EBA/GL/2017/05

11/09/2017

Wytyczne

Wytyczne w sprawie oceny ryzyka technologii informacyjno-komunikacyjnych w ramach procesu przeglądu i oceny nadzorczej (SREP)

1. Zgodność i obowiązki sprawozdawcze

Status niniejszych wytycznych

1. Niniejszy dokument zawiera wytyczne wydane zgodnie z art. 16 rozporządzenia (UE) nr 1093/20101. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy i instytucje finansowe dokładają wszelkich starań, aby zastosować się do tych wytycznych i zaleceń.

2. Wytyczne przedstawiają stanowisko EUNB w sprawie odpowiednich praktyk nadzoru w ramach Europejskiego Systemu Nadzoru Finansowego lub tego, jak należy stosować prawo europejskie w konkretnym obszarze. Właściwe organy określone w art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010, do których wytyczne mają zastosowanie, powinny stosować się do wytycznych poprzez wprowadzenie ich odpowiednio do swoich praktyk (np. poprzez dostosowanie swoich ram prawnych lub procesów nadzorczych), również jeżeli wytyczne są skierowane przede wszystkim do instytucji.

Wymogi dotyczące sprawozdawczości

3. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy muszą poinformować EUNB, czy stosują się lub czy zamierzą zastosować się do niniejszych wytycznych lub danego zalecenia lub podają powody niestosowania się do dnia 13.11.2017. W przypadku braku informacji w tym terminie właściwe organy zostaną uznane przez EUNB za niestosujące się do niniejszych wytycznych. Informacje należy przekazać poprzez wysłanie formularza dostępnego na stronie internetowej EUNB na compliance@eba.europa.eu z dopiskiem „EBA/GL/2017/05”. Informacje przekazują osoby upoważnione do informowania o niestosowaniu się do wytycznych w imieniu właściwych organów. Wszelkie zmiany dotyczące stosowania się do wytycznych także należy zgłaszać do EUNB.

4. Zgodnie z art. 16 ust. 3 przekazywane informacje publikuje się na stronie internetowej EUNB.

1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12).

2. Przedmiot, zakres stosowania i definicje

Przedmiot i zakres stosowania

5. Niniejsze wytyczne sporządzone na podstawie art. 107 ust. 3 dyrektywy 2013/36/UE[2] mają na celu zapewnienie zbieżności praktyk nadzorczych w ocenie ryzyka technologii informacyjno-komunikacyjnych (ICT) w ramach procesu przeglądu i oceny nadzorczej (SREP), o którym mowa w art. 97 dyrektywy 2013/36/UE i który został szczegółowo omówiony w Wytycznych EUNB dotyczących wspólnych procedur i metod stosowanych w ramach procesu przeglądu i oceny (SREP)[3]. W wytycznych określono w szczególności kryteria oceny, które właściwe organy powinny stosować w ocenie nadzorczej zarządzania i strategii instytucji w obszarze technologii informacyjno-komunikacyjnych oraz w ocenie nadzorczej kontroli i ekspozycji na ryzyko związane z technologiami informacyjno-komunikacyjnymi. Niniejsze wytyczne stanowią integralną część wytycznych EUNB dotyczących SREP.

6. Właściwe organy powinny stosować wytyczne zgodnie z poziomem stosowania SREP określonym w wytycznych EUNB dotyczących SREP oraz zgodnie z zasadami minimalnego zaangażowania i wymogami proporcjonalności w nich ustanowionymi.

Adresaci

7. Niniejsze wytyczne są skierowane do właściwych organów, o których mowa w art. 4 ust. 2 ppkt (i) rozporządzenia (UE) nr 1093/2010.

[2] Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (1) - Dz.U. L 176 z 27.6.2012, s. 338).

[3] EBA/GL/2014/13

Definicje

8. O ile nie określono inaczej, pojęcia stosowane i zdefiniowane w dyrektywie 2013/36/WE i rozporządzeniu (UE) nr 575/2013 oraz definicje z wytycznych EUNB dotyczących SREP mają w niniejszych wytycznych takie samo znaczenie. Ponadto do celów niniejszych wytycznych stosuje się następujące definicje:

Systemy ICT	Ustanowienie ICT jako części mechanizmu lub sieci połączonej wspierającego operacje danej instytucji.
Usługi ICT	Usługi świadczone przez systemy ICT na rzecz jednego lub kilku użytkowników wewnętrznych lub zewnętrznych. Przykłady obejmują wprowadzanie danych, przechowywanie danych, przetwarzanie danych oraz usługi sprawozdawczości, lecz również monitorowanie usługi wspierania przedsiębiorstw i decyzji.
Ryzyko związane z dostępnością i ciągłością ICT	Ryzyko negatywnego wpływu na wyniki oraz dostępność systemów i danych ICT, w tym niezdolność do terminowego przywrócenia usług instytucji ze względu na awarię elementów sprzętu lub oprogramowania ICT, braki w zarządzaniu systemem ICT lub wszelkie inne zdarzenia omówione w Załączniku poniżej.
Ryzyko związane z bezpieczeństwem ICT	Ryzyko nieupoważnionego dostępu do systemów i danych ICT w instytucji lub spoza instytucji (np. cyberataki), jak omówiono w Załączniku.
Ryzyko związane ze zmianą ICT	Ryzyko wynikające z niezdolności instytucji do zarządzania zmianami systemu ICT w terminowy i kontrolowany sposób, zwłaszcza w przypadku szeroko zakrojonych i kompleksowych programów zmiany, jak omówiono w Załączniku.
Ryzyko związane z integralnością danych ICT	Ryzyko, że dane zgromadzone i przetwarzane przez systemy ICT są niekompletne, niedokładne lub niespójne w różnych systemach ICT, na przykład w wyniku niedostatecznych kontroli podczas różnych etapów cyklu życia danych ICT (tj. projektowania architektury danych, tworzenia modelu danych lub słowników danych, sprawdzania wprowadzonych danych, kontroli ekstrakcji, przesyłania i przetwarzania danych włącznie z wydanymi danymi wyjściowymi) lub braku takich kontroli, zakłócania zdolności instytucji do świadczenia usług i wytwarzania informacji na temat zarządzania (ryzykiem) i finansów) w prawidłowy i terminowy sposób, jak omówiono w

	Załączniku.
Ryzyko związane z outsourcingiem ICT	Ryzyko, że zaangażowanie osoby trzeciej lub innego podmiotu Grupy (outsourcing wewnątrzgrupowy) w świadczenie systemów ICT lub powiązanych usług negatywnie wpłynie na wynik instytucji i zarządzanie ryzykiem, jak objaśniono w Załączniku.

3. Wykonanie

Data rozpoczęcia stosowania

9. Niniejsze wytyczne mają zastosowanie od dnia 1 stycznia 2018 r.

4. Wymogi związane z oceną ryzyka ICT

Tytuł 1 - Przepisy ogólne

10. Właściwe organy powinny przeprowadzić ocenę ryzyka ICT i mechanizmów zarządzania oraz strategii ICT jako część procesu SREP zgodnie z zasadami minimalnego zaangażowania i kryteriami proporcjonalności określonymi w tytule 2 wytycznych EUNB dotyczących SREP. Oznacza to w szczególności, że:

    a. częstotliwość oceny ryzyka ICT będzie zależała od zasad minimalnego zaangażowania wynikających z kategorii SREP, do której dana instytucja jest przypisana oraz jej specjalnego programu oceny nadzorczej oraz

    b. zakres, szczegółowość i intensywność oceny ICT powinny być proporcjonalne do wielkości, struktury i środowiska operacyjnego instytucji, a także charakteru, skali i kompleksowości jej działań.

11. Zasada proporcjonalności ma zastosowanie w niniejszych wytycznych do zakresu, częstotliwości i intensywność zaangażowania nadzorczego i dialogu z instytucją oraz oczekiwań nadzorczych związanych z normami, które instytucja powinna stosować.

12. Właściwe organy mogą opierać się na pracach już przeprowadzonych przez instytucję lub właściwy organ w kontekście oceny innych rodzajów ryzyka elementów SREP oraz uwzględnić te prace w celu aktualizacji oceny. W szczególności, przeprowadzając oceny określone w niniejszych wytycznych właściwe organy powinny wybrać najodpowiedniejsze podejście i najodpowiedniejszą metodologię w zakresie oceny nadzorczej, które są najlepiej dostosowane do instytucji i proporcjonalne, a właściwe organy powinny wykorzystać istniejące i dostępne dokumenty (np. odpowiednie sprawozdania i inne dokumenty, zebrania z kadrą zarządzającą (ryzykiem), ustalenia z kontroli na miejscu) w celu przekazania informacji o ocenie właściwych organów.

13. Właściwe organy powinny podsumować ustalenia z przeprowadzonych ocen kryteriów określonych w niniejszych wytycznych i wykorzystać je do celów opracowania wniosków z oceny elementów SREP zgodnie z wytycznymi EUNB dotyczącymi SREP.

14. Ocena zarządzania i strategii ICT przeprowadzona zgodnie z tytułem 2 niniejszych wytycznych powinna w szczególności prowadzić do ustaleń zawierających podsumowanie ustaleń dotyczących elementu SREP dotyczącego oceny zarządzania wewnętrznego i kontroli w całej instytucji zgodnie z tytułem 5 wytycznych EUNB dotyczących SREP oraz znajdować odzwierciedlenie w odpowiedniej punktacji tego elementu SREP. Ponadto właściwe organy powinny wziąć pod uwagę, że każdy istotny negatywny wpływ oceny strategii ICT na strategię biznesową instytucji lub wszelkie obawy, które instytucja ma niewystarczające zasoby ICT i zdolności w zakresie ICT do przeprowadzania i wspierania ważnych

planowanych zmian strategicznych, powinien zostać odnotowany w analizie modelu biznesowego przeprowadzonej zgodnie z tytułem 4 wytycznych EUNB dotyczących SREP.

15. Wynik oceny ryzyka ICT, jak określono w tytule 3 niniejszych wytycznych, powinien dostarczać informacje o ustaleniach w wyniku oceny ryzyka operacyjnego. Należy traktować go jako informację o odpowiedniej punktacji zgodnie z tytułem 6.4 wytycznych EUNB dotyczących SREP.

16. Zwraca się uwagę, że chociaż zazwyczaj właściwe organy powinny ocenić podkategorie ryzyka w ramach głównych kategorii (tj. ryzyko ICT zostanie ocenione jako część ryzyka operacyjnego), jeżeli właściwe organy uznają określone podkategorie za istotne, mogą dokonać ich oceny w sposób indywidualny. Jeżeli w związku z tym ryzyko ICT miałoby zostać określone przez właściwy organ jako ryzyko poważne, niniejsze wytyczne zawierają również tabelę punktów (tabela 1), która powinna służyć do informowania o punktacji każdej podkategorii oddzielnie w odniesieniu do ryzyka ICT w wyniku ogólnego podejścia do punktacji ryzyka w odniesieniu do kapitału w wytycznych EUNB dotyczących SREP

17. Aby sprawdzić, czy ryzyko ICT należy uznać za poważne, co wiąże się z możliwością oceny i punktacji ryzyka ICT jako oddzielnej podkategorii ryzyka operacyjnego, właściwe władze mogą zastosować kryteria określone w sekcji 6.1 wytycznych EUNB dotyczących SREP.

