

AUDYT ZARZĄDZANIA CIĄGŁOŚCIĄ DZIAŁANIA NA PODSTAWIE ISO 22301:2012

PODSTAWOWE ZAGADNIENIA ORAZ DEFINICJE W ISO 22301



PODSTAWOWE ZAGADNIENIE - RYZYKO

- ✘ Zastosowanie wytycznych ISO 22313 dla ciągłości działania oraz wytycznych **ISO 31000** do zarządzania ryzykiem
- ✘ **Ryzyko** – skutek niepewności w odniesieniu do celów

CIĄGŁOŚĆ DZIAŁANIA OPARTA O ISO 22301

- ✗ ISO 22301 określa, co musi być zrobione; właściwie udokumentowany system zarządzania ciągłością działania opisuje, jak wymagane procesy muszą zostać zrealizowane.
- ✗ Wymaga audytów wewnętrznych
- ✗ Poddaje weryfikacji efektywne zarządzanie
- ✗ Zapewnia, że organizacja w pełni nadzoruje swoje działania



ZAWARTOŚĆ ISO 22301

W KONTEKŚCIE CYKLU PDCA

- ✗ 0 Wstęp
- ✗ 1 Zakres
- ✗ 2 Referencje normatywne
- ✗ 3 Terminy i definicje

PLAN

- ✗ 4 Kontekst organizacji
- ✗ 5 Przywództwo
- ✗ 6 Planowanie
- ✗ 7 Wsparcie

DO

- ✗ 8 Funkcjonowanie

CHECK

- ✗ 9 Ocena funkcjonowania

ACT

- ✗ 10 Doskonalenie



ISO 22301 – 3. Terminy i definicje

TERMINY I DEFINICJE (WYBÓR)

- ✘ **Działanie** – proces lub zbiór procesów realizowanych przez organizację lub w jej imieniu, które tworzą lub wspierają jeden lub więcej produktów/usług
- ✘ **Ciągłość działania** – zdolność organizacji do ciągłego dostarczania produktów lub usług na akceptowalnym, wcześniej zdefiniowanym poziomie, po wystąpieniu incydentu zakłócającego
- ✘ **Zarządzanie ciągłością działania** - holistyczny proces zarządzania, identyfikujący potencjalne zagrożenia organizacji i skutki, jakie te zagrożenia mogą wywierać na działalność w przypadku ich wystąpienia, który zapewnia kształtowanie odporności organizacji i umożliwia skuteczną reakcję w celu ochrony interesów kluczowych interesariuszy, jej reputacji, marki i działalności kreującej wartości

TERMINY I DEFINICJE (WYBÓR)

- ✗ **Plan ciągłości działania** - udokumentowane procedury, które po wystąpieniu zakłócenia wspierają organizację w reagowaniu, uzyskiwaniu sprawności, oraz odbudowie działania na wcześniej zdefiniowanym poziomie operacyjnym
- ✗ **Program ciągłości działania** - procesy ciągłego zarządzania oraz ładu korporacyjnego, wspierane przez najwyższe kierownictwo oraz odpowiednie zasoby w celu wdrożenia i utrzymania zarządzania ciągłością działania
- ✗ **Incydent** – sytuacja, która może prowadzić lub mogłaby doprowadzić do przerwania działania, straty, niebezpieczeństwa lub kryzysu
- ✗ **Analiza wpływu na działanie (business impact analysis BIA)** – proces analizy działań oraz skutków, jakie przerwanie tych działań może spowodować

TERMINY I DEFINICJE (WYBÓR)

- ✗ **Maksymalny akceptowalny przestój (maximum acceptable outage MAO), *lub* Maksymalny dopuszczalny czas zakłócenia (maximum tolerable period of disruption MTPD)** – czas, po którym w przypadku niepożądanego zdarzenia skutki nie dostarczania produktu/usługi stają się nieakceptowalne
- ✗ **Minimalne cele ciągłości działania (minimum business continuity objective MBCO)** – minimalny poziom usług lub produktów, który jest akceptowalny przez organizację dla osiągnięcia celów jej działalności w trakcie wystąpienia zakłócenia
- ✗ **Działania priorytetowe (prioritized activities)** – działania, którym w przypadku wystąpienia incydentu musi być nadany priorytet w celu zminimalizowania skutków

TERMINY I DEFINICJE (WYBÓR)

- ✖ **Docelowy czas odzyskania danych (recovery point objective RPO)** – czas graniczny, do którego informacja wykorzystywana przez określone działanie musi zostać odzyskana w celu umożliwienia wznowienia tego działania
- ✖ **Docelowy czas wznowienia działalności (recovery time objective RTO)** – czas od wystąpieniu incydentu, w którym musi zostać
 - + wznowione dostarczanie produktu lub usługi lub
 - + wznowione działanie lub
 - + zapewniony zestaw zasobów

A pair of thin-framed glasses with round lenses is resting on an open book. The book's pages are filled with text, and the background is softly blurred, suggesting a desk or study area. The overall tone is professional and academic.

