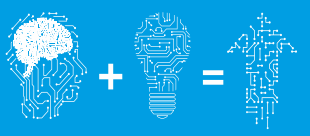
Sygnity

Data Governance w przetwarzaniu dużych wolumenów danych

Wiesław Wyszogrodzki
Menedżer Rozwoju Biznesu



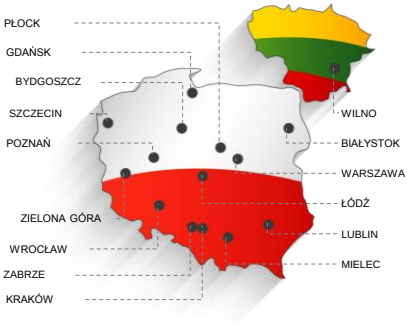
Sygnity
Business-Innovation-Now

AGENDA

- O Sygnity
- Data Governance
  - kilka liczb
  - definicje
  - wyzwania
  - korzyści
- Program Data Governance etapy realizacji
- Data Governance w instytucjach finansowych
- Podsumowanie

O SYGNITY

Sygnity
Business-Innovation-Now



+24 LATA WSPIERAMY BIZNES NASZYCH KLIENTÓW

+20 LAT NA GPW

+8000 ZREALIZOWANYCH PROJEKTÓW

+1200 SPECJALISTÓW

HISTORIA

1988 POWSTAJE EMAX

1991 POWSTAJE COMPUTERLAND

1995 COMPUTERLAND DEBIUTUJE NA GPW JAKO DRUGA FIRMA Z BRANŻY IT

1998 COMPUTERLAND PRZEJMUJE KONTROLĘ NAD UAB BALTIJOUS KOMPIUTERIU CENTRAS

2000 MAX ELEKTRONIK DOŁĄCZA DO GRUPY EMAX

2002 DEBIUT EMAX NA GPW

2004 GEOMAR DOŁĄCZA DO GRUPY COMPUTERLAND

2007 W WYNIKU POŁĄCZENIA COMPUTERLAND I EMAX POWSTAJE SYGNITY. DRUGA CO DO WIELKOŚCI GIEŁDOWA SPÓŁKA INFORMATYCZNA W POLSCE

2011 UZYSKANIE CERTYFIKATU ISO 27001

2012 SYGNITY INTERNATIONAL

2013 POTWIERDZENIE ZDOLNOŚCI DO PRZETWARZANIA INFORMACJI NIEJAWNYCH NATO

O SYGNITY

Sygnity
Business-Innovation-Now

Pracujemy dla największych banków, przedsiębiorstw i instytucji publicznych, budując wspólnie z nimi lepszą przyszłość dla nas wszystkich.

SEKTORY gospodarki, które obsługujemy

BANKOWOŚĆ I FINANSE

ADMINISTRACJA CENTRALNA I SAMORZĄDOWA

UTILITIES I ODBIORCY MEDIÓW

Data Governance - kilka liczb

Zasoby danych:
- wg IBM 90% wszystkich danych wygenerowanych zostało w ciągu ostatnich kilku lat
- wg Gartnera w ciągu najbliższych pięciu lat dane firm wzrosnąo800%
- 20% firm posiada zasoby powyżej 500TB,
- 8% firm ma ich mniej niż 1 TB

Odzyskanie danych:
- w 32% firm odbudowa danych po całkowitej utracie zajęłaby od 5 do10 dni
- w 20% nie ma rozwiązań do odtwarzania danych tzw. eDiscovery
- w 25% posiadane rozwiązania określane są jako słabe

Budżety na rozwój DG to kwota od 200 tys do 500 tys USD na rok
- 40% firm nie ma specjalnego budżetu
- 60% tych którzy mieli wdrożone korzysta z modelu w chmurze

Wdrażanie polityki Data Governance:
- 44% nie posiadało formalnej polityki DG
- 22% nie planuje wprowadzenia polityki DG
- 11% planuje wdrożyć w okresie 6 miesięc
- 39,7% wdrożenia za ponad rok
- 22,2 % nie planuje

