OCENA ZDOLNOŚCI ORGANIZACJI DO ZARZĄDZANIA KRYZYSOWEGO

KONFERENCJA CIĄGŁOŚĆ DZIAŁANIA
WYZWANIA DLA SYSTEMU INFRASTRUKTURY KRYTYCZNEJ
26-27 LISTOPADA 2015 JACHRANKA K./WARSZAWY

World Sec Info LTD
WORLD SECURITY INFORMATION

World Sec Info LTD
590 Kingston Road
SW20 8DN London
United Kingdom

World Sec Info LTD o/Polska
Ogrodowa 31/35
00-893 Warszawa
Polska

Security Professionals

- Kryzys a incydent
- Dojrzałość organizacji
- Poziomy zaawansowania
- 9 grup wskaźników

AGENDA

O czym w wystąpieniu?

PODSTAWA PREZENTACJI

- Niniejsza prezentacja powstała na podstawie:
- Draftu standardu 22325, zamknięcie 12 października 2015;
- Standardu BS 11200:2014;
- Standardu Technicznego ISO 22317 – Przewodnik do analizy BIA.

Security Professionals

World Sec Info LTD
World Security Information

INCYDENT A KRYZYS (NA PODSTAWIE BS 11200:2014) - PRZEWIDYWANIE

INCYDENT

- Incydent co do zasady jest przewidywalny i można nim zarządzać (rozwiązać) za pomocą predefiniowanych rozwiązań, zawartych w procedurach choć ich specyficzny czas, charakter czy konsekwencja (skutek) mogą się różnić w szczegółach (detalach).

KRYZYS

- Kryzys jest wyjątkowym nieprzewidzianym, często źle zarządzanym wydarzeniem lub **kombinacją wydarzeń**, które tworzą dla organizacji wyjątkowe wyzwania. Z tego powodu kryzys jest trudno zarządzalny przez wcześniej zdefiniowane plany i procedury.

INCYDENT A KRYZYS - POCZĄTEK

INCYDENT

- Incydent może pojawić się bez ostrzeżenia lub w krótkim czasie od zdarzenia, albo przez stopniowe pogłębianie się uszkodzeń lub utraty kontroli . Znaki ostrzegawcze tego typu wydarzeń, istniejących lub zbliżających się, są krytycznymi elementami zarządzania incydentami.

KRYZYS

- Kryzys pojawia się nagle, bez ostrzeżenia lub wynika z incydentu, który nie został dostrzeżony/obsłużony, a wynikiem są bezpośrednie implikacje strategiczne. Kryzys może też wynikać z sytuacji, gdy ukryte problemy w organizacji narażone są na ujawnienie i w związku z tym wynikają głębokie konsekwencje reputacyjne.

PILNOŚĆ I „CIŚNIENIE”

INCYDENT

- Reagowanie na incydenty zazwyczaj obejmuje krótki okres działalności i zostaje rozwiązany przed narażeniem na przestój (obniżenie usług) w dłuższym okresie czasu lub stałym znaczącym wpływem na organizację.

KRYZYS

- Kryzys jest uznawany za działanie bardziej pilne, a reakcja może trwać dłuższy okres czasu do upewnienia się, że skutki zostały zminimalizowane.

WPŁYW

INCYDENT

- Incydenty, jako działania niepożądane są dość dobrze rozumiane i w związku z tym podatne na działania planowane (predefiniowane) w procedurach i planach. Skutki incydentów są oszacowane dość precyzyjnie.

KRYZYS

- Ze względu na swój strategiczny charakter kryzysy mogą zakłócić lub wpłynąć na całą organizację, a nawet przekroczyć granice organizacji, lokalizacji czy nawet sektora. Ponieważ kryzysy są zwykle skomplikowane i z natury niepewne, np. z przyczyn braku kompletu informacji do podjęcia decyzji, oszacowanie wpływu i rozprzestrzenienia jest bardzo trudne do zrealizowania.

NADZÓR NAD MEDIAMI (KOMUNIKACJA)

INCYDENT

- Efektywne zarządzanie incydentem przyciąga nieznacznie lub w niewielkim stopniu pozytywna uwagę mediów, tam gdzie zdarzenia są szybko ujawnione i dobrze zarządzane (łagodzone), a biznes szybko wraca do normalnego działania. Czasem zdarzenie może przyciągnąć uwagę mediów z negatywnym nastawieniem, nawet jeśli incydent jest zarządzany poprawnie, ale ma potencjał do eskalacji w kryzys.

KRYZYS

- Kryzys jest wydarzeniem, które przyciąga publiczne i medialne zainteresowanie, z potencjalnie negatywnym postrzeganiem reputacji organizacji. Przedstawienie problemu może być w mediach społecznościowych i tradycyjnych niedokładne i nieprecyzyjne, a jako takie może szybko wpłynąć na eskalację kryzysu.

ZDOLNOŚĆ (ŁATWOŚĆ) ZARZĄDZANIA Z WYKORZYSTANIEM PLANÓW I PROCEDUR

INCYDENT

- Incydent może być rozwiązany za pomocą predefiniowanych procedur i z zaplanowanym ujawnieniem, zminimalizowaniem skutku oraz przywróceniem do normalnego poziomu działań. Odpowiedź na incydent może mieć dostępne odpowiednie zaplanowane zasoby.

