مدیریت مخاطرات در تولید و توسعه پروژه‌های نرم‌افزاری

علی کریمی
استادیار دانشگاه جامع امام حسین (ع)
فرهاد کریمی
دانشجوی دکتری دانشگاه جامع امام حسین (ع)
علی طلوعی‌فر
دانشجوی دکتری دانشگاه جامع امام حسین (ع)
محمد آل ابریشم‌کار
دانشجوی کارشناسی ارشد دانشگاه جامع امام حسین (ع)

چکیده

در دنیای امروز، پروژه‌های نرم‌افزاری به‌طور فزاینده‌ای پیچیده‌تر شده و عوامل مخاطره‌آمیز در این پروژه‌ها افزایش یافته است. این پیچیدگی‌ها ناشی از عوامل مختلفی از جمله تغییرات سریع فناوری، نیازهای متغیر مشتریان و فشارهای رقابتی است. به همین دلیل، مدیریت مؤثر مخاطرات نقش حیاتی در موفقیت پروژه‌های نرم‌افزاری ایفا می‌کند. مدیریت مخاطرات به‌عنوان یک فرآیند نظام‌مند و ساختاریافته، به شناسایی، ارزیابی و کنترل مخاطرات و عدم‌قطعیت‌های مرتبط با پروژه‌های نرم‌افزاری می‌پردازد. این فرآیند به مدیران پروژه‌ها کمک می‌کند تا با شناسایی زودهنگام مخاطرات، برنامه‌ریزی‌های لازم برای جلوگیری از بروز مشکلات جدی را انجام دهند. عدم توجه به مخاطرات می‌تواند منجر به تأخیر در تحویل، افزایش هزینه‌ها و در نهایت شکست پروژه شود. با بهره‌گیری از فناوری‌ها، استانداردها و تجربیات در حال توسعه، می‌توان فرآیندهای مدیریت مخاطرات را به‌طور مداوم بهبود بخشید. این بهبود مستمر نه‌تنها به کاهش مخاطرات کمک می‌کند، بلکه می‌تواند به بهینه‌سازی منابع و زمان نیز منجر شود. در این راستا، استفاده از فنون و ابزارهای نرم‌افزاری نوین می‌تواند به شفاف‌سازی و تسهیل فرآیند مدیریت مخاطرات کمک نماید. در این مقاله، ضمن بررسی دقیق‌تر و تحلیل عمیق‌تر این مباحث، به بررسی مفهوم و فنون مدیریت مخاطرات، انواع مخاطرات و مراحل مدیریت مخاطرات خواهیم پرداخت.

واژه‌های کلیدی: پروژه نرم‌افزاری، مدیریت مخاطرات، شناسایی و ارزیابی مخاطرات، چالش‌های توسعه نرم‌افزار، بهینه‌سازی منابع و زمان.

۱- مقدمه

در پروژه‌های نرم‌افزاری، مخاطرات[۱] می‌توانند ناشی از عوامل مختلفی مانند تغییرات در نیازمندی‌ها، مشکلات فنی، کمبود منابع انسانی و تأخیر در زمان‌بندی پروژه باشند. مدیریت مخاطرات به فرآیند شناسایی، ارزیابی و اولویت‌بندی مخاطرات به همراه اقدامات مؤثر برای کاهش یا کنترل احتمال و تأثیر آن‌ها اشاره دارد. فرآیند مدیریت مخاطره شامل اِعمال نظام‌مند[۲] خط‌مشی‌ها، رویه‌ها و شیوه‌ها برای فعالیت‌های برقراری ارتباط و مشاوره، ایجاد زمینه و ارزیابی، درمان، نظارت، بررسی، ثبت و گزارش مخاطره است و باید جزء لاینفک مدیریت و تصمیم‌گیری باشد و در ساختار، عملیات و فرآیندهای سازمان ادغام شود (Sravan et al., ۲۰۲۳).

می‌توان آن را در سطوح راهبردی، عملیاتی، برنامه‌ریزی یا پروژه به‌کار برد. کاربردهای زیادی از فرآیند مدیریت مخاطره در یک سازمان وجود دارد که برای دستیابی به اهداف و متناسب با زمینه خارجی و داخلی که در آن اعمال می‌شوند، سفارشی شده است. ماهیت پویا و متغیر رفتار و فرهنگ انسانی باید در طول فرآیند مدیریت مخاطره در نظر گرفته شود. اگرچه فرآیند مدیریت مخاطره اغلب به‌صورت متوالی ارائه می‌شود، اما در عمل تکراری است (Sarigiannidis & Chatzoglou, ۲۰۱۱).

۲- انواع مخاطرات در پروژه‌های نرم‌افزاری

در متون مختلف، به چندین فهرست از مخاطرات بالقوه توسعه نرم‌افزار (نشانگرهای مخاطره نرم‌افزار[۳]) اشاره شده است. نشانگرهای مخاطره نرم‌افزار، به مدیران پروژه‌ها در شناسایی، ارزیابی و مدیریت مخاطرات بالقوه در پروژه‌های نرم‌افزاری کمک می‌کنند. این نشانگرها می‌توانند شامل؛ نشانگرهای مربوط به زمانبندی، هزینه، کیفیت، مخاطرات فنی و یا مربوط به مخاطرات سازمانی باشند. استفاده از نشانگرهای مخاطره نرم‌افزار، دارای مزایای زیادی است که از جمله می‌توان به بهبود تصمیم‌گیری، کاهش مخاطره، بهبود کیفیت و افزایش موفقیت پروژه اشاره نمود. روپونن و لیتینن[۴] در سال ۲۰۰۰، مخاطرات نرم‌افزار را به شش دسته زیر طبقه‌بندی کرده‌اند:

۱) مخاطرات زمان‌بندی و برنامه‌ریزی
۲) مخاطرات وظیفه‌مندی سیستم
۳) مخاطرات برون‌سپاری (پیمانکاران فرعی)
۴) مخاطرات مدیریت نیازمندی‌ها
۵) مخاطرات استفاده از منابع و کارایی
۶) مخاطرات مدیریت کارکنان

بوهم و راس[۵] در سال ۱۹۸۹ فهرستی از ۱۰ مورد اصلی مخاطرات نرم‌افزار را پیشنهاد کرده‌اند. جدول ۱ نشان می‌دهد که چگونه این فهرست را می‌توان با شش دسته‌بندی پیشنهادی روپونن و لیتینن (۲۰۰۰) ادغام نمود.

