

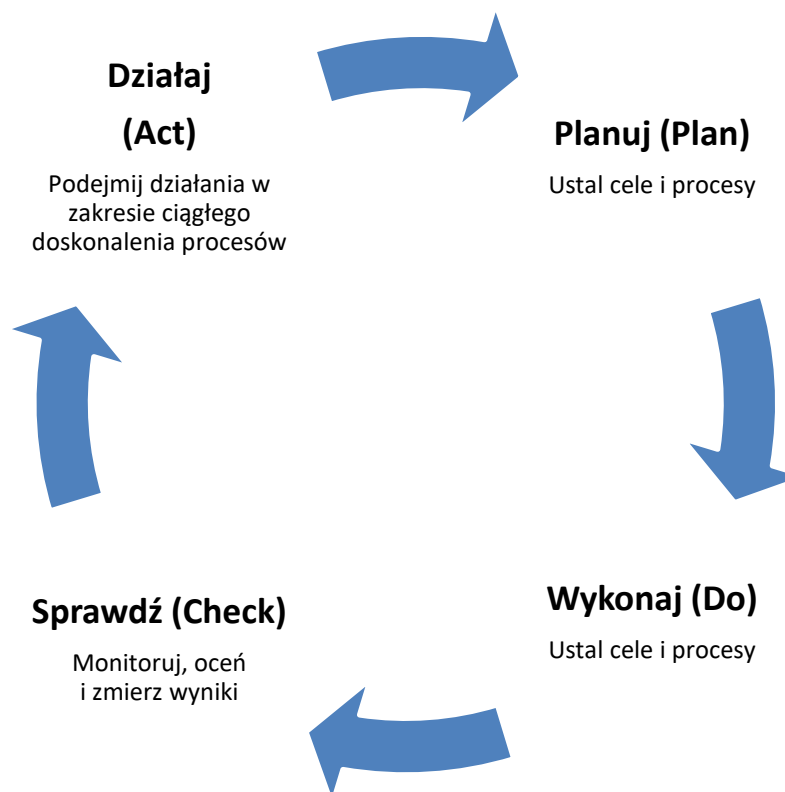
	Edycja	7
	Strona/ stron	1 z 4
ZAŁĄCZNIK NR 1 DO POLITYKI BEZPIECZEŃSTWA INFORMACJI	Data edycji załącznika	12.06.2025

FAZY POSTĘPOWANIA. CYKL DEMINGA

1. Fazy postępowania (Cykl Deminga)

- 1.1. Jednym z podstawowych założeń *Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)* jest podejście procesowe dla zapewnienia bezpieczeństwa przetwarzanych *Informacji*.
- 1.2. Podejście procesowe odzwierciedla zastosowany cykl PDCA („Plan” – „Do” – „Check” – „Act”), zwany również cyklem Deminga (patrz. Rys. 1.), który zakłada czteroetapową sekwencję prac lub działań, co pozwala na odpowiednie nimi zarządzanie oraz nadzorowanie ich stanu realizacji.

Rys. 1. Cykl PDCA (cykl Deminga)



1.3. Poszczególne fazy postępowania stanowią:

- **faza planowania** - „Planuj” („Plan”) - zaplanuj sposób realizacji działań lub prac (tj. ustanów politykę i cele, zidentyfikuj *Procesy* i odpowiedzialności, określ procedury odnoszące się do *Zarządzania ryzykiem* i doskonalenia SZBI),
- **faza wykonania** - „Wykonaj” („Do”) - wykonaj to, co zostało zaplanowane (tj. wdróż i stosuj politykę, środki nadzoru, *Procesy* i procedury),

- **faza sprawdzania - „Sprawdź” („Check”)** - sprawdź lub oceń czy działania lub prace zostały wykonane właściwie (tj. monitoruj, oceń i – tam gdzie to właściwe – zmierz wyniki działania *Procesów*),
- **faza działania - „Działaj” („Act”)** - pełnij nadzór oraz podejmij działania doskonalące (tzw. *Ciągłe doskonalenie*).

2. Faza planowania

2.1. Celem podejmowanych w ramach fazy planowania czynności jest zapewnienie, że *System Zarządzania Bezpieczeństwem Informacji (SZBI)* został ustanowiony prawidłowo, w sposób odpowiedni dokonano *Identyfikacji ryzyka* i opracowano *Plan postępowania z ryzykiem*.