KRYZYS

- Kryzys, za sprawą kombinacji jego nowości, ryzyka błędu, potencjalnej skali i czasu oddziaływania zdarzenia jest trudny do rozwiązania przez wdrożenie predefiniowanych procedur i planów. Wymaga elastycznej, kreatywnej, strategicznej oraz długotrwałej odpowiedzi, która ma swoje źródło w wartościach organizacji.

- **ISO/IEC 27035:2011** Information technology - Security techniques - Information security incident management; Obecnie w trakcie rewizji przez trzy kolejne standardy:
  - **ISO/IEC DIS 27035-1** Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management
  - **ISO/IEC DIS 27035-2** Information technology -- Security techniques -- Information security incident management -- Part 2: Guidelines to plan and prepare for incident response
  - **ISO/IEC PDTS 27035-3** Information technology -- Security techniques -- Information security incident management -- Part 3: Guidelines for CSIRT operations
- **ISO 22320:2011** Societal security — Emergency management — Requirements for incident response, obecnie w rewizji:
  - **ISO/AWI 22320** Societal security -- Emergency management -- Requirements for incident response;

STANDARDY DOTYCZĄCE INCYDENTÓW

Przykłady

DOJRZAŁOŚĆ ORGANIZACJI

Niemowlę	Dziecko	Młodzież	Dorosłość
• Brak zasad • Brak zgodności	• Zgodność z przepisami	• Zgodność z przepisami • ISO, BS, GMP etc.	• Własny standard • Zgodność z przepisami i standardami, ISO, BS, GMP etc.

NIEMOWLĘ

- Wiodące podejście: „jakoś to będzie”;
- Szacowanie i ocena ryzyka: „w locie”;
- Kontekst szacowania i oceny ryzyka – czy mi się opłaca? (**odpowiedź brzmi – jeszcze nie**);
- Odsetek firm: Bardzo dużo;
- Wypełniane standardy: ZYSK (utrzymanie się).

DZIECKO

- Wiodące podejście: „aby się nie przyczepili”;
- Szacowanie i ocena ryzyka: „w locie”;
- Kontekst szacowania i oceny ryzyka: czy mi się opłaca? (odpowiedź brzmi – na dwoje babka wróżyła);
- Odsetek firm: Dużo;
- Wypełniane standardy: ZYSK ze spełnieniem minimum wymagań z przepisów prawa.

MŁODZIEŻ

- Wiodące podejście: „bezpieczeństwo elementem walki konkurencyjnej”;
- Szacowanie i ocena ryzyka: „mechaniczne”;
- Kontekst szacowania i oceny ryzyka: czy mi się opłaca? (odpowiedź – tak, jakaś wartość dodana będzie).
- Odsetek firm: Średnio;
- Wypełniane standardy: ZYSK, ze spełnieniem wymagań klientów (łańcuch dostaw), wymagania prawne w pełni.

DOROSŁY

- Wiodące podejście: „WIEM że mi się opłaca”;
- Szacowanie i ocena ryzyka: organiczne (każdy dział, pojawia się CRO);
- Kontekst szacowania ryzyka: jak jeszcze mogę oszczędzić – zapobiegając stratom (czasem jako jednostka biznesowa);
- Odsetek firm: Mało;
- Wypełniane standardy: liczymy koszty (rachunkowość zarządcza, ROI, NPV). Realizacja przepisów, standardów (ISO, BS) – „przy okazji”. Nowe standardy – bez żadnych problemów.