متدولوژی‌های شناسایی مخاطرات نرم‌افزار توسط بوهم (۱۹۹۱)، کیل[۶] و همکاران (۱۹۹۸)، روپونن و لیتینن (۲۰۰۰)، بارکی[۷] و همکاران (۱۹۹۳) و IEEE (۲۰۰۱) ارائه شده است. یکی از مؤثرترین ابزارها برای شناسایی و ارزیابی مخاطرات نرم‌افزار،

---

۱ Risks
۲ Systematic
۳ Software Risk Indicators (SRIs)
۴ Ropponen and Lyytinen
۵ Boehm and Ross
۶ Keil
۷ Barki

فهرست‌های بررسی (چک‌لیست[1]) تخصصی است که توسط چندین نویسنده نیز به آن‌ها اشاره شده است. کارولاک[2] (۱۹۹۶) و جونز[3] (۱۹۹۴) دامنه مخاطرات نرم‌افزار را برای دخیل کردن مخاطرات راهبردی، از قبیل مخاطرات بازاریابی و مخاطرات مالی گسترش داده‌اند (Galin, ۲۰۱۶).

جدول ۱ – ده مخاطره مهم نرم‌افزار (Galin, ۲۰۱۶)

شماره	دسته‌بندی مخاطرات نرم‌افزار (روپونن و لیتینن)	شماره	دسته‌بندی مخاطرات نرم‌افزار (بوهم و راس)	توضیحات
۱	مخاطرات مدیریت کارکنان	۱	کمبود نیروی انسانی	کمبود و جابه‌جایی کارکنان کیفی
۲	زمان‌بندی و برنامه‌ریزی	۲	بودجه و برنامه‌های زمانی غیرواقعی	تخمین اشتباه (خیلی کم) زمان و بودجه توسعه نرم‌افزار
۳	وظیفه‌مندی سیستم	۳	توسعه اشتباه وظایف نرم‌افزار	توسعه وظایف نرم‌افزار که غیرضروری یا اشتباه تعریف شده‌اند.
		۴	توسعه اشتباه رابط کاربری	رابط کاربری نامناسب یا دشوار
۴	مدیریت نیازمندی‌ها	۵	روکش طلایی	اضافه کردن ویژگی‌های غیرضروری («سوت و زنگوله‌ها») به دلیل علائق حرفه‌ای، غرور یا درخواست‌های کاربر
		۶	جریان مستمر تغییرات نیازمندی‌ها	تغییرات غیرقابل کنترل و غیرقابل پیش‌بینی در وظایف و ویژگی‌های سیستم
۵	پیمانکاران فرعی	۷	ضعف در مؤلفه‌های تأمین‌شده از بیرون	پایین بودن کیفیت مؤلفه‌های برون‌سپاری‌شده سیستم
		۸	ضعف در انجام وظایف برون‌سپاری‌شده	کیفیت پایین یا عدم قطعیت در انجام وظایف برون‌سپاری‌شده
۶	مصرف منابع و کارایی	۹	ضعف‌های کارایی بلادرنگ	کارایی ضعیف سیستم
		۱۰	فراتر رفتن از توانایی‌های علم کامپیوتر	عدم امکان پیاده‌سازی سیستم به دلیل نبود راه‌حل‌های فنی و/یا توان محاسباتی کافی

۳- مراحل مدیریت مخاطرات

این مراحل در شکل ۱ نشان داده شده است. در ادامه، هر یک از مراحل به‌صورت تفصیلی، مورد بررسی قرار خواهد گرفت.

۳-۱- ارتباطات و مشاوره

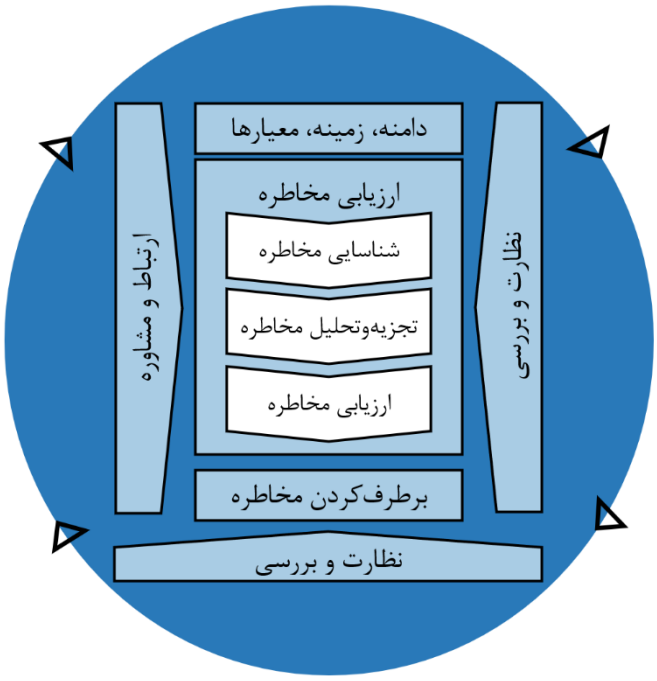
هدف از ارتباطات و مشاوره کمک به ذینفعان مربوطه در درک مخاطرات است، مبنایی که بر اساس آن تصمیم‌گیری می‌شود و دلایلی که چرا اقدامات خاص موردنیاز است. ارتباطات با هدف ارتقای آگاهی و درک مخاطرات انجام می‌شود، در حالی که مشاوره شامل دریافت بازخورد و اطلاعات برای پشتیبانی از تصمیم‌گیری است.

هماهنگی نزدیک بین این دو باید تبادل اطلاعات واقعی، به‌موقع، مرتبط، دقیق و قابل‌فهم را تسهیل کند و در عین حال، محرمانه‌بودن، یکپارچگی اطلاعات و حقوق حریم خصوصی افراد را نیز مدنظر قرار دهد. ارتباطات و مشاوره با ذینفعان داخلی و خارجی مناسب، باید در تمام مراحل فرآیند مدیریت مخاطرات صورت گیرد (Mohamud Sharif & Basri, ۲۰۱۱).

۳-۱-۱- ارتباطات و مشاوره هدفمند

– برای هر مرحله از فرآیند مدیریت مخاطره، زمینه‌های مختلف تخصصی را گرد هم بیاورید؛

– اطمینان حاصل کنید که دیدگاه‌های مختلف در هنگام تعریف معیارهای مخاطرات و هنگام ارزیابی مخاطرات به‌درستی در نظر گرفته می‌شوند؛
– ارائه اطلاعات کافی برای تسهیل نظارت بر مخاطرات و تصمیم گیری؛
– ایجاد حس فراگیری و مالکیت در میان افرادی که تحت تأثیر مخاطرات قرار دارند.



شکل ۱: مراحل مدیریت مخاطرات (Hutchins, ۲۰۱۸)

۳-۲- دامنه، زمینه و معیارها

هدف از ایجاد دامنه، زمینه و معیارها، سفارشی‌کردن فرآیند مدیریت مخاطرات، ارزیابی موثر و درمان مناسب مخاطرات است. دامنه، زمینه و معیارها شامل تعریف دامنه فرآیند و درک زمینه‌های بیرونی و درونی مخاطرات است.