18. Podczas stosowania wytycznych właściwe organy powinny, w stosownym przypadku, uwzględnić niewyczerpujący wykaz podkategorii ryzyka ICT i scenariuszy ryzyka, zgodnie z Załącznikiem, z zastrzeżeniem, że w Załączniku położono nacisk na ryzyko ICT, które może prowadzić do strat o poważnych skutkach. Właściwe organy mogą wykluczyć niektóre rodzaje ryzyka ICT uwzględnione w taksonomii, jeżeli nie są istotne dla oceny. Oczekuje się, że instytucje utrzymają własne taksonomie ryzyka niż będą stosować taksonomię ryzyka ICT ustanowioną w Załączniku.

19. W przypadku gdy niniejsze wytyczne stosuje się w odniesieniu do transgranicznych grup bankowych i ich podmiotów oraz powołano kolegium organów nadzoru, zaangażowane właściwe organy powinny, w kontekście swojej współpracy w ramach oceny SREP określonej w sekcji 11.1 wytycznych EUNB dotyczących SREP, uspójnić w maksymalnym zakresie ścisły i szczegółowy zakres poszczególnych informacji w sposób jednolity dla wszystkich podmiotów grupy.

Tytuł 2 - Ocena zarządzania i strategii instytucji w zakresie ICT

2.1 Zasady ogólne

20. Właściwe organy powinny ocenić, czy ogólne zarządzanie instytucji oraz ramy kontroli wewnętrznej należycie uwzględniają systemy ICT i powiązane rodzaje ryzyka, a jeżeli organ zarządzający odpowiednio zajmuje się i zarządza tymi aspektami, jako że ICT stanowią integralny element prawidłowego funkcjonowania instytucji.

21. Przeprowadzając ocenę, właściwe organy powinny powołać się na wymogi i normy dobrego zarządzania wewnętrznego oraz na ustalenia w zakresie kontroli ryzyka zgodnie z Wytycznymi EUNB w sprawie zarządzania wewnętrznego (GL 44)[4] oraz wytyczne międzynarodowe w tym obszarze w zakresie, w jakim mają one zastosowanie w świetle specyfiki systemów i rodzajów ryzyka ICT.

22. Ocena, o której mowa w niniejszym tytule, nie obejmuje konkretnych elementów zarządzania systemem ICT, zarządzania ryzykiem i kontroli, które są ukierunkowane na zarządzanie specjalnymi rodzajami ryzyka ICT, o których mowa w tytule 3 niniejszych wytycznych, lecz dotyczy następujących obszarów:

    a. strategii ICT - czy instytucja ma strategię w obszarze ICT, która podlega odpowiedniemu zarządzaniu i jest zgodna ze strategią biznesową instytucji;

    b. ogólnego zarządzania wewnętrznego – czy ogólne ustalenia instytucji dotyczące zarządzania wewnętrznego są adekwatne w stosunku do systemów ICT instytucji oraz

    c. ryzyka ICT w ramach zarządzania ryzykiem instytucji – czy zarządzanie ryzykiem w instytucji i ramy kontroli wewnętrznej zapewniają odpowiednie zabezpieczenia systemom ICT instytucji.

23. Litera a) przywołana w ust. 22, w kontekście dostarczania informacji o elementach zarządzania w instytucji, powinna stanowić podstawę oceny modelu biznesowego, o którym mowa w tytule 4 wytycznych EUNB w sprawie SREP. Litery b) i c) uzupełniają oceny tematów, o których mowa w tytule 5 wytycznych EUNB dotyczących SREP, a ocena opisana w niniejszych wytycznych zostanie wykorzystana w odpowiedniej ocenie na podstawie tytułu 5 wytycznych EUNB dotyczących SREP.

24. Wynik tej oceny powinien, w stosownym przypadku, uzupełniać ocenę zarządzania ryzykiem i kontroli, o której mowa w tytule 3 niniejszych wytycznych.

2.2 Strategia ICT

25. Na podstawie niniejszej sekcji właściwe organy powinny ocenić, czy instytucja posiada strategię ICT, która podlega odpowiedniemu nadzorowi ze strony organu zarządzającego instytucji, jest spójna ze

[4] Wytyczne EUNB w sprawie zarządzania wewnętrznego, GL 44 z dnia 27 września 2011 r.

strategią biznesową, zwłaszcza jeżeli chodzi o aktualizację ICT oraz planowanie lub wdrażanie ważnych i kompleksowych zmian ICT, a także wspiera model biznesowy instytucji.

2.2.1 Rozwój i adekwatność strategii ICT

26. Właściwe organy powinny ocenić, czy instytucja wdrożyła odpowiednie ramy, proporcjonalne do charakteru, skali i kompleksowości działań ICT, w celu przygotowania i rozwoju strategii ICT instytucji. Przy przeprowadzaniu tej oceny właściwe organy powinny uwzględnić, czy:

    a. kierownictwo wyższego szczebla[5] linii biznesowej(-ych) jest odpowiednio zaangażowane w definicję strategicznych priorytetów ICT instytucji oraz czy kierownictwo wyższego szczebla komórki ICT jest świadome rozwoju, projektowania i wdrażania kluczowych strategii i inicjatyw biznesowych w celu zapewnienia ciągłego dostosowania między systemami ICT, usługami ICT i komórką ICT (tj. osobami odpowiedzialnymi za zarządzanie i wdrażanie tych systemów i usług) a strategią biznesową instytucji, a także czy ICT są skutecznie aktualizowane;

    b. strategia ICT jest dokumentowana i wspierana konkretnymi planami wdrażania, zwłaszcza jeżeli chodzi o kluczowe etapy i planowanie zasobów (w tym zasobów finansowych i ludzkich) w celu zapewnienia, że są realistyczne i umożliwiają wprowadzenie strategii ICT;

    c. instytucja okresowo aktualizuje swoją strategię ICT, zwłaszcza podczas zmiany strategii biznesowej, aby zapewnić ciągłe dostosowanie celów, planów i działań biznesowych w ujęciu średnio- lub długoterminowym do ICT, oraz

    d. organ zarządzający instytucji zatwierdza strategię ICT i plany wdrażania oraz monitoruje jej wdrażanie.

2.2.2 Wdrażanie strategii ICT

27. Jeżeli strategia ICT instytucji wiąże się z wymogiem wdrożenia ważnych i kompleksowych zmian ICT lub zmian o istotnych implikacjach dla modelu biznesowego instytucji, właściwe organy powinny ocenić, czy instytucja posiada ramy kontroli odpowiednie do jej wielkości, działalności w obszarze ICT oraz poziomu działań związanych ze zmianą w celu wspierania skutecznego wdrażania strategii ICT instytucji. Przy przeprowadzaniu tej oceny właściwe organy powinny uwzględnić, czy ramy kontroli:

    a. obejmują procesy zarządzania (np. postępy i monitorowanie budżetu oraz sprawozdawczość w tych obszarach) i odpowiednie organy (np. biuro zarządzania projektami, grupę sterowania ICT lub równoważne jednostki) w celu skutecznego wspierania wdrażania programów strategicznych ICT;

    b. przewidują definicje i przydział ról i obowiązków w celu wdrożenia programów strategicznych ICT, ze zwróceniem szczególnej uwagi na doświadczenie kluczowych zainteresowanych stron w organizowaniu, sterowaniu i monitorowaniu ważnych i kompleksowych zmian ICT oraz

[5] Kierownictwo wyższego szczebla i organ zarządzający zgodnie z definicją w dyrektywie 2013/36/UE z dnia 26 czerwca 2013 r., w art. 3 pkt 7 („organ zarządzający") i art. 3 pkt 9 („kierownictwo wyższego szczebla").

zarządzanie dużymi organizacjami i wpływ na zasoby ludzkie (tj. zarządzanie niechęcią do zmian, szkolenia, komunikacja).

c. zapewniają niezależne komórki kontroli i audytu wewnętrznego w celu zagwarantowania, że ryzyko powiązane z wdrażaniem strategii ICT zostało zidentyfikowane, ocenione i skutecznie ograniczone oraz że wprowadzone ramy zarządzania w celu wdrażania strategii są skuteczne; oraz

d. obejmują proces planowania i przeglądu planowania, który zapewnia elastyczność reagowania na ważnego stwierdzone problemy (np. napotkane problemy z wdrażaniem lub opóźnienia) lub zmiany zewnętrzne (np. ważne zmiany w środowisku biznesowym, kwestie technologiczne lub innowacje), aby zapewnić terminowe dostosowanie strategicznego planu wdrażania.

2.3 Ogólne zarządzanie wewnętrzne

28. Zgodnie z tytułem 5 wytycznych EUNB dotyczących SREP właściwe organy powinny ocenić, czy instytucja posiada odpowiednią i przejrzystą strukturę korporacyjną, która „odpowiada potrzebom", i czy wdrożyła stosowne mechanizmy zarządzania. W odniesieniu do systemów ICT oraz zgodnie z Wytycznymi EUNB w sprawie zarządzania wewnętrznego ocena ta powinna służyć ustaleniu, czy instytucja:

    a. posiada solidną i przejrzystą strukturę organizacyjną z jasnym podziałem obowiązków w obszarze ICT, włącznie z organem zarządzającym i jego komitetami, a osoby pełniące kluczową odpowiedzialność za ICT (np. dyrektor ds. informatyki, dyrektor operacyjny lub osoby pełniące równoważne funkcje) mają odpowiedni pośredni lub bezpośredni dostęp do organu zarządzającego, aby zapewnić odpowiednie zgłaszanie i omawianie ważnych informacji lub problemów mających związek z ICT oraz podejmowanie decyzji w tych sprawach na szczeblu organu zarządzającego; oraz

    b. a organ zarządzający zna i rozwiązuje kwestie związane z ryzykiem w obszarze ICT;

29. Oprócz sekcji 5.2 wytycznych EUNB dotyczących SREP właściwe organy powinny ocenić, czy polityka i strategia outsourcingu ICT uwzględnia, w stosownym przypadku, wpływ outsourcingu ICT na działalność i model biznesowy instytucji.

2.4 Ryzyko ICT w ramach zarządzania ryzykiem instytucji

30. Podczas oceny ogólnego zarządzania ryzykiem w instytucji oraz kontroli wewnętrznych zgodnie z tytułem 5 wytycznych EUNB dotyczących SREP właściwe organy powinny rozważyć, czy ramy zarządzania ryzykiem i kontroli wewnętrznych instytucji zapewniają odpowiednie zabezpieczenie systemów ICT instytucji w taki sposób, który jest dostosowany do wielkości i działań instytucji oraz jej profilu ryzyka ICT zgodnie z tytułem 3. Właściwe organy powinny w szczególności określać:

    a. czy gotowość do podejmowania ryzyka oraz ICAAP obejmują ryzyko ICT, w ramach szerszej kategorii ryzyka operacyjnego, na potrzeby definicji ogólnej strategii ryzyka i ustalenia kapitału wewnętrznego oraz

b. ryzyko ICT mieści się w zakresie ogólnego zarządzania ryzykiem w instytucji oraz w ramach kontroli wewnętrznej.

31. Właściwe organy powinny przeprowadzić ocenę w ramach lit. a) powyżej z uwzględnieniem obydwu oczekiwanych i przeciwnych scenariuszy, np. scenariuszy uwzględnionych w teście warunków skrajnych specyficznym dla instytucji lub teście warunków skrajnych o charakterze nadzorczym.

32. Ze szczególnym uwzględnieniem lit. b) właściwe organy powinny ocenić, czy komórki niezależnej kontroli i audytu wewnętrznego, wyszczególnione w ust. 104 lit. a), 104 lit. d), 105 lit. c) wytycznych EUNB dotyczących SREP są w stanie zapewnić odpowiedni poziom niezależności między ICT a komórkami kontroli i audytu, mając na uwadze wielkość oraz profil ryzyka ICT instytucji.

2.5 Podsumowanie ustaleń

33. Wyniki powinny znaleźć odzwierciedlenie w podsumowaniu ustaleń, o których mowa w tytule 5 wytycznych EUNB dotyczących SREP i stanowić część odpowiedniej punktacji zgodnie z uwagami w tabeli 3 wytycznych EUNB dotyczących SREP.

34. W celu oceny strategii ICT przy jej przeprowadzaniu należy uwzględnić następujące punkty:

a. czy właściwe organy doszły do wniosku, że ramy zarządzania instytucji są nieadekwatne na potrzeby opracowania i wdrożenia strategii ICT instytucji na podstawie pkt 2.2, a dane te powinny zostać wykorzystane w ocenie zarządzania wewnętrznego instytucji, o której mowa w tytule 5 pkt 87 lit. a) wytycznych EUNB dotyczących SREP;

b. jeżeli właściwe organy dojdą do wniosku na podstawie powyższych ocen w pkt 2.2, że nastąpiłoby znaczne przesunięcie między strategią ICT a strategią biznesową, które miałoby znaczny niekorzystny wpływ na długoterminową działalność instytucji lub jej cele finansowe, zrównoważony rozwój instytucji lub jej model biznesowy, lub też obszary działalności/linie biznesowe instytucji, które zostały określone jako najistotniejsze w ust. 62 lit. a) wytycznych EUNB dotyczących SREP, a następnie informacje te powinny być wykorzystane do oceny modelu biznesowego, o której mowa w tytule 4 wytycznych dotyczących SREP, pkt 70 lit. b) i c) oraz

c. jeżeli właściwe organy dojdą do wniosku na podstawie powyższych ocen w pkt 2.2, że instytucja nie ma dostatecznych zasobów ICT i zdolności z zakresu wdrażania ICT do przeprowadzenia i wspierania ważnych planowanych zmian strategicznych, informacja ta powinna znaleźć się w ocenie modelu biznesowego, o której mowa w tytule 4 pkt 70 lit. b) wytycznych EUNB dotyczących SREP.

Tytuł 3 - Ocena kontroli i ekspozycji instytucji na ryzyko ICT

3.1 Uwagi ogólne

35. Właściwe organy powinny ocenić, czy instytucja odpowiednio określiła, oceniła i ograniczyła swoje ryzyka ICT. Proces ten powinien być częścią ram operacyjnego zarządzania ryzykiem i zbieżny z podejściem mającym zastosowanie do ryzyka operacyjnego.

36. Właściwe organy powinny najpierw określić istotne rodzaje nieodłącznego ryzyka ICT, na które instytucja jest lub może być narażona, a następnie ocenić skuteczność ram, procedur i kontroli zarządzania ryzykiem ICT instytucji w celu ograniczenia ryzyka. Wynik kontroli powinien znaleźć odzwierciedlenie w podsumowaniu ustaleń, które jest wykorzystywane do punktacji ryzyka operacyjnego w wytycznych dotyczących SREP. Jeżeli ryzyko ICT jest uznawane za istotne, a właściwe organy chcą przyznać indywidualną punktację, wówczas należy wykorzystać tabelę 1 do przyznania punktacji w postaci podryzyka ryzyka operacyjnego.

37. Przy przeprowadzaniu oceny na podstawie tego tytułu właściwe organy powinny wykorzystać wszystkie dostępne źródła informacji określone w tytule 6 ust. 127 wytycznych EUNB dotyczących SREP, np. działania instytucji z zakresu zarządzania ryzykiem, sprawozdawczość i wyniki, jako podstawę do identyfikacji ich nadzorczych priorytetów oceny. Właściwe organy powinny również wykorzystać inne źródła informacji do przeprowadzenia oceny, w tym, w stosownym przypadku, następujące źródła:

    a. samodzielną ocenę kontroli i ryzyka ICT (jeżeli została uwzględniona w informacjach ICAAP);
    b. informacje zarządcze powiązane z ryzykiem ICT przedłożone organowi zarządczemu instytucji, np. okresowe lub pojedyncze sprawozdania dotyczące ryzyka ICT (w tym baza danych dotycząca strat operacyjnych), dane dotyczące ekspozycji na ryzyko ICT przekazane przez komórkę zarządzania ryzykiem instytucji;
    c. ustalenia z audytu wewnętrznego i zewnętrznego powiązane z ICT zgłoszone komitetowi ds. audytu instytucji.

3.2 Określenie istotnych rodzajów ryzyka ICT

38. Właściwe organy powinny na bieżąco oceniać istotne rodzaje ryzyka, na jakie narażona jest lub może być instytucja, za pomocą przedstawionych poniżej działań.

3.2.1 Przegląd profilu ryzyka ICT instytucji

39. Podczas przeglądu profilu ryzyka ICT instytucji właściwe organy powinny rozważyć wszelkie odpowiednie informacje na temat ekspozycji instytucji na ryzyko ICT, w tym informacje, o których mowa w ust. 37 i stwierdzone poważne niedociągnięcia lub słabości w organizacji ICT i kontrolach obejmujących całą

instytucję na podstawie tytułu 2 niniejszych wytycznych, a w stosownym przypadku, przegląd tych informacji w proporcjonalny sposób. W ramach przeglądu właściwe organy powinny rozważyć:

a. potencjalny wpływ znacznych zakłóceń systemów ICT instytucji na system finansowy, zarówno na szczeblu krajowym, jak i międzynarodowym;
b. czy instytucja może być przedmiotem ryzyka bezpieczeństwa ICT lub ryzyka związanego z dostępnością i ciągłością ICT w wyniku zależności internetowych, wysokiego poziomu przyjętych innowacyjnych rozwiązań ICT lub innych biznesowych kanałów dystrybucji, które mogą uczynić z niej bardziej prawdopodobny cel cyberataków;
c. czy instytucja może być bardziej narażona na ryzyko bezpieczeństwa ICT, ryzyko związane z dostępnością i ciągłością, ryzyko związane z integralnością danych ICT lub ryzyko związane ze zmianą ICT ze względu na kompleksowość (np. w wyniku fuzji lub przejęć) lub przestarzałość systemów ICT;
d. czy instytucja wprowadza istotne zmiany do swoich systemów ICT lub komórki ICT (np. w wyniku fuzji, przejęć, zbycia lub przemieszczenia swoich kluczowych systemów ICT), co może mieć negatywny wpływ na stabilność lub prawidłowe funkcjonowanie systemów ICT i może prowadzić do istotnego ryzyka związanego z dostępnością i ciągłością ICT, ryzyka bezpieczeństwa ICT, ryzyka związanego ze zmianą ICT lub ryzyka związanego z integralnością danych ICT;
e. czy instytucja korzystała z outsourcingu usług ICT lub systemów ICT w ramach grupy lub poza nią, przez co mogła być narażona na istotne ryzyko związane z outsourcingiem ICT;
f. czy instytucja wdraża agresywne środki mające na celu ograniczenie kosztów ICT, które może prowadzić do ograniczenia koniecznych inwestycji w ICT, zasobów i wiedzy fachowej w dziedzinie informatyki i może zwiększyć ekspozycję na wszystkie rodzaje ryzyka ICT w taksonomii;
g. czy lokalizacja ważnych operacji/centrów danych ICT (np. regiony, kraje) może narażać instytucje na klęski żywiołowe (np. powodzie, trzęsienia ziemi), niestabilność polityczną lub konflikty pracownicze i niepokoje społeczne, które mogą prowadzić do istotnego wzrostu ryzyka związanego z dostępnością i ciągłością ICT oraz ryzyka bezpieczeństwa ICT.

3.2.2 Przegląd krytycznych systemów i usług ICT

40. W ramach procesu określania ryzyka ICT z potencjalnym istotnym wpływem ostrożnościowym na instytucję właściwe organy powinny dokonać przeglądu dokumentacji instytucji oraz wydać opinię, w jakim zakresie systemy i usługi ICT są krytyczne dla odpowiedniego funkcjonowania, dostępności, ciągłości i bezpieczeństwa kluczowych działań instytucji.

41. W tym celu właściwe organy powinny dokonać przeglądu metodologii i procesów stosowanych przez instytucję w celu określenia systemów i usług ICT, które są krytyczne, mając na uwadze, że niektóre systemy i usługi ICT mogą zostać uznane za krytyczne przez instytucje z perspektywy ciągłości i dostępności, bezpieczeństwa (np. zapobiegania nadużyciom) oraz poufności (np. poufnych danych). Dokonując przeglądu, właściwe organy powinny mieć na względzie, że krytyczne systemy i usługi ICT powinny spełniać co najmniej jeden z następujących warunków:

a. wspierają podstawowe operacje biznesowe i kanały dystrybucji (np. bankomaty, bankowość internetowa i mobilna) instytucji;

b. wspierają istotne procesy zarządzania i funkcje korporacyjne, w tym zarządzanie ryzykiem (np. systemy zarządzania ryzykiem i środkami pieniężnymi);

c. podlegają specjalnym wymogom ustawowym i wykonawczym (jeżeli podlegają), które obejmują coraz większe wymogi w zakresie dostępności, odporności lub bezpieczeństwa (np. przepisy dotyczące ochrony danych lub możliwego „maksymalnego czasu wznowienia funkcji" – maksymalnego czasu, w którym system lub proces musi zostać przywrócony po incydencie oraz akceptowalnego poziomu utraty danych – maksymalnego czasu, w którym dane mogą zostać utracone w przypadku incydentu) w przypadku niektórych ważnych usług systemowych (w stosownym przypadku);

d. przetwarzają lub przechowują dane poufne lub chronione, do których nieupoważniony dostęp mógłby mieć znaczny wpływ na reputację instytucji, wyniki finansowe lub kondycję albo ciągłość działalności (np. bazy danych z wrażliwymi danymi klientów) oraz

e. zapewniają podstawowe funkcje, które są kluczowe dla odpowiedniego funkcjonowania instytucji (np. usługi telekomunikacyjne i usługi łączności, usługi ICT i usługi bezpieczeństwa cybernetycznego).

3.2.3 Identyfikacja istotnych rodzajów ryzyka w odniesieniu do krytycznych systemów i usług ICT

42. Mając na uwadze przeprowadzone przeglądy profilu ryzyka ICT instytucji i krytycznych systemów i usług ICT powyżej, właściwe organy powinny wydać opinię na temat istotnych ryzyk ICT, które, z perspektywy nadzorczej, mogą mieć znaczny wpływ ostrożnościowy na krytyczne systemy i usługi ICT instytucji.

43. Podczas oceny potencjalnego wpływu ryzyka ICT na krytyczne systemy i usługi ICT instytucji, właściwe organy powinny uwzględnić:

a. wpływ finansowy, w tym (lecz nie wyłącznie) utratę środków lub aktywów, potencjalne rekompensaty dla klientów, koszty prawne i koszty zaradcze, szkody umowne, utratę dochodów;

b. potencjalne zakłócenia w prowadzeniu działalności, z uwzględnieniem (lecz nie wyłącznie) krytyczności narażonych usług finansowych, liczby klientów lub oddziałów i pracowników potencjalnie narażonych;

c. potencjalny wpływ na renomę instytucji na podstawie krytyczności narażonej obsługi bankowej lub działalności operacyjnej (np. kradzież danych klientów), profil zewnętrzny/eksponowanie narażonych systemów i usług ICT (np. systemy mobilne lub systemy bankowości internetowej, punkt sprzedaży, bankomaty lub systemy płatności);

d. wpływ regulacyjny, w tym możliwość cenzury publicznej ze strony organu regulacyjnego, kar pieniężnych lub nawet zmiany pozwoleń.

e. Strategiczny wpływ na instytucję, na przykład jeżeli produkt strategiczny lub plan biznesowy ulegną naruszeniu lub kradzieży.

44. Właściwe organy powinny zatem zakwalifikować stwierdzone ryzyka ICT, które są uznawane za istotne, do następujących kategorii ryzyka ICT, które zostały dodatkowo opisane i zilustrowane przykładami w Załączniku. Właściwe organy powinny określić w odniesieniu do rodzajów ryzyka ICT w Załączniku w ramach oceny na podstawie tytułu 3:

    a. Dostępność ICT oraz ryzyko dla ciągłości działania
    b. Ryzyko dla bezpieczeństwa ICT
    c. Ryzyko związane ze zmianą ICT
    d. Ryzyko związane z integralnością danych ICT
    e. Ryzyko związane z outsourcingiem ICT.

    Celem kwalifikacji jest wsparcie właściwych organów w ustalaniu, które ryzyko jest istotne (jeżeli w ogóle), a tym samym powinno być przedmiotem dokładniejszego lub pogłębionego przeglądu na kolejnych etapach oceny.

3.3 Ocena kontroli w celu ograniczenia istotnego ryzyka ICT

45. Aby ocenić rezydualne ryzyko ekspozycji ICT, właściwe organy powinny sprawdzić, jak instytucje identyfikują, monitorują, oceniają i ograniczają istotne ryzyko stwierdzone przez właściwe organy w ocenie, o której mowa powyżej.

46. W tym celu, w odniesieniu do stwierdzonego istotnego ryzyka ICT, właściwe organy powinny dokonać przeglądu mających zastosowanie:

    a. strategii politycznej zarządzania ryzykiem ICT, procesów i pułapów tolerancji ryzyka;
    b. ram zarządzania i nadzorowania organizacyjnego;
    c. zakresu audytu wewnętrznego i ustaleń oraz
    d. kontroli ryzyka ICT, które odnoszą się w szczególności do stwierdzonego istotnego ryzyka ICT.

47. Oceny powinny uwzględniać wynik analizy ogólnych ram zarządzania ryzykiem i kontroli wewnętrznego, o których mowa w tytule 5 wytycznych EUNB dotyczących SREP, a także zarządzania i strategii instytucji, o których mowa w tytule 2 niniejszych wytycznych, ponieważ istotne niedociągnięcia w tych obszarach mogą mieć wpływ na zdolność instytucji do zarządzania ekspozycją na ryzyko ICT i ograniczania go. W stosownym przypadku właściwe organy powinny również wykorzystać źródła informacji podane w ust. 37 niniejszych wytycznych.

48. Właściwe organy powinny przeprowadzić ocenę w następujących etapach, w sposób, który jest proporcjonalny do charakteru, skali i kompleksowości działań instytucji i przez stosowanie przeglądu nadzorczego, który jest odpowiedni dla profilu ryzyka ICT instytucji.

3.3.1 Strategia polityczna zarządzania ryzykiem ICT, procesy i pułapy tolerancji ryzyka

49. Właściwe organy powinny sprawdzić, czy instytucja opracowała odpowiednie strategie polityczne zarządzania ryzykiem, procesy i pułapy tolerancji w odniesieniu do stwierdzonych istotnych rodzajów

ryzyka ICT. Mogą być one częścią ram zarządzania ryzykiem operacyjnym lub zostać ujęte w oddzielnym dokumencie. W ramach tej oceny właściwe organy powinny uwzględnić, czy:

a. polityka zarządzania ryzykiem została sformalizowana i zatwierdzona przez organ zarządzający i zawiera wystarczające wytyczne dotyczące gotowości do podejmowania ryzyka ICT, głównych celów zarządzania ryzykiem ICT lub stosowanych pułapów tolerancji ryzyka ICT. Odpowiednia strategia polityczna zarządzania ryzykiem ICT powinna zostać również podana do wiadomości odpowiednich zainteresowanych stron;

b. mająca zastosowanie strategia polityczna obejmuje wszystkie kluczowe elementy zarządzania ryzykiem w odniesieniu do stwierdzonych istotnych rodzajów ryzyka;

c. instytucja wdrożyła proces i procedury bazowe dotyczące identyfikacji (np. „samodzielną ocenę kontroli ryzyka, analizę scenariusza ryzyka) i monitorowania odpowiednich rodzajów istotnego ryzyka oraz

d. instytucja wprowadziła mechanizm sprawozdawczości dotyczący zarządzania ryzykiem ICT, który w sposób terminowy zapewnia informacje kierownictwu wyższego szczebla i organowi zarządzającemu i który umożliwia kierownictwu wyższego szczebla lub organowi zarządzającemu ocenę i monitorowanie, czy plany i działania dotyczące ograniczenia ryzyka ICT instytucji są spójne z zatwierdzoną gotowością do podejmowania ryzyka lub zatwierdzonymi pułapami tolerancji (w stosownym przypadku) oraz monitorowanie zmian istotnych rodzajów ryzyka ICT.

3.3.2 Ramy zarządzania i nadzorowania organizacyjnego

50. Właściwe organy powinny ocenić, jak mające zastosowanie role i obowiązki z obszaru zarządzania ryzykiem zostały włączone w organizację wewnętrzną w celu zarządzania stwierdzonym istotnym ryzykiem ICT oraz jego nadzorowania. W związku z tym właściwe organy powinny ocenić, czy instytucja:

a. posiada jasne role i obowiązki w zakresie identyfikacji, oceny, monitorowania, ograniczania, zgłaszania i nadzorowania odpowiedniego istotnego ryzyka ICT;

b. udowodniła, że role i obowiązki w obszarze ryzyka, zostały jasno określone, przydzielone i włączone we wszystkie odpowiednie części (np. linie biznesowe, IT) i procesy organizacji, w tym role i obowiązki związane z gromadzeniem i agregowaniem informacji na temat ryzyka i zgłaszania ich kierownictwu wyższego szczebla lub organowi zarządzającemu;

c. wykazała, że działania z zakresu zarządzania ryzykiem bazują na dostatecznych i odpowiednich jakościowo zasobach ludzkich i technicznych. Aby ocenić wiarygodność mających zastosowanie planów ograniczania ryzyka, właściwe organy powinny również ocenić, czy instytucja przydzieliła dostateczne środki budżetowe lub inne niezbędne zasoby w celu ich wdrożenia;

d. wykazała odpowiednie działania następcze i reakcje organu zarządzającego w odniesieniu do ważnych ustaleń komórki niezależnej kontroli dotyczących ryzyka ICT, z uwzględnieniem ewentualnej delegacji niektórych aspektów komitetu, jeżeli takowe istnieją oraz

e. wykazała, że oczekiwania dotyczące mających zastosowanie regulacji i strategii politycznych ICT zostały odnotowane i podlegają udokumentowanemu przeglądowi i sprawozdawczości ze strony niezależnej komórki kontroli z naciskiem na powiązane ryzyka.

3.3.3 Zakres audytu wewnętrznego i ustalenia

51. Właściwe organy powinny rozważyć, czy komórka audytu wewnętrznego jest skuteczna, jeżeli chodzi o audyt mających zastosowanie ram kontroli ryzyka ICT, sprawdzając czy:

    a. ramy kontroli ryzyka ICT zostały poddane audytowi z wymaganą jakością, dogłębnością i częstotliwością oraz są dostosowane do wielkości, działań i profilu ryzyka ICT instytucji;

    b. plan audytu obejmuje audyt krytycznego ryzyka ICT określonego przez instytucję;

    c. ważne ustalenia z audytu ICT, w tym uzgodnione działania, zostały zgłoszone organowi zarządzającemu oraz

    d. ustalenia z audytu, w tym uzgodnione działania, były przedmiotem działań następczych i sprawozdań z postępów okresowo przeglądanych przez kierownictwo wyższego szczebla oraz komitet ds. audytu.

3.3.4 Kontrole ryzyka ICT, które odnoszą się w szczególności do stwierdzonego istotnego ryzyka ICT

52. W przypadku stwierdzonego istotnego ryzyka ICT właściwe organy powinny ocenić, czy instytucja wprowadziła specjalne kontrole w celu zajęcia się takim ryzykiem. Poniższe sekcje zawierają niewyczerpujący wykaz specjalnych kontroli, które należy rozważyć przy ocenie istotnych rodzajów ryzyka stwierdzonych na podstawie pkt 3.2.3, które są sklasyfikowane w następujących kategoriach ryzyka ICT:

    a. ryzyko związane z dostępnością i ciągłością ICT;
    b. ryzyko związane z bezpieczeństwem ICT;
    c. ryzyko związane ze zmianą ICT;
    d. ryzyko związane z integralnością danych ICT;
    e. ryzyko związane z outsourcingiem ICT.

(a) Kontrole w celu zarządzania istotnym ryzykiem związanym z dostępnością i ciągłością ICT

53. Oprócz wymogów określonych w wytycznych EUNB dotyczących SREP (ust. 279-281) właściwe organy powinny ocenić, czy instytucja wdrożyła odpowiednie ramy identyfikacji, rozumienia, pomiaru i ograniczania ryzyka związanego z dostępnością i ciągłością ryzyka.

54. Na potrzeby tej oceny właściwe organy powinny przede wszystkim uwzględnić, czy ramy:

    a. określają krytyczne procesy ICT i odpowiednie systemy wsparcia ICT, które powinny być częścią planów odporności biznesowej i ciągłości wraz:

        i. ze szczegółową analizą zależności między krytycznymi procesami biznesowymi i systemami wsparcia;

        ii. z określeniem celów związanych z odzyskiwaniem w celu wspierania systemów ICT (np. typowo określonych przez przedsiębiorstwo lub uregulowania w obszarze maksymalnego czasu wznowienia funkcji i akceptowalnego poziomu utraty danych);

iii. z odpowiednim planowaniem awaryjnym, aby umożliwić dostępność, ciągłość i odzyskiwanie krytycznych systemów i usług ICT w celu minimalizacji zakłóceń w operacjach instytucji w akceptowalnych granicach;

b. obejmują strategie i normy odporności biznesowej oraz kontroli ciągłości, a także kontrole operacyjne, które uwzględniają:

i. działania mające na celu uniknięcie sytuacji, w której pojedynczy scenariusz, incydent lub klęska mogą mieć wpływ zarówno na systemy produkcji, jak i odzyskiwania ICT;

ii. procedury tworzenia kopii zapasowych i odzyskiwania systemu ICT w odniesieniu do krytycznych programów i danych, które zapewniają przechowywanie kopii zapasowych w bezpiecznej i dostatecznie oddalonej lokalizacji, aby incydent lub klęska nie mogły zniszczyć lub naruszyć tych krytycznych danych;

iii. rozwiązania z zakresu monitorowania do terminowego wykrywania incydentów dotyczących dostępności lub ciągłości ICT;

iv. udokumentowany proces zarządzania incydentami i przekazywania spraw na wyższy poziom kompetencji, który obejmuje również wytyczne dotyczące różnych ról i obowiązków związanych z zarządzaniem incydentami i przekazywaniem spraw na wyższy poziom kompetencji, członków komitetu(-ów) kryzysowego(-ych) i łańcuch zamówień w sytuacji awaryjnej;

v. działania fizyczne mające na celu ochronę krytycznej infrastruktury ICT instytucji (np. centrów danych) od ryzyka związanego ze środowiskiem (np. ryzyka powodzi lub innych klęsk żywiołowych) oraz zapewnienie odpowiedniego środowiska operacyjnego dla systemów ICT (np. klimatyzacji);

vi. procesy, role i obowiązki, aby zapewnić, że również systemy i usługi ICT z outsourcingu są objęte odpowiednimi planami i rozwiązaniami z zakresu odporności biznesowej i ciągłości;

vii. rozwiązania z zakresu planowania i monitorowania wyników i możliwości krytycznych systemów i usług ICT z określonymi wymogami w obszarze dostępności w celu wykrywania ważnych ograniczeń związanych z wynikami i możliwościami w odpowiednim czasie;

viii. rozwiązania w celu ochrony krytycznych działań lub usług internetowych (np. usług bankowości elektronicznej), w razie potrzeby i w stosownym przypadku, przed zablokowaniem usługi lub innymi cyberatakami z internetu, których celem jest uniemożliwienie lub utrudnienie dostępu do tych działań i usług;

c. rozwiązania z zakresu testowania dostępności i ciągłości ICT w kontekście szeregu realistycznych scenariuszy obejmujących cyberataki, testy awarii i testy kopii zapasowych w odniesieniu do krytycznych programów i danych, które:

i. są zaplanowane, sformalizowane i udokumentowane, a wyniki testów wykorzystywane do poprawy skuteczności rozwiązań z zakresu dostępności i ciągłości ICT;

ii. obejmują zainteresowane strony i funkcje w organizacjach, takie jak zarządzanie linią biznesową włącznie z ciągłością działalności, zespoły reagowania na incydenty i kryzysu, a także odpowiednie zainteresowane podmioty zewnętrzne w ekosystemie;

iii. organ zarządzający i kierownictwo wyższego szczebla są odpowiednio zaangażowani (np. jako członkowie zespołów zarządzania kryzysowego) i otrzymują informacje o wynikach testów.

(b) Kontrole na potrzeby zarządzania istotnym ryzykiem związanym z bezpieczeństwem ICT

55. Właściwe organy powinny ocenić, czy instytucja stworzyła skuteczne ramy identyfikowania, zrozumienia, pomiaru i ograniczania ryzyka związanego z bezpieczeństwem ICT. W ocenie tej właściwe organy powinny przede wszystkim uwzględnić, czy ramy obejmują:

a. jasno określone role i obowiązki w odniesieniu do:
   i. osoby(osób) lub komitetów, które są odpowiedzialne za codzienne zarządzanie bezpieczeństwem ICT i za opracowywanie dalekosiężnych strategii bezpieczeństwa ICT oraz są z tego rozliczane, ze uwzględnieniem ich koniecznej niezależności;
   ii. projektu, wdrażania, monitorowania kontroli bezpieczeństwa ICT oraz zarządzania nimi;
   iii. ochrony krytycznych systemów i usług ICT przez przyjęcie przykładu procesu oceny podatności, zarządzania pakietem naprawczym programów, ochrony punktu końcowego (np. złośliwe oprogramowanie), narzędzi wykrywania wtargnięć i zapobiegania im;
   iv. monitorowania, klasyfikacji i obsługi zewnętrznych bądź wewnętrznych incydentów związanych z bezpieczeństwem ICT, włącznie z reagowaniem na incydenty oraz wznowieniem i odzyskiwaniem systemów i usług ICT;
   v. regularne i proaktywne oceny zagrożeń w celu utrzymania odpowiednich kontroli bezpieczeństwa;

b. strategię bezpieczeństwa ICT, która uwzględnia i, w stosownym przypadku, uruchamia międzynarodowo uznane normy bezpieczeństwa ICT oraz zasady bezpieczeństwa (np. zasadę najmniejszego uprzywilejowania, tj. ograniczenie dostępu do minimalnego poziomu, który umożliwia normalne funkcjonowanie na potrzeby zarządzania prawem dostępu, oraz zasadę ochrony w głąb, tj. warstwowych mechanizmów bezpieczeństwa, które zwiększają bezpieczeństwo całego systemu na potrzeby zaprojektowania architektury bezpieczeństwa);

c. proces identyfikacji systemów, usług i dostosowanych wymogów z obszaru bezpieczeństwa odzwierciedlających potencjalne ryzyko oszustw lub ewentualnych możliwych przypadków niewłaściwego stosowania lub nadużyć danych poufnych wraz z udokumentowanymi oczekiwaniami w zakresie bezpieczeństwa, które należy przyjąć w odniesieniu do tych zidentyfikowanych systemów, usług i danych ICT, dostosowanymi do tolerancji ryzyka instytucji i monitorowanymi w celu prawidłowego wdrożenia;

d. udokumentowany proces zarządzania incydentami w zakresie i przekazywania spraw na wyższy poziom kompetencji, który obejmuje wytyczne dotyczące różnych ról i obowiązków związanych z zarządzaniem incydentami i przekazywaniem spraw na wyższy poziom kompetencji, członków komitetu(-ów) kryzysowego(-ych) i łańcuch zamówień w sytuacjach awaryjnych dotyczących bezpieczeństwa;

e. rejestrowania użytkowników i działalności administracyjnej w celu umożliwienia skutecznego monitorowania oraz terminowego wykrywania nieupoważnionej działalności i reagowania na nią, wspomagania lub przeprowadzania dochodzeń karnych w związku z incydentami dotyczącymi bezpieczeństwa. Instytucja powinna wprowadzić strategie rejestrowania określające odpowiednie typy logów, które należy utrzymać oraz ich okres zatrzymania;

f. kampanie uświadamiające i informacyjne lub inicjatywy służące informowaniu wszystkich szczebli w instytucji o bezpiecznym korzystaniu i ochronie systemów ICT instytucji oraz głównych rodzajów ryzyka związanych z bezpieczeństwem ICT, które powinni znać, zwłaszcza jeżeli chodzi o istniejące i zmieniające się zagrożenia cybernetyczne (np. wirusy komputerowe, możliwe nadużycia wewnętrzne lub zewnętrzne, ataki, cyberataki) oraz ich rola w ograniczaniu przypadków łamania zasad bezpieczeństwa;

g. odpowiednie fizyczne środki bezpieczeństwa (np. telewizja przemysłowa, alarmy przeciwwłamaniowe, drzwi ochronne) w celu zapobiegania przypadkom nieupoważnionego dostępu do krytycznych i wrażliwych systemów ICT;

h. działania mające na celu ochronę systemów ICT przed atakami z internetu (tj. cyberatakami) lub innymi zewnętrznymi sieciami (np. tradycyjne połączenia telekomunikacyjne lub połączenia z zaufanymi partnerami). Właściwe organy powinny sprawdzić, czy ramy instytucji uwzględniają:

   i. proces i rozwiązania mające na celu utrzymanie kompletnego i aktualnego inwentarza i przeglądu wszystkich zewnętrznych punktów połączenia z siecią (np. witryn internetowych, aplikacji internetowych, WIFI, dostępu zdalnego), za pomocą których strony trzecie mogłyby włamać się do wewnętrznych systemów ICT.

   ii. ściśle zarządzane i monitorowane środki bezpieczeństwa (np. zapory sieciowe, serwery proxy, przekaźniki poczty, antywirusy i skanery treści) w celu zabezpieczenia przepływu przychodzącego i wychodzącego w sieci (np. e-maili) oraz połączeń sieciowych zewnętrznych, za pomocą których osoby trzecie mogą włamać się do wewnętrznych systemów ICT;

   iii. procesy i rozwiązania mające na celu zabezpieczenie witryn i aplikacji, które mogą być przedmiotem bezpośrednich ataków z internetu/z zewnątrz u służyć jako punkty wejścia do systemów wewnętrznych ICT. W ujęciu ogólnym obejmuje to połączenie uznanych praktyk bezpiecznego rozwoju, praktyk usprawnienia systemu ICT i monitorowania podatności, a także wdrożenie dodatkowych rozwiązań w dziedzinie bezpieczeństwa, takich jak na przykład stosowanie zapór systemowych lub systemów wykrywania włamania lub zapobiegania włamaniu (IPS);

   iv. okresowe testy zabezpieczenia przed przenikaniem w celu oceny skuteczności wdrożonych środków i procesów z zakresu cybernetycznego i wewnętrznego bezpieczeństwa ICT. Testy te powinni przeprowadzać pracownicy i eksperci zewnętrzni z niezbędnym doświadczeniem, wraz z udokumentowanymi wynikami testów oraz wnioskami przekazanymi kierownictwu wyższego szczebla lub organowi zarządzającemu. W razie potrzeby i w stosownym przypadku instytucja powinna wywnioskować z wspomnianych testów, gdzie należy poprawić kontrole i procesy bezpieczeństwa oraz uzyskać lepszą gwarancję ich skuteczności.

(c) Kontrole na potrzeby zarządzania istotnym ryzykiem związanym ze zmianą ICT

56. Właściwe organy powinny ocenić, czy instytucja wdrożyła skuteczne ramy identyfikowania, rozumienia, pomiaru i ograniczania ryzyka związanego ze zmianą ICT dostosowane do charakteru, skali i złożoności działań instytucji oraz profilu ryzyka ICT instytucji. Ramy instytucji powinny obejmować ryzyko powiązane z opracowaniem, testowaniem i zatwierdzaniem zmian systemów ICT, w tym opracowaniem lub zmianą oprogramowania, przed jego przeniesieniem do środowiska produkcji, oraz zagwarantować adekwatne zarządzanie cyklem życia ICT. W ocenie tej właściwe organy powinny przede wszystkim uwzględnić, czy ramy obejmują:

a. udokumentowane procesy zarządzania zmianami systemów ICT (np. zarządzanie konfiguracją i pakietem naprawczym) i danych (np. usuwanie wirusów lub korygowanie danych) oraz ich kontroli przez zapewnienie odpowiedniego zaangażowania osób odpowiedzialnych za zarządzanie ryzykiem ICT w istotne zmiany ICT, które mogą mieć znaczny wpływ na profil ryzyka lub ekspozycję instytucji;

b. specyfikacje dotyczące wymaganego podziału obowiązku podczas różnych etapów wdrażania procesów zmiany ICT (np. projektowanie i opracowywanie rozwiązania, testowanie i zatwierdzanie nowego oprogramowania oraz zmian, migracja i wdrażanie w środowisku produkcyjnym oraz usuwanie wirusów) z naciskiem na wdrożone rozwiązania i podział obowiązków w celu zarządzania zmianami produkcji systemów i danych ICT oraz ich kontroli przez pracowników ICT (np. programistów, administratorów systemów ICT, administratorów bazy danych) lub każdej innej strony (np. użytkowników biznesowych, usługodawców);

c. środowiska testowe, które odpowiednio odzwierciedlają środowiska produkcji;

d. inwentarz aktywów istniejących aplikacji i systemów ICT w środowisku produkcyjnym, a także środowisko testów i rozwoju, tak aby wymagane zmiany (np. aktualizacje lub modernizacje, zestawy naprawcze systemów, zmiany konfiguracyjne) mogły być przedmiotem odpowiedniego zarządzania, wdrażanego i monitorowanego w odniesieniu do właściwych systemów ICT;

e. proces monitorowania cyklu życia używanych systemów ICT oraz zarządzania nimi, aby zagwarantować, że nadaj spełniają i wspierają aktualne wymogi w obszarze przedsiębiorstw i zarządzania ryzykiem oraz dopilnować, że używane rozwiązania i systemy ICT wciąż są wspierane przez klientów oraz że wciąż towarzyszą im odpowiednie procedury cyklu życia opracowanych programów;

f. system kontroli i odpowiednie procedury w celu zapobiegania nieupoważnionym zmianom w kodzie źródłowym oprogramowania, które zostało opracowane wewnętrznie;

g. proces przeprowadzania weryfikacji bezpieczeństwa i podatności nowych lub znacznie zmodyfikowanych systemów i programów ICT przed dopuszczeniem ich do produkcji i narażeniem na ewentualne cyberataki;

h. proces i rozwiązania w celu zapobiegania nieupoważnionemu i niezamierzonemu ujawnieniu danych poufnych, przy przemieszczaniu, archiwizowaniu, wyrzucaniu ub niszczeniu systemów ICT;

i. niezależne procesy przeglądu i zatwierdzania w celu ograniczenia ryzyka błędów ludzkich podczas wprowadzania zmian do systemów ICT, z których wiele ma niekorzystny wpływ na dostępność, ciągłość lub bezpieczeństwo instytucji (np. istotne zmiany w konfiguracji zapory) lub bezpieczeństwo instytucji (np. zmiany zapory).

(d) Kontrole na potrzeby zarządzania istotnym ryzykiem związanym integralnością danych ICT

57. Właściwe organy powinny ocenić, czy instytucja wdrożyła skuteczne ramy identyfikowania, rozumienia, pomiaru i ograniczania ryzyka związanego z integralnością danych ICT dostosowane do charakteru, skali i złożoności działań instytucji oraz profilu ryzyka ICT instytucji. Ramy instytucji powinny obejmować ryzyko związane z ochroną integralności danych przechowywanych i przetworzonych przez systemy ICT. W ocenie tej właściwe organy powinny przede wszystkim uwzględnić, czy ramy obejmują:

a. strategię, która określa role i obowiązki związane z zarządzaniem integralnością danych w systemach ICT (np. architekta danych, inspektorów ds. danych[6], osób odpowiedzialnych za ochronę danych[7], właścicieli/rządców danych[8]) i pozwala określić, które dane są krytyczne z perspektywy integralności danych i powinny podlegać specjalnym kontrolom ICT (np. automatycznym kontrolom zatwierdzania danych wejściowych, kontrolom przekazywania danych, uzgodnieniom itp.) lub przeglądom (np. kontroli kompatybilności z architekturą danych) na różnych etapach cyklu życia danych ICT);

b. udokumentowaną architekturę danych, model danych lub słownik danych, które zostały zatwierdzone z udziałem odpowiednich zainteresowanych stron z obszaru działalności biznesowej i IT w celu wspierania niezbędnej spójności danych w systemach ICT oraz zyskania pewności, że architektura danych, model danych lub słownik danych pozostają dostosowane do potrzeb przedsiębiorstwa i zarządzania ryzykiem;

c. strategię dotyczącą dopuszczalnego zastosowania i bazowania na systemach obliczeniowych użytkowników końcowych, zwłaszcza jeżeli chodzi o identyfikację, rejestrację i dokumentację ważnych rozwiązań obliczeniowych dla użytkowników końcowych (tj. podczas przetwarzania ważnych danych) oraz oczekiwanych poziomów bezpieczeństwa w celu zapobiegania nieupoważnionym modyfikacjom, zarówno samego narzędzia, jak i danych w nim przechowywanych;

d. udokumentowane procesy postępowania z wyjątkami w celu rozwiązania stwierdzonych problemów z integralnością danych ICT zgodnie z ich krytycznością i wrażliwością.

58. W przypadku instytucji nadzorowanych, które podlegają zasadom efektywnej agregacji danych o ryzyku i sprawozdawczości w zakresie ryzyka Bazylejskiego Komitetu Nadzoru Bankowego 239[9], właściwe organy powinny dokonać przeglądu analizy ryzyka instytucji pod kątem sprawozdawczości w zakresie ryzyka i

[6] Inspektor ds. danych jest odpowiedzialny za przetwarzanie i wykorzystywanie danych.

[7] Osoba odpowiedzialna za ochronę danych odpowiada za bezpieczny nadzór nad danymi, ich transport i przechowywanie.

[8] Rządca danych jest odpowiedzialny za zarządzanie i dopasowanie elementów danych – zarówno treści, jak i metadanych.

[9] Bazylejski Komitet Nadzoru Bankowego, Zasady efektywnej agregacji danych o ryzyku i sprawozdawczości w zakresie ryzyka (Principles for effective risk data aggregation and risk reporting), styczeń 2013 r., zasady dostępne online: http://www.bis.org/publ/bcbs239.pdf.

zdolności do agregacji danych w świetle zasad i przygotowanych dokumentów, z uwzględnieniem wdrażania chronologicznych i przejściowych ustaleń dotyczących tych zasad.

(e) Kontrole na potrzeby zarządzania istotnym ryzykiem związanym z outsourcingiem ICT

59. Właściwe organy powinny ocenić, czy strategia outsourcingu instytucji, zgodnie z wymogami zawartymi w wytycznych dotyczących outsourcingu Komitetu Europejskich Obszarów Nadzoru Bankowego (2006) oraz w następstwie wymogu określonego w ust. 85 lit. d) wytycznych EUNB dotyczących SREP, odnosi się odpowiednio do outsourcingu ICT, w tym do outsourcingu wewnątrzgrupowego zapewniającego usługi ICT w ramach grupy. Przy ocenie ryzyka związanego z outsourcingiem ICT właściwe organy powinny uwzględnić, czy ryzyko związane z outsourcingiem ICT może być również objęte oceną nieodłącznego ryzyka operacyjnego na podstawie ust. 240 lit. j) wytycznych EUNB dotyczących SREP w celu uniknięcia powielania pracy lub obliczeń.

60. Właściwe organy powinny w szczególności ocenić, czy instytucja posiada skuteczne ramy identyfikacji, zrozumienia i pomiaru ryzyka związanego z outsourcingiem ICT, a w szczególności czy zapewnia kontrole i środowisko kontroli w celu ograniczania ryzyka związanego z istotnymi usługami ICT objętymi outsourcingiem, które są dostosowane do wielkości, działań i profilu ryzyka ICT instytucji i obejmują:

a. ocenę wpływu outsourcingu ICT na zarządzanie ryzykiem instytucji w powiązaniu z korzystaniem z usługodawców (np. dostawców usług w chmurze) oraz ich usług w procesie przetargu, udokumentowaną i uwzględnianą przez kierownictwo wyższego szczebla lub organ zarządczy podczas podejmowania decyzji o outsourcingu usług. Instytucja powinna dokonać przeglądu strategii zarządzania ryzykiem ICT oraz kontroli i środowiska kontroli dostawców, aby dopilnować, że są zgodne z wewnętrznymi celami instytucji w zakresie zarządzania ryzykiem oraz gotowości do podejmowania ryzyka. Przegląd powinien być okresowo aktualizowany w czasie trwania umowy o outsourcing, z uwzględnieniem cech usług podlegających outsourcingowi;

b. monitorowanie ryzyka ICT usług objętych outsourcingiem w czasie trwania umowy o outsourcingu w ramach zarządzania ryzykiem instytucji, które jest uwzględniane w sprawozdaniach dotyczących zarządzania ryzykiem ICT w instytucji (np. sprawozdawczość dotycząca ciągłości biznesowej, sprawozdawczość dotycząca bezpieczeństwa);

c. monitorowanie i porównanie świadczonego poziomu usług z umownie uzgodnionym poziomem usług, który powinien stanowić część umowy o outsourcing usług lub umowy o gwarantowanym poziomie usług (SLA) oraz

d. adekwatny personel oraz adekwatne zasoby i kompetencje do monitorowania ryzyka ICT i zarządzania tym ryzykiem ze strony usług objętych outsourcingiem.

3.4 Podsumowanie ustaleń i punktacja

61. W wyniku powyższej oceny właściwe organy powinny uzyskać pogląd na temat ryzyka ICT instytucji. Opinia ta powinna znaleźć odzwierciedlenie w podsumowaniu ustaleń, które właściwe organy powinny

uwzględnić przy przyznawaniu punktów za ryzyko operacyjne w tabeli 6 wytycznych EUNB dotyczących SREP. Właściwe organy powinny opierać swoją opinię na istotnych rodzajach ryzyka ICT z uwzględnieniem następujących uwag, które będą podstawą oceny ryzyka operacyjnego:

a. Uwagi dotyczące ryzyka

i. profil i ekspozycja instytucji na ryzyko ICT;
ii. stwierdzone krytyczne systemy i usługi ICT oraz
iii. istotny charakter ryzyka ICT pod kątem krytycznych systemów ICT.

b. Uwagi dotyczące zarządzania i kontroli

i. polityka i strategia w zakresie zarządzania ryzykiem ICT instytucji i jej ogólna strategia oraz gotowość do podejmowania ryzyka są ze sobą spójne;
ii. ramy organizacyjne w zakresie zarządzania ryzykiem ICT są solidne i przewidują wyraźny podział obowiązków i zadań między podejmujących ryzyko a komórki ds. zarządzania ryzykiem i kontroli ryzyka;
iii. systemy pomiaru i monitorowania ryzyka ICT oraz sprawozdawczości w jego zakresie są odpowiednie oraz
iv. ramy kontroli istotnych rodzajów ryzyka ICT są solidne.

62. Jeżeli właściwe organy uznają ryzyko ICT za istotne, a właściwy organ podejmie decyzję o ocenie i punktacji tego ryzyka jako podkategorii ryzyka operacyjnego, poniższa tabela (tabela 1) zawiera dane na temat punktacji ryzyka ICT.

Tabela 1: Względy nadzorcze istotne przy określaniu punktacji ryzyka ICT

Punktacja ryzyka	Pogląd nadzorczy	Czynniki związane z ryzykiem nieodłącznym	Czynniki związane z odpowiedniością zarządzania i mechanizmów kontroli
1	Brak dostrzegalnego ryzyka wystąpienia istotnych skutków ostrożnościowych dla instytucji, uwzględniając poziom ryzyka nieodłącznego oraz zarządzania i kontroli.	• Źródła informacji, które należy uwzględnić na podstawie ust. 37, nie wskazują na znaczną ekspozycję na ryzyko ICT. • Charakter profilu ryzyka ICT instytucji, w połączeniu z przeglądem krytycznych systemów ICT oraz istotnych rodzajów ryzyka dla systemów i usług ICT, nie ujawniają istotnego ryzyka ICT.	
2	Istnieje niskie ryzyko wystąpienia istotnych skutków ostrożnościowych dla instytucji,	• Źródła informacji, które należy uwzględnić na podstawie ust. 37, nie wskazują na ekspozycję na istotne ryzyko ICT. • Charakter profilu ryzyka ICT	• Polityka i strategia w zakresie ryzyka ITC instytucji i jej ogólna

	uwzględniając poziom ryzyka nieodłącznego oraz zarządzania i kontroli.	instytucji w połączeniu z przeglądem krytycznych systemów ICT i istotnych rodzajów ryzyka ICT w odniesieniu do systemów i usług ICT wykazał ograniczoną ekspozycję na ryzyko ICT (np. nie większe niż 2 na 5 według wstępnie zdefiniowanych kategorii ryzyka ICT).	strategia oraz gotowość do podejmowania ryzyka są ze sobą spójne. • Ramy instytucjonalne w zakresie ryzyka ITC są solidne i przewidują wyraźny podział obowiązków i zadań między podejmujących ryzyko a komórki ds. zarządzania ryzykiem i kontroli ryzyka. • Systemy pomiaru i monitorowania ryzyka finansowania oraz sprawozdawczości w jego zakresie są odpowiednie. • Ramy kontroli ryzyka operacyjnego są prawidłowe.
3	Istnieje średnie ryzyko wystąpienia istotnych skutków ostrożnościowych dla instytucji, uwzględniając poziom ryzyka nieodłącznego oraz zarządzania i kontroli.	• Źródła informacji, które należy uwzględnić na podstawie ust. 37, wskazują na możliwą ekspozycję na istotne ryzyko ICT. • Charakter profilu ryzyka ICT instytucji w połączeniu z przeglądem krytycznych systemów ICT i istotnych rodzajów ryzyka ICT w odniesieniu do systemów i usług ICT wykazał podwyższoną ekspozycję na ryzyko ICT (np. 3 lub więcej na 5 według wstępnie zdefiniowanych kategorii ryzyka ICT).	
4	Istnieje wysokie ryzyko wystąpienia istotnych skutków ostrożnościowych dla instytucji, uwzględniając poziom ryzyka nieodłącznego oraz zarządzania i kontroli.	• Źródła informacji, które należy uwzględnić na podstawie ust. 37, zawierają wiele przesłanek ekspozycji na istotne ryzyko ICT. • Charakter profilu ryzyka ICT instytucji w połączeniu z przeglądem krytycznych systemów ICT i istotnych rodzajów ryzyka ICT w odniesieniu do systemów i usług ICT wykazał wysoką ekspozycję na ryzyko ICT (np. 4 lub 5 na 5 według wstępnie zdefiniowanych kategorii ryzyka ICT).	

Załącznik – Taksonomia ryzyka ICT

Pięć kategorii ryzyka ICT z niewyczerpującym wykazem ryzyk ICT o potencjalnie poważnym znaczeniu oraz wpływie na działalność operacyjną, renomę lub wyniki finansowe

Kategorie ryzyka ICT	Ryzyka ICT (wykaz niewyczerpujący [10])	Opis ryzyka	Przykłady
Ryzyko związane z dostępnością i ciągłością ICT	Nieodpowiednie zdolności w zakresie zarządzania	Brak zasobów (np. sprzętu, oprogramowania, pracowników, usługodawców) może prowadzić do braku zdolności do takiego skalowania usługi, aby odpowiadała potrzebom biznesowym, przerw w działaniu systemu, pogorszenia usługi lub błędów operacyjnych.	• Niedobór zdolności może mieć wpływ na wskaźniki przesyłu i dostępność sieci (internet) w przypadku usług, takich jak bankowość internetowa. • Brak pracowników (wewnętrznych lub zewnętrznych) może prowadzić do przerw w działaniu systemu lub błędów operacyjnych.
	Awarie systemu ICT	Brak dostępności ze względu na awarie sprzętu.	• Brak przechowywania/nieodpowiednie przechowywanie (twarde dyski), awaria/nieprawidłowe działanie serwera lub innych urządzeń ICT spowodowane np. brakiem konserwacji.
		Brak dostępności ze względu na awarie sprzętu i wirusy.	• Pętla nieskończona w oprogramowaniu uniemożliwia wykonanie transakcji. • Przestoje w wyniku ciągłego wykorzystywania przestarzałych systemów i rozwiązań ICT, które nie spełniają aktualnych wymogów w zakresie dostępności lub odporności albo nie są już obsługiwane przez dystrybutorów.
	Nieadekwatne planowanie ciągłości ICT i	Brak planowanych rozwiązań z zakresu dostępności lub ciągłości, abo też naprawy w następstwie klęski (np. przywrócenie centrum danych) po uruchomieniu	• Różnice w konfiguracji między pierwotnym a wtórnym centrum danych może prowadzić do braku zdolności do przywrócenia centrum danych w celu

[10] Ryzyka ICT są wymienione w kategorii ryzyka, na którą mają największy wpływ, jednak mogą one również mieć wpływ na inne kategorie ryzyka

Kategorie ryzyka ICT	Ryzyka ICT (wykaz niewyczerpujący [10])	Opis ryzyka	Przykłady
	naprawy w następstwie klęski	reagowania na incydent.	zapewnienia planowanej ciągłości usługi.
	Cyberataki o charakterze zakłócającym i destrukcyjnym	Ataki przeprowadzane w różnym celu (np. aktywizm, szantaż), które prowadzą do przeciążenia systemu i sieci, uniemożliwiając dostęp do usług internetowych uprawnionym użytkownikom.	• Rozproszone ataki typu „odmowa usługi" są przeprowadzane za pomocą wielu systemów komputerowych w internecie pod kontrolą hakera, który wysyła znaczną ilość pozornie uprawnionych wniosków o usługę internetową (np. w bankowości elektronicznej).
Ryzyko związane z bezpieczeństwem ICT	Cyberataki lub inne zewnętrzne ataki ICT	Ataki przeprowadzane z internetu lub poza siecią w różnych celach (np. oszustwa, szpiegostwa, aktywizmu/sabotażu, terroryzmu cybernetycznego) z zastosowaniem różnych technik (np. inżynierii społecznej, prób wtargnięcia z wykorzystaniem słabych punktów, rozpowszechnianiem złośliwego oprogramowania) prowadzących do przejęcia kontroli nad wewnętrznymi systemami ICT.	Różne rodzaje ataków: • Zaawansowane, trwałe zagrożenie przejęciem kontroli nad systemami wewnętrznymi lub kradzież informacji (np. kradzież tożsamości, informacji dotyczących karty kredytowej). • Złośliwe oprogramowanie (np. typu ransomware), które szyfruje dane w celu szantażowania. • Zarażenie wewnętrznych systemów ICT wirusami typu koń trojański w celu przeprowadzenia złośliwych działań w systemie w ukryty sposób. • Wykorzystanie słabych punktów systemu ICT lub aplikacji (internetowej) (np. wstrzyknięcie SQL itp.) w celu uzyskania dostępu do wewnętrznego systemu ICT.
		Przeprowadzanie oszukańczych transakcji płatniczych przez hakerów w następstwie złamania lub obejścia zabezpieczeń bankowości elektronicznej lub usług płatniczych lub zaatakowania i wykorzystania słabych punktów zabezpieczeń w wewnętrznych systemach płatniczych instytucji.	• Ataki na bankowość elektroniczną lub usługi płatnicze w celu dokonania nieuprawnionych transakcji. • Utworzenie i przesyłanie oszukańczych transakcji płatniczych w wewnętrznych systemach płatniczych instytucji (np. fałszywych wiadomości SWIFT).

Kategorie ryzyka ICT	Ryzyka ICT (wykaz niewyczerpujący [10])	Opis ryzyka	Przykłady
		Przeprowadzenie fałszywych transakcji na papierach wartościowych przez hakerów w następstwie złamania lub obejścia zabezpieczenia usług bankowości elektronicznej, które zapewnia również dostęp do rachunków inwestycyjnych klienta.	• Ataki typu „pump and dump", gdzie atakujący zyskują dostęp do rachunków inwestycyjnych klientów w bankowości elektronicznej i wystawiają fałszywe zlecenia kupna lub sprzedaży w celu wpłynięcia na cenę rynkową lub zyski rynkowe na podstawie wcześniej ustanowionych pozycji papierów wartościowych.
		Ataki na połączenia komunikacyjne i konwersacje wszelkiego typu lub systemy ICT w celu zgromadzenia informacji lub popełnienia oszustwa.	• Podsłuchiwanie/przechwycenie niechronionych transmisji uwierzytelnionych danych w formie zwykłego tekstu.
	Nieodpowiednie zabezpieczenie wewnętrzne ICT	Uzyskanie nieupoważnionego dostępu do krytycznych systemów ICT w instytucji do różnych celów (np. w celu popełnienia oszustwa, przeprowadzenia i ukrycia nieuczciwych działań handlowych, kradzieży danych, aktywizmu/sabotażu) za pomocą różnych technik (np. nadużycia lub przenoszenia przywilejów, kradzieży tożsamości, inżynierii społecznej, wykorzystania słabych punktów w systemach ICT, wprowadzenia złośliwego oprogramowania).	• Instalacja programów rejestrujących naciśnięcie klawiszy w celu kradzieży tożsamości i haseł użytkowników i zdobycia nieuprawnionego dostępu do poufnych danych lub popełnienia przestępstwa. • Złamanie/odgadnięcie słabych haseł w celu zyskania nielegalnych lub większych praw dostępu. • Administrator systemu wykorzystuje systemy operacyjne lub funkcje bazy danych (do bezpośredniej modyfikacji bazy danych) do popełnienia przestępstwa.
		Nieuprawnione manipulacje ICT w wyniku nieodpowiednich procedur i praktyk zarządzania dostępem ICT.	• Brak dezaktywowania lub usunięcia niepotrzebnych kont, np. kont pracowników, którzy zmienili stanowisko lub odeszli z instytucji, w tym kont dla gości lub dostawców, którzy nie potrzebują już dostępu, zapewniających nieuprawniony dostęp do systemów ICT. • Przyznanie nadmiernych praw i przywilejów w zakresie dostępu umożliwiających nieuprawniony

Kategorie ryzyka ICT	Ryzyka ICT (wykaz niewyczerpujący [10])	Opis ryzyka	Przykłady
			dostęp lub ukrycie nieuczciwych działań.
		Zagrożenia dla bezpieczeństwa wynikające z braku świadomości o zagrożenia, jeżeli pracownicy nie rozumieją, ignorują lub nie stosują strategii i procedur bezpieczeństwa ICT.	• Pracownicy, którzy brali udział w ataku (tj. inżynieria społeczna). • Złe praktyki dotyczące danych uwierzytelniających, udostępnianie haseł, używanie haseł łatwych do odgadnięcia, używanie tego samego hasła do różnych celów itp. • Przechowywanie nieszyfrowanych danych poufnych w laptopach lub przenośnych urządzeniach do przechowywania danych (np. kluczach USB), które mogą zostać utracone lub skradzione.
		Nieuprawnione przechowywanie lub przesyłanie danych poufnych poza instytucję.	• Osoby dokonujące kradzieży lub świadomego przecieku lub przemytu informacji poufnych na rzecz nieupoważnionych osób lub do wiadomości publicznej.
	Nieodpowiednie fizyczne zabezpieczenie ICT	Nieodpowiednie stosowanie lub kradzież aktywów ICT w drodze fizycznego dostępu powodującego szkody, utratę aktywów lub danych lub związane z innymi ewentualnymi zagrożeniami.	• Fizyczne włamanie budynków biurowych lub centrów danych w celu kradzieży sprzętu ICT (np. komputerów, laptopów, rozwiązań do przechowywania) lub kopiowanie danych w drodze fizycznego dostępu do systemów ICT.
		Świadome lub przypadkowe uszkodzenie fizycznych aktywów ICT w wyniku aktu terroryzmu, wypadków lub niefortunnych/błędnych czynności ze strony pracowników instytucji lub osób trzecich (dostawców, serwisantów).	• Fizyczne akty terroryzmu (np. bomby) lub sabotażu aktywów ICT. • Zniszczenie centrum danych spowodowane przez pożar, zalanie lub inne czynniki.
		Niedostateczna ochrona fizyczna przed klęskami żywiołowymi prowadząca do częściowego lub całkowitego zniszczenia systemów/centrów danych ICT w wyniku klęsk żywiołowych.	• Trzęsienia ziemi, ekstremalne upały, wichury, śnieżyce, powodzie, pożary, pioruny.
Ryzyko	Nieodpowiednie	Incydenty spowodowane niewykrytymi błędami lub	• Przekazanie do produkcji niedostatecznie

Kategorie ryzyka ICT	Ryzyka ICT (wykaz niewyczerpujący [10])	Opis ryzyka	Przykłady
związane ze zmianą ICT	kontrole zmian systemów ICT i rozwoju ICT	słabymi punktami w wyniku zmiany (np. nieprzewidziane skutki zmiany lub niedostateczne zarządzanie zmianą w wyniku braku testów lub nieprawidłowych praktyk z zakresu zarządzania zmianą) np. oprogramowania, systemów i danych ICT.	przetestowanego oprogramowania lub zmiany w konfiguracji o nieoczekiwanie przeciwnych skutkach dla danych (np. uszkodzenie, usunięcie) lub wyników systemu ICT (awaria, spadek wydajności). • Niekontrolowane zmiany systemów ICT lub danych w środowisku produkcyjnym. • Przekazanie do produkcji źle zabezpieczonych systemów ICT i aplikacji internetowych stwarzających szanse dla ataku hakerów na świadczone usługi internetowe lub złamanie wewnętrznych systemów ICT. • Niekontrolowane zmiany w kodzie źródłowym wewnętrznie opracowanego oprogramowania. • Niedostateczne przetestowanie w wyniku braku adekwatnego środowiska testowego.
	Nieodpowiednia architektura ICT	Słabe zarządzanie architekturą ICT na etapie projektowania, tworzenia i konserwacji systemów ICT (np. oprogramowanie, sprzęt, dane) może z czasem prowadzić do złożonych, trudnych i kosztownych pod względem zarządzania i sztywnych systemów ICT, które nie są odpowiednio dostosowane do potrzeb biznesowych i nie spełniają rzeczywistych wymogów w zakresie zarządzania ryzykiem.	• Nieodpowiednio zarządzane zmiany w systemach ICT, oprogramowaniu lub danych w dłuższym okresie, prowadzące do złożonych, niejednorodnych i trudnych do zarządzania systemów i struktur ICT, wywołujących wiele negatywnych skutków biznesowych i ryzyko dla zarządzania (np. brak elastyczności i sprawności, incydenty i awarie ICT, wysokie koszty operacyjne, osłabione bezpieczeństwo ICT oraz słabsza odporność, ograniczona jakość danych i słabsze zdolności w zakresie sprawozdawczości). • Nadmierne dostosowanie do indywidualnych potrzeb i nadmierna rozbudowa komercyjnych pakietów oprogramowania z programami opracowanymi wewnętrznie, prowadzące do

Kategorie ryzyka ICT	Ryzyka ICT (wykaz niewyczerpujący [10])	Opis ryzyka	Przykłady
			niezdolności do wprowadzenia dalszych aktualizacji i modernizacji oprogramowania komercyjnego oraz ryzyka braku obsługi przez dystrybutora.
	Nieodpowiedni cykl życia i nieodpowiednie zarządzanie pakietami naprawczymi	Brak konserwacji i odpowiedniej inwentaryzacji wszystkich aktywów ICT wspierających i powiązanych z odpowiednimi praktykami zarządczymi w obszarze cyklu życia i pakietów naprawczych. Prowadzi to do niedostatecznego poziomu naprawy (a zatem większej słabości) przestarzałych systemów ICT, które mogą być niedostosowane do potrzeb biznesowych i potrzeb związanych z zarządzaniem ryzykiem.	• Przestarzałe i nienaprawiane systemy ICT mogą wywoływać niekorzystne skutki biznesowe i skutki w obszarze zarządzania ryzykiem (np. brak elastyczności i sprawności, przestoje ICT, gorsze bezpieczeństwo ICT i gorsza odporność).
Ryzyko związane z integralnością danych ICT	Nieprawidłowe przetwarzanie danych ICT lub posługiwanie się tymi danymi	Ze względu na błędy lub awarie systemu, komunikacji lub stosowania, albo też błędnie przeprowadzone procesy ekstrakcji, transferu i wprowadzenia dane mogą ulec zniszczeniu lub utracie.	• Błąd systemu informatycznego podczas przetwarzania pakietu naprawczego prowadzący do nieprawidłowego salda na rachunkach bankowych klientów. • Nieprawidłowo wykonane zlecenia. • Utrata danych w wyniku błędu powielania danych (tworzenia kopii zapasowej).
	Nieprawidłowo zaprojektowane kontrole zatwierdzania danych w systemach ICT	Błędy dotyczące braku lub nieskutecznych kontroli automatycznego wprowadzania i akceptacji danych (np. w przypadku używanych danych osób trzecich), transferów danych, kontroli przetwarzania i wyprowadzania danych w systemach ICT (np. kontrole zatwierdzania wprowadzania, uzgodnienia danych).	• Niedostateczne lub nieważne formatowanie/zatwierdzanie danych wprowadzanych do aplikacji lub interfejsów użytkowników. • Brak kontroli uzgadniania danych w odniesieniu do osiągniętych wyników • Brak kontroli przeprowadzonych procesów ekstrakcji danych (np. wyszukiwań w bazie danych) prowadzących do błędnych danych. • Używanie fałszywych danych zewnętrznych.
	Nieprawidłowa kontrola zmian	Błędne dane wprowadzone w wyniku braku kontroli poprawności i uzasadnionego charakteru czynności	• Programiści lub administratorzy baz danych mający bezpośredni dostęp do danych i zmieniający dane w

Kategorie ryzyka ICT	Ryzyka ICT (wykaz niewyczerpujący [10])	Opis ryzyka	Przykłady
	danych w systemach produkcji ICT.	przeprowadzanych na danych w ramach produkcji systemów ICT	systemach produkcji ICT w niekontrolowany sposób, np. w przypadku incydentu ICT.
	Źle zaprojektowane lub zarządzane przepływy danych, modele danych, słowniki danych lub architektura danych	Źle zarządzane architektury danych, modele danych, przepływy danych lub słowniki danych mogą prowadzić do wielu wersji tych samych danych w systemach ICT, które nie są już spójne w wyniku odmiennie stosowanych modelów danych lub definicji danych oraz różnic w generowaniu i procesie zmiany danych podstawowych.	• Występowanie różnych baz danych klientów w podziale na produkt lub jednostkę biznesową z różnymi definicjami i polami danych, prowadzące do nieuzgodnionych i trudnych do porównania i integracji danych klientów na poziomie całej instytucji finansowej lub grupy.
Ryzyko związane z outsourcingiem ICT	Nieodpowiednia odporność usług osoby trzeciej lub innej jednostki grupy	Brak dostępności krytycznych usług ICT, usług telekomunikacyjnych i mediów podlegających outsourcingowi. Utrata lub zniszczenie danych krytycznych/wrażliwych powierzonych usługodawcy	• Niedostępność kluczowych usług w wyniku awarii systemów lub aplikacji ICT (objętych outsourcingiem). • Zerwanie łączy telekomunikacyjnych. • Przerwy w dostawie prądu.
	Nieodpowiednie zarządzanie outsourcingiem	Poważne pogorszenie usługi lub brak usługi w następstwie niedostatecznego przygotowania lub procesów kontroli dostawcy usługi objętej outsourcingiem. Nieskuteczne zarządzanie outsourcingiem może prowadzić do braku odpowiednich umiejętności i zdolności do pełnej identyfikacji, oceny, ograniczenia i monitorowania ryzyka ICT oraz może ograniczać zdolności operacyjne instytucji.	• Niedostateczne procedury reagowania na incydenty, umowne mechanizmy kontroli i gwarancje wynikające z umowy z usługodawcą, które zwiększają zasadniczą zależność od osób trzecich lub dystrybutorów. • Nieodpowiednie kontrole zarządzania zmianą dotyczące środowiska dostawcy usług ICT mogą prowadzić do znacznego pogorszenia usługi lub jej braku.
	Nieodpowiednie zabezpieczenie osoby trzeciej lub innej jednostki	Hakerstwo systemów ICT osoby trzeciej będącej usługodawcą z bezpośrednim wpływem na usługi objęte outsourcingiem lub dane krytyczne/poufne przechowywane przez usługodawcę.	• Hakerstwo usługodawców przez przestępców lub terrorystów jako punktu wejścia do systemów ICT instytucji w celu uzyskania dostępu do danych krytycznych/wrażliwych przechowywanych przez

Kategorie ryzyka ICT	Ryzyka ICT (wykaz niewyczerpujący [10])	Opis ryzyka	Przykłady
	grupy	Pracownicy usługodawcy posiadający nieuprawniony dostęp do danych krytycznych/wrażliwych przechowywanych przez usługodawcę	usługodawcę lub ich zniszczenia. • Złośliwe aplikacje po stronie usługodawcy próbujące dokonać kradzieży i sprzedaży danych wrażliwych.