RYZYKO – KONTEKST WEWNĘTRZNY

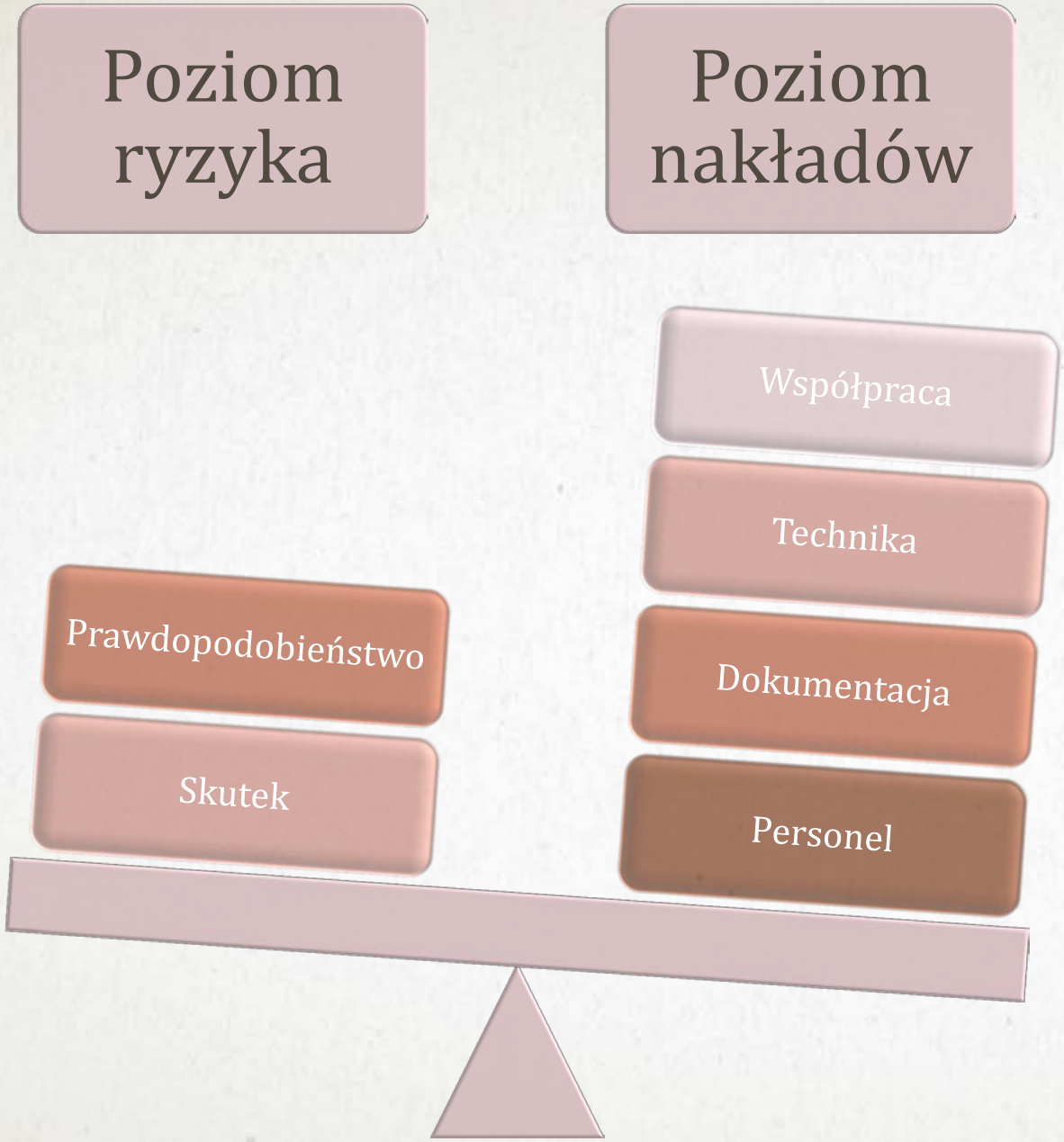
Niemowlę	Dziecko	Młodzież	Dorosłość
• Prawa ekonomii, • Cel: przeżycie.	• Zgodność z przepisami • Cel: uniknięcie problemów niedopełnienia. • Sposób: każdy odpowiedzialny samodzielnie.	• Zgodność z przepisami • ISO, BS, GMP etc. • Cel: poszerzenie odbiorców (reputacja firmy, budowanie marki) • Sposób: każdy odpowiedzialny samodzielnie.	• Własny standard • Zgodność z przepisami, ISO, BS, GMP etc. • Cel: świadome zarządzanie kosztami. • Sposób: Zintegrowane zarządzanie, obszary wsparte specjalistami metodycznymi.

- Poziom organizacji – zależny od poziomu zaawansowania.
- Poziom 1 – najniższy z możliwych poziomów.
- Poziom 4 – najwyższy z możliwych poziomów.

Jak można wykorzystać ten model i wdrożyć jako rozwiązanie kreujące system?

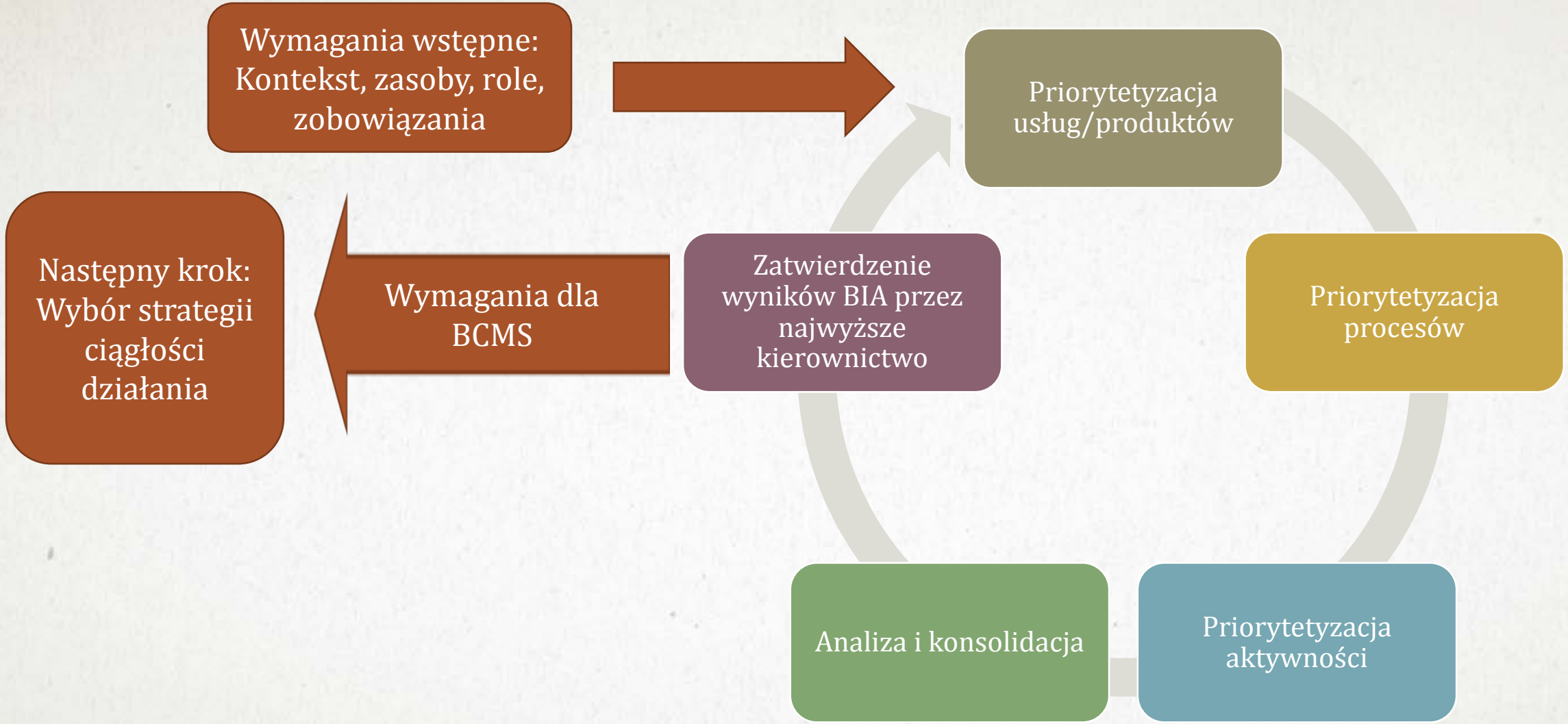
- Poziom stwierdzonego ryzyka (lub zagrożenia), jako element wskazujący na minimalny system zabezpieczeń (myślenie oparte o ryzyko);
- WARUNEK: Opracowany standard bezpieczeństwa, poziomujący stosowane zabezpieczenia;