ISO 22301:2012 – 4. KONTEKST ORGANIZACJI

KONTEKST ORGANIZACJI

- ✗ Zrozumienie potrzeb i oczekiwań zainteresowanych stron
 - + Zainteresowane strony
 - + Ich wymagania
- ✗ Wymagania prawne i regulacyjne
- ✗ Ustalenie odpowiedniego zakresu systemu
 - + Części organizacji objęte systemem
 - + Produkty i usługi
 - + Istotne procesy oraz ich powiązania

ISO 22301:2012 – 5. PRZYSWÓDZTWO

A person in a dark suit is walking away from the viewer down a long, brightly lit tunnel. The tunnel is formed by a series of repeating, concentric arches that create a strong sense of perspective and depth. The arches are dark, and the light comes from the far end of the tunnel, creating a silhouette effect on the person and highlighting the structure of the arches.

PRZYWÓDZTWO

✖ Przywództwo i zaangażowanie

- + Odpowiednie osoby z kierownictwa wyższego szczebla powinny wykazać swoje zaangażowanie w zarządzanie ciągłością działania

✖ Zaangażowanie kierownictwa

- + ustanowienie polityk i celów, które są zgodne ze strategicznymi kierunkami organizacji
- + Integracja z procesami działania (biznesowymi)
- + Dostępność zasobów
- + Komunikowanie istotności
- + Zapewnienie osiągnięcia celów systemu
- + Nadzorowanie i wspieranie
- + Promowanie doskonalenia
- + Wspieranie działania pozostałych osób w zakresie własnych zadań i odpowiedzialności

PRZYWÓDZTWO

✘ Polityka

- + Odpowiednia do celów organizacji
- + Wprowadza ramowe zasady dla osiągania celów ciągłości działania
- + Obejmuje zaangażowanie w stosowanie wymogów oraz w ciągłe doskonalenie
- + Udokumentowana i dostępna
- + Zakomunikowana

✘ Zadania, odpowiedzialność i uprawnienia w organizacji

Wyższe kierownictwo powinno zapewnić przydzielenie zadań i odpowiedzialności

- ✘ Wskazać odpowiedzialnych i uprawnionych do zapewnienia zgodności z wymaganiami normy
- ✘ Zapewnić sobie raportowanie o wykonaniu

A close-up photograph of a person's hands signing a document. The person is wearing a white long-sleeved shirt and a light blue tie with a small pattern. They are holding a black fountain pen in their right hand and signing a white document. Their left hand is holding the document steady. The background is slightly blurred, showing more of the person's clothing and the document. The text 'ISO 22301: 2012 - 6. PLANOWANIE' is overlaid in the center of the image.

ISO 22301: 2012 - 6. PLANOWANIE

PLANOWANIE

- ✗ Działania związane z ryzykiem oraz szansami
 - + Dla zapewnienia, że system zarządzania przyniesie zamierzone korzyści
 - + W celu zapobiegania lub redukcji niepożądanych skutków

Planowanie:

- + Akcji związanych z ryzykiem i szansami
- + Sposobu
 - ✗ Integrowania działań z zarządzaniem ciągłością i ich implementacji
 - ✗ Oceny skuteczności tych działań

A photograph of a modern, silver computer monitor on a dark, reflective desk. The monitor is tilted slightly to the right. The text 'ISO 22301:2012 - 7. WSPARCIE' is overlaid in a bold, dark brown font, centered horizontally and slightly below the middle of the image. The text has a subtle reflection on the desk surface below it. The background is a plain, light-colored wall.

