

Wzór informacji zwrotnej dla Komitetu Audytu, zawierającej ustalenia z realizacji audytu rekomendowanego pn. *Wybrane zagadnienia w obszarze zarządzania ciągłością działania jednostki (bezpieczeństwo informacji)*.

I. Informacje ogólne

Nazwa jednostki	
Nazwisko i imię kierownika jednostki	
Nazwisko i imię kierownika komórki audytu (KAW)	
Kontakt telefoniczny do KAW	
Kontakt e-mail do KAW	
Audyt przeprowadzono w okresie	od.....do.....
Kto przeprowadził audyt	audytor wewnętrzny/ audytor wewnętrzny przy udziale eksperta z jednostki/ audytor wewnętrzny przy udziale eksperta zewnętrznego (<i>niepotrzebne skreślić</i>)
Liczba osobodni KAW przeznaczonych na realizację zadania audytowego	

II. Wyniki ustaleń audytu

Data ostatnio przeprowadzonego w jednostce audytu bezpieczeństwa informacji	
Czy w jednostce przeprowadzano corocznie audyt bezpieczeństwa informacji?	TAK/NIE (<i>niepotrzebne skreślić</i>)
Przyczyny braku przeprowadzania corocznych audytów bezpieczeństwa informacji	

Obiekt 1. Plan ciągłości działania systemów teleinformatycznych		
	TAK/NIE	KRÓTKIE UZASADNIENIE
1. Czy w jednostce wdrożono plan ciągłości działania systemów teleinformatycznych?		
2. Czy w ww. planie określono kompleksowo i precyzyjnie role, zadania i zakres odpowiedzialności uczestników procesu?		
3. Czy ww. plan ciągłości działania jest aktualny w części		

dotyczącej osób realizujących wyznaczone im zadania w sytuacji kryzysowej?		
4. Czy ww. plan ciągłości działania był okresowo aktualizowany, szczególnie w części dotyczącej infrastruktury teleinformatycznej, zasobów teleinformatycznych?		
5. Czy ww. plan ciągłości działania był okresowo testowany?		Jeśli tak, proszę wskazać datę ostatnio przeprowadzonego testu planu ciągłości działania systemów teleinformatycznych w jednostce
6. Czy w jednostce opracowano regulacje wewnętrzne w badanym zakresie?		
7. Czy obowiązujące regulacje wewnętrzne są aktualne?		
8. Czy obowiązujące regulacje wewnętrzne są kompletne?		
9. Czy obowiązujące regulacje wewnętrzne są adekwatne?		
10. Czy obowiązujące regulacje wewnętrzne są skuteczne?		
11. Czy stwierdzono zgodność z wymaganiami określonymi w § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI?		
12. Czy stwierdzono zgodność z regulacjami wewnętrznymi?		
13. Czy zidentyfikowano dobre praktyki w badanym zakresie? Jeśli tak, to proszę podać jakie.		
Ocena obiektu wg metodyki Cobit 4.1 (w skali 0-5)		

Obiekt 2. Zarządzanie incydentami bezpieczeństwa informacji		
	TAK/NIE	KRÓTKIE UZASADNIENIE
14. Czy opracowano regulacje wewnętrzne w badanym zakresie?		
15. Czy obowiązujące regulacje wewnętrzne są aktualne?		
16. Czy obowiązujące regulacje wewnętrzne są kompletne?		
17. Czy obowiązujące regulacje wewnętrzne są adekwatne?		
18. Czy obowiązujące regulacje wewnętrzne są skuteczne?		
19. Czy regulacje wewnętrzne określają definicję incydentu bezpieczeństwa informacji, tryb i sposób postępowania w przypadku jego zaistnienia, zadania i obowiązki osób uczestniczących w procesie		

(łącznie)?		
20. Czy regulacje wewnętrzne zakomunikowano uczestnikom procesu?		
21. Czy prowadzony jest rejestr incydentów bezpieczeństwa informacji?		
22. Ile incydentów bezpieczeństwa informacji zostało ujętych w ww. rejestrze w 2023 roku?		
23. Czy incydenty bezpieczeństwa obsługiwano zgodnie z regulacjami wewnętrznymi w tym zakresie?		
24. Czy działania służące wykrywaniu, reagowaniu oraz zapobieganiu występowaniu incydentów bezpieczeństwa informacji, w opinii audytora wewnętrznego, były skuteczne?		
25. Czy stwierdzono zgodność z wymaganiami określonymi w § 20 ust. 2 pkt 13 rozporządzenia KRI?		
26. Czy stwierdzono zgodność z regulacjami wewnętrznymi?		
27. Czy zidentyfikowano dobre praktyki w badanym zakresie? Jeśli tak, to proszę podać jakie.		
Ocena obiektu wg metodyki Cobit 4.1 (w skali 0-5)		