MODEL OCENY PRZYJĘTY W IS) 22325



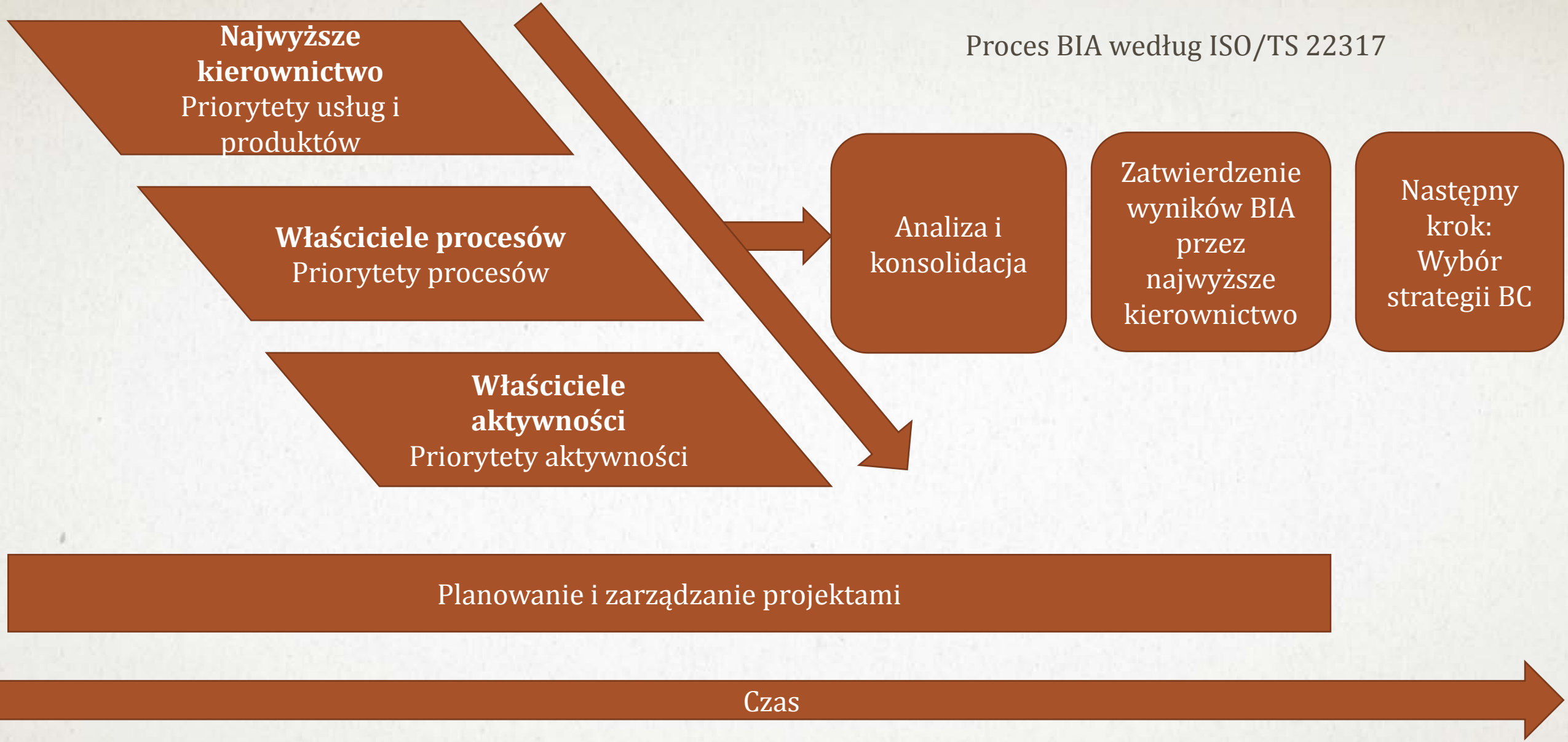
INNE WYKORZYSTANIE MODELU OCENY

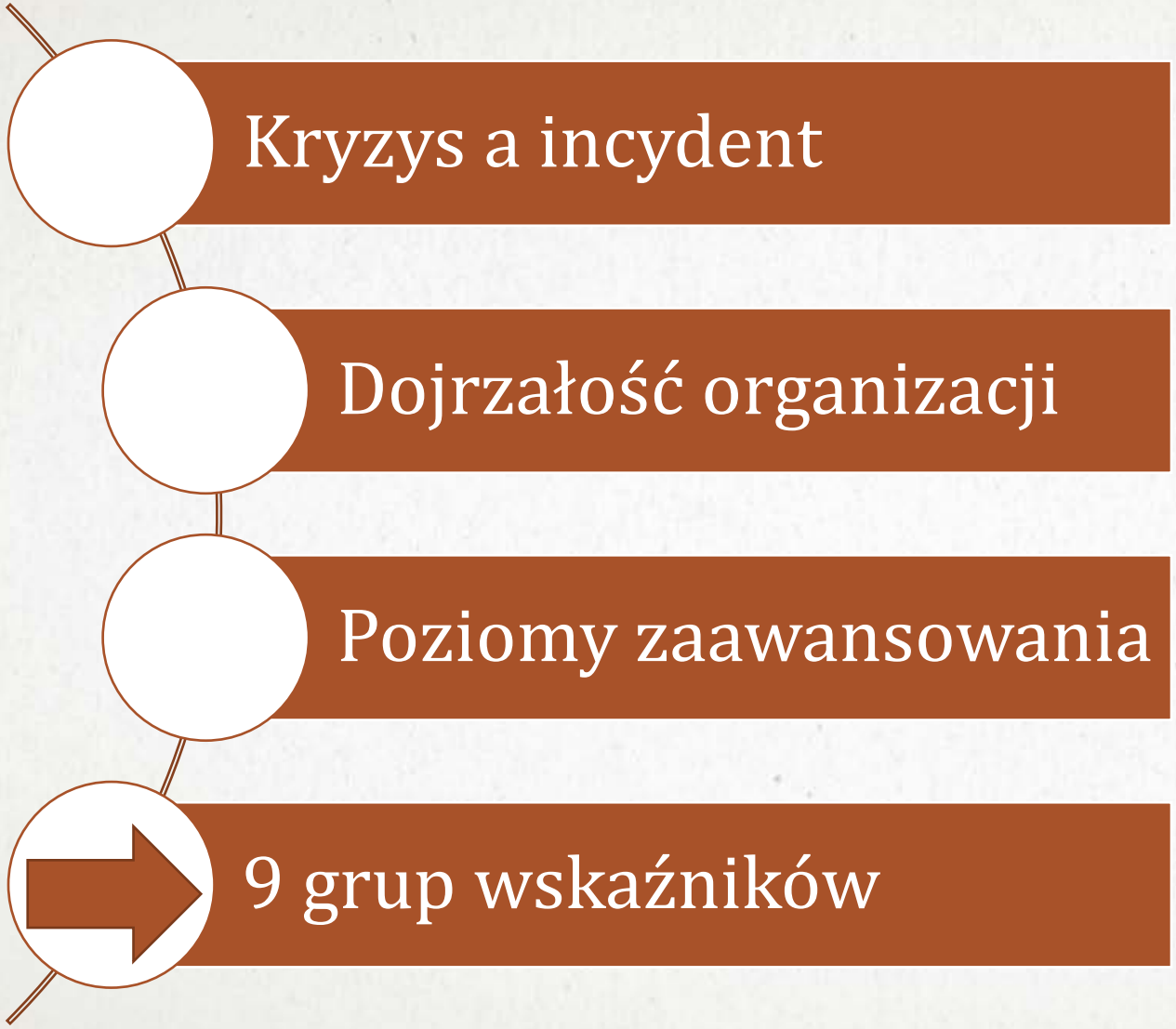
DLACZEGO TAK?



- Cykl życia analizy BIA – według ISO/TS 22317

Proces BIA według ISO/TS 22317





- Poziom organizacji – zależny od poziomu zaawansowania.
- Poziom 1 – najniższy z możliwych poziomów.
- Poziom 4 – najwyższy z możliwych poziomów.

Jak można wykorzystać ten model i wdrożyć jako rozwiązanie kreujące system?

- Poziom stwierdzonego ryzyka (lub zagrożenia), jako element wskazujący na minimalny system zabezpieczeń (myślenie oparte o ryzyko);
- WARUNEK: Opracowany standard bezpieczeństwa, poziomujący stosowane zabezpieczenia;

MODEL OCENY PRZYJĘTY W IS) 22325

PRZYWÓDZTWO I KOMPETENCJE

Poziom	Opis
Poziom 1	Cele zarządzania kryzysowego zostały zdefiniowane. Rola i obowiązki organizacji w sytuacji zagrożenia zostały określone.
Poziom 2	Cele zarządzania kryzysowego zostały zharmonizowane z celami organizacji, a najwyższe je popiera Liderzy są świadomi ról i obowiązków innych organizacji w sytuacji awaryjnej i promują współpracę.
Poziom 3	Procedury zostały wdrożone w celu doskonalenia na podstawie incydentów, zdarzeń potencjalnie niebezpiecznych, szkoleń i testów. W testach i ćwiczeniach biorą udział zarządzający. Najwyższe kierownictwo zapewnia zasoby niezbędne do określenia słabych i mocnych stron w obszarze odporności organizacji.
Poziom 4	Kierownictwo zatwierdziło politykę zarządzania kryzysowego (awaryjnego) jak i długoterminowego planu strategicznego, który identyfikuje przyszłe zagrożenia. Kierownictwo przydziela środki na wspieranie działalności badawczo-rozwojowej do zwiększenia swojej zdolności do radzenia sobie z obecnymi i przyszłymi zagrożeniami.

Źródło: projekt standardu ISO 22325

ZARZĄDZANIE ZASOBAMI

Poziom	Opis
Poziom 1	Podstawowe zasoby (np. personel, obiekty, narzędzia, technika, wyposażenie, budżet) są na miejscu do obsługi z przewidywanymi incydentami.
Poziom 2	Cele zarządzania zasobami zostały określone na podstawie wyników oceny ryzyka. Istnieje polityka dla zarządzania zasobami w zakresie sytuacji kryzysowych.
Poziom 3	Wykazy zasobów są aktualizowane, udokumentowane i śledzone, w tym określono zasoby dostępne do natychmiastowego wdrożenia. Zasoby te są również dostępne w celu wsparcia organizacji partnerskich. Wydzielono budżet, do zapewnienia elastycznej alokacji zasobów. System wsparcia rodziny i umów się z specjalistów od zdrowia psychicznego zostały ustalone.
Poziom 4	Cele zarządzania zasobami uwzględniają procesy badań i innowacji w rozwiązywania problemów i uwzględniają wymaganie ciągłego doskonalenia. Stosowane są najlepsze praktyki i nowoczesna technologia. Umowy zapewniają alternatywne i dodatkowe zasoby oraz współdzielą i integrują zasoby z innymi organizacjami. Zasoby są elastyczne i zdolne do reagowania na przyszłe zagrożenia. Główne wnioski wyciągnięte z prawdziwych zdarzeń, ćwiczeń i testów warunków skrajnych są udokumentowane i wykorzystywane

Źródło: projekt standardu ISO 22325

INFORMACJA I KOMUNIKACJA

Poziom	Opis
Poziom 1	System informacji i komunikacji w organizacji został wdrożony.
Poziom 2	System informacji i komunikacji, wspiera wymianę informacji i komunikacji w organizacji.
Poziom 3	Plany dla wewnętrznej i zewnętrznej informacji i komunikacji zostały wdrożone. System informacji i komunikacji, wspiera wymianę informacji między organizacjami i audytorium oraz zapewnia ciągłość systemu teleinformatycznego.
Poziom 4	Zaawansowany plan informacji i został wdrożony i zintegrowane z innymi organizacjami. Stosowane są najlepsze praktyki i nowoczesna technologia. Główne wnioski wyciągnięte z prawdziwych zdarzeń, ćwiczeń i testów warunków skrajnych są udokumentowane i wykorzystywane

Źródło: projekt standardu ISO 22325

OCENA RYZYKA

Poziom	Opis
Poziom 1	Ryzyka zostały zidentyfikowane, ale nie zostały przeanalizowane i uwzględnione w planowaniu długoterminowym.
Poziom 2	Jakościowa ocena ryzyka została przeprowadzona.
Poziom 3	Pół-ilościowa ocena ryzyka zgodnie z normą ISO 31000, pkt 5.4, została przeprowadzona.
Poziom 4	Ilościowa ocena ryzyka zgodnie z normą ISO 31000, pkt 5.4, została przeprowadzona.

Źródło: projekt standardu ISO 22325

ODPOWIEDŹ NA INCYDENTY

Poziom	Opis
Poziom 1	Polityka kierowania i kontroli została stworzona i organizacja jest w stanie w stopniu podstawowym reagować na incydent.
Poziom 2	System kierowania i kontroli został wdrożony. Role i odpowiedzialności w systemie kierowania i kontroli zostały określone i powierzone. Struktura systemu dowodzenia i kontroli jest aktualizowana i przekazywana do zainteresowanych stron.
Poziom 3	System kierowania i kontroli jest przygotowany do współdziałania w ramach wielu organizacji do reakcji na incydent. Organizacja jest w stanie reagować na eskalujące incydenty. Skuteczność odpowiedzi incydent jest mierzona w stosunku do szczególnych celów.
Poziom 4	System kierowania i kontroli został wdrożony zgodnie z normą ISO 22320.

Źródło: projekt standardu ISO 22325

KOORDYNACJA I WSPÓŁPRACA

Poziom	Opis
Poziom 1	Organizacja posiada wiedzę o zasadach odpowiedzi na incydent (sytuacje kryzysową) innych odpowiednich organizacji.
Poziom 2	Organizacja ma podpisane ramowe umowy (porozumienia) o współpracy z innymi, odpowiednimi organizacjami.
Poziom 3	Organizacja ma podpisane umowy (porozumienia) o współpracy, który określają działania organizacji. Cele są ustanowione w celu zapewnienia skutecznej i priorytety, trwałej koordynacji i współpracy na szczeblach taktycznych i strategicznych między organizacjami.
Poziom 4	Koordynacja i współpraca została zrealizowana zgodnie z normą ISO 22320. Umowy (porozumienia) o wspólnej koordynacji i współpracy są sprawdzane i aktualizowane. Koordynacja i współpraca jest testowana i oceniana w trakcie ćwiczeń oraz podczas ciągłych działań doskonalących. Organizacja umożliwia integrację z partnerami współpracy poprzez wymianę ekspertów, w stosownych przypadkach. Organizacja wdrożyła ISO 22397.

