Wytyczne

EBA/GL/2019/04

28 listopada 2019 r.

Wytyczne EUNB w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT

Obowiązki w zakresie zgodności z przepisami i sprawozdawczości

Status niniejszych wytycznych

1. Niniejszy dokument zawiera wytyczne wydane na mocy art. 16 rozporządzenia (UE) nr 1093/2010[1]. 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. W wytycznych określono stanowisko EUNB w sprawie właściwych praktyk nadzorczych w ramach Europejskiego Systemu Nadzoru Finansowego lub sposobu, w jaki należy stosować prawo Unii Europejskiej w danym 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 nadzoru), również jeżeli wytyczne są skierowane przede wszystkim do instytucji.

Wymogi sprawozdawcze

3. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy mają obowiązek poinformować EUNB w terminie do dnia ([dd.mm.yyyy]) o tym, czy stosują się lub czy zamierzają stosować się do niniejszych wytycznych, albo podać uzasadnienie niestosowania się do nich. W razie nieprzekazania tej informacji w wyznaczonym terminie EUNB uzna, że właściwe organy nie stosują się do niniejszych wytycznych. Informacje należy przekazać poprzez wysłanie formularza dostępnego na stronie internetowej EUNB na adres compliance@eba.europa.eu z dopiskiem „EBA/GL/2019/04”. Powiadomienia przekazują osoby odpowiednio upoważnione do informowania o stosowaniu się do wytycznych w imieniu właściwych organów. Do EUNB należy także zgłaszać wszelkie zmiany dotyczące stosowania się do wytycznych.

4. Powiadomienia zostaną opublikowane na stronie internetowej EUNB, zgodnie z art. 16 ust. 3.

[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).

Przedmiot, zakres stosowania i definicje

Przedmiot

5. Niniejsze wytyczne opierają się na przepisach art. 74 dyrektywy 2013/36/UE (dyrektywy w sprawie wymogów kapitałowych) dotyczących zarządzania wewnętrznego oraz wynikają z mandatu uprawniającego do wydawania wytycznych przewidzianego w art. 95 ust. 3 dyrektywy (UE) 2015/2366 (drugiej dyrektywy w sprawie usług płatniczych).

6. Niniejsze wytyczne określają środki zarządzania ryzykiem, które instytucje finansowe (zdefiniowane w ust. 9 poniżej) muszą stosować zgodnie z art. 74 dyrektywy w sprawie wymogów kapitałowych, aby zarządzać ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (ICT) i ryzykiem związanym z bezpieczeństwem ICT w odniesieniu do wszystkich działań, jak również środki, które muszą stosować zgodnie z art. 95 ust. 1 drugiej dyrektywy w sprawie usług płatniczych dostawcy usług płatniczych (zdefiniowani w ust. 9 poniżej), aby zarządzać ryzykiem operacyjnym i ryzykiem związanym z bezpieczeństwem ICT (odpowiadającym „ryzyku związanemu z technologiami i bezpieczeństwem ICT") w odniesieniu do usług płatniczych, które świadczą. Niniejsze wytyczne obejmują wymagania dotyczące bezpieczeństwa informacji, w tym cyberbezpieczeństwa, w zakresie, w jakim informacje są przechowywane w systemach ICT.

Zakres stosowania

7. Niniejsze wytyczne mają zastosowanie do zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT instytucji finansowych (zdefiniowanych w ust. 9). Na potrzeby niniejszych wytycznych pojęcie „ryzyko związane z technologiami i bezpieczeństwem ICT" w odniesieniu do świadczenia usług płatniczych odnosi się do ryzyka operacyjnego i ryzyka dla bezpieczeństwa, o których mowa w art. 95 drugiej dyrektywy w sprawie usług płatniczych.

8. W przypadku dostawców usług płatniczych (zdefiniowanych w ust. 9) niniejsze wytyczne mają zastosowanie do świadczenia usług płatniczych zgodnie z zakresem i mandatem z art. 95 drugiej dyrektywy w sprawie usług płatniczych. W odniesieniu do instytucji (zdefiniowanych w ust. 9) niniejsze wytyczne mają zastosowanie do wszystkich realizowanych przez nie działań.

Odbiorcy

9. Niniejsze wytyczne są skierowane do instytucji finansowych, które na potrzeby niniejszych wytycznych oznaczają (1) dostawców usług płatniczych zgodnie z definicją zawartą w art. 4 pkt 11 drugiej dyrektywy w sprawie usług płatniczych oraz (2) instytucji oznaczających instytucje kredytowe i firmy inwestycyjne zgodnie z definicją zawartą w art. 4 ust. 1 pkt 3 rozporządzenia (UE) nr 575/2013. Niniejsze wytyczne mają zastosowanie również do właściwych organów określonych w art. 4 ust. 1 pkt 40 rozporządzenia (UE) nr 575/2013, w tym Europejskiego Banku Centralnego, w odniesieniu do spraw dotyczących zadań powierzonych mu rozporządzeniem (UE) nr 1024/2013, a także do właściwych organów w rozumieniu drugiej

dyrektywy w sprawie usług płatniczych, określonych w art. 4 pkt 2 ppkt (i) rozporządzenia (UE) nr 1093/2010.

Definicje

10. O ile nie określono inaczej, pojęcia stosowane i zdefiniowane w dyrektywie 2013/36/UE (dyrektywie w sprawie wymogów kapitałowych), rozporządzeniu (UE) nr 575/2013 (rozporządzeniu w sprawie wymogów kapitałowych) oraz dyrektywie (UE) 2015/2366 (drugiej dyrektywie w sprawie usług płatniczych) mają w niniejszych wytycznych takie samo znaczenie. Ponadto do celów niniejszych wytycznych stosuje się następujące definicje:

Ryzyko związane z technologiami i bezpieczeństwem ICT	Ryzyko strat wynikające z naruszenia poufności, naruszenia integralności systemów i danych, nieodpowiedniości lub niedostępności systemów i danych, lub też niezdolności do zmiany technologii informacyjnej w rozsądnym czasie i przy uwzględnieniu rozsądnych kosztów w przypadku zmiany wymogów w zakresie otoczenia lub prowadzenia działalności gospodarczej (tj. elastyczność)[2]. Obejmuje to ryzyko związane z bezpieczeństwem ICT wynikające z nieodpowiednich lub niepomyślnie zrealizowanych procesów wewnętrznych lub zdarzeń zewnętrznych, w tym cyberataków lub nieodpowiedniego zabezpieczenia fizycznego.
Organ zarządzający	(a) W przypadku instytucji kredytowych i firm inwestycyjnych termin ten ma takie samo znaczenie jak w definicji zawartej w art. 3 ust. 1 pkt 7 dyrektywy 2013/36/UE. (b) W przypadku instytucji płatniczych lub instytucji pieniądza elektronicznego termin ten oznacza dyrektorów lub osoby odpowiedzialne za zarządzanie instytucjami płatniczymi i instytucjami pieniądza elektronicznego oraz, w stosownych przypadkach, osoby odpowiedzialne za zarządzanie działalnością instytucji płatniczych i instytucji pieniądza elektronicznego. (c) W przypadku dostawców usług płatniczych, o których mowa w art. 1 ust. 1 lit. c), e) i f) dyrektywy (UE) 2015/2366, termin ten ma znaczenie zgodne z obowiązującymi przepisami prawa unijnego lub prawa krajowego.
Incydent operacyjny lub incydent bezpieczeństwa	Pojedyncze zdarzenie lub seria powiązanych zdarzeń nieplanowanych przez instytucję finansową, które mają lub prawdopodobnie będą mieć niekorzystny wpływ na integralność, dostępność, poufność lub uwierzytelnienie usług.

[2] Definicja pochodząca z wytycznych EUNB dotyczących wspólnych procedur i metod stosowanych w ramach procesu przeglądu i oceny nadzorczej z dnia 19 grudnia 2014 r. (EBA/GL/2014/13) zmienionych wytycznymi EBA/GL/2018/03.

