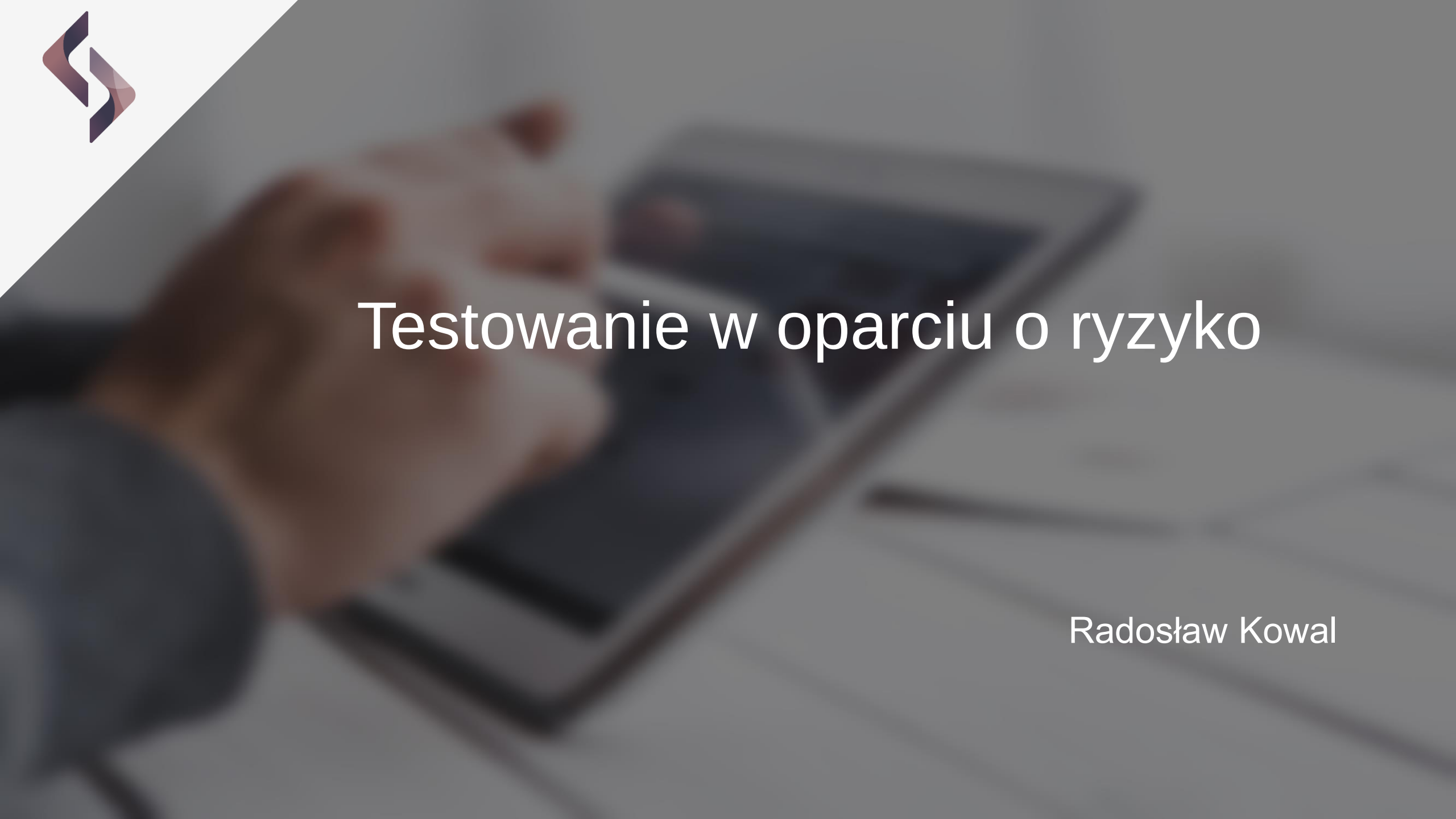


Testowanie w oparciu o ryzyko

Radosław Kowal

Co to takiego?

Ryzyko wg Was…

Ryzyko

Termin ryzyko (ang. *risk*) wywodzi się z języka włoskiego (*wł. *Risico**), w którym oznacza przede wszystkim przedsięwzięcie, którego wynik jest nieznany albo niepewny, lub możliwość, że coś się uda albo nie uda.

Ryzyko wg ISTQB

Ryzyko jest możliwością wystąpienia w przyszłości zdarzenia o niepożądanych konsekwencjach. O poziomie ryzyka decyduje prawdopodobieństwo wystąpienia niekorzystnego zdarzenia oraz jego wpływ (tj. wynikające z niego szkody).

Ryzyko wg PMBoK

Ryzyko to prawdopodobieństwo wystąpienia sytuacji, która może oddziaływać na dalszy przebieg projektu — jego jakość, zakres, koszty i/lub harmonogram. Istotne jest, że wpływ ten może być zarówno pozytywny, jak i negatywny, ponadto może wpływać pozytywnie na jeden a negatywnie na inny obszar tego samego projektu. Charakterystycznym dla ryzyka jest możliwość oszacowania prawdopodobieństwa jego wystąpienia oraz siły oddziaływania na projekt.

Ryzyko wg PRINCE2

Ryzyko jest zdarzeniem lub ich zbiorem, które w sytuacji wystąpienia mogą mieć wpływ na osiągnięcie celów projektu. Oznacza ono wprost niepewność wyniku. Metodyka PRINCE2 rozróżnia dwa typy ryzyka:

Zagrożenie — prawdopodobne zdarzenie mające negatywny wpływ na realizację celów.

Szansa/okazja — prawdopodobne zdarzenie, mające pozytywny wpływ na realizację założonych celów

Ryzyko w projekcie

Ryzyko można definiować jako przypadek, niebezpieczeństwo, możliwość lub sytuację występującą w projekcie z niepożądanymi konsekwencjami — potencjalny problem.
Poziom ryzyka będzie określony prawdopodobieństwem wystąpienia zdarzenia i jego wpływem.

Najważniejsze cechy ryzyka

Ryzyko istnieje, kiedy istnieje prawdopodobieństwo wystąpienia problemu, który może pogorszyć zdanie klienta, użytkownika, uczestnika lub interesariusza o jakości produktu, lub sukcesie projektu.

Ryzyko może, ale nie musi wystąpić – niepewność.

Zazwyczaj prawdopodobieństwo wystąpienia ryzyka jest trudne do oszacowania, a tym bardziej do przedstawienia go w miarach ilościowych.

Zazwyczaj używa się miar jakościowych, a nie ilościowych (znikome, duże itp.).

Najważniejsze cechy ryzyka

Przy wystąpieniu ryzyka mogą być odczuwalne jego konsekwencje.

Wystąpienie ryzyka generuje dodatkowe koszty.

Aby uniknąć niekorzystnych skutków oraz dodatkowych kosztów, należy zapobiegać ryzykom.

Prawdopodobieństwo wystąpienia awarii

Można wyróżnić kilka czynników, które mają wpływ na wystąpienie awarii w czasie eksploatacji oprogramowania:

- Złożone funkcjonalności składające się z dużej ilości modułów.
- Częste zmiany kodu w różnych obszarach systemu.
- Niska jakość analizy w czasie projektowania systemu.
- Niska jakość wymagań, dostarczonych do zespołu deweloperskiego.

Prawdopodobieństwo wystąpienia awarii

- Duża ilość osób zaangażowanych w projekt.
- Presja czasu.
- Ograniczone zasoby ludzkie oraz sprzętowe.

Prawdopodobieństwo wystąpienia awarii w oprogramowaniu jest czynnikiem indywidualnym, zależy od konkretnej implementacji. Stąd lista może być krótsza bądź dłuższa.

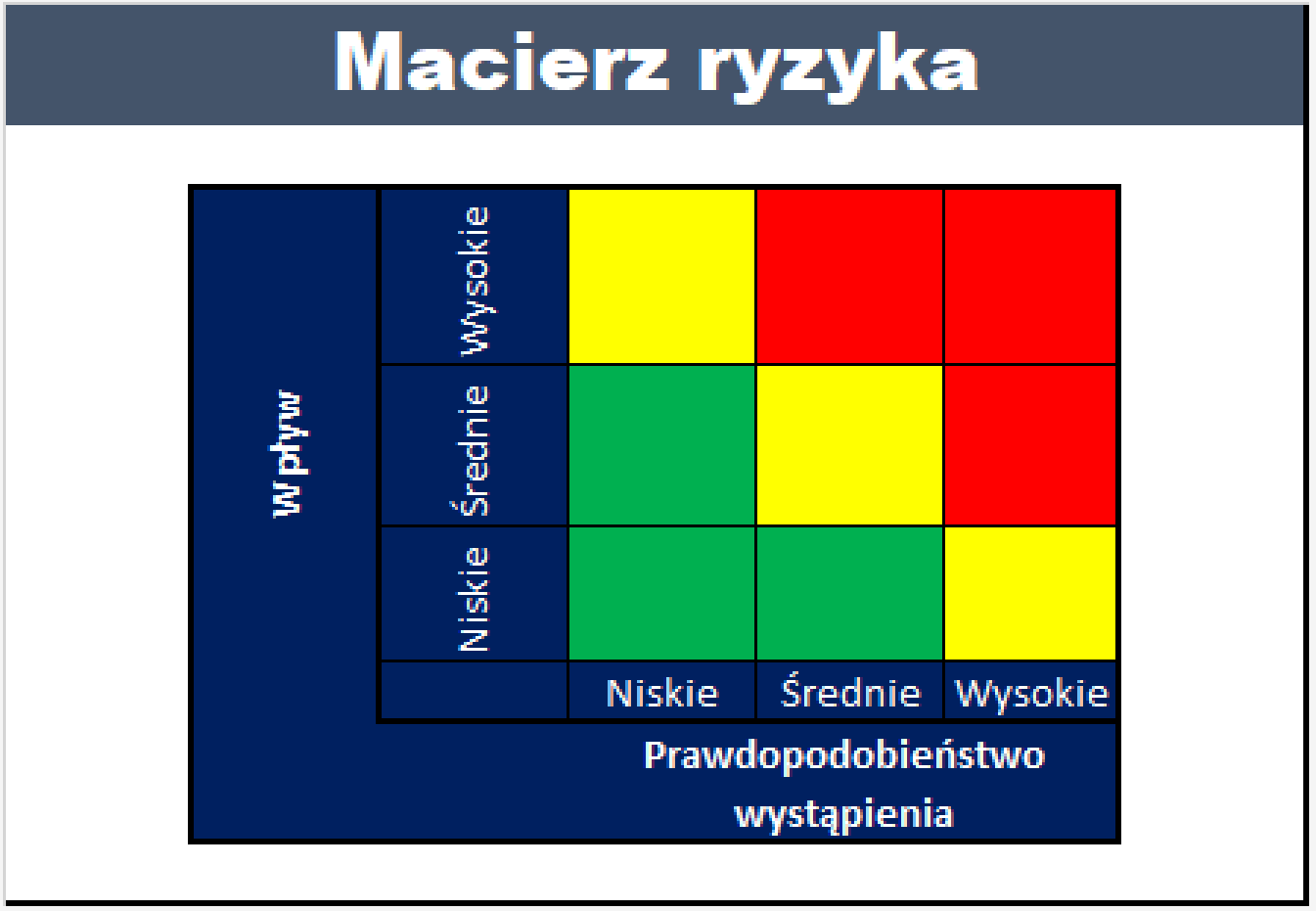
Poziom ryzyka

Prawdopodobieństwo wystąpienia awarii można spróbować oszacować przy pomocy poziomu ryzyka. Wykorzystuje się do tego trzy czynniki:
Poziom ryzyka (*ang. risk level*)
Wpływ ryzyka (*ang. risk impact*)
Prawdopodobieństwo ryzyka (*ang. risk likelihood*)

Poziom ryzyka

poziom ryzyka = prawdopodobieństwo zdarzenia * wpływ zdarzenia

Poziom ryzyka



Prawdopodobieństwo oraz wpływ

Prawdopodobieństwa wystąpienia ryzyka oraz jego wpływ:

A – niskie prawdopodobieństwo, niski wpływ

B – mało prawdopodobne, duży wpływ

C – średnie prawdopodobieństwo, średni wpływ

D – wysokie prawdopodobieństwo wystąpienia, duży wpływ

E – wysokie prawdopodobieństwo wystąpienia, niski wpływ

F – najwyższe prawdopodobieństwo wystapienia, najwyższy wpływ

Priorytety od najwyższego do najniższego:

F > D > B > C > E > A

Pytanie

Która z poniższych odpowiedzi zawiera NAJLEPSZĄ definicję poziomu ryzyka?
a) Poziom ryzyka oblicza się poprzez zsumowanie prawdopodobieństw wystąpienia wszystkich sytuacji problemowych oraz wynikających z nich szkód finansowych.
b) Poziom ryzyka szacuje się poprzez pomnożenie prawdopodobieństwa wystąpienia zagrożenia dotyczącego systemu i szansy wywołania przez to zagrożenie strat finansowych.
c) Poziom ryzyka oblicza się jako kombinację prawdopodobieństwa wystąpienia niepożądanego zdarzenia i przewidywanego wpływu tego zdarzenia.
d) Poziom ryzyka to suma wszystkich potencjalnych zagrożeń dotyczących systemu pomnożona przez sumę wszystkich potencjalnych strat związanych z tym systemem.

Odpowiedź

Która z poniższych odpowiedzi zawiera NAJLEPSZĄ definicję poziomu ryzyka?
a) Odpowiedź niepoprawna. Ryzyko określa się na podstawie kombinacji prawdopodobieństwa wystąpienia sytuacji problemowych oraz szkód, które mogą z nich wyniknąć (czyli wpływu). Nie można go obliczyć poprzez zsumowanie powyższych czynników (prawdopodobieństwo wyraża się liczbą z przedziału od 0 do 1, a szkody mogą być liczone w złotówkach).
b) Odpowiedź niepoprawna. Ryzyko określa się na podstawie kombinacji prawdopodobieństwa i wpływu. Ta definicja uwzględnia tylko pewność i szansę (oba te pojęcia są formą prawdopodobieństwa), nie uwzględnia natomiast wpływu (czyli szkód).
c) Odpowiedź poprawna. Patrz sylabus p. 5.5.1.
d) Odpowiedź niepoprawna. Ryzyko określa się na podstawie kombinacji prawdopodobieństwa i wpływu. Ta definicja uwzględnia tylko zagrożenia i straty (zagrożenie oznacza niekorzystne zdarzenie, podobnie jak ryzyko, a strata jest formą wpływu), nie uwzględnia natomiast prawdopodobieństwa.

Zalety testowania opartego na ryzyku

- Wszystkie czynności procesu testowego (**planowanie, analiza, monitorowanie**) są odnoszone do poziomu ryzyka.
- Koncentruje się na pytaniu, co może pójść źle, jeśli nastąpi awaria.
- Konieczne jest ustalenie możliwych ryzyk – rodzajów awarii oraz przeanalizowania wpływu ich pojawienia się.

Zalety testowania opartego na ryzyku

- Testowanie weryfikuje, czy poszczególne ryzyka naprawdę istnieją w systemie, czy też nie. Gdy test wykonał się z wynikiem pozytywnym — oznacza to, że ryzyko związane z tym testem nie istnieje lub jego wystapienie jest bardzo mało prawdopodobne.
- Im więcej testów pokrywa dany obszar ryzyka, tym wzrasta przekonanie o tym, że ryzyko nie stanowi już takiego zagrożenia.
- Priorytetyzacja testów – ryzyka — optymalizujemy naszą pracę pod kątem dostępnych zasobów oraz czasu.

Rodzaje ryzyk

Ryzyko projektowe – ryzyko związane z zarządzaniem i kontrolą projektu (testowego), np. braki w zasobach, rygorystyczny harmonogram, zmieniające się wymagania itp.

Ryzyko projektowe

Ryzyka Projektowe	Skutek
środowisko testowe, dostepność narzędzi	może opóźnić proces testowy
dostępność testerów i ich kwalifikacje	może wpłynąć negatywnie na jakość przygotowywanych testów
niska jakość artefaktów testowych	może wprowadzić kadrę zarządzającą w błąd, przy podejmowaniu decyzji dotyczących produktu
duże zmiany w zakresie i definicji produktu	opóźnienie procesu testowania, zwiększenie kosztów testowania
dostępność wykwalifikowanych członków zespołu	opóźnienie projektu
konflikty w zespole	zmniejszają morale i efektywność zespołu
brak wsparcia kadry zarządzającej	problemy z finansowaniem projektu, problemy z rozwiązywaniem konfliktów, możliwość anulowania projektu

Czynniki występowania ryzyka projektowego

Ryzyka Projektowe	Skutek	Czynnik
środowisko testowe, dostepność narzędzi	może opóźnić proces testowy	Techniczne/Dostawcy
dostępność testerów i ich kwalifikacje	może wpłynąć negatywnie na jakość przygotowywanych testów	Techniczne
niska jakość artefaktów testowych	może wprowadzić kadrę zarządzającą w błąd, przy podejmowaniu decyzji dotyczących produktu	Techniczne
duże zmiany w zakresie i definicji produktu	opóźnienie procesu testowania , zwiększenie kosztów testowania	Organizacyjne
dostępność wykwalifikowanych członków zespołu	opóźnienie projektu	Organizacyjne
konflikty w zespole	zmniejszają morale i efektywność zespołu	Organizacyjne
brak wsparcia kadry zarządzającej	problemy z finansowaniem projektu, problemy z rozwiązywaniem konfliktów, możliwość anulowania projektu	Organizacyjne

Ryzyko projektowe - sytuacje

Ryzyko projektowe obejmuje sytuacje, których zaistnienie może mieć negatywny wpływ na możliwość osiągnięcia celów projektu. Przykłady ryzyka projektowego to:

• *problemy związane z projektem, takie jak*: potencjalne opóźnienia w dostawach, ukończeniu zadań bądź spełnieniu kryteriów wyjścia (definicji ukończenia); niedokładne oszacowanie, realokacja środków do projektów o wyższym priorytecie lub ogólne cięcia kosztów w całej organizacji, które mogą skutkować niewystarczającym finansowaniem projektu; wprowadzenie w ostatniej chwili zmian wymagających dokonania licznych przeróbek;

• *problemy organizacyjne, takie jak*: niewystarczające kwalifikacje lub przeszkolenie pracowników bądź braki kadrowe; konflikty i problemy wynikające z doboru personelu; brak dostępności użytkowników, pracowników struktur biznesowych lub ekspertów merytorycznych z powodu sprzecznych priorytetów biznesowych;

Ryzyko projektowe - sytuacje

- *problemy techniczne, takie jak*: niedostateczne doprecyzowanie wymagań; brak możliwości spełnienia wymagań z uwagi na ograniczenia czasowe; nieudostępnienie na czas środowiska testowego; zbyt późne przeprowadzenie konwersji danych, zaplanowanie migracji lub udostępnienie potrzebnych do tego narzędzi; wady w procesie wytwarzania oprogramowania mogące wpływać na spójność lub jakość produktów prac projektowych, kodu, konfiguracji, danych testowych i przypadków testowych; kumulacja defektów lub innego rodzaju dług techniczny powstały na skutek problemów z zarządzaniem defektami lub innych podobnych problemów;
- *problemy związane z dostawcami, takie jak:* niedostarczenie niezbędnego produktu lub usługi przez zewnętrznego dostawcę bądź ogłoszenie przez niego upadłości; utrudnienia w realizacji projektu wynikające z problemów związanych z umowami.

Ryzyko projektowe może dotyczyć zarówno czynności związanych z wytwarzaniem oprogramowania, jak i jego testowaniem. W niektórych przypadkach za zarządzanie ryzykiem projektowym odpowiadają kierownicy projektów, ale zdarza się również, że za czynniki ryzyka projektowego związane z testowaniem odpowiedzialność ponoszą kierownicy testów.

Ryzyko projektowe

ZADANIE – podaj przykłady ryzyk projektowych

Ryzyko produktowe

Inaczej nazywane **ryzykiem jakościowym**. Do tych ryzyk zaliczymy wszystkie zdarzenia, które mogą wystąpić w trakcie trwania projektu, powodując, że produkt nie będzie spełniał założonych celów. Poniżej zamieszczone są przykłady, związane z ryzykiem produktowym:

- błędy związane z integracją ze sprzętem,
- brak pamięci w urządzeniu,
- niepoprawne zaokrąglenia.

Ryzyko produktowe

Ryzyka Produktowe	Skutek
wysoka złożoność struktury modułu	zwiększa prawdopobieństwo defektu
skomplikowana architektura	gorsza pielęgnowalność systemu
niewykorzystanie lub błędne wykorzystywanie wzorców projektowych podczas kodowania	pogarsza lub uniemożliwia testowalność
nowi niedoświadczeni programiści w zespole	większe ryzyko wprowadzenia defektów
nowe technologie wykorzystywane w projekcie	większe ryzyko błedów na poziomie integracji
brak przeszkolenia w prowadzeniu inspekcji formalnych	zwiększa prawdopodobieństwo nie znalezienia defektów podczas statycznej analizy kodu
napięte harmonogramy	stres, niedokładność, większe szanse na popełnienie pomyłki
nowe regulacje prawne	ryzyko błędnego działania pod kątem biznesowym

Ryzyko produktowe

Przykładami czynników ryzyka produktowego mogą być następujące problemy:
• niewykonywanie przez oprogramowanie zakładanych funkcji zgodnie ze specyfikacją;
• niewykonywanie zakładanych funkcji oprogramowania zgodnie z potrzebami użytkowników, klientów i/lub interesariuszy;
• niedostateczne spełnienie przez architekturę systemu określonych wymagań niefunkcjonalnych;
• niepoprawne wykonywanie konkretnych obliczeń w niektórych okolicznościach;
• błędy w kodzie struktury sterowania pętlą;
• zbyt długi czas odpowiedzi w systemie transakcyjnym wysokiej wydajności;
• niezgodność informacji zwrotnych na temat doświadczenia użytkownika z oczekiwaniami dotyczącymi produktu.

Pytanie

Która z poniższych odpowiedzi jest NAJPRAWDOPODOBNIEJ przykładem ryzyka PRODUKTOWEGO?

a) Oczekiwane zabezpieczenia mogą nie być obsługiwane przez funkcjonalności architektury systemu.

b) Developerzy mogą nie mieć czasu na usunięcie wszystkich defektów wykrytych przez zespół testowy.

c) Przypadki testowe mogą nie zapewnić pełnego pokrycia wyspecyfikowanych wymagań.

d) Środowisko do testów wydajnościowych może nie być gotowe przed terminem dostarczenia produktu.

Odpowiedź

Która z poniższych odpowiedzi jest NAJPRAWDOPODOBNIEJ przykładem ryzyka PRODUKTOWEGO?

a) Odpowiedź poprawna. Jeśli funkcjonalności architektury systemu nie obsługują oczekiwanych zabezpieczeń, system może mieć poważne wady. Problem dotyczy bezpośrednio wytwarzanego systemu, w związku z czym mamy do czynienia z ryzykiem produktowym.

b) Odpowiedź niepoprawna. Niedotrzymanie przez programistów harmonogramu to problem związany z prowadzeniem projektu, a więc mamy do czynienia z ryzykiem projektowym.

c) Odpowiedź niepoprawna. Jeśli przypadki testowe nie zapewniają pełnego pokrycia wymagań, oznacza to, że testowanie może nie spełnić wymagań planu testów. W tej sytuacji mamy do czynienia z ryzykiem projektowym.

d) Odpowiedź niepoprawna. Jeśli środowisko testowe do testów wydajnościowych nie jest gotowe, nie można przeprowadzić testowania (lub trzeba je przeprowadzić w innym środowisku), co wpływa na sposób prowadzenia projektu. W związku z tym mamy do czynienia z ryzykiem projektowym.

Ryzyko produktowe

ZADANIE – podaj przykłady ryzyk produktowych

Ryzyko w procesie testowym

W pierwszym kroku powinniśmy się skupić na identyfikacji wszystkich ryzyk. Jeśli nie jest to pierwszy projekt, najlepszym punktem wyjścia do zrealizowania tego jest przegląd dokumentów z retrospektyw z poprzednich projektów. Dzięki temu będziemy mogli stworzyć wstępną listę. Co więcej, można ją uzupełnić o dane z sesji burzy mózgów czy wykonać niezależną, subiektywną analizę projektu. W niektórych przypadkach jest możliwość skorzystania z zewnętrznych lub wewnętrznych list kontrolnych.

Ryzyko w procesie testowym

Mając już spisane wszystkie ryzyka, możemy podejść do ich podziału na ryzyka projektowe oraz produktowe. Trzeba mieć świadamość, że nie będą to listy zamknięte, a nowe ryzyka będą się pojawiać podczas trwania projektu.

Ryzyko w procesie testowym

W kolejnym kroku należy przystąpić do oceny ryzyk, kiedy to każdemu z nich przypisujemy odpowiednie prawdopodobieństwo wystąpienia, a także wpływ ewentualnego zajścia danego zdarzenia. Najczęściej prawdopodobieństwo określa się w skali od 1 do 5. Z kolei wpływ dobrze jest zapisywać słownie, ze względu na potrzebę raportowania kierownictwu, a następnie również przetłumaczyć na skalę w zakresie 1-5, przyjmując jako wykładnię krytyczność wpływu. Dobrymi przykładami wpływu danego ryzyka może być utrata reputacji, złamanie prawa, czy negatywny wpływ na bezpieczeństwo.

Ryzyko w procesie testowym

Następny etap to łagodzenie zidentyfikowanych ryzyk. W przypadku **ryzyk jakościowych**, do każdego należy przypisać odpowiednią liczbę testów, która pokryje je w pełni. W przypadku braku testów dla wybranych ryzyk oznacza to, że zostały one zaakceptowane przez zespół. W przypadku **ryzyk planowania**, sprawa jest trochę bardziej skomplikowana, gdyż w niektórych przypadkach nie jesteśmy stanie dokonać wcześniej żadnych działań, aby je zminimalizować. W takim przypadku dobrą opcją jest przygotowanie potencjalnych działań naprawczych, dzięki czemu reakcja na wystąpienie konkretnego ryzyka będzie szybsza oraz bardziej właściwa. Takimi działaniami może być zorganizowanie potencjalnego zastępstwa, czy posiadanie alternatywnych źródeł dostaw.

Ryzyko w procesie testowym

Jak widzimy, zarządzanie ryzykiem podczas całego procesu testowego jest istotnym elementem. Wynika z tego także szereg korzyści, takich jak ułatwione przydzielanie priorytetów do konkretnych wymagań, a później testów. Z punktu widzenia całego projektu możemy znacznie szybciej wykryć zagrożone obszary, a dzięki temu kluczowe defekty. Dodatkowo wiemy które obszary należy bardziej przetestować w głąb. Wdrażając wszystkie czynności łagodzące ryzyka, możemy ograniczyć skutki działań niepożądanych do minimum.

Rozważ poniższą listę niepożądanych wyników, które mogą wystąpić jako ryzyka produktowe i projektowe.

A. Nieprawidłowe sumy w raportach.
B. Zmiany w kryteriach akceptacji podczas testów akceptacyjnych.
C. Użytkownicy uważają miękką klawiaturę za zbyt trudną do użycia.
D. System reaguje zbyt wolno na wprowadzanie danych przez użytkownika podczas wpisywania warunku wyszukiwania.
E. Testerzy nie mogą zgłaszać wyników testów podczas codziennych spotkań (daily stand-up meeting).

Które z poniższych odpowiedzi poprawnie klasyfikuje te czynniki jako ryzyka projektowe i ryzyka produktowe?

a) Ryzyko produktowe: B, E Ryzyko projektowe: A, C, D
b) Ryzyko produktowe: A, C, D Ryzyko projektowe: B, E
c) Ryzyko produktowe: A, C, D, E Ryzyko projektowe: B
d) Ryzyko produktowe: A, C Ryzyko projektowe: B, D, E.

Rozważ poniższą listę niepożądanych wyników, które mogą wystąpić jako ryzyka produktowe i projektowe.

Rozważ poniższą listę niepożądanych wyników, które mogą wystąpić jako ryzyka produktowe i projektowe.
A. Nieprawidłowe sumy w raportach. /ryzyko produktowe/
B. Zmiany w kryteriach akceptacji podczas testów akceptacyjnych. /ryzyko projektowe/
C. Użytkownicy uważają miękką klawiaturę za zbyt trudną do użycia. /ryzyko produktowe/
D. System reaguje zbyt wolno na wprowadzanie danych przez użytkownika podczas wpisywania warunku wyszukiwania. /ryzyko produktowe/
E. Testerzy nie mogą zgłaszać wyników testów podczas codziennych spotkań (daily stand-up meeting). /ryzyko projektowe/
Które z poniższych odpowiedzi poprawnie klasyfikuje te czynniki jako ryzyka projektowe i ryzyka produktowe?

a) Ryzyko produktowe: B, E Ryzyko projektowe: A, C, D
b) Ryzyko produktowe: A, C, D Ryzyko projektowe: B, E
c) Ryzyko produktowe: A, C, D, E Ryzyko projektowe: B
d) Ryzyko produktowe: A, C Ryzyko projektowe: B, D, E.

Testowanie oparte na ryzyku a jakość produktu

Wiedzę na temat ryzyka można wykorzystać do odpowiedniego ukierunkowania działań wykonywanych podczas testowania. Na podstawie ryzyka można podejmować decyzje co do tego, gdzie i kiedy należy rozpocząć testowanie, a także identyfikować obszary wymagające większej uwagi. Celem testowania jest zmniejszenie prawdopodobieństwa wystąpienia niekorzystnego zdarzenia bądź ograniczenie jego wpływu. W związku z tym testowanie przyczynia się do łagodzenia ryzyka, a także dostarcza informacje na temat zidentyfikowanych czynników ryzyka — w tym ryzyka resztkowego (rezydualnego - ryzyko pozostające w testowanym obiekcie po podjęciu wszelkich możliwych bądź też wszelkich (ekonomicznie zasadnych) kroków zmierzających do jego uniknięcia, nie rozwiązanego).

Testowanie oparte na ryzyku a jakość produktu

Podejście do testowania oparte na ryzyku umożliwia prewencyjne obniżanie poziomu ryzyka produktowego. Jednym z elementów tego podejścia jest analiza ryzyka produktowego, która obejmuje identyfikowanie czynników tego typu ryzyka oraz szacowanie prawdopodobieństwa wystąpienia i wpływu każdego z nich. Uzyskane w ten sposób informacje na temat ryzyka produktowego można wykorzystać do planowania testów, specyfikowania, przygotowywania i wykonywania przypadków testowych oraz monitorowania i nadzorowania testów. Wczesna analiza ryzyka produktowego przyczynia się do powodzenia całego projektu.

Testowanie oparte na ryzyku a jakość produktu

W przypadku podejścia opartego na ryzyku wynik przeprowadzonej analizy ryzyka produktowego umożliwia:

- wskazanie odpowiednich technik testowania;
- określenie konkretnych typów testów, które należy wykonać (np. testy zabezpieczeń, testy dostępności);
- określenie zakresu wykonywanych testów;
- ustalenie priorytetów testowania w sposób sprzyjający jak najwcześniejszemu wykryciu defektów krytycznych;
- ustalenie, czy w celu zmniejszenia ryzyka należy wykonać inne czynności niezwiązane (np. przeprowadzić szkolenie dla niedoświadczonych projektantów).

Testowanie oparte na ryzyku a jakość produktu

Testowanie oparte na ryzyku pozwala skorzystać ze wspólnej wiedzy i spostrzeżeń interesariuszy projektu do przeprowadzenia analizy ryzyka produktowego. Aby zminimalizować prawdopodobieństwo awarii produktu, w ramach zarządzania ryzykiem wykonuje się usystematyzowane czynności obejmujące:

- analizowanie potencjalnych problemów (czynników ryzyka) i regularne dokonywanie ich ponownej oceny;
- ustalanie, które czynniki ryzyka są istotne i wymagają podjęcia działań;
- podejmowanie działań mających na celu złagodzenie ryzyka;
- tworzenie planów awaryjnych na wypadek faktycznego wystąpienia określonych czynników ryzyka.

Ponadto testowanie pozwala zidentyfikować nowe czynniki ryzyka, wskazać czynniki wymagające złagodzenia oraz zmniejszyć niepewność związaną z ryzykiem.

Ryzyka najczęściej zgłaszane przez testerów

- Problemy z dostępnością środowiska testowego
- Problemy z narzędziami lub dostępnością narzędzi.
- Brakująca lub niepełna dokumentacja.
- Niejasne lub często zmieniające się wymagania.
- Problemy z testowalnością.
- Problemy w zespole na linii tester-developer.
- Napięte harmonogramy, testy wymagają czasem większej uwagi.

Testowanie a ryzyko

Testowanie uwzględnia ryzyko na trzy następujące sposoby:
Testowanie ukierunkowane (*ang. targeted testing*)
Priorytetyzacja (*ang. prioritized testing*)
Raportowanie (*ang. reporting*)
Powyższe zdarzenia powinny występować podczas całego cyklu wytwarzania oprogramowania.

Tester a ryzyko

- Właścicielem ryzyka zawsze jest biznes, a nie zespół developerski.
- Biznes decyduje o akceptacji aktualnego poziomu ryzyka i jest zainteresowany, aby był na jak najniższym poziomie.
- Testerzy zapewniają obiektywne informacje interesariuszom biznesowym, właścicielowi produktu na temat poziomu ryzyka.
- Tester nie jest osobą decyzyjną, ale jego zadania powinny uwzględniać poziom dopuszczalnego ryzyka.

Ryzyko w testowaniu

Pojęcia ryzyka używa się dla zdecydowania gdzie zacząć testowanie i gdzie przetestować bardziej dogłębnie

Etapy rozpoznania ryzyka:

➔Identyfikacja ryzyk

➔Szacowanie wpływu ryzyk na projekt – ocena ryzyka

➔Plany redukujące ryzyka – łagodzenie ryzyka

➔Plany „B” – zarządzanie ryzykiem

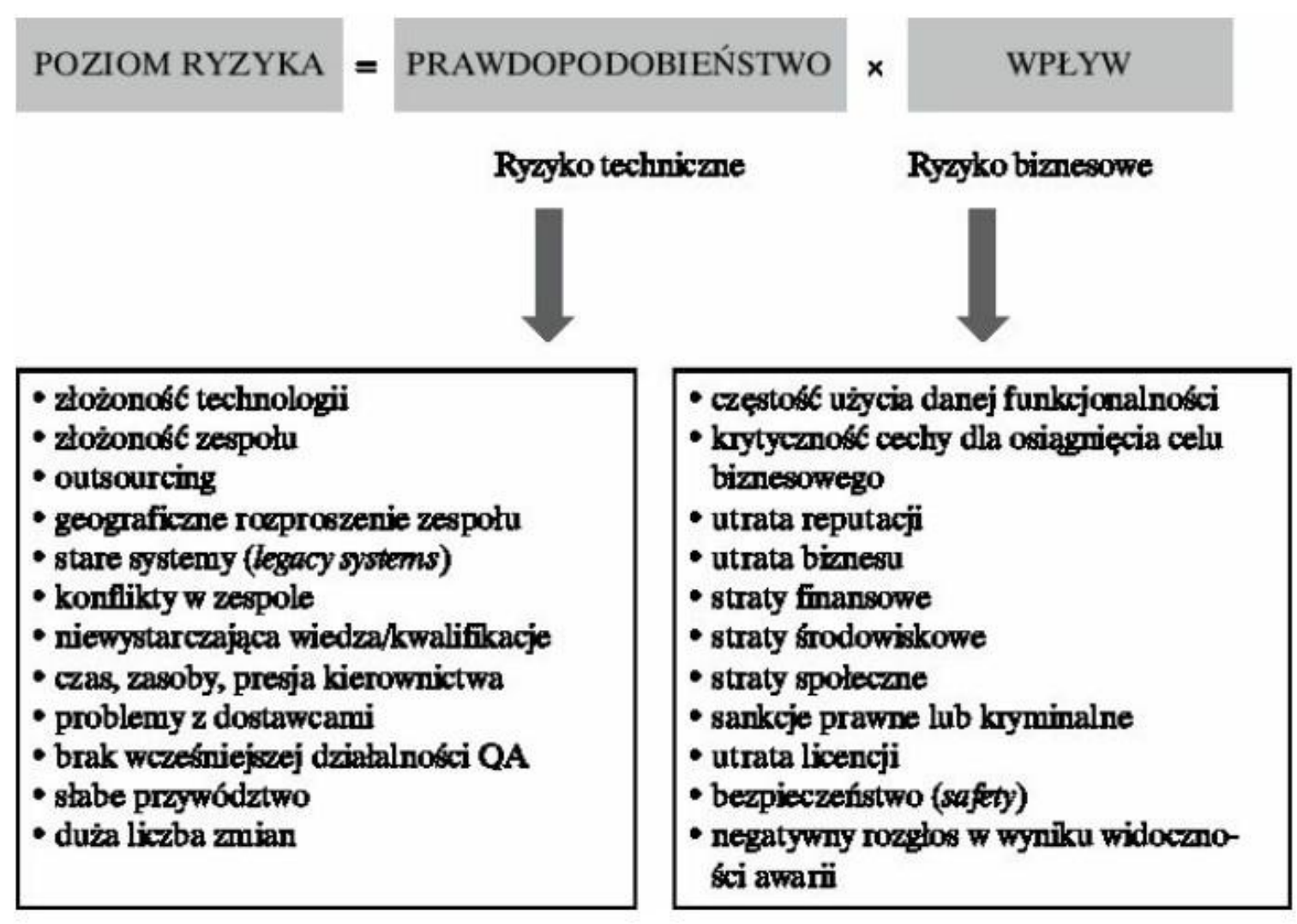
➔Wszystkie czynności testowe odnosimy do poziomu ryzyka

Ryzyko w testowaniu

Techniki identyfikacji:

- Rozmowy z ekspertami
- Niezależne oceny
- Wykorzystanie szablonów ryzyka
- Retrospektywy projektu
- Warsztaty dotyczące ryzyka
- Burza mózgów
- Listy kontrolne
- Odwołanie się do przeszłego doświadczenia

Ryzyko w testowaniu – ocena ryzyka



Ryzyko w testowaniu - łagodzenie

Łagodzenie ryzyka to proces, w którym podejmuje się decyzje i implementuje metryki w celu redukcji ryzyka lub utrzymania go na określonym poziomie.
Istnieją cztery główne sposoby łagodzenia ryzyka:
łagodzenie ryzyka (ang. *risk mitigation*) przez przedsięwzięcie czynności prewencyjnych, zapobiegających pojawieniu się ryzyka lub zmniejszających ich ewentualną dotkliwość;
plany awaryjne (ang. *contingency plans*) mające na celu zredukować siłę oddziaływania ryzyka, które rzeczywiście nastąpi;
transfer ryzyka (ang. *risk transfer*), czyli przeniesienie ryzyka na stronę trzecią (np. ubezpieczyciela), który będzie ponosił skutki ewentualnego wystąpienia ryzyka;
zignorowanie i zaakceptowanie ryzyka, które polega po prostu na tym, że nie podejmuje się żadnych akcji do momentu wystąpienia tego ryzyka.

Ryzyko w testowaniu – łagodzenie przez testowanie

Wykrywanie awarii pozwala na usunięcie defektu (potencjalnego źródła ryzyka)
Wykonanie testów daje nam informację o prawdopodobieństwie wystąpienia ryzyka
Poziom ryzyka wyznacza zakres i dokładność testowania

Jak testerzy mogą łagodzić ryzyko?

- priorytetyzacja testów według poziomu ryzyka; wykorzystywanie umiejętności najbardziej doświadczonych osób;
- wybór odpowiednich technik projektowania testów; przeprowadzanie szkoleń z testowania czy tworzenia testowalnego kodu o wysokiej jakości;
- przeprowadzanie przeglądów i inspekcji;
- przeprowadzanie przeglądów projektów testów;
- zdefiniowanie zakresu i intensywności testów regresji;
- stosowanie wczesnego prototypowania;
- automatyzowanie projektowania i wykonywania testów;
- uzyskanie określonego poziomu niezależności;

Ryzyko w testowaniu – łagodzenie przez testowanie

- Zarządzamy przez cały cykl życia projektu
- Sprawdzamy czy proces redukcji ryzyka przebiega prawidłowo
- Raportujemy, zgłaszamy do kierownictwa – podstawa decyzji o kolejnej fazie projektu oraz archiwizujemy dane

W związku z postępem projektu, lista ryzyk powinna być okresowo przeglądana i kierownik testów powinien dla każdego ryzyka produktowego przedyskutować następujące kwestie:

- czy dane ryzyko zostało prawidłowo oszacowane?
- czy czynności łagodzenia ryzyka (np. wykonanie testów) zostały przeprowadzone?
- jakie są efekty czynności łagodzących ryzyko (np. wyniki testów)?
- czy w stosunku do danego ryzyka należy przeprowadzić dodatkowe czynności, np. więcej testów?
- czy można dane ryzyko usunąć z listy ryzyk?
- dodanie nowych ryzyk do listy

Ryzyko w testowaniu – kiedy stosujemy?

W poniższych scenariuszach:

- Podejście RBT może być stosowane zawsze, gdy występuje ograniczenie czasu, kosztów i zasobów projektu oraz zawsze, gdy istnieje potrzeba optymalizacji zasobów.
- Podejście RBT jest stosowane, gdy program jest bardziej złożony i dostosowuje nową technologię, co wiąże się z wieloma wyzwaniami.
- Kiedy program jest projektem badawczo-rozwojowym i jest to projekt pierwszego rodzaju, a projekt zawiera szereg niewiadomych i zagrożeń.

Identyfikacja ryzyka

Identyfikacja ryzyka

W ramach czynności identyfikacji ryzyka, wykonuje się następujące działania:

- Możliwie najdokładniej określa się, co może pójść nie tak.
- Identyfikacja ryzyka jest to kluczowy etap, ponieważ w przeciwieństwie do następnych etapów, nie znamy liczby ryzyk.
- Identyfikacja ryzyk może dotyczyć różnych **typów ryzyk**, związanych z typem testów, których wykonywanie będzie minimalizować to ryzyko.
- Produktem końcowym etapu identyfikacji ryzyka jest lista ryzyk, która jest możliwie kompletna.

Analiza ryzyka

Po dokonaniu identyfikacji potencjalnych ryzyk należy je przeanalizować, to znaczy oszacować ich poziom, czyli efekty ich prawdopodobnego wystąpienia. O ile identyfikacja polega na dostarczeniu jak największej liczby ryzyk, o tyle analiza pozwala na ich skategoryzowanie, bądź uszeregowanie od najważniejszych do najmniej istotnych (priorytetyzacja).

Klasyfikacja ryzyka

Klasyfikacji ryzyka możemy dokonać na podstawie charakterystyk jakościowych oprogramowania:

- **funkcjonalność**
- **użyteczność**
- **niezawodność**
- **przenaszalność**
- **efektywność**

Łagodzenie ryzyka

Po określeniu ryzyk, ich poziomu, kategoryzacji oraz klasyfikacji, przystępuje się do kolejnego etapu — łagodzenia ryzyka. Etap ten polega na przygotowaniu planów mających na celu zapobieżenie w możliwie jak największym stopniu wystąpienia ryzyk oraz opracowania planów awaryjnych, gdyby jednak ryzyko wystąpiło w rzeczywistości.

Monitorowanie ryzyka

Po zaplanowaniu działań prewencyjnych oraz metod łagodzenia ryzyka, które rzeczywiście nastąpi, przechodzi się do fazy monitorowania. Polega ona na ciągłej obserwacji stanu systemu. Dzięki temu poziom ryzyka w produkcie jest widoczny na bieżąco. Dodatkowo następuje automatyczny proces kontroli ryzyka oraz procesów towarzyszących takich jak łagodzenie ryzyka. Poprzez pomiary możemy określić, czy uzyskaliśmy zadowalający poziom ryzyka.

Techniki testowania opartego na ryzyku – wybór technik

Podczas wyboru odpowiedniej techniki powinniśmy wziąć pod uwagę:

➢ dostępność zasobów oraz kwalifikacje personelu – niektóre metody wymagają doświadczenia w ich stosowaniu;
➢ czas poświęcony na wdrożenie oraz stosowanie metody;
➢ koszt (np. dodatkowe szkolenia czy koszt wynikający z czasu, jaki członkowie zespołu poświęcają na wykonywanie czynności wymaganych przez metodę);
➢ dostępność wymaganych przez metodę danych

Techniki testowania opartego na ryzyku – Analiza SWOT

Analiza SWOT to jedna z metod analitycznych przedsiębiorstwa. Cechuje ją prostota i szybkość zastosowania.
SWOT to w rzeczywistości akronim angielskich słów:
•**S** jak strengths – mocne strony
•**W** jak weaknesses – słabe strony
•**O** jak opportunities – szanse
•**T** jak threats – zagrożenia
Analiza SWOT to analiza mocnych i słabych stron oraz szans i zagrożeń przedsiębiorstwa.

Techniki testowania opartego na ryzyku – Analiza SWOT

Mocne strony to pozytywne czynniki wewnętrzne. Stanowią o wewnętrznej sile firmy. Należy o nie dbać, aby utrzymać je również w przyszłości. Mogą zostać wykorzystane do działań związanych z ekspansją firmy. Przykłady mocnych stron to:

•Wysokie kwalifikacje zatrudnionych pracowników
•Ponadprzeciętnie dobrze zorganizowana praca firmy (np. poprawnie wdrożone metodologie zarządzania)
•Duże zasoby finansowe zgromadzone w przeszłości

Słabe strony to negatywne czynniki wewnętrzne. Należy skupić się na ich eliminacji, aby nie osłabiły mocnych stron. Ograniczają one bowiem sprawność przedsiębiorstwa i hamują jego rozwój. Przykłady słabych stron to:

•Ograniczony proces produkcyjny, wpływający na niską jakość produktu
•Przestarzałe, awaryjne maszyny, które doprowadzają do przestoju w produkcji
•Duża rotacja pracowników

Techniki testowania opartego na ryzyku – Analiza SWOT

Szanse

Szanse to pozytywne zewnętrzne zjawiska i procesy, które mogą zostać wykorzystane do rozwoju i ekspansji firmy. Mogą również zniwelować słabe strony przedsiębiorstwa. Należy skupić się na tym, aby maksymalnie je wykorzystać. Przykładowe szanse to: wzrost popytu na oferowane przez przedsiębiorstwo produkty; otwarcie nowego rynku; zwiększenie się liczby mieszkańców miasta, w którym działa firma (więcej potencjalnych pracowników).

Zagrożenia

Zagrożenia to negatywne zewnętrzne zjawiska i procesy, które mogą blokować rozwój firmy. Należy skupić się na znalezieniu kroków zaradczych, aby zagrożenia nie wpłynęły na działalność firmy. Przykłady zagrożeń: zwiększenie się liczby zakładów pracy w miejscowości, w której działa firma (zagrożenie utraty pracowników); nowa konkurencja importująca produkty taniej niż wynosi ich produkcja w miejscu działalności firmy; zwiększenie podatków lub inne zmiany prawne.

Techniki testowania opartego na ryzyku – Analiza SWOT

Techniki testowania opartego na ryzyku – FMEA

FMEA (*ang. Failure Mode and Effect Analysis*) — analiza skutków i wad. Pionierem stosowania FMEA było w latach sześćdziesiątych NASA, realizujące program lotów kosmicznych „Apollo”. Metodą FMEA weryfikowano projekty różnych elementów statków kosmicznych, aby zapewnić bezpieczeństwo uczestnikom wyprawy. Po sukcesie w przemyśle kosmicznym, z FMEA skorzystał przemysł lotniczy i atomowy. W latach siedemdziesiątych i osiemdziesiątych metodę zaczęto wykorzystywać w Europie w przemyśle chemicznym, elektronicznym, a w szczególności w samochodowym. W połowie lat osiemdziesiątych metoda została przyjęta w branży motoryzacyjnej przez Ford Motor Company, który pracował razem z wybranymi dostawcami, ustalając doskonalenie projektowania i procesu produkcji.

Techniki testowania opartego na ryzyku – FMEA

W odniesieniu do architektury systemu FMEA polega na identyfikacji i analizie możliwych stanów uszkodzeń (failure modes) elementów systemu, wyznaczaniu wpływu, jakie te stany mogą mieć na działanie innych elementów i całego systemu, oraz na ocenie możliwych konsekwencji tego wpływu na środowisko zewnętrzne. Ocena możliwości wystąpienia (prawdopodobieństwa, częstotliwości) i skutków uszkodzeń systemu jest podstawą analizy krytyczności. Na tej podstawie ustalane są progi ryzyka dla systemu.

Techniki testowania opartego na ryzyku – kroki FMEA

Metoda FMEA pozwala w praktyce realizować jakościowe założenie **zero defektów**, a także potrzebę *ciągłego doskonalenia*. Metoda FMEA odpowiada na następujące pytania:

- Co jest celem projektowania?
- Czy produkt będzie odpowiadał oczekiwaniom przyszłych klientów?
- Czy zaprojektowany wyrób może być z powodzeniem produkowany?
- Co może ulec awarii?
- W jaki sposób produkt może ulec awarii?
- Jak często produkt będzie ulegał awarii?
- Jakie są konsekwencje awarii?
- Jak awaria wpływa na niezawodność/bezpieczeństwo systemu?

FMEA – cele formalne

W przypadku analizy FMEA można wyróżnić kilka celów formalnych:
•Konsekwentne i trwałe wyeliminowanie wad wyrobu (słabych miejsc wyrobu) przez rozpoznawanie rzeczywistych przyczyn ich powstania.
•Unikanie wystąpienia rozpoznanych, a także jeszcze nieznanych wad w nowych wyrobach i procesach przez wykorzystanie wiedzy i doświadczeń z już przeprowadzonych analiz.
Technika analizy FMEA pozwala na:
•Analizę przyczyn i skutków awarii
•Rozpoznanie i ocena potencjalnych awarii systemu oraz ich wpływu
•Analizę od najniższego poziomu szczegółowości

FMEA – kroki

Technika analizy FMEA dzieli się na kilka etapów:

- **Zdefiniowanie analizowanego systemu** — aby przeprowadzić jakąkolwiek analizę, należy dokładnie poznać system, jego architekturę, części składowe, interfejsy wewnętrzne oraz zewnętrzne.
- **Zdefiniowanie możliwych typów awarii oraz oszacowanie ich częstotliwości**
- **Analiza systemu** — identyfikacja potencjalnych przyczyn awarii oraz działań korekcyjnych
- **Identyfikacja metod detekcji awarii oraz działań korekcyjnych naprawczych lub prewencyjnych**
- **Określenie przyczyn awarii**, ich konsekwencji, przewidywanie niezawodności, lista zagrożeń i ryzyk oraz lista krytycznych elementów

Techniki testowania opartego na ryzyku – tabela FMEA

FMEA przeprowadzana jest zwykle przy użyciu arkusza kalkulacyjnego, w którym uzupełnia się tabelę FMEA. Istnieje wiele różnych wersji takiej tabeli, które różnią się poziomem szczegółowości niektórych informacji. Przykładowa tabela może zawierać następujące informacje:

- nazwa funkcji, w której może wystąpić awaria;
- możliwa awaria (ryzyko produktowe);
- możliwa przyczyna awarii;
- konsekwencje awarii;
- Pr. – prawdopodobieństwo wystąpienia awarii (ang. likelihood);
- W. – wpływ;
- Dotkl. – dotkliwość (ang. severity); w niektórych wersjach FMEA ten parametr się pomija;
- RPN – priorytet ryzyka (ang. Risk Priority Number), definiowany jako iloczyn: RPN = Pr · W · Dotkl;
- metoda wykrywania i zalecane czynności.

Techniki testowania opartego na ryzyku – tabela FMEA

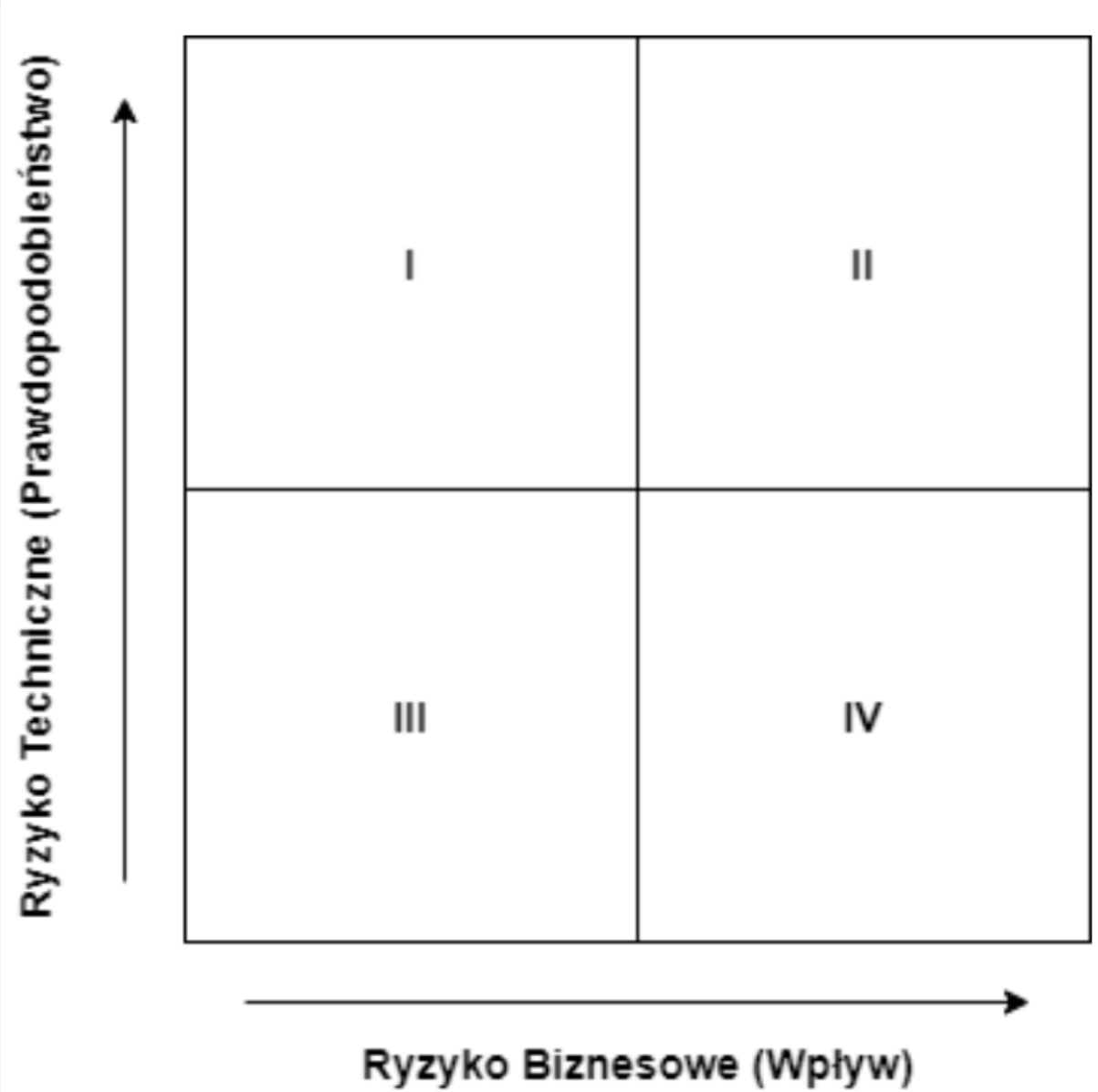
Funkcja	Możliwa awaria	Możliwa przyczyna awarii	Konsekwencje awarii	Pr.	W.	Dotkl.	RNP	Metoda wykrywania i zalecane czynności
System Plików	Fizyczne uszkodzenie	Mechaniczna	Utrata danych	5	1	1	5	Inspekcja oraz zabezpieczenie mechaniczne nośników danych
System Plików	Błąd odczytu	Błąd aplikacji	Wyświetlenie niepoprawnej informacji	4	3	2	24	Testowanie jakości oraz stosowanie technik białoskrzynkowych
Bazy Danych	Błąd zapisu	Naruszenie klucza	Brak możliwości operowania	5	3	3	45	Inspekcja projekt, struktury bazy, testowanie interfejsów
Zarządz. Kursami	Możliwość zduplikowania kursu	Błąd aplikacji w module ad	Redundantna informacja w bazie oraz być może na ekranie informacyjnym	2	5	4	40	Testowanie czarnoskrzynkowe
Wyświetlanie Informacji	Informacja niepełna lub błędna	Błąd aplikacji	Zmniejszenie użyteczności dla pasażera	3	3	1	9	Testowanie czarnoskrzynkowe, inspekcja funkcji getDisplayString
Ekran	Brak komunikacji z ekranem	Błąd sieci	Irytacja pasażerów	3	2	1	6	Kontrola infrastuktury sieciowej, okresowe przeglądy
Ekran	Awaria ekranu	Mechaniczne uszkodzenie	Irytacja pasażerów	4	2	1	8	Okresowe kontrole gotowości zespołu techników do szybkiej naprawy

Techniki testowania opartego na ryzyku – PRISMA

Product Risk Managment

Metoda PRiSMA została stworzona przez van Veenedaala. Jest to metoda lekka i prosta w zastosowaniu. Głównym elementem tej metody jest **macierz ryzyka produktowego** (*ang. product risk matrix*). Złożona z czterech kwadrantów, powstałych w wyniku podzielenia każdego z czynników ryzyka (prawdopodobieństwo, wpływ) na dwie grupy (wartości niskie, wartości wysokie).

Techniki testowania opartego na ryzyku – PRISMA



Każdy z kwadrantów określa inny typ ryzyka. Oznaczenia I, II, III oraz IV są to jedynie etykiety, nie mają one znaczenia liczbowego. Macierz ryzyka produktowego wraz z naniesionymi ryzykami, będzie dla interesariuszy bardziej zrozumiała niż lista ryzyk z przypisanymi do nich wartościami prawdopodobieństwa, wpływu oraz poziomu.

Techniki testowania opartego na ryzyku – PRISMA

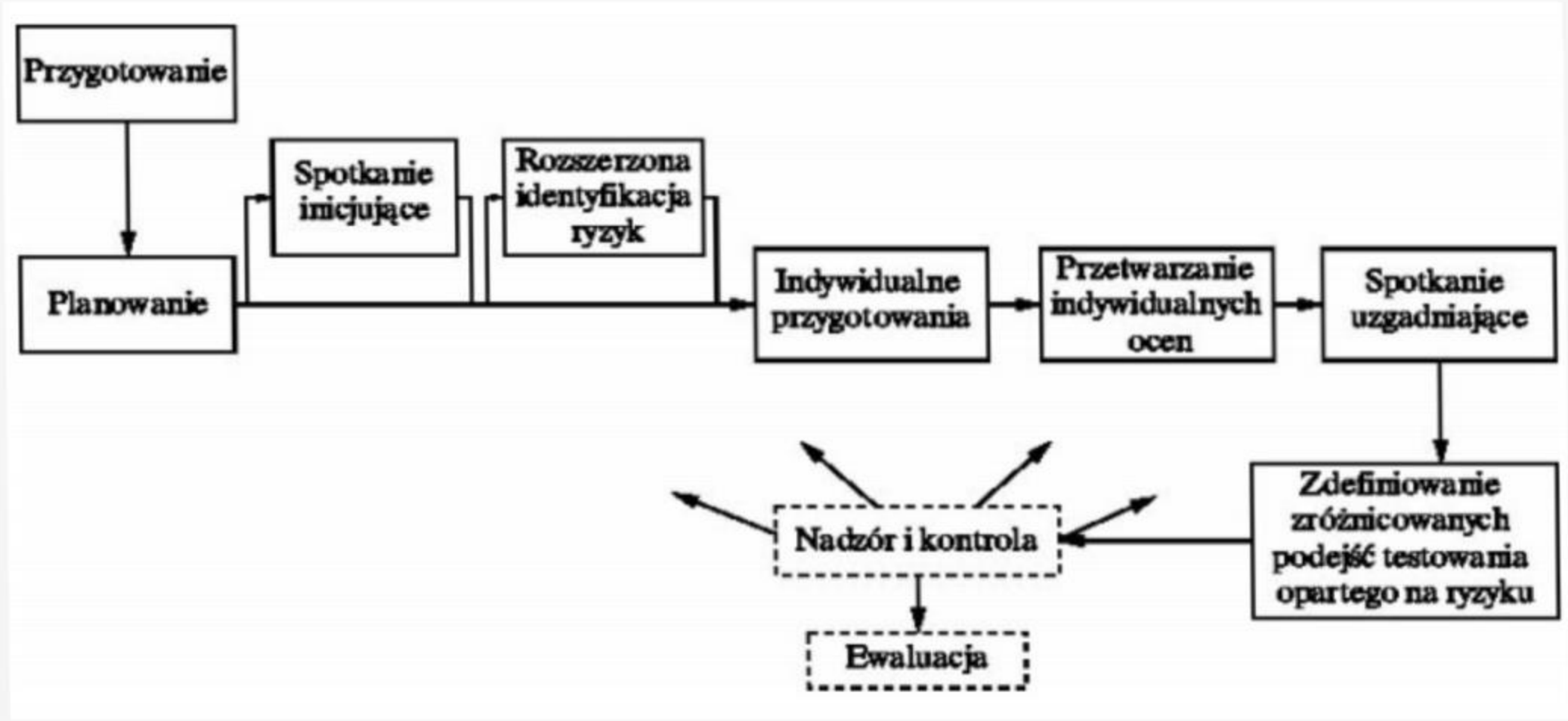
Czynniki dla wpływu:

- obszary krytyczne (identyfikowane na podstawie analizy użycia systemu oraz tego, w jaki sposób system może ulec awarii);
- obszary widoczne (czyli takie, w których użytkownicy mogą bezpośrednio odczuć awarię, jeśli coś pójdzie nie tak, jak trzeba);
- najczęściej używane obszary (podział funkcji na te, których użytkownicy używają zawsze, często, okazjonalnie lub rzadko i oszacowanie wpływu na podstawie tej klasyfikacji);
- istotność z biznesowego punktu widzenia (tzn. jaka jest ważność poszczególnych cech systemu z punktu widzenia biznesowego celu jego działania);
- koszt zmian (zwykle wykorzystywany w tzw. systemach systemów).

Czynniki dla prawdopodobieństwa:

- złożoność (np. w sensie złożoności cyklomatycznej, skomplikowanej logiki);
- liczba zmian (jest ona ważnym czynnikiem defektotwórczym);
- nowe technologie i metody;
- presja czasu;
- brak doświadczenia;
- rozproszenie geograficzne zespołu;
- kod nowy vs. re-używalny;
- interfejsy
- rozmiar
- historia defektów
- jakość wymagań

Techniki testowania opartego na ryzyku – PRISMA



Techniki testowania opartego na ryzyku – PRISMA

Faza przygotowania:
Obejmuje zdefiniowanie procesów oraz identyfikacje czynników ryzyka technicznego i biznesowego, ustalenie wag dla każdego czynnika, zdefiniowanie zakresu wykorzystywanej skali ocen oraz zdefiniowanie reguł w zakresie postępowania w procesie nadawania rangi i szacowania.
Ustalenie czynników dla wpływu:
•**Obszary krytyczne** — są identyfikowane na podstawie analizy użycia systemu oraz w jaki sposób system może ulec awarii.
•**Obszary widoczne** — obszary, które w przypadku awarii mają bezpośredni wpływ na użytkownika.
•**Najczęściej używane obszary** — podział funkcji na te, których użytkownicy używają najczęściej, często, okazjonalnie, rzadko, wcale i oszacowanie ich wpływu na podstawie tej klasyfikacji.
•**Istotność z biznesowego punktu widzenia** — jaka jest ważność poszczególnych cech systemu z punktu widzenia biznesowego.
•**Koszt zmian**

Techniki testowania opartego na ryzyku – PRISMA

Faza przygotowania:
Ustalenie czynników dla prawdopodobieństwa:
•**Złożoność** — złożoność cyklomatryczna (używana do pomiaru stopnia skomplikowania programu), skomplikowana logika
•**Liczba zmian** — ważny czynnik defektotwórczy
•**Nowe technologie i metody**
•**Presja czasu**
•**Brak doświadczenia**
•**Rozproszenie geograficzne zespołu**
•**Kod źrodłowy (nowy) vs kod źródłowy stary (reużywany, legacy)**
•**Interfejsy**
•**Poprzednio znalezione defekty**
•**Jakość wymagań**

Techniki testowania opartego na ryzyku – PRISMA

Faza planowania:

- Przeprowadzana przez kierownika testów, skupia się na następujących czynnościach:
- Zdefiniowanie zakresu produktu, który będzie poddawany analizie ryzyka.
- Dostrojenie czynników oraz reguł.
- Zebranie niezbędnej dokumentacji np. dokumentu wymagań czy projektu architektury.
- Identyfikacja ryzyk produktowych — bazuje na zbiorze wymagań oraz innych dostępnych dokumentach.
- Identyfikacja i wybór interesariuszy — zespół analizy ryzyka powinien być maksymalnie zróżnicowany umożliwiając różne punkty widzenia na jakość systemu.
- Przypisanie czynników do poszczególnych interesariuszy — nie każdy interesariusz musi oceniać poziom danego ryzyka. Oceniane powinny być elementy, które są ważne z jego (interesariusza) punktu widzenia..

Techniki testowania opartego na ryzyku – PRISMA

Spotkanie inicjujące (opcjonalnie):

- jego celem jest szczegółowe poinformowanie członków zespołu o planowanym procesie analizy ryzyka oraz uzyskanie odpowiedniego zaangażowania ludzi.

Techniki testowania opartego na ryzyku – PRISMA

Rozszerzona identyfikacja ryzyk (opcjonalnie):
Celem tego kroku jest rozszerzenie początkowego zbioru ryzyk określonego w fazie Planowania, a także wykrycie niezgodności między wymaganiami a ryzykami produktowymi. W tej fazie używa się głównie techniki *Burzy Mózgów*. Identyfikuje się dwa typy problemów:

- **Jest ryzyko, nie ma wymagania** — należy dodać wymaganie (aby wykryć defekty odpowiednio wcześnie) lub usunąć ryzyko (jeśli nie chcemy testować więcej niż to konieczne)
- **Jest wymaganie, nie ma ryzyka** — w takim przypadku należy rozszerzyć listę istniejących ryzyk (w celu uzyskania lepszego pokrycia testami) lub usunąć wymaganie (jeśli nie chcemy tworzyć więcej niż jest potrzebne)

Techniki testowania opartego na ryzyku – PRISMA

Faza indywidualnego przygotowania jego celem jest dostarczenie indywidualnych, niezależnych danych wejściowych do procesu analizy ryzyka oraz ocena czynników przypisanych poszczególnym ryzykom i przesłanie wyników do kierownika testów. Metoda PRiSMA wymaga, aby rozkład poszczególnych ocen dla każdego czynnika był możliwie równomierny, aby oceny nie skupiały się na granicach skali lub jednym konkretnym miejscu. Aby osiągnąć cel — trzeba dokonać analizy każdego ryzyka z osobna — dzięki czemu ułożą się według priorytetów od najważniejszych do najmniej ważnych.

Kierownik projektu	Wpływ		Prawdopodobieństwo	
Czynniki	WidOb	IstBiz	Złoż	NTech
Wagi	1,0	2,0	1,0	2,0
R1: brak komunikacji z ekranem	4	5	1	5
R2: niepoprawna informacja na ekranie	5	5	3	1
R3: niewygodny interfejs	2	1	1	2
R4: błędy w logice biznesowej	1	3	5	4
R5: wolne działanie systemu	2	4	4	4

Techniki testowania opartego na ryzyku – PRISMA

Przetwarzanie ocen indywidualnych
upewnienie się, że wszyscy interesariusze przesłali swoje oceny. Zebranie wszystkich ocen, stworzenie pierwszej roboczej wersji macierzy ryzyka. Weryfikuje się również reguły oceniania — każdą różnicę należy udokumentować oraz przygotować się do spotkania uzgadniającego.

Uśrednione oceny	Wpływ		Prawdopodobieństwo	
Czynniki	**WidOb**	**IstBiz**	**Złoż**	**NTech**
Wagi	**1,0**	**2,0**	**1,0**	**2,0**
R1: brak komunikacji z ekranem	4,5	4,0	2,0	5,0
R2: niepoprawna informacja na ekranie	5,0	5,0	4,0	1,0
R3: niewygodny interfejs	1,5	1,0	1,0	1,5
R4: błędy w logice biznesowej	2,0	2,5	4,5	4,0
R5: wolne działanie systemu	3,0	3,5	2,5	3,5

Techniki testowania opartego na ryzyku – PRISMA

Faza przetwarzania indywidualnych ocen. Liczymy ważoną ocenę:

Ryzyko	Wpływ	Prawdopodobieństwo
R1: brak komunikacji z ekranem	4,5+8,0=12,5	2,0+10,0=12,0
R2: niepoprawna informacja na ekranie	5,0+10,0=15,0	4,0+2,0=6,0
R3: niewygodny interfejs	1,5+2,0=3,5	1,0+3,0=4,0
R4: Błędy w logice biznesowej	2,0+5,0=7,0	4,5+8,0=12,5
R5: Wolne działanie systemu	3,0+7,0=10,0	2,5+7,0=9,5

Techniki testowania opartego na ryzyku – PRISMA

Spotkanie uzgadniające:
Następuje konfrontacja uczestników ze sposobami postrzegania ryzyk przez pozostałych członków zespołu. Dyskutuje się prawdopodobieństwa oraz wpływ poszczególnych ryzyk. W przypadku istnienia uwag (oceny indywidualne) — należy te uwagi przedyskutować oraz poprawić. Celem tej fazy jest uzyskanie możliwie najdalej idącego konsensusu. Wyróżnia się kilka technik uzyskiwania konsensusu:

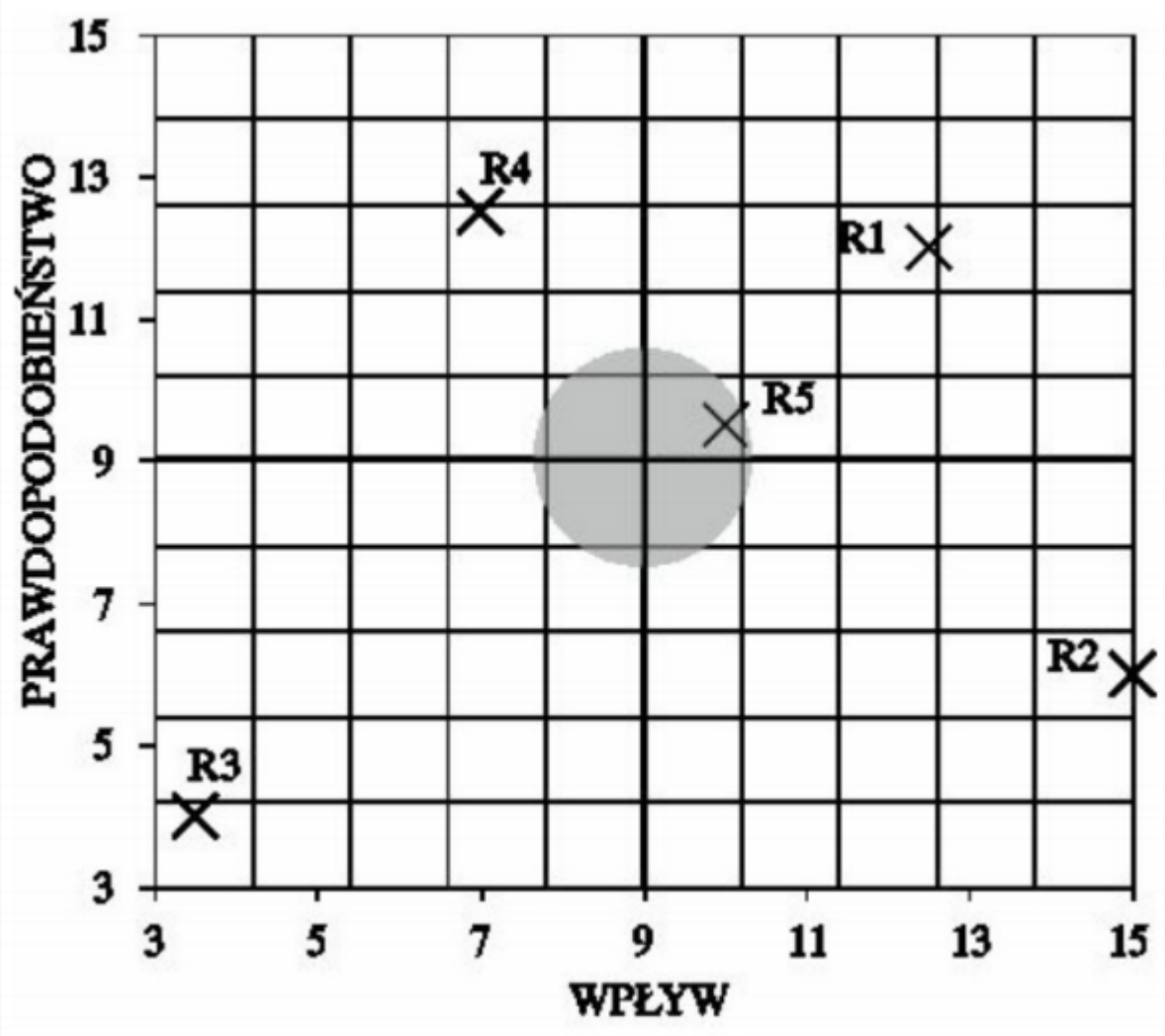
- **głosowanie,**
- **zaangażowanie eksperta,**
- **upoważnienie członka zespołu do podjęcia ostatecznej decyzji,**
- **przedyskutowanie sprawy,**
- **wybór surowszej oceny** — więcej pracy związanej z łagodzeniem ryzyka, szybszy konsensus.

Techniki testowania opartego na ryzyku – PRISMA

Zdefiniowanie zróżnicowanych technik podejść testowania opartego na ryzyku:
Celem tego kroku jest zdefiniowanie do podejścia zgodnego z pozycją poszczególnych ryzyk na macierzy ryzyka. Podejście musi spełniać kilka cech:
•**skuteczne** — koncentracja na najważniejszych ryzykach,
•**efektywne** — niemarnowanie czasu na długie testowanie ryzyk o niskim priorytecie,
•**czynności testowe są wykonywane w zgodzie z ryzykami produktowymi.**

Techniki testowania opartego na ryzyku – PRISMA

Macierz ryzyka produktowego:



Techniki testowania opartego na ryzyku – PRISMA

Metody łagodzenia ryzyka:

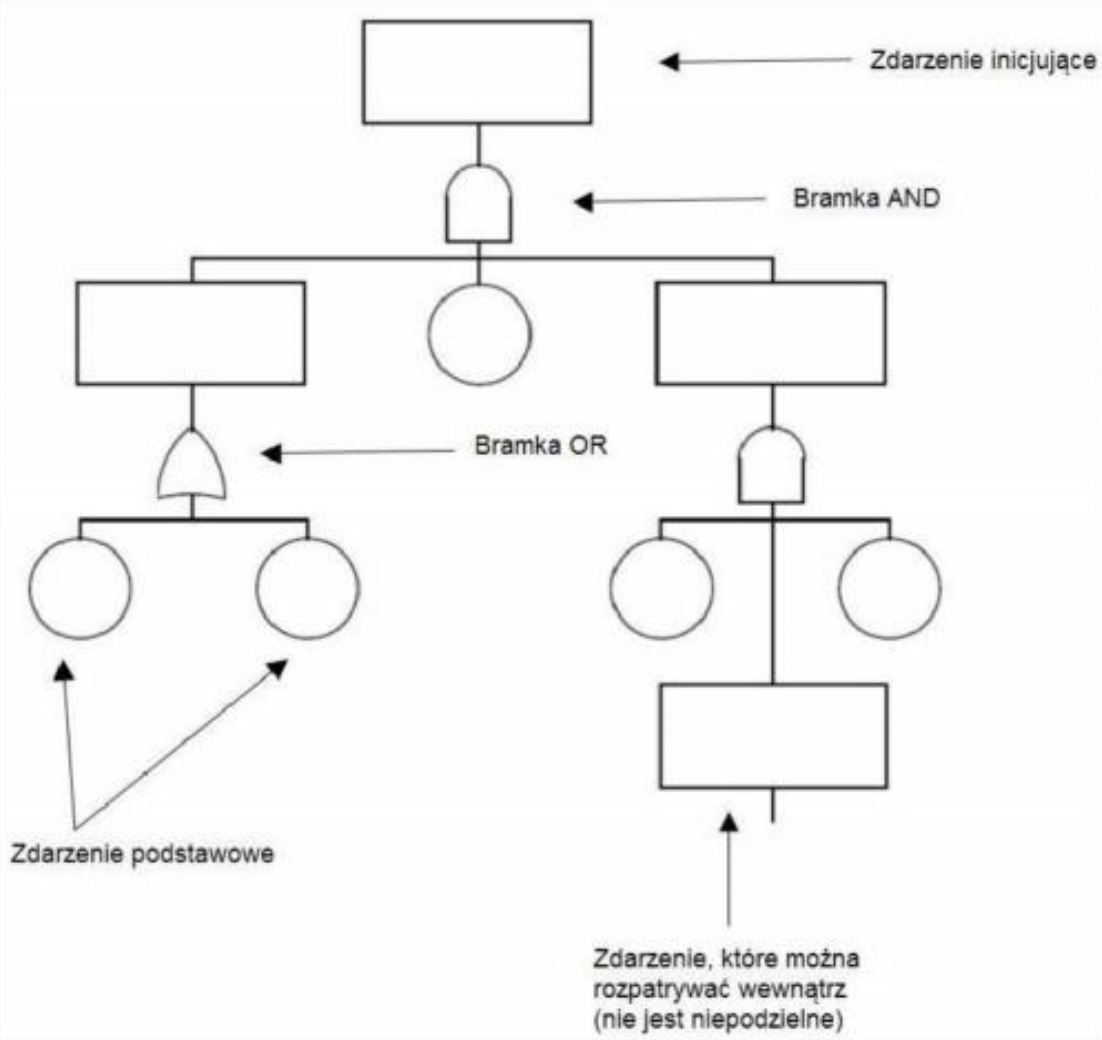
Ryzyko	Kwadrant	Wpływ	Prawdopodobieństwo	Metody łagodzenia
R1	II	wysoki	wysokie	wczesny prototyp systemu sprawdzający połączenie z ekranem
R2	IV	wysoki	niskie	testowanie białoskrzynkowe (kryterium MC/DC) oraz inspekcje kodu
R5	IV	wysoki	niskie	testy wydajnościowe, inspekcja projektu bazy danych
R4	I	niski	wysokie	testowanie eksploracyjne oraz testowanie oparte na przypadkach użycia
R3	III	niski	niskie	brak (poziom znikomy, nie ma potrzeby alokacji zasobów na testowanie tego ryzyka)

Techniki testowania opartego na ryzyku – FTA

- Analiza drzewa awarii
- Określa przyczyny źródłowe (root cause) awarii
- Określa prawdopodobieństwo niepożądanych zdarzeń
- Dobrze sprawdza się w przypadku dużych i skomplikowanych systemów, a także systemów o znaczeniu krytycznym
- W sposób graficzny prezentuje zależności pomiędzy kombinacjami zdarzeń
- Metoda dedukcyjna – top-down

Techniki testowania opartego na ryzyku – FTA

Przykładowe drzewo awarii:



5 x dlaczego?

Jest jedną z metod pozwalających na wykrywanie przyczyn problemów (lub defektów). Jest to zasada, którą stosujemy w celu ustalenia podstawowej przyczyny problemu. Zadawanie kilku pytań „Dlaczego?” pozwala dojść do źródła zakłóceń, gruntownie zbadać ich przyczynę i skupić się na ich skutecznym rozwiązywaniu. Dzięki zadawaniu pytań „Dlaczego?” problem staje się bardziej zrozumiały, przez co podstawowa przyczyna jego powstania jest łatwiejsza do zidentyfikowania i wyeliminowania. Analiza **5 Whys** pozwala odpowiedzieć na pytania:

- dlaczego powstał problem?
- dlaczego go nie zauważyliśmy?
- jak go rozwiązać?

5 x dlaczego? - zasady

Reguły i wskazówki pomocne do prawidłowego wykonania analizy[2]:
1.Konieczne jest prawidłowe sformułowanie i zapisanie problemu, a także jego zrozumienie przez uczestników.
2.Należy dbać o logikę ciągu przyczynowo-skutkowego oraz odróżnienie przyczyn od objawów. Aby upewnić się, że przyczyny źródłowe na pewno prowadzą do błędu, można odwrócić powstałe w analizie zdania za pomocą zwrotu „i dlatego”.
3.Analizę należy wykonywać krok po kroku, nie skakać do konkluzji. Przyczyn należy szukać w procesach, nie w ludziach. Błędem jest określać przyczynę źródłową jako „błąd ludzki”, „nieuwaga pracownika” itp..
4.Należy pytać „dlaczego”, aż do określenia przyczyny źródłowej, a zatem takiej, której eliminacja sprawi, że błąd już nie wystąpi.
5.Poleca się wykonywać analizę na papierze czy tablicy, zamiast na komputerze.
6.Niezbędne jest zaangażowanie kierownictwa, moderatora oraz prawidłowo dobranej grupy.
7.Ważna jest atmosfera szczerości i zaufania.

5 x dlaczego? - przykład

Problem – Nie wysłaliśmy biuletynu informującego o najnowszych aktualizacjach oprogramowania na czas.
1.Dlaczego nie wysłaliśmy biuletynu na czas? Aktualizacje nie zostały wdrożone do ostatecznego terminu.
2.Dlaczego aktualizacje nie zostały wdrożone na czas? Ponieważ programiści wciąż pracowali nad nowymi funkcjami.
3.Dlaczego programiści wciąż pracowali nad nowymi funkcjami? Jeden z nowych programistów nie znał procedur.
4.Dlaczego nowy programista nie znał wszystkich procedur? Nie był odpowiednio przeszkolony.
5.Dlaczego nie został odpowiednio przeszkolony? Ponieważ dyrektor ds. technicznych jest przekonany, że nowi pracownicy nie potrzebują dokładnych szkoleń i powinni się uczyć podczas pracy

5 x dlaczego? - przykład

1. **Dlaczego użytkownik skarżył się, że nie może skorzystać z funkcji „Wyślij e-mail” w naszej aplikacji?**

Ponieważ w najnowszym wydaniu był błąd.

2. **Dlaczego w najnowszej wersji był błąd?**

Ponieważ nie testowaliśmy tego scenariusza.

3. **Dlaczego nie przetestowaliśmy tego scenariusza?**

Ponieważ przetestowaliśmy tylko dogłębnie funkcje opracowane w bieżącym sprincie. Nie przeprowadziliśmy testów regresji dla wszystkich innych funkcji aplikacji.

4. **Dlaczego nie przetestowaliście wszystkich pozostałych funkcji aplikacji?**

Ponieważ „Wyślij e-mail” to funkcja, która została stworzona wcześniej, a nie w ramach bieżącego sprintu, więc testowanie wszystkich funkcji dla każdego wydania jest niepraktyczne.

5. Dlaczego uważacie, że testowanie wszystkich funkcji jest niepraktyczne?

Ponieważ nasza aplikacja jest tak obszerna, że ręczne wykonanie testów regresji dla każdej pojedynczej funkcji wymagałoby zbyt wiele czasu i opóźniłoby proces

Pytania, jakie warto zadać przed podjęciem decyzji co testujemy

- które elementy aplikacji mogą zostać przetestowane we wczesnej fazie?
- które części kodu/moduły są najbardziej skomplikowane i dlatego najbardziej narażone na wystąpienie błędów?
- która funkcjonalność jest najważniejsza z punktu widzenia zastosowania projektu? która funkcjonalność jest najbardziej widoczna dla klienta?
- które z wymagań zostały zmienione lub ogólnie zdefiniowane?
- która funkcjonalność ma największy wpływ na bezpieczeństwo aplikacji?
- która funkcjonalność ma największy wpływ na finanse?

Pytania, jakie warto zadać przed podjęciem decyzji co testujemy

- które elementy testowanej aplikacji mają największe znaczenie dla klienta?
- które aspekty podobnych, ukończonych poprzednio projektów powodowały problemy?
- które elementy podobnych, ukończonych projektów powodowały największe problemy w fazie utrzymania (maintenance)?
- co programiści uznają na najbardziej narażony na ryzyko element aplikacji?
- która część systemu była tworzona pod presją czasu?
- jaki rodzaj problemów może spowodować negatywną reakcję klienta?
- jaki rodzaj testów może pokryć możliwie najwięcej funkcjonalności?
- które z poprzednio wykonanych przypadków testowych powodowały wykrycie błędów? (test case value)

kowal.radek@gmail.com

https://www.linkedin.com/in/radoslaw-kowal/