PROCESOWE PODEJŚCIE DO CYBERBEZPIECZEŃSTWA

PROCESOWE PODEJŚCIE DO CYBERBEZPIECZEŃSTWA JEST ELEMENTEM STANDARDU CYBERBEZPIECZEŃSTWA PPBW DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW ORAZ INSTYTUCJI PUBLICZNYCH, OPRACOWANEGO PRZEZ POLSKĄ PLATFORMĘ BEZPIECZEŃSTWA WEWNĘTRZNEGO.

SPIS TREŚCI

03

INFORMACJE WPROWADZAJĄCE

- Wdrażanie standardu cyberbezpieczeństwa, jak również, szerzej – całościowe podejście do zarządzania cyberbezpieczeństwem musi być traktowane jako proces.

- Oznacza to, że wymagało będzie podejmowania zaplanowanych decyzji, zapewniających wykorzystanie określonych zasobów (kompetencji, narzędzi, umiejętności) dla osiągnięcia pożądanych celów, oraz skoordynowania aktywności mających ze sobą współpracować podmiotów[1].

- Poniżej opracowany został uproszczony schemat procesowego podejścia do wdrażania standardu. Jest to wyłącznie propozycja podejścia, każdorazowo wybór działań powinien być dostosowany do charakterystyki podmiotu, zasobów, jakimi dysponuje.

- Oczywiście samo wdrożenie standardu to zaledwie początek. Ma to służyć stworzeniu ram dla zaplanowania i implementacji działań organizacyjnych, technicznych i innych nakierowanych na zapewnianie cyberbezpieczeństwa.

- Poniżej zaprezentowany został przykładowy schemat procesowego podejścia do wdrażania samego standardu. Następnie wskazane zostały wybrane (w żaden sposób nie wyczerpujące!) przykłady procesów zarówno organizacyjnych jak i technicznych, które powinny zostać wdrożone w organizacji.

1) Por. Bogdanienko J. (2010) Organizacja i zarządzanie w zarysie, Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, Warszawa, s. 16-17.

WDROŻENIE STANDADRU CYBERBEZPIECZEŃSTWA

URUCHOMIENIE PROCESU WDRAŻANIA STANDARDU

ZAPLANOWANIE CAŁOŚCI PROCESU

ETAP 1 STANDARDU PPBW

KROK 1: Wyznaczenie osoby odpowiedzialnej za nadzór nad zrealizowaniem całościowego procesu zarządzania aktywami informacyjnymi (ZAI) – kierownika procesu ZAI.

KROK 2: Określenie ról i odpowiedzialności za poszczególne działania:

Zadanie 1: Identyfikacje aktywów informacyjnych
(np. każdy dział, zespół, pracownik – wypisuje aktywa (grupy aktywów) za pomocą, których realizuje swoje działania – nadzór kierownik procesu ZAI).
Zadanie 2: Identyfikacja i przypisanie właściciela dla każdego z aktywów
(kierownik procesu ZAI w porozumieniu z ww. pracownikami ustala właścicieli poszczególnych grup aktywów – decyzje akceptuje kierownictwo).
Zadanie 3: Określenie wymagań związanych z ochroną aktywów
(właściciel odpowiedzialny jest za określenie wymagań prawnych i innych związanych z ochroną aktywów, których jest właścicielem).
Zadanie 4: Określenie wartości aktywów i ich klasyfikacja
(kierownik procesu ZAI przygotowuje klasyfikacje aktywów informacyjnych – akceptacja przez kierownictwo. Następnie, właściciele aktywów zobowiązani są oznaczyć aktywa zgodnie z klasyfikacją).
Zadanie 5: Identyfikacja obecnie stosowanych zabezpieczeń
(właściciele aktywów identyfikują stosowane zabezpieczenia dla swoich aktywów).
Zadanie 6: Określenie akceptowalnego poziomu ryzyka
(kierownictwo ustala i akceptuje akceptowalny poziom ryzyka).
Zadanie 7: Umieszczenie wszystkich zebranych informacji w rejestrze
(właściciele aktywów, pod nadzorem kierownika procesu ZAI uzupełniają rejestr).

ETAP 2 STANDARDU PPBW - Zarządzanie ryzykiem

KROK 1: Wyznaczenie osoby odpowiedzialnej za nadzór nad zrealizowaniem całościowego procesu zarządzania ryzykiem (ZR) – kierownika procesu ZR.