Kadra kierownicza wyższego szczebla	(a) W przypadku instytucji kredytowych i firm inwestycyjnych termin ten ma takie samo znaczenie jak w definicji zawartej w art. 3 ust. 1 pkt 9 dyrektywy 2013/36/UE. (b) W przypadku instytucji płatniczych lub instytucji pieniądza elektronicznego termin ten oznacza osoby fizyczne pełniące funkcje wykonawcze w instytucji i odpowiedzialne przed organem zarządzającym za bieżące zarządzanie instytucją. (c) W przypadku dostawców usług płatniczych, o których mowa w art. 1 ust. 1 lit. c), e) i f) dyrektywy (UE) 2015/2366, termin ten ma znaczenie zgodne z obowiązującymi przepisami prawa unijnego lub prawa krajowego.
Apetyt na ryzyko	Łączny poziom i rodzaje ryzyka, jakie dostawcy usług płatniczych i instytucje są skłonne podejmować w ramach swojej zdolności do ponoszenia ryzyka – zgodnie ze swoim modelem działalności – w celu realizacji swoich celów strategicznych.
Komórka ds. audytu	(a) W przypadku instytucji kredytowych i firm inwestycyjnych komórka ds. audytu została określona w rozdziale 22 wytycznych EUNB w sprawie zarządzania wewnętrznego (EBA/GL/2017/11). (b) W przypadku dostawców usług płatniczych niebędących instytucjami kredytowymi komórka ds. audytu musi być niezależną komórką w obrębie podmiotu dostawcy usług płatniczych lub komórką niezależną od dostawcy usług płatniczych i może być komórką ds. audytu wewnętrznego lub zewnętrznego.
Projekty ICT	Wszelkie projekty lub ich część, których przedmiotem jest zmiana, zastąpienie, wycofanie lub wdrożenie systemów i usług ICT. Projekty ICT mogą stanowić część szerszych programów ICT lub programów transformacji działalności.
Strona trzecia	Organizacja, która nawiązała relacje biznesowe lub zawarła z podmiotem umowę na dostawę produktu lub świadczenie usługi[3].
Zasób informacyjny	Gromadzenie informacji w postaci materialnej bądź niematerialnej, które zasługują na ochronę.
Zasób ICT	Zasób w postaci oprogramowania lub sprzętu występujący w otoczeniu biznesowym.
Systemy ICT[4]	Ustanowienie ICT jako części mechanizmu lub sieci połączonej wspierającej operacje instytucji finansowej.
Usługi ICT[5]	Usługi świadczone przez systemy ICT na rzecz przynajmniej jednego użytkownika wewnętrznego lub zewnętrznego. Przykłady obejmują wprowadzanie danych, przechowywanie

[3] Definicja z elementów podstawowych G7 dla zarządzania ryzykiem cybernetycznym strony trzeciej w sektorze finansowym.
[4] Definicja z wytycznych w sprawie oceny ryzyka technologii informacyjno-komunikacyjnych w ramach procesu przeglądu i oceny nadzorczej (SREP) (EBA/GL/2017/05).
[5] Tamże.

danych, przetwarzanie danych oraz usługi sprawozdawczości, jak również monitorowanie oraz usługi wspierania biznesu i procesów decyzyjnych.

Wdrożenie

Data rozpoczęcia stosowania

11. Niniejsze wytyczne mają zastosowanie od dnia 30 czerwca 2020 r.

Uchylenie

12. Wytyczne w sprawie środków bezpieczeństwa dotyczących ryzyk operacyjnych i ryzyk dla bezpieczeństwa (EBA/GL/2017/17) wydane w 2017 r. zostaną uchylone i zastąpione niniejszymi wytycznymi z dniem rozpoczęcia stosowania niniejszych wytycznych.

Wytyczne w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT

1.1. Zasada proporcjonalności

1. Wszystkie instytucje finansowe powinny stosować się do przepisów określonych w niniejszych wytycznych z uwzględnieniem zasady proporcjonalności, biorąc pod uwagę rozmiar instytucji finansowej, jej organizację wewnętrzną oraz charakter, zakres, złożoność i ryzykowność usług i produktów, które instytucja finansowa dostarcza lub zamierza dostarczać.

1.2. Zarządzanie i strategia

1.2.1. Zarządzanie

2. Organ zarządzający powinien zapewnić, aby instytucja finansowa dysponowała odpowiednim zarządzaniem wewnętrznym i ramami kontroli wewnętrznej w odniesieniu do ryzyka związanego z technologiami i bezpieczeństwem ICT. Organ zarządzający powinien jasno określić role i obowiązki funkcji ICT, zarządzania ryzykiem dla bezpieczeństwa informacji oraz ciągłości działalności, w tym organu zarządzającego i jego komitetów.

3. Organ zarządzający powinien zapewnić, aby liczba członków personelu instytucji finansowej i ich umiejętności były odpowiednie dla bieżącego wspierania potrzeb operacyjnych w zakresie ICT oraz procesów zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT

oraz dla zapewnienia wdrażania strategii ICT. Organ zarządzający powinien zapewnić, aby przydzielony budżet pozwalał na realizację powyższego. Ponadto instytucje finansowe powinny zapewnić, aby wszyscy członkowie personelu, w tym osoby pełniące najważniejsze funkcje, odbywały odpowiednie szkolenie w zakresie ryzyka związanego z technologiami i bezpieczeństwem ICT, w tym w zakresie bezpieczeństwa informacji, co roku lub – stosownie do wymogów – częściej (zob. punkt 1.4.7).

4. Organ zarządzający ponosi ogólną odpowiedzialność za ustalenie, zatwierdzenie i nadzorowanie realizacji strategii ICT przez instytucje finansowe w ramach ich ogólnej strategii biznesowej, jak również za ustanowienie skutecznych ram zarządzania ryzykiem w odniesieniu do ryzyka związanego z technologiami i bezpieczeństwem ICT.

1.2.2. Strategia

5. Strategia ICT powinna być dostosowana do ogólnej strategii biznesowej instytucji finansowych i powinna określać:

   a) w jaki sposób instytucje finansowe powinny się rozwijać, aby skutecznie wspierać strategię biznesową i uczestniczyć w niej, włączając w to rozwój struktury organizacyjnej, zmiany systemu ICT oraz najważniejsze zależności względem stron trzecich;
   b) planowaną strategię i rozwój architektury ICT, w tym zależności względem stron trzecich;
   c) jasne cele dotyczące bezpieczeństwa informacji, skoncentrowane na systemach ICT i usługach ICT, personelu i procesach.

6. Instytucje finansowe powinny określić plany działań obejmujących środki stosowane w dążeniu do realizacji celu strategii ICT. Informacje o nich powinny być przekazane całemu zainteresowanemu personelowi (w tym – w stosownych przypadkach – wykonawcom i dostawcom zewnętrznym). Plany działań należy poddawać okresowym przeglądom w celu zapewnienia ich przydatności i stosowności. Instytucje finansowe powinny również ustanowić procesy służące monitorowaniu i pomiarowi skuteczności realizacji strategii ICT.

1.2.3. Korzystanie z usług dostawców zewnętrznych

7. Bez uszczerbku dla wytycznych EUNB w sprawie outsourcingu (EBA/GL/2019/02) i art. 19 drugiej dyrektywy w sprawie usług płatniczych instytucje finansowe powinny zapewnić skuteczność środków ograniczania ryzyka określonych w ramach zarządzania ryzykiem, w tym środków określonych w niniejszych wytycznych, w sytuacji powierzania dostawcom zewnętrznym, w tym podmiotom należącym do tej samej grupy, funkcji operacyjnych związanych z usługami płatniczymi lub usług ICT i systemów ICT w związku z dowolnym rodzajem działalności bądź w sytuacji korzystania z usług stron trzecich.

8. Aby zapewnić ciągłość usług ICT i systemów ICT, instytucje finansowe powinny zadbać o to, aby umowy, w tym umowy o gwarantowanym poziomie świadczenia usług (zarówno w zwykłych okolicznościach, jak i w razie zakłócenia usługi – zob. rozdział 1.7.2), zawierane z dostawcami

(dostawcami usług objętych outsourcingiem, podmiotami należącymi do tej samej grupy lub dostawcami zewnętrznymi) obejmowały następujące elementy:

a) stosowne i proporcjonalne cele i środki związane z bezpieczeństwem informacji, w tym wymogi takie jak minimalne wymogi w zakresie bezpieczeństwa; specyfikacje cyklu życia danych instytucji finansowej; wszelkie wymogi dotyczące szyfrowania danych, bezpieczeństwa sieci i procesów monitorowania bezpieczeństwa oraz lokalizacji centrów danych;
b) procedury operacyjne i procedury postępowania na wypadek incydentu bezpieczeństwa, w tym przekazywanie informacji o incydentach jednostkom wyższego szczebla i sprawozdawczość.

9. Instytucje finansowe powinny monitorować i uzyskać zapewnienia co do poziomu zgodności działania takich dostawców z określonymi celami i środkami bezpieczeństwa oraz parametrami docelowymi skuteczności działania instytucji finansowej.

1.3. Ramy zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT

1.3.1. Organizacja i cele

10. Instytucje finansowe powinny określić ryzyko związane z technologiami i bezpieczeństwem ICT oraz zarządzać nim. Funkcje ICT odpowiedzialne za systemy ICT, procesy i operacje związane z bezpieczeństwem powinny dysponować odpowiednimi procesami i środkami kontroli, aby zapewnić identyfikowanie, analizowanie, pomiar, monitorowanie i zgłaszanie wszystkich rodzajów ryzyka oraz zarządzanie nimi, a także przestrzeganie limitu apetytu na ryzyko instytucji finansowej, jak również aby zapewnić zgodność realizowanych przez nie działań z wymogami zewnętrznymi i wewnętrznymi.

11. Instytucje finansowe powinny powierzyć odpowiedzialność za zarządzanie i nadzorowanie ryzyka związanego z technologiami i bezpieczeństwem ICT komórce ds. kontroli, przestrzegając wymogów rozdziału 19 wytycznych EUNB w sprawie zarządzania wewnętrznego (EBA/GL/2017/11). Instytucje finansowe powinny zapewnić niezależność i obiektywność komórki ds. kontroli poprzez odpowiednie oddzielenie jej od procesów operacji ICT. Komórka ds. kontroli powinna odpowiadać bezpośrednio przed organem zarządzającym i ponosić odpowiedzialność za monitorowanie i kontrolowanie przestrzegania ram zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT. Powinna zapewnić, aby ryzyko związane z technologiami i bezpieczeństwem ICT było identyfikowane, oceniane, monitorowane oraz objęte pomiarem, zarządzaniem i sprawozdawczością. Instytucje finansowe powinny zapewnić, aby ta komórka ds. kontroli nie odpowiadała za żaden audyt wewnętrzny.

    Komórka ds. audytu wewnętrznego powinna, stosując podejście oparte na ocenie ryzyka, mieć możliwość dokonania niezależnego przeglądu i zapewnienia obiektywnego zagwarantowania zgodności wszystkich działań związanych z technologiami i bezpieczeństwem ICT oraz wszystkich jednostek instytucji finansowej z polityką i procedurami instytucji finansowej oraz

wymogami zewnętrznymi, przestrzegając przy tym rozdziału 22 wytycznych EUNB w sprawie zarządzania wewnętrznego (EBA/GL/2017/11).

12. Instytucje finansowe powinny określić i przypisać najważniejsze role i obowiązki oraz stosowne struktury raportowania w celu zapewnienia skuteczności ram zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT. Ramy te powinny być w pełni uwzględnione w ogólnych procesach zarządzania ryzykiem instytucji finansowych i dostosowane do nich.

13. Ramy zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT powinny obejmować procesy służące:

    a) ustaleniu apetytu na ryzyko związane z technologiami i bezpieczeństwem ICT, stosownie do apetytu na ryzyko instytucji finansowej;
    b) zidentyfikowaniu i ocenie ryzyka związanego z technologiami i bezpieczeństwem ICT, na które narażona jest instytucja finansowa;
    c) określeniu środków ograniczania ryzyka, w tym środków kontroli, w celu ograniczenia ryzyka związanego z technologiami i bezpieczeństwem ICT;
    d) monitorowaniu skuteczności tych środków, jak również liczby zgłoszonych incydentów, w tym – w przypadku dostawców usług płatniczych – incydentów zgłaszanych zgodnie z art. 96 drugiej dyrektywy w sprawie usług płatniczych wpływających na działania związane z ICT, a także podjęciu działań w celu skorygowania tych środków w razie konieczności;
    e) przedstawianiu organowi zarządzającemu sprawozdań na temat ryzyka związanego z technologiami i bezpieczeństwem ICT oraz środków kontroli;
    f) stwierdzaniu i poddawaniu ocenie, czy istnieje ryzyko związane z technologiami i bezpieczeństwem ICT wynikające z ważnej zmiany w systemie ICT lub usługach ICT, procesach lub procedurach lub zaistniałe w następstwie istotnego incydentu operacyjnego lub incydentu bezpieczeństwa.

14. Instytucje finansowe powinny zapewnić, aby ramy zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT były udokumentowane oraz stale udoskonalane na podstawie wniosków wyciągniętych w trakcie ich wdrażania i monitorowania. Ramy zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT powinny być zatwierdzane i poddawane przeglądowi przez organ zarządzający co najmniej raz w roku.

1.3.2. Określanie funkcji, procesów i zasobów

15. Instytucje finansowe powinny określić, ustanowić i utrzymać zaktualizowany schemat funkcji biznesowych, ról i procesów pomocniczych w celu określenia znaczenia każdej i każdego z nich oraz zależności między nimi w związku z ryzykiem związanym z technologiami i bezpieczeństwem ICT.

16. Ponadto instytucje finansowe powinny określić, ustanowić i utrzymać zaktualizowany schemat zasobów informacyjnych wspierających funkcje biznesowe i procesy pomocnicze, takie jak systemy ICT, personel, wykonawcy, osoby trzecie oraz zależności od innych systemów i procesów wewnętrznych i zewnętrznych, tak aby móc co najmniej zarządzać zasobami informacyjnymi, które służą wspieraniu ich krytycznych funkcji i procesów biznesowych.

1.3.3. Klasyfikacja i ocena ryzyka

17. Instytucje finansowe powinny klasyfikować zidentyfikowane funkcje biznesowe, procesy pomocnicze i zasoby informacyjne, o których mowa w ust. 15 i 16, pod kątem krytycznego znaczenia.

18. Aby określić krytyczne znaczenie tych funkcji biznesowych, procesów pomocniczych i zasobów informacyjnych, instytucje finansowe powinny brać pod uwagę przynajmniej wymogi dotyczące poufności, integralność i dostępności. Należy jasno określić zakres odpowiedzialności i obowiązków w zakresie zasobów informacyjnych.

19. Instytucje finansowe przy okazji przeprowadzania oceny ryzyka powinny dokonywać przeglądu adekwatności klasyfikacji zasobów informacyjnych i odpowiedniej dokumentacji.

20. Instytucje finansowe powinny określić ryzyko związane z technologiami i bezpieczeństwem ICT, które wpływa na zidentyfikowane i sklasyfikowane funkcje biznesowe, procesy pomocnicze i zasoby informacyjne, stosownie do ich krytycznego znaczenia. Ocenę ryzyka należy przeprowadzać i dokumentować raz w roku lub – w razie konieczności – częściej. Tego rodzaju ocenę ryzyka należy przeprowadzać również w razie jakichkolwiek ważnych zmian infrastruktury, procesów i procedur wpływających na funkcje biznesowe, procesy pomocnicze lub zasoby informacyjne, a w konsekwencji – aktualizować ocenę ryzyka instytucji finansowych.

21. Instytucje finansowe powinny zapewnić ciągłe monitorowanie zagrożeń i podatności właściwych dla ich procesów biznesowych, funkcji pomocniczych i zasobów informacyjnych oraz regularnie dokonywać przeglądu scenariuszy ryzyka, które mają na nie wpływ.

1.3.4. Ograniczanie ryzyka

22. Na podstawie ocen ryzyka instytucje finansowe powinny określić, jakie środki są konieczne do ograniczenia zidentyfikowanego ryzyka związanego z technologiami i bezpieczeństwem ICT do dopuszczalnych poziomów, jak również określić, czy konieczne są zmiany w obrębie istniejących procesów biznesowych, środków kontroli, systemów ICT i usług ICT. Instytucja finansowa powinna brać pod uwagę czas potrzebny na wdrożenie takich zmian oraz czas na podjęcie odpowiednich działań tymczasowych służących ograniczaniu ryzyka związanego z technologiami i bezpieczeństwem ICT w taki sposób, aby pozostać w granicach apetytu na ryzyko związane z technologiami i bezpieczeństwem ICT określonego dla danej instytucji finansowej.

23. Instytucje finansowe powinny określić i wdrożyć środki ograniczania zidentyfikowanego ryzyka związanego z technologiami i bezpieczeństwem ICT oraz środki służące ochronie zasobów informacyjnych stosownie do ich klasyfikacji.

1.3.5. Sprawozdawczość

24. Instytucje finansowe powinny zgłaszać wyniki oceny ryzyka organowi zarządzającemu w sposób jasny i terminowy. Tego rodzaju sprawozdawczość odbywa się bez uszczerbku dla obowiązku

dostawców usług płatniczych w zakresie dostarczania właściwym organom aktualnej i kompleksowej oceny ryzyka, o której mowa w art. 95 ust. 2 dyrektywy (UE) 2015/2366.

1.3.6. Audyt

25. Zarządzanie instytucją finansową, systemy i procesy związane z ryzykiem związanym z technologiami i bezpieczeństwem ICT powinny być regularnie badane przez audytorów posiadających odpowiednią wiedzę, umiejętności i wiedzę specjalistyczną z zakresu ryzyka związanego z technologiami i bezpieczeństwem ICT oraz z zakresu płatności (w przypadku dostawców usług płatniczych), aby zapewnić organowi zarządzającemu niezależną gwarancję ich skuteczności. Audytorzy powinni być niezależni w obrębie instytucji finansowej lub niezależni od instytucji finansowej. Częstotliwość i przedmiot audytów powinny być współmierne do danego ryzyka związanego z technologiami i bezpieczeństwem ICT.

26. Organ zarządzający instytucji finansowej powinien zatwierdzić plan audytu, w tym wszelkie audyty ICT i ich istotne zmiany. Plan audytu i jego realizacja, w tym częstotliwość audytu, powinny odzwierciedlać ryzyko związane z technologiami i bezpieczeństwem ICT wpisane w funkcjonowanie instytucji finansowej i być względem niego proporcjonalne, a także powinny być regularnie aktualizowane.

27. Należy ustalić formalny proces działań następczych, w tym uregulować terminową weryfikację i działania naprawcze w odniesieniu do najważniejszych ustaleń z audytu ICT.

1.4. Bezpieczeństwo informacji

1.4.1. Polityka bezpieczeństwa informacji

28. Instytucje finansowe powinny opracować i udokumentować politykę bezpieczeństwa informacji, która powinna określać zasady wysokiego szczebla i uregulowania służące ochronie poufności, integralności i dostępności danych i informacji instytucji finansowych i ich klientów. W przypadku dostawców usług płatniczych polityka ta określona jest w dokumencie dotyczącym strategii w zakresie bezpieczeństwa przyjmowanym zgodnie z art. 5 ust. 1 lit. j) dyrektywy (UE) 2015/2366. Polityka bezpieczeństwa informacji powinna być dostosowana do celów instytucji finansowej w obszarze bezpieczeństwa informacji i oparta na odpowiednich wynikach procesu oceny ryzyka. Polityka powinna zostać przyjęta przez organ zarządzający.

29. Powinna ona zawierać opis najważniejszych ról i obowiązków w zarządzaniu bezpieczeństwem informacji, a także określać wymogi obowiązujące personel i wykonawców oraz mające zastosowanie do procesów i technologii związanych z bezpieczeństwem informacji, przy założeniu że personel i wykonawcy na każdym szczeblu odpowiadają za zapewnienie bezpieczeństwa informacji instytucji finansowej. Polityka powinna zapewniać poufność, integralność i dostępność krytycznych zasobów logicznych i fizycznych instytucji finansowych, źródeł oraz danych wrażliwych, niezależnie od tego, czy są to dane przechowywane (ang. *data at rest*), dane przesyłane (ang. *data in transit*) czy też dane wykorzystywane (ang. *data in use*). Polityka bezpieczeństwa informacji powinna być przedstawiona wszystkim członkom personelu i wykonawcom instytucji finansowej.

30. Na podstawie polityki bezpieczeństwa informacji instytucje finansowe powinny ustanowić i wdrożyć środki bezpieczeństwa służące ograniczeniu ryzyka związanego z technologiami i bezpieczeństwem ICT, na które są one narażone. Środki te powinny obejmować:

    a) organizację i zarządzanie zgodnie z ust. 10 i 11;
    b) bezpieczeństwo logiczne (rozdział 1.4.2);
    c) bezpieczeństwo fizyczne (rozdział 1.4.3);
    d) bezpieczeństwo operacji ICT (rozdział 1.4.4);
    e) bezpieczeństwo monitorowania (rozdział 1.4.5);
    f) przeglądy, ocenę i testowanie bezpieczeństwa informacji (rozdział 1.4.6);
    g) szkolenie i świadomość w zakresie bezpieczeństwa informacji (rozdział 1.4.7).

1.4.2. Bezpieczeństwo logiczne

31. Instytucje finansowe powinny określić, udokumentować i wdrożyć procedury logicznej kontroli dostępu (zarządzanie tożsamością i dostępem). Procedury te powinny zostać wdrożone oraz być egzekwowane, monitorowane i poddawane okresowym przeglądom. W ramach tych procedur należy również przewidzieć środki kontroli służące monitorowaniu nieprawidłowości. Procedury te powinny wprowadzać co najmniej następujące elementy (termin „użytkownik" oznacza użytkownika technicznego):

    (a) **Zasada wiedzy koniecznej, możliwie ograniczonych uprawnień oraz rozdziału obowiązków:** instytucje finansowe powinny zarządzać prawami dostępu do zasobów informacyjnych i systemów pomocniczych zgodnie z zasadą wiedzy koniecznej, również w odniesieniu do dostępu zdalnego. Użytkownicy powinni mieć minimalne prawa dostępu, jakie są ściśle konieczne do realizacji właściwych im obowiązków (zasada „możliwie ograniczonych uprawnień"), tj. w celu zapobieżenia nieuzasadnionemu dostępowi do dużych zbiorów danych oraz zapobieżenia przydziałowi takiej konfiguracji praw dostępu, która mogłaby zostać wykorzystana do ominięcia zabezpieczeń (zasada „rozdziału obowiązków").

    (b) **Odpowiedzialność użytkownika**: instytucje finansowe, na tyle, na ile to możliwe, powinny ograniczyć wykorzystanie kont generycznych i kont współdzielonych (grupowych) oraz zapewnić możliwość ustalenia tożsamości każdego z użytkowników w powiązaniu z czynnościami wykonanymi w systemach ICT.

    (c) **Uprzywilejowany dostęp**: instytucje finansowe powinny wdrożyć ścisłe środki kontroli uprzywilejowanego dostępu do systemu poprzez ścisłe ograniczenie i uważne monitorowanie kont o podwyższonych uprawnieniach dostępu do systemu (np. kont administratorów). W celu zapewnienia bezpiecznej komunikacji i zmniejszenia ryzyka zdalny dostęp administracyjny do krytycznych systemów ICT należy przyznawać jedynie na zasadzie wiedzy koniecznej i przy zastosowaniu metod silnego uwierzytelniania.

    (d) **Rejestrowanie działalności użytkownika:** rejestrowana i monitorowana powinna być działalność przynajmniej wszystkich użytkowników uprzywilejowanych. Dzienniki dostępu powinny być zabezpieczone przed niedozwoloną modyfikacją lub usunięciem wpisów i przechowywane przez okres współmierny do krytycznego znaczenia określonych funkcji biznesowych, procesów pomocniczych i zasobów informacyjnych,

zgodnie z rozdziałem 1.3.3, bez uszczerbku dla wymogów dotyczących przechowywania danych określonych w prawie unijnym i krajowym. Instytucja finansowa powinna wykorzystywać te informacje do ułatwienia stwierdzania i prowadzenia dochodzeń w sprawie nieprawidłowych działań wykrytych w ramach świadczenia usług.

(e) **Zarządzanie dostępem:** udzielanie, wycofywanie lub modyfikowanie praw dostępu powinno odbywać się terminowo, zgodnie z wcześniej określonym schematem procesu zatwierdzania, w którym uczestniczy osoba odpowiedzialna za informacje, których dostęp dotyczy (osoba odpowiedzialna za zasób informacyjny). W przypadku rozwiązania stosunku pracy prawa dostępu zostają niezwłocznie odebrane.

(f) **Potwierdzenie uprawnień**: prawa dostępu powinny być poddawane okresowemu przeglądowi w celu zapewnienia, aby użytkownicy nie posiadali nadmiernych uprawnień i aby prawa dostępu były odbierane, gdy nie są już konieczne.

(g) **Metody uwierzytelniania:** instytucje finansowe powinny egzekwować metody uwierzytelniania, które są dostatecznie stabilne, aby odpowiednio i skutecznie zapewnić przestrzeganie polityki i procedur kontroli dostępu. Metody uwierzytelniania powinny być współmierne względem krytycznego charakteru systemów ICT, informacji lub procesów, których dotyczy dostęp. Powinny one obejmować przynajmniej złożone hasła lub silniejsze metody uwierzytelniania (takie jak uwierzytelnianie dwuelementowe), dobrane stosownie do występującego ryzyka.

32. Elektroniczny dostęp do danych i systemów ICT za pośrednictwem aplikacji powinien być ograniczony do minimum niezbędnego do świadczenia danej usługi.

1.4.3. Bezpieczeństwo fizyczne

33. Instytucje finansowe powinny określić, udokumentować i wdrożyć środki bezpieczeństwa fizycznego w celu ochrony swojego terenu, centrów danych oraz obszarów wrażliwych przed nieupoważnionym dostępem i zagrożeniami środowiskowymi.

34. Zezwolenie na fizyczny dostęp do systemów ICT powinny mieć jedynie upoważnione osoby. Upoważnienia powinny być przydzielane zgodnie z zadaniami i obowiązkami danej osoby, jedynie osobom odpowiednio przeszkolonym i monitorowanym. Dostęp fizyczny powinien być poddawany regularnemu przeglądowi, aby zapewnić niezwłoczne odebranie praw dostępu, gdy nie są one konieczne.

35. Odpowiednie środki służące ochronie przed zagrożeniami środowiskowymi powinny być współmierne względem znaczenia budynków lub krytycznego charakteru operacji lub systemów ICT usytuowanych w tych budynkach.

1.4.4. Bezpieczeństwo operacji ICT

36. Instytucje finansowe powinny wdrożyć procedury służące zapobieganiu problemom z bezpieczeństwem systemów ICT i usług ICT oraz ograniczać do minimum ich wpływ na dostarczanie usług ICT. Procedury te powinny obejmować następujące środki:

a) identyfikację potencjalnych podatności, które należy oceniać i naprawiać poprzez zapewnienie aktualizacji oprogramowania i oprogramowania firmware, włączając w to

oprogramowanie zapewniane przez instytucje finansowe użytkownikom wewnętrznym i zewnętrznym, poprzez wprowadzanie krytycznych poprawek zabezpieczeń oraz poprzez wdrażanie kompensacyjnych środków kontroli;

b) wdrażanie poziomów bazowych konfiguracji bezpieczeństwa dla wszystkich elementów sieciowych;
c) wdrażanie segmentacji sieci, systemów zapobiegania utracie danych oraz szyfrowania ruchu w sieci (zgodnie z klasyfikacją danych);
d) wdrażanie ochrony punktów końcowych, w tym serwerów, stanowisk pracy i urządzeń mobilnych; instytucje finansowe powinny ocenić, czy punkty końcowe spełniają standardy bezpieczeństwa zdefiniowane przez nie przed udzieleniem im dostępu do sieci korporacyjnej;
e) zapewnienie mechanizmów służących weryfikowaniu integralności oprogramowania, oprogramowania firmware i danych;
f) szyfrowanie danych przechowywanych i przesyłanych (stosownie do klasyfikacji danych).

37. Ponadto instytucje finansowe powinny na bieżąco określać, czy zmiany w istniejącym środowisku operacyjnym mają wpływ na istniejące środki bezpieczeństwa lub czy wymagają wprowadzenia dodatkowych środków mających na celu stosowne ograniczenie danego ryzyka. Zmiany takie należy wprowadzać w ramach realizowanego przez daną instytucję finansową formalnego procesu zarządzania zmianą, który powinien zapewnić odpowiednie planowanie, testowanie, dokumentowanie, zatwierdzanie i wdrażanie zmian.

1.4.5. Monitorowanie bezpieczeństwa

38. Instytucje finansowe powinny ustanowić i wdrożyć politykę i procedury służące wykrywaniu nieprawidłowości, które mogą wpływać na bezpieczeństwo informacji w instytucjach finansowych, a także stosownemu reagowaniu na takie zdarzenia. W ramach stałego monitorowania instytucje finansowe powinny wdrażać odpowiednie i skuteczne narzędzia wykrywania i zgłaszania fizycznych lub logicznych włamań, a także przypadki naruszenia poufności, integralności i dostępności zasobów informacyjnych. Procesy stałego monitorowania i wykrywania obejmują:

    a) odpowiednie czynniki wewnętrzne i zewnętrzne, w tym funkcje biznesowe i funkcje administracyjne ICT;
    b) transakcje służące wykrywaniu nieprawidłowości w korzystaniu z dostępu przez osoby trzecie lub inne podmioty oraz wewnętrznych nieprawidłowości w korzystaniu z dostępu;
    c) potencjalne zagrożenia wewnętrzne i zewnętrzne.

39. Instytucje finansowe powinny określić i wdrożyć procesy i struktury organizacyjne w celu identyfikowania i stałego monitorowania zagrożeń dla bezpieczeństwa, które mogłyby w znaczącym stopniu wpłynąć na ich zdolności do świadczenia usług. Instytucje finansowe powinny aktywnie monitorować zmiany związane z rozwojem technologii, aby mieć pewność, że są świadome zagrożeń dla bezpieczeństwa. Instytucje finansowe powinny wdrażać środki

wykrywania, przykładowo, w celu stwierdzenia ewentualnych wycieków informacji, kodu złośliwego i innych zagrożeń dla bezpieczeństwa oraz powszechnie znanych luk w zabezpieczeniach oprogramowania i sprzętu, a także powinny sprawdzać je pod kątem nowych aktualizacji zabezpieczeń.

40. Proces monitorowania bezpieczeństwa powinien również pomagać instytucji finansowej w zrozumieniu charakteru incydentu operacyjnego lub incydentu bezpieczeństwa w celu zidentyfikowania trendów oraz wspierania postępowań wyjaśniających prowadzonych w organizacji.

1.4.6. Przeglądy, ocena i testowanie bezpieczeństwa informacji

41. Instytucje finansowe powinny przeprowadzać szereg przeglądów, ocen i testów bezpieczeństwa informacji, aby zapewnić skuteczne identyfikowanie podatności systemów ICT i usług ICT. Przykładowo instytucje finansowe mogą prowadzić analizę luk względem standardów bezpieczeństwa informacji, przeglądy zgodności, audyty wewnętrzne i zewnętrzne systemów informacji lub przeglądy bezpieczeństwa fizycznego. Co więcej, instytucje powinny rozważać dobre praktyki, takie jak przeglądy kodu źródłowego, ocenę podatności na zagrożenia, testy penetracyjne czy rozwiązania zakładające utworzenie tzw. „zespołu atakującego" wewnątrz organizacji.

42. Instytucje finansowe powinny ustanowić i wdrożyć ramy testowania bezpieczeństwa informacji, które służą potwierdzeniu stabilności i skuteczności środków bezpieczeństwa informacji oraz zapewniają uwzględnienie w tych ramach zagrożeń i podatności stwierdzonych podczas monitorowania zagrożeń oraz w procesie oceny ryzyka związanego z technologiami i bezpieczeństwem ICT.

43. Ramy testowania bezpieczeństwa informacji powinny zapewniać przeprowadzanie testów:

    a) przez niezależnych testerów posiadających dostateczną wiedzę, umiejętności i wiedzę fachową w zakresie środków bezpieczeństwa informacji, niezaangażowanych w rozwój środków bezpieczeństwa informacji;
    b) obejmujących skanowanie podatności i testy penetracyjne (w tym, gdy jest to konieczne i stosowne, testy penetracyjne ukierunkowane na zagrożenie) współmierne względem poziomu ryzyka określonego w procesach i systemach biznesowych.

44. Instytucje finansowe powinny przeprowadzać testy środków bezpieczeństwa na bieżąco i powtarzać je. W odniesieniu do wszystkich krytycznych systemów ICT (ust. 17) testy te należy przeprowadzać co najmniej raz w roku, a w przypadku dostawców usług płatniczych będą one stanowić część kompleksowej oceny ryzyka dla bezpieczeństwa związanego ze świadczonymi usługami płatniczymi, prowadzonej na podstawie art. 95 ust. 2 drugiej dyrektywy w sprawie usług płatniczych. Systemy inne niż krytyczne należy testować regularnie zgodnie z podejściem opartym na ocenie ryzyka, nie rzadziej jednak niż co 3 lata.

45. Instytucje finansowe powinny zapewnić, aby testy środków bezpieczeństwa przeprowadzano w razie zmiany infrastruktury, procesów lub procedur, w razie zmian spowodowanych ważnymi incydentami operacyjnymi lub incydentami bezpieczeństwa lub w razie zmian wynikających z udostępnienia nowych lub znacząco zmienionych krytycznych aplikacji z dostępem do Internetu.

46. Instytucje finansowe powinny monitorować i oceniać wyniki testów bezpieczeństwa i odpowiednio aktualizować stosowane środki bezpieczeństwa bez zbędnej zwłoki w przypadku systemów ICT o krytycznym znaczeniu.

47. W przypadku dostawców usług płatniczych ramy testowania powinny również obejmować środki bezpieczeństwa istotne dla (1) terminali płatniczych i urządzeń wykorzystywanych do świadczenia usług płatniczych, (2) terminali płatniczych i urządzeń wykorzystywanych do uwierzytelniania użytkowników usług płatniczych oraz (3) urządzeń i oprogramowania dostarczanych użytkownikom usług płatniczych przez dostawców usług płatniczych w celu wygenerowania lub otrzymania kodu uwierzytelniającego.

48. Na podstawie stwierdzonych zagrożeń dla bezpieczeństwa i wprowadzonych zmian należy przeprowadzić testy w celu uwzględnienia scenariuszy dotyczących istotnych i znanych potencjalnych ataków.

1.4.7. Szkolenie i świadomość w zakresie bezpieczeństwa informacji

49. Instytucje finansowe powinny opracować program szkoleniowy, w tym okresowe programy zwiększania świadomości na temat bezpieczeństwa, przeznaczone dla wszystkich pracowników i wykonawców, aby mieć pewność, że są oni przeszkoleni do realizacji swoich zadań i obowiązków zgodnie z odpowiednią polityką i procedurami bezpieczeństwa, co ma służyć ograniczeniu błędów ludzkich, kradzieży, oszustw, nadużyć lub strat, a także że wiedzą oni, jak reagować na ryzyko związane z bezpieczeństwem informacji. Instytucje finansowe powinny zapewnić, aby wszyscy członkowie personelu i wykonawcy odbyli takie szkolenie co najmniej raz w roku.

