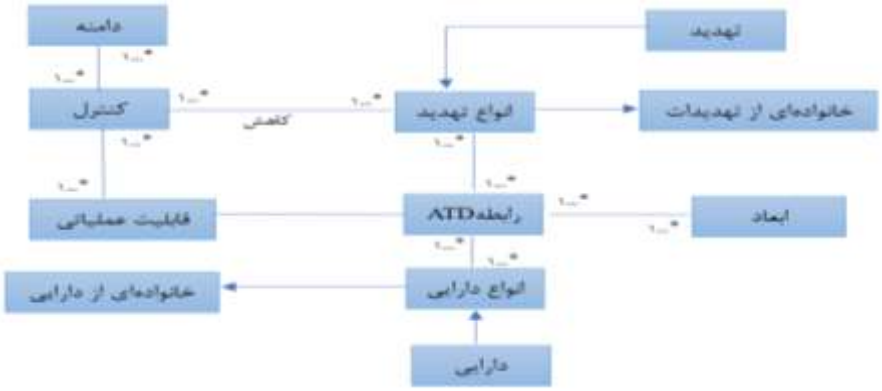
1 meta-pattern

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.

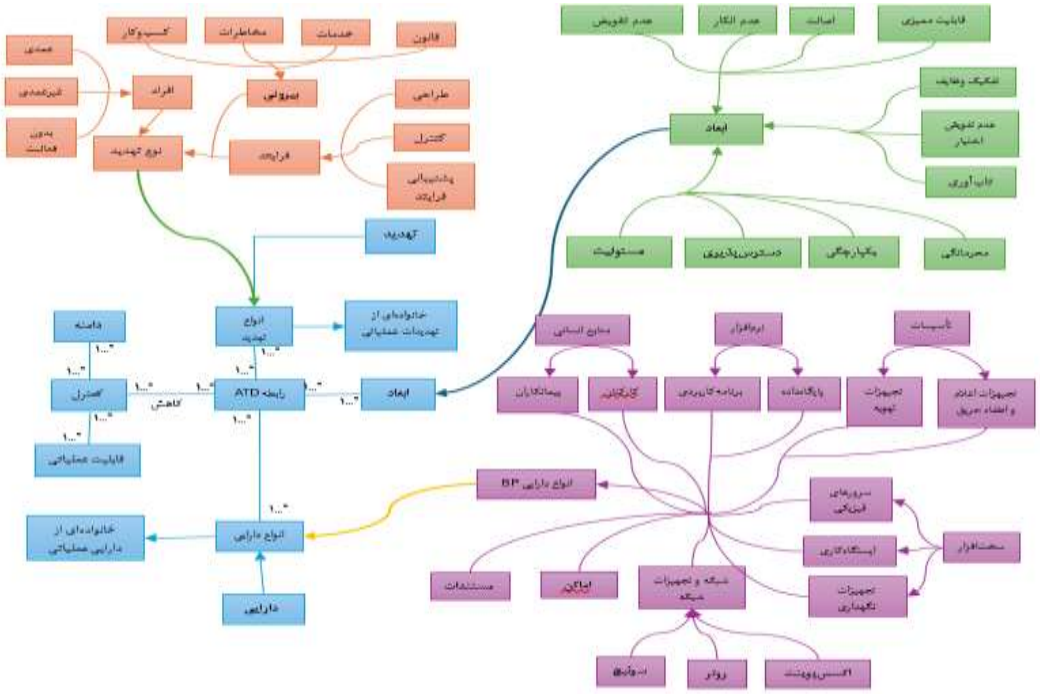
بنابراین، این رابطه سه تایی است (**ATD**: نوع دارایی - نوع تهدید - ابعاد[1]) بین انواع دارایی ها، انواع تهدیدها و ابعادی که با آن تأثیر تهدیدها و آسیبی که ممکن است از طریق آنها به ارزش دارایی وارد شوند را نشان می‌دهد. ابعاد رابطه یکی دیگر از روابط موجود بین انواع تهدیدها و کنترل‌های موجود است که می‌تواند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

این فراالگو 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 فراالگو به عنوان پایه تعریف شوند.

1 ATD: Asset type - Threat type- Dimension



شکل ۲-فرا الگوی**MARISMA**



شکل ۳ -مدل پیشنهادی الگوی**MARISMA-BP.**

کنترل‌های امنیتی

همانطور که شکل ۳ نشان می‌دهد، کنترل‌های امنیتی انواع تهدید را کاهش می‌دهند (متاالگوی 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 فراالگوی ماریسما (به کادر فراالگو، 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 زمینه ها(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 فراالگو 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

مدل‌های فرآیند کسب‌وکار مناسب‌تر هستند. این کنترل‌ها معمولاً با استفاده از تجزیه‌وتحلیل استانداردهای اصلی امنیت و فرآیندهای کسب‌وکار انتخاب می‌شوند (فعالیت **A.1**).