KROK 2: Określenie ról i odpowiedzialności za poszczególne działania:

Faza 1: Identyfikacja ryzyka
Zadanie 1: Identyfikacja zagrożeń, które mogą negatywnie oddziaływać na bezpieczeństwo aktywów
(działanie to może być realizowane np. przez właścicieli aktywów we współpracy z grupami roboczymi np. złożonych z osób z odpowiednich działów, o odpowiednich funkcjach – pod nadzorem kierownika procesu ZR).
Zadanie 2: Identyfikacja podatności na ryzyko
(działanie to powinno być realizowane np. przez właścicieli aktywów – pod nadzorem kierownika procesu ZR – powinno brać pod uwagę wyniki Etapu 1, zadanie 5).
Faza 2: Analiza ryzyka
Zadanie 1: Ocena potencjalnych skutków wystąpienia zidentyfikowanych zagrożeń
(działanie to powinno być realizowane np. przez właścicieli aktywów – pod nadzorem kierownika procesu ZR zgodnie z przyjętą metodyką).
Zadanie 2: Ocena prawdopodobieństwa wystąpienia zagrożenia
(działanie to powinno być realizowane np. przez właścicieli aktywów – pod nadzorem kierownika procesu ZR zgodnie z przyjętą metodyką).
Faza 3: Ocena analizowanego ryzyka.
Zadanie 1: Porównanie wyników analizy ryzyka z wcześniej określonymi akceptowalnymi poziomami ryzyka
(zadanie realizowane przez kierownika procesu ZR – pod nadzorem kierownictwa zgodnie z przyjętą metodyką).
Faza 4: Wybór i realizacja strategii postępowania z ryzykiem.
Zadanie 1: Wybór metody zarządzania ryzykiem i jego komunikacja
(zadanie realizowane przez kierownika procesu ZR – pod nadzorem kierownictwa).

ETAP 3 STANDARDU PPBW - Wybór zabezpieczeń i ich implementacja

KROK 1: Kierownik procesu ZR dokonuje wyboru działania w kontekście wyników oceny ryzyka. Kierownictwo akceptuje wybór działań.

KROK 2: Kierownik procesu ZR wraz z właścicielami aktywów dokonuje wyboru konkretnych zabezpieczeń określając odpowiedzialność za ich implementacje (jeśli zdecydowano się na zastosowanie zabezpieczeń).

ETAP 4 STANDARDU PPBW - Testowanie bezpieczeństwa, monitoring, audyt, ciągłe doskonalenie

KROK 1: Kierownik procesu ZR wraz z właścicielami aktywów prowadzą regularny monitoring funkcjonowania zadań, analizują możliwe udoskonalenia.

Kierownictwo nadzoruje działania i akceptują kluczowe kierunki działań.

PRZYKŁADOWY SZABLON HARMONOGRAMU

HARMONOGRAM WDROŻENIA STANDARDU CYBERBEZPIECZEŃSTWA													
			2019										
LP	ZADANIE	OSOBA ODPOWIEDZIALNA	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII
1	Ustalenie harmonogramu, budżetu procesu wdrażania standardu	Prezes Zarządu	✓											
2	Wybór kierownika procesu ZAI	Prezes Zarządu		✓										
3														
4														
5														
6														
7														
8														
9														
10														

06

WYBRANE PROCESY ORGANIZACYJNE

PROCEDURA ZAPEWNIENIA BEZPIECZEŃSTWA ZASOBÓW LUDZKICH[2]:

1. Przygotowanie postępowania sprawdzającego kandydatów.
2. Uzgodnienie warunków zatrudnienia, zasad bezpieczeństwa i odpowiedzialności.
3. Nadanie praw dostępu zgodnie z pełnioną funkcją, zakresem odpowiedzialności.
4. Prowadzenie działań uświadamiających, szkoleń, treningów.
5. Nadzór nad czynnościami, podejmowanymi przez pracownikiem w związku z zakończeniem zatrudnienia.
6. Zwrot aktywów.
7. Odebranie praw dostępu.

PROCEDURA ZWIĄZANA Z TWORZENIEM POLITYK BEZPIECZEŃSTWA[3]:

1. Stworzenie dokumentu polityki bezpieczeństwa.
2. Zatwierdzenie polityki przez kierownictwo.
3. Ustanowienie właściciela polityki i zasad związanych z jej przeglądem i doskonaleniem.
4. Zakomunikowanie faktu stworzenia polityki wszystkim zainteresowanym stronom.
5. Wdrożenie polityki.
6. Przegląd polityki i jej doskonalenie.

