Główne problemy rozwiązywane przez Platformę Zarządzania Bezpieczeństwem

Procesy zarządzania bezpieczeństwem nie są już wyspami. Kiedyś, szeroko rozumiane procesy bezpieczeństwa - zarządzanie ciągłością działania, bezpieczeństwem informacji, obsługa incydentów oraz analiza ryzyka czy działania audytowe – były obsługiwane przez oddzielne, dedykowane jednostki. Ponieważ wymiana informacji miała charakter formalny (pisma, zestawienia czy raporty), każdy z działów stosował własne rozwiązanie dedykowane tylko do swoich potrzeb. Obecnie wymagania regulacji i norm narzucają potrzebę całościowego podejścia do ww. podprocesów.

Brak integracji i skalibrowania różnych rozwiązań to zbyt wolna reakcja i niższa jakość informacji zarządczej oraz obowiązkowego raportowania. Wiele dedykowanych systemów, które skupione są na wąskiej funkcji bez *świadomości innych procesów*, powoduje, że organizacja nie jest w stanie sprawnie koordynować, analizować i raportować zewnętrznie i wewnętrznie poziomu ryzyka oraz zagrożeń. Nie ma np. możliwości łatwego przełożenia zarejestrowanych incydentów na aktualizację prognoz prawdopodobieństwa oraz skutków poszczególnych ryzyk czy ustalenia należytego priorytetu dla incydentu bezpieczeństwa przy wykorzystaniu informacji z analizy wpływu na biznes z obszaru BCM.

Bezpieczeństwo zależy od współdziałania całej organizacji, a nie pojedynczych departamentów. Obecnie cała organizacja musi być świadomie zaangażowana w zarządzanie bezpieczeństwem. Przy czym nie może to być skutecznie realizowane, jeśli biznes będzie bombardowany ankietami, arkuszami czy mailami pochodzącymi z różnych działów czy departamentów. Co ważne, biznes i jednostki wsparcia, nie są już tylko dostarczycielami danych (analiza BIA, analiza ryzyka itp.). Kolejne regulacje, jak np. wymagania EBA w zakresie outsourcingu, wydają się wskazywać potrzebę sprawnej współpracy bezpieczeństwa z departamentami biorącymi udział w uzgadnianiu i realizacji usług zewnętrznych: odpowiednio dostosowane umowy, wstępna oraz okresowa weryfikacja dostawców pod kątem ryzyk, określenie funkcji (procesów) krytycznych czy regularny audyt istniejących umów outsourcingowych. Sprawne działanie przy minimalizacji obciążenia biznesu możliwe jest dzięki zastosowaniu rozwiązania, które potrafi raz uzyskane informacje (np. podczas BIA, rejestracji incydentu czy szacowania ryzyka) zaadresować i udostępnić potrzebującym ich jednostkom. Dbając przy tym o automatyzację – obieg procesu, powiadomienia, dynamiczne dokumenty i raporty.

Przykłady regulacji wymagających sprawnego współdziałania całej organizacji

Ustawa o krajowym systemie cyberbezpieczeństwa

- Zarządzanie ryzykiem.
- Proporcjonalne środki zapobiegawcze – planowanie, wdrażanie, kontrola.
- Baza zagrożeń i podatności.
- Zarządzanie Ciągłością Działania – wdrażanie, dokumentowanie, testowanie i utrzymywanie planów.
- Incydenty bezpieczeństwa – rejestracja, priorytetyzacja i raportowanie.