۲-انواع تهدیدات مربوط به فرآیندهای کسب‌وکار را با مطالعه و تجزیه‌وتحلیل طبقه‌بندی‌های مختلف تهدیدات مناسب برای این زمینه تعریف و انتخاب کنید (فعالیت **A.2**).

۳-شناسایی و تعریف انواع دارایی‌های اطلاعاتی که لازم است محافظت شود. این دارایی‌ها با مطالعه و ۳تجزیه‌وتحلیل طبقه‌بندی‌های اصلی دارایی برای فرآیندهای کسب‌وکار موجود انتخاب می‌شوند (فعالیت **A.3**).

۳- شناسایی تهدیدهای بالقوه‌ای که ممکن است در حوزه فرآیند کسب‌وکار مرتبط باشند. این تهدیدها با مطالعه و تجزیه‌وتحلیل طبقه‌بندی تهدیدات اصلی برای فرآیندهای کسب‌وکار موجود (فعالیت **A.4**) انتخاب می‌شوند.

۴- مجموعه ابعادی را که بخشی از انواع دارایی‌ها را تشکیل می‌دهند و به آن مربوط می‌شوند، 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 ماتریس‌های رابطه است، بنابراین اجازه می‌دهد ماتریسی تولید شود که تهدیدات را به کنترل‌ها مرتبط می‌کند، و یک مقدار اولیه برای درصد وقوع یک تهدید برای یک کنترل خاص تعریف می‌کند (فعالیت **A. 6**).

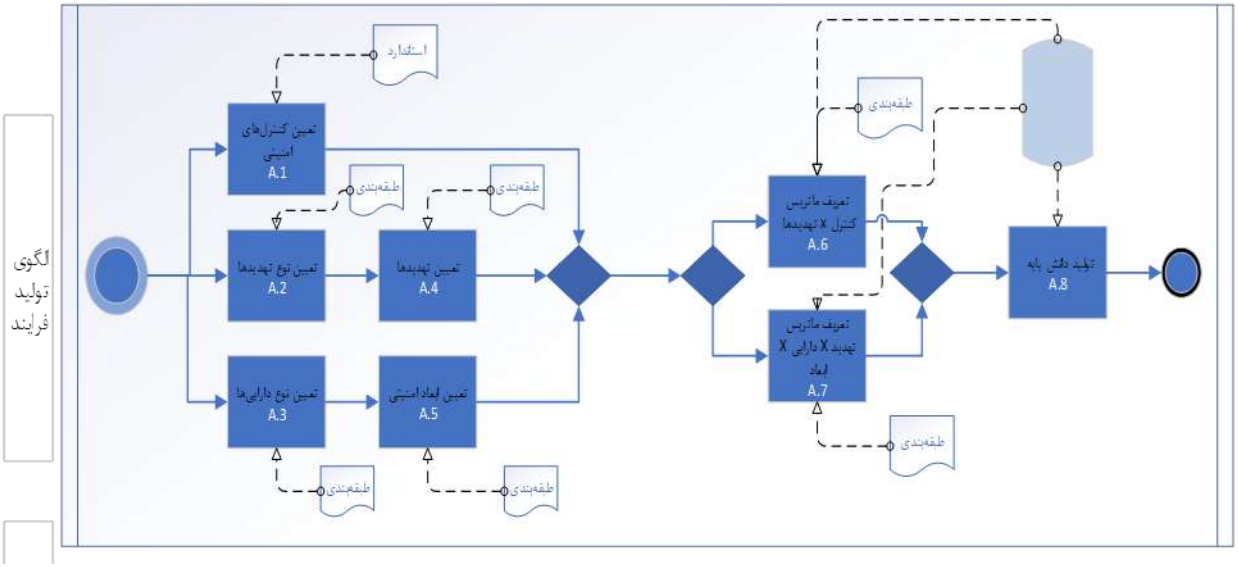
۶- ماتریسی که با آن تهدیدها را به انواع دارایی مرتبط می‌کند نیز ایجاد می‌شود که ابعاد امنیتی را نشان می‌دهد که توسط عمل تهدید برای هر نوع دارایی به خطر می افتد (فعالیت **A.7**).

