PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Ciągłość działania w działalności sektora publicznego

Tadeusz Zawistowski

Zawistowski consultions

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Program webinarium

1. Ciągłość działania – wprowadzenie
2. Wymagania, w tym przepisy prawa dotyczące ciągłości działania
3. System zarządzania ciągłością działania
4. Norma PN-EN ISO 22301:2020-04
5. Doświadczenie w zakresie wdrażania i stosowania rozwiązań z zakresu ciągłości działania

Zawistowski consultions

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Ciągłość działania – wprowadzenie

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Ciągłość działania

- zdolność organizacji do ciągłego dostarczania wyrobów i usług w akceptowalnych ramach czasowych przy zdefiniowanej wcześniej zdolności do działania w czasie zakłócenia,

PN-EN ISO 22301:2020-04

- zarządzanie ciągłością działania – holistyczny proces zarządzania, identyfikujący potencjalne zagrożenia dla organizacji i skutki, jakie te zagrożenia mogą wywołać w przypadku ich wystąpienia, który zapewnia ramowe struktury budowania odporności organizacji i umożliwia skuteczną reakcję w celu ochrony interesów jej kluczowych interesariuszy, jej reputacji, marki i działalności kreujących wartość

PN-EN ISO 22300:2018-07

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Definicje
PN-EN ISO 22301:2020-04

- **Działanie** – zestaw obejmujący jedno zadanie lub więcej zadań z określonym wyjściem
- **Proces** – zbiór działań wzajemnie powiązanych lub wzajemnie oddziałujących, który przekształca dane wejściowe w dane wyjściowe
- **Zakłócenie** – incydent, przewidywane lub niespodziewane zdarzenie, powodujące nieplanowane, negatywne odchylenie od oczekiwanego dostarczenia wyrobów i usług zgodnego z celami organizacji
- **Incydent** – zdarzenie, które może dotyczyć lub może doprowadzić do zakłócenia, straty, nagłego wypadku lub kryzysu
- **Wpływ** – wynik zakłócenia mający wpływ na cele
- **Zasób** – wszystkie aktywa (w tym urządzenia i wyposażenie), ludzie, umiejętności, technologie, pomieszczenia, zapasy i informacje (elektroniczne i nieelektroniczne), których dostępności organizacja potrzebuje w celu prowadzenia działania i osiągania celu

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Parametry

- maksymalny akceptowalny przestój / przerwa w dostawie – **MAO**
- maksymalny tolerowany okres zakłócenia – **MTPD** – czas, po którym niekorzystne skutki powstałe w wyniku niedostarczenia wyrobu lub usług albo nierealizowania działalności stają się nieakceptowalne

  (Maximum Acceptable Outage)

  (Maximum Tolerable Period of Disruption)

PN-EN ISO 22300:2018-07

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Parametry

- docelowy punkt odtworzenia danych – **RPO** – punkt w czasie, z którego informacja używana przez konkretną działalność musi być przywrócona aby umożliwić tej działalności wznowienie funkcjonowania
  - (Recovery Point Objective)

- czas wznowienia działania – **RTO** – okres następujący po incydencie, w czasie którego:
  - wyrób lub usługa musi zostać ponownie dostarczona lub
  - działalność musi zostać wznowiona lub
  - zasoby muszą być odtworzone

- W przypadku wyrobów, usług i działalności docelowy czas wznowienia działalności musi być krótszy niż czas, po którym niekorzystne skutki powstałe w wyniku niedostarczenia wyrobu lub usług albo niewykonania działalności stają się nieakceptowalne.
  - (Recovery Time Objective)

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Wymagania, w tym przepisy prawa dotyczące ciągłości działania

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Wymagania

Konstytucja:

- „(…) pragnąc na zawsze **zagwarantować prawa obywatelskie, a działaniu instytucji publicznych zapewnić rzetelność i sprawność,** w poczuciu odpowiedzialności przed Bogiem lub przed własnym sumieniem, ustanawiamy Konstytucję Rzeczypospolitej Polskiej jako prawa podstawowe dla państwa (…)”

Art. 8. KPA § 1.:

- Organy administracji publicznej **prowadzą postępowanie w sposób budzący zaufanie** jego uczestników do władzy publicznej, kierując się zasadami proporcjonalności, bezstronności i równego traktowania.