Istotność polityki Data Governance w organizacji:
- 60 % niezmiernie istotna
- 36% bardzo ważna
- 4 % trochę istotna
- 0,5 % nieistotna

* źródło: raport Rand Secure Data – Data Governance Survey 2013

(badanie firm dużych z USA i Kanady – zysk od 10 do 100 mln USD Zatrudnienie od 1000 do 5000 pracowników)

Data Governance

Data Governance jest dyscypliną zajmującą się podnoszeniem jakości danych, przy czym dane są traktowane jako składnik aktywów przedsiębiorstwa. Data Governance to podejmowanie decyzji w celu optymalizacji, bezpieczeństwa i wykorzystania danych, jako istotnej wartości w działalności przedsiębiorstwa.

Data Governance to proces standaryzacji procesów, technologii oraz polityk/reguł w ramach organizacji, dla uzyskania optymalnej wartości z przetwarzanych danych.

Data Governance odgrywa kluczową rolę w wyrównywaniu rozbieżności między sprzecznymi często zasadami działalności komórek organizacyjnych, które mogą przyczyniać się do powstawania nieprawidłowości w danych.

Typowa komercyjna organizacja ma nadmierną ilość danych o swoich klientach, partnerach biznesowych i produktach. Organizacja nawet może nie wiedzieć gdzie znajdują się te dane i czy są one wiarygodne.

Dane są jednocześnie największym źródłem wartości organizacji i jej największym źródłem ryzyka. Niska jakość danych w zarządzaniu często oznacza złe decyzje biznesowe i większe narażenie na naruszenia zgodności z przepisami. Zdolność do podnoszenia, jakości danych może pomóc organizacji zapewnić lepszą obsługę, znacznie mniejszy wysiłek na funkcjonowanie zgodne z przepisami i sprawozdawczością.

Materiał opracowano na podstawie publikacji „The IBM Data Governance Unified Process" – Sunil Soares

Data Governance

Zarządzanie danymi to proces, w ramach którego należy zdefiniować: kto, kiedy, gdzie i jak, wprowadza poszczególne informacje, a także kto, kiedy, gdzie i jak, kontroluje, czy wprowadzane wartości są prawidłowe.

Jeśli coś jest procesem, to potrzebne są standardy. A jak są standardy to warto je komunikować i mierzyć. Błędów nie da się uniknąć, ale przekraczanie pewnego progu to już jest niedbalstwo. Ten próg powinien być jasno wyznaczony.

Jak utrzymać czystość i porządek w bazach danych? Co zrobić, aby dane miały wartość dla przedsiębiorstwa? Kilka wskazówek, które można zastosować:

Przed wdrożeniem jakiegokolwiek systemu (ERP, CRM, BI, itd.) warto myśleć o przyszłość. Wyobrazić sobie najgorszy możliwy scenariusz pracy na tych aplikacjach, a następnie zastanowić się nad działaniami, które warto podjąć, aby do takiej sytuacji nie doszło. Jest to klasyczne zarządzanie ryzykiem. Czarne scenariusze mają największe prawdopodobieństwo realizacji. Już od początku warto mieć zaimplementowane w systemie rozwiązania, które umożliwią czyszczenie i porządkowanie danych.

Raz wprowadzone wartości danych nie są wieczne. Wiele parametrów się zmienia, dlatego na bieżąco powinna być weryfikowana aktualność rekordów. Dla danych teleadresowych klientów można to przykładowo robić poprzez kontakt bezpośredni, np. akcje email i tele-marketingowe; można też rozważyć aktualizację bądź uzupełnianie danych przy wykorzystaniu baz danych dostarczonych przez firmy zewnętrze.

