WSPARCIE REALIZACJI AUDYTU PLANÓW CIĄGŁOŚCI ŚWIADCZENIA USŁUG PUBLICZNYCH W POLSCE

Najlepsze praktyki dla funkcji audytu wewnętrznego

Funded by the European Union

OECD
BETTER POLICIES FOR BETTER LIVES

Ministry of Finance
Republic of Poland

Niniejszy dokument został opracowany przy wsparciu finansowym Unii Europejskiej. Opinii wyrażonych w niniejszym dokumencie w żaden sposób nie można traktować jako oficjalnego stanowiska Unii Europejskiej.

Projekt został sfinansowany przez Unię Europejską za pośrednictwem Instrumentu Wsparcia Technicznego i wdrożony przez OECD we współpracy z Komisją Europejską.

Niniejsze tłumaczenie zostało zlecone przez Dyrekcję ds. Zarządzania Publicznego i OECD nie może zagwarantować jego dokładności. Jedynymi oficjalnymi wersjami są teksty w języku angielskim i/lub francuskim.

Projekt okładki autorstwa Meral Gedik z wykorzystaniem zdjęcia z © Lukasz Pawel Szczepanski/Shutterstock.com.

Informacje o niniejszym dokumencie

Kryzys związany z pandemią COVID-19 uwypuklił kilka obszarów, w których rządy muszą poprawić sposób zarządzania kryzysami i zdarzeniami nadzwyczajnymi, w tym wyzwania wpływające na świadczenie krytycznych usług publicznych. Część z tych wyzwań obejmowała te związane z cyfryzacją.

Niniejszy dokument ma na celu przekazanie informacji i wspieranie wszystkich osób przeprowadzających audyty wewnętrzne w sektorze publicznym w Polsce, pracujących w ramach funkcji audytu wewnętrznego i wszystkich innych funkcji wykonujących czynności związane z audytem lub zapewnieniem, bezpośrednio lub pośrednio. Opisuje kontekst związany z audytem planów ciągłości świadczenia usług publicznych wraz z implikacjami i doświadczeniami związanymi z cyfryzacją usług publicznych. Ważne jest, aby wziąć pod uwagę wszystkie aspekty cyfryzacji, aby zapewnić, że plany ciągłości działania pozostaną adekwatne i aktualne.

W niniejszych wytycznych omówiono elementy planu ciągłości działania i wyszczególniono aspekty audytu efektywności w obszarze cyfryzacji w odniesieniu do następujących tematów: wybór rodzaju audytu, zasoby, cele, zakres, ocena ryzyka, kryteria, zaangażowanie interesariuszy, zalecenia dotyczące zawartości listy kontrolnej i niezbędnych kompetencji wspierających audytorów. Przyczyni się to do zwiększenia gotowości funkcji audytu wewnętrznego do realizacji zadań w tym obszarze na wszystkich szczeblach administracji publicznej w Polsce. Jest to przewodnik dla osób zajmujących się zapewnianiem, że zarządzanie przez organizację procesami ciągłości i związanymi z nimi ryzykami jest skuteczne i zgodne z celami organizacji. Pomoże to organizacjom lepiej przygotować się na wypadek sytuacji wyjątkowych lub zdarzeń nadzwyczajnych.

Niniejsze wytyczne opisują międzynarodowe regulacje związane z ciągłością oraz elementy standardów. Elementy te obejmują: kontekst organizacji, przywództwo, planowanie, wsparcie, działanie, ocenę wyników i doskonalenie. Wytyczne opisują również politykę zarządzania ciągłością działania w polskim Ministerstwie Finansów i związaną z tym odpowiedzialność.

Wytyczne zawierają międzynarodowe przykłady dobrych praktyk, w tym zagadnienia związane z ciągłością działania, takie jak: zestawy narzędzi, strategie i kroki mające na celu opracowanie odpowiedniego planu awaryjnego. Zawierają również odpowiednie przykłady audytu planowania ciągłości działania, w tym przykłady celów, zakresu, kryteriów i odpowiednich zaleceń. Przykłady te zawierają wskazówki dotyczące struktury i języka, które można wykorzystać przy opracowywaniu podobnego rodzaju audytu dotyczącego planowania ciągłości działania.

OECD pragnie wyrazić uznanie dla polskiego Ministerstwa Finansów za wsparcie w opracowaniu niniejszych wytycznych w ramach Instrumentu Wsparcia Technicznego.

Spis treści

1 Wprowadzenie

Instytut Audytorów Wewnętrznych (IIA) definiuje audyt wewnętrzny jako „niezależną i obiektywną działalność zapewniającą i doradczą, której celem jest przysparzanie wartości i usprawnienie działalności operacyjnej organizacji. Pomaga organizacji osiągnąć cele poprzez systematyczną i dokonywaną w uporządkowany sposób ocenę ładu organizacyjnego, zarządzania ryzykiem i procesów kontroli oraz przyczynia się do poprawy ich działania". W ramach całego globalnego sektora publicznego istnieją różne rodzaje audytów, które są przeprowadzane w różnych celach. (IIA, 2024[1])

Kryzys związany z pandemią COVID-19 podniósł znaczenie sposobu, w jaki rządy zarządzają kryzysami. Wywołał niepewność we wszystkich sektorach na całym świecie, zwłaszcza w sektorze publicznym. Była to sytuacja szczególnie skomplikowana, ponieważ należało zapewnić świadczenie krytycznych usług publicznych, podczas gdy większość urzędników państwowych została zmuszona do zmiany charakteru świadczenia swojej pracy na zdalny i wirtualny w ciągu kilku tygodni. Wymagało to od wszystkich podmiotów publicznych odpowiedniego planowania ciągłości działania. Co więcej, ogromny wzrost cyfryzacji i popularności pracy zdalnej, przy jednoczesnej konieczności utrzymania świadczenia usług publicznych, spowodował powstanie wielu nowych zagrożeń. Komórki audytu wewnętrznego były wykorzystywane na wiele sposobów przez różne rządy na całym świecie. Działalność niektórych komórek audytu wewnętrznego miała istotne znaczenie w wielu rolach związanych z kryzysem, podczas gdy inne kontynuowały swoje zwykłe czynności operacyjne.

Zakres audytu

Czym jest plan ciągłości działania?

Ciągłość działania odnosi się do zdolności organizacji do kontynuowania dostarczania produktów lub usług z wcześniej określoną wydajnością w akceptowalnych ramach czasowych w przypadku występowania zakłóceń. Plan ciągłości działania (BCP) to udokumentowany przewodnik, który pomaga organizacji reagować na zakłócenia oraz wznawiać, odzyskiwać i przywracać świadczenie usług.

Z szerszej perspektywy, plan ciągłości działania można postrzegać jako proces budowania systemu zarządzania ciągłością działania (BCMS) i jego wyników. System zarządzania ciągłością działania ma na celu zarządzanie zdolnością organizacji do kontynuowania działalności w przypadku występowania zakłóceń. Wspiera on cele strategiczne, poprawia reputację i zwiększa niezawodność. System zarządzania ciągłością działania buduje zaufanie wśród partnerów biznesowych i zmniejsza zarówno ryzyko prawne, jak i finansowe, a także koszty związane z zakłóceniami. Uwzględnia również oczekiwania odpowiednich stron, zabezpiecza życie i mienie, chroni środowisko i zwiększa skuteczność organizacji w przypadku występowania zakłóceń poprzez proaktywne zarządzanie ryzykiem (ISO, 2019[2]). System zarządzania ciągłością działania powinien obejmować następujące elementy:

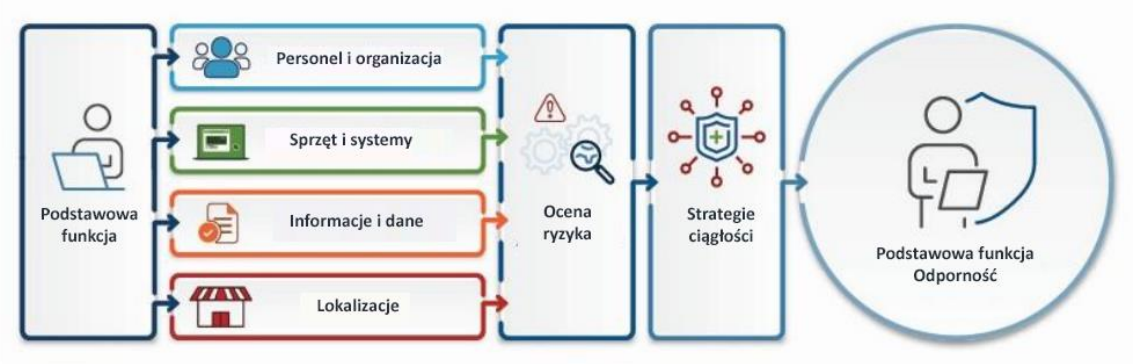
- politykę;
- kompetentne osoby o określonych odpowiedzialnościach;
- procesy zarządzania związane z:
  - polityką,

- planowaniem,
- wdrożeniem i obsługą,
- oceną działalności,
- przeglądem zarządzania,
- ciągłym doskonaleniem;

- udokumentowanymi informacjami wspierającymi kontrolę operacyjną i umożliwiającymi ocenę działalności.

Rysunek 1.1 przedstawia przykład ogólnego procesu modelu planu ciągłości działania w ramach rządu federalnego USA. Organizacje muszą najpierw zidentyfikować swoje podstawowe funkcje. Następnie określają czynniki planowania niezbędne do realizacji tych funkcji, przeprowadzają oceny ryzyka dla każdego czynnika planowania, a na koniec identyfikują i wdrażają strategie ciągłości w celu uwzględnienia obszarów o największej podatności na zagrożenia.

Rysunek 1.1. Ramy planowania ciągłości działania w rządzie federalnym USA



Źródło: (FEMA, 2023[3]).

Znaczenie planu ciągłości działania w sektorze publicznym

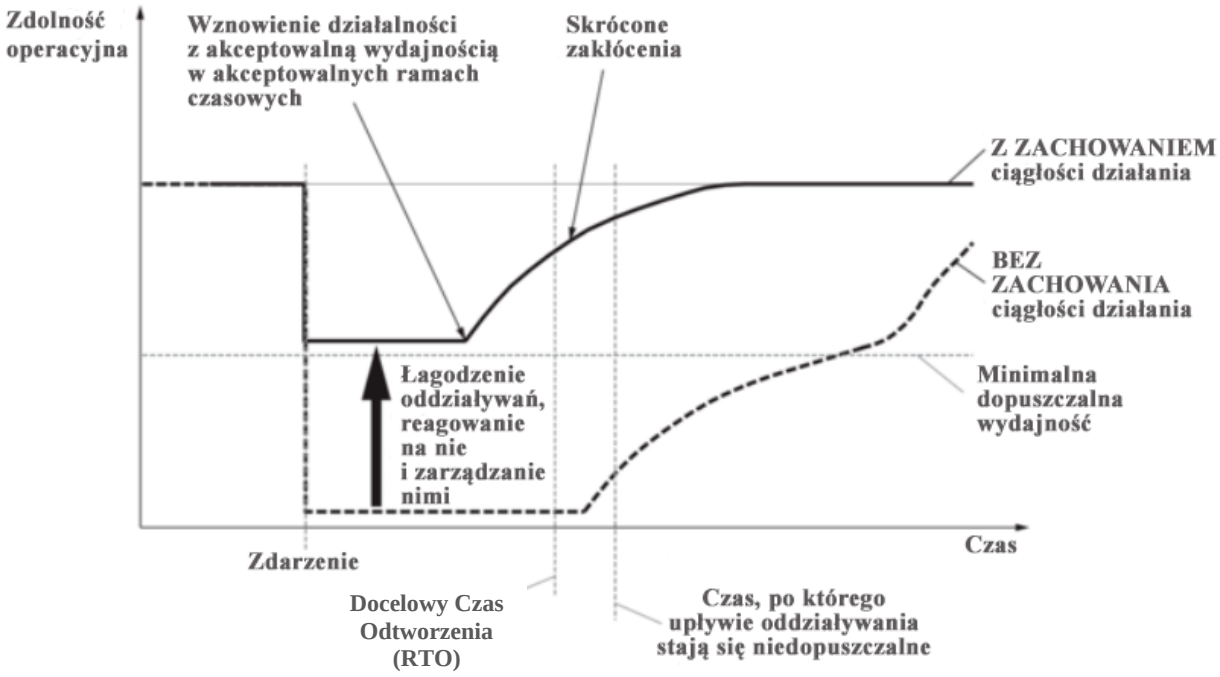
Zagrożenia krytyczne mogą rozwijać się szybko i rozprzestrzeniać w sposób nieprzewidywalny przekraczając granice różnych krajów. Ryzyka te mogą mieć znaczący wpływ na cały kraj, zakłócać funkcjonowanie podstawowej infrastruktury, szkodzić kluczowym zasobom środowiskowym, obciążać finanse publiczne i zmniejszać zaufanie publiczne do rządu. Skuteczne zarządzanie ryzykiem może pomóc w utrzymaniu lub zwiększeniu przewagi konkurencyjnej danego kraju. Ma to kluczowe znaczenie w obliczu niepewności związanej z geopolityką, środowiskiem, społeczeństwem i gospodarką (OECD, 2014[4]). Zapewnienie ciągłości świadczenia podstawowych usług publicznych w czasach kryzysu ma kluczowe znaczenie dla dobrobytu i bezpieczeństwa obywateli oraz znacząco wpływa na proces wznowienia funkcjonowania.

W obliczu zakłóceń w rutynowej działalności organizacje muszą zapewnić ciągłość działania istotnych funkcji. Zakłócenia te często prowadzą do ograniczenia zasobów, aktywów i możliwości. W takich scenariuszach nacisk kładziony jest na utrzymanie najistotniejszej działalności z niewielkim lub zerowym marginesem na przestoje, podczas gdy działania, które można odłożyć, są wstrzymywane. Kluczowe dla organizacji jest przeanalizowanie swoich działań operacyjnych w celu określenia, które zadania muszą być kontynuowane bez zakłóceń, a które można zminimalizować, opóźnić lub odłożyć na bok. Ustalanie priorytetowych zasobów w potencjalnie ograniczonej liczbie scenariuszy wymaga zrozumienia potrzeb organizacji w zakresie personelu, sprzętu, systemów, informacji, danych i lokalizacji w celu wypełnienia jej misji. Analizując podatność każdego czynnika planowania na szeroki wachlarz zagrożeń

i niebezpieczeństw, organizacje mogą lepiej zrozumieć ogólne ryzyko, na jakie narażona jest każda istotna funkcja. Alokacja personelu, sprzętu, danych i lokalizacji jest jedną z wielu strategii, które mogą pomóc zmniejszyć ryzyko i zapewnić, że organizacje będą nadal wykonywać swoje podstawowe funkcje przy minimalnym lub zerowym przestoju (FEMA Office of National Continuity Programs, 2023[5]).

Rysunek 1.2 pokazuje, w jaki sposób ciągłość działania może być skuteczna w łagodzeniu skutków w niektórych sytuacjach.

Rysunek 1.2. Ilustracja skuteczności ciągłości działania w przypadku nagłych zakłóceń



Źródło: (ISO, 2019[2]).

Nowoczesne strategie zarządzania ciągłością działania są ściśle powiązane z cyfryzacją administracji. W miarę jak zadania administracyjne stają się coraz bardziej cyfrowe, bezpieczeństwo i zdolność adaptacji użytkowanych systemów znacząco wpływają na ciągłość działania. Cyfryzacja stwarza również możliwości wzmocnienia ciągłości działania w sytuacjach kryzysowych. Na przykład podczas pandemii COVID-19 przyjęcie rozwiązania pracy zdalnej i zadań administracji cyfrowej w sektorach, takich jak: podatki, architektura i udzielanie zamówień publicznych pomogło utrzymać podstawowe funkcje administracyjne. Oznacza to, że podczas audytu planu ciągłości działania kluczowe jest pytanie: „Czy cyfrowe funkcje administracji mogą być odpowiednio wykonywane w sytuacji kryzysowej?” oraz „Czy kierownictwo i pracownicy są przygotowani na te zmiany (wywołane sytuacją kryzysową)?”.

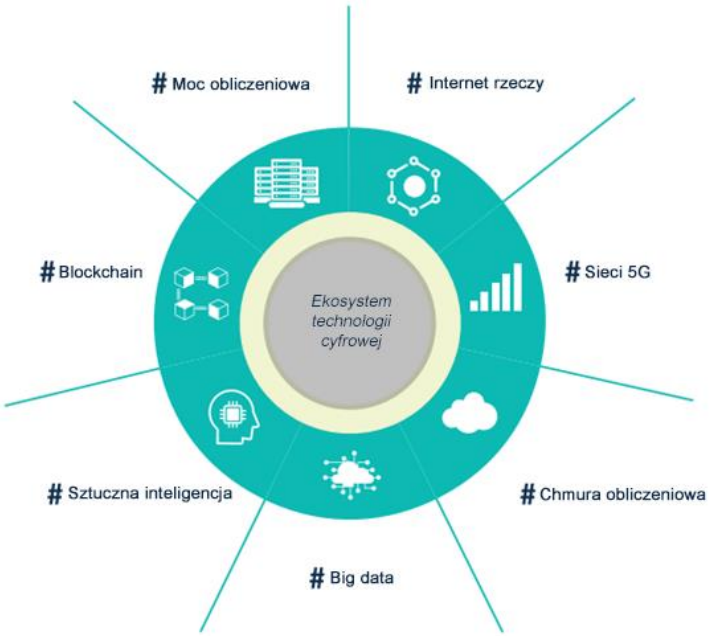
Doświadczenia związane z pandemią COVID-19 pokazały, że szybkość reakcji i jakość ciągłości świadczenia usług publicznych w sytuacji kryzysowej może mieć ogromny wpływ na życie obywateli. Pandemia COVID-19 stanowiła poważne wyzwanie dla ciągłości świadczenia usług publicznych. Na przykład, gdy instytucje edukacyjne zostały nagle zamknięte z powodu lockdownów, nauczyciele szybko przeszli na zdalne nauczanie za pośrednictwem platform internetowych i materiałów cyfrowych, wszędzie tam, gdzie pozwalała na to infrastruktura (UN, 2020[6]). Pomimo tych reakcji, znacznie pogłębiła się luka edukacyjna podczas zakłóceń spowodowanych przez COVID-19, a ogólne osiągnięcia akademickie spadły w krajach OECD w latach 2018-2022, jak wynika z Programu Międzynarodowej

Oceny Umiejętności Uczniów OECD (OECD, 2024[7]) (Kuhfeld et al., 2022[8]). Ten przykład pokazuje, jak ważne jest utrzymanie w jak największym stopniu ciągłości i jakości usług publicznych.

Transformacja cyfrowa

Digitalizacja to dostosowanie analogowych danych i procesów do formatu nadającego się do odczytu maszynowego. Cyfryzacja to wykorzystanie technologii cyfrowych, co skutkuje nowymi działaniami lub modyfikacjami istniejących działań. Transformacja cyfrowa powszechnie dotyczy ekonomicznych i społecznych skutków cyfryzacji i digitalizacji. Aby opracować politykę dla ery cyfrowej, kluczowe znaczenie ma świadomość głównych elementów ewoluującego ekosystemu technologii cyfrowej oraz wszelkich możliwości (i wyzwań) wynikających z ich zastosowania. Ponadto niezbędne jest zrozumienie toczącej się rewolucji informatycznej oraz tego, w jaki sposób dane i ich przepływy wpływają na jednostki, gospodarkę i społeczeństwo w szerszym ujęciu. Wreszcie, ważne jest, aby zidentyfikować kluczowe cechy transformacji cyfrowej, w tym sposób, w jaki napędzają one nowe i ewoluujące modele biznesowe oraz jakie mogą być ich konsekwencje dla polityki publicznej (OECD, 2019[9]). Zobacz infografikę 1.1, aby zapoznać się z aspektami ekosystemu technologii cyfrowej.

Infografika 1.1. Ekosystem technologii cyfrowej



Na początku pandemii COVID-19 zarówno decydenci polityczni, jak i naukowcy spodziewali się, że pandemia i wynikające z niej polityki ograniczania rozprzestrzeniania się koronawirusa przyspieszą cyfryzację, co może mieć istotne konsekwencje dla rynków pracy i produktywności. Wielu pracowników musiało przestawić się z pracy w biurze na pracę w domu, a działalność gospodarcza wymagająca kontaktu została ograniczona. W rezultacie wiele firm musiało dostosować się do pracy zdalnej i poszerzyć swoją działalność o tryb online, co wymagało zmian w działalności operacyjnej, logistyce i prawdopodobnie szybkich inwestycji w technologie informacyjno-komunikacyjne (ICT). Podczas pandemii COVID-19 te formy cyfryzacji, które pozwoliły firmom działać zdalnie, mogły wspierać zatrudnienie i wydajność pracy, a także istniała nadzieja, że w dłuższej perspektywie zwiększą produktywność firm i pracowników. Z kolei oczekiwania dotyczące długoterminowego wpływu na rynek

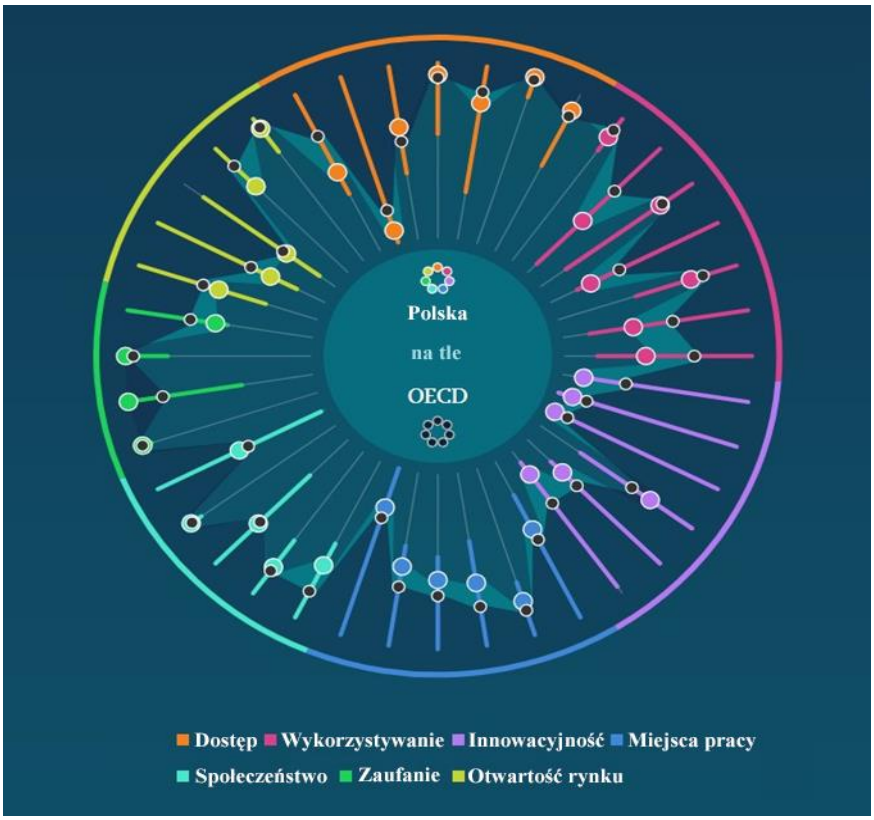
pracy były bardziej zróżnicowane, włącznie z obawami, że cyfryzacja może wyprzeć rzesze pracowników o niskich i średnich kwalifikacjach.

Chociaż możliwe są kolejne naturalne pandemie, w przyszłości mogą wystąpić inne potencjalne zakłócenia, które mogą mieć wpływ na otoczenie, w którym działa jednostka. Możliwe zakłócenia mogą obejmować:

- Zaprojektowane pandemie: istnienie inżynierii genetycznej i bioinżynierii stwarza ryzyko najbardziej niszczycielskich pandemii w historii ludzkości. Ponieważ ich celem jest spowodowanie śmiertelności, mają one znaczący wpływ na społeczeństwo.
- Syndrom Kesslera: nadzwyczajna liczba satelitów krążących wokół Ziemi nadal generuje możliwości technologiczne i ekonomiczne. Jednocześnie zwiększa to ryzyko kolizji, a ich reakcja łańcuchowa (znana również jako Syndrom Kesslera) może potencjalnie zniszczyć światowe systemy komunikacyjne i cofnąć wiele lat postępu.
- Sztuczna inteligencja rozwijająca się w sposób niezależny, niezrównoważony: przyspieszony rozwój technologii popycha społeczeństwo do rozwoju superinteligencji. W miarę jak uczenie maszynowe i sztuczna inteligencja zmniejszają ilość ludzkiego wkładu niezbędnego do funkcjonowania społeczeństwa, maszyny będą odpowiedzialne za wykonywanie nowych zadań. Jeśli nauka i samodoskonalenie (sztucznej inteligencji) przekroczą dopuszczalne granice, istnieje ryzyko, że ludzkość straci kontrolę nad swoim rozwojem (OECD, 2021[10]).

OECD opracowała zestaw narzędzi *Going Digital Toolkit,* który opiera się na siedmiu wymiarach ram zintegrowanej polityki cyfryzacji *Going Digital*, obejmujących różne obszary polityki, aby pomóc w zapewnieniu, że podejście do realizacji obietnicy transformacji cyfrowej „dla wszystkich" obejmuje całą gospodarkę i społeczeństwo. Infografika 1.2 przedstawia obecną sytuację w Polsce na tle innych krajów OECD.

Infografika 1.2. Wskaźniki cyfryzacji *Going Digital* OECD – Polska na tle krajów OECD



Źródło: (OECD, 2024[11]).

Cyfryzacja w sektorze publicznym po pandemii

Temat cyfryzacji oraz tego, w jaki sposób rządy nieustannie przechodzą transformację i zarządzają nią, jest integralny w kontekście planowania ciągłości działania. W związku z tym audytorzy muszą zrozumieć jej znaczenie, a w szczególności sposób, w jaki powstała i rozwinęła się w ostatnich latach.

Cyfryzacja i transformacja powodują odejście od *status quo* i wymagają od rządów innowacji. Są również szansą pozwalającą na poprawę zdolności do reakcji, odpowiedzialności, sprawności i wydajności. Rządy muszą zaakceptować tę zmianę i wspierać kulturę innowacji, aby ułatwić pracownikom i organizacjom eksperymentowanie, uczenie się i rozwój. Ponieważ kultura sektora publicznego będzie ewoluować wraz ze zmieniającymi się potrzebami, rosnącą elastycznością i produktywnością, wszystkie zainteresowane strony muszą być świadome stale zmieniających się zagrożeń.

Ponieważ cyfryzacja wiąże się z bazowaniem na danych, rządy będą dążyć do optymalizacji danych poprzez ulepszanie i rozwijanie podejść do gromadzenia, zestawiania, analizy i rozpowszechniania danych. Wykorzystywanie i udostępnianie danych obejmuje zarówno sektor publiczny, jak i prywatny. Rząd odgrywa rolę w zapewnianiu dostępności, użyteczności i możliwości działania na różnych szczeblach administracji rządowej. W tym kontekście dane powinny być odpowiednio zabezpieczone i chronione. Audytorzy mogą odegrać w tym rolę, zapewniając, że wraz z tym, jak dane stają się publicznie dostępne, istnieją odpowiednie mechanizmy kontroli w celu ich zabezpieczenia.

Pandemia COVID-19 pokazała, że rządy nie były przygotowane do radzenia sobie z kryzysem na różne sposoby. Od tego czasu stała się ona jednak katalizatorem rozpoczęcia cyfrowej transformacji w celu

zbudowania zrównoważonego i silnego cyfrowo społeczeństwa. Pandemia dała rządom możliwość odegrania kluczowej roli w pokonywaniu przeszkód społecznych. Technologie cyfrowe zostały wykorzystane do reagowania na kryzysy w perspektywie krótkoterminowej, a także, w idealnym przypadku, do ożywienia polityki i innych narzędzi w perspektywie długoterminowej.

Wprowadzenie nowych technologii odegrało ważną rolę w wysiłkach rządu mających na celu koordynację reakcji na COVID-19, zapewniając funkcjonowanie społeczeństwa podczas lockdownów i odkrywanie rozwiązań w różnych sektorach. W okresie po zakończeniu reagowania kryzysowego rządy nadal pracują nad przywracaniem funkcjonalności i odbudową.

Podczas pandemii rządy wdrożyły inicjatywy i przyjęły polityki mające na celu polepszenie ogólnej łączności. Taki scenariusz miał miejsce we wszystkich krajach. Ten poziom wzmocnionej łączności ma wpływ na ciągłość działania administracji, ponieważ osiągnął on skalę większą niż kiedykolwiek wcześniej. Ten poziom łączności był transformacyjny w wielu sektorach.

Wirtualna komunikacja stała się standardem, który był przeciwieństwem tradycyjnego podejścia do interakcji osobistych. Stworzono różne standardy operacyjne, aby umożliwić większą zdolność adaptacji i współpracy. Platformy wideo zwiększyły wygodę i interakcję w wielu regionach geograficznych. Pozwoliło to na komunikację oraz dzielenie się informacjami i pomysłami w czasie rzeczywistym. Jednakże przejście na komunikację wirtualną często odbywało się bez odpowiedniej oceny związanego z tym ryzyka, dotyczącego luk w zabezpieczeniach IT i potencjalnie nieupoważnionych uczestników spotkań online. W przyszłości plany ciągłości działania muszą zapewniać, że narzędzia i oprogramowanie używane w sytuacjach nadzwyczajnych zostały poddane niezbędnym ocenom bezpieczeństwa.

Ryzyka związane z umiejętnościami cyfrowymi powinny (w szczególności) zostać uwzględnione. Podczas gdy oprogramowanie jest podatne na zagrożenia, to użytkownicy są często furtką do skorzystania z tych podatności. Ważne jest, aby w przypadku, gdy plan ciągłości działania obejmuje wprowadzenie alternatywnych metod lub narzędzi wspierających działanie, wszyscy pracownicy posiadali niezbędne przeszkolenie i umiejętności do ich wykorzystania. W ramach planów zawsze podejmowane są działania zapobiegawcze w celu zapewnienia regularnego przeprowadzania i powtarzania szkoleń.

Cyfryzacja wpłynęła również na ogólny proces kształtowania polityki rządów na całym świecie. Przed pandemią COVID-19 przepisy i polityki (zasady działania) były często uważane za sztywne i podlegały długim procesom, które wymagały akceptacji. W miarę postępu pandemii pilność podejmowania decyzji stawała się wysoka, a sam proces podejmowania decyzji stawał się złożony, co wymagało bieżącego przyjmowania polityk i podejmowania działań.

Planowanie ciągłości działania często wiąże się z koniecznością zakupu różnych towarów lub usług. Zwiększony poziom cyfryzacji, którego doświadczyliśmy podczas pandemii COVID-19 odegrał dużą rolę w usprawnieniu procesów rządowych. Dzięki nim można było szybciej reagować na pilne potrzeby związane z rozwiązywaniem kwestii dotyczących pandemii. Audytorzy muszą być świadomi, że plany ciągłości działania dla każdego działu mogą dopuszczać wyjątki od wprowadzonych mechanizmów kontroli zamówień. Muszą także rozumieć, że nawet te plany muszą zostać zatwierdzone przez odpowiednie organy i muszą istnieć jasne wymagania dotyczące tego, kiedy należy podjąć działania na ich podstawie (United Nations Department of Economic and Social Affairs, 2022[12]).

Wpływ cyfryzacji na funkcję audytu wewnętrznego

Zintegrowane zapewnienie definiuje się jako *ramy, które umożliwiają organizacji maksymalizację zakresu zapewnienia wiarygodności w spójny i skoordynowany sposób poprzez unikanie powielania lub luk w funkcjach kontrolnych*. Zintegrowane zapewnienie może stać się nową normą w erze cyfrowej. Istnieje wiele możliwości analizy i monitorowania użytkowników końcowych, które umożliwią wzmocnienie pierwszej i drugiej linii obrony, przy znacznie bardziej zautomatyzowanym zapewnianiu bezpieczeństwa

w czasie rzeczywistym. Audyt wewnętrzny będzie musiał bardzo wyraźnie wyodrębnić i wyartykułować swoją rolę trzeciej linii lub nową rolę, aby nie stać się przestarzałym lub nieskutecznym. Dane organizacyjne czasami maskują przydatne informacje na temat skuteczności mechanizmów kontroli, zarządzania ryzykiem, etycznego zachowania, wyników i stabilności finansowej. Zidentyfikowanie tych obszarów i opisanie ich w sposób, który wzbudzi zainteresowanie kierownictwa wyższego szczebla, wyróżni przyszłych dostawców usług zapewniających. (Chartered Institute of Internal Auditors, 2023[13])

Podczas gdy tradycyjną rolą audytorów jest wydanie zapewnienia na temat mechanizmów kontrolnych, a nie udzielanie konsultacji audytowanym w zakresie ich wiedzy specjalistycznej, to jednak doradztwo może być przydatne w kontekście planowania ciągłości działania. Biorąc pod uwagę tempo rozwoju technologicznego, następujące tematy powinny być na pierwszym planie i należy je rozważyć w kontekście przyszłościowego myślenia o środowisku cyfrowym: współpraca, łączność i komunikacja (Chartered Institute of Internal Auditors, 2023[13]).

W stale ewoluującym krajobrazie technologii cyfrowych organizacje sektora publicznego stoją przed krytycznym wyzwaniem, jakim jest dostosowanie się do zmian przy jednoczesnym zapewnieniu nieprzerwanego świadczenia usług. Audyty wewnętrzne odgrywają kluczową rolę w ocenie gotowości i odporności tych organizacji na zakłócenia cyfrowe. Era cyfrowa zapoczątkowała falę transformacji w sektorze publicznym, zmuszając organizacje do integracji zaawansowanych technologii i procesów cyfrowych. Ta integracja, choć korzystna, wprowadza złożoność i wyzwania, szczególnie w zakresie utrzymania ciągłości świadczenia usług w obliczu szybkich zmian technologicznych. Audyty wewnętrzne muszą zatem dostosować swoje metodologie, aby skutecznie ocenić sprawność, odporność i gotowość organizacji w tym cyfrowym krajobrazie. Dlatego jednym z głównych celów audytu wewnętrznego jest ocena ram i zdolności organizacji do zarządzania zmianami w technologiach i procesach cyfrowych, zapewniając ciągłość świadczenia usług publicznych. Obejmuje to analizę dostosowania inicjatyw cyfrowych do strategii, solidności infrastruktury IT oraz skuteczności praktyk zarządzania ryzykiem w obliczu transformacji cyfrowej.

Audytorzy powinni rozpocząć od kompleksowego przeglądu oceny ryzyka organizacji i strategii zarządzania dotyczących technologii cyfrowych. Obejmuje to ocenę procesów identyfikacji, analizy i ograniczania ryzyk związanych z transformacją cyfrową oraz sposobu, w jaki procesy te są zintegrowane z ogólnymi ramami zarządzania ryzykiem w organizacji.

Współpraca

Cyfryzacja organizacji doprowadziła do zmiany w kierunku kultury współpracy. Obszary, których audytorzy powinni być świadomi, obejmują:

- Zarządzanie danymi: ponieważ systemy oparte na dyskach twardych są zastępowane sieciami opartymi na chmurze, ich mechanizmy kontrolne, szczególnie w zakresie dostępu, muszą być silne.
- Zależność: ponieważ organizacje często polegają na platformach stron trzecich, które stają się częścią ich działalności, muszą istnieć odpowiednie mechanizmy kontrolne w celu utrzymania ciągłości działania i zarządzania dostawcami.
- Mechanizmy kontrolne: w miarę wprowadzania zmian we wszystkich aspektach organizacji należy dokonać niezbędnej aktualizacji odpowiednich mechanizmów kontrolnych, ponieważ ważne jest, aby pozostały one odpowiednie i skuteczne.
- Kultura: zmiany technologiczne zachodzą znacznie szybciej niż zmiany kulturowe. Ponieważ technologia może stwarzać możliwości większej synergii, funkcje i zarządzanie działające w sposób silosowy będą stanowić ryzyko dla sukcesu operacyjnego.
- Dezinformacja: ponieważ informacje w organizacjach mogą być udostępniane za pośrednictwem witryn wiki (umożliwiających edytowanie treści przez użytkowników) lub innych

niekontrolowanych platform, ważne jest, aby audytorzy i decydenci rozumieli krytyczne ryzyka z tym związane.

- Innowacyjność: ponieważ istnieje presja na wprowadzanie innowacji przez organizacje, audytorzy muszą być w stanie doradzić w zakresie ryzyka/korzyści związanych z tymi zakłóceniami bez utrudniania innowacji.

Łączność

Cyfryzacja zwiększyła wzajemne powiązania między ludźmi, danymi i systemami. Obszary, których audytorzy powinni być świadomi, obejmują:

- Dostęp do danych: wzrost dostępu do danych w organizacjach zwiększa ryzyko związane z prywatnością danych i skutecznością praktyk w zakresie cyberbezpieczeństwa, ponieważ rośnie prawdopodobieństwo niestosowania przyjętych praktyk oraz błędów ludzkich.
- Aktywa: przy większej łączności istnieje większa ilość aktywów cyfrowych. Należy wziąć to pod uwagę zarówno w kontekście prowadzonej działalności (aspekty operacyjne), jak również sami audytorzy powinni być świadomi, jak te aktywa funkcjonują, aby lepiej je chronić.
- Zewnętrzni interesariusze: w zależności od organizacji rządowej i jej działalności ważne jest, aby stosowane były wystarczające praktyki (ochrony danych), ponieważ dane stają się coraz szerzej dostępne.

Komunikacja

Łączność i współpraca nie funkcjonowałyby dobrze bez skutecznej komunikacji. Obszary, których audytorzy powinni być świadomi, to:

- Ludzie: gdy organizacje przystosowują się do cyfryzacji, często koncentrują się na samej technologii. Organizacja i audytorzy muszą być świadomi ryzyka związanego z zarządzaniem zmianą organizacyjną i z samymi ludźmi.
- Komunikacja: zapewnienie regularnej edukacji wszystkich pracowników, aby byli świadomi przyjętego sposobu postępowania przy komunikacji wewnętrznej i zewnętrznej.

Wszystkie wymienione tematy mogą być przedmiotem audytów. Są one istotne w kontekście planów ciągłości działania, a także związanych z nimi aspektami cyfryzacji. Nawet pomimo ewolucji technologii i zmian w sposobie działania, podstawowe mechanizmy kontrolne zawsze będą wymagały przeprowadzenia audytu.

Podręcznik na temat uczciwości w sektorze publicznym OECD podkreśla, że przejrzystość i otwartość są podstawowymi zasadami silnego zarządzania. Można to w szczególności wspierać zwiększając dostępność informacji i danych. Ramka 1.1 opisuje to dokładniej.

Ramka 1.1. Podręcznik na temat uczciwości w sektorze publicznym OECD (Rozdział 13 – Uczestnictwo)

Rozdział 13.2.1: Rząd jest otwarty i przejrzysty, zapewniając terminowy i nieograniczony dostęp do informacji i otwarte dane publiczne.

Przejrzystość jest niezbędna dla uczciwości w sektorze publicznym, ponieważ zwiększa koszty ukrywania i oszustw związanych z działaniami korupcyjnymi. Z perspektywy behawioralnej, przejrzystość może również ograniczyć nieetyczne zachowania, ponieważ postrzeganie, że czyjeś zachowanie jest widoczne i potencjalnie obserwowane, wprowadza element odpowiedzialności, który utrudnia uzasadnienie nieetycznych działań. Otwarty rząd, dostęp do informacji i otwarte dane

publiczne to trzy kluczowe narzędzia, które rządy mogą wykorzystać do zapewnienia przejrzystości i odpowiedzialności.

Otwarty rząd

Otwarty rząd można zdefiniować jako „kulturę rządzenia, która promuje zasady przejrzystości, uczciwości, odpowiedzialności i uczestnictwa interesariuszy w celu wspierania demokracji i wzrostu sprzyjającego włączeniu społecznemu". Kluczowe zasady otwartego rządu zostały wyszczególnione w Zaleceniu OECD w sprawie otwartego rządu i obejmują:

- Przejrzystość – ujawnianie i późniejsza dostępność odpowiednich danych i informacji rządowych.
- Uczciwość – spójne dostosowanie i przestrzeganie wspólnych wartości etycznych, zasad i norm w celu utrzymania i priorytetowego traktowania interesu publicznego nad interesami prywatnymi w sektorze publicznym.
- Odpowiedzialność – odpowiedzialność i obowiązek rządu w zakresie informowania obywateli o podejmowanych decyzjach, a także dostarczania informacji o działaniach i wynikach działania całego rządu i jego urzędników publicznych.
- Udział interesariuszy – wszystkie sposoby, w jakie interesariusze mogą być zaangażowani w cykl polityki oraz projektowanie i świadczenie usług, w tym poprzez dostarczanie informacji, konsultacje i zaangażowanie.

Wytyczne, a także struktury i mechanizmy wdrażania, koordynacji i oceny (np. strategie i plany działania, zespoły wykonawcze lub jednostki ds. otwartego lub cyfrowego rządu, platformy lub portale, bazy danych, pulpity nawigacyjne, zestawy narzędzi itp.) wspierają organizacje publiczne w ich codziennych wysiłkach na rzecz stosowania zasad otwartego rządu.

Źródło: (OECD, 2020[14]).

2 Przepisy i normy

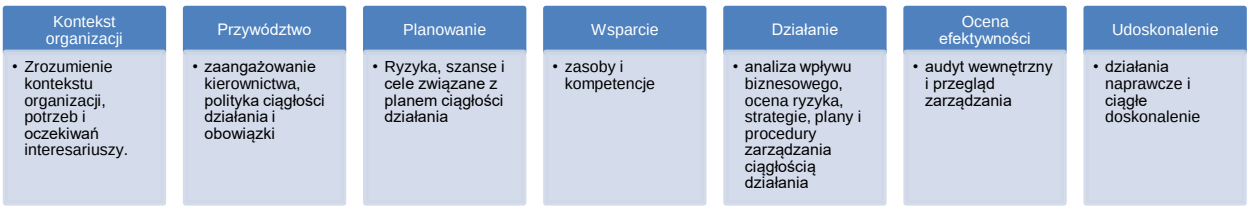
Regulacje w sprawie ciągłości działania

ISO 22301 (Systemy zarządzania ciągłością działania)

ISO 22301:2019[1] (Bezpieczeństwo i odporność – Systemy Zarządzania Ciągłością Działania – Wymagania) określa kryteria wdrażania, utrzymywania i doskonalenia systemu zarządzania w celu ochrony przed zakłóceniami, zmniejszania prawdopodobieństwa ich wystąpienia, przygotowania się na nie, reagowania na nie i odzyskiwania sprawności po ich wystąpieniu.

Norma ISO 22301 przedstawia siedem elementów systemu zarządzania ciągłością działania, które obejmują: kontekst organizacji, przywództwo, planowanie, wsparcie, działanie, ocenę efektywności i doskonalenie, jak pokazano na Rysunek 2.1. Norma ISO 22301 wyraźnie wspomina o roli audytora wewnętrznego. Audytor wewnętrzny (w myśl ISO) okresowo przeprowadza audyty w celu zapewnienia, że system zarządzania ciągłością działania jest zgodny ze standardami organizacji i normami ISO oraz jest skutecznie wdrażany i utrzymywany. Audyt wewnętrzny stanowi sedno oceny efektywności systemu zarządzania ciągłością działania wraz z przeglądem zarządzania.

Rysunek 2.1. ISO 22301 Systemy Zarządzania Ciągłością Działania – elementy norm



Źródło: Wersja zmieniona przez Międzynarodową Organizację Normalizacyjną (ISO, 2019[2]).

Zalecenie OECD w sprawie zarządzania ryzykiem krytycznym

Zalecenie OECD *w sprawie zarządzania ryzykiem krytycznym* zachęca wszystkie organizacje do zapewnienia ciągłości działania, ze szczególnym uwzględnieniem operatorów infrastruktury krytycznej. Można to osiągnąć poprzez:

- Opracowywanie standardów i zestawów narzędzi zaprojektowanych do zarządzania ryzykiem w odniesieniu do działalności lub świadczenia podstawowych usług,

[1] Norma ta jest również dostępna w polskiej wersji językowej: PN-EN ISO 22301:2020-04.

- Zapewnienie, że infrastruktura krytyczna, systemy informatyczne i sieci będą nadal funkcjonować po wystąpieniu wstrząsu,
- Wymaganie od służb interwencyjnych stacjonujących w obiektach infrastruktury krytycznej utrzymania planów. Zapewnia to, że mogą one kontynuować pełnienie swoich funkcji w przypadku sytuacji wyjątkowej, o ile jest to racjonalnie wykonalne,
- Zachęcanie małych, lokalnych firm do przyjmowania proporcjonalnych środków odporności biznesowej (OECD, 2014[4]).

Ramy ciągłości działania (Wielka Brytania i Kanada)

W celu ustanowienia ram ochrony ludności w sytuacjach kryzysowych w Wielkiej Brytanii uchwalona została ustawa o zarządzaniu kryzysowym *(Civil Contingencies Act)* z 2004 r. Ustawa ta wymaga od podmiotów reagujących na pierwszej linii utrzymywania wewnętrznych rozwiązań w zakresie zarządzania ciągłością działania, a od władz lokalnych promowania zarządzania ciągłością działania wśród organizacji komercyjnych i wolontariackich. Rząd centralny oferuje zestaw narzędzi zarządzania ciągłością działania, aby pomóc poszczególnym instytucjom w skutecznym ustanowieniu ich planów ciągłości działania. Zestaw narzędzi zawiera informacje na temat przydzielania obowiązków, konfigurowania i wdrażania zarządzania ciągłością działania w organizacji oraz ciągłego zarządzania (zob. Ramka 2.1).

Ramka 2.1. Zestaw narzędzi do zarządzania ciągłością działania w Wielkiej Brytanii

Skuteczne zarządzanie programem (zarządzania ciągłością działania) zapewnia ustanowienie i utrzymanie zdolności zarządzania ciągłością działania w organizacji. Proces ten obejmuje trzy etapy.

Przypisanie obowiązków

- Wyznaczenie osoby na poziomie kierownictwa, która będzie odpowiedzialna za zarządzanie ciągłością działania.
- Przydzielenie jednej lub kilku osobom odpowiedzialności za rozwój programu.

Ustanowienie i wdrożenie zarządzania ciągłością działania w organizacji

- Zakres, cele i założenia zarządzania ciągłością działania w organizacji.
- Działania lub „program" wymagany do ich realizacji.
- Komunikowanie programu wewnętrznym interesariuszom.
- Organizowanie odpowiednich szkoleń dla pracowników.
- Zapewnienie ukończenia działań.
- Wstępne przetestowanie rozwiązań w zakresie zarządzania ciągłością działania organizacji.

Bieżące zarządzanie

- Regularny przegląd i aktualizacja planów ciągłości działania organizacji i powiązanych z nimi dokumentów.
- Dalsze promowanie ciągłości działania w całej organizacji.
- Zarządzanie programem ćwiczeń.
- Aktualizowanie programu zarządzania ciągłością działania poprzez wyciąganie wniosków i stosowanie dobrych praktyk.

Źródło: (UK Government, n.d.[15]).

Ramka 2.2. Strategie zarządzania ciągłością działania zawarte w brytyjskim zestawie narzędzi

LUDZIE

- Inwentaryzacja umiejętności pracowników niewykorzystywanych w ramach ich obecnych ról – w celu umożliwienia przesunięć.
- Mapowanie procesów i dokumentacja – aby umożliwić pracownikom podejmowanie ról, z którymi nie są zaznajomieni.
- Szkolenie w zakresie wielu umiejętności dla każdej osoby.
- Szkolenie przekrojowe umiejętności wielu osób.
- Planowanie zastępstw.
- Korzystanie ze wsparcia osób trzecich, poparte umowami kontraktowymi.

- Geograficzne rozdzielenie osób lub grup o kluczowych umiejętnościach może zmniejszyć prawdopodobieństwo utraty wszystkich osób zdolnych do pełnienia określonej roli.

LOKALE

- Przeniesienie pracowników do innych obiektów należących do organizacji, takich jak obiekty szkoleniowe.
- Zastąpienie pracowników wykonujących mniej pilne procesy biznesowe pracownikami wykonującymi czynności o wyższym priorytecie. Podczas korzystania z tej opcji należy zachować ostrożność, aby zaległości w mniej pilnych pracach nie stały się niemożliwe do opanowania.
- Praca zdalna – może to być praca z domu lub z innych lokalizacji.
- Korzystanie z pomieszczeń zapewnianych przez inne organizacje, w tym przez specjalistów zewnętrznych.
- Alternatywne źródła urządzeń, maszyn i innego sprzętu.

TECHNOLOGIA

- Utrzymywanie tej samej technologii w różnych lokalizacjach, które nie zostaną dotknięte tymi samymi zakłóceniami działalności.
- Utrzymywanie starszego sprzętu jako awaryjnego zamiennika lub części zamiennych.

INFORMACJE

- Należy upewnić się, że dane są archiwizowane i przechowywane poza siedzibą firmy.
- Niezbędna dokumentacja jest bezpiecznie przechowywana (np. w ognioodpornym sejfie).
- Kopie niezbędnej dokumentacji są przechowywane w innym miejscu.

DOSTAWCY I PARTNERZY

- Przechowywanie dodatkowych materiałów eksploatacyjnych w innej lokalizacji.
- Pozyskiwanie materiałów z dwóch lub wielu źródeł.
- Identyfikacja alternatywnych dostawców.
- Zachęcanie lub wymaganie od dostawców/partnerów posiadania potwierdzonej zdolności do zapewnienia ciągłości działania.
- Istotne klauzule karne w umowach na dostawę.

INTERESARIUSZE

- Ustanowienie mechanizmów dostarczania informacji interesariuszom.
- Rozwiązania skierowane do grup szczególnie wrażliwych.

Źródło: (UK Government, n.d.[15]).

Kanadyjski bank *Business Development Bank of Canada* (BDC), który jest w całości własnością rządu Kanady, opracował kroki niezbędne do przygotowania planu reagowania w sytuacji awaryjnej i planu na wypadek wystąpienia klęski żywiołowej. Kroki te mają zastosowanie do klęsk żywiołowych, wszelkiego rodzaju wypadków lub nieprzewidzianych zdarzeń, które mogłyby zakłócić działalność. We wszystkich scenariuszach, rząd musi zachować zdolność do kontynuowania swojej działalności. Ramka 2.3 opisuje kroki, które należy podjąć.

Ramka 2.3. Sposób opracowania planu reagowania w sytuacji awaryjnej i planu na wypadek wystąpienia klęski żywiołowej na przykładzie banku Business Development Canada

Poniżej opisano kroki, które należy podjąć w celu zaplanowania sposobu reagowania w sytuacji awaryjnej lub wystąpienia klęski żywiołowej.

- Powołanie zespołu ds. gotowości na wypadek sytuacji awaryjnej.
- Identyfikacja podstawowych usług i funkcji.
- Określenie wymaganych zestawów umiejętności i ponownego przydziału obowiązków personelowi.
- Identyfikacja potencjalnych problemów.
- Przygotowanie planu dla każdej istotnej usługi/funkcji.
- Porównanie z „listą kontrolną gotowości".
- Przegląd z zespołem ds. gotowości na wypadek sytuacji awaryjnej.
- Weryfikacja, testowanie i aktualizacja planu.

Źródło: (Business Development Canada, n.d.[16]).

Regulacje dotyczące ciągłości działania w Polsce

W Unii Europejskiej dyrektywa UE 2022/2557 w sprawie odporności podmiotów krytycznych[2] z 2022 r. w art. 13 stanowi, że: Państwa członkowskie zapewniają, aby podmioty krytyczne wprowadzały odpowiednie i proporcjonalne środki techniczne, środki bezpieczeństwa i środki organizacyjne służące zapewnieniu ich odporności, w oparciu o odpowiednie informacje dostarczone przez państwa członkowskie dotyczące oceny ryzyka państwa członkowskiego oraz wyników oceny ryzyka podmiotu krytycznego. Obejmuje to punkt (d), który określa środki niezbędne do: odtworzenia po incydentach, z należytym uwzględnieniem środków na rzecz ciągłości działania oraz identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej (European Union, 2022[17]).

W Polsce przepisy takie jak rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, ogólne rozporządzenie o ochronie danych, rozporządzenie w sprawie Biuletynu Informacji Publicznej oraz Kodeks postępowania administracyjnego przewidują obowiązek nieprzerwanego świadczenia usług publicznych. Na przykład art. 8 (paragraf 1) Kodeksu postępowania administracyjnego stanowi, że organy administracji publicznej prowadzą postępowanie w sposób budzący zaufanie jego uczestników do władzy publicznej, kierując się zasadami proporcjonalności, bezstronności i równego traktowania. Zgodnie z art. 12 paragraf 1 tego samego Kodeksu, organy administracji publicznej powinny działać w sprawie wnikliwie i szybko, posługując się możliwie najprostszymi środkami prowadzącymi do jej załatwienia. Ponadto art. 35 paragraf 1 stanowi, że organy administracji publicznej obowiązane są załatwiać sprawy bez zbędnej zwłoki. Podczas planowania i przeprowadzania audytów ciągłości świadczenia usług publicznych należy również wziąć pod uwagę inne szczegółowe przepisy, na przykład ustawę o krajowym systemie cyberbezpieczeństwa.

Standardy kontroli zarządczej dla sektora finansów publicznych wymagają, aby kierownik każdej jednostki sektora finansów publicznych zapewnił mechanizmy utrzymujące ciągłość jej działania. Ponadto minister kierujący działem administracji rządowej oraz kierownik jednostki samorządu

[2] Uchylająca dyrektywę Rady 2008/114/WE.

terytorialnego są również odpowiedzialni za funkcjonowanie kontroli zarządczej – w tym za zachowanie ciągłości – odpowiednio na poziomie całego działu administracji rządowej lub całego samorządu terytorialnego. Na przykład Ministerstwo Finansów, poprzez Zarządzenie Ministra Finansów z dnia 24 lutego 2022 r. w sprawie wprowadzenia Polityki Zarządzania Ciągłością Działania, wymaga od Ministerstwa Finansów i podległych mu jednostek ustanowienia planu ciągłości działania i wprowadza politykę planowania i wdrażania zarządzania ciągłością działania (BCM). Polityka zarządzania ciągłością działania Ministra Finansów oparta jest na normie ISO 22301, a Ramka 2.4 przedstawia jej podstawowe elementy.

Ramka 2.4. Polityka zarządzania ciągłością działania w polskim Ministerstwie Finansów

Polityka zarządzania ciągłością działania obejmuje następujące działania:

1. Określenie ról poszczególnym pracownikom i przypisanie im zadań i odpowiedzialności.
2. Zidentyfikowanie procesów i powiązań między nimi. Określenie głównych i pomocniczych procesów organizacji.
3. Przeprowadzenie analizy wpływu biznesowego (BIA) w celu zidentyfikowania krytycznych procesów.
4. Przeprowadzenie analizy ryzyka dla tych krytycznych procesów.
5. Opracowanie strategii ciągłości działania.
6. Sformułowanie planów ciągłości działania.

Celem analizy wpływu biznesowego jest identyfikacja krytycznych procesów i zasobów wymaganych do ich utrzymania lub wznowienia, a także określenie skutków przerwania tych procesów w określonych przedziałach czasowych. Analiza wpływu biznesowego powinna określić kluczowe wskaźniki: Docelowy Czas Odtworzenia (RTO) i Docelowy Punkt Odtworzenia (RPO).

Polityka wyraźnie stwierdza, że na system zarządzania ciągłością działania mają wpływ poziomy rozwoju i wdrożenia innych powiązanych systemów. Innymi słowy, oznacza to, że system zarządzania ciągłością działania powinien działać prawidłowo w zakresie bezpieczeństwa IT, bezpieczeństwa informacji, bezpieczeństwa fizycznego, zarządzania kryzysowego i ochrony danych osobowych.

3 Atrybuty audytu

Wybór typu audytu

Audyt planowania ciągłości działania ma na celu ocenę skuteczności, efektywności i zdolności adaptacyjnych planów ciągłości działania. Dlatego audyt planowania ciągłości działania można sklasyfikować jako audyt efektywnościowy. Oznacza to, że główne części wytycznych dotyczących audytu efektywnościowego można zastosować do audytu planowania ciągłości działania. Audyt planowania ciągłości działania może być częścią szerzej zakrojonego audytu, który obejmuje również aspekty zgodności i audytu finansowego. W stosownych przypadkach należy również rozważyć wpływ ram regulacyjnych lub instytucjonalnych na wyniki efektywności badanej jednostki (INTOSAI, 2019[18]).

Harmonogram i zasoby

Norma ISO 22301 wymaga regularnych audytów wewnętrznych (w rozumieniu ISO) w zakresie planu ciągłości działania. Ocena ryzyka jest niezbędna do ustalenia optymalnego czasu przeprowadzenia audytu. Jeśli plan ciągłości działania został niedawno wdrożony lub istnieją znane problemy, mogą być wymagane częstsze audyty. Harmonogram audytów planowania ciągłości działania powinien uwzględniać czynniki ryzyka, takie jak zasoby do wdrożenia planu ciągłości działania, wsparcie kierownictwa, środowisko operacyjne oraz stabilność i bezpieczeństwo operacji IT.

Podczas planowania audytu kluczowe jest pragmatyczne uwzględnienie harmonogramów i zapotrzebowania na zasoby. Takie podejście zapewnia, że proces audytu jest ekonomiczny, efektywny, skuteczny i terminowy, zgodnie z uznanymi zasadami metod zarządzania projektami. Audyty są często postrzegane jako projekty, obejmujące planowanie, organizowanie, zabezpieczenie, zarządzanie, przywództwo i kontrolę zasobów w celu osiągnięcia określonych celów.

Głównym celem powinno być:

- Ustalenie praktycznych harmonogramów dla każdego zadania, w oparciu o zaplanowaną metodologię i inne istotne czynniki, takie jak procedury audytu wewnętrznego, poprzednie audyty, opinie interesariuszy, oczekiwany dostęp do informacji i dostępność zasobów.
- Identyfikacja i koordynacja odpowiedniej liczby zasobów, w tym audytorów, osób nadzorujących i interesariuszy w celu realizacji określonych zadań w oczekiwanych ramach czasowych z uwzględnieniem kompetencji zespołu.
- Obliczanie wydatków związanych z podróżami, szkoleniami, sprzętem, zewnętrznymi ekspertami merytorycznymi i innymi kosztami dodatkowymi. Wewnętrzne zasoby kadrowe są zazwyczaj budżetowane pod względem dni roboczych i monitorowane za pośrednictwem wewnętrznego systemu.

Cele

Cele audytu planowania ciągłości działania koncentrują się na ocenie skuteczności, efektywności i zdolności adaptacyjnych planów ciągłości działania, szczególnie w odpowiedzi na wyzwania cyfrowe. Obejmuje to (US GAO, 2014[19]) (INTOSAI, 2016[20]) (IIA, 2019[21]):

- Zapewnienie, że usługi publiczne mają niezbędną odporność operacyjną, umożliwiającą szybkie przywrócenie funkcjonowania po różnych zakłóceniach, takich jak cyberataki i awarie IT.
- Weryfikację zgodności z odpowiednimi przepisami, regulacjami i standardami związanymi z planowaniem ciągłości działania i bezpieczeństwem cyfrowym w nadzwyczajnych sytuacjach, zapewniając, że usługi publiczne spełniają obowiązkowe wymagania.
- Ocenę skuteczności praktyk zarządzania ryzykiem w zakresie identyfikacji, oceny i ograniczania ryzyka związanego z cyfryzacją, w tym z cyberzagrożeniami oraz obaw związanych z prywatnością danych.
- Ocenę efektywności w celu ustalenia, czy zasoby przydzielone do planowania ciągłości, w tym zasoby finansowe, ludzkie i technologiczne, są wykorzystywane w sposób efektywny i skuteczny w celu wspierania osiągania celów odporności. Obejmuje to fundusze na nieprzewidziane wydatki i ocenę, czy pozycje są odpowiednio finansowane.
- Sprawdzenie, czy plan ciągłości działania obejmuje wszystkie powiązane ryzyka w przypadku prywatyzacji części usług publicznych (jeśli ma to zastosowanie).

Ramka 3.1. Przykład celu audytu

Audytor Generalny Australii – Zarządzanie ciągłością działania (2014)

- Cel: Celem audytu była ocena adekwatności praktyk i procedur wybranych podmiotów rządu australijskiego w zakresie zarządzania ciągłością działania. Aby osiągnąć ten cel Australijskie Narodowe Biuro Audytu (ANAO) przyjęło odgórne kryteria odnoszące się do ustanowienia, wdrożenia i przeglądu rozwiązań w zakresie ciągłości działania tych podmiotów. ANAO oceniła ramy i praktykę zarządzania ciągłością działania, w tym kluczową dokumentację (taką jak polityka zarządzania ciągłością działania i plany ciągłości działania), reakcje podmiotów na rzeczywiste zdarzenia, ćwiczenia i testy zarządzania ciągłością działania oraz monitorowanie i przegląd.

Źródło: (ANAO, 2014[22]).

Zakres

Zakres określa parametry audytu. Odnosi się do najważniejszych pytań i sposobu przeprowadzenia zadania. Określa zagadnienie, które zostanie ocenione/na temat którego zostanie opracowany raport, dokumenty/zapisy, które zostaną poddane przeglądowi, okres i lokalizacje (jeśli takie istnieją), które zostaną zbadane. Zakres jest wyraźnie uzależniony od celów (i pytań) audytu. Należy zauważyć, że wszelkie modyfikacje celów mogą mieć również wpływ na zakres. Tworzenie zakresu audytu jest ważną częścią projektowania audytu. Zakres audytu można ustalić, odpowiadając na serię pytań. Pomoże to właściwie go zdefiniować. Przy określaniu zakresu audytu należy również wziąć pod uwagę dodatkowe kwestie. Będą się one różnić w zależności od organizacji. Obejmują one między innymi:

- dostępność wiarygodnych danych i źródeł informacji,
- zasoby wewnętrzne do przeprowadzenia audytu,
- dostępność audytorów z odpowiednimi umiejętnościami,
- dostęp do ekspertów merytorycznych (w razie potrzeby),
- koszty związane z audytem (np. koszty podróży lub innych potrzeb operacyjnych),
- ograniczenia czasowe audytu,
- wszelkie inne kwestie lub tematy, które mogą mieć wpływ na zakres audytu.

Zakres audytu może również obejmować potencjalne zagadnienia, które były częścią zaleceń z poprzednich sprawozdań z audytu (jeśli zostaną uznane za istotne i ważne) (INTOSAI, 2019[18]).

Zgodnie publikacją IIA, plan ciągłości działania można uznać za część środków zarządzania kryzysowego, ale każdy kraj może go zdefiniować i rozróżnić na swój własny sposób[3]. Zdefiniowanie tej koncepcji w węższy sposób, wraz z reagowaniem w sytuacji awaryjnej (ER) i zarządzaniem w sytuacji kryzysowej (CM), może pomóc w jasnym określeniu zakresu audytu planowania ciągłości działania, jak pokazano na Rysunek 3.1. Reagowanie w sytuacji awaryjnej odnosi się do początkowej reakcji, której celem jest zminimalizowanie szkód dla życia, obiektów i aktywów spowodowanych kryzysem lub katastrofą oraz złagodzenie skutków kryzysu. Obejmuje to na przykład takie środki jak izolowanie zakażonych osób podczas pandemii, zapobieganie rozprzestrzenianiu się infekcji wśród pracowników oraz podejmowanie środków ewakuacji i ochrony obiektów w przypadku katastrofy naturalnej. Reagowanie w sytuacji awaryjnej należy zakończyć w ciągu kilku minut do kilku godzin po wystąpieniu sytuacji kryzysowej. Zarządzanie w sytuacji kryzysowej koncentruje się na utrzymaniu funkcji organizacji po kryzysie. Wiąże się to na przykład z przywróceniem podstawowych funkcji służących utrzymaniu organizacji, takich jak: komunikacja między kierownictwem a pracownikami, komunikacja z obywatelami i sieć usług. W związku z tym zarządzanie w sytuacji kryzysowej następuje w ciągu kilku dni po katastrofie. Plan ciągłości działania koncentruje się na minimalizowaniu przerw w świadczeniu usług spowodowanych katastrofami i utrzymaniu podstawowych funkcji usługowych. Dlatego plan ciągłości działania obejmuje okres kilku dni lub tygodni po katastrofie, a w zależności od sytuacji może trwać nawet dłużej (Everest et al., 2008[23]).

Rysunek 3.1. Różnice między reagowaniem w sytuacji awaryjnej, zarządzaniem w sytuacji kryzysowej i ciągłością działania

Źródło: (Everest et al., 2008[23])

Ramka 3.2. Przykłady zakresu

Agencja Zdrowia Publicznego Kanady: Audyt planów ciągłości działania dla usług krytycznych (2022)

- Zakres: Zakres tego audytu obejmował przegląd próbki planów ciągłości działania dotyczących usług krytycznych ujętych pod kategorią „Przygotowanie na sytuacje awaryjne i reagowanie na choroby zakaźne". Audyt nie obejmował przeglądu zarządzania planami

[3] Przykładowo, w Polsce art. 2 ustawy o zarządzaniu kryzysowym definiuje, że zarządzanie kryzysowe „[...] polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej".

ciągłości działania i powiązanymi z nimi bazami danych, ani adekwatności szablonów i analiz wpływu biznesowego. Zbadaliśmy, czy Departament Zdrowia Kanady oraz Agencja Zdrowia Publicznego Kanady posiadały aktualne plany ciągłości działania, aby umożliwić ciągłość świadczenia usług w obecnym środowisku, niezależnie od formatu tych planów.

Departament Spraw Ludności Rdzennej i Obszarów Północnych Kanady: Audyt planowania ciągłości działania (2017)

- Zakres: Zakres audytu koncentrował się na ocenie ram zarządzania (tj. polityk i zakresu odpowiedzialności, a także ról i obowiązków oraz monitorowania i nadzoru w celu wdrożenia programu planowania ciągłości działania), rozwoju planowania ciągłości działania, gotowości i świadomości programu planowania ciągłości działania Departamentu oraz ustanowionych mechanizmów kontrolnych w celu zapewnienia, że Departament Spraw Ludności Rdzennej i Obszarów Północnych Kanady ma zdolność do realizacji programu planowania ciągłości działania zgodnie z obowiązującymi przepisami i politykami.

Departament Bezpieczeństwa Publicznego Kanady: Audyt programu planowania ciągłości działania (2016)

- Zakres: Zakres audytu obejmował zbadanie zarządzania programem planowania ciągłości działania Departamentu i rozwiązań w zakresie zarządzania ryzykiem, a także adekwatności planów ciągłości działania. Obejmowało to plany ciągłości działania dla rządu Kanady i Kanadyjskiego Centrum Reagowania na Incydenty Cybernetyczne oraz powiązane dokumenty pomocnicze z marca 2016 r. Zakres audytu obejmował plany zarządzania kryzysowego, ramy reagowania i protokoły (procedury) Departamentu w celu kierowania, informowania, ułatwiania i koordynowania zintegrowanego reagowania federalnego na zagrożenie lub sytuację kryzysową.

Źródło: (Health Canada, 2022[24]) (Indigenous and North Affairs Canada, 2017[25]) (Public Safety Canada, 2016[26]).

Ocena ryzyka

Ocena ryzyka jest niezbędna do określenia kryteriów audytu i ustalenia strategii audytu. Audytorzy wewnętrzni muszą zidentyfikować ryzyka związane z ustanowieniem i wdrożeniem planu ciągłości działania na etapie planowania (programowania) audytu i ocenić działania organizacji w zakresie zarządzania ryzykiem w odniesieniu do tych ryzyk.

Poniżej przedstawiono przykłady kategorii ryzyka w zakresie planu ciągłości działania i w zakresie cyfryzacji.

- Organizacja nie ustanowiła planu ciągłości działania.
- Plan ciągłości działania nie został odpowiednio udokumentowany – kwestia zgodności.
- Plan ciągłości działania jest niekompletny (np. nieskutecznie/niekompletnie testowany[4], niska wykonalność, brak precyzyjnego określenia odpowiedzialności, pominięci interesariusze i brak uwzględnienia dostaw zewnętrznych – usług outsourcingowych).

[4] Przykłady możliwych testów mogą obejmować personel (np. zwiększone obciążenie pracą, przetwarzanie transakcji i inne specyficzne procesy operacyjne), technologię (np. testowanie procesu odzyskiwania danych, systemów, aplikacji i sieci) oraz obiekty (np. czynniki środowiskowe, zasilanie awaryjne i bezpieczeństwo fizyczne).

- Pracownicy mają niską świadomość na temat planu ciągłości działania, a szkolenia w tym zakresie nie są wystarczające.
- Niskie wsparcie ze strony kierownictwa.
- Brak wykwalifikowanego personelu do wdrożenia planów (np. personel nie jest zaznajomiony z narzędziami lub procesami cyfrowymi).
- Plan ciągłości działania nie ma wystarczającego oddziaływania nawet przy pełnym wdrożeniu.
- Nie poświęca się odpowiedniej uwagi znanym zagrożeniom lub słabościom.
- Istnieje lepszy – pod względem efektywności i oszczędności – sposób realizacji przy mniejszych zasobach.
- Ryzyka związane z dostawcami lub wykonawcami.

Kryteria

Kryteria są opracowywane w celu pomiaru sposobu realizacji zadań w stosunku do oczekiwań. Kryteria są punktami odniesienia, które są wykorzystywane do oceny badanego tematu. Podobnie jak w przypadku wszystkich audytów wewnętrznych, kryteria mogą być ilościowe i/lub jakościowe. Kryteria mogą być ogólne lub szczegółowe, koncentrujące się na tym, co powinno być zgodnie z przepisami prawa, regulacjami lub celami; czego się oczekuje, zgodnie z rozsądnymi zasadami, wiedzą naukową i najlepszymi praktykami; lub co mogłoby być, biorąc pod uwagę lepsze warunki. Powinny opisywać obszary, pod kątem których audytowany będzie oceniany.

Zazwyczaj kryteria są opracowywane i przekazywane podczas fazy planowania (programowania), aby zachęcić do ich akceptacji, ale bardziej złożone audyty, takie jak audyty planów ciągłości świadczenia usług publicznych, mogą stworzyć sytuację, w której są one definiowane później w procesie audytu. Może to być skomplikowane, ponieważ plan ciągłości świadczenia usług publicznych może zawsze ewoluować ze względu na różne aspekty organizacji.

W ramach fazy projektowania (programowania) ważne jest, aby funkcja audytu wewnętrznego (IAF) omówiła kryteria audytu z audytowanym. Ten poziom współpracy pomoże zapewnić wspólne i powszechne zrozumienie kryteriów, które zostaną wykorzystane jako punkty odniesienia (podczas oceny audytowanego obszaru). Zapewni również informacje zwrotną na temat możliwości ich zastosowania i zasadności. Zaangażowanie audytowanego może również zwiększyć prawdopodobieństwo zgodzenia się z ustaleniami i zaleceniami. Choć przejrzystość jest kluczowa, to ostateczna decyzja dotycząca adekwatnych kryteriów audytu, zależnych od jego rodzaju, spoczywa na funkcji audytu wewnętrznego (INTOSAI, 2019[18]).

Ważne jest, aby przy definiowaniu celów i kryteriów audytu planów ciągłości świadczenia usług publicznych uwzględnić kilka zagadnień, które są istotne dla wszystkich organizacji. Podczas opracowywania kryteriów można wziąć pod uwagę następujące kwestie (ISO, 2019[2]; US NIST, 2020[27]; ISACA, 2024[28]):

- Plany ciągłości działania są zgodne z ogólnymi celami strategicznymi organizacji i celami transformacji cyfrowej, zapewniając świadczenie usług o kluczowym znaczeniu dla interesariuszy.
- Plany ciągłości działania opierają się na kompleksowej ocenie ryzyka, która obejmuje ryzyka cyfrowe, identyfikując potencjalne zagrożenia dla ciągłości świadczenia usług i wpływ tych zagrożeń.
- Zewnętrzni dostawcy i partnerzy, zwłaszcza ci świadczący usługi cyfrowe, powinni zostać poddani ocenie, aby upewnić się, że nie staną się słabym ogniwem w planowaniu ciągłości

działania. Należy upewnić się, że jest to uwzględnione w postaci testów przeprowadzanych podczas oceny każdego dostawcy, oprogramowania, usługodawcy itp.

- Mechanizmy ciągłego monitorowania, przeglądu i ulepszania planu ciągłości działania, uwzględniają wnioski wyciągnięte z ćwiczeń, incydentów i zmian w środowisku cyfrowym.

Kryteria te odnoszą się do nadrzędnego tematu planowania ciągłości działania. Podczas opracowywania kryteriów operacyjnych lub technicznych i/lub podkryteriów należy wziąć pod uwagę następujące kwestie (FEMA, 2010[29]; CISA GOV, 2024[30]):

- Należy uwzględnić obecność jasnych procedur reagowania na incydenty i odzyskiwania danych, które są regularnie testowane i aktualizowane, zapewniając szybkie przywrócenie świadczenia usług przy minimalnych zakłóceniach. Może to obejmować wszystkie działania organizacji.
- Ocena adekwatności infrastruktury IT i rozwiązań technologicznych do wspierania planów ciągłości działania, w tym tworzenia kopii zapasowych danych, rozwiązań w zakresie odzyskiwania danych i środków cyberbezpieczeństwa; zapewnienie, że zwykłe działania organizacyjne mogą być kontynuowane przy minimalnych zakłóceniach.
  - Środki cyberbezpieczeństwa: ocena niezawodności zabezpieczeń cyberbezpieczeństwa pod kątem ochrony cyfrowych usług publicznych.
  - Interoperacyjność i integracja systemów: zdolność do płynnego świadczenia usług w ramach różnych platform i systemów cyfrowych.
  - Ochrona danych i prywatności: plany ciągłości działania uwzględniają przepisy dotyczące ochrony danych i prywatności.
- Należy ocenić, czy pracownicy zostali odpowiednio przeszkoleni i są świadomi swoich ról w planie ciągłości działania, ze szczególnym uwzględnieniem umiejętności cyfrowych i świadomości cyberbezpieczeństwa, aby skutecznie ograniczać zagrożenia cyfrowe. Obejmie to regularną aktualizację ról i obowiązków.
- Określenie, czy istnieją skuteczne plany komunikacji w celu informowania interesariuszy, w tym opinii publicznej i organizacji partnerskich, w trakcie i po incydencie, przy zachowaniu przejrzystości i zaufania. Ogólna strategia i proces planu komunikacji mogą zostać włączone do całościowego procesu wyciągania wniosków (lessons learned).

Ramka 3.3. Przykład kryteriów audytowych

Agencja Zdrowia Publicznego Kanady: Audyt planów ciągłości działania dla usług krytycznych (2022)

- Kryterium 1: Departament i Agencja opracowały plany ciągłości działania, aby zapewnić ciągłość swoich krytycznych usług i krytycznych usług wsparcia, które są testowane i aktualizowane dla zidentyfikowanych usług krytycznych.

Było to jedyne kryterium przeprowadzonego w 2022 r. zadania audytowego. W związku z tym, że agencja była jedną z wiodących w ramach krajowego reagowania na pandemię, ryzyko stale się pojawiało i ewoluowało. Ponieważ środowisko pracy zmieniło się drastycznie, plany ciągłości działania stały się przestarzałe. Zwiększyło to ryzyko braku ciągłości świadczenia usług krytycznych (przy przewidywanym dalszym występowaniu zakłócenia). Podstawowym celem audytu było zapewnienie, że: *Departament i Agencja utrzymały aktualne plany ciągłości działania podczas pandemii*.

Departament Spraw Ludności Rdzennej i Obszarów Północnych Kanady: Audyt planowania ciągłości działania (2017)

- Kryterium 1: Ramy zarządzania

- Wdrożony został program planowania ciągłości działania departamentu z odpowiednimi i jasno określonymi celami, rolami, obowiązkami i odpowiedzialnościami.
- Ważne aspekty innych programów ciągłości działania, w tym bezpieczeństwo technologii informatycznych (IT), zarządzanie incydentami i wewnętrzne zarządzanie kryzysowe, są skutecznie zintegrowane w ramach programu planowania ciągłości działania.

- Kryterium 2: Opracowywanie planów ciągłości działania
  - Istnieją odpowiednie i adekwatne mechanizmy kontrolne wspierające opracowanie planów ciągłości działania.
- Kryterium 3: Gotowość i świadomość programu planowania ciągłości działania
  - Istnieją odpowiednie i adekwatne mechanizmy kontrolne wspierające utrzymanie planów ciągłości działania.
  - Istnieją odpowiednie i adekwatne mechanizmy kontrolne wspierające gotowość planów ciągłości działania.
  - Istnieją odpowiednie i adekwatne mechanizmy kontrolne promujące świadomość na temat planów ciągłości działania.
- Kryterium 4: Zasoby programu planowania ciągłości działania
  - Istnieją odpowiednie i adekwatne mechanizmy kontrolne w celu utrzymania zdolności niezbędnych do realizacji programu planowania ciągłości działania zgodnie z obowiązującymi przepisami i politykami.

Przeprowadzony w 2017 r. audyt był priorytetem dla departamentu, ponieważ ostatnie wydarzenia wymagały zastosowania planów ciągłości działania.

Departament Bezpieczeństwa Publicznego Kanady: Audyt programu planowania ciągłości działania (2016)

- Kryterium 1: Istnieją ramy zarządzania, które są zintegrowane z Federalnym Planem Reagowania w Sytuacjach Wyjątkowych i obejmują zatwierdzone opisy ról, obowiązków, polityk, komitety nadzorcze i zasoby.
- Kryterium 2: Istnieje analiza wpływu biznesowego, która jasno identyfikuje krytyczne usługi biznesowe niezbędne dla utrzymania działalności podczas incydentu oraz określa wymagania w zakresie odzyskiwania i priorytetowe krytyczne usługi do odzyskania.
- Kryterium 3: Strategie ciągłości działania i odzyskiwania danych zostały zidentyfikowane, ocenione, wybrane i zatwierdzone, a plany ciągłości działania są zgodne z polityką, standardami rządowymi i wytycznymi.
- Kryterium 4: Plany ciągłości działania podlegają testowaniu i walidacji, co obejmuje przygotowanie raportów z wyciągniętych wniosków (lessons learned) oraz aktualizację planów ciągłości działania po testach lub rzeczywistych zdarzeniach w celu odzwierciedlenia wyciągniętych wniosków i uwzględnienia zmian w Departamencie i jego środowisku operacyjnym.

Przeprowadzony w 2016 r. audyt był wynikiem analizy wpływu biznesowego, która została przeprowadzona 5 lat wcześniej. Analiza wykazała, że główną krytyczną usługą departamentu jest zarządzanie zintegrowanym federalnym reagowaniem na sytuacje kryzysowe zapewnianym przez Rządowe Centrum Operacyjne. Następnie w 2013 r. stworzono plan ciągłości działania. Trzy lata później powstała kolejna wersja, która była katalizatorem przeprowadzonego audytu.

Źródło: (Health Canada, 2022[24]; Indigenous and North Affairs Canada, 2017[25]; Public Safety Canada, 2016[26]).

Zaangażowanie interesariuszy

Zaangażowanie zarówno wewnętrznych (w tym kierownictwa i członków zespołu audytu wewnętrznego), jak i zewnętrznych interesariuszy ma kluczowe znaczenie dla skutecznego planowania i przeprowadzania audytu. Opracowanie odpowiedniego programu zadania jest uzależnione od zakresu komunikacji z wewnętrznymi interesariuszami. Program zadania powinien zostać stworzony wspólnym wysiłkiem wewnętrznych interesariuszy. Korzystne jest, aby wszyscy członkowie zespołu audytowego rozmawiali i osiągnęli konsensus w sprawie programu zadania, matrycy projektowej, osi czasu projektu i innych wybranych narzędzi. W miarę rozwoju audytu kluczowe znaczenie ma utrzymanie otwartych kanałów komunikacji, a kierownictwo (zespołu audytowego) powinno dążyć do realizacji programu zadania. Wybrane narzędzia powinny promować ciągłe zaangażowanie interesariuszy i kierownictwa.

Inicjowanie komunikacji z zewnętrznymi interesariuszami, na przykład z audytowanym, na etapie programowania zadania i utrzymywanie jej przez cały proces ma zasadnicze znaczenie. Należy omówić wszystkie elementy, w tym: temat, cel, kryteria, pytania itp. Zapewni to, że audytowany otrzyma jasną informację na temat realizowanego zadania i umożliwi wyjaśnienie potencjalnego wpływu zadania na audytowanego. Mimo że powinna istnieć taka relacja, audytowany nie może wpływać na proces audytu. Celem jest wspieranie współpracy i pozytywnej interakcji.

W audyt planowania ciągłości działania mogą być zaangażowani następujący interesariusze:

- Przywództwo (kierownictwo).
- Zespół ds. zarządzania kryzysowego.
- Funkcja zarządzania ryzykiem.
- Cyfrowe, funkcje operacyjne IT, bezpieczeństwo IT i biuro ochrony danych.
- Planowanie ciągłości działania i menedżerowie ds. utrzymania.
- Menedżerowie zasobów do wdrażania planu ciągłości działania.
- Funkcja utrzymania obiektów (budynków, biur, infrastruktury).
- Kierownicy ds. operacji biznesowych w każdym departamencie/dziale/jednostce.
- Funkcja szkoleniowa związana z planem ciągłości działania.

Lista kontrolna audytu planowania ciągłości działania

Gdy przyjęte zostanie podejście systemowe w audycie planowania ciągłości działania, lista kontrolna może zostać skutecznie wykorzystana. Ten rodzaj audytu, skoncentrowany na ocenie efektywności systemów zarządzania, odpowiada na szeroki zakres pytań (zob. Ramka 3.4). Pytania te odnoszą się do przebiegu działań, identyfikują wszelkie słabości i oceniają potencjał poprawy.

Ramka 3.4. Lista kontrolna audytu planowania ciągłości działania

Zarządzanie programem planowania ciągłości działania

1. Wdrożony został program planowania ciągłości działania departamentu z odpowiednimi i jasno określonymi celami, rolami, obowiązkami i odpowiedzialnościami.

1.1. Odpowiednia polityka planowania ciągłości działania, standardy bezpieczeństwa operacyjnego i dokumentacja techniczna są opracowywane w ramach departamentu lub dostosowywane do polityki rządu Kanady. Polityka planowania ciągłości działania została zatwierdzona przez kierownictwo wyższego szczebla i opisuje kluczowe role i obowiązki w zakresie zarządzania działaniami

planowania ciągłości działania organizacji oraz podejście organizacji do przeprowadzania analiz wpływu biznesowego, opracowywania planów i ustaleń oraz utrzymywania gotowości.

1.2. Urzędnik ds. bezpieczeństwa w departamencie (DSO) kieruje i koordynuje program planowania ciągłości działania.

1.3. Koordynator ds. planowania ciągłości działania w departamencie został formalnie wyznaczony do pełnienia ról i obowiązków określonych w Standardzie Bezpieczeństwa Operacyjnego – Programie Planowania Ciągłości Działania.

1.4. Grupa robocza ds. planowania ciągłości działania została powołana przez kierownictwo wyższego szczebla, ma zdefiniowane odpowiednie role i obowiązki, spotyka się regularnie i regularnie przedstawia swoje działania Komitetowi Wykonawczemu.

1.5. Koordynator ds. planowania ciągłości działania w departamencie utrzymuje regularną komunikację i koordynację działań w zakresie planowania ciągłości działania z Koordynatorem ds. bezpieczeństwa IT i Urzędnikiem ds. bezpieczeństwa w departamencie.

2. Kierownictwo wyższego szczebla aktywnie i odpowiednio wspiera rozwój i wdrażanie programu planowania ciągłości działania.

2.1. Kierownictwo wyższego szczebla jest odpowiedzialne za wspieranie, nadzorowanie, kierowanie, zatwierdzanie i finansowanie rozwoju, wdrażania i testowania programu Ciągłości Działania, polityki, planów, działań i ustaleń.

2.2. Wystarczające zasoby finansowe i inne są przeznaczone na planowanie ciągłości działania.

Analiza wpływu biznesowego

3. Zidentyfikowano usługi biznesowe i krytyczne departamentu oraz przeprowadzono analizę wpływu biznesowego.

3.1. Istnieją procesy, których celem jest określenie charakteru działalności departamentu (np. roli, zakresu uprawnień) i usług, które musi on świadczyć zgodnie ze swoim aktem założycielskim lub innymi przepisami, polityką rządu, zobowiązaniami wobec innych departamentów oraz zawartymi umowami.

3.2. Usługi krytyczne zostały zidentyfikowane i uszeregowane pod względem ważności na podstawie: Minimalnego poziomu usług (MSL), Maksymalnych dopuszczalnych czasów przestojów (MAD), Docelowego Punktu Odtworzenia (RPO) i Docelowego Czasu Odtworzenia (RTO).

3.3. Niedawno przeprowadzono ocenę zagrożeń i ryzyka/podatności dla krytycznych usług w celu ich identyfikacji i oceny: Wszystkich potencjalnych źródeł zakłóceń; Bezpośrednich i pośrednich skutków zakłóceń dla departamentu; Poziomu szkód dla Kanadyjczyków i rządu w przypadku gdy zakłócenie na nich wpływa.

3.4. Zidentyfikowano zależności (procesy), które wspierają krytyczne usługi bezpośrednio lub pośrednio, zarówno wewnętrznie, jak i zewnętrznie względem departamentu.

3.5. Kadra kierownicza wyższego szczebla dokonuje przeglądu i zatwierdza analizę wpływu biznesowego danego departamentu.

Plany ciągłości działania i ich postanowienia

4. Strategie ciągłości działania i odzyskiwania danych zostały zidentyfikowane, ocenione, wybrane i zatwierdzone dla każdej krytycznej usługi.

4.1. Dla wszystkich krytycznych usług określono możliwe sposoby zapewnienia ciągłości działania

i odzyskiwania danych.

4.2. Przeprowadzono ocenę każdego sposobu, biorąc pod uwagę wpływ na departament, korzyści, ryzyko, wykonalność, wymagania dotyczące wydajności oraz koszty.

5. Plany ciągłości działania są opracowywane w celu wspierania wdrażania zatwierdzonych strategii i są zgodne z wymogami polityki.

5.1. Plany ciągłości działania są opracowywane w celu identyfikacji następujących pozycji: Krytyczne usługi, zasoby informacyjne i zależności zidentyfikowane w analizie wpływu biznesowego; Zatwierdzone strategie ciągłości i odzyskiwania danych; Środki radzenia sobie z wpływem i skutkami zakłóceń; Zespoły reagowania i odzyskiwania danych, w tym skład i informacje kontaktowe; Role, obowiązki i zadania zespołów, w tym interesariuszy wewnętrznych i zewnętrznych, oraz jasno określone stanowiska funkcyjne i zastępstwa; Zasoby i procedury zapewniające ciągłość świadczenia usług; Mechanizmy i procedury koordynacji i raportowania, w tym procesy współpracy z innymi departamentami, agencjami i służbami interwencyjnymi, w razie potrzeby w celu koordynacji planu ciągłości działania; Uprawnienia do aktywacji planu ciągłości działania; Centra Operacji Kryzysowych na wszystkich poziomach (lokalnym, regionalnym i krajowym); oraz Procedury ewakuacji i schronienia na miejscu.

5.2. Wszystkie pojedyncze punkty awarii zostały zidentyfikowane i uwzględnione w planach ciągłości działania.

5.3. Opracowywane są odpowiednie plany komunikacji i materiały wspierające komunikację kryzysową z pracownikami, partnerami biznesowymi, dostawcami, rządem, mediami zewnętrznymi i innymi kluczowymi interesariuszami.

5.4. Kierownictwo wyższego szczebla dokonuje przeglądu, zatwierdza i finansuje wybrane plany ciągłości działania, w tym przegląda i zatwierdza plany osób trzecich.

5.5. Plany ciągłości działania są dostępne w łatwo dostępnych lokalizacjach i formatach na wypadek wystąpienia zakłóceń.

6. Podjęto działania w celu zapewnienia, że plany mogą zostać wprowadzone w życie, a w razie potrzeby zawierane są formalne umowy lub porozumienia.

6.1. Wszystkie niezbędne działania zostały zakończone i sformalizowane w celu zapewnienia, że plany mogą zostać wprowadzone w życie, a tam, gdzie to konieczne, zawarto umowy lub porozumienia w celu sformalizowania sposobu postępowania i ustalenia komu przysługuje priorytet dostępu.

6.2. W przypadkach, gdy departamenty i/lub osoby trzecie współuczestniczą w świadczeniu usługi krytycznej, istnieją rozwiązania zapewniające spójność planów opracowywanych przez te podmioty.

Utrzymanie gotowości programu planowania ciągłości działania

7. Wdrożono skuteczny program szkoleń i podnoszenia świadomości w zakresie planu ciągłości działania.

7.1. Koordynator ds. planowania ciągłości działania departamentu został odpowiednio przeszkolony do pełnienia przypisanych mu funkcji i obowiązków.

7.2. Wdrożono odpowiedni program szkoleń i podnoszenia świadomości w zakresie planu ciągłości działania (w tym szkoleń przekrojowych), jest on udokumentowany, obejmuje plan szkoleń i podnoszenia świadomości oraz został przeprowadzony na wszystkich poziomach organizacji.

7.3. Szkolenia z zakresu planu ciągłości działania (w tym szkolenia przekrojowe) i podnoszenie

świadomości są stale wzmacniane, okresowo weryfikowane i podlegają walidacji.

8. Plany ciągłości działania są regularnie poddawane przeglądom i aktualizowane.

8.1. Istnieją procesy zapewniające, że plany ciągłości działania są aktualizowane i zatwierdzane pod kątem wszelkich zmian, takich jak: listy kontaktów, nowe programy, ramy planowania strategicznego, zmiany legislacyjne i fizyczne relokacje, oraz corocznie weryfikowane przez kierownictwo i koordynatora ds. planowania ciągłości działania.

8.2. Aktualny wykaz krytycznych usług i powiązanych informacji, zasobów i zależności jest utrzymywany i dostarczany do Departamentu Bezpieczeństwa Publicznego Kanady na żądanie.

9. Plany ciągłości działania są regularnie testowane poprzez sprawdzenie w praktyce i zatwierdzane w celu zapewnienia efektywnego i skutecznego reagowania i odzyskiwania danych.

9.1. Testowanie i zatwierdzanie wszystkich planów odbywa się regularnie i obejmuje testy warunków skrajnych (stress testing) oraz dokumentację sprawdzeń.

9.2. Po wszystkich sprawdzeniach i po każdym zakłóceniu przygotowywany jest raport z (podjętych) działań i plan dalszego działania, a plany dalszego działania zostały zatwierdzone przez kadrę kierowniczą wyższego szczebla i wdrożone.

9.3. Plany ciągłości działania są korygowane w celu odzwierciedlenia zaobserwowanych wniosków.

10. Tam, gdzie jest to konieczne, zapewnia się Centra Operacji Kryzysowych (EOC) i lokalizacje alternatywne oraz utrzymuje się je w stanie gotowości.

10.1. Istnieją procedury zapewniające pozyskiwanie i utrzymywanie awaryjnych dostaw i zasobów dla Centrów Operacji Kryzysowych i lokalizacji alternatywnych.

11. Koordynator ds. planowania ciągłości działania departamentu monitoruje wszystkie działania w ramach programu planowania ciągłości działania, w tym analizę wpływu biznesowego, plan ciągłości działania, ćwiczenia, raporty z działań oraz programy szkoleniowe i podnoszące świadomość.

11.1. Koordynator ds. planowania ciągłości działania departamentu dokonuje przeglądu wszystkich analiz wpływu biznesowego w celu zapewnienia kompletności uzasadnień i specyfikacji (MSL, MAD, RTO i RPO).

11.2. Koordynator ds. planowania ciągłości działania departamentu dokonuje przeglądu wszystkich planów ciągłości działania w celu zapewnienia kompletności i aktualności treści.

11.3. Koordynator ds. planowania ciągłości działania departamentu sprawdza wszystkie materiały ćwiczeniowe i raporty z działań pod kątem ich stosowności i kompletności.

11.4. Koordynator ds. planowania ciągłości działania departamentu monitoruje działania szkoleniowe i podnoszące świadomość, aby zweryfikować, czy zostały one przeprowadzone zgodnie z harmonogramem.

Źródło: Zmodyfikowano na podstawie dokumentu Departamentu Bezpieczeństwa Publicznego Kanady (2016[26]), Audyt programu planowania ciągłości działania, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-bsnss-cntnty-plnnng-prgrm/2016-bsnss-cntnty-plnnng-prgrm-en.pdf.

Zalecenia

Podobnie jak w przypadku ogólnych zasad audytu, związek między ustaleniami, wnioskami i zaleceniami musi być dostatecznie zrozumiany (wyjaśniony). Niezbędne jest opracowanie zaleceń mających na celu skorygowanie niedociągnięć w planie ciągłości działania jednostki. Plan ciągłości działania ma istotne

znaczenie, a zatem zalecenia powinny być konkretne, mierzalne, wskazujące osoby odpowiedzialne, istotne i określone w czasie. Powinny one odnosić się do przyczyn niedociągnięć i wspierać poprawę programów, działania i osiąganych wyników. Ogólnie rzecz biorąc zalecenia powinny mieć na celu wyeliminowanie lub zmniejszenie rozbieżności między dowodami a kryteriami audytu (INTOSAI, 2019[18]). Ramka 3.5 opisuje przykład zalecenia odnoszącego się do audytu zarządzania ciągłością działania.

Ramka 3.5. Przykład zaleceń

Wspólna Jednostka Kontrolna ONZ – Zarządzanie ciągłością działania w organizacjach systemu Narodów Zjednoczonych (2021 r.)

- Zalecenia:
  - Dokonać przeglądu swoich ram zarządzania ciągłością działania i upewnić się, że podstawowe elementy określone w niniejszym raporcie zostały ustanowione i są przypisane odpowiednim interesariuszom, aby umożliwić skuteczną koordynację procesów i praktyk w zakresie ciągłości działania, budować spójność w ich wdrażaniu i promować odpowiedzialność na wszystkich poziomach.
  - Zapewnić że elementy utrzymania, ćwiczenia i przeglądu ich planów ciągłości działania są stosowane w sposób spójny i zdyscyplinowany w celu potwierdzenia, że plany pozostają odpowiednie (adekwatne) i skuteczne.
  - Wzmocnienie mechanizmów uczenia się w celu zwiększenia odporności organizacyjnej poprzez wprowadzenie wymogu dokonywania przeglądów z działań zakłócających funkcjonowanie oraz okresowych przeglądów wewnętrznych ram zarządzania ciągłością działania.
  - Przekazywanie raportów ich organom ustawodawczym i zarządzającym na temat postępów we wdrażaniu polityki dotyczącej systemu zarządzania odpornością organizacyjną i jej zaktualizowanych wskaźników wydajności oraz podkreślanie dobrych praktyk i wyciągniętych wniosków, zwłaszcza w obszarze zarządzania ciągłością działania.
  - Przeprowadzanie wewnętrznej oceny zarządzania ciągłością operacji biznesowych podczas pandemii COVID-19 w celu zidentyfikowania luk, podatności, dobrych praktyk i wyciągniętych wniosków oraz dostosowania polityk, procesów i procedur, w szczególności w obszarach, takich jak: zasoby ludzkie, zarządzanie technologiami informacyjno-komunikacyjnymi oraz bezpieczeństwo i higiena pracy, a także wskazanie niezbędnych środków w celu lepszego przygotowania się na przyszłe zakłócające incydenty i reagowania na nie.
  - Przy najbliższej okazji powinno się rozważyć wnioski z wewnętrznej oceny zarządzania ciągłością działania podczas pandemii COVID-19 przygotowanej przez dyrektorów wykonawczych swoich organizacji i na tej podstawie podjąć odpowiednie decyzje w celu wyeliminowania zidentyfikowanych luk i zagrożeń oraz zapewnienia ciągłości działania.

Źródło: (UN JIU, 2021[31]).

Raportowanie

Ogólne zasady obowiązujące w odniesieniu do sprawozdania z audytu można zastosować do raportowania audytu planowania ciągłości działania. Sprawozdanie z audytu powinno być kompleksowe, przekonujące, aktualne, przyjazne dla czytelnika i wyważone. Powinno zawierać wszystkie niezbędne informacje w zakresie celu audytu i pytań, przedstawiać przekonującą argumentację, powinno być

przygotowane na czas, napisane prostym i jasnym językiem oraz ma przedstawiać dowody audytu w sposób bezstronny. Zgodnie z opisem zawartym w rozporządzeniu[5] struktura raportu powinna obejmować następujące sekcje: temat i cel, zakres, data rozpoczęcia, ustalenia i ocenę według kryteriów, zalecenia, ewentualne zastrzeżenia, ogólną ocenę kontroli zarządczej, data i nazwisko(a) audytora wewnętrznego (w tym podpis(y)). Procedury kontroli jakości powinny być zintegrowane z procesem audytu, aby zapewnić spójność i dokładność. Ustalenia audytu powinny zostać omówione z audytowanymi przed sfinalizowaniem raportu. Dzięki tej współpracy zalecenia zostaną sfinalizowane, a raport powinien zostać przekazany wszystkim interesariuszom.

W odniesieniu do raportu z audytu planowania ciągłości działania należy zwrócić uwagę na następujące kwestie:

- Zapewnienie terminowości raportu z audytu. Biorąc pod uwagę rosnące ryzyko kryzysów, kluczowe znaczenie ma zapewnienie odpowiedniej terminowości (dostarczenia raportu na czas).
- Ponieważ plan ciągłości działania jest częścią pakietu zarządzania kryzysowego, należy upewnić się, że zalecenia audytu są jasne i możliwe do wykonania.
- Należy upewnić się, że raport zawiera szczegółowy przegląd zagrożeń cyfrowych i ich potencjalnego wpływu na ciągłość działania.
- Należy podkreślić wszelkie luki w zarządzaniu ryzykiem cyfrowym organizacji i zalecane ulepszenia.
- Należy upewnić się, że plan ciągłości działania jest dostosowany do zmian w środowisku operacyjnym, w tym zmian w operacjach IT, cyberzagrożeń i cyfryzacji.
- Należy pamiętać, aby uwzględnić analizę efektywności i skuteczności alokacji zasobów związanych z planem ciągłości działania, w tym zasobów finansowych, ludzkich i technologicznych.
- Należy pamiętać, aby uwzględnić ocenę zgodności planu ciągłości działania z odpowiednimi przepisami prawa, regulacjami i standardami, szczególnie w czasach kryzysu.

Kompetencje wspierające audytorów w cyfryzacji

Istnieje kilka kompetencji wymaganych do wspierania audytorów w erze cyfrowej. Niezależnie od tego, czy tematem są plany ciągłości świadczenia usług publicznych, czy inne powiązane tematy, funkcje audytu wewnętrznego muszą zapewnić, że ich audytorzy posiadają niezbędną wiedzę i umiejętności do skutecznego przeprowadzania audytów i innych przeglądów. Możliwe umiejętności, na które należy położyć szczególny nacisk, obejmują (Chartered Institute of Internal Auditors, 2023[13]):

- Elastyczność: transformacje cyfrowe zachodzą we wszystkich programach realizowanych we wszystkich instytucjach rządowych. Wszyscy audytorzy muszą być w stanie pracować w środowisku, które jest elastyczne. Wszyscy zaangażowani muszą być gotowi do zdobywania nowej wiedzy w związku z zachodzącymi zmianami.
- Zdolności analityczne: audytorzy muszą posiadać wiedzę na temat technik analizy przyczyn źródłowych (np. metoda 5 why, analiza drzewa błędów itp.). Jest to podstawowa umiejętność przeprowadzania audytów, która jest wykorzystywana do rozwiązywania kluczowych kwestii związanych z zadaniem audytowym.

[5] §18 Rozporządzenia Ministra Finansów w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu.

- Kodowanie: posiadanie umiejętności związanych z kodowaniem nie powinno być już zdolnością wyjątkową, ale raczej wymogiem na poziomie minimalnym. Podstawowe kodowanie staje się niezbędną umiejętnością w rozmowach z informatykami i innymi nowymi pracownikami.
- Wspieranie współpracy: w erze cyfrowej umiejętność współpracy jest ważną i pożądaną umiejętnością. Obejmuje ona zarządzanie spotkaniami online, małymi grupami i/lub warsztatami. Te umiejętności interpersonalne są niezbędne dla wszystkich audytorów w środowisku, które obejmuje spotkania w przestrzeni wirtualnej.
- Inicjatywa: środowiska pracy zmieniają się na całym świecie. Audytorzy w pewne dni fizycznie przebywający w towarzystwie współpracowników (dzięki modelu pracy hybrydowej i telepracy) powinni mieć możliwość wykorzystania swoich umiejętności podczas osobistych spotkań z audytowanymi, obserwowania praktyk i poznawania doświadczeń kulturowych.
- Prezentowanie: audytorzy powinni posiadać umiejętność przekazywania i prezentowania informacji różnym grupom. Ponieważ koncepcja raportowania stale ewoluuje, zdolność właściwej prezentacji informacji interesariuszom jest umiejętnością niezbędną dla wszystkich audytorów.

Odniesienia

ANAO (2014), *Business Continuity Management*, https://www.anao.gov.au/sites/default/files/ANAO_Report_2014-2015_06.pdf (accessed on 26 April 2024). [22]

Business Development Canada (n.d.), *8 steps for planning your emergency and disaster plan*, Strategy and Planning, https://www.bdc.ca/en/articles-tools/business-strategy-planning/manage-business/business-continuity-8-steps-building-plan (accessed on 31 July 2024). [16]

Chartered Institute of Internal Auditors (2023), *Impact of digitisation on the internal audit activity*. [13]

CISA GOV (2024), *Cybersecurity Best Practices*, https://www.cisa.gov/topics/cybersecurity-best-practices (accessed on 28 April 2024). [30]

European Union (2022), *DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities*, https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed on 13 October 2024). [17]

Everest, D. et al. (2008), *Business Continuity Management*, The Institute of Internal Auditors, https://iiabrasil.org.br/korbilload/upl/ippf/downloads/businesscontinu-ippf-00000001-24012018114224.pdf. [23]

FEMA (2023), *Federal Continuity Directive*, https://www.fema.gov/sites/default/files/documents/fema_federal-continuity-directive-planning-framework.pdf (accessed on 31 July 2024). [3]

FEMA (2010), *Developing and Maintaining Emergency Operations Plans*, https://www.fema.gov/sites/default/files/2020-05/CPG_101_V2_30NOV2010_FINAL_508.pdf (accessed on 28 April 2024). [29]

FEMA Office of National Continuity Programs (2023), *Federal Continuity Directive Continuity Planning Framework for the Federal Executive Branch*. [5]

Health Canada (2022), *Audit of Business Continuity Plans for Critical Services*, https://www.canada.ca/content/dam/hc-sc/documents/corporate/transparency/corporate-management-reporting/internal-audits/business-continuity-plans-critical-services/business-continuity-plans-critical-services-en.pdf (accessed on 31 July 2024). [24]

IIA (2024), *The Definition of Internal Auditing*, What are the Standards, https://www.theiia.org/en/standards/what-are-the-standards/definition-of-internal-audit/ (accessed on 7 February 2024). [1]

IIA (2019), *GTAG 3: Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance*, https://www.theiia.org/en/content/guidance/recommended/supplemental/gtags/gtag-continuous-auditing/ (accessed on 28 April 2024). [21]

Indigenous and North Affairs Canada (2017), *Audit of Business Continuity Planning*, [25]

https://www.rcaanc-cirnac.gc.ca/DAM/DAM-CIRNAC-RCAANC/DAM-AEV/STAGING/texte-text/au_bucp_1513259607995_eng.pdf (accessed on 31 July 2024).

INTOSAI (2019), *ISSAI 300 Performance Audit Principles*, https://www.intosai.org/fileadmin/downloads/documents/open_access/ISSAI_100_to_400/issai_300/ISSAI_300_en_2019.pdf (accessed on 7 February 2024). [18]

INTOSAI (2016), *Disaster Risk Reduction - Business Continuity Planning (2013)*, [20]

ISACA (2024), *Effective IT Governance at your Fingertips*, https://www.isaca.org/resources/cobit (accessed on 28 April 2024). [28]

ISO (2019), *ISO 22301:2019 Business continuity management systems Requirements*, International Organization for Standardization, https://www.iso.org/standard/75106.html (accessed on 28 April 2024). [2]

Kuhfeld, M. et al. (2022), "The pandemic has had devastating impacts on learning. What will it take to help students catch up?", *Brookings*, https://www.brookings.edu/articles/the-pandemic-has-had-devastating-impacts-on-learning-what-will-it-take-to-help-students-catch-up/ (accessed on 13 May 2024). [8]

OECD (2024), *PISA 2022 Results (Volume IV): How Financially Smart Are Students?*, PISA, OECD Publishing, Paris, https://doi.org/10.1787/5a849c2a-en. [7]

OECD (2024), *Poland*, OECD Going Digital Toolkit, https://goingdigital.oecd.org/countries/pol (accessed on 31 July 2024). [11]

OECD (2021), *Global Scenarios 2035: Exploring Implications for the Future of Global Collaboration and the OECD*, OECD Publishing, Paris, https://doi.org/10.1787/df7ebc33-en. [10]

OECD (2020), *OECD Public Integrity Handbook*, OECD Publishing, Paris, https://doi.org/10.1787/ac8ed8e8-en. [14]

OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, https://doi.org/10.1787/9789264312012-en. [9]

OECD (2014), "Recommendation of the Council on the Governance of Critical Risks", *OECD Legal Instruments*, OECD/LEGAL/0405, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0405. [4]

Public Safety Canada (2016), *Audit of Business Continuity Planning Program*, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-bsnss-cntnty-plnnng-prgrm/2016-bsnss-cntnty-plnnng-prgrm-en.pdf (accessed on 31 July 2024). [26]

UK Government (n.d.), *How prepared are you?*, https://assets.publishing.service.gov.uk/media/5a7b283de5274a34770e9d01/Business_Continuity_Managment_Toolkit.pdf (accessed on 31 July 2024). [15]

UN (2020), *The role of public service and public servants during the COVID-19 pandemic*, https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-79-the-role-of-public-service-and-public-servants-during-the-covid-19-pandemic/ (accessed on 31 July 2024). [6]

UN JIU (2021), *Business continuity management in United Nations system organizations*, https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_6_english_2.pdf (accessed on [31]

26 April 2024).

United Nations Department of Economic and Social Affairs (2022), *The Future of Digital Government: Trends, Insights and Conclusions*, https://www.un-ilibrary.org/content/books/9789210019446c010/read (accessed on 9 April 2024). [12]

US GAO (2014), *Standards for Internal Control in the Federal Government*, https://www.gao.gov/assets/gao-14-704g.pdf (accessed on 28 April 2024). [19]

US NIST (2020), *Security and Privacy Controls for Information Systems and Organizations*, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (accessed on 28 April 2024). [27]

Słownik pojęć

Terminy z definicjami

Termin	Definicja
Analiza wpływu biznesowego (BIA)	Proces określania krytyczności działań organizacyjnych i związanych z nimi wymagań dotyczących zasobów w celu zapewnienia odporności operacyjnej i ciągłości działania w trakcie i po zakłóceniu działalności.
Digitalizacja	Umieszczanie informacji w formie cyfrowej, która może być wykorzystywana przez komputery i inny sprzęt elektroniczny.
Cyfryzacja	Wykorzystanie technologii cyfrowych do zmiany formy organizacji pracy i zapewnienia możliwości nowych działań i możliwości produkcyjnych.
Centra Operacji Kryzysowych (EOC)	Centralna „struktura koordynacyjna" dowodzenia i kontroli odpowiedzialna za zarządzanie reagowaniem w sytuacji wyjątkowej, gotowością na wypadek sytuacji wyjątkowej, zarządzaniem sytuacjami wyjątkowymi i funkcjami zarządzania klęskami żywiołowymi na poziomie strategicznym podczas sytuacji wyjątkowej.
Technologie informacyjne i komunikacyjne (ICT)	Rozszerzony termin dla technologii informatycznej (IT), który podkreśla rolę ujednoliconej komunikacji i integracji telekomunikacji (linii telefonicznych i sygnałów bezprzewodowych) i komputerów, a także niezbędnego oprogramowania korporacyjnego, oprogramowania pośredniczącego, pamięci masowej i audiowizualnego, które umożliwiają użytkownikom dostęp, przechowywanie, przesyłanie, zrozumienie i manipulowanie informacjami.
Maksymalny Dopuszczalny Czas Przestoju (MAD)	Absolutnie najdłuższy czas przestoju, jaki organizacja może tolerować przed poniesieniem poważnych konsekwencji.
Minimalne Poziomy Usług (MSL)	Poziom, do którego proces musi zostać przywrócony w okresie przywracania działania: przywrócenie normalnego poziomu usług może zostać odłożone na później.
Docelowy Punkt Odtworzenia (RPO)	Wiek plików, które muszą zostać odzyskane z kopii zapasowej w celu wznowienia normalnych operacji w przypadku awarii komputera, systemu lub sieci w wyniku awarii sprzętu, programu lub komunikacji.
Docelowy Czas Odtworzenia (RTO)	Maksymalny tolerowany czas, przez jaki komputer, system, sieć lub aplikacja mogą nie działać po wystąpieniu awarii lub katastrofy.