POLSKI KOMITET NORMALIZACYJNY

Normalizacja dla bezpieczeństwa informacyjnego

J. Krawiec, G. Ożarek

Kwiecień, 2010

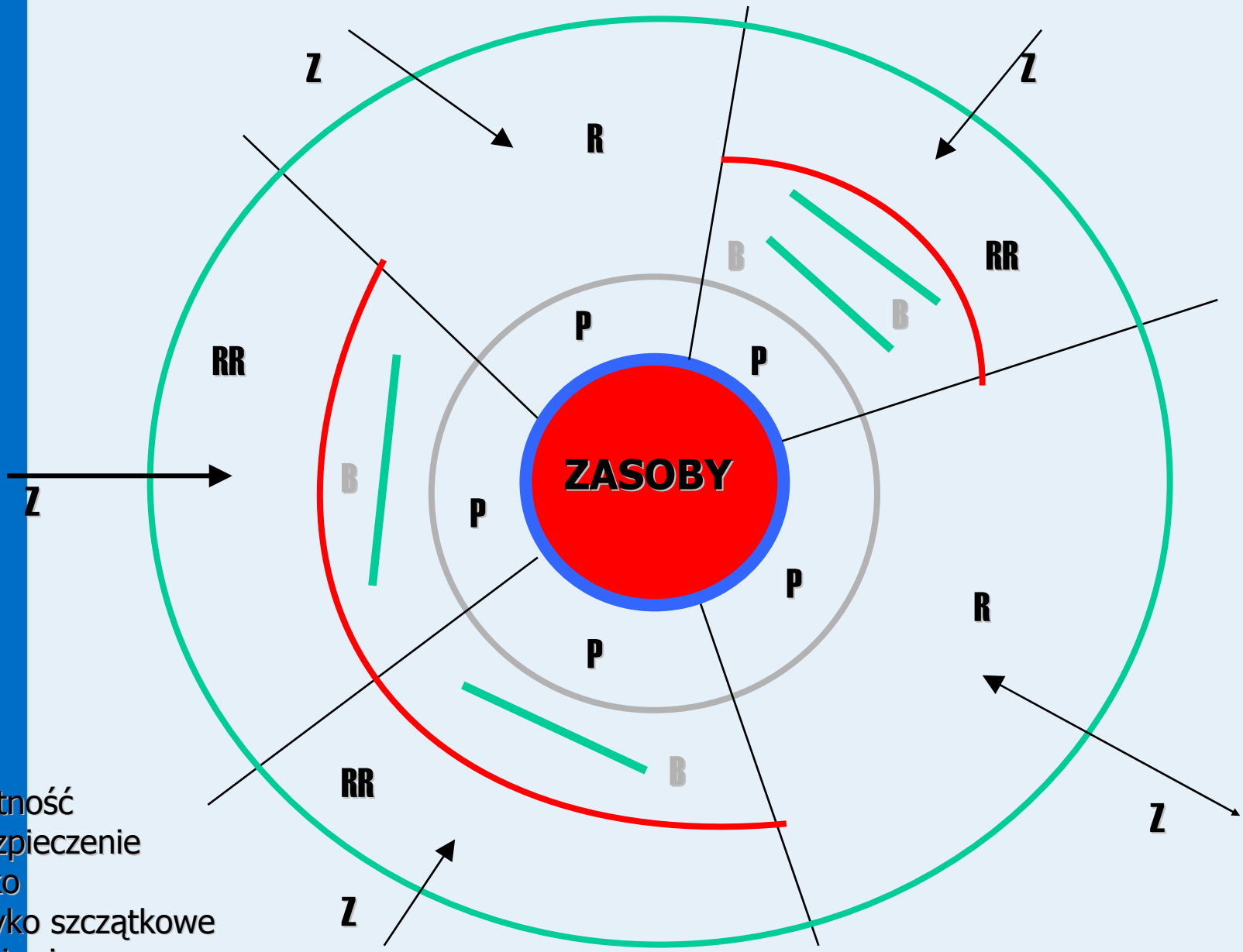
Polski Komitet Normalizacyjny, 00-050 Warszawa, ul. Świętokrzyska 14b

POLSKI KOMITET NORMALIZACYJNY

Plan wystąpienia

- Ogólny model bezpieczeństwa
- Jak należy przygotować organizację do wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI)
- Jak wdrożyć SZBI w organizacji
- Certyfikować czy nie certyfikować SZBI
- Jak przygotować się do audytu strony drugiej lub trzeciej