این ماتریس‌ها از اهمیت عمده‌ای برخوردارند، زیرا به عنوان مخزن دانشی که الگو را ارائه می‌کند، این امکان را می‌دهند که ویژگی‌های پویایی خود را در انطباق با تغییرات و سرعت در تولید تحلیل مخاطرات داشته باشیم. دانش ترکیبی متخصص امنیت سایبری و کارشناس فرآیند کسب‌وکار نیز یک جنبه کلیدی در این مرحله خواهد بود، زیرا بازخورد به وظایف **A.1-A.5** با پیکربندی ماتریس‌ها 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 ۱خلاصه‌ای از مراجع استفاده شده در هر یک از منابع را نشان می‌دهد:

جدول۱: 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) ENISA taxonomy of threats (2016)

موسسه مهندسی نرم افزار (SEI)[1] 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 طبقه بندی تهدیدات خود را بر اساس استانداردهای اصلی مخاطرات موجود توسعه داد (مارینوس و همکاران، ۲۰۱۶) و (مارینوس و همکاران، ۲۰۱۹). در نهایت، CAPEC[2] طبقه‌بندی خود را براساس فهرست‌بندی الگوهای حمله مورد استفاده برای بهره برداری از آسیب‌پذیری‌های سیستم، توسعه داد (بارنوم، ۲۰۰۸).

علاوه بر این، BPMN [3] استانداردی 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 حوزه های 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 قبلا ذکر شد، فراالگوی چارچوب MARISMA (کادر متاالگوی MARISMA در شکل ۳) شامل تمام موجودیت ها است. برای انجام تجزیه‌وتحلیل مخاطرات، مانند کنترل‌های امنیتی، تهدیدات، دارایی‌ها و ابعاد امنیتی، همراه با روابط بین این عناصر انواع دارایی‌ها برای فرآیندهای کسب‌وکار (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 کسب‌وکار ابعاد امنیتی که تحت تأثیر قرار خواهند گرفت توسط دارایی ها 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 جدول۳ مراجعه کنید). در نهایت انواع تهدیدهایی که ممکن است بر فرآیندهای کسب وکار 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 بخش های 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 می شویم که مجموعه ای از کنترل ها (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 کسب‌وکار درگیر هستند، کنترل های فردی (۸ کنترل) تعریف شده در استاندارد نیز در نظر گرفته شده است، و دسته بندی‌های دیگر مانند فیزیکی و فنی را کنار می‌گذاریم، زیرا در این تکرار اول در نظر گرفته نشده اند. 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 کسب‌وکار 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
	تجهیزات اداری (بدون مراقبت)	پرینتر، فکس، دیش ماهواره و تجهیزات ارتباط رادیویی
	ذخیره‌سازها	SAN Storage انواع UFD،External HDD[1]، لپ‌تاپ، تبلت، Tape، ODD[2]
منابع انسانی	کارکنان سازمان	کارکنان بخش‌های مختلف سازمان
	پیمانکاران	نیروهای شرکت‌های طرف قرارداد، شرکای کسب وکار 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
	تجهیزات تهویه مطبوع	تجهیزات خنک‌کننده سایت‌ها و رک‌ها
	تجهیزات اعلان و اطفای حریق	حسگرهای دود، سامانه‌های اعلان و اطفای حریق
	تجهیزات کنترل دسترسی	دزدگیر، دوربین‌ها و دستگاه‌های کنترل تردد
فرایند	فرایند مدیریت پروژه	پروژه‌های اجرایی مرتبط با امنیت اطلاعات
	فرایند توسعه سیستم‌های اطلاعاتی	کلیه فرایندهای توسعه سیستم‌های اطلاعاتی برون‌سپاری شده و داخلی
سامانه/نرم‌افزار	سرورهای مجازی	VMware
	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 برنامه‌های خاص منظوره کسب‌وکار شرکت
	پایگاه‌های داده	Oracle, MS SQL, MySQL
	سیستم‌های‌عامل و میان‌افزارها	لینوکس و ویندوز

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

ابعاد امنیتی

ابعاد انتخاب شده به عنوان مبنای الگوی MARISMA-BP بر اساس نتایج تجزیه‌وتحلیل 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 (سالنیتری 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[1])	توانایی یک سیستم برای مسئول دانستن کاربران برای اعمالشان (مانند سوء استفاده از اطلاعات).
قابلیت ممیزی (AD)[2]	توانایی یک سیستم برای نظارت دائمی و غیرقابل عبور از تمام اقدامات انجام شده توسط انسان یا ماشین در مدل فرآیند کسب‌وکار.
اصالت (AT[3])	توانایی یک سیستم برای تأیید هویت در اطلاعاتی که ارائه می‌دهد.
دسترس‌پذیری[4](AV)	یک سیستم باید اطمینان حاصل کند که تمام اجزای مدل زمانی که توسط کاربران مجاز مورد نیاز است در دسترس و عملیاتی هستند.
محرمانگی[5](CO)	یک سیستم باید اطمینان حاصل کند که فقط کاربران مجاز به اطلاعات و فرآیندها دسترسی دارند.
یکپارچگی[6](IN)	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[1](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[2](ND)	توانایی سیستم برای نیاز به این که مجموعه ای از اقدامات فقط توسط کاربران اختصاص داده شده اجرا شود.
تفکیک وظایف[3](SD)	توانایی سیستم برای وادار کردن دو یا چند فرد مختلف برای انجام یک کار یا مجموعه ای از وظایف مرتبط.
تعهد به فرایند[4](BD)	توانایی فرآیند کسب‌وکار برای الزام همان فرد به مسئولیت تکمیل مجموعه ای از وظایف مرتبط.
تاب‌آوری[5](RE)	توانایی پیش‌بینی، مقاومت، بازیابی و انطباق با شرایط نامطلوب، استرس‌ها، حملات یا سازش‌های سیستمی که از منابع سایبری استفاده می‌کنند یا توسط آنها فعال می‌شوند.

