

Efektywne zarządzanie projektami zabezpieczeń systemów informatycznych w oparciu o metodę PRINCE2™

**dr inż. Mariusz Stawowski
CLICO Sp. z o.o.**

Plan wystąpienia

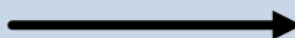
- Wprowadzenie
- Problemy organizacyjne projektów zabezpieczeń
- Praktyczne aspekty zastosowania metody PRINCE2™
- Podsumowanie



Wprowadzenie

- Raporty nt. incydentów bezpieczeństwa oraz wykonywane w polskich przedsiębiorstwach audyty bezpieczeństwa pokazują, iż w wielu systemach informatycznych pomimo wdrożenia kosztownych produktów zabezpieczeń wartościowe zasoby IT nie są właściwie chronione.
- Częstym tego powodem jest źle wykonany projekt zabezpieczeń.
- Błędy projektu zabezpieczeń sprawiają, że zastosowane w systemach informatycznych środki ochrony nie wykonują poprawnie swoich zadań, a jedynie sprawiają mylne poczucie bezpieczeństwa.

OPRACOWANIE DOKUMENTU PROJEKTU



WDROŻENIE ZABEZPIECZEŃ

1.	SPRECYZOWANIE ZAŁOŻEŃ PROJEKTU ORAZ ZEBRANIE DANYCH O SYSTEMIE INFORMATYCZNYM
2.	ANALIZA RYZYKA I SPECYFIKACJA WYMAGAŃ BEZPIECZEŃSTWA
3.	OPRACOWANIE ARCHITEKTURY ZABEZPIECZEŃ SIECI
4.	WYBÓR PRODUKTÓW DO WDROŻENIA PROJEKTU ORAZ USTALENIE WYTYCZNYCH DO INSTALACJI I KONFIGURACJI ZABEZPIECZEŃ
5.	OPRACOWANIE INFRASTRUKTURY ZARZĄDZANIA ZABEZPIECZEŃ
6.	USTALENIE WYMAGAŃ I ODPOWIEDZIALNOŚCI PERSONELU OBSŁUGI
7.	OPRACOWANIE ZASAD ZARZĄDZANIA ZABEZPIECZEŃ I OBSŁUGI INCYDENTÓW
8.	OPRACOWANIE PLANU TESTÓW AKCEPTACYJNYCH

1.	INSTALACJA ORAZ KONFIGURACJA ZABEZPIECZEŃ I SYSTEMU ZARZĄDZANIA
2.	SZKOLENIA KADRY IT
3.	OPRACOWANIE DOKUMENTACJI PO-WYKONAWCZEJ
4.	OPRACOWANIE INSTRUKCJI ZARZĄDZANIA ZABEZPIECZEŃ I OBSŁUGI INCYDENTÓW
5.	TESTY AKCEPTACYJNE
6.	DOSTROJENIE KONFIGURACJI ZABEZPIECZEŃ
7.	UZUPEŁNIENIE DOKUMENTACJI I ODDANIE ZABEZPIECZEŃ DO EKSPLOATACJI



ŚRODOWISKO PROJEKTU

- INTERESARIUSZE (BIZNES, UŻYTKOWNICY, DOSTAWCY)
- KONKURENCJA, INNE PROJEKTY, ...

Brak odpowiedniej współpracy i niedostateczne zaangażowanie kierownictwa firmy i użytkowników produktów projektu (administratorów zabezpieczeń)

- Pracownicy firmy nie zgadzają się na wdrożenie zaleceń projektu (np. zablokowanie GG, odebranie praw administratora, itp.)
- Przekroczony czas realizacji projektu (np. brak wymaganego wsparcia lokalnych administratorów, interpretacja wymagań została zmieniona w czasie realizacji projektu).

Brak odpowiedniej współpracy i niedostateczne zaangażowanie kierownictwa firmy i użytkowników produktów projektu (administratorów zabezpieczeń)

- Często projektant/integrator unika kontaktu z klientem – uważa, że wie od niego lepiej jakich zabezpieczeń potrzebuje.
- Wdrożone zabezpieczenia nie odpowiadają wymaganiom klienta (np. niedokładnie zdefiniowane produkty końcowe projektu, zbyt wygórowane wymagania, klient nie otrzymał odpowiednich narzędzi, dokumentów i szkoleń).

Brak jasno określonych celów biznesowych, koncentracja na IT

- Problem z uzyskaniem budżetu (np. na szkolenia, na audyt)
- Wdrożony projekt nie ma uzasadnienia biznesowego (np. koszt wdrożona zabezpieczeń przekracza wartość chronionych zasobów).

Brak jasno określonych celów biznesowych, koncentracja na IT

- Rozwój systemu informatycznego będzie wymagał dużych nakładów na modyfikację/rozbudowę wdrożonych zabezpieczeń (brak skalowalności).
- Brak jednomyślności i spory pomiędzy interesariuszami projektu (klient - dostawca, także wewnątrz firmy klienta, np. dział IT i dział bezpieczeństwa).

Oszczędności na analizie wymagań - zabezpieczenia ustalone bez analizy ryzyka, tylko w oparciu o „dobre praktyki”

- Wdrożone zabezpieczenia są nieadekwatne do rzeczywistych potrzeb (np. kosztowne zabezpieczenia zostały wdrożone pomimo występowania niewielkiego ryzyka, zaś dla istotnych zagrożeń środki ochrony nie zostały wdrożone).
- Niewłaściwe wykorzystanie budżetu (np. zakup urządzeń o zbyt dużej wydajności lub niepotrzebnych funkcjach, a brak środków na narzędzia raportowania i szkolenia kadry IT).
- Brak analizy wymagań w zakresie utrzymania ciągłości działania.

Niedostateczna kontrola zmian konfiguracji*

- Tymczasowe ustawienia konfiguracji zabezpieczeń zostają oddane do eksploatacji.
- Zabezpieczenia zostają tymczasowo wyłączone w czasie ustalania przyczyn nieprawidłowego działania aplikacji.

****Przykłady z audytów:***

1. W systemie bankowości internetowej strefa DMZ została tymczasowo połączona ze strefą wewnętrzną.

2. W sieci LAN instytucji finansowej moduły FW/IPS w switchach zostały wyłączone na skutek problemów wydajnościowych działania aplikacji.

Niedostateczna kontrola jakości - w konsekwencji błędy projektu i implementacji zabezpieczeń wychodzą dopiero w trakcie eksploatacji

- Do wdrożenia projektu zostały użyte produkty o nieodpowiedniej jakości* (stabilności, wydajności, itp.).
- Do realizacji projektu zostali zaangażowani wykonawcy o niedostatecznych kwalifikacjach.

***Przykład:**

Urządzenia UTM zastosowane w Centrum Danych. Zablokowanie modułu IPS w UTM spowodowało niedostępność usług Centrum Danych przez ponad 24 godziny.

Niedostateczna kontrola jakości - w konsekwencji błędy projektu i implementacji zabezpieczeń wychodzą dopiero w trakcie eksploatacji

- Niewłaściwie zdefiniowane testy akceptacyjne, skoncentrowane na identyfikacji podatności chronionych zasobów, a nie weryfikacji poprawności działania wdrożonych zabezpieczeń.
- Audyt wykonany niezależnie, po zakończeniu projektu zabezpieczeń, wykazuje słabości ale projektu nie można już zmienić.

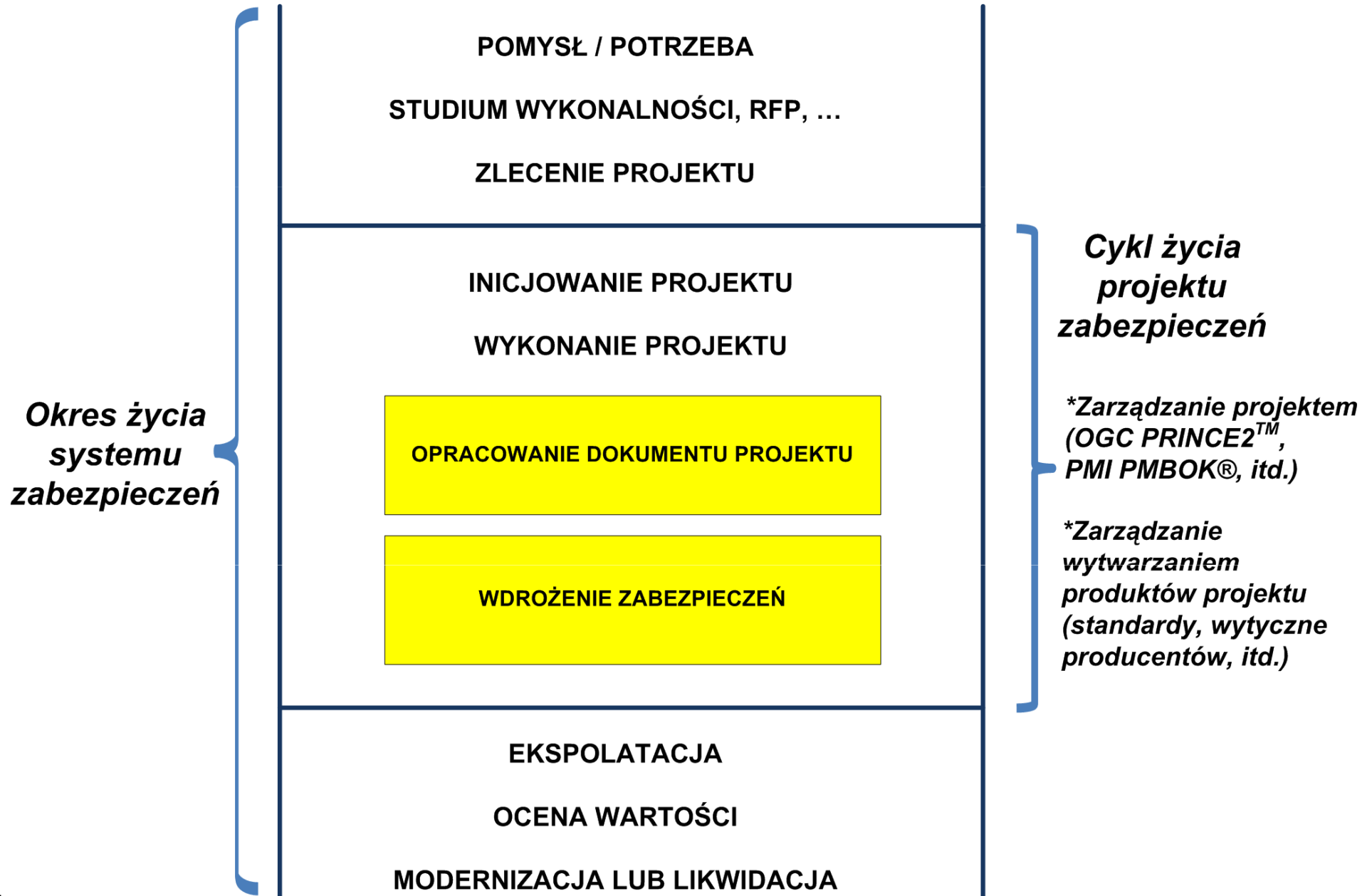
Zarządzanie projektem

- PRINCE2™ (Projects In a Controlled Environment).
- Własność brytyjskiego Office of Government Commerce (OGC).
- Uniwersalna metoda zarządzania projektami.
- Zastosowanie w projektach dowolnego rodzaju i wielkości.
- Łatwo dopasowuje się do środowiska projektu.



Wykład omawia praktyczne aspekty zastosowania metody PRINCE2™ w projektach zabezpieczeń systemów informatycznych.

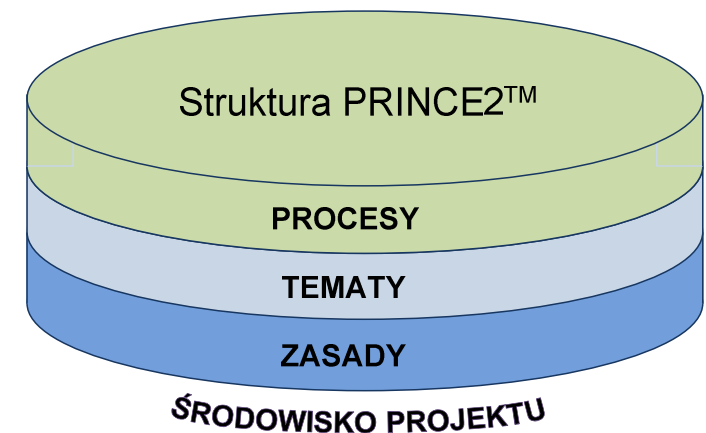
Zarządzanie projektem



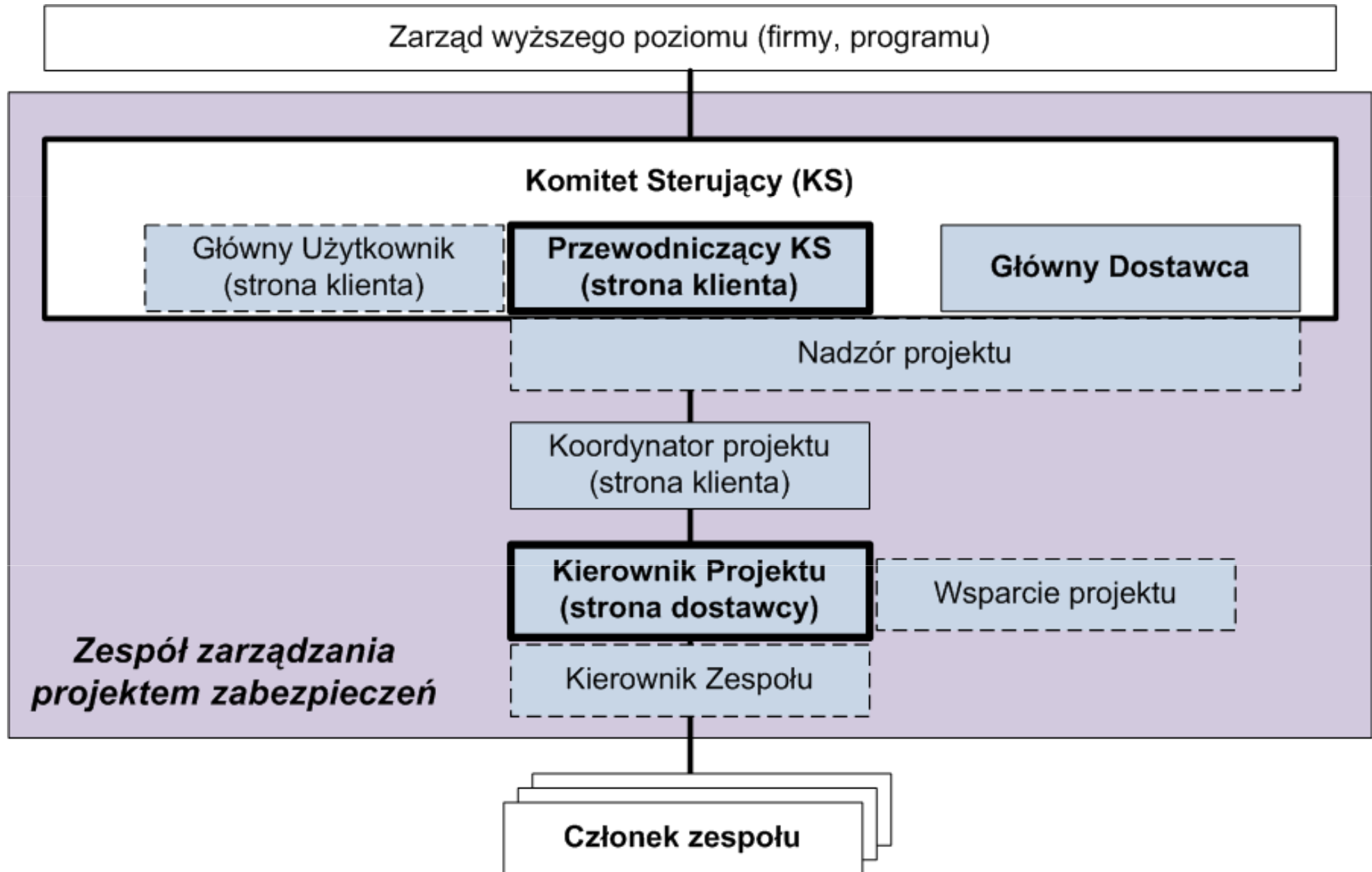
Zarządzanie projektem

PRINCE2™ to strukturalna metoda zarządzania projektami:

- **Zasady (*Principles*)** - muszą być przestrzegane przez cały czas trwania projektu (np. stałe uzasadnienie biznesowe, skoncentrowanie na produktach).
- **Tematy (*Themes*)** - odnoszą się do kluczowych aspektów projektu - uzasadnienie biznesowe, organizacja, jakość, plany, ryzyko, zmiany i postęp.
- **Procesy (*Processes*)** - to czynności jakie należy wykonać w ramach zarządzania projektem (np. inicjowanie projektu, zarządzaniem etapem, zamykanie projektu).
- **Środowisko projektu (*Project environment*)** - PRINCE2™ to metoda ogólna, którą należy dostosować do środowiska projektu, m.in. rozmiaru i skomplikowania projektu, typu projektu, specyfiki firmy, itd.



Zespół zarządzania projektem



Uzasadnienie biznesowe (*Business Case*)

- Powody realizacji projektu, ustalone na podstawie oszacowania kosztów, ryzyka i spodziewanych zysków.
- W PRINCE2™ uzasadnienie biznesowe jest tworzone przed rozpoczęciem projektu, a w czasie trwania projektu uszczegóławiane i weryfikowane.

Uzasadnienie biznesowe dostawcy nie pokrywa się z uzasadnieniem biznesowym klienta (?)

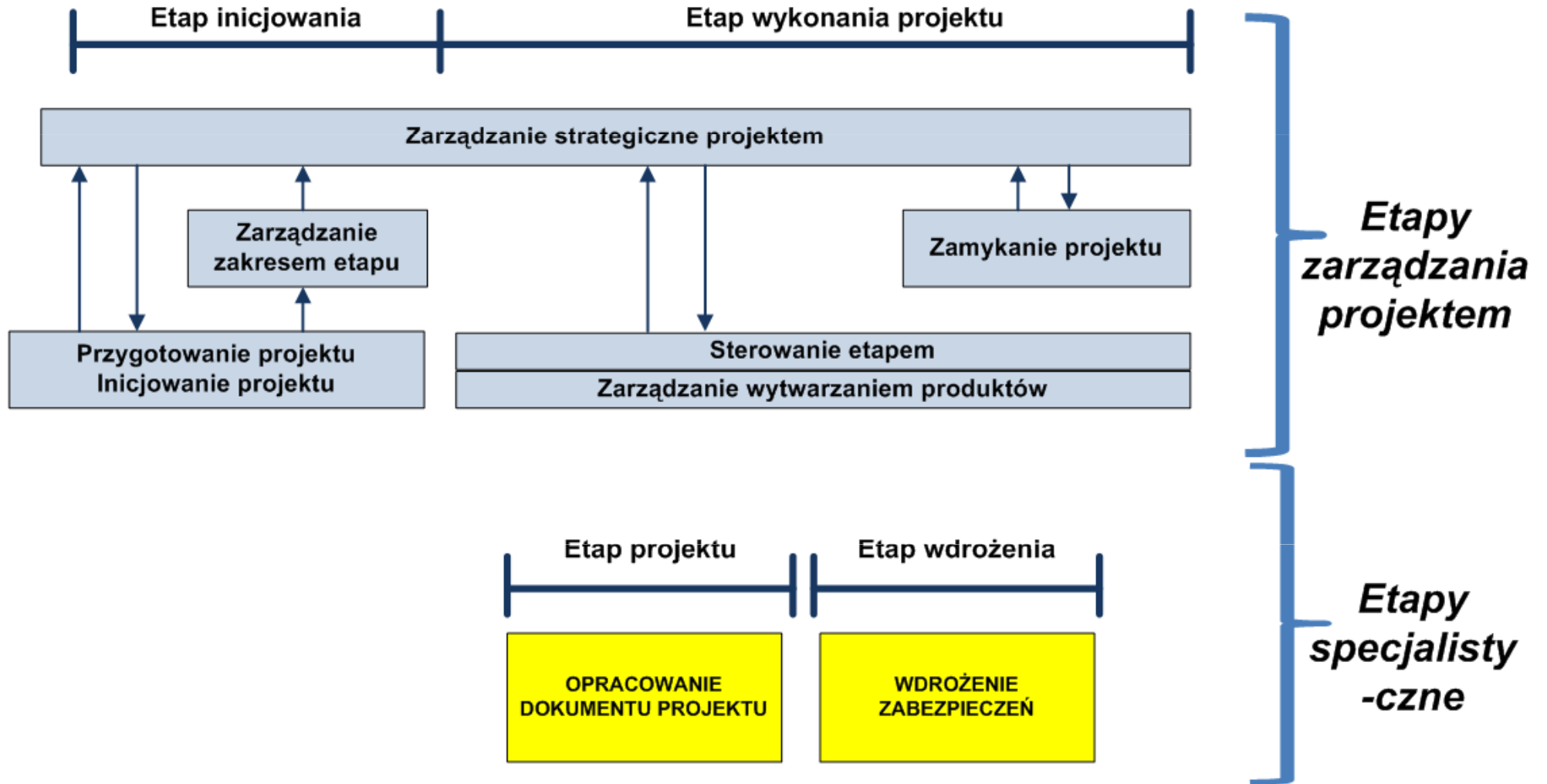
Uzasadnienie biznesowe

- W przypadku projektu zabezpieczeń trudno jest wskazać zyski finansowe z produktów projektu.
- Zabezpieczenia IT można traktować jak ubezpieczenie biznesu firmy, tzn. brak zabezpieczeń oznacza ryzyko dla firmy.
- Odpowiednio zabezpieczony system informatyczny zapewnia firmie dobre warunki do prowadzenia działalności biznesowej, m.in.:
 - możliwość szybkiego i bezpiecznego wprowadzania nowych usług IT i przez to możliwość rozszerzenia oferty,
 - większy dostęp do klientów, zwiększenie satysfakcji klientów, podwyższenie konkurencyjności rynkowej, itp.

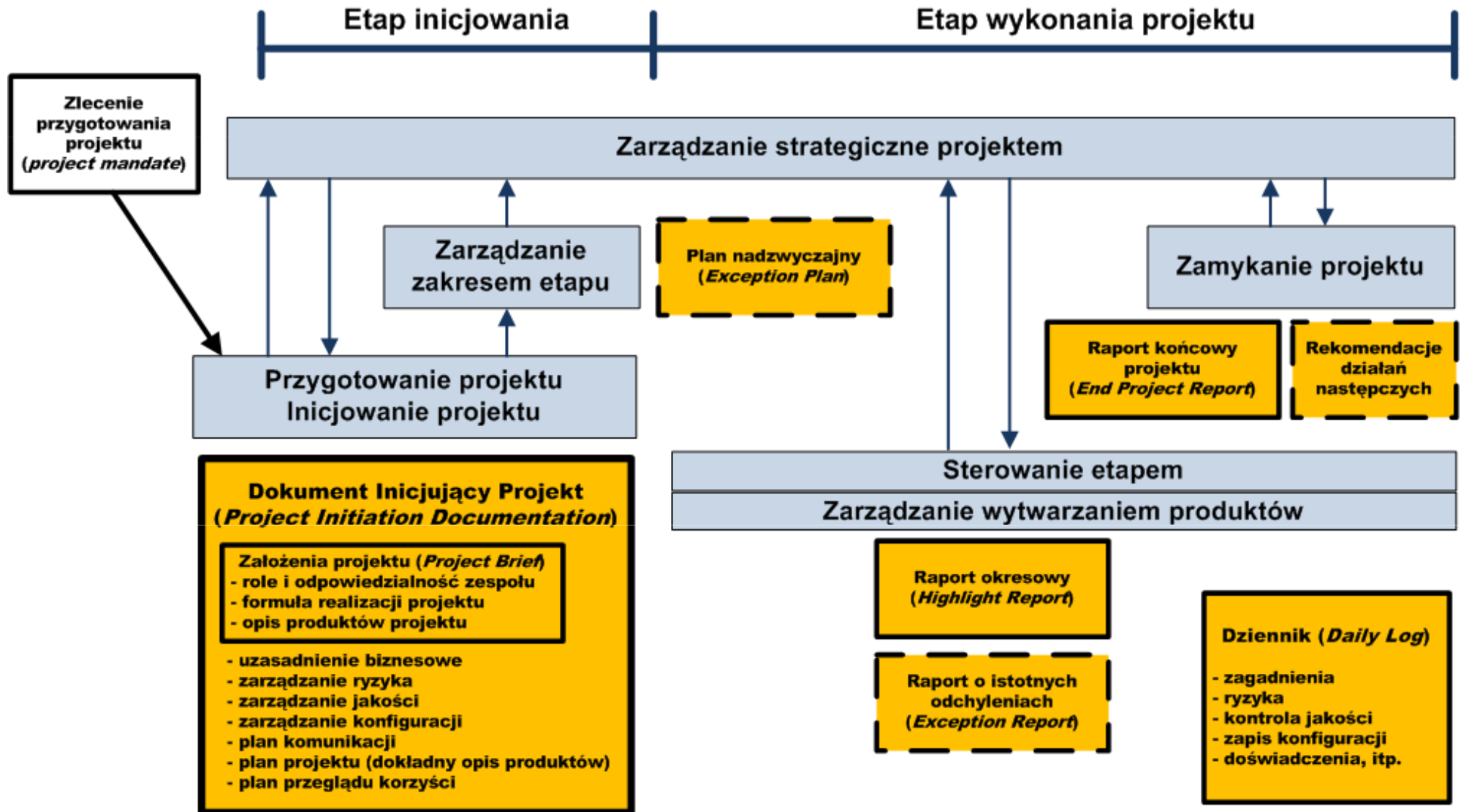
Uzasadnienie biznesowe

- Uzasadnienie biznesowe powinno konkretnie opisywać jakie zasoby IT będą chronione przed istotnymi zagrożeniami, jakie jest znaczenie (wartość) tych zasobów dla biznesu firmy i na jakie ryzyko narażona jest firma w razie zlekceważenia bezpieczeństwa.
- Poprawnie zdefiniowane uzasadnienie biznesowe pomaga działowi IT uzyskać zasoby (budżet) na właściwą realizację projektu (m.in. szkolenia, audyt).

Etapy i czynności (procesy) w projekcie



Produkty zarządcze (dokumenty, raporty, ...)



Planowanie oparte na produktach (*Product-based planning*)

1. W założeniach projektu tworzymy ogólny opis produktów projektu.
 - Dokument projektu zabezpieczeń
 - Wdrożone zabezpieczenia (techniczne, organizacyjne, itd.)
2. Tworzymy Diagram Struktury Produktów (*Product Breakdown Structure*).
3. W planie projektu tworzymy szczegółowe opisy produktów (w tym harmonogram prac).
4. Tworzymy Diagram Następstwa Produktów (*Product Flow Diagram*).

Diagram Struktury Produktów

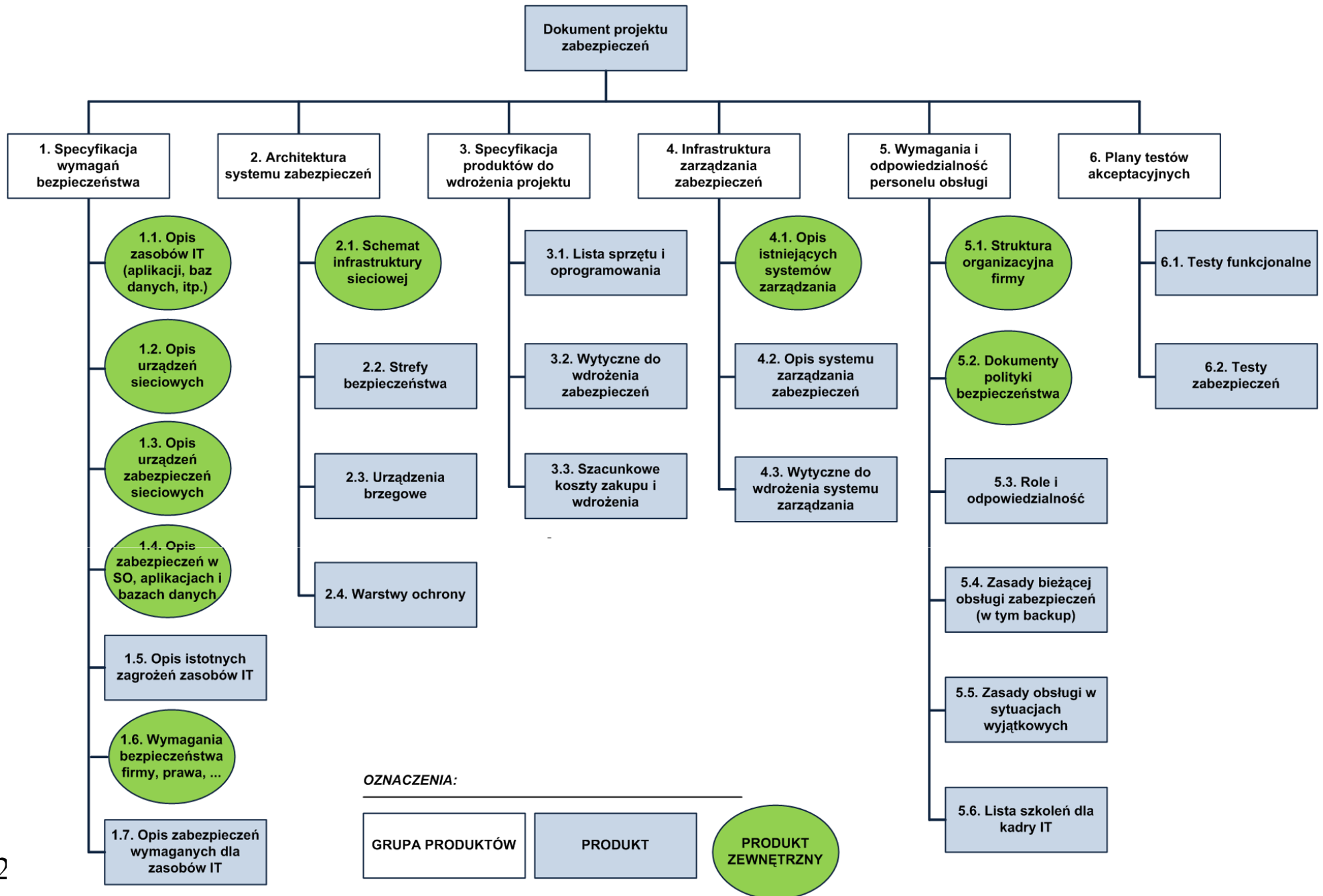
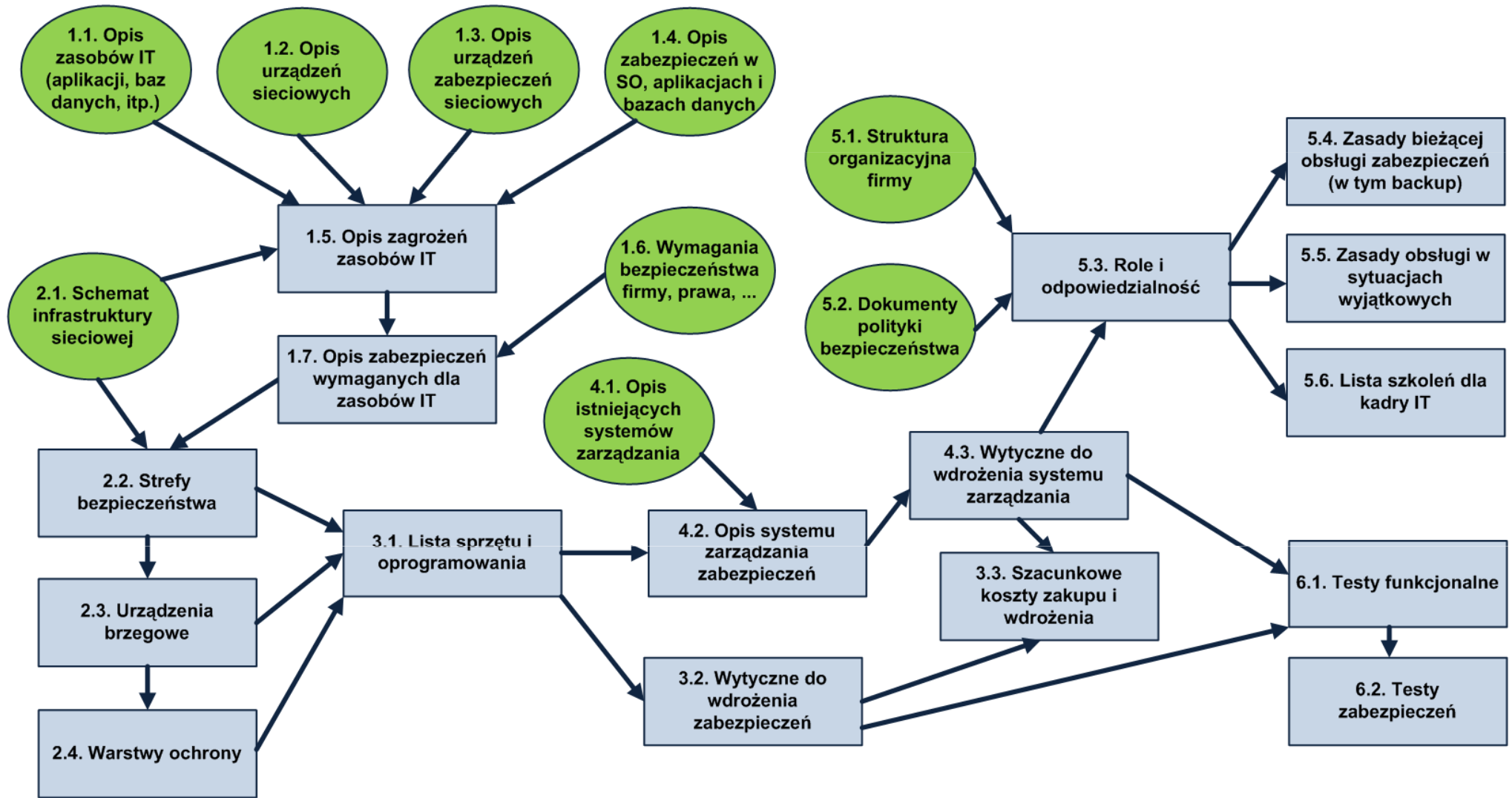


Diagram Następnstwa Produktów



Przegląd jakości (*Quality Review*)

- Prezentacja produktów pośrednich użytkownikom (administratorom zabezpieczeń).
- Testy akceptacyjne, audyt, ...

W przypadku projektu zabezpieczeń korzystne jest rozdzielenie prac pomiędzy dwóch wykonawców – projektant i integrator:

- *Integrator w trakcie wdrożenia zweryfikuje jakość dokumentu projektu.*
- *Projektant po wdrożeniu zabezpieczeń może zweryfikować prace integratora.*
- *Mniejsze ryzyko „napompowania” kosztów projektu, gdy projektant nie sprzedaje oprogramowania/urządzeń do wdrożenia zabezpieczeń.*

Podsumowanie

- Zastosowanie PRINCE2™ (lub innej sprawdzonej metody) do zarządzania projektem zabezpieczeń nie daje gwarancji sukcesu projektu, ale znacznie zmniejsza ryzyko wystąpienia problemów natury organizacyjnej, m.in.:
 - Brak odpowiedniej współpracy i niedostateczne zaangażowanie kierownictwa firmy i użytkowników.
 - Brak jasno określonych celów biznesowych projektu.
 - Oszczędności na analizie wymagań - zabezpieczenia ustalone bez analizy ryzyka, tylko w oparciu o „dobre praktyki”.
 - Niedostateczna kontrola zmian konfiguracji i jakości.

Pytania

Mariusz Stawowski
mstawow@clico.pl