ISO 22301:2012 – 7. WSPARCIE

WSPARCIE

- ✗ Zasoby
- ✗ Kompetencje
 - + Personelu, mającego wpływ na wykonanie na podstawie odpowiedniego wykształcenie, szkoleń i doświadczenia
 - + Podejmowanie działań zapewniających takie kompetencje oraz ocenia ich skuteczności
- ✗ Świadomość
 - + Osoby pracujące w organizacji powinny mieć świadomość: istnienia polityki ciągłości działania, swoich zadań związanych ze skutecznością systemu, skutków niespełnienia wymogów, swojej roli w przypadku wystąpienia zdarzeń zakłócających działanie
- ✗ Komunikacja
 - ✗ Co będzie komunikowane, kiedy, z kim się komunikować



ISO 22301:2012 – 8. FUNKCJONOWANIE

FUNKCJONOWANIE

- ✗ Ocena wpływu na biznes (BIA)
 - + Ustanowienie, wdrożenie i utrzymanie formalnego procesu służącego wyznaczaniu priorytetów i celów zapewnienia ciągłości oraz odzyskiwania sprawności działania
 - + BIA powinna obejmować:
 - ✗ Identyfikację działań wspierających zapewnienie dostarczania produktów i usług
 - ✗ Szacowanie skutków upływu czasu, w którym działania te nie są wykonywane
 - ✗ Ustanawianie ram czasowych wznowiania tych działań na określonym, minimalnym akceptowalnym poziomie, z rozważeniem skutków nie wznowienia ich w określonym czasie
 - ✗ Identyfikację powiązań oraz zasobów wspierających te działania (w tym dostawcy, partnerzy, inne zainteresowane strony)

FUNKCJONOWANIE

✕ Ocena ryzyka

- + Ustanowienie, wdrożenie i utrzymanie formalnego procesu identyfikowania, analizy i oceny ryzyka wystąpienia incydentów zakłócających działanie organizacji

(ISO 31000)

+ Organizacja powinna:

- ✕ Identyfikować ryzyka zakłócenia priorytetowych działań oraz procesy, systemy, informacje, ludzi, aktywa, partnerów i inne zasoby je wspierające
- ✕ Systematycznie analizować ryzyko
- ✕ Identyfikować ryzyka wymagające podjęcia działań (postępowania)
- ✕ Określać sposoby postępowania z ryzykiem

FUNKCJONOWANIE

- ✖ Strategia ciągłości biznesowej
 - + Identyfikowanie możliwości oraz wybór (na podstawie BIA i oceny ryzyka)
 - ✖ W celu ochrony działań priorytetowych
 - ✖ Ich stabilizacji, ciągłości, wznawiania i odzyskiwania
 - ✖ Ograniczania skutków, reagowania na nie oraz zarządzania nimi

FUNKCJONOWANIE

- ✗ Strategia ciągłości biznesowej, cd.
 - + Ustanowienie wymagań dla zasobów, w celu wdrożenia wybranej strategii
 - ✗ Ludzie, informacje i dane, budynki, środowisko
 - ✗ Wyposażenie, ekwipunek, wyżywienie
 - ✗ Systemy ICT, transport, finanse
 - ✗ Dostawcy i partnerzy
 - + Zabezpieczenie i minimalizowanie
 - ✗ Redukcja prawdopodobieństwa wystąpienia zakłócenia
 - ✗ Skrócenie czasu zakłócenia
 - ✗ Ograniczenie wpływu na kluczowe produkty i usługi

FUNKCJONOWANIE

- ✗ Ustanowienie oraz wdrożenie procedur ciągłości działania
 - + Opracowanie, wdrożenie, utrzymanie i udokumentowanie procedur (włącznie z niezbędnymi postanowieniami)
 - + Procedury powinny:
 - ✗ Wprowadzać odpowiedni protokół komunikacji wewnętrznej i zewnętrznej
 - ✗ Precyzyjnie określać natychmiastowe kroki podejmowane podczas wystąpienia zakłócenia
 - ✗ Być elastyczne, aby pozwalać na reagowanie na nieprzewidziane zagrożenia oraz zmiany warunków wewnętrznych i zewnętrznych
 - ✗ Skupiać się na skutkach zdarzeń potencjalnie mogących zakłócić funkcjonowanie
 - ✗ Być opracowane na podstawie przyjętych założeń oraz analizy wzajemnych powiązań
 - ✗ Być skutecznymi w minimalizowaniu skutków poprzez wdrożenie odpowiednich strategii

FUNKCJONOWANIE

- ✘ Ustanowienie oraz wdrożenie procedur ciągłości działania, cd
 - + Struktura reagowania za incydenty
 - ✘ Ustanowienie, udokumentowanie i wdrożenie procedur oraz struktury zarządzania (reagowanie na incydenty zakłócające, odpowiedzialny, uprawniony i kompetentny personel)
 - ✘ Struktura reagowania powinna:
 - ✱ Identyfikować możliwe skutki które uzasadniają podjęcie działań
 - ✱ Oceniać naturę i zakres oraz potencjalny skutek incydentów zakłócających,
 - ✱ Uruchamiać odpowiednie reakcje ciągłości działania
 - ✱ Posiadać procesy i procedury aktywacji, funkcjonowania, koordynowania i komunikowania reakcji
 - ✱ Posiadać dostępne zasoby wsparcia procesów i procedur, pozwalające na zarządzanie incydentami zakłócającymi w celu minimalizacji ich skutków
 - ✱ Komunikować się z zainteresowanymi stronami i organami, jak również z mediami