7

Data Governance - wyzwania / korzyści

Data Governance - Wyzwania czyli dlaczego organizacje powinny wdrażać ten program :

- Niespójne Data Governance może spowodować niespójność pomiędzy celami biznesowymi i systemami IT,
- Polityki zarządzania nie są powiązane z wymaganiami gromadzenia i raportowania danych,
- Ryzyka nie są zarządzane z perspektywy wspólnego cyklu repozytorium danych, polityki, standardów i procesów kalkulacji,
- Metadane i słowniki biznesowe nie są używane do łączenia semantycznych różnic wielu aplikacji w przedsiębiorstwie,
- Elementy regulacyjne i architektury są wdrażane zanim modelowane są długoterminowe skutki,
- Zarządzanie między domenami różnych danych i organizacyjnymi granicami może być trudne do wykonania,
- Często niejasne jest to co powinno być regulowane.

Data Governance - Korzyści, jakie organizacja może uzyskać dzięki tej polityce:

- poprawa poziomu zaufania użytkowników do danych prezentowanych w raportach,
- zapewnienie spójności danych między wieloma raportami z różnych części organizacji lub pochodzących od podmiotów współpracujących,
- zapewnienie odpowiedniego zabezpieczenia informacji o firmie na potrzeby audytorów i regulatorów,
- poprawa poziomu znajomości odbiorcy dla prowadzenia inicjatyw np. regulacyjnych,
- bezpośredni wpływ na trzy czynniki najbardziej istotne dla organizacji: **zwiększenie, przychodów, obniżenie kosztów i zmniejszenie ryzyka.**

8

Data Governance – proces Oceny Dojrzałości

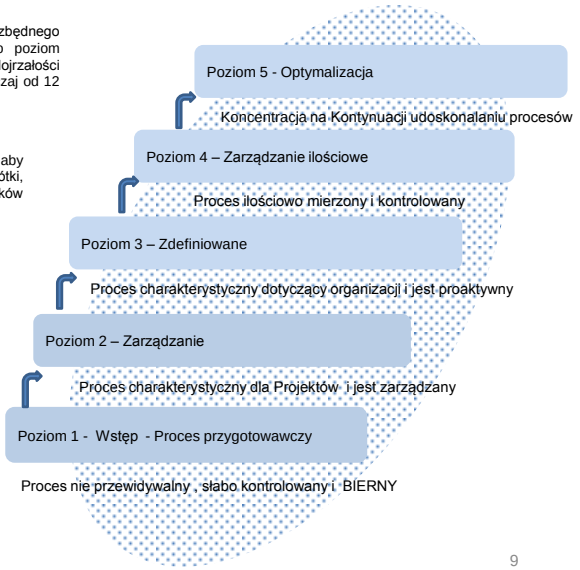
Sygnity Business-Innovation-Now

Zbudowanie programu Data Governance niezbędnego do oceny funkcjonowania organizacji, od obecnego poziom dojrzałości (stan obecny) do pożądanego poziomu dojrzałości (przyszłego), wymaga okresu czasu, który trwa zazwyczaj od 12 do 18 miesięcy.

Okres ten musi być wystarczająco długi, aby uzyskać pozytywne wyniki, a jednocześnie na tyle krótki, aby nadal zapewnić finansowanie od głównych uczestników / sponsorów programu.

Proces ten stanowi ramy ustalania priorytetów działań, punkt wyjścia, wspólnego języka i metodologii do pomiaru postępu realizacji procesu.

Ostatecznie, to uporządkowany zbiór elementów oferuje stały, wymierny postęp do osiągnięcia końcowego pożądanego stanu dojrzałości.



Data Governance - Ocena Dojrzałości

Sygnity Business-Innovation-Now

Wymiary oceny

Główne kategorie oceny, które biorą udział w opracowaniu programu Data Governance, są to zarówno procedury ale również narzędzia informatyczne, technologie i techniki zarządzania informacją.

1. Zarządzanie ryzykiem i zgodność danych - jest to metodologia, w której zagrożenia są identyfikowane, kwalifikowane, policzalne, unikalne, akceptowane, złagodzone lub przenaszalne poza organizację.

2. Tworzenie wartości - jest procesem, w którym dane są kwalifikowane i zliczane dla prowadzenia działalności w celu zmaksymalizowania wartości danych.

3. Struktury organizacyjne i świadomość - odnosi się do poziomu wzajemnej odpowiedzialności między biznesem i IT.

4. ***Zarządzanie*** - jest to jakościowa kontrola danych mająca na celu zwiększenia aktywów, ograniczenie ryzyka i kontrolę organizacji.

5. *Polityka* - są to spisane zasady pożądanego zachowania organizacji.

6. Zarządzanie jakością danych - odnosi się do metod pomiaru, poprawiania, certyfikacji jakości i integralności procesu produkcji, testowania i archiwizacji danych.

7. Zarządzanie cyklem życia informacji - jest systematyczne podejście oparte na regułach do gromadzenia, używania, przechowywania i usuwania informacji.

8. Bezpieczeństwo informacji i danych osobowych - odnosi się do polityk, praktyk i kontroli stosowanych przez organizację w celu zmniejszenia ryzyka i ochrony zasobów danych.

9. Architektura danych - jest projekt architektoniczny strukturalnych i niestrukturalnych systemów danych i aplikacji, który umożliwia dostępność i dystrybucję danych dla odpowiednich użytkowników.

10. Klasyfikacja i Metadane - odnosi się do metod i narzędzi wykorzystywanych do tworzenia wspólnych semantycznie definicji terminów biznesowych i informatycznych, modeli danych i repozytoriów.

11. Audyt Rejestrowania i Raportowania Informacji - odnosi się do procesów organizacyjnych do monitorowania i pomiaru wartości danych, zagrożeń i skuteczności zarządzania danymi.

Data Governance – etapy realizacji

Sygnity Business-Innovation-Now

Etap 1 – Uzgodnienie celu i zakresu projektu

Przeprowadzenie procesu oceny dojrzałości Data Governance

Najlepszym sposobem dla rozpoczęcia programu Data Governance jest przeprowadzenie oceny stanu obecnego zgodnie z poniższymi wytycznymi:

- *aktualny stan*: gdzie jesteśmy dzisiaj?
- *stan w przyszłości*: gdzie chcielibyśmy być w przyszłości?
- *plan działań*: jakich ludzi, procesów, technologii i inicjatyw potrzebujemy dla określenia zasad i polityk aby wypełnić lukę pomiędzy obecnym i przyszłym stanem?

Etap 2 - Pozyskanie sponsora projektu

Organizacja musi wyznaczyć ogólnych właścicieli programu Data Governance. Z reguły identyfikowano szefa ochrony informacji, jako właściciela programu Data Governance (tzw. ABI). Obecnie, właścicielem programu Data Governance staje się pion CIO (członek zarządu odpowiedzialny za IT), a nie obszar BI czy obszar architektury danych. Data Governance może również znajdować się, zwłaszcza w bankach, w dziale ryzyka. Oto pytania, na które należy odpowiedzieć :

- czy Data Governance powinno być "własnością" działu IT czy działu biznesowego?
- w jaki sposób można wykorzystać istniejące publiczne inicjatywy Data Governance?
- które działy organizacji powinny być zaangażowane w Data Governance?

Analiza struktury organizacyjnej, wzajemnych zależności ale również precyzyjne zidentyfikowanie procesu przepływu danych i określenie kluczowych dla podejmowania decyzji miejsc i osób spowoduje, że projekt pozyska sponsorów dających gwarancję jego realizacji.

Data Governance – etapy realizacji

Sygnity Business-Innovation-Now

Etap 3 – Budowa Mapy Drogowej

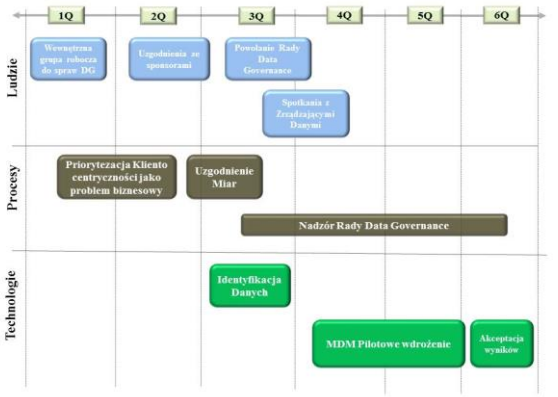
Data Governance potrzebuje opracowania planu działania w celu zniwelowania różnic między obecnym stanem i osiągnięcia pożądanego stanu przyszłego. Program Data Governance musi również zawierać "szybkie sukcesy"- obszary, w których inicjatywa może być bliska długoterminowej wartości biznesowej.

Trzy pod-zadania ułatwiają budowę i rozwój mapy drogowej Data Governance:

1) Podsumowanie wyników badania dojrzałości Data Governance,

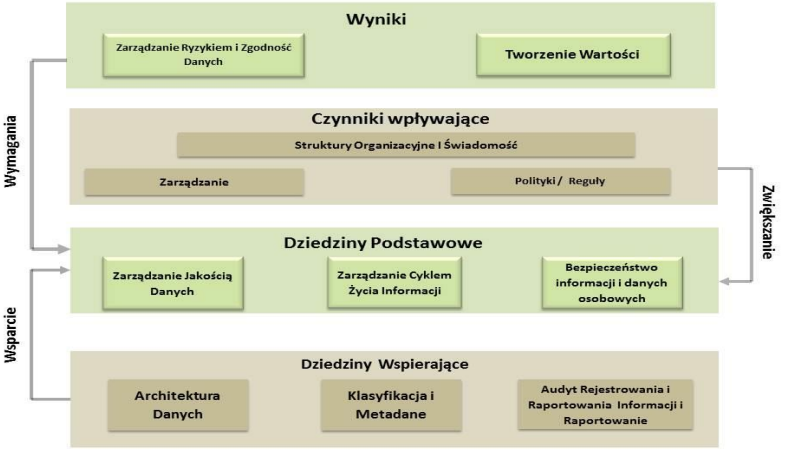
2) Stworzenie listy kluczowych ludzi, procesów i inicjatyw technologicznych niezbędnych dla wypełnienia luk wyróżnionych podczas oceny.

3) Tworzenie planu działania na podstawie priorytetów dla kluczowych inicjatyw.



Data Governance - powiązanie wymiarów

Wyniki – ostateczny cel programu Data Governance. Określają wymagania dla Dziedzin Podstawowych, które warunkują osiągnięcie celu programu. Podstawą są : Architektura Danych, Metadane i Procesy wspierające.



Data Governance w instytucjach finansowych

Zalecenia Komisji Nadzoru Finansowego
dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego

8. Rekomendacja 8

Bank powinien posiadać sformalizowane zasady zarządzania danymi wykorzystywanymi w ramach prowadzonej działalności, obejmujące w szczególności zarządzanie architekturą oraz jakością danych i zapewniające właściwe wsparcie działalności banku.

Zarządzanie architekturą danych

8.1. Bank powinien dysponować wiedzą dotyczącą tego, jakie dane przetwarzane są w ramach prowadzonej przez niego działalności, jakie są ich źródła (w tym z określeniem, czy są to źródła wewnętrzne, czy zewnętrzne) oraz w jakich jednostkach, procesach i systemach realizowane jest to przetwarzanie. W tym celu bank powinien przeprowadzić inwentaryzację przetwarzanych danych oraz systematycznie przeglądać rezultaty tej inwentaryzacji pod kątem zgodności ze stanem faktycznym. Bank powinien również przeanalizować zasadność (uwzględniając w szczególności skalę i specyfikