

ANALIZA RYZYKA PROJEKTU IT

Metodyka PRINCE2 - Nowy oddział firmy outsourcingowej

Projekt: Infrastruktura IT dla 200 pracowników

Budżet całkowity: 6 046 397 zł brutto

Okres realizacji: 10 miesięcy

Data analizy: Czerwiec 2025

1. IDENTYFIKACJA RYZYK

1.1 Ryzyka finansowe

R001 - Przekroczenie budżetu projektu

- **Opis:** Całkowity budżet 6,05 mln zł brutto może zostać przekroczony
- **Kategoria:** Finansowe
- **Prawdopodobieństwo:** Średnie (35%)
- **Wpływ:** Wysoki (przekroczenie o 5-15% = 300-900k zł)
- **Przyczyny:**
 - Brak doświadczenia w projektach tej skali
 - Nieprzewidziane koszty integracji systemów
 - Wzrost cen sprzętu IT (inflacja)
 - Dodatkowe wymagania podczas wdrożenia

R002 - Wzrost kosztów licencji oprogramowania

- **Opis:** Roczne koszty OPEX (1,64 mln zł) mogą wzrosnąć w kolejnych latach
- **Kategoria:** Finansowe/Operacyjne
- **Prawdopodobieństwo:** Wysokie (65%)
- **Wpływ:** Średni (wzrost 10-20% rocznie = 164-328k zł)
- **Przyczyny:**
 - Naturalna inflacja cen licencji Microsoft, SAP
 - Dodatkowe moduły funkcjonalne
 - Wzrost liczby użytkowników
 - Zmiany w modelach licencjonowania (per user → per usage)

R003 - Wzrost kosztów maintenance

- **Opis:** Roczne koszty serwisu (745k zł) mogą wzrosnąć ponad założenia
- **Kategoria:** Finansowe/Operacyjne

- **Prawdopodobieństwo:** Średnie (45%)
- **Wpływ:** Średni (wzrost o 15-25% = 110-186k zł)
- **Przyczyny:**
 - Większe zużycie sprzętu niż przewidywane
 - Inflacja kosztów roboczej serwisu
 - Dodatkowe wymagania SLA

1.2 Ryzyka techniczne

R004 - Opóźnienia w dostawach sprzętu

- **Opis:** Laptopy, serwery i infrastruktura sieciowa mogą mieć dłuższe terminy dostaw
- **Kategoria:** Techniczne/Logistyczne
- **Prawdopodobieństwo:** Średnie (50%)
- **Wpływ:** Średni (opóźnienie 2-6 tygodni)
- **Przyczyny:**
 - Problemy w globalnych łańcuchach dostaw
 - Wysokie zapotrzebowanie na sprzęt IT
 - Specyficzne konfiguracje sprzętu
 - Procedury celne i logistyczne

R005 - Problemy kompatybilności systemów ERP

- **Opis:** Systemy księgowe (SAP/Comarch) mogą wymagać dodatkowej konfiguracji
- **Kategoria:** Techniczne/Integracyjne
- **Prawdopodobieństwo:** Średnie (35%)
- **Wpływ:** Wysoki (dodatkowe 150-300k zł + 3-6 tygodni)
- **Przyczyny:**
 - Złożoność integracji z istniejącymi systemami klientów
 - Wymagania compliance finansowe
 - Niestandardowe modyfikacje ERP
 - Problemy z migracją danych

R006 - Instalacja w przebudowanej hali magazynowej

- **Opis:** Adaptacja infrastruktury do specyfiki budynku
- **Kategoria:** Techniczne/Infrastrukturalne
- **Prawdopodobieństwo:** Średnie (40%)
- **Wpływ:** Średni (dodatkowe 50-150k zł + 1-3 tygodnie)
- **Przyczyny:**

- Nieoczekiwane problemy z okablowaniem strukturalnym
- Wymagania dodatkowych wzmocnień konstrukcyjnych
- Problemy z zasilaniem i klimatyzacją
- Konieczność dodatkowych pozwoleń budowlanych

R007 - Problemy z infrastrukturą Wi-Fi 6E

- **Opis:** Nowa technologia może wymagać dodatkowej optymalizacji
- **Kategoria:** Techniczne
- **Prawdopodobieństwo:** Niskie (25%)
- **Wpływ:** Średni (dodatkowe 30-80k zł + 1-2 tygodnie)
- **Przyczyny:**
 - Interference z istniejącymi sieciami
 - Problemy z pokryciem w specyficznej architekturze budynku
 - Konieczność fine-tuningu konfiguracji

1.3 Ryzyka harmonogramowe

R008 - Opóźnienia w realizacji (10 miesięcy)

- **Opis:** Harmonogram może ulec wydłużeniu z powodu koordynacji wielu dostawców
- **Kategoria:** Harmonogramowe
- **Prawdopodobieństwo:** Średnie (45%)
- **Wpływ:** Wysoki (opóźnienie 2-8 tygodni)
- **Przyczyny:**
 - Brak doświadczenia w zarządzaniu projektami IT tej skali
 - Koordynacja między wieloma dostawcami
 - Zależności między fazami projektu
 - Nieprzewidziane problemy techniczne

R009 - Dostępność wykwalifikowanych specjalistów

- **Opis:** Trudności w znalezieniu doświadczonych instalatorów i konfiguratorów
- **Kategoria:** Zasobowe
- **Prawdopodobieństwo:** Średnie (40%)
- **Wpływ:** Średni (opóźnienie 1-4 tygodnie + wzrost kosztów o 5-10%)
- **Przyczyny:**
 - Wysokie zapotrzebowanie na specjalistów IT
 - Wymagania specjalistycznej wiedzy (Cisco, SAP, bezpieczeństwo)
 - Konkurencja z innymi projektami

- Sezonowość dostępności (wakacje, święta)

R010 - Zależności od dostawców zewnętrznych

- **Opis:** Opóźnienia u kluczowych dostawców wpływają na cały projekt
- **Kategoria:** Harmonogramowe/Dostawcy
- **Prawdopodobieństwo:** Średnie (35%)
- **Wpływ:** Wysoki (opóźnienie 3-10 tygodni)
- **Przyczyny:**
 - Problemy finansowe dostawców
 - Przekierowanie zasobów na inne projekty
 - Siła wyższa (choroby, awarie)

1.4 Ryzyka operacyjne

R011 - Adaptacja 200 użytkowników

- **Opis:** Pracownicy będą potrzebowali czasu na przystosowanie się do nowych systemów
- **Kategoria:** Operacyjne/Ludzkie
- **Prawdopodobieństwo:** Wysokie (75%)
- **Wpływ:** Średni (spadek produktywności o 15-25% przez 2-6 miesięcy)
- **Przyczyny:**
 - Różny poziom kompetencji IT wśród pracowników
 - Opór przed zmianami
 - Skomplikowane procedury w nowych systemach
 - Równoczesne uruchomienie wielu systemów

R012 - Problemy z bezpieczeństwem cyberbezpieczeństwa

- **Opis:** Podatności w początkowej konfiguracji systemów
- **Kategoria:** Bezpieczeństwo
- **Prawdopodobieństwo:** Średnie (45%)
- **Wpływ:** Wysoki (potencjalne straty 100-500k zł + przestoje)
- **Przyczyny:**
 - Złożoność konfiguracji zabezpieczeń
 - Błędy ludzkie podczas instalacji
 - Nieaktualne patches i definicje
 - Targeted attacks na nową infrastrukturę

R013 - Problemy z zarządzaniem zmianą organizacyjną

- **Opis:** Opór przed nowymi procesami pracy i technologiami
- **Kategoria:** Organizacyjne
- **Prawdopodobieństwo:** Średnie (40%)
- **Wpływ:** Średni (obniżenie efektywności o 10-20% przez 3-9 miesięcy)
- **Przyczyny:**
 - Brak zaangażowania managementu
 - Niewystarczające komunikowanie korzyści
 - Przeciążenie pracowników nowymi narzędziami
 - Kultura organizacyjna oporna na zmiany

1.5 Ryzyka regulacyjne i compliance

R014 - Zmiany wymogów RODO i compliance finansowe

- **Opis:** Nowe regulacje mogą wymagać dodatkowych zabezpieczeń
 - **Kategoria:** Regulacyjne
 - **Prawdopodobieństwo:** Niskie (20%)
 - **Wpływ:** Średni (dodatkowe 50-200k zł)
 - **Przyczyny:**
 - Zmiany w przepisach UE dotyczących ochrony danych
 - Nowe wymagania nadzoru finansowego (KNF)
 - Zmiany w standardach branżowych
-

2. ANALIZA I OCENA RYZYK

2.1 Matryca ryzyk (uporządkowane według priorytetu)

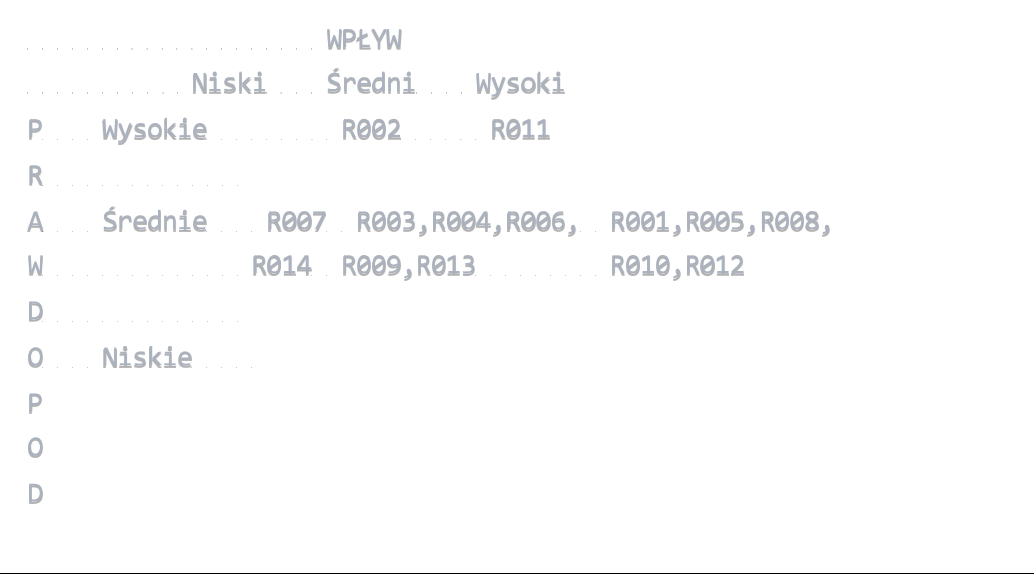
| Ryzyko | Prawdopodobieństwo | Wpływ | Poziom ryzyka | Priorytet |
|-----------------------------------|--------------------|--------|---------------|-----------|
| R011 - Adaptacja użytkowników | Wysokie (75%) | Średni | 🔴 Wysokie | 1 |
| R002 - Wzrost kosztów licencji | Wysokie (65%) | Średni | 🔴 Wysokie | 2 |
| R004 - Opóźnienia dostaw | Średnie (50%) | Średni | 🟡 Średnie | 3 |
| R008 - Opóźnienia realizacji | Średnie (45%) | Wysoki | 🔴 Wysokie | 4 |
| R012 - Problemy bezpieczeństwa | Średnie (45%) | Wysoki | 🔴 Wysokie | 5 |
| R003 - Wzrost kosztów maintenance | Średnie (45%) | Średni | 🟡 Średnie | 6 |
| R013 - Zarządzanie zmianą | Średnie (40%) | Średni | 🟡 Średnie | 7 |
| R006 - Instalacja w hali | Średnie (40%) | Średni | 🟡 Średnie | 8 |
| R009 - Dostępność specjalistów | Średnie (40%) | Średni | 🟡 Średnie | 9 |
| R001 - Przekroczenie budżetu | Średnie (35%) | Wysoki | 🔴 Wysokie | 10 |
| R005 - Kompatybilność ERP | Średnie (35%) | Wysoki | 🔴 Wysokie | 11 |
| R010 - Zależności dostawców | Średnie (35%) | Wysoki | 🔴 Wysokie | 12 |
| R007 - Problemy Wi-Fi 6E | Niskie (25%) | Średni | 🟢 Niskie | 13 |
| R014 - Zmiany regulacyjne | Niskie (20%) | Średni | 🟢 Niskie | 14 |

2.2 Tolerancja ryzyka

Progi tolerancji dla projektu:

- **Budżet:** +5% (302k zł) - 🟡 żółty, +10% (605k zł) - 🔴 czerwony
- **Harmonogram:** +2 tygodnie - 🟡 żółty, +6 tygodni - 🔴 czerwony
- **Funkcjonalność:** Opóźnienie > 2 miesiące - 🔴 czerwony
- **Bezpieczeństwo:** Jakiegokolwiek naruszenie danych - 🔴 czerwony

2.3 Mapa ciepła ryzyk



3. STRATEGIE ZARZĄDZANIA RYZYKAMI

3.1 Ryzyka wysokie - wymagają natychmiastowych działań

R011 - Adaptacja użytkowników ●

- **Strategia:** Ograniczanie (Mitigate)
- **Działania:**
 - Szkolenia podstawowe 3 tygodnie przed uruchomieniem
 - Power users w każdym dziale (20 osób) - szkolenia zaawansowane
 - Dokumentacja krok-po-kroku dla każdego systemu
 - Help Desk Level 1 przez pierwsze 6 miesięcy
 - Stopniowe wprowadzanie funkcjonalności (soft launch)
- **Odpowiedzialny:** Manager HR + IT Manager
- **Budżet:** 120k zł (dodatkowe szkolenia)

R008 - Opóźnienia realizacji ●

- **Strategia:** Ograniczanie (Mitigate)
- **Działania:**
 - Zatrudnienie doświadczonego Project Managera (zewnętrzny)
 - Bufor 15% w harmonogramie każdej fazy
 - Równoległa realizacja niezależnych zadań
 - Tygodniowe steering committee meetings
 - Plan awaryjny - fazowe uruchomienie (100+100 osób)
- **Odpowiedzialny:** Project Manager
- **Budżet:** 80k zł (PM + bufory)

R012 - Problemy bezpieczeństwa ●

- **Strategia:** Ograniczanie (Mitigate)
- **Działania:**
 - Security audit przed go-live (zewnętrzna firma)
 - Penetration testing po uruchomieniu
 - 24/7 SOC monitoring przez pierwszych 6 miesięcy
 - Backup systemów w trybie real-time
 - Cyber insurance dla infrastruktury IT
- **Odpowiedzialny:** CISO + Security Manager
- **Budżet:** 100k zł (audyt + monitoring)

R001 - Przekroczenie budżetu ●

- **Strategia:** Ograniczanie + Transfer (Mitigate + Transfer)
- **Działania:**

- Fixed-price contracts z dostawcami (95% wartości)
- Miesięczny monitoring kosztów vs. plan
- Approval workflow dla zmian > 10k zł
- Rezerwa budżetowa 8% (485k zł)
- Insurance coverage dla głównych dostawców
- **Odpowiedzialny:** CFO + Project Manager
- **Budżet:** Rezerwa 485k zł

R005 - Kompatybilność ERP

- **Strategia:** Ograniczanie (Mitigate)
- **Działania:**
 - POC (Proof of Concept) przed pełnym wdrożeniem
 - Dedykowany team integracyjny (SAP + Comarch specialists)
 - Sandbox environment dla testów
 - Fallback scenario - używanie istniejących systemów
- **Odpowiedzialny:** ERP Integration Lead
- **Budżet:** 150k zł (POC + specialists)

3.2 Ryzyka średnie - regularny monitoring

R004 - Opóźnienia dostaw

- **Strategia:** Ograniczanie (Mitigate)
- **Działania:**
 - Zamówienia sprzętu z 8-tygodniowym wyprzedzeniem
 - Alternatywni dostawcy dla 80% pozycji (Dell+HP+Lenovo)
 - Monitoring statusu dostaw co tydzień
 - Buffer stock dla krytycznych komponentów (10%)
- **Odpowiedzialny:** Procurement Manager
- **Budżet:** 50k zł (buffer stock)

R003 - Wzrost kosztów maintenance

- **Strategia:** Akceptacja + Monitoring
- **Działania:**
 - 3-letnie kontrakty maintenance z fixed pricing
 - SLA agreements z penalty clauses
 - Benchmark kosztów co 6 miesięcy
- **Odpowiedzialny:** Operations Manager

- **Budżet:** W ramach rezerwy

R006 - Instalacja w hali

- **Strategia:** Ograniczanie (Mitigate)
- **Działania:**
 - Detalijna inspekcja budynku przed rozpoczęciem
 - Konsultacje z architektem konstrukcji
 - Flexible cabling solutions (raised floor alternatywy)
- **Odpowiedzialny:** Infrastructure Manager
- **Budżet:** 40k zł (konsultacje + adaptacje)

3.3 Ryzyka niskie - podstawowy monitoring

R007 - Problemy Wi-Fi 6E

- **Strategia:** Akceptacja + Monitoring
- **Działania:**
 - Site survey przed instalacją
 - Professional installation przez certified engineers
 - Performance monitoring przez pierwsze 3 miesiące

R014 - Zmiany regulacyjne

- **Strategia:** Akceptacja
- **Działania:**
 - Quarterly compliance reviews
 - Subscription do regulatory updates
 - Flexible architecture umożliwiającą adaptacje

4. PLANY AWARYJNE (CONTINGENCY)

4.1 Scenariusz 1: Opóźnienie realizacji > 6 tygodni

Trigger: Kumulacyjne opóźnienie przekracza 6 tygodni **Działania:**

- Uruchomienie fazowe: Faza 1 (100 osób) → Faza 2 (100 osób)
- Temporary workspace z podstawową infrastrukturą
- Praca zdalna dla części zespołów z company laptops
- Przyspieszenie dostaw kluczowych komponentów (express delivery) **Budżet:** 200k zł (temporary solutions)

4.2 Scenariusz 2: Przekroczenie budżetu > 15%

Trigger: Prognozowane przekroczenie budżetu o > 900k zł **Działania:**

- Redukcja scope do minimum viable product (MVP)
- Postponement części funkcjonalności na fazę 2
- Renegocjacje z dostawcami (volume discounts)
- Alternative financing (leasing zamiast zakupu) **Oszczędności:** 300-600k zł

4.3 Scenariusz 3: Krytyczne problemy bezpieczeństwa

Trigger: Wykrycie poważnych podatności lub breach **Działania:**

- Immediate isolation affected systems
- Emergency security team activation
- Rollback do poprzedniej konfiguracji
- External security forensics
- Customer notification protocol (24h) **Budżet:** 150k zł (emergency response)

4.4 Scenariusz 4: Problemy z adaptacją użytkowników

Trigger: Spadek produktywności > 30% po 4 tygodniach **Działania:**

- Intensive coaching sessions (1:1)
- Simplified workflows implementation
- Extended parallel running ze starymi systemami
- Additional training materials (video, interactive) **Budżet:** 80k zł (dodatkowe szkolenia)

5. MONITORING I KONTROLA

5.1 Kluczowe wskaźniki ryzyka (KRI)

| Wskaźnik | Próg żółty | Próg czerwony | Częstotliwość monitoringu |
|-------------------------|----------------|----------------|---------------------------|
| Odchylenie budżetu | >3% | >8% | Tygodniowo |
| Opóźnienie harmonogramu | > 1 tydzień | >4 tygodnie | Tygodniowo |
| Opóźnienie dostaw | >25% pozycji | >50% pozycji | Tygodniowo |
| Problemy techniczne | >5/tydzień | >15/tydzień | Dziennie |
| Security incidents | >2/miesiąc | >1 critical | Real-time |
| User adoption rate | <70% po 4 tyg. | <50% po 8 tyg. | Tygodniowo |
| System uptime | <99% | <97% | Real-time |
| Integration issues | >3/tydzień | >10/tydzień | Dziennie |

5.2 Raportowanie ryzyk

Estructura raportów:

- **Daily standups:** Kluczowe ryzyka operacyjne
- **Weekly risk reports:** Status wszystkich średnich i wysokich ryzyk
- **Monthly steering committee:** Pełny risk dashboard + trend analysis
- **Quarterly risk reviews:** Update risk register + nowe ryzyka

Responsiblity matrix:

- **Project Manager:** Overall risk management, reporting, escalation
- **Risk Manager:** Risk register maintenance, analysis, recommendations
- **Department Heads:** Departmental risk identification, mitigation execution
- **Steering Committee:** Risk acceptance, budget approval, strategic decisions

5.3 Eskalacja ryzyk

Level 1 - Project Team (do 50k zł impact)

- **Czas reakcji:** 24h
- **Decyzje:** Operational mitigations, minor budget reallocations

Level 2 - Steering Committee (50-200k zł impact)

- **Czas reakcji:** 48h
- **Decyzje:** Budget increases, scope changes, vendor changes

Level 3 - Executive Board (>200k zł impact)

- **Czas reakcji:** 72h
- **Decyzje:** Major budget increases, project cancellation, strategic pivots

6. BUDŻET ZARZĄDZANIA RYZYKAMI

6.1 Alokacja budżetu ryzyka

Całkowity budżet zarządzania ryzykami: 1 025 000 zł

| Kategoria | Budżet (zł) | % całości | Przeznaczenie |
|--------------------------|-------------|-----------|---|
| Rezerwa budżetowa | 485 000 | 47.3% | Nieprzewidziane koszty, przekroczenia |
| Security & Compliance | 250 000 | 24.4% | Audyty, monitoring, cyber insurance |
| Change Management | 120 000 | 11.7% | Dodatkowe szkolenia, coaching |
| Contingency operations | 100 000 | 9.8% | Temporary solutions, express deliveries |
| Risk management overhead | 70 000 | 6.8% | Risk manager, monitoring tools, reporting |

6.2 Risk-adjusted budget

Oryginalny budżet: 6 046 397 zł

Risk management: 1 025 000 zł

Total project budget: 7 071 397 zł

Probability-weighted expected costs:




- P90 (90% confidence): 6 850 000 zł
 - P75 (75% confidence): 6 450 000 zł
 - P50 (median): 6 150 000 zł
-

7. WNIOSKI I REKOMENDACJE

7.1 Ocena ogólna ryzyka projektu

Poziom ryzyka:  **ŚREDNI do WYSOKIEGO**

Projekt charakteryzuje się **umiarkowanym do wysokiego ryzyka** ze względu na:





-  **Pozytywne:** Sprawdzone technologie, doświadczeni dostawcy, jasne wymagania biznesowe
-  **Wyzwania:** Duża skala (200 użytkowników), złożoność integracji, nowa lokalizacja
-  **Ryzyka:** Change management, cybersecurity, budget overrun

7.2 Kluczowe czynniki sukcesu





1. **Doświadczony Project Manager** z track record w projektach IT 100M+
2. **Zaangażowanie top management** w change management
3. **Proactive risk monitoring** z weekly reviews
4. **Security-first approach** od początku projektu
5. **Flexible scope management** z fazowaniem w razie problemów

7.3 Główne rekomendacje





NATYCHMIAST (przed rozpoczęciem):

-  Zatrudnienie dedykowanego Risk Managera
-  Zabezpieczenie budżetu awaryjnego 1M zł
-  Podpisanie insurance coverage dla cyber risks
-  Ustalenie contingency plans z dostawcami

W TRAKCIE PROJEKTU:

-  Tygodniowy monitoring KRI indicators
-  Agile approach z możliwością pivoting
-  Security audits na każdym etapie
-  Intensive change management od początku

PO URUCHOMIENIU:

-  6-miesięczny hypercare support
-  Continuous risk monitoring
-  Lessons learned documentation
-  Benefits realization tracking

7.4 Go/No-Go rekomendacja

 **PROJEKT REKOMENDOWANY** pod warunkiem:

1. **Budżet awaryjny:** Zabezpieczenie 1M zł rezerwy (15% base budget)
2. **Timeline buffer:** Dodanie 15% buforu czasowego (1.5 miesiąca)
3. **Risk management:** Dedicated risk manager przez cały projekt
4. **Change readiness:** Intensive change management program
5. **Security priority:** Security-by-design approach

Prawdopodobieństwo sukcesu przy spełnieniu warunków: 78%

Dokument przygotowany: Czerwiec 2025
Metodyka: PRINCE2 Risk Management
Następna aktualizacja: Co miesiąc w trakcie realizacji
Status: FINAL v1.0

ZAŁĄCZNIKI

- Załącznik A:** Risk Register (szczegółowy)
Załącznik B: Risk Heat Map (wizualizacja)
Załącznik C: Contingency Plans (szczegółowe procedury)
Załącznik D: KRI Dashboard Template
Załącznik E: Risk Escalation Procedures