FUNKCJONOWANIE

- ✖ Ustanowienie oraz wdrożenie procedur ciągłości działania, cd
 - + Ostrzeganie i komunikowanie
 - ✖ Ustanowienie, wdrożenie i utrzymanie procedur
 - ✖ Wykrywania incydentów i regularnego ich monitorowania
 - ✖ Wewnętrznej komunikacji w organizacji,
 - ✖ Zewnętrznej komunikacji dotyczącej ryzyka, również na poziomie krajowym, oraz dostępu do systemów informowania i doradzania
 - ✖ Zapewnienia środków komunikowania w przypadku wystąpienia incydentu zakłócającego
 - ✖ Wsparcia komunikacji z agencjami ratownictwa
 - ✖ Zapisywania istotnych informacji o incydentach, podejmowanych działaniach, oraz na przykład wprowadzenie:
 - ✖ Ostrzegania zainteresowanych stron, zapewnienia współpracy między nimi, odpowiedniego lokalu oraz wyposażenia

FUNKCJONOWANIE

- ✘ Ustanowienie oraz wdrożenie procedur ciągłości działania, cd
 - + Plany ciągłości działania
 - ✘ Ustanowienie udokumentowanych procedur reagowania na incydenty zakłócające działanie oraz sposobu utrzymania lub odzyskiwania działań w ramowym zakładanym czasie
 - ✘ Plany wspólnie powinny obejmować i zawierać:
 - ✱ Ustalone zadania i odpowiedzialności osób i zespołów
 - ✱ Proces aktywacji procedur reagowania
 - ✱ Szczegóły natychmiastowego zarządzania skutkami (z uwzględnieniem bezpieczeństwa osób, opcji strategicznych, taktycznych i operacyjnych, zabezpieczenia przed dalszymi stratami)

FUNKCJONOWANIE

- ✘ Ustanowienie oraz wdrożenie procedur ciągłości działania, cd
 - ✘ Plany wspólnie powinny obejmować i zawierać, cd.:
 - ✘ Szczegóły dotyczące zasad i warunków komunikowania się z pracownikami i ich krewnymi, kluczowymi stronami i agencjami ratownictwa
 - ✘ Sposób utrzymania i wznowiania priorytetowych działań z zakładanym czasem
 - ✘ Szczegóły kontaktowania się z mediami
 - ✘ Strategia komunikowania się i preferowane metody
 - ✘ Wytyczne lub wzorce oświadczeń dla mediów
 - ✘ Odpowiednie osoby
 - ✘ Proces wycofywania się po ustaniu incydentu

FUNKCJONOWANIE

- ✗ Ustanowienie oraz wdrożenie procedur ciągłości działania, cd
 - + Każdy plan powinien określać:
 - ✗ Zastosowanie i zakres
 - ✗ Cele
 - ✗ Kryteria i procedury aktywacji
 - ✗ Procedury wdrożenia
 - ✗ Zadania, odpowiedzialność i uprawnienia
 - ✗ Wymagania i procedury komunikowania się
 - ✗ Wewnętrzne i zewnętrzne zależności i współdziałanie
 - ✗ Wymagania dla zasobów
 - ✗ Procesy przepływu informacji i dokumentacji

FUNKCJONOWANIE

- ✗ Ustanowienie oraz wdrożenie procedur ciągłości działania, cd
 - + **Odzyskiwanie sprawności:**
 - ✗ Udokumentowane procedury odbudowy i powrotu do pełnej działalności po okresie przejściowym
 - ✗ Środki zastosowane do wspierania uruchomienia normalnego działania po ustaniu incydentu.

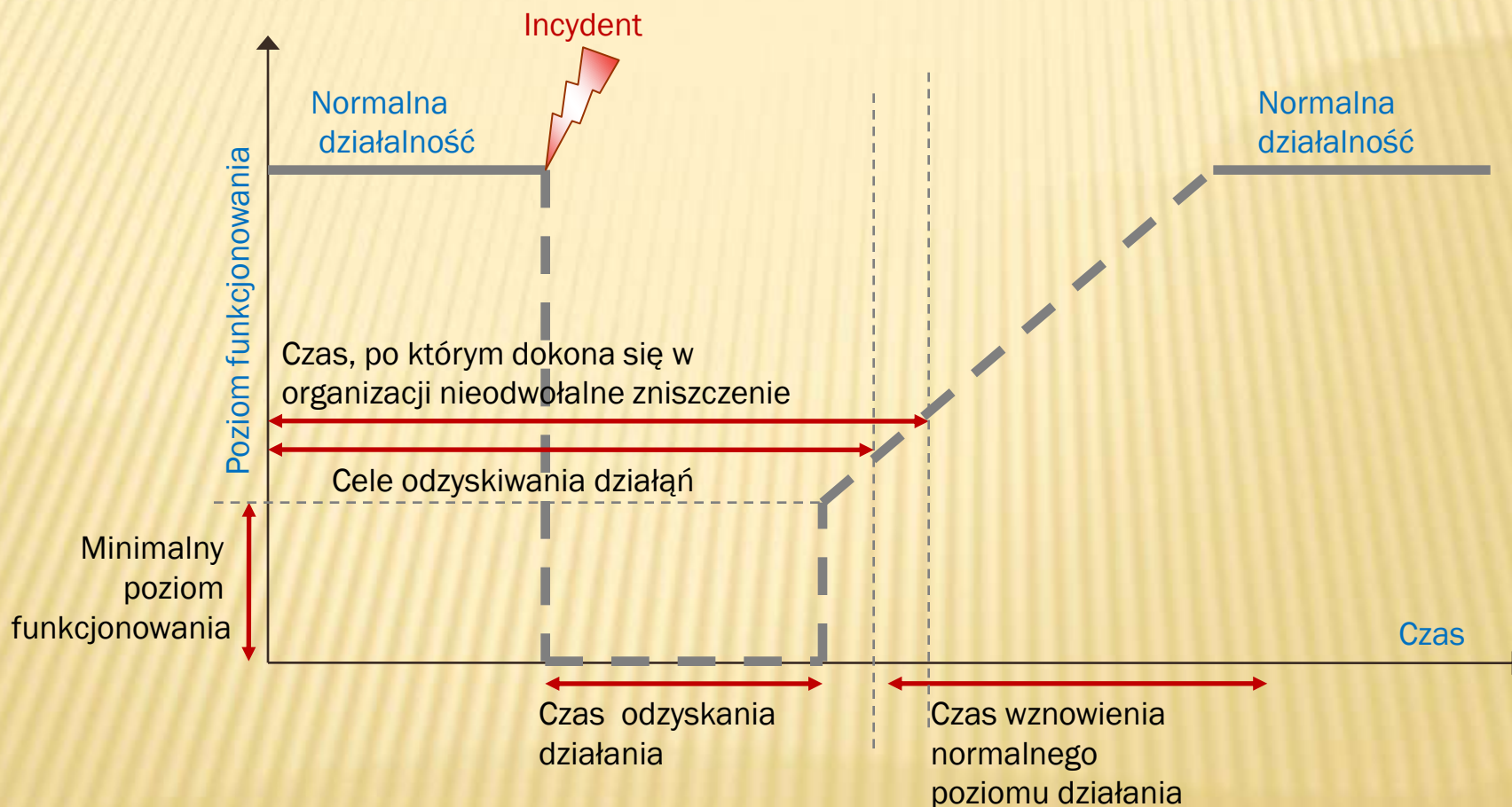
FUNKCJONOWANIE

× Ćwiczenia i testowanie

+ Planów ciągłości w celu stwierdzenia,

- × Spójności z zakresem i celem SZCD
- × Wykorzystania właściwych scenariuszy, z dobrze zaplanowanymi celami
- × Że w całości zebrane potwierdzają realizację zgodnie z założeniami i wymogami czasowymi
- × Że minimalizują ryzyko zakłócenia
- × Że po zakończeniu tworzone są formalne raporty wyników
- × Które są analizowane z myślą o doskonaleniu
- × Są przeprowadzane w zaplanowanych odstępach czasowych oraz w przypadku istotnych zmian w organizacji

ODZYSKIWANIE DZIAŁAŃ



ISO 22301:2012 – 9. OCENA WYKONANIA



OCENA WYKONANIA

- ✖ Monitorowanie, pomiar, analiza i ocena
- ✖ Audyt wewnętrzny
- ✖ Przegląd kierowniczy

ISO 22301:2012 – 10. DOSKONALENIE



DOSKONALENIE

- ✗ Niezgodności i działania korygujące
- ✗ Ciągłe doskonalenie

DZIĘKUJĘ ZA UWAGĘ

sylwia.wystub@isaca.katowice.pl

swystub@aksis.pl



Trust in, and value from, information systems

Katowice Chapter