Obiekt 3. Kopie bezpieczeństwa		
	TAK/NIE	KRÓTKIE UZASADNIENIE
28. Czy opracowano regulacje wewnętrzne w badanym zakresie?		
29. Czy obowiązujące regulacje wewnętrzne są aktualne?		
30. Czy obowiązujące regulacje wewnętrzne są kompletne?		
31. Czy obowiązujące regulacje wewnętrzne są adekwatne?		
32. Czy obowiązujące regulacje wewnętrzne są skuteczne?		
33. Czy regulacje wewnętrzne zakomunikowano uczestnikom procesu?		
34. Czy wykonywane są kopie bezpieczeństwa danych w systemach teleinformatycznych organizacji według ustalonego harmonogramu?		
35. Czy kopie bezpieczeństwa są przechowywane w 2		

niezależnych lokalizacjach, tzn. co najmniej jedna kopia znajduje się w lokalizacji innej niż lokalizacja serwerowni?		
36. Czy kopie bezpieczeństwa są testowane pod względem ich jakości po odtworzeniu?		
37. Czy proces tworzenia i testowania kopii bezpieczeństwa jest dokumentowany?		
38. Czy stwierdzono zgodność z wymaganiami określonymi w § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI?		
39. Czy stwierdzono zgodność z regulacjami wewnętrznymi?		
40. Czy zidentyfikowano dobre praktyki w badanym zakresie? Jeśli tak, to proszę podać jakie.		
Ocena obiektu wg metodyki Cobit 4.1 (w skali 0-5)		

Obiekt 4. Analiza ryzyka bezpieczeństwa informacji i plan postępowania z ryzykiem		
	TAK/NIE	KRÓTKIE UZASADNIENIE
41. Czy opracowano regulacje wewnętrzne w badanym zakresie?		
42. Czy obowiązujące regulacje wewnętrzne są aktualne?		
43. Czy obowiązujące regulacje wewnętrzne są kompletne?		
44. Czy obowiązujące regulacje wewnętrzne są adekwatne?		
45. Czy obowiązujące regulacje wewnętrzne są skuteczne?		
46. Czy regulacje wewnętrzne zakomunikowano uczestnikom procesu?		
47. Czy w jednostce przeprowadzana jest okresowa analiza ryzyka utraty integralności, dostępności i poufności informacji?		
48. Czy opracowano plan postępowania z ryzykiem bezpieczeństwa informacji?		
49. Czy proces analizy ryzyka bezpieczeństwa informacji jest dokumentowany?		
50. Czy wyniki analizy ryzyka bezpieczeństwa informacji wraz z planem postępowania z ryzykiem są przekazywane kierownikowi jednostki?		
51. Czy podejmowane w jednostce działania związane z		

minimalizowaniem ryzyka utraty informacji w wyniku awarii wynikały z analizy ryzyka i planu postępowania z ryzykiem?		
52. Czy stwierdzono zgodność z wymaganiami określonymi w § 20 ust. 2 pkt 3 rozporządzenia KRI?		
53. Czy stwierdzono zgodność z regulacjami wewnętrznymi?		
54. Czy zidentyfikowano dobre praktyki w badanym zakresie? Jeśli tak, to proszę podać jakie.		
Ocena obiektu wg metodyki Cobit 4.1 (w skali 0-5)		

III. Ocena stanu zarządzania w obiektach audytu, wg modelu dojrzałości stosowanego w metodyce COBIT 4.1.

Obiekty audytu	Kryteria oceny				Ocena obiektów audytu
	Legalność	Skuteczność	Kompletność	Adekwatność	
1. Plan ciągłości działania systemów teleinformatycznych	Ocena audytora	Ocena audytora	Ocena audytora	Ocena audytora	Ocena audytora
2. Zarządzanie incydentami bezpieczeństwa informacji	Ocena audytora	Ocena audytora	Ocena audytora	Ocena audytora	Ocena audytora
3. Kopie bezpieczeństwa	Ocena audytora	Ocena audytora	Ocena audytora	Ocena audytora	Ocena audytora
4. Analiza ryzyka i plan postępowania z ryzykiem	Ocena audytora	Ocena audytora	Ocena audytora	Ocena audytora	Ocena audytora

IV. Ocena stanu zarządzania w badanym obszarze

Ocena wg modelu dojrzałości stosowanego w metodyce COBIT 4.1.						
Kryterium	0 Nieistniejące	1 Wstępne /dorażne	2 Powtarzalne lecz intuicyjne	3 Zdefiniowane procesy	4 Kontrolowane i mierzalne	5 Zoptymalizowane

Legalność						
Skuteczność						
Kompletność						
Adekwatność						
Ogólna ocena zarządzania						
Ocena kontroli zarządczej wg poziomów¹						

V. Informacja o zaleceniach audytu

Liczba wydanych zaleceń ogółem	
w tym na poziomie istotności:	
kluczowym	
znaczącym	
niskim	
Proszę wymienić wszystkie zalecenia o kluczowym poziomie istotności (o ile takie wydano)	1. 2. 3.

¹ Poziomy funkcjonowania kontroli zarządczej: 1 - nie funkcjonuje, 2 - funkcjonuje w ograniczonym zakresie, 3 - funkcjonuje.