Ogólny model bezpieczeństwa



Legenda:
P – podatność
B – zabezpieczenie
R – ryzyko
RR – ryzyko szczątkowe
Z - zagrożenia

POLSKI KOMITET NORMALIZACYJNY

Zagrożenia

Rozmyślne
Podsłuch
Modyfikacja
Włamanie do systemu
Złośliwy kod
Kradzież

Przypadkowe
Pomyłki
Skasowanie pliku
Błędne skierowanie
Uszkodzenia fizyczne

POLSKI KOMITET NORMALIZACYJNY

Klasy bezpieczeństwa

A
System zweryfikowany

B
B3 Obszary poufne
B2 Zabezpieczenie strukturalne
B1 Etykietowany poziom zabezpieczeń

C
C2 Dostęp kontrolowany
C1 Dobrowolna kontrola dostępu

D
Ochrona minimalna

POLSKI KOMITET NORMALIZACYJNY

Podstawowe atrybuty danych i informacji

POLSKI KOMITET NORMALIZACYJNY

POLSKI KOMITET NORMALIZACYJNY

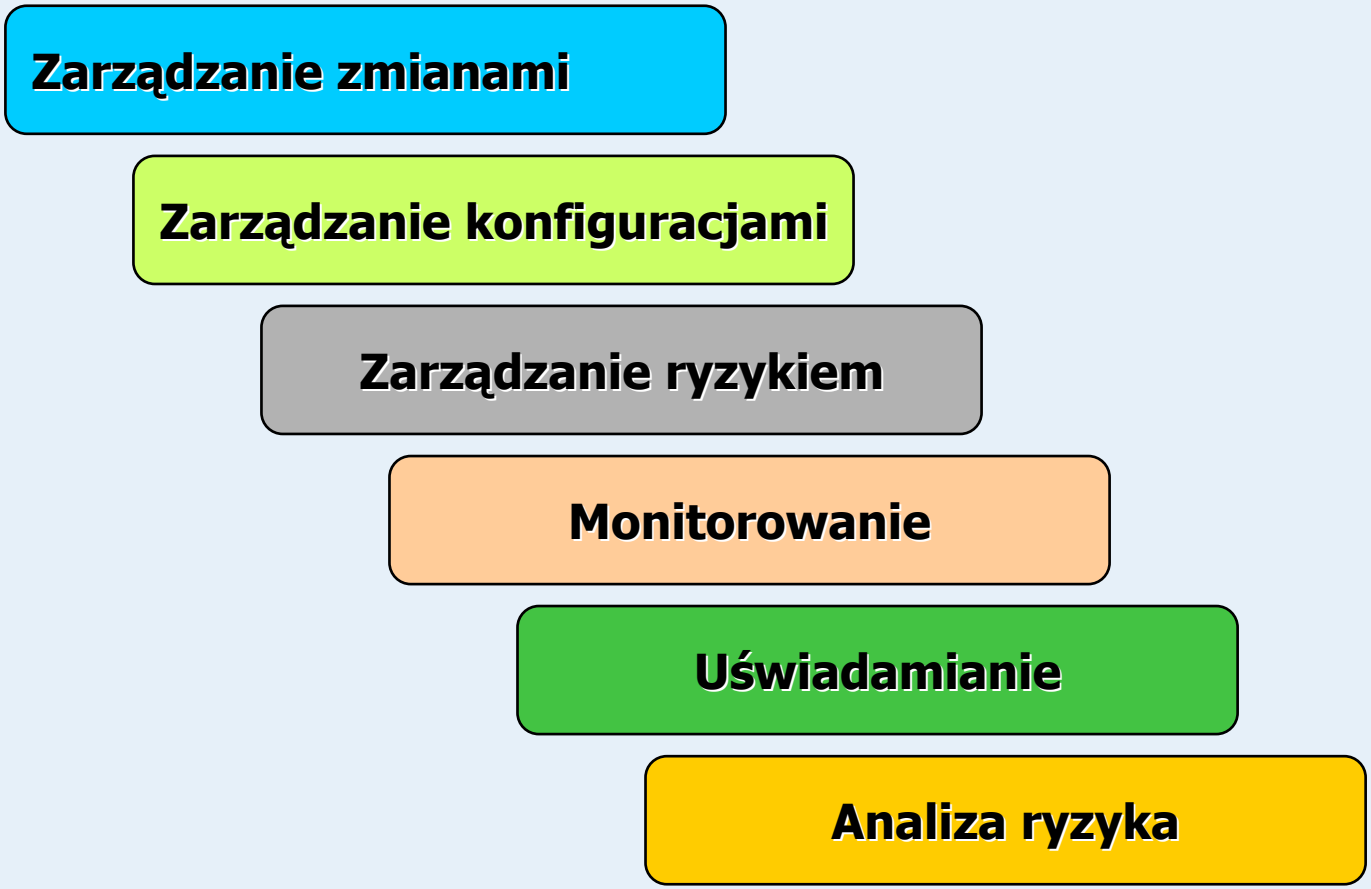
Oparty na podejściu wynikającym z ryzyka biznesowego