2.2. Planując *SZBI* UCK rozważyło tzw. *Kontekst wewnętrzny* i *Kontekst zewnętrzny* organizacji, potrzeby i oczekiwania *Stron zainteresowanych*, a także określiło *Ryzyka* i szanse, do których należy się odnieść w celu:

- zapewnienia, że *SZBI* może osiągnąć zamierzone wyniki,
- zapobieżenia wystąpieniu niepożądanych skutków lub ich zredukowania,
- *Ciągłego doskonalenia*.

2.3. UCK zaplanowało:

- działania odnoszące się do określonych *Ryzyk* i szans,
- sposób ich zintegrowania i wdrożenia w *Procesach* składających się na *SZBI* oraz oceny ich skuteczności.

2.4. Podejmowane przez UCK działania w ramach tej fazy to:

- określenie założeń do dalszego planowania i wdrożenia *SZBI*, w tym dotyczących, przede wszystkim:
 - celów i oczekiwań związanych z funkcjonowaniem *SZBI*, które decydują o wyborze metod i technik umożliwiających osiągnięcie tych celów,
 - zakresu *SZBI*,
 - wyboru metody budowania *SZBI*,
 - delegowania uprawnień,
 - czasu realizacji, potrzebnych *Zasobów* oraz przewidywanych kosztów wdrożenia *SZBI*,
 - poddania *SZBI* certyfikacji trzeciej strony,
- ustanowienie *Polityki Bezpieczeństwa Informacji (PBI)* zawierającej wytyczne, tj. cele i zasady postępowania, w odniesieniu do *Bezpieczeństwa informacji* oraz innych procedur składających się na *SZBI*, a zwłaszcza procedur dotyczących *Zarządzania ryzykiem*,
- dokonanie *Szacowania ryzyka w Bezpieczeństwie informacji*, w tym analizy i oceny poszczególnych rodzajów *Ryzyk*, na jakie narażona jest organizacja, dzięki czemu można zidentyfikować *Zagrożenia* dla *Aktywów*, ocenić *Podatność* na *Zagrożenia* i *Prawdopodobieństwo* ich wystąpienia oraz estymować potencjalne skutki, a także wskazać i określić odpowiednie działania zarządcze i priorytety dla *Zarządzania ryzykiem w Bezpieczeństwie informacji* oraz wdrożyć mechanizmy zarządzania, służące ochronie przed tymi *Ryzykami*,
- opracowanie *Planów postępowania z ryzykiem* dla *Aktywów* o *Ryzykach* większych niż ustalony poziom *Ryzyka akceptowalnego*.

2.5. W przypadku dokonania *Identyfikacji ryzyka* na poziomie nieakceptowalnym możliwe są takie warianty postępowania, jak:

- *Zachowanie ryzyka* (np. w przypadku, gdy *Działania korygujące* są zbyt kosztowne lub niewykonalne ze względu na charakter *Procesu*),
- *Przeniesienie ryzyka* (inaczej *Transfer ryzyka*): dzielenie *Ryzyka* z inną stroną / innymi stronami (np. umowa z ubezpieczycielem, finansowanie *Ryzyka*),
- *Redukowanie ryzyka*: działania mające na celu zmniejszenie *Ryzyka*, np. poprzez usunięcie źródła *Ryzyka*, wdrożenie dodatkowych *Zabezpieczeń*,
- *Unikanie ryzyka*: wycofanie się z realizacji określonych celów i zadań (np. nierozpoczynanie lub niekontynuowanie działań generujących *Ryzyko*).

2.6. Wszelkie czynności podejmowane w ramach fazy planowania są dokumentowane (wraz z określeniem narzędzi oraz technik zastosowanych dla wykonania czynności tej fazy).

3. Faza wykonania

3.1. Celem podejmowanych w ramach fazy wykonania czynności jest zapewnienie skutecznego działania *SZBI*.

3.2. W ramach fazy wykonania ma miejsce wdrożenie i eksploatacja przyjętej Polityki Bezpieczeństwa Informacji (PBI) oraz ustalonych *Zabezpieczeń* i szczegółowych procedur, w tym identyfikacja *Grup informacji*.

3.3. Dokonaną ww. identyfikację *Grup informacji* oraz ich podział wg grup *Zabezpieczeń* odzwierciedla dokonana przez UCK *Klasyfikacji informacji*.

3.4. W zależności od podjętych w trakcie fazy planowania decyzji dotyczących *Postępowania z ryzykiem*, które odzwierciedla *Plan postępowania z ryzykiem*, w ramach tej fazy wdraża się ustalone uprzednio działania.

3.5. Po ograniczeniu lub przetransferowaniu *Ryzyka nieakceptowalnego* może pozostać tzw. *Ryzyko szczątkowe*. Wdrożone mechanizmy kontrolne winny zapewnić natychmiastową identyfikację i zarządzanie również tego rodzaju *Ryzykiem*.