Źródło: projekt standardu ISO 22325

ZARZĄDZANIE KRYZYSOWE

Poziom	Opis
Poziom 1	Plan reagowania kryzysowego został wdrożony, jest aktualny i dostępny.
Poziom 2	Plan reagowania kryzysowego obejmuje: **zakres**; **cele** biorąc pod uwagę ludzkie życie i zdrowie, funkcje społeczne, aktywa ekonomiczne i środowiskowe; **role i obowiązki** oraz **świadomość** personelu. Plan jest aktualizowany po znaczącym incydencie lub poważnej zmianie w organizacji.
Poziom 3	Plan reagowania kryzysowego obejmuje: • uwzględnienie opinii zainteresowanych stron; • wnioski wyciągnięte z wcześniejszych incydentów; • mierzalne cele. Plan jest oceniany i aktualizowany po ćwiczeniach i szkoleniach.
Poziom 4	Plan reagowania kryzysowego został zintegrowany z innymi planami w organizacji w celu zapewnienia ciągłości operacji. Organizacja starannie planuje reagowanie kryzysowego z uwzględnieniem innych organizacji z zamiarem promowania koordynacji i współpracy w czasie dużych incydentów, zgodnie z normą ISO 22397.

Źródło: projekt standardu ISO 22325

ĆWICZENIA

Poziom	Opis
Poziom 1	Ćwiczenia są prowadzone, ale organizacja nie posiada formalnego programu ćwiczeń.
Poziom 2	Program ćwiczeń, został ustanowiony z uwzględnieniem celów organizacji. Ćwiczenia są prowadzone regularnie. Pracownicy są przeszkoleni do wykonywania powierzonych obowiązków.
Poziom 3	Program jest zintegrowany, oparty na kompetencjach, oceniany, regularnie aktualizowany i uwzględnia opinie zainteresowanych stron. Ćwiczenia są mierzone w odniesieniu do celów i są odpowiednio do nich dostosowane.
Poziom 4	Program ćwiczeń zostały wdrożone zgodnie z normą ISO 22398. Główne wnioski wyciągnięte z ćwiczeń są rejestrowane i ujmowane w planowaniu przyszłej odpowiedzi na incydent. Programy ćwiczeń zostały opracowane z innymi organizacjami. Programy ćwiczeń są stale udoskonalane.

Źródło: projekt standardu ISO 22325

ŁAGODZENIE (MINIMALIZACJA) SKUTKÓW

Poziom	Opis
Poziom 1	Planowanie minimalizacji skutków zostały opracowane.
Poziom 2	Planowanie minimalizacji zostało zrealizowane na podstawie scenariuszy zagrożenia. Wyniki działania są rejestrowane i poddawane okresowej weryfikacji.
Poziom 3	Planowanie minimalizacji skutków uwzględnia wymagania interesariuszy. Wyniki działań łagodzących są ilościowo mierzone i wykorzystywane w aktualizacji planu.
Poziom 4	Łagodzenie obejmuje planowanie badań i poszukiwania innowacji w rozwiązywaniu problemów, gdzie konwencjonalne metody lub technologie mogą nie być skuteczne. Zaawansowana technologia jest wykorzystywana w minimalizacji zagrożeń.

Źródło: projekt standardu ISO 22325

Proces oceny:

- Planowanie;
- Gromadzenie danych;
- Analiza;
- Raportowanie
  - Szablon podsumowania
  - Szablon raportu

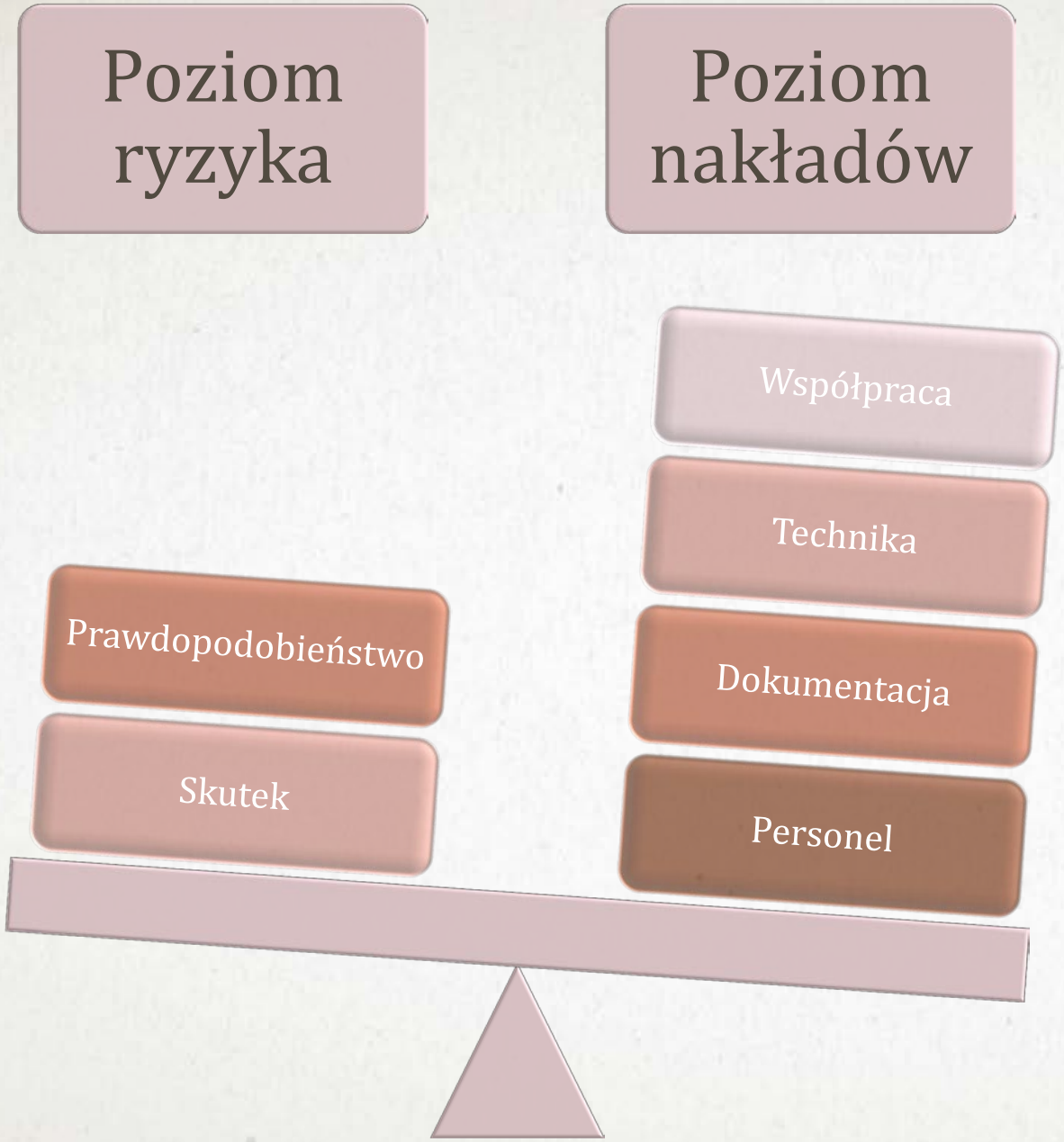
Ciągłe doskonalenie.

DALSZA ZAWARTOŚĆ STANDARDU

PRZYKŁAD STANDARDU

Poziom	*Poziomy dokumentacji*	*Czas reakcji*	*Aktualizacja*
3	Dokumentacja na poziomie 2 oraz: szczegółowe opracowanie na temat prawdopodobieństwa wystąpienia wraz z szacunkami skutku. Informacje na temat zagrożeń i postępowania z nimi umieszczone w dokumentach o charakterze strategicznym	Dokumentacja na poziomie 2 oraz: sposób przeciwdziałania – zadania prewencyjne, szczegółowo opisane.	Ciągły nadzór nad aktualnością dokumentacji, poprzez osobę / komórkę wyznaczoną do nadzoru.
2	Dokumentacja na poziomie 1 oraz: Opracowania wskazujące źródła zagrożeń wraz z typowanymi skutkami	Dokumentacja na poziomie 1 oraz: sposób postępowania po materializacji (uspokojenie środowiska)	Monitoring zmian w prawie wewnętrznym i zewnętrznym, oraz przegląd realizowany nie rzadziej niż raz na kwartał.
1	Dokumentacja na poziomie minimalnym, zawierająca informacje ogólne na temat występowania zagrożenia (lista)	Ogólne informacje na temat neutralizacji zagrożenia.	Przegląd okresowy aktualności dokumentacji wynikający z przepisu prawa, a jeśli przepis prawa nie określa – nie rzadziej niż raz na 12 miesięcy.
0	Brak dokumentacji	Brak dokumentacji	Brak aktualizacji

Źródło: Metodyka Audytu Bezpieczeństwa IBII, wersja z 2012 roku



INNE WYKORZYSTANIE MODELU OCENY

- 5 filarów bezpieczeństwa;
- Filary bezpieczeństwa poziomowane na 4 poziomy;
- Poziomy zaangażowania w filarze – równe z poziomami ryzyka;
- Miara ryzyka – jako wymaganie dla każdego z filarów;
- Waga zabezpieczeń - skuteczność w oddziaływaniu na zagrożenie lub łagodzenie/zmniejszanie skutków wystąpienia.
- Opracowanie – grudzień 2012, IBII

INDEKS BEZPIECZEŃSTWA FIZYCZNEGO

W oparciu o Metodykę KGP w sprawie uzgadniania planów ochrony obiektów, obszarów i urządzeń podlegających obowiązkowej ochronie

Security Professionals

World Sec Info LTD
World Security Information

DZIĘKUJĘ ZA UWAGĘ

GRZEGORZ KRZEMIŃSKI
GK@WORLDSECINFO.CO.UK
TEL: +48511252787
PHONE: +44(0)7464745044

World Sec Info LTD
WORLD SECURITY INFORMATION

World Sec Info LTD
590 Kingston Road
SW20 8DN London
United Kingdom

World Sec Info LTD o/Polska
Ogrodowa 31/35
00-893 Warszawa
Polska

Security Professionals