SZBI

Ustanawianie Wdrażanie Eksploatacja
Monitorowanie
Utrzymywanie Doskonalenie

POLSKI KOMITET NORMALIZACYJNY

Procesy zarządzania bezpieczeństwem systemów informacyjnych



POLSKI KOMITET NORMALIZACYJNY

Działaj zgodnie z PDCA

POLSKI KOMITET NORMALIZACYJNY

Schemat wdrożenia SZBI oparty na modelu PDCA

POLSKI KOMITET NORMALIZACYJNY

Planuj

Zapoznaj się opisem modelu ustanowienia, wdrożenia, zarządzania, monitorowania oraz przeglądu SZBI - z treścią normy **PN-ISO/IEC 27001**

Zapoznaj się z normami uszczegóławiającymi: PN-ISO/IEC 17799, PN-ISO/IEC 27005 oraz PN-ISO/IEC 27006

POLSKI KOMITET NORMALIZACYJNY

Planuj

Określ posiadane aktywa (m.in. sklasyfikuj dane i informacje),

Opracuj politykę bezpieczeństwa informacyjnego (PBI)

Określ zagrożenia dla aktywów poprzez szacowanie ryzyka

Opracuj procesy i procedury ważne z punktu widzenia zarządzania ryzykiem

POLSKI KOMITET NORMALIZACYJNY

Planuj

Dokonaj analizy ekonomicznej: kosztów wdrożenia systemu i kosztów ewentualnych strat z tytułu jego braku

Podejmij strategiczną decyzję dotyczącą ustanowienia SZBI

POLSKI KOMITET NORMALIZACYJNY

Planuj

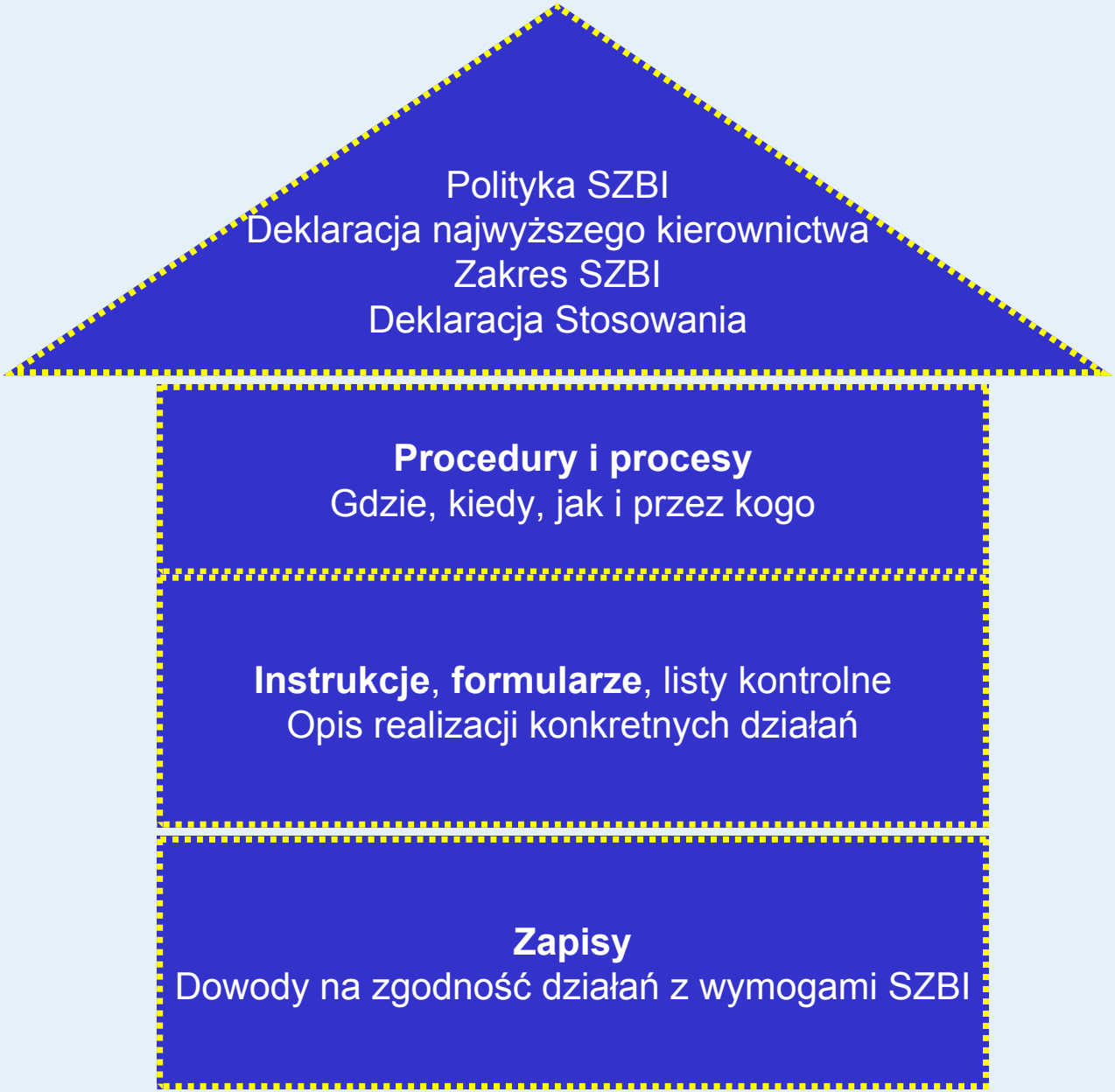
Opracuj harmonogram działań wdrażających

Przygotuj **plan postępowania z ryzykiem**

Dokument **planu postępowania z ryzykiem** przedstawia zabezpieczenia, które będą zastosowane w celu ograniczenia zidentyfikowanego ryzyka

POLSKI KOMITET NORMALIZACYJNY

Struktura dokumentów SZBI



POLSKI KOMITET NORMALIZACYJNY

Wykonuj

Wdrażaj zabezpieczenia
zgodnie z celami stosowania zabezpieczeń zapisanymi
w
Deklaracji stosowania
Cele stosowania zabezpieczeń i zabezpieczenia (załącznik A)

POLSKI KOMITET NORMALIZACYJNY

Wykonuj

Wdrażaj procedury:

Działań zapobiegawczych

Działań korygujących

Nadzoru nad dokumentami

Prowadzenia audytów wewnętrznych

Wdrażaj programy uświadamiania personelu!

POLSKI KOMITET NORMALIZACYJNY

Wykonuj

Zdefiniuj pomiar skuteczności zabezpieczeń

Wykorzystuj w praktyce SZBI

POLSKI KOMITET NORMALIZACYJNY

Sprawdzaj

Monitoruj system w celu identyfikowania naruszeń bezpieczeństwa, wykrywania błędów przetwarzania, wykrywania incydentów

Wykonuj pomiar skuteczności zabezpieczeń

Wykonuj przeglądy szacowania ryzyka

POLSKI KOMITET NORMALIZACYJNY

Sprawdzaj

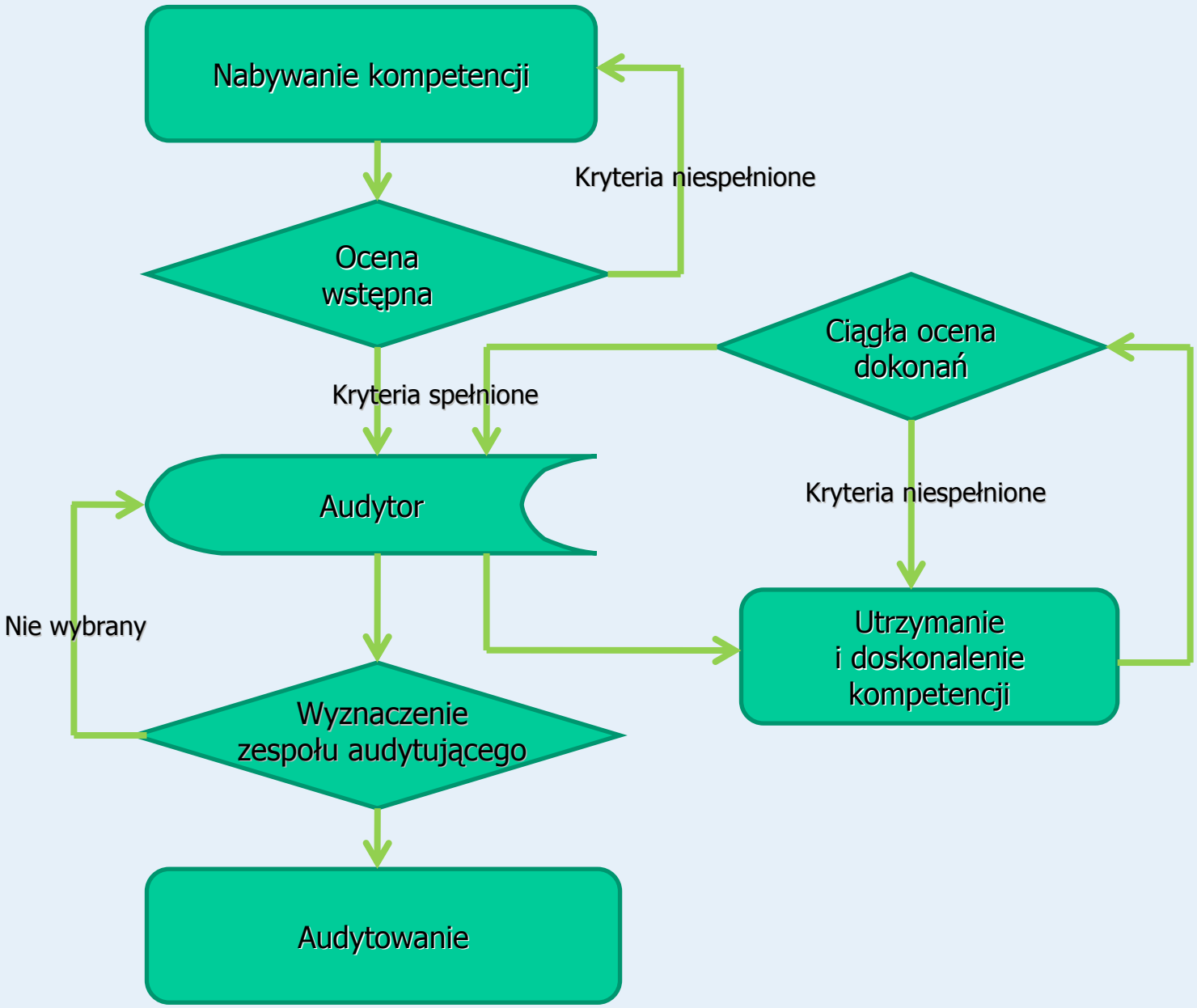
Badaj działanie systemu – jego wydajność, efektywność