۳-۲-۱- تعریف دامنه

سازمان باید دامنه و محدوده فعالیت‌های مدیریت مخاطرات خود را مشخص کند. از آنجایی که فرآیند مدیریت مخاطرات ممکن است در سطوح مختلف (مانند فعالیت‌های راهبردی، عملیاتی، برنامه‌ریزی، پروژه یا سایر فعالیت‌ها) به‌کار گرفته شود، مهم است که دامنه مورد نظر، اهداف مربوطه و همسویی آنها با اهداف سازمانی مشخص گردد (Arıkan & Yürekten, ۲۰۲۰).

هنگام برنامه‌ریزی رویکرد، ملاحظات زیر باید مورد توجه قرار گیرد:

– اهداف و تصمیماتی که باید اتخاذ شوند؛
– نتایج مورد انتظار از مراحلی که در فرآیند برداشت می‌شود؛
– زمان، مکان، انضمام‌ها و موارد استثنایی خاص؛
– ابزارها و فنون مناسب ارزیابی مخاطره؛

---

۱ Checklists
۲ Karolak
۳ Jones

– منابع مورد نیاز، مسئولیت‌ها و سوابق باید نگهداری شود؛

– روابط با سایر پروژه‌ها، فرآیندها و فعالیت‌ها مشخص شود.

۳-۲-۲- زمینه بیرونی و داخلی

زمینه بیرونی و درونی، محیطی است که سازمان به‌دنبال تعریف و دستیابی به اهداف خود است. زمینه فرآیند مدیریت مخاطرات باید از درک محیط بیرونی و داخلی که سازمان در آن فعالیت می‌کند، ایجاد شود و باید محیط خاص فعالیتی را که فرآیند مدیریت مخاطرات در آن اعمال می‌شود، منعکس نماید.

درک زمینه و محیط سازمانی به دلایل زیر مهم است:

- مدیریت مخاطرات در چارچوب اهداف و فعالیت‌های سازمان صورت می‌گیرد.
- عوامل سازمانی می‌توانند منبع خطر باشند.
- هدف و دامنه فرآیند مدیریت مخاطرات ممکن است با اهداف کل سازمان مرتبط باشد.
- سازمان باید بستر بیرونی و درونی فرآیند مدیریت مخاطرات را با در نظر گرفتن عوامل ذکر شده ایجاد کند.

۳-۲-۳- تعریف معیارهای مخاطرات

سازمان باید میزان و نوع مخاطرات قابل پذیرش نسبت به اهداف خود را مشخص کند. همچنین، باید معیارهایی را برای ارزیابی اهمیت مخاطرات و حمایت از فرآیندهای تصمیم‌گیری، تعریف نماید. معیارهای مخاطرات باید با چارچوب مدیریت مخاطرات هم‌راستا و متناسب با هدف و دامنه فعالیت موردنظر سازمان تنظیم شوند. معیارهای مخاطرات باید ارزش‌ها، اهداف و منابع سازمان را منعکس کنند و با خط‌مشی‌ها و اظهارات مربوط به مدیریت مخاطرات سازگار باشند. معیارها باید با در نظر گرفتن تعهدات سازمان و نظرات ذینفعان تعریف شوند. این معیارها باید در ابتدای فرآیند ارزیابی مخاطرات ایجاد شوند، اما با توجه به پویا بودن آن‌ها، در صورت لزوم باید به‌طور مستمر بررسی و اصلاح شوند (Shehzad et al., ۲۰۲۲).

برای تعیین معیارهای مخاطرات، موارد زیر باید در نظر گرفته شود:

- ماهیت و نوع عدم قطعیت‌هایی که می‌تواند بر نتایج و اهداف (اعم از محسوس و ناملموس) تأثیر بگذارد؛
- چگونگی پیامدها (اعم از مثبت و منفی) و احتمال وقوع آن‌ها تعریف و اندازه‌گیری می‌شوند؛
- عوامل مرتبط با زمان؛
- سازگاری در استفاده از اندازه‌گیری‌ها؛
- نحوه تعیین سطح مخاطرات؛
- چگونگی ترکیب‌ها و توالی مخاطرات متعدد در نظر گرفته می‌شود؛
- ظرفیت سازمان.

۳-۳- شناسایی مخاطرات نرم‌افزاری

هدف از شناسایی مخاطرات؛ یافتن، شناسایی و توصیف خطراتی است که ممکن است به سازمان کمک کند یا از دستیابی به اهدافش جلوگیری نماید. اطلاعات مرتبط، مناسب و به‌روز در شناسایی مخاطرات مهم است. سازمان می‌تواند از طیف وسیعی از فنون برای شناسایی عدم قطعیت‌هایی که ممکن است بر یک یا چند هدف تأثیر بگذارد استفاده کند. ابزار اصلی برای شناسایی مخاطرات نرم‌افزاری، فهرست‌های بررسی (چک‌لیست‌ها) است که شرایط تیم، پروژه و مشتری را که احتمالاً منجر به مخاطرات

نرم‌افزاری می‌شود، مشخص می‌کند. سازمان باید قادر باشد خطرات را شناسایی کند، خواه منابع آنها تحت کنترل باشد یا نباشد. باید در نظر گرفت که ممکن است بیش از یک نوع نتیجه وجود داشته باشد که ممکن است پیامدهای ملموس یا نامشهود مختلفی را به دنبال داشته باشد و عوامل زیر و ارتباط بین این عوامل باید در نظر گرفته شود (Makajić-Nikolić, ۲۰۲۰):

- منابع خطر ملموس و نامشهود؛
- علل و حوادث؛
- تهدیدها و فرصت‌ها؛
- آسیب‌پذیری‌ها و قابلیت‌ها؛
- تغییرات در زمینه بیرونی و داخلی؛
- شاخص‌های خطرات نوظهور؛
- ماهیت و ارزش دارایی‌ها و منابع؛
- پیامدها و تأثیر آنها بر اهداف؛
- محدودیت‌های دانش و قابلیت اطمینان اطلاعات؛
- عوامل مرتبط با زمان؛
- تعصبات، مفروضات و باورهای افراد درگیر.

فهرست‌های بررسی از این نوع، توسط بوهم و راس (۱۹۸۹)، بوهم (۱۹۹۱)، بارکی و همکاران (۱۹۹۳) و روپونن و لیتینن (۲۰۰۰) پیشنهاد شده است. شناسایی مخاطرات نرم‌افزاری باید با شروع واقعی پروژه (مرحله پیش از پروژه) آغاز شده و در طول اجرای پروژه تا زمان تکمیل آن به‌صورت دوره‌ای تکرار شود (Galin, ۲۰۱٦).