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Wymagania prawne

- Standard kontroli zarządczej;
- Rozporządzenie w sprawie KRI;
- RODO;
- Rozporządzenie w sprawie BIP;
- KPA;
- Przepisy regulujące terminy realizacji usług publicznych, jak również innych działań;
- Przepisy regulujące zagadnienia wspomagające, techniczne i organizacyjne.

Zawistowski consultans

Standard kontroli zarządczej

Ciągłość działalności:

- Należy zapewnić istnienie mechanizmów służących utrzymaniu ciągłości działalności jednostki sektora finansów publicznych wykorzystując, między innymi, wyniki analizy ryzyka.

Rozporządzenie w sprawie KRI

- Zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, **uszkodzeniami lub zakłóceniami**;
- Zabezpieczenie informacji w sposób uniemożliwiający nieuprawnione jej ujawnienie, modyfikacje, **usunięcie lub zniszczenie**;
- Zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom **bezpieczeństwa informacji**; (integralność i dostępność);
- Zapewnienie odpowiedniego poziomu **bezpieczeństwa** w systemach teleinformatycznych.

(odwołanie do PN-ISO/IEC 24762 - Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie)

- norma wycofana

RODO

Wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić:

- zdolność do **ciągłego zapewnienia** poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- zdolność do **szybkiego przywrócenia** dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

- Informowanie o naruszeniach – **72 h**.

BIP

- W przypadku awarii, brak dostępności strony głównej BIP dla odwiedzającego stronę nie powinien być dłuższy niż 8 godzin.

- W przypadku awarii, brak dostępności strony podmiotowej BIP dla odwiedzającego stronę **nie powinien być dłuższy niż 24 godziny.**

KPA

- Art.12.§1. Organy administracji publicznej powinny działać w sprawie wnikliwie i szybko, posługując się możliwie najprostszymi środkami prowadzącymi do jej załatwienia.
- §2. Sprawy, które nie wymagają zbierania dowodów, informacji lub wyjaśnień, powinny być **załatwione niezwłocznie**.

- Art.35.§1. Organy administracji publicznej obowiązane są załatwiać sprawy bez zbędnej zwłoki.
- §3. Załatwienie sprawy wymagającej postępowania wyjaśniającego powinno nastąpić **nie później niż w ciągu miesiąca**, a sprawy szczególnie skomplikowanej – **nie później niż w ciągu dwóch miesięcy od dnia wszczęcia postępowania**, zaś w postępowaniu odwoławczym – w ciągu miesiąca od dnia otrzymania odwołania.

KSC

- Podmiot publiczny zgłasza incydent **niezwłocznie, nie później niż w ciągu 24 godzin** od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

- Incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Ustawa o zarządzaniu kryzysowym

- Sytuacja kryzysowa – sytuacja wpływająca negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołująca znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków.

- Zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na:
  - zapobieganiu sytuacjom kryzysowym,
  - przygotowaniu do przejmowania kontroli nad sytuacjami kryzysowymi w drodze zaplanowanych działań,
  - reagowaniu w przypadku wystąpienia sytuacji kryzysowych,
  - usuwaniu ich skutków oraz
  - odtwarzaniu zasobów i infrastruktury krytycznej.

Zawistowski consultions

Ustawa o zarządzaniu kryzysowym

- Infrastruktura krytyczna obejmuje systemy:
- (…)
- zapewniające ciągłość działania administracji publicznej,

- Zespół zarządzania kryzysowego (określenie składu, miejsca i trybu pracy),
- Centra zarządzania kryzysowego,

- Raport o zagrożeniach bezpieczeństwa narodowego,
- Plan Zarządzania Kryzysowego na poziomie Ministra,
- Krajowy Plan Zarządzania Kryzysowego,
- Narodowy Program Ochrony Infrastruktury Krytycznej.

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Inne przepisy

- Przepisy dotyczące bezpieczeństwa i higieny pracy, ochrony pożarowej i prawo budowlane
- Ustawa o dostępie do informacji publicznej
- Ustawa o rachunkowości
- (…)

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

System zarządzania ciągłością działania (SZCD)

Zawistowski consultans

SZCD

System zarządzania – powiązane lub oddziałowujące elementy organizacji ustanawiające politykę i cele oraz procesy do ich osiągania

System, na który składają się m.in.:

- Polityka,
- Cele,
- Struktura organizacyjna,
- Zadania, odpowiedzialności i uprawnienia,
- Procesy m.in. planowania i działań operacyjnych,
- Dokumentacja,
- Zasoby,
- Ustalone sposoby postępowania,
- (…).

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

SZCD

- Podejście systemowe (uwzględnia wszystkie kluczowe aspekty)
- Zapewnienie kompleksowego i całościowego podejścia w oparciu o PDCA
- Wyposażenie w narzędzia
- Oparte na zwalidowanych rozwiązaniach
- Model otwarty

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Norma
PN-EN ISO 22301:2020-04

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Struktura normy

1. Zakres normy
2. Powołania normatywne
3. Terminy i definicje
4. Kontekst organizacji
5. Przywództwo
6. Planowanie
7. Wsparcie
8. Działania operacyjne
9. Ocena efektów działania
10. Doskonalenie

Zawistowski consultions

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

BIA

- **B**usiness **I**mpact **A**nalysis
- Analiza wpływu biznesowego

- proces analizy wpływu w czasie zakłócenia na organizację

- Analizujemy skutek wynikający z przerwania ciągłości działania w określonych przedziałach czasowych odnosząc się do wpływu na np.:
  - bezpieczeństwo (życie lub zdrowie),
  - spełnienie wymagań prawnych (w tym zapewnienia usług),
  - zaufanie,
  - jakość,
  - finanse,
  - cele.

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Dokumentacja CD

- Strategia ciągłości działania
- Plan/plany ciągłości działania
- Procedury ciągłości działania
- Procedury działania w sytuacji kryzysowej/ zakłócenia
- Procedury odtworzeniowe
- Procedury przywrócenia normalnej działalności
- Procedury informowania lub ostrzegania
- Wykaz zasobów
- Scenariusz testów
- Plan testów

- Regulamin pracy
- Regulamin organizacyjny
- Procedury operacyjne

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Doświadczenie w zakresie wdrażania i stosowania rozwiązań z zakresu ciągłości działania

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Dobre praktyki

- Powiązanie ciągłości działania z oceną ryzyka w zakresie KZ i BI
- Strategia ciągłości działania
- Plany i procedury odtworzeniowe w obszarze IT
- Wprojektowanie alternatywnych sposobów działania w przypadku zakłócenia w procesy i procedury
- Powiązanie ciągłości działania z zarządzaniem kryzysowym
- Rozwiązania organizacyjno-prawne zapewaniające elastyczność i możliwość działania w sytuacji wystąpienia zakłócenia
- Koordynator/ Zespół ds. CD

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Problemy i błędy

- Nie zdefiniowane usługi/ produkty i ich standardy
- Brak rozumienia /stosowania podejścia procesowego
- Istotne jest to, co jest ważne z punktu widzenia bieżącego interesu politycznego
- Ograniczone środki finansowe
- Konflikt i brak właściwego zrozumienia relacji prawo a zarządzenie
- Wdrożenie rozwiązań w procesach wspomagających z pominięciem procesów operacyjnych
- Postrzeganie CD wyłącznie przez pryzmat wybranych zagadnień zazwyczaj IT i siatki zastępstw
- Obawa przed zarzutem niegospodarności (nadmiarowość)
- Niewłaściwe podejście do strat finansowych (m.in. przez pryzmat celu organizacji a nie Skarbu Państwa, bez uwzględnienia kosztów „postoju")
- Subiektywna ocena istotności
- Założenie, że rozwiązania z zakresu zarzadzania kryzysowego są wystarczające
- Braki w świadomości i kompetencjach
- Organizacja jako luźna federacja mało powiązanych departamentów

Zawistowski consultans

PROGR@M
WIEDZA I UMIEJĘTNOŚCI
= KOMPETENCJE

Dziękuję za uwagę!

Kontakt:

- tadeusz@tz-c.pl
- https://www.tz-c.pl/
- https://www.linkedin.com/company/38092846/

Zawistowski consultans