1.5. Zarządzanie operacjami ICT

50. Instytucje finansowe powinny zarządzać własnymi operacjami ICT według udokumentowanych i wdrożonych procesów i procedur (które w przypadku dostawców usług płatniczych obejmują dokument dotyczący strategii w zakresie bezpieczeństwa zgodny art. 5 ust. 1 lit. j) drugiej dyrektywy w sprawie usług płatniczych), które są zatwierdzane przez organ zarządzający. Powyższy zestaw dokumentów powinien określać sposób działania instytucji finansowych, monitorowania i kontrolowania systemów i usług ICT, w tym dokumentowania krytycznych operacji ICT, a także powinien umożliwiać instytucjom finansowym utrzymanie aktualnego spisu zasobów ICT.

51. Instytucje finansowe powinny zapewnić, aby realizacja operacji ICT była dostosowana do wymogów biznesowych. Instytucje finansowe powinny w miarę możliwości utrzymać i doskonalić wydajność operacji ICT, w tym rozważyć, w jaki sposób ograniczyć potencjalne błędy wynikające z realizacji zadań w procesach ręcznego wprowadzania danych.

52. Instytucje finansowe powinny wdrożyć procedury logowania i monitorowania krytycznych operacji ICT, aby umożliwić wykrywanie, analizowanie i korektę błędów.

53. Instytucje finansowe powinny prowadzić zaktualizowany spis swoich zasobów ICT (w tym systemów ICT, urządzeń sieciowych, baz danych itp.). Spis zasobów ICT powinien zawierać konfigurację zasobów ICT oraz powiązania i wzajemne zależności między różnymi zasobami ICT, aby umożliwić właściwą konfigurację i proces zarządzania zmianą.

54. Spis zasobów ICT powinien być dostatecznie szczegółowy, aby możliwa była niezwłoczna identyfikacja zasobu ICT, jego lokalizacji, klasyfikacji bezpieczeństwa oraz osoby odpowiedzialnej. Wzajemne zależności między zasobami powinny być udokumentowane, aby stanowić pomoc przy reagowaniu na incydenty bezpieczeństwa i incydenty operacyjne, w tym cyberataki.

55. Instytucje finansowe powinny monitorować cykle życia zasobów ICT i zarządzać nimi, aby zapewnić dalsze spełnianie i wspieranie wymogów biznesowych i wymogów w zakresie zarządzania ryzykiem. Instytucje finansowe powinny monitorować, czy ich zasoby ICT są wspierane przez zewnętrznych lub wewnętrznych dostawców i programistów oraz czy wszystkie poprawki zabezpieczeń i aktualizacje są stosowane na podstawie udokumentowanych procesów. Należy oceniać i ograniczać ryzyko wynikające z przestarzałych lub nieobsługiwanych zasobów.

56. Instytucje finansowe powinny wdrożyć procesy planowania i monitorowania działalności i zdolności w celu terminowego zapobiegania problemom systemów ICT i niedoborowi zdolności ICT, wykrywania ich oraz reagowania na nie.

57. Instytucje finansowe powinny określić i wdrożyć procedury tworzenia kopii zapasowych i przywracania danych oraz systemów ICT w celu zapewnienia ich możliwie szybkiego odtworzenia. Zakres i częstotliwość tworzenia kopii zapasowych należy ustalić stosownie do wymogów biznesowych w zakresie przywracania danych i systemów oraz krytycznego charakteru danych i systemów ICT oraz oceniać zgodnie z przeprowadzoną oceną ryzyka. Testowanie procedur tworzenia kopii zapasowych oraz przywracania powinno odbywać się okresowo.

58. Instytucje finansowe powinny zapewnić, aby kopie zapasowe danych i systemów ICT były przechowywane w sposób bezpieczny i w dostatecznej odległości od obiektu głównego, aby nie były narażone na to samo ryzyko.

3.5.1 Zarządzanie incydentami ICT i problemami

59. Instytucje finansowe powinny ustanowić i wdrożyć proces zarządzania incydentami i problemami w celu monitorowania i rejestrowania incydentów operacyjnych i incydentów bezpieczeństwa ICT oraz w celu umożliwienia instytucjom finansowym kontynuowania lub wznowienia w sposób terminowy krytycznych funkcji i procesów biznesowych w razie wystąpienia zakłócenia. Instytucje finansowe powinny określić odpowiednie kryteria i progi mające na celu klasyfikację zdarzenia jako incydent operacyjny lub incydent bezpieczeństwa zgodnie z definicją podaną w części „Definicje" w niniejszych wytycznych, jak również powinny określić wskaźniki wczesnego ostrzegania, które mają służyć za ostrzeżenie umożliwiające wczesne wykrywanie tego rodzaju incydentów. Tego rodzaju kryteria i progi w odniesieniu do dostawców usług płatniczych określane są bez uszczerbku dla klasyfikacji poważnych incydentów zgodnie z art. 96 drugiej dyrektywy w sprawie usług płatniczych oraz wytycznych dotyczących zgłaszania poważnych incydentów zgodnie z drugą dyrektywą w sprawie usług płatniczych (EBA/GL/2017/10).

60. Aby ograniczyć do minimum wpływ negatywnych zdarzeń i umożliwić terminowe odtworzenie danych i systemów, instytucje finansowe powinny ustanowić właściwe procesy i struktury organizacyjne w celu zapewnienia spójnego i zintegrowanego monitorowania incydentów operacyjnych i incydentów bezpieczeństwa, postępowania z nimi i prowadzenia działań następczych oraz w celu zidentyfikowania głównej przyczyny i wyeliminowania jej, aby zapobiec ponownemu wystąpieniu incydentów. W procesie zarządzania incydentami i problemami należy określić:

    a) procedury służące identyfikowaniu, śledzeniu, rejestrowaniu, kategoryzowaniu i klasyfikowaniu incydentów według priorytetu na podstawie ich krytycznego znaczenia biznesowego;
    b) role i obowiązki dla różnych scenariuszy incydentu (np. błędy, nieprawidłowe funkcjonowanie, cyberataki);
    c) procedury zarządzania problemami w celu wskazania, zbadania i rozwiązania głównej przyczyny jednego lub wielu incydentów – instytucja finansowa powinna przeanalizować incydenty operacyjne lub incydenty bezpieczeństwa, które mogą prawdopodobnie wpłynąć na instytucję finansową, a które zidentyfikowano lub które wystąpiły w ramach organizacji lub poza nią, a ponadto powinna uwzględnić główne wnioski płynące z takich analiz i odpowiednio zaktualizować środki bezpieczeństwa;
    d) skuteczne plany komunikacji wewnętrznej, w tym procedury zgłaszania incydentów i przekazywania informacji o nich jednostkom wyższego szczebla – również w odniesieniu do skarg klientów związanych z bezpieczeństwem – w celu zapewnienia, aby:
        i) incydenty o potencjalnie dużym niekorzystnym wpływie na krytyczne systemy ICT i usługi ICT były zgłaszane odpowiedniej kadrze kierowniczej wyższego szczebla i kadrze kierowniczej wyższego szczebla ds. ICT;
        ii) organ zarządzający był na bieżąco informowany o znaczących incydentach oraz co najmniej o oddziaływaniu incydentu, reakcji i dodatkowych środkach kontroli ustalonych w następstwie incydentów.

e) procedury reagowania na incydenty, służące ograniczeniu oddziaływania incydentu oraz zapewnieniu terminowego przywrócenia operacyjności i bezpieczeństwa usługi;
f) konkretne plany komunikacji zewnętrznej dla krytycznych funkcji biznesowych i procedur służące:
    i) współpracy z odpowiednimi zainteresowanymi stronami w celu skutecznego reagowania na incydenty i powrotu do stanu sprzed incydentu;
    ii) terminowemu zapewnieniu informacji osobom trzecim (np. klientom, innym uczestnikom rynku, organowi nadzoru) stosownie do potrzeb oraz zgodnie z obowiązującymi przepisami.

1.6. Zarządzanie projektami ICT i zarządzanie zmianą

1.6.1. Zarządzanie projektami ICT

61. Instytucja finansowa powinna wdrożyć proces zarządzania programami lub projektami, w którym określone są role, obowiązki i zakresy odpowiedzialności, w celu skutecznego wspierania realizacji strategii ICT.

62. Instytucja finansowa powinna odpowiednio monitorować i łagodzić ryzyko wynikające z jej portfolio projektów ICT (zarządzanie projektami), uwzględniając również ryzyko, które może wynikać z wzajemnych zależności między różnymi projektami oraz z zależności różnych projektów od tych samych zasobów lub tej samej wiedzy fachowej.

63. Instytucja finansowa powinna ustanowić i wdrożyć politykę zarządzania projektami ICT, która obejmuje co najmniej:

    a) cele projektu;
    b) role i obowiązki;
    c) ocenę ryzyka projektu;
    d) plan projektu, ramy czasowe i kroki;
    e) kluczowe etapy;
    f) wymogi dotyczące zarządzania zmianą.

64. Polityka zarządzania projektami ICT powinna zapewniać analizę wymagań dotyczących bezpieczeństwa informacji oraz podlegać zatwierdzeniu przez funkcję niezależną od funkcji odpowiedzialnej za rozwój.

65. Instytucja finansowa powinna zapewniać, aby wszystkie obszary, na które ma wpływ projekt ICT, były reprezentowane w zespole projektowym, a zespół projektowy posiadał wiedzę wymaganą do zapewnienia bezpiecznej i pomyślnej realizacji projektu.

66. Ustanowienie i postęp projektów ICT oraz powiązanego ryzyka powinno być zgłoszone organowi zarządzającemu, indywidualnie lub zbiorowo, w zależności od znaczenia i rozmiaru projektów ICT, regularnie i na bieżąco, stosownie do potrzeb. Instytucje finansowe powinny uwzględniać w ramach zarządzania ryzykiem ryzyko projektowe.

1.6.2. Nabywanie i rozwój systemów ICT

67. Instytucje finansowe powinny opracować i wdrożyć proces regulujący nabywanie, rozwój i utrzymywanie systemów ICT. Proces ten powinien być zaprojektowany zgodnie z podejściem opartym na ocenie ryzyka.

68. Instytucja finansowa powinna zapewnić, aby przed nabyciem lub rozwojem systemu ICT odpowiednie kierownictwo biznesowe w sposób jasny zdefiniowało i zatwierdziło wymogi funkcjonalne i niefunkcjonalne (w tym wymogi w zakresie bezpieczeństwa informacji).

69. Instytucja finansowa powinna zapewnić, aby istniały środki służące ograniczaniu ryzyka nieumyślnego lub umyślnego manipulowania systemami ICT podczas rozwijania i wdrażania w środowisku produkcji.

70. Instytucje finansowe powinny dysponować metodyką służącą testowaniu i zatwierdzeniu systemów ICT przed pierwszym użyciem. W metodyce tej należy uwzględniać krytyczny charakter procesów biznesowych i zasobów. Testowanie powinno zapewnić zgodne z zamierzeniem działanie nowych systemów ICT. Należy korzystać ze środowisk testowych adekwatnie odzwierciedlających środowisko produkcji.

71. Instytucje finansowe powinny testować systemy ICT, usługi ICT oraz środki bezpieczeństwa informacji w celu zidentyfikowania potencjalnych podatności, naruszeń i incydentów bezpieczeństwa.

72. Instytucja finansowa powinna wdrożyć oddzielne środowiska ICT w celu zapewnienia odpowiedniego podziału obowiązków oraz ograniczenia wpływu niezweryfikowanych zmian na systemy produkcji. W szczególności instytucja finansowa powinna zapewnić oddzielenie środowiska produkcji od środowiska rozwoju, testowania i pozostałych środowisk innych niż środowisko produkcji. Instytucja finansowa powinna zapewnić integralność i poufność danych produkcyjnych w środowiskach innych niż środowisko produkcji. Dostęp do danych dotyczących produkcji jest ograniczony do upoważnionych użytkowników.

73. Instytucje finansowe powinny wdrożyć środki służące ochronie integralności kodów źródłowych systemów ICT rozwijanych wewnątrz organizacji. Powinny również dokumentować rozwój, wdrażanie, obsługę lub konfigurację systemów ICT w sposób kompleksowy, aby ograniczyć niepotrzebną zależność od ekspertów merytorycznych. Dokumentacja systemu ICT powinna w stosownych przypadkach obejmować co najmniej dokumentację użytkownika, dokumentację techniczną systemu oraz procedury operacyjne.

74. Procesy instytucji finansowej w zakresie nabywania i rozwijania systemów ICT powinny mieć zastosowanie również do systemów ICT rozwijanych lub zarządzanych przez użytkowników końcowych funkcji biznesowej spoza organizacji ICT (np. aplikacje komputerowe użytkowników końcowych), zgodnie z podejściem opartym na ocenie ryzyka. Instytucja finansowa powinna prowadzić rejestr tych aplikacji, które wspierają krytyczne funkcje lub procesy biznesowe.

1.6.3. Zarządzanie zmianą ICT

75. Instytucje finansowe powinny ustanowić i wdrożyć proces zarządzania zmianą ICT w celu zapewnienia, aby wszystkie zmiany systemów ICT były rejestrowane, testowane, oceniane, zatwierdzane, wdrażane i weryfikowane w sposób kontrolowany. Instytucje finansowe powinny uwzględniać zmiany w czasie sytuacji awaryjnych (tj. zmiany, które muszą być wprowadzone możliwie szybko) zgodnie z procedurami zapewniającymi odpowiednie zabezpieczenia.

76. Instytucje finansowe powinny określić, czy zmiany w istniejącym środowisku operacyjnym mają wpływ na istniejące środki bezpieczeństwa lub wymagają podjęcia dodatkowych działań mających na celu ograniczenie danego ryzyka. Zmiany te powinny być zgodne z formalnym procesem zarządzania zmianą w instytucji finansowej.

1.7. Zarządzanie ciągłością działania

77. Instytucje finansowe powinny ustanowić rozsądny proces zarządzania ciągłością działania w celu osiągnięcia maksymalnego stopnia zdolności świadczenia usług na bieżąco oraz ograniczenia strat w razie poważnego zakłócenia działalności zgodnie z art. 85 ust. 2 dyrektywy 2013/36/UE oraz tytułem VI wytycznych EUNB w sprawie zarządzania wewnętrznego (EBA/GL/2017/11).

1.7.1. Analiza wpływu na działalność

78. W ramach rozsądnego zarządzania ciągłością działania instytucje finansowe powinny prowadzić analizę wpływu na działalność, analizując swoje narażenie na poważne zakłócenia działalności oraz oceniając potencjalne oddziaływanie (w tym wpływ na poufność, integralność i dostępność) w wymiarze ilościowym i jakościowym, z wykorzystaniem danych wewnętrznych lub zewnętrznych (np. danych dostawców zewnętrznych istotnych dla procesu biznesowego lub publicznie dostępnych danych, które mogą być istotne dla analizy wpływu na działalność) oraz analizy scenariuszy. Analiza wpływu na działalność powinna uwzględniać również krytyczny charakter zidentyfikowanych i sklasyfikowanych funkcji biznesowych, procesów pomocniczych, zasobów stron trzecich i zasobów informacyjnych, a także zależności między nimi, zgodnie z rozdziałem 1.3.3.

79. Instytucje finansowe powinny zapewnić, aby ich systemy ICT i usługi ICT były zaprojektowane i dostosowane do analizy wpływu na działalność, przykładowo poprzez powielenie pewnych krytycznych komponentów w celu zapobieżenia zakłóceniom powodowanym przez zdarzenia wpływające na te komponenty.

1.7.2. Plany ciągłości działania

80. Na podstawie analizy wpływu na działalność instytucje finansowe powinny ustanowić plany służące zapewnieniu ciągłości działania (tzw. plany ciągłości działania), które powinny być udokumentowane i zatwierdzone przez organy zarządzające. Plany te powinny uwzględniać w szczególności rodzaje ryzyka, które mogą wpływać negatywnie na systemy ICT i usługi ICT. Plany

te powinny wspierać realizację celów w zakresie ochrony oraz, w razie potrzeby, przywrócenia poufności, integralności i dostępności ich funkcji biznesowych, procesów pomocniczych i zasobów informacyjnych. Instytucje finansowe w trakcie ustanawiania tych planów powinny koordynować własne działania z odpowiednimi zainteresowanymi stronami, wewnętrznymi i zewnętrznymi, stosownie do potrzeb.

81. Instytucje finansowe powinny dysponować planami ciągłości działania w celu zapewnienia odpowiedniej reakcji na potencjalne scenariusze awarii i być zdolne do przywrócenia operacji krytycznej działalności biznesowej po zakłóceniach z zachowaniem zakładanego czasu wznowienia funkcji (RTO; będącego maksymalnym czasem od incydentu, w którym należy przywrócić system lub proces) oraz akceptowalnego poziomu utraty danych (RPO; będącego maksymalnym akceptowalnym okresem, w którym może dojść do utraty danych w razie incydentu). Na wypadek poważnego zakłócenia działalności, które spowoduje uruchomienie określonych planów ciągłości działania, instytucje finansowe powinny ustalić priorytety kroków na rzecz ciągłości działania, stosując podejście oparte na ocenie ryzyka, mogąc opierać się przy tym na ocenach ryzyka dokonanych zgodnie z rozdziałem 1.3.3. W przypadku dostawców usług płatniczych może to obejmować przykładowo ułatwianie dalszej realizacji transakcji krytycznych przy jednoczesnym kontynuowaniu działań naprawczych.