2) Więcej: ISO 27001.
3) Ibid.

07

WYBRANE PROCESY ZWIĄZANE Z BEZPIECZEŃSTWEM FIZYCZNYM

PROCEDURY USTANAWIANIA OBSZARÓW BEZPIECZNYCH[4]:

1. Wyznaczenie obszarów bezpiecznych.
2. Wdrożenie zabezpieczeń fizycznych w obszarach, pomieszczeniach itd.
3. Wdrożenie mechanizmów ochrony przed zjawiskami zewnętrznymi i środowiskowymi.
4. Ustalenie i zakomunikowanie zasad pracy w obszarach bezpiecznych.
5. Zapewnienie bezpieczeństwa obszarów publicznie dostępnych, obszaru dostaw i załadunku.

PROCEDURY ZAPEWNIANIA BEZPIECZEŃSTWA FIZYCZNEGO SPRZĘTU[5]:

1. Ustalenie zasad bezpiecznego ulokowania sprzętu.
2. Zapewnienie systemów wspomagających.
3. Zapewnienie bezpieczeństwa okablowania.
4. Ustalenie zasad bezpiecznego zbywania sprzętu lub jego przekazywania do ponownego użytku.

4) Ibid.
5) Ibid.

08

WYBRANE PROCESY ZWIĄZANE Z BEZPIECZEŃSTWEM TECHNICZNYM

PROCEDURY ZWIĄZANE Z TWORZENIEM KOPII ZAPASOWYCH[6]:

1. Ustalenie zakresu: czyli aktywów, których kopie zapasowe będzie wykonywane.
2. Ustalenie harmonogramu, częstotliwości i określonych sytuacji w wypadku których tworzy się kopie zapasowe.
3. Tworzenia kopii zapasowych.
4. Przechowywanie kopii zapasowych.
5. Testowanie kopii zapasowych.
6. Odzyskiwanie danych i systemów informatycznych z kopii zapasowych (wedle wcześniej ustalonych reguł).

PROCEDURA ANALIZY LOGÓW[7]:

1. Określenie zakresu.
2. Konfigurowanie systemu zarządzania logami, skonfigurowanie każdego włączonego do systemu klienta.
3. Gromadzenie logów.
4. Normalizacja zebranych danych.
5. Indeksowanie.
6. Magazynowanie.
7. Korelacja.
8. Tworzenie poziomu odniesienia.
9. Alarmy.
10. Raporty.