در این مدل ما مبحث «تاب آوری» را نیز به الگوی خود اضافه کردیم، زیرا جهت تداوم فرآیندهای کسب‌وکار باید سازمان توانایی مدیریت رخدادهای امنیت اطلاعات را داشته باشد و جهت کاهش این رخدادهایی که ممکن است مستقیم کسب‌وکار 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 تجزیه‌وتحلیل و مطالعه طبقه‌بندی امنیت عملیاتی تعریف شده است مخاطرات (سبولا و همکاران، ۲۰۱۴) که سعی در شناسایی و سازماندهی منابع عملیاتی دارد مخاطرات امنیتی، همانطور که در طبقه‌بندی تهدیدات ENISAرخ می‌دهد (مارینوس و همکاران، ۲۰۱۶). درواقع مجموعه ای از انواع تهدیدها در نظر گرفته شده که سعی شده است تهدیدهایی که مرتبط با مدل‌های فرایند کسب‌وکار است استفاده شود. نزدیک ترین آنها هستند مربوط به مدل‌های فرآیند کسب‌وکار شرح انواع تهدید در جدول ۴ نشان داده شده است.

جدول ٤: 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.
فرایند	انواع تهدیدات مرتبط با شکست‌های مشکل ساز فرآیندهای داخلی برای انجام آن گونه که مورد نیاز یا مورد انتظار است. زیرگروه‌های پشتیبانی کننده آن شامل طراحی یا اجرای فرآیند، کنترل‌های فرآیند و فرآیندهای پشتیبانی می‌شود.
بیرونی	حقوقی: انواع تهدیدها با مخاطراتی سروکار دارند که به دلیل رعایت مقررات، قوانین و دعوای حقوقی عناصر، ممکن است بر سازمان تأثیر بگذارند. 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). کسب وکار: انواع تهدیدات مربوط به عوامل شکست تامین کننده، شرایط بازار و شرایط اقتصادی. با مخاطرات های عملیاتی ناشی از تغییرات در محیط کسب وکار سازمان سر و کار دارد. خدمات: با مخاطرات ناشی از وابستگی سازمان با طرف های خارجی برای ادامه عملیات (ثبت‌احوال، خدمات اضطراری، شاپرک، اداره برق و غیره) سروکار دارد.

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 تجزیه‌وتحلیل مخاطرات و یک متخصص فرآیند کسب‌وکار) به طور رضایت بخشی تکمیل شده است.

جدول۵: ابعاد و انواع دارایی‌های BPMN

ابعاد

انواع دارایی‌ها	مسئولیت پذیری	قابلیت ممیزی	اصالت	دسترس‌پذیری	محرمانگی	یکپارچگی	عدم انکار	عدم تفویض اختیار	تفکیک وظایف	تعهد به فرایند	تاب‌آوری
اسناد و سوابق سازمانی	X	X		X	X	X	X	X	X	X	
شبکه و تجهیزات مرتبط				X							X
سخت‌افزارها											X
منابع انسانی	X						X	X	X	X	
دارایی‌های زیرساختی											
فرایند	X	X	X	X	X	X	X	X	X	X	X
سامانه/نرم‌افزار											X

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

۱. مسئولیت‌پذیری یکی از اصول مهم در مدیریت اسناد و سوابق سازمانی است که اطمینان می‌دهد هر فعالیت، تصمیم و اقدام در سازمان به درستی ثبت شده و افرادی که مسئول آن‌ها هستند به درستی شناسایی شده‌اند. این اصل کمک می‌کند تا شفافیت و اعتماد در سازمان حفظ شود و اقدامات انجام شده به راحتی قابل پیگیری باشد. با پیاده‌سازی این راهکارها، سازمان‌ها می‌توانند اطمینان حاصل کنند که مسئولیت‌پذیری به‌درستی در تمامی فعالیت‌ها و فرآیندها به اجرا درآمده و سوابق سازمانی به‌طور کامل و دقیق ثبت شده است. جنبه‌های مسئولیت‌پذیری شامل و موارد زیر است:
   - تعیین وظایف و واگذاری مسئولیت‌ها
   - 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 به‌طور 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 کنترل‌شده 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 محدودکننده