Rekomendacja EBA w zakresie umów outsourcingowych

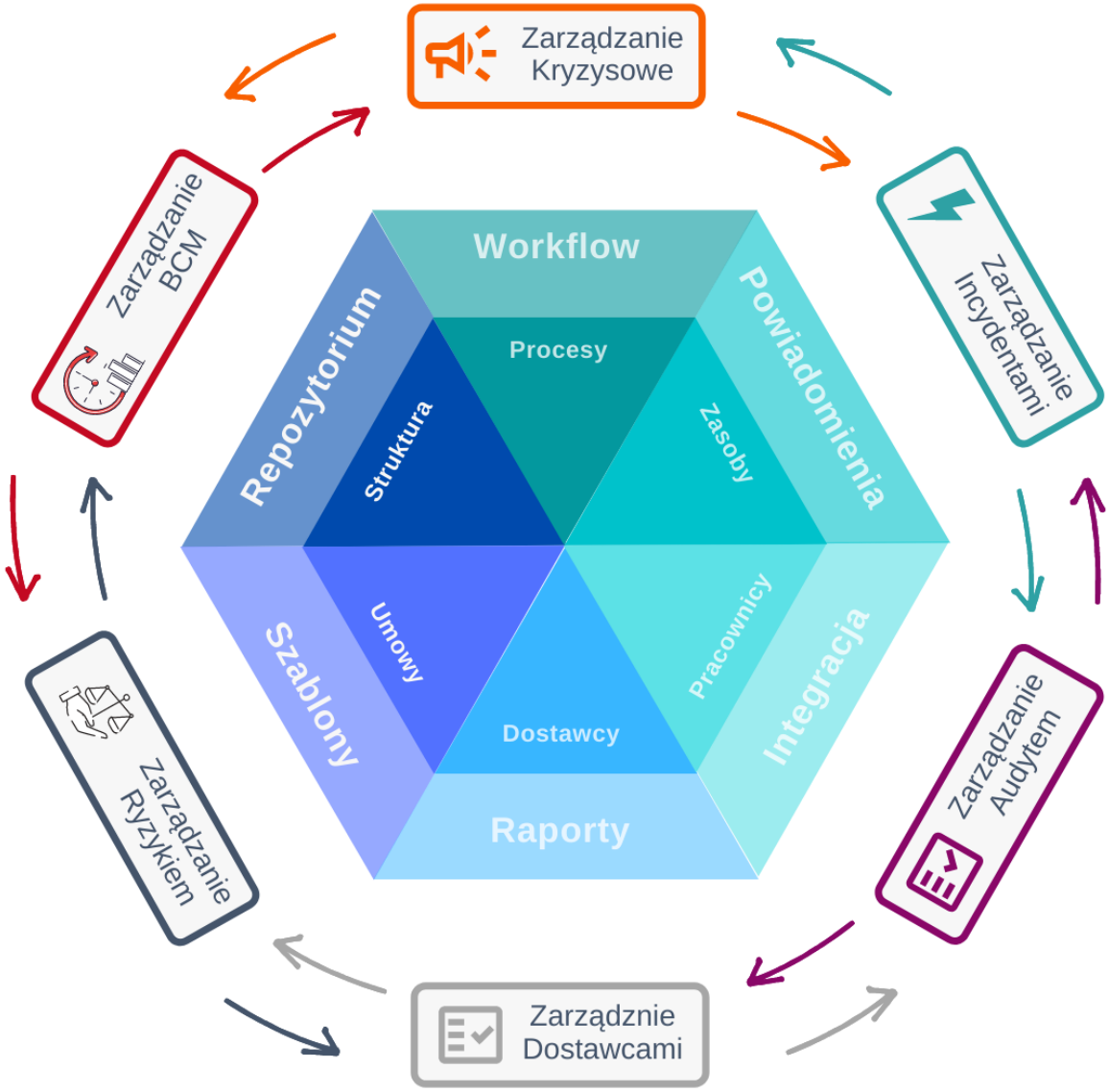
- Analiza ryzyka dostawców.
- Dokumentacja i rejestr umów.
- Identyfikacja funkcji krytycznych.
- Kontrola wewnętrzna.
- Planowanie ciągłości działania.
- Zatwierdzanie nowych umów.

Platforma BCMLogic to:

Moduły merytoryczne z wbudowaną wiedzą ekspercką, które mogą być wdrożone jednocześnie lub stopniowo zastępować *wyspowe* aplikacje, wnosząc istotną wartość dodaną z każdym kolejnym modułem.

Moduły techniczne automatyzujące pracę, ułatwiające wymianę informacji dotyczących bezpieczeństwa pomiędzy jednostkami i przede wszystkim minimalizujące narzut tych procesów na działanie biznesu.

Wspólna warstwa danych o bezpieczeństwie, umożliwiająca import danych z dowolnych źródeł i systemów, sprawne przetworzenie oraz udostępnienie ich tam gdzie potrzeba w odpowiednim zakresie i czasie.



Więcej informacji: www.bcmlogic.com

BCM LOGIC

BCMLogic Solutions Sp z o.o.
Aleje Jerozolimskie 125/127
02-117 Warszawa

biuro@bcmlogic.com
tomasz.gliszczynski@bcmlogic.com
Tel. +48 504 142 205