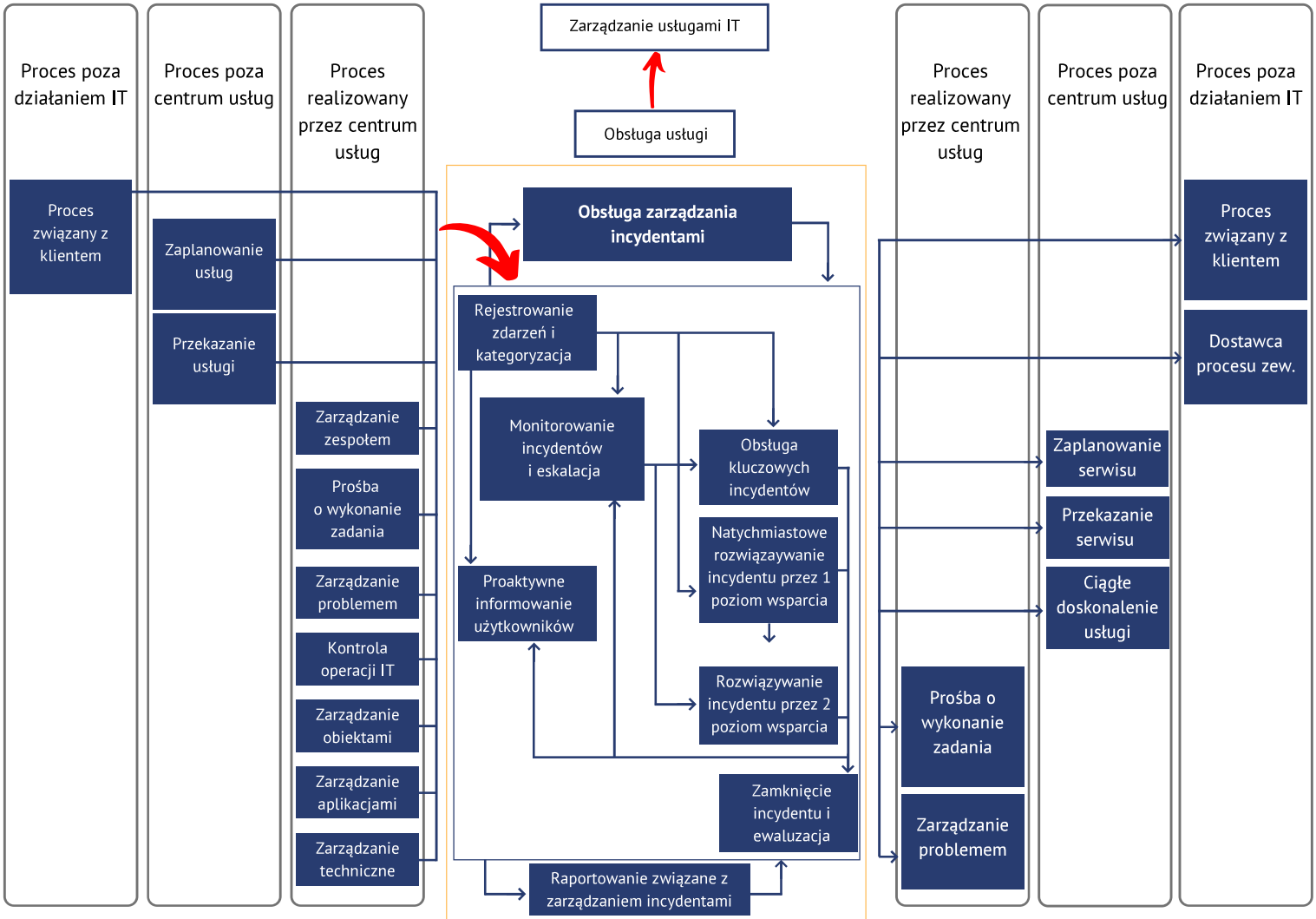
6) Por. Procedury tworzenia kopii zapasowych. Załącznik nr 2, Polityki Bezpieczeństwa Informacji Świętokrzyskiego Urzędu Wojewódzkiego.
7) https://www.computerworld.pl/news/Analiza-logow-potencjal-do-wykorzystania,382493,5.html