- کاهش انگیزه کارکنان
- کندی در فرآیند تصمیم‌گیری
- 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 سازمان‌هایی که با داده‌ها و اطلاعات حساس کار می‌کنند، اهمیت بسیاری دارد. حفظ محرمانگی در اسناد و سوابق سازمانی نیازمند توجه مستمر و پیاده‌سازی سیاست‌ها و روش‌های 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 می‌کند. این امر در سازمان‌ها از اهمیت بالایی برخوردار است، زیرا اطلاعات نادرست یا ناقص می‌تواند منجر به تصمیمات نادرست و مشکلات جدی شود. یکپارچگی اسناد و سوابق به سازمان‌ها کمک می‌کند تا اطلاعات دقیق و قابل اعتمادی داشته باشند که می‌توانند بر اساس آن تصمیمات استراتژیک و عملیاتی خود را اتخاذ کنند.

۷. دسترس‌پذیری در اسناد و مدارک سازمانی به معنای اطمینان از این است که اطلاعات و داده‌ها برای کاربران مجاز به موقع و به صورت مطمئن در دسترس باشند .این امر در مدیریت اطلاعات سازمانی بسیار حیاتی است زیرا دسترس‌پذیری ناکافی می‌تواند منجر به اختلال در عملیات، کاهش بهره‌وری و حتی از دست رفتن فرصت‌های کسب‌وکار شود. اطمینان از دسترس‌پذیری اطلاعات می‌تواند بهره‌وری سازمان را افزایش داده و از تلفات داده‌ها جلوگیری کند.

۸. تعهد به فرآیند در اسناد و مدارک سازمانی به معنای پایبندی به رویه‌ها و استانداردهای تعیین‌شده برای مدیریت، نگهداری و به‌روزرسانی 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 کنترل های امنیتی نشان داده شده در جدول۶، ما یک سری نگاشت بین عناصر بر اساس طبقه بندی های مختلف انجام داده ایم. اول، ما تهدیدات (تعریف شده در طبقه بندی SEI و ENISA) را با کنترل های تعریف شده توسط NIST 80053 ترسیم کرده ایم، که نشان می دهد کدام کنترل ها می توانند تهدیدات را کاهش دهند (براساس یادداشت فنی CMU/SEI-2014-TN006)، و دوم، ما کنترل های ISO27002:2022 را با کنترل های NIST برای مدل خود نگاشت کرده‌ایم.

مجموعه‌ای از کنترل‌های امنیتی که امکان تهدیدات احتمالی را فراهم می‌کند و حمله به سیستمی که باید با آن مواجه شود ازاستاندارد 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 کنترل ها در مقابل نوع تهدیدات برای الگوی MARISMA-BP

کنترل‌ها	انواع تهدیدها		
	اقدام‌های انسانی	فرآیندهای داخلی ناموفق	رویدادهای بیرونی

		غیر عمدی	عمدی	بدون عمل	طراحی فرآیند	کنترل‌های فرآیند	پشتیبانی	مخاطرات	مسائل حقوقی	کسب‌وکار	خدمات مشاوره
سیاست‌های امنیت اطلاعات	1.5	X		X	X	X	X	X	X	X	X
نقش‌ها و مسئولیت های امنیت اطلاعات	2.5	X			X	X	X				X
تفکیک وظایف	3.5	X			X	X					
مسئولیت های مدیریت	4.5	X		X	X	X					
تماس با نهادهای بالادستی	5.5	X		X	X				X		
تماس با گروه های ذینفع خاص	6.5	X			X				X		
هوش تهدید	7.5	X		X							
امنیت اطلاعات در مدیریت پروژه	8.5				X		X		X	X	X
موجودی اطلاعات و سایر دارایی‌های مرتبط	9.5				X				X		
استفاده قابل قبول از اطلاعات و سایر دارایی‌های مرتبط	10.5								X		
بازگشت دارایی‌ها	11.5				X				X		
طبقه‌بندی اطلاعات	12.5				X		X		X	X	
برچسب گذاری اطلاعات	13.5	X	X		X				X		
انتقال اطلاعات	14.5	X	X		X		X	X	X	X	X
کنترل دسترسی	15.5										
مدیریت هویت	16.5	X	X						X	X	
اطلاعات احراز هویت	17.5	X	X								
حقوق دسترسی	18.5	X	X								
امنیت اطلاعات در روابط	19.5						X		X	X	X

ترل‌ها		انواع تهدیدها									
		اقدام‌های انسانی				فرآیندهای داخلی ناموفق			رویدادهای بیرونی		
		غیر عمدی	عمدی	بدون عمل	طراحی فرآیند	کنترل‌های فرآیند	پشتیبانی	مخاطرات	مسائل حقوقی	کسب‌وکار	خدمات مس ائل
تامین کننده											
رداختن به امنیت اطلاعات در قراردادهای تامین کننده	20.5						X				X
دیریت امنیت اطلاعات در زنجیره تامین ICT	21.5						X				X
ظارت، بررسی و مدیریت تغییر خدمات تامین کننده	22.5						X	X	X		
نیت اطلاعات برای استفاده از خدمات ابری	23.5		X		X			X	X	X	X
رنامه ریزی و آماده سازی مدیریت حوادث امنیت اطلاعات	24.5	X	X	X	X						
رزیابی و تصمیم گیری در مورد رویدادهای امنیت اطلاعات	25.5	X	X	X	X	X					
اسخ به حوادث امنیت اطلاعات	26.5	X	X	X							
ادگیری از حوادث امنیت اطلاعات	27.5	X	X	X							
جموعه شواهد	28.5										
نیت اطلاعات در هنگام	29.5	X	X	X							

کنترل‌ها		انواع تهدیدها										
		اقدام‌های انسانی		فرآیندهای داخلی ناموفق				رویدادهای بیرونی				
		غیر عمدی	عمدی	بدون عمل	طراحی فرآیند	کنترل‌های فرآیند	پشتیبانی	مخاطرات	مسائل حقوقی	کسب‌وکار	مسائل	خدمات
اختلال												
سادگی ICT برای تداوم کسب‌وکار	30.5											
شناسایی الزامات قانونی، قانونی، مقرراتی و قراردادی	31.5	X	X	X	X	X	X	X	X	X	X	
حقوق مالکیت معنوی	32.5	X	X		X			X				
حفاظت از سوابق	33.5	X	X		X	X		X				X
حریم خصوصی و حفاظت از PII	34.5	X	X	X				X				
بررسی مستقل امنیت اطلاعات	35.5					X	X	X				X
رعایت سیاست ها و استانداردهای امنیت اطلاعات	36.5	X	X	X	X	X	X	X	X	X	X	X
رویه های عملیاتی مستند	37.5	X	X	X	X			X	X	X	X	X
دربالگری	1.6	X	X	X			X	X				
شرایط و ضوابط استخدام	2.6	X	X	X			X	X				
آگاهی، آموزش و آموزش امنیت اطلاعات	3.6			X			X	X				
فرآیند انضباطی	4.6	X	X	X				X				
مسئولیت های پس از خاتمه یا تغییر شغل	5.6	X	X					X				

کنترل‌ها		انواع تهدیدها									
		اقدام‌های انسانی		فرآیندهای داخلی ناموفق				رویدادهای بیرونی			
		غیر عمدی	عمدی	بدون عمل	طراحی فرآیند	کنترل‌های فرآیند	پشتیبانی	مخاطرات	مسائل حقوقی	کسب‌وکار	خدمات
رادادهای محرمانه یا عدم افشا	6.6	X					X	X			
س از راه دور	7.6	X	X	X	X	X	X			X	
زارش رویداد امنیت اطلاعات	8.6		X		X	X		X			

ماتریس-T دارایی-T/تهدید/ابعاد

فراالگوی (متا الگو) شامل یک رابطه س تعریف شده است (به کادر متاالگوی 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 کنترل هایی که آنها را کاهش می دهند)، توانستیم جدول ۷ را تکمیل کنیم.

جدول ۷ این رابطه پیچیده تجزیه‌وتحلیل 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.

جدول۷-ماتریس تهدید-دارایی-ابعاد (ATD)[1] برای الگوی MARISMA-BP.

انواع تهدید		انواع دارایی																			
		اسناد و سوابق سازمانی		شبکه و تجهیزات مرتبط		سخت‌افزارها				منابع انسانی		دارایی‌های زیرساختی						فرایند			سامانه/ نرم‌افزار
		سند کاغذی	سند الکترونیکی	سرو سرهای پایه شبکه	تجهیزات اکتیو شبکه	میزبان‌ها و سرورها	تجهیزات دسترسی به اطلاعات	تجهیزات اداری (بدون مراقبت)	ذخیره‌سازها	کارکنان سازمان	سایرکاران	تجهیزات تأمین برق	لینک‌های سرویس دهنده و ارتباطی	تجهیزات تهویه مطبوع	تجهیزات اعلان و اطفای حریق	تجهیزات کنترل دسترسی	فرایند مدیریت پروژه	فرایند توسعه سیستم‌های اطلاعاتی	سرورهای مجازی	سامانه‌های کاربردی	بانگاه‌های داده	سیستم‌های عامل و میان‌افزارها
زیر تهدید		NRACAD	NRACAD	NRADAV	ADCOINAV	NRADAV	NRADAV	NRADAV	NRADAV	All	All	ADAV	ADAV	ADAV	ADAV	NRAD	ADATCOINAV	ADATCOINAV	ADAV	ADAV	ADAV	ADAV
عمدی		AVCOINADAT	AVCOINADAT	AVCOINADAT	NRAD	NRAD	NRAD	NRAD	NRAD	All	All	ADAV	ADAV	ADAV	ADAV	AVCOINADAT	AVCOINADAT	AVCOINADAT	AVCOINADAT	AVCOINADAT	AVCOINADAT	AVCOINADAT
اقدامات افراد		AVCOINADAT	AVCOINADAT	NRAD	NRAD	NRAD	NRAD	NRAD	NRAD	All	All	ADAV	ADAV	ADAV	ADAV	AVCOINADAT	AVCOINADAT	AVCOINADAT	AVCOINADAT	AVCOINADAT	AVCOINADAT	AVCOINADAT

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

فرایندهای داخلی ناموفق	طراحی فرایند	کنترل‌های فرایند	فرایندهای پشتیبانی	مخاطرات
رویدادهای بیرونی	All	All	AVCOINADAT	AVCOINADAT
	NRAD	All	AVCOINADAT	AVCOINADAT
	NRAD	All	AVCOINADAT	AVCOINADAT
	NRAD	All	AVCOINADAT	AVCOINADAT
	NRAD	All	AVCOINADAT	AVCOINADAT
	NRAD	All	AVCOINADAT	AVCOINADAT
	NRAD	All	AVCOINADAT	AVCOINADAT
	ADAV	All	ADAVRE	ADAV
	ADAV	All	ADAVRE	ADAV
	ADAV	All	ADAVRE	ADAV
	ADAV	All	ADAVRE	ADAV
	All	All	AVCOINADAT	AVCOINADAT
	All	All	AVCOINADAT	AVCOINADAT
	NRAD	All	AVCOINADAT	AVCOINADAT
	NRAD	All	AVCOINADAT	AVCOINADAT
	NRAD	All	AVCOINADAT	AVCOINADAT
	NRAD	All	AVCOINADAT	AVCOINADAT
	NRAD	All	AVCOINADAT	AVCOINADAT
	AVCOINADAT	All	AVCOINADAT	AVCOINADAT
	AVCOINADAT	All	AVCOINADAT	AVCOINADAT
	AVCOINADAT	All	AVCOINADAT	AVCOINADAT
	AVCOINADAT	All	AVCOINADAT	AVCOINADAT
	AVCOINADAT	All	AVCOINADAT	AVCOINADAT
	AVCOINADAT	All	AVCOINADAT	AVCOINADAT
	AVCOINADAT	All	AVCOINADAT	AVCOINADAT
	AVCOINADAT	All	AVCOINADAT	AVCOINADAT
	AVCOINADAT	All	AVCOINADAT	AVCOINADAT
	AVCOINADAT	All	AVCOINADAT	AVCOINADAT
	AVCOINADAT	All	AVCOINADAT	AVCOINADAT
	AVCOINADAT	All	AVCOINADAT	AVCOINADAT

راهنمای جداول	ابعاد	مسائل حقوقی	مسائل کسب و کار	وابستگی به خدمات
		AVCOINADAT	All	AVCOINADAT
		AVCOINADAT	All	AVCOINADAT
		AVCOINADAT	All	AVCOINADAT
		AVCOINADAT	All	AVCOINADAT
		AVCOINADAT	All	AVCOINADAT
		AVCOINADAT	All	AVCOINADAT
		AVCOINADAT	All	AVCOINADAT
		AVCOINADAT	All	AVCOINADAT
		AVCOINADAT	All	AVCOINADAT
		ADAV	ADAV	ADAV
		ADAV	ADAV	ADAV
		ADAV	ADAV	ADAV
		ADAV	ADAV	ADAV
		ADAV	ADAV	ADAV
		All	All	All
		All	All	All
		AVCOINADAT	AVCOINADAT	AVCOINADAT
		AVCOINADAT	AVCOINADAT	AVCOINADAT
		AVCOINADAT	AVCOINADAT	AVCOINADAT
		AVCOINADAT	AVCOINADAT	AVCOINADAT
		AVCOINADAT	AVCOINADAT	AVCOINADAT
		AVCOINADAT	AVCOINADAT	AVCOINADAT
		AVCOINADAT	AVCOINADAT	AVCOINADAT
		AVCOINADAT	AVCOINADAT	AVCOINADAT
		AVCOINADAT	AVCOINADAT	AVCOINADAT