۳-۴- تجزیه‌وتحلیل مخاطرات

هدف از تجزیه‌وتحلیل مخاطره؛ درک ماهیت و ویژگی‌های آن از جمله در صورت لزوم، سطح مخاطره است. تجزیه‌وتحلیل مخاطره شامل بررسی دقیق عدم قطعیت‌ها، منابع مخاطره، پیامدها، احتمال، رویدادها، سناریوها، کنترل‌ها و اثربخشی آنها است. یک رویداد می‌تواند علل و پیامدهای متعددی داشته باشد و می‌تواند اهداف متعددی را تحت تأثیر قرار دهد. تجزیه‌وتحلیل مخاطره را می‌توان با درجات مختلفی از جزئیات و پیچیدگی، بسته به هدف تجزیه‌وتحلیل، در دسترس بودن و قابلیت اطمینان اطلاعات و منابع موجود انجام داد. فنون تحلیل، بسته به شرایط و کاربرد موردنظر می‌تواند کیفی، کمی یا ترکیبی از این‌ها باشد (Dewi & Dharmawan, ۲۰۲٤). تجزیه‌وتحلیل مخاطره شامل عواملی به شرح زیر است:

- احتمال رویدادها و پیامدها؛
- ماهیت و بزرگی پیامدها؛
- پیچیدگی و اتصال؛
- عوامل مرتبط با زمان و نوسانات؛
- اثربخشی کنترل‌های موجود؛
- سطوح حساسیت و اعتماد به نفس.

تحلیل مخاطره ممکن است تحت تأثیر هر گونه اختلاف‌نظرها، سوگیری‌ها، ادراک از مخاطره و قضاوت‌ها قرار بگیرد. علاوه‌براین، عواملی مانند کیفیت اطلاعات استفاده‌شده، مفروضات و استثناهایی که در نظر گرفته شده‌اند، محدودیت‌های فنون و نحوه اجرای

آنها نیز تأثیرگذار هستند. این عوامل باید در نظر گرفته شده، مستند شوند و به تصمیم‌گیرندگان اطلاع داده شوند. تعیین کمیت برای رویدادهای بسیار نامطمئن ممکن است چالش‌برانگیز باشد؛ به‌ویژه هنگام تحلیل رویدادهایی که عواقب شدید دارند. در این‌گونه موارد، استفاده از ترکیب فنون مختلف معمولاً بینش بیشتری را فراهم می‌کند. تحلیل مخاطره به‌عنوان ورودی برای ارزیابی مخاطره عمل کرده و تصمیم‌گیری در خصوص چگونگی مدیریت آن، همچنین مناسب‌ترین راهبردها و روش‌های مدیریت مخاطره را ارائه می‌دهد. نتایج این تحلیل، بینش‌هایی برای تصمیم‌گیری فراهم می‌کند که در آن انتخاب‌ها انجام می‌شوند و گزینه‌ها شامل انواع مختلف مخاطره با سطوح متفاوت، پیشنهاد می‌شوند (Odzaly et al., ۲۰۱۸).

۳-۵- ارزیابی مخاطرات نرم‌افزاری

ارزیابی مخاطرات نرم‌افزاری شناسایی‌شده شامل؛ فرآیند کلی شناسایی مخاطره، تحلیل مخاطره و ارزیابی مخاطره است. ارزیابی مخاطره باید به‌صورت نظام‌مند، مکرر، مشترک و با تکیه بر دانش و دیدگاه ذینفعان انجام شود. باید از بهترین اطلاعات موجود استفاده کند که در صورت لزوم با بررسی بیشتر تکمیل شود و عمدتاً بر موارد زیر تاکید دارد (Galin, ۲۰۱۶):

- برآورد احتمال وقوع مخاطره نرم‌افزاری در صورت عدم مدیریت مخاطره - یعنی احتمال وقوع[۱]
- برآورد خسارت در صورت وقوع مخاطره نرم‌افزاری - یعنی برآورد خسارت[۲]

برآوردهای احتمال وقوع و برآورد خسارت می‌توانند بر اساس تجربیات به‌دست‌آمده از پروژه‌های قبلی، با استفاده از مدل‌های شبیه‌سازی و غیره انجام شوند. ارزیابی باید با تعیین اولویت‌ها با توجه به مخاطرات نرم‌افزار و چگونگی حل‌وفصل آنها دنبال شود. بدیهی است که یک مخاطره نرم‌افزاری با احتمال وقوع و برآورد خسارت بالا، اولویت بالایی دارد و مخاطره‌ای با احتمال وقوع و برآورد خسارت پایین، اولویت پایینی دارد. یکی از روش‌های رایج برای اولویت‌بندی مخاطرات نرم‌افزاری، محاسبه میزان مخاطره[۳] آن‌ها است که با فرمول زیر به دست می‌آید:

میزان مخاطره = برآورد خسارت × احتمال وقوع

هدف از ارزیابی مخاطره، حمایت از اتخاذ تصمیمات است. ارزیابی مخاطره شامل مقایسه نتایج تجزیه‌وتحلیل مخاطره با معیارهای تعیین‌شده برای مخاطره به‌منظور شناسایی نیاز به اقدامات اضافی می‌باشد. این امر می‌تواند منجر به اتخاذ تصمیمات زیر شود:

- هیچ کار بیشتری انجام ندهید؛
- گزینه‌های حل‌وفصل خطر را در نظر بگیرید؛
- تجزیه‌وتحلیل بیشتری برای درک بهتر مخاطره انجام دهید؛
- کنترل‌های موجود را حفظ کنید؛
- در اهداف بازنگری کنید.

تصمیمات باید زمینه وسیع‌تر و پیامدهای واقعی و درک‌شده برای ذینفعان خارجی و داخلی را در نظر بگیرد. نتیجه ارزیابی مخاطره باید ثبت، ابلاغ و سپس در سطوح مناسب سازمان تایید شود (Haidabrus et al., ۲۰۲۲).

---

۱ Prob(mat)
۲ Est(dam)
۳ Exp(risk)

۳-۶- برطرف‌کردن مخاطرات

هدف، انتخاب و اجرای گزینه‌هایی برای پرداختن به مخاطرات است. برطرف‌کردن مخاطرات شامل یک فرآیند تکراری از موارد زیر است:

- تدوین و انتخاب گزینه‌های درمان خطر؛
- برنامه‌ریزی و اجرای درمان خطر؛
- ارزیابی اثربخشی آن درمان؛
- تصمیم‌گیری در مورد اینکه آیا مخاطره باقی‌مانده قابل قبول است یا خیر؛
- در صورت عدم پذیرش، انجام درمان بیشتر.

۳-۶-۱- انتخاب گزینه‌های برطرف‌کردن مخاطرات

انتخاب مناسب‌ترین گزینه(ها) برای درمان مخاطره شامل، تعادل میان منافع بالقوه حاصل از دستیابی به اهداف و هزینه‌ها، تلاش یا معایب اجرایی است. گزینه‌های درمان مخاطره لزوماً و متقابلاً منحصربه‌فرد نبوده و در همه شرایط ممکن است مناسب نباشند (Chen & Deng, ۲۰۲٤).

گزینه های برطرف کردن خطر ممکن است شامل یک یا چند مورد از موارد زیر باشد:

- اجتناب از خطر با تصمیم برای شروع یا ادامه فعالیتی که منجر به خطر می‌شود؛
- پذیرش یا افزایش مخاطره برای دنبال کردن یک فرصت؛
- حذف منبع خطر؛
- تغییر احتمال؛
- تغییر پیامدها؛
- به اشتراک گذاشتن مخاطره (به‌عنوان مثال از طریق قراردادها، خرید بیمه و غیره)؛
- حفظ خطر با تصمیم آگاهانه.

توجیه درمان مخاطره فراتر از ملاحظات اقتصادی است و باید تمامی تعهدات سازمان، تعهدات داوطلبانه و دیدگاه‌های ذینفعان را در نظر گرفت. انتخاب گزینه‌های درمان مخاطره باید با اهداف سازمان، معیارهای مخاطره و منابع موجود هماهنگ باشد. هنگام انتخاب گزینه‌های درمان مخاطره، سازمان باید ارزش‌ها، ادراکات و مشارکت بالقوه ذینفعان، همچنین مناسب‌ترین راه‌های ارتباط و مشورت با آنها را مد نظر قرار دهد. هرچند تمامی درمان‌های مخاطره به یک اندازه مؤثرند، برخی از آنها برای برخی از ذینفعان ممکن است قابل قبول‌تر از دیگران باشند. حتی اگر درمان‌های مخاطره با دقت طراحی و اجرا شوند، ممکن است نتایج مورد انتظار را به همراه نداشته و پیامدهای ناخواسته‌ای به بار آورند. نظارت و بازنگری باید بخش جدایی‌ناپذیر از اجرای درمان مخاطره باشد تا اطمینان حاصل شود که اَشکال مختلف درمان، مؤثر باقی می‌مانند. درمان مخاطره همچنین، ممکن است خطرات جدیدی را ایجاد کند که باید مدیریت شوند. در صورتی‌که هیچ گزینه درمانی در دسترس نباشد یا گزینه‌های موجود نتوانند خطر را به اندازه کافی کاهش دهند، خطر باید ثبت شده و تحت بررسی مداوم قرار گیرد. تصمیم‌گیرندگان و سایر ذینفعان باید از ماهیت و میزان مخاطره باقی‌مانده پس از درمان آن آگاه باشند. خطر باقی‌مانده باید مستند شده و تحت نظارت، بررسی و در صورت لزوم درمان‌های بیشتر قرار گیرد (Hasanah et al., ۲۰۲٤).

۳-۶-۲- تهیه و اجرای طرح‌های برطرف‌کردن مخاطرات

هدف از طرح‌های درمان مخاطره، مشخص کردن نحوه اجرای گزینه‌های درمانی انتخابی است؛ به‌طوری که ترتیبات برای دست‌اندرکاران درک شده و پیشرفت در برابر طرح درمان، قابل نظارت باشد. طرح درمان باید به‌وضوح، ترتیب اجرای درمان خطر را مشخص کند. برنامه‌های درمانی باید با مشاوره با ذینفعان مناسب در برنامه‌ها و فرآیندهای مدیریتی سازمان ادغام شوند (Tavares et al., ۲۰۱۹). اطلاعات ارائه‌شده در برنامه درمانی، باید شامل موارد زیر باشد:

- منطق انتخاب گزینه‌های درمانی، از جمله مزایای مورد انتظار برای به‌دست آوردن؛
- کسانی که مسئول تصویب و اجرای طرح هستند؛
- اقدامات پیشنهادی؛
- منابع موردنیاز، از جمله موارد احتمالی؛
- معیارهای عملکرد؛
- محدودیت‌ها؛
- گزارش و نظارت موردنیاز؛
- مدت زمانی که انتظار می‌رود اقدامات انجام و تکمیل شوند.

۳-۷- نظارت و بررسی

هدف از نظارت و بازنگری، تضمین و بهبود کیفیت و اثربخشی طراحی فرآیند، اجرا و نتایج است. نظارت مستمر و بازنگری دوره‌ای فرآیند مدیریت مخاطره و نتایج آن باید بخشی از برنامه‌ریزی کلان فرآیند مدیریت مخاطره باشد و مسئولیت‌ها به‌وضوح تعریف شده باشند. نظارت و بازنگری باید در تمام مراحل فرآیند انجام شود. این فعالیت‌ها شامل برنامه‌ریزی، جمع‌آوری و تجزیه‌وتحلیل اطلاعات، ثبت نتایج و ارائه بازخورد است. نتایج نظارت و بازنگری باید در تمامی فعالیت‌های مدیریت عملکرد، اندازه‌گیری و گزارش‌دهی سازمان گنجانده شود (Laukkarinen et al., ۲۰۱۷).

فعالیت‌های نظام‌مند و دوره‌ای برای نظارت بر اجرای برنامه مدیریت مخاطرات موردنیاز است. هدف از فعالیت‌های نظارتی به شرح زیر است:

- تعیین کارآمدی اقدامات مدیریت مخاطره؛
- به‌روزرسانی ارزیابی مخاطره با درنظرگرفتن مخاطرات نرم‌افزاری تازه شناسایی‌شده.

۳-۸- ثبت و گزارش

فرآیند مدیریت مخاطرات و نتایج آن باید از طریق سازوکارهای مناسب مستند و گزارش شود. هدف از ثبت و گزارش به شرح زیر است:

- ارتباط فعالیت‌ها و نتایج مدیریت مخاطرات در سراسر سازمان؛
- ارائه اطلاعات برای تصمیم‌گیری؛
- بهبود فعالیت‌های مدیریت مخاطرات؛
- کمک به تعامل با ذینفعان، از جمله کسانی که مسئولیت و پاسخگویی برای فعالیت‌های مدیریت مخاطرات را دارند.

تصمیمات مربوط به ایجاد، نگهداری و مدیریت اطلاعات مستند باید با دقت در نظر گرفته شوند، اما محدود به موارد زیر نباشند: نحوه استفاده از آنها، حساسیت اطلاعات و زمینه‌های خارجی و داخلی. گزارش‌دهی، بخشی جدایی‌ناپذیر از حاکمیت سازمان است و باید کیفیت گفت‌وگو با ذینفعان را ارتقا دهد و از مدیریت عالی و نهادهای نظارتی در انجام مسئولیت‌هایشان پشتیبانی کند (Sion et al., ۲۰۲۱). عواملی که برای گزارش باید در نظر گرفته شوند به شرح زیر، اما محدود به موارد زیر نیستند:

- ذینفعان مختلف و نیازها و الزامات اطلاعاتی خاص آنها؛
- هزینه، فراوانی و به موقع بودن گزارش؛
- روش گزارش‌دهی؛
- ارتباط اطلاعات با اهداف سازمانی و تصمیم‌گیری.