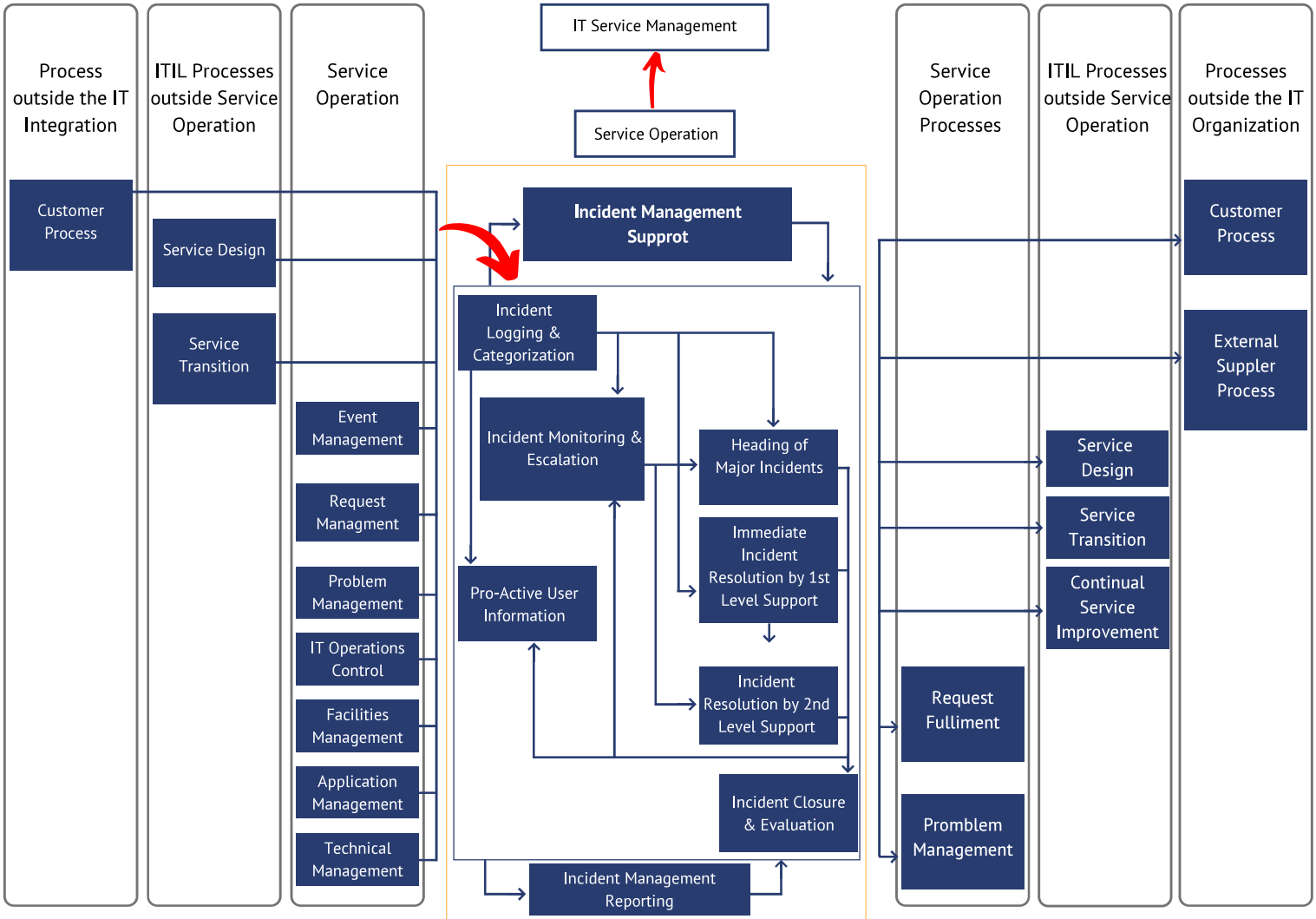
09

WYBRANE PROCESY ZWIĄZANE Z BEZPIECZEŃSTWEM TECHNICZNYM

PROCEDURA ZARZĄDZANIA INCYDENTAMI

Procedura zarządzania incydentami, została opisana w ramach metodyki ITIL. Poniżej oryginalna wersja oraz tłumaczenie.


Proces poza działaniem IT
Proces poza centrum usług
Proces realizowany przez centrum usług
Zarządzanie usługami IT
Obsługa usługi
Proces poza działaniem IT
Proces poza centrum usług
Proces realizowany przez centrum usług
Proces związany z klientem
Zaplanowanie usług
Przekazanie usługi
Obsługa zarządzania incydentami
Rejestrowanie zdarzeń i kategoryzacja
Monitorowanie incydentów i eskalacja
Obsługa kluczowych incydentów
Natychmiastowe rozwiązywanie incydentu przez 1 poziom wsparcia
Proaktywne informowanie użytkowników
Rozwiązywanie incydentu przez 2 poziom wsparcia
Zamknięcie incydentu i ewaluacja
Raportowanie związane z zarządzaniem incydentami
Zarządzanie zespołem
Prośba o wykonanie zadania
Zarządzanie problemem
Kontrola operacji IT
Zarządzanie obiektami
Zarządzanie aplikacjami
Zarządzanie techniczne
Prośba o wykonanie zadania
Zarządzanie problemem
Zaplanowanie serwisu
Przekazanie serwisu
Ciągłe doskonalenie usługi
Proces związany z klientem
Dostawca procesu zew.


Process outside the IT Integration
ITIL Processes outside Service Operation
Service Operation
IT Service Management
Service Operation
Service Operation Processes
ITIL Processes outside Service Operation
Processes outside the IT Organization
Customer Process
Service Design
Service Transition
Event Management
Request Managment
Problem Management
IT Operations Control
Facilities Management
Application Management
Technical Management
Incident Management Supprot
Incident Logging & Categorization
Incident Monitoring & Escalation
Heading of Major Incidents
Immediate Incident Resolution by 1st Level Support
Pro-Active User Information
Incident Resolution by 2nd Level Support
Incident Closure & Evaluation
Incident Management Reporting
Request Fulliment
Promblem Management
Service Design
Service Transition
Continual Service Improvement
Customer Process
External Suppler Process

POLSKA PLATFORMA
BEZPIECZEŃSTWA WEWNĘTRZNEGO

Polska Platforma Bezpieczeństwa Wewnętrznego

ul. Słowackiego 17/11
60-822 Poznań
www.ppbw.pl
tel.: (61) 663 02 21
e-mail: standard-cyber@ppbw.pl

Fundusze Europejskie Inteligentny Rozwój
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Projekt pt.: „Cyberbezpieczeństwo – standard PPBW dla MŚP i instytucji publicznych" współfinansowany ze środków Unii Europejskiej.