POLSKI KOMITET NORMALIZACYJNY

Składowe kompetencji audytorów

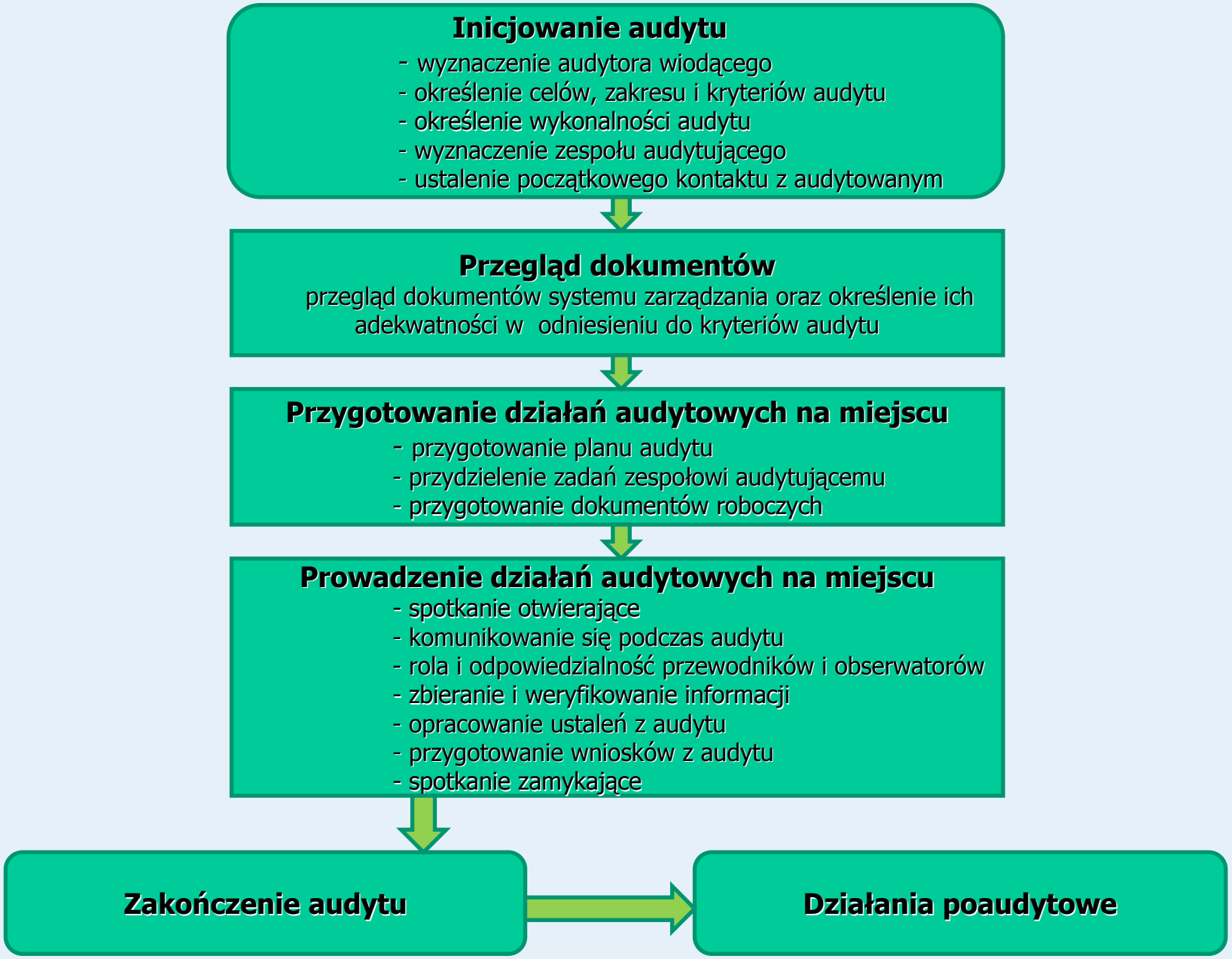
POLSKI KOMITET NORMALIZACYJNY

Etapy oceny audytora

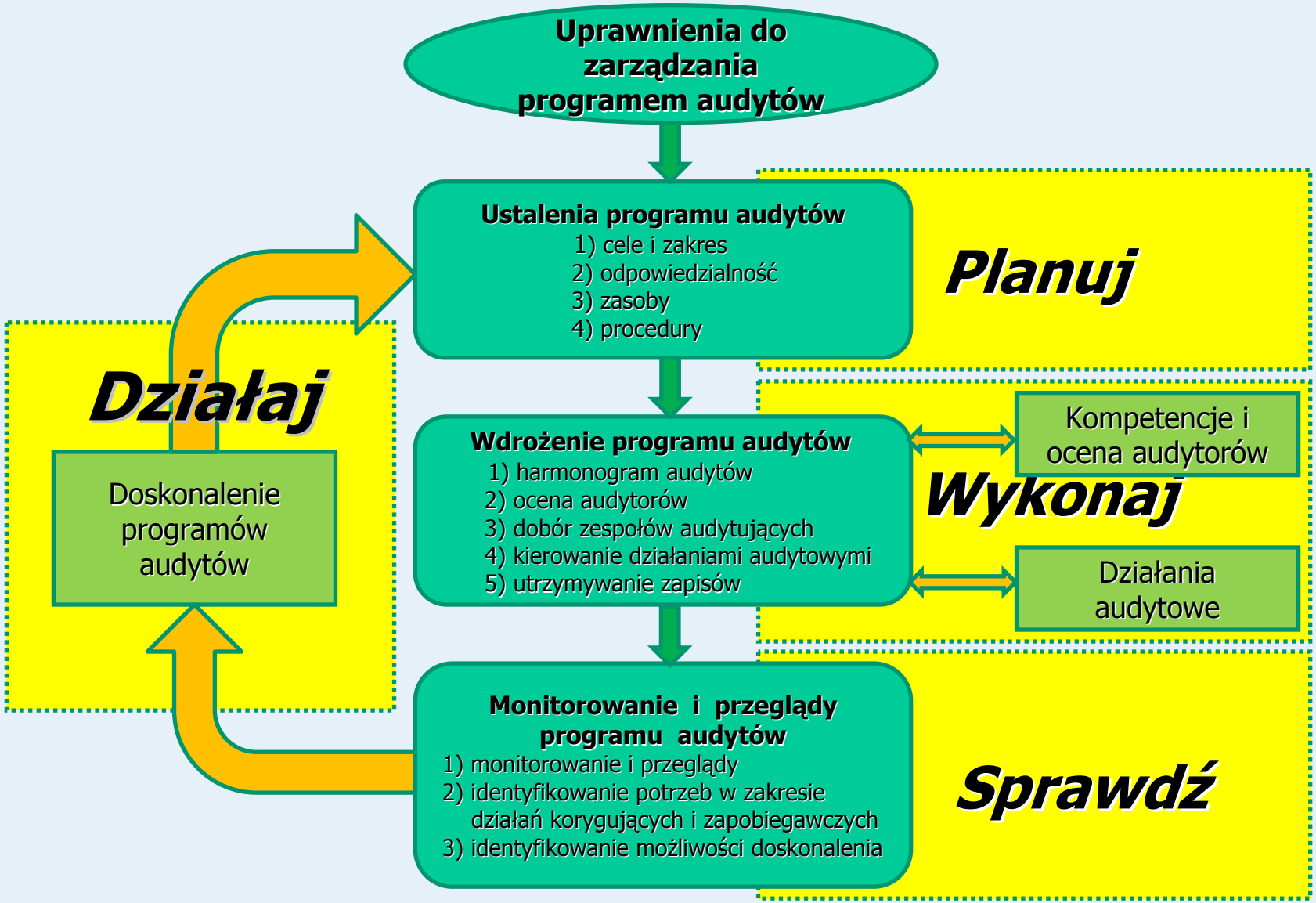


POLSKI KOMITET NORMALIZACYJNY

Standardowy proces audytu



Proces zarządzania programem audytu



POLSKI KOMITET NORMALIZACYJNY

Działaj

Konserwuj i usprawniaj funkcjonowanie systemu

Wdrażaj zidentyfikowane udoskonalenia

Podejmuj stosowne działania korygujące lub zapobiegawcze

POLSKI KOMITET NORMALIZACYJNY

Uwaga!

- Norma PN-ISO/IEC 27001 nie jest typową normą IT
- Jest *sui generis* przewodnikiem ukazującym tworzenie kultury bezpieczeństwa informacyjnego

POLSKI KOMITET NORMALIZACYJNY

Certyfikować czy nie certyfikować SZBI?

Certyfikat to świadectwo dojrzałości

POLSKI KOMITET NORMALIZACYJNY

Przygotowanie do audytu zewnętrznego - jakie dokumenty?

Polityka bezpieczeństwa informacyjnego

Deklaracja stosowania

Dokumenty wymagane przez PN-ISO/IEC 27001 oraz opis SZBI

Opis metody i raport z szacowania ryzyka

Udokumentowane procedury

Plan postępowania z ryzykiem

Zapisy z realizacji procesów, incydentów

Opis skuteczności zabezpieczeń

POLSKI KOMITET NORMALIZACYJNY

Co interesuje audytorów?

Zgodność dokumentacji z wymaganiami

Dostępność dokumentacji

Zarządzanie dokumentacją

Wdrożenie zapisów dla wybranych zabezpieczeń

POLSKI KOMITET NORMALIZACYJNY

Korzyści

POLSKI KOMITET NORMALIZACYJNY

Źródło:

PN-ISO/IEC 27001:2007

PN-ISO/IEC 27006:2009

PN-I-13335-1:1999

Krawiec J., Ożarek G.: Certyfikacja w informatyce. Wyd. PKN, Warszawa, 2010

www.pkn.pl