٤- اقدامات و فعالیت‌های مدیریت مخاطرات

فعالیت‌ها و اقدامات مختلفی (که معمولاً «اقدامات مدیریت مخاطرات[1]» یا RMA نامیده می‌شوند) را می‌توان انجام داد. اهداف RMA جلوگیری از مخاطرات نرم‌افزاری، شناسایی زودهنگام مخاطرات و حل‌وفصل آن‌ها است. بوهم و راس (۱۹۸۹)، بوهم (۱۹۹۱)، روپونن و لیتینن(۲۰۰۰) و کارولاک (۱۹۹۶) از جمله کسانی هستند که اقدامات متنوعی را برای مدیریت مخاطرات پیشنهاد کرده‌اند (Galin, ۲۰۱٦). جدول ۲ فهرستی از اقدامات مدیریت مخاطرات محتمل و تأثیر آن‌ها در پیشگیری یا حل‌وفصل مخاطرات نرم‌افزاری را ارائه می‌دهد.

جدول ۲- اقدامات رایج مدیریت مخاطرات و سهم آنها

		سهم در مدیریت مخاطرات نرم‌افزار		
شماره	**فعالیت مدیریت مخاطرات نرم‌افزاری**	**جلوگیری از مخاطره**	**شناسایی سریع مخاطره**	**حل‌وفصل مخاطره**
	مدیریت مخاطرات داخلی نرم‌افزار			
۱	به‌کارگیری تحلیل عمیق و تفصیلی بر روی نیازمندی‌ها، زمان‌بندی‌ها و هزینه‌های تخمینی	❊		
۲	سازماندهی کارآمد پروژه، کارکنان کافی و اندازه تیم	❊		
۳	آموزش کارکنان	❊		
۴	آماده‌سازی و آموزش جانشین برای جایگزینی در مواقع جابه‌جایی نیرو و افزایش حجم کاری پیش‌بینی‌نشده	❊		
۵	ایجاد زمینه برای مشارکت کاربران در فرایند توسعه	❊		
۶	به‌کارگیری کنترل کارآمدِ تغییرات (غربالگری درخواست‌های تغییر)	❊		
۷	به‌کارگیری اقدامات فشرده تضمین کیفیت نرم‌افزار، مانند بازرسی، بازبینی طراحی و معیارسنجی	❊		
۸	بررسی دوره‌ای، برای اطمینان از در دسترس‌بودن به‌موقع کارکنان مجرب شرکت که در حال حاضر مشغول پروژه‌های دیگری هستند		❊	
۹	فراهم کردن مشارکت اعضای حرفه‌ای تیم که دارای دانش و تجربه در زمینه مخاطرات نرم‌افزاری هستند			❊

[1] Risk Management Action (RMA)

۱۰	زمان‌بندی فعالیت‌های مرتبط با مخاطرات نرم‌افزار در سریع‌ترین زمان ممکن برای فراهم کردن فرصت حل مشکلات در صورت بروز آن‌ها			*
۱۱	نمونه‌سازی اولیه ماژول‌های مرتبط با مخاطرات نرم‌افزار یا برنامه‌های کاربردی پروژه			*
۱۲	تدوین سناریوهای مرتبط با مخاطرات نرم‌افزاری برای ماژول‌های پیچیده یا برنامه‌های کاربردی پروژه			*
۱۳	شبیه‌سازی ماژول‌های مرتبط با مخاطرات نرم‌افزاری یا برنامه‌های کاربردی پروژه			*
	مدیریت مخاطرات پیمانکاران فرعی نرم‌افزار			
۱	تهیه قراردادهای جامع و کامل با پیمانکاران فرعی و تامین‌کنندگان، به همراه انجام فرآیند بازنگری قراردادها	*		
۲	مشارکت در فعالیت‌های کنترل کیفیت نرم‌افزار و کنترل پیشرفت داخلی پیمانکاران فرعی، به منظور جلب همکاری آنها در اجرای بهینه قرارداد		*	
۳	سازماندهی همکاری با متخصصان دارای دانش و تجربه خاص در صورت نیاز			*
۴	استخدام مشاوران برای حمایت از تیم در نبود دانش و تجربه کافی			*
	مدیریت مخاطرات مشتریان نرم‌افزار			
۱	تنظیم قراردادهای جامع و کامل با مشتریان، به همراه انجام فرآیند بازنگری قراردادها	*		
۲	مذاکره با مشتری برای تغییر نیازمندی‌های مرتبط با بخش‌های پرمخاطره پروژه			*
۳	مذاکره با مشتری برای تغییر زمانبندی بخش‌های پرمخاطره پروژه			*

این اقدامات مدیریت مخاطرات را می‌توان به دسته‌های زیر گروه‌بندی کرد:

۱) **اقدامات مدیریت مخاطرات داخلی**: که در داخل سازمان توسعه‌دهنده نرم‌افزار اعمال می‌شود.

۲) **اقدامات مدیریت مخاطرات پیمانکاری فرعی**: که به ارتباط بین توسعه‌دهنده نرم‌افزار و پیمانکاران فرعی و تامین‌کنندگان او می‌پردازد.

۳) **اقدامات مدیریت مخاطرات مشتری**: که به ارتباط بین توسعه‌دهنده نرم‌افزار و مشتری می‌پردازد.

نکاتی برای پیاده‌سازی:

در هنگام برنامه‌ریزی برای اقدامات مدیریت مخاطرات، باید به نکات زیر توجه داشت:

۱) برخی از اقدامات مدیریت مخاطرات، می‌توانند از انواع مختلف مخاطرات نرم‌افزار جلوگیری کرده، آن‌ها را شناسایی یا حل‌وفصل کنند.

۲) برخی از مخاطرات نرم‌افزار را می‌توان با چندین اقدام مرتبط با مدیریت مخاطره مورد بررسی قرار داد.

۳) کارآمدی یک اقدام مدیریت مخاطره بسته به پروژه و شرایط محیطی، می‌تواند کاملاً متفاوت باشد.

۵- فرایند مدیریت مخاطرات

فرآیند مدیریت مخاطرات شامل فعالیت‌های طرح‌ریزی، اجرا و نظارت است. خانم الن ام. هال (۱۹۹۸) کتابی تالیف کرده است که به‌طور عمده به این فرآیند مرتبط است. شکل ۲ فرآیند مدیریت مخاطرات نرم‌افزار را نشان می‌دهد.

۱) فعالیت‌های طرح‌ریزی:

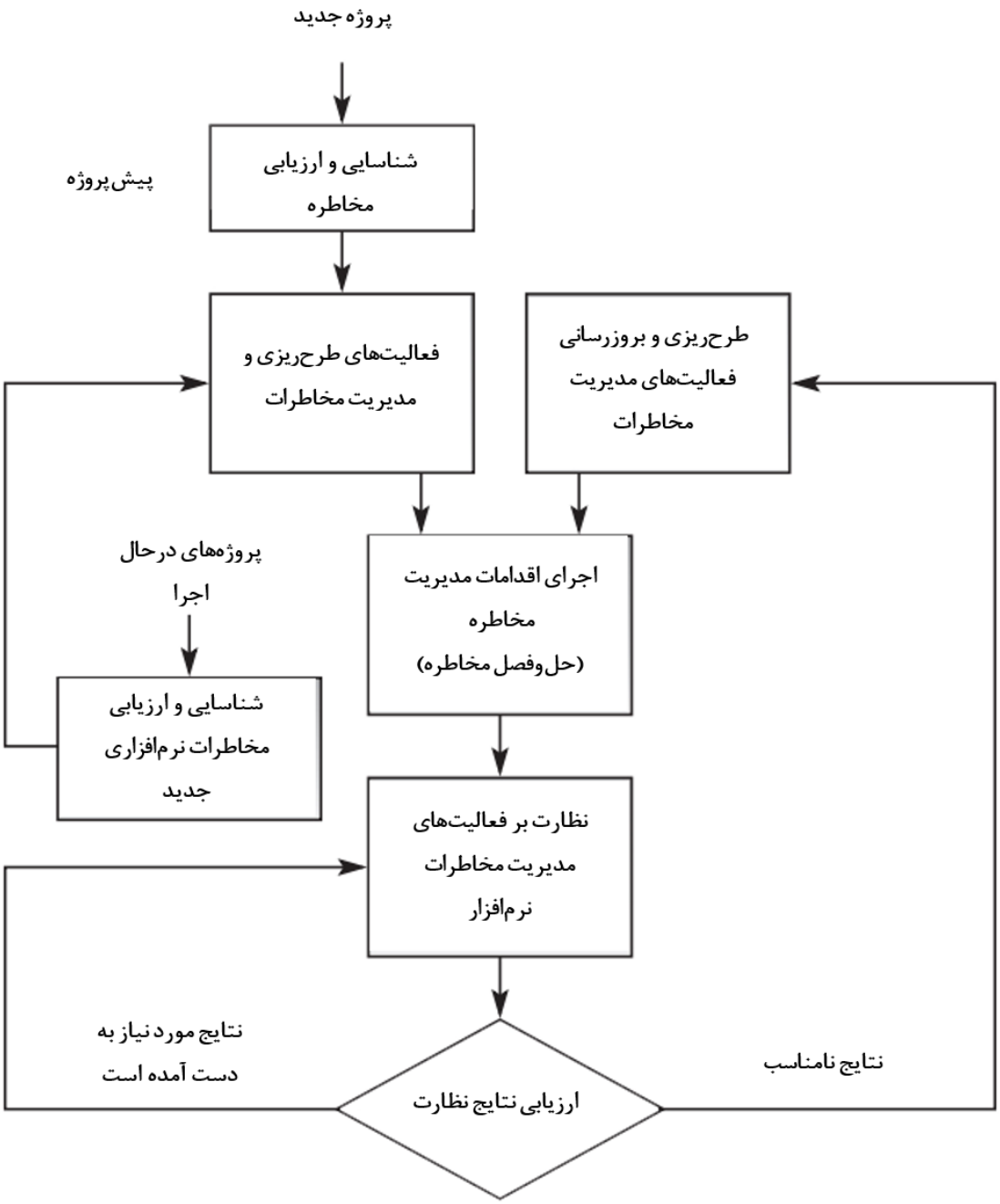
هدف از فعالیت‌های مختلف طرح‌ریزی، آغاز اقداماتی برای مدیریت مخاطره است که می‌تواند به مخاطرات نرم‌افزاری شناسایی‌شده و ارزیابی‌شده پاسخ دهد. فعالیت‌های طرح‌ریزی مشابهی (اگرچه با همان درجه جزئیات نیستند) بخشی از فرآیند بازنگری پیش‌نویس طرح پیشنهادی هستند. فعالیت‌های مرتبط با برنامه‌ریزی شامل موارد زیر می‌باشند:

- **شناسایی مخاطرات نرم‌افزاری**

  مطالب این بخش، همان موارد توضیح داده شده در بخش ۳-۳ می‌باشد.

- **ارزیابی مخاطرات نرم‌افزاری شناسایی‌شده**

  مطالب این بخش، همان موارد توضیح داده شده در بخش ۳-۵ می‌باشد.



شکل ۲: فرآیند مدیریت مخاطرات نرم‌افزار

- **طرح‌ریزی اقدامات مدیریت مخاطرات**

تیم مدیریت مخاطرات نرم‌افزار موظف است راه‌های جایگزین برای حل‌وفصل مخاطرات نرم‌افزاری شناسایی‌شده را در نظر بگیرد. اقدامات مدیریت مخاطرات شامل مجموعه‌ای از اقدامات داخلی، مربوط به پیمانکاران فرعی و مرتبط با مشتری است. فهرستی از اقدامات مدیریت مخاطرات محتمل و تأثیر آن‌ها در پیشگیری یا حل‌وفصل مخاطرات نرم‌افزاری در جدول ۲ ارائه شد. هنگام تهیه فهرست پیشنهادی اقدامات مدیریت مخاطرات، تیم طرح‌ریزی باید موارد زیر را در نظر بگیرد:

- اولویتی که به مخاطرات نرم‌افزاری اختصاص یافته است؛
- نتایج موردانتظار از یک اقدام طرح‌ریزی‌شده مدیریت مخاطرات (حل‌وفصل کامل یا جزئی)؛
- هزینه‌ها و تلاش‌های سازمانی موردنیاز برای اجرای اقدام مدیریت مخاطرات.

۲) اجرا

برای اجرای برنامه مدیریت مخاطرات، لازم است کارکنان، مسئولیت شخصی برای هر اقدام مدیریت مخاطرات و برنامه زمان‌بندی اجرای آن را بر عهده بگیرند.

۳) نظارت بر اجرای برنامه مدیریت مخاطرات

مطالب این بخش، همان موارد توضیح داده شده در بخش ۳-۷ می‌باشد.

٦- نتیجه‌گیری

مدیریت مخاطرات در پروژه‌های نرم‌افزاری یک فرآیند ضروری است که می‌تواند شانس موفقیت پروژه را افزایش دهد. این فرآیند شامل شناسایی، ارزیابی و مدیریت مخاطرات به‌گونه‌ای است که تیم‌های پروژه بتوانند با اطمینان بیشتری به سمت اهداف خود حرکت کنند. با شناسایی و ارزیابی دقیق مخاطرات، تیم‌ها می‌توانند نقاط ضعف و تهدیدات بالقوه را شناسایی کرده و در نتیجه اقداماتی را برای کاهش تأثیرات منفی آن‌ها طراحی کنند. در این مقاله، به بررسی انواع مخاطرات نرم‌افزاری پرداخته شد. همچنین، مراحل مدیریت مخاطرات در بخش‌های مختلف مورد بررسی قرار گرفت. در مرحله شناسایی، تمامی مخاطرات ممکن شناسایی می‌شوند و در مرحله ارزیابی، هر مخاطره بر اساس احتمال وقوع و تأثیر آن بر پروژه ارزیابی می‌شود. این مراحل به تیم‌های پروژه امکان می‌دهد که با دقت بیشتری به بررسی مخاطرات پرداخته و برنامه‌های مؤثرتری برای مدیریت آن‌ها طراحی کنند.

توسعه راهبردهای مؤثر برای مدیریت مخاطرات به تیم‌های پروژه این امکان را می‌دهد که از بروز مشکلات جدی جلوگیری کنند. به‌عنوان مثال، شناسایی مخاطرات فنی در مراحل ابتدایی پروژه می‌تواند به تیم کمک کند تا از انتخاب فناوری‌های ناکارآمد یا نامناسب اجتناب کند. همچنین، ارزیابی مخاطرات مالی می‌تواند به پیش‌بینی هزینه‌های اضافی و تأمین منابع مالی مناسب کمک کند.

توجه به مدیریت مخاطرات نه‌تنها به بهبود کیفیت نرم‌افزار کمک می‌کند، بلکه منجر به افزایش رضایتمندی مشتری و کاهش هزینه‌ها نیز می‌شود. هنگامی که مخاطرات به‌طور مؤثر مدیریت شوند، احتمال تأخیر در تحویل پروژه و نیاز به اصلاحات گسترده کاهش می‌یابد. این امر به تیم‌ها امکان می‌دهد تا بر ارائه محصول نهایی باکیفیت تمرکز کنند و در نتیجه، رضایتمندی مشتری را افزایش دهند. علاوه‌براین، با کاهش هزینه‌های ناشی از مشکلات غیرمنتظره، سازمان‌ها می‌توانند منابع خود را به‌صورت بهینه مدیریت کرده و در نهایت به سودآوری بیشتری دست یابند.

در نهایت، مدیریت مخاطرات به‌عنوان یکی از اجزای کلیدی در فرآیند مدیریت پروژه‌های نرم‌افزاری شناخته می‌شود و باید به‌طور جدی مورد توجه مدیران پروژه‌های نرم‌افزاری قرار گیرد. با اتخاذ رویکردی نظام‌مند در مدیریت مخاطرات، تیم‌های پروژه می‌توانند به‌طور مؤثر بر چالش‌ها غلبه کرده و موفقیت پروژه‌های خود را تضمین نمایند.

۷- مراجع

Arıkan, S. M., & Yürekten, Ö. (۲۰۲۰). Software Risk Management Process Improvement Experience in Enterprise Projects. ۲۰۲۰ Turkish National Software Engineering Symposium (UYMS),

Chen, X., & Deng, Y. (٢٠٢٤). Evidential software risk assessment model on ordered frame of discernment. *Expert systems with applications*, *250*, ١٢٣٧٨٦.

Dewi, R. S., & Dharmawan, Y. S. (٢٠٢٤). A Proposed Model for Embedding Risk Proportion in Software Development Effort Estimation. *Procedia Computer Science*, *234*, ١٧٧٧-١٧٨٤.

Galin, D. (٢٠١٦). *Software quality assurance: from theory to implementation*. Pearson education.

Haidabrus, B., Druzhinin, E., & Psarov, O. (٢٠٢٢). Taxonomy of Risks in Software Development Projects. ٢٠٢٢ ٦٣rd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS),

Hasanah, S. U., Santosa, P. I., & Ferdiana, R. (٢٠٢٤). Exploring Innovative Approaches for Software Development Risk Assessment and Management. ٢٠٢٤ ٨th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE),

Hutchins, G. (٢٠١٨). *ISO 31000: 2018 enterprise risk management*. Greg Hutchins.

Laukkarinen, T., Kuusinen, K., & Mikkonen, T. (٢٠١٧). DevOps in regulated software development: case medical devices. ٢٠١٧ IEEE/ACM ٣٩th International Conference on Software Engineering: New Ideas and Emerging Technologies Results Track (ICSE-NIER),

Makajić-Nikolić, D. (٢٠٢٠). ISO ٣١٠٠٠: Risk Management Guidelines. In *Encyclopedia of Sustainable Management* (pp. ١-٤). Springer.

Mohamud Sharif, A., & Basri, S. (٢٠١١). Software risk assessment: a review on small and medium software projects. Software Engineering and Computer Systems: Second International Conference, ICSECS ٢٠١١, Kuantan, Pahang, Malaysia, June ٢٧-٢٩, ٢٠١١, Proceedings, Part II ٢,

Odzaly, E. E., Greer, D., & Stewart, D. (٢٠١٨). Agile risk management using software agents. *Journal of Ambient Intelligence and Humanized Computing*, *9*, ٨٢٣-٨٤١.

Sarigiannidis, L., & Chatzoglou, P. D. (٢٠١١). Software development project risk management: A new conceptual framework. *Journal of Software Engineering and Applications*, *4*(٠٥), ٢٩٣.

Shehzad, N., Iqbal, M. A., & Amjad, M. (٢٠٢٢). A review of risk management in agile development. ٢٠٢٢ International Conference on Digital Transformation and Intelligence (ICDI),

Sion, L., Van Landuyt, D., Yskout, K., Verreydt, S., & Joosen, W. (٢٠٢١). Automated threat analysis and management in a continuous integration pipeline. ٢٠٢١ IEEE Secure Development Conference (SecDev),

Sravan, S. S., Ganesh, C. S., Kiran, K., Chandra, T. A., Aparna, K., & Vignesh, T. (٢٠٢٣). Significant Challenges to espouse DevOps Culture in Software Organisations By AWS: A methodical Review. ٢٠٢٣ ٩th International conference on advanced computing and communication systems (ICACCS),

Tavares, B. G., da Silva, C. E. S., & de Souza, A. D. (٢٠١٩). Risk management analysis in Scrum software projects. *International Transactions in Operational Research*, *26*(٥), ١٨٨٤-١٩٠٥.

Risk management in software projects production and development

Ali Karimi
Assistant Professor of Imam Hossein Comprehensive University

Farhad Karimi
Ph.D. Student of Imam Hossein Comprehensive University

Ali Tolui far[۱]
Ph.D. Student of Imam Hossein Comprehensive University

Mohammad Alabrishamkar
M.Sc. Student of Imam Hossein Comprehensive University

۱-۱-

۲-۱- Abstract

In today's world, software projects have become increasingly complex, and the risk factors associated with them have risen. These complexities stem from various factors, including rapid technological changes, evolving customer demands, and competitive pressures. For this reason, effective risk management plays a critical role in the success of software projects. As a systematic and structured process, risk management involves identifying, assessing, and controlling the risks and uncertainties associated with software projects. This process helps project managers to identify risks early on and make the necessary plans to prevent serious issues from arising. Neglecting risks can lead to delivery delays, increased costs, and ultimately, project failure. By leveraging evolving technologies, standards, and experiences, risk management processes can be continuously improved. This ongoing improvement not only helps reduce risks but can also lead to optimization of resources and time. In this regard, the use of modern software tools and techniques can aid in clarifying and streamlining the risk management process. In this paper, we will conduct a more detailed examination and in-depth analysis of these topics, exploring the concept and techniques of risk management, the various types of risks, and the stages of risk management.

۳-۱- Keywords: Software Project, Risk Management, Risk Identification and Assessment, Challenges in Software Development, Resource and Time Optimization.

۱-Corresponding Author