4. Faza sprawdzania

4.1. Celem podejmowanych w ramach fazy sprawdzania czynności jest weryfikacja oraz utrzymanie efektywności *Systemu Zarządzania Bezpieczeństwem Informacji*, tj. w szczególności weryfikacja czy utrzymana jest spójność dokumentacji *SZBI* z podejmowanymi przez UCK *Procesami*, a także czy wdrożone *Zabezpieczenia* funkcjonują efektywnie, zgodnie z zamierzeniami.

4.2. W ramach fazy sprawdzania sprawdzane jest wykonanie procedur i wymogów Polityki Bezpieczeństwa Informacji (PBI) oraz dokonywana jest okresowa ocena *Ryzyk akceptowalnych*.

4.3. Faza sprawdzania przy tym obejmuje przegląd procedur zarządzania oraz eksploatacji *Zabezpieczeń*, a także bieżący *Przegląd ryzyka* z uwzględnieniem zmieniających się technologii, *Zabezpieczeń*, *Zagrożeń*, *Podatności*, a także wymagań prawa powszechnie obowiązującego i *Zainteresowanych stron*.

4.4. W ramach fazy sprawdzenia można zastosować cykl PDCA („Plan” – „Do” – „Check” – „Act”), który zakłada czteroetapową sekwencję prac nad stwierdzoną lub potencjalną *Niezgodnością*, a tym samym pozwala na odpowiednie nią zarządzanie i nadzorowanie stanu realizacji wdrożonych działań.

4.5. W ramach fazy sprawdzania wykorzystuje się następujące techniki testowania:

- rutynowe sprawdzenie – regularnie wykonywane procedury w ramach podejmowanych przez UCK *Procesów*, które pozwalają wykryć nieprawidłowości,
- samokontrolujące się procedury – narzędzia umożliwiające natychmiastowe wykrycie błędów, które mogą pojawić się w trakcie wykonywania jakiegoś *Procesu* (np. narzędzie monitorujące sieć, które powoduje uruchomienie się alarmu w momencie wystąpienia błędu),
- uczenie się od innych – zbadanie, jak inne instytucje rozwiązują tożsame problemy z zakresu *Bezpieczeństwa informacji*,
- audyty *SZBI* – działania wykonywane regularnie z wykorzystaniem odpowiednio dobranej próby aktualnych zapisów i dokumentów oraz rozmów z zaangażowanym w badany *Proces* kierownictwem i osobami, mające na celu określenie poprawności funkcjonowania *SZBI*, w ramach których weryfikuje się czy:
 - Polityka Bezpieczeństwa Informacji (PBI) oraz inne procedury *SZBI* są aktualne, przestrzegane i spełniają zamierzone cele,
 - metodyka *Szacowania ryzyka* jest odpowiednia,
 - wdrożone *Zabezpieczenia*, w tym np. *Zabezpieczenia* fizyczne i informatyczne, są odpowiednie, poprawnie zaimplementowane, skonfigurowane i działają zgodnie z zamierzeniami,
 - *Ryzyka* *szczątkowe* są odpowiednio oszacowane i akceptowalne dla *Najwyższego Kierownictwa*,
 - rekomendacje wynikające z poprzednich audytów zostały zrealizowane,
 - *SZBI* jest zgodny z wymaganiami normy PN-EN ISO/IEC 27001 oraz wymaganiami prawa powszechnie obowiązującego,
- przeglądy *SZBI* – działania, których celem jest sprawdzenie efektywności funkcjonowania *SZBI*, zidentyfikowanie elementów wymagających udoskonalenia i podjęcia odpowiednich *Działań korygujących i zapobiegawczych*.
- analiza trendów – działania prowadzone regularnie, wskazujące obszary wymagające ulepszeń.

5. Faza działania

5.1. W ramach fazy działania podejmuje się działania prowadzące do ciągłego doskonalenia *SZBI*.

5.2. W ramach tej fazy, na podstawie wniosków wyciągniętych z czynności przeprowadzonych w fazie sprawdzania, w tym z oceny funkcjonowania wdrożonych *Zabezpieczeń*, podejmuje się wszelkiego rodzaju działania doskonalące, w tym działania:

- korygujące (w celu wyeliminowania *Niezgodności* lub innych niepożądanych sytuacji),
- zapobiegawcze (w celu wyeliminowania przyczyny potencjalnej *Niezgodności* lub innych niepożądanych sytuacji), tj.:
 - naprawcze,
 - prewencyjne.