ابعاد	
AC: مسئولیت‌پذیری	NR: عدم انکار
IN : یکپارچگی	ND: عدم تفویض اختیار
CO : محرمانگی	BD: تعهد به فرایند
AV : دسترس‌پذیری	RE: تاب‌آوری
AT : اعتبار	SD: جدایی وظیفه
	AD: قابلیت ممیزی

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 کسب‌وکاری 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 برروی یکدیگر تأثیر می‌گذارد. به عنوان مثال یک سرور فیزیکی دارای سیستم عامل است و برروی آن برنامه‌کاربردی نصب شده و کارمندان (حتی پیمانکاران) می‌توانند به آن در سطوح مختلف دسترسی داشته باشند. درصورتی‌که کارمندی چه به صورت عمدی/غیرعمدی اختلالی در سرور فیزیکی بوجود آورد که سبب عدم دسترس‌پذیری به آن شود، می‌تواند کل دارایی‌های اطلاعاتی وابسته را با اختلال عدم دسترس‌پذیری مواجه کند.

در فرایند مدیریت مخاطرات باید وابستگی بین انواع دارایی‌های اطلاعاتی، انواع تهدیدها و ابعاد امنیت اطلاعات درنظر 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 مطرح‌شده 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 فرآیندهای 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 پرسشنامه‌ها تأیید کرد که کنترل‌های پیشنهادی چارچوب، انطباق با استاندارد ISO/IEC 27005 را تسهیل می‌کند.

سوال تحقیق ۲: مؤلفه‌های کلیدی چارچوب MARISMA-BP برای کاهش مخاطرات در طراحی فرآیندهای بانکی کدامند؟

فرایند پاسخ به سوال ۲ و یافته‌ها:

- فراالگوی ATD (دارایی-تهدید-بُعد) به عنوان هسته اصلی چارچوب شناسایی شد.
- ۸۵٪ پاسخ‌دهندگان 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 یافته‌ها:

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، دسترس‌پذیری) و روابط آنها با دارایی‌ها و تهدیدها.
- تأیید روابط ماتریس‌ها و اولویت‌بندی کنترل‌های امنیتی بر اساس تجربیات عملی.
- پیشنهاد بهبودها برای افزایش تاب‌آوری 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، نه‌تنها از جریمه‌های 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 ISO 27001، NIST CSF) 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 بانک‌ها از چارچوب‌های ناهمگون و پراکنده استفاده می‌کنند که انطباق کافی با الزامات نظارتی داخلی ندارند. الگوی حاضر با تلفیق استانداردهای بین‌المللی و مقررات بومی، این خلأ را مرتفع می‌سازد.

۲ مزایای رقابتی نسبت به سایر الگوهای متداول

- کاهش هزینه‌های انطباق: از طریق مکانیزه‌سازی فرآیندهای نظارت بر مخاطرات و گزارش‌دهی به مراجع ناظر.
- جلب اعتماد ذی‌نفعان: با افزایش شفافیت در فرآیندهای امنیتی و ارتقای کارایی در صیانت از داده‌های حساس.

پیشنهادها

با استناد به یافته‌های این مطالعه، پیاده‌سازی الگوی ارائه‌شده می‌تواند به بانک‌ها و مؤسسات مالی کمک کند تا ضمن ارتقا امنیت اطلاعات و هماهنگی با فرایندهای کسب‌وکار، مزیت رقابتی قابل‌توجهی در مقایسه با سایر نهادهای هم‌صنف خود ایجاد نمایند. موارد زیر حاصل استخراج نتایج الگوی ارائه شده و پیشنهاد برای بانک‌ها و مؤسسات اعتباری می‌باشد:

۱ استقرار چارچوب‌های پویا

- ایجاد واحدهای ارزیابی مستمر امنیتی برای نظارت بر تهدیدات نوظهور.
- استفاده از تست‌های نفوذ و شبیه‌سازی حملات به‌صورت دوره‌ای.

۲ آموزش و فرهنگ‌سازی

- توسعه برنامه‌های آموزشی اختصاصی برای کارکنان در سطوح مختلف (از مدیران ارشد تا اپراتورها).
- برگزاری کارگاه‌های آگاهی‌بخشی درباره فیشینگ، مهندسی اجتماعی و حفاظت از داده‌ها.

۳ همکاری صنعتی و فناوری:

- مشارکت در پلتفرم‌های اشتراک اطلاعات تهدیدات سایبری (مانند CERTهای 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 businessprocess- - 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 (Ljubl) 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 andTechnology; 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, Wierzchoń 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.
- 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.
- 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.
- 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.
- 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 – Aframework 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.
- 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.
- 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.
- 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/COVER, URL https://link.springer.com/chapter/10.1007/978- 3-319-10557-4_39