82. Instytucja finansowa powinna w swoim planie ciągłości działalności rozważyć szereg różnych scenariuszy, na które może być narażona, w tym skrajnych, ale prawdopodobnych, w tym scenariusze związane z cyberatakami, a także ocenić potencjalny wpływ takich scenariuszy. Na podstawie tych scenariuszy instytucja finansowa powinna opisać, w jaki sposób zapewniana jest ciągłość systemów ICT i usług, a także bezpieczeństwo informacji instytucji finansowej.

1.7.3. Plany reagowania i odtworzenia systemów i usług

83. Na podstawie analizy wpływu na działalność (ust. 78) oraz prawdopodobnych scenariuszy (ust. 82) instytucje finansowe powinny opracować plany reagowania i odtworzenia systemów i usług. Plany te powinny określać, jakie warunki mogą wywołać uruchomienie planów i jakie działania należy podjąć w celu zapewnienia dostępności, ciągłości i odtworzenia co najmniej krytycznych systemów ICT i usług ICT instytucji finansowych. Plany reagowania i odtworzenia systemów i usług powinny służyć spełnieniu celu odtworzenia operacji instytucji finansowych.

84. Plany reagowania i odtworzenia systemów i usług powinny obejmować zarówno opcje odtworzenia krótkoterminowego, jak i długoterminowego. Plany powinny:

    a) koncentrować się na przywróceniu operacji krytycznych funkcji biznesowych, procesów pomocniczych, zasobów informacyjnych oraz zależności między nimi w celu uniknięcia niekorzystnych skutków dla funkcjonowania instytucji finansowych i dla systemu finansowego, w tym dla systemów płatniczych i użytkowników usług płatniczych, jak również w celu zapewnienia realizacji bieżących transakcji płatności;
    b) być dokumentowane i udostępniane jednostkom biznesowym i wspomagającym oraz być łatwo dostępne w sytuacji awaryjnej;

c) być aktualizowane zgodnie z wnioskami wyciągniętymi z incydentów, testów, zgodnie ze zidentyfikowanymi nowymi rodzajami ryzyka i zagrożeniami oraz zmienionymi celami i priorytetami odtworzenia systemów i usług.

85. Plany powinny też uwzględniać opcje alternatywne, na wypadek sytuacji gdy odtworzenie może nie być wykonalne w perspektywie krótkoterminowej ze względu na koszty, ryzyko, logistykę lub nieprzewidziane okoliczności.

86. Co więcej, w ramach planów reagowania i odtworzenia systemów i usług instytucja finansowa powinna rozważyć i wdrożyć środki na rzecz ciągłości, aby ograniczyć skutki uchybień dostawców zewnętrznych, które mają zasadnicze znaczenie dla ciągłości usług ICT instytucji finansowej (stosownie do zapisów na temat planów ciągłości działań zawartych w wytycznych EUNB w sprawie outsourcingu (EBA/GL/2019/02)).

1.7.4. Testowanie planów

87. Instytucje finansowe powinny okresowo testować własne plany ciągłości działania. W szczególności powinny zapewnić, aby plany ciągłości działania dotyczące ich krytycznych funkcji biznesowych, procesów pomocniczych, zasobów informacyjnych i zależności między nimi (włączając w to w stosownych przypadkach funkcje, procesy i zasoby zapewniane przez osoby trzecie) były testowane co najmniej raz w roku, zgodnie z ust. 89.

88. Plany ciągłości działania powinny być aktualizowane co najmniej raz do roku na podstawie wyników testów, aktualnej wiedzy o zagrożeniach oraz wniosków wyciągniętych z wcześniejszych zdarzeń. Wszelkie zmiany celów dotyczących odtworzenia systemów i usług (w tym celów zakładanego czasu wznowienia funkcji, jak i dopuszczalnego poziomu utraty danych) lub zmiany w funkcjach biznesowych, procesach pomocniczych i zasobach informacyjnych powinny być w stosownych przypadkach uznawane za podstawę do aktualizacji planów ciągłości działania.

89. W wyniku przeprowadzanych przez instytucje finansowe testów planów ciągłości działania należy wykazać, że plany te zapewniają podtrzymanie działalności do czasu przywrócenia krytycznych operacji. W szczególności powinny one:

a) obejmować testowanie odpowiedniego zestawu poważnych, ale prawdopodobnych scenariuszy, w tym scenariuszy branych pod uwagę przy opracowywaniu planów ciągłości działania (jak również, w stosownych przypadkach, testowanie usług świadczonych przez osoby trzecie); powinno to obejmować przekierowanie krytycznych funkcji biznesowych, procesów pomocniczych i zasobów informacyjnych na środowisko przywracania gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej oraz wykazanie, że mogą one być prowadzone w ten sposób przez wystarczająco reprezentatywny okres oraz że normalne funkcjonowanie może zostać przywrócone później;
b) być zaplanowane w taki sposób, aby sprawdzić założenia, na których opierają się plany ciągłości działania, w tym zasady zarządzania i plany komunikacji kryzysowej; oraz

c) obejmować procedury służące weryfikacji możliwości odpowiedniego reagowania przez personel i wykonawców, systemy ICT i usługi ICT na scenariusze określone w ust. 89 lit. a).

90. Wyniki testów powinny być udokumentowane, a wszelkie stwierdzone niedociągnięcia ujawnione w testach należy przeanalizować, ustosunkować się do nich i zgłosić organowi zarządzającemu.

1.7.5. Komunikacja kryzysowa

91. W przypadku zakłócenia lub sytuacji awaryjnej oraz w czasie wdrażania planów ciągłości działania instytucje finansowe powinny zapewnić skuteczne środki komunikacji kryzysowej, aby wszystkie właściwe zainteresowane podmioty wewnętrzne i zewnętrzne, w tym – o ile wymagają tego przepisy krajowe – właściwe organy, jak również stosowni dostawcy usług (dostawcy usług objętych outsourcingiem, podmioty należące do tej samej grupy lub dostawcy zewnętrzni) otrzymywali informacje terminowo i w odpowiedni sposób.

1.8. Zarządzanie relacjami z użytkownikami usług płatniczych

92. Dostawcy usług płatniczych powinni opracować i wdrożyć procesy mające na celu zwiększenie świadomości użytkowników usług płatniczych w zakresie zagrożeń dla bezpieczeństwa związanych z usługami płatniczymi poprzez udzielanie użytkownikom usług płatniczych wsparcia i porad.

93. Wsparcie i porady oferowane użytkownikom usług płatniczych powinny być aktualizowane w świetle nowych zagrożeń i podatności, a użytkownicy usług płatniczych powinni być informowani o wszelkich zmianach.

94. Jeżeli funkcjonalność produktu na to pozwala, dostawcy usług płatniczych powinni umożliwić użytkownikom usług płatniczych wyłączenie określonych funkcji płatniczych związanych z usługami płatniczymi świadczonymi przez dostawców usług płatniczych na rzecz użytkowników usług płatniczych.

95. Jeśli zgodnie z art. 68 ust. 1 dyrektywy (UE) 2015/2366 dostawca usług płatniczych uzgodnił z płatnikiem limity wydatków dla transakcji płatniczych wykonywanych za pomocą określonych instrumentów płatniczych, dostawca usług płatniczych powinien zapewnić płatnikowi możliwość dostosowania tych limitów do maksymalnego ustalonego limitu.

96. Dostawcy usług płatniczych powinni zapewnić użytkownikom usług płatniczych możliwość otrzymywania powiadomień dotyczących podjętych lub nieudanych prób wykonania transakcji płatniczych w celu umożliwienia im wykrywania przypadków użycia ich kont w sposób nielegalny lub w celach przestępczych.

97. Dostawcy usług płatniczych powinni na bieżąco informować użytkowników usług płatniczych o procedurach bezpieczeństwa mających wpływ na użytkowników usług płatniczych w zakresie świadczenia usług płatniczych.

98. Dostawcy usług płatniczych powinni udzielić wsparcia użytkownikom usług płatniczych w przypadku wszelkich pytań, wniosków o udzielenie wsparcia, powiadomień o nieprawidłowościach lub kwestii bezpieczeństwa związanych z usługami płatniczymi. Użytkownikom usług płatniczych należy zapewnić stosowne informacje o sposobie, w jaki można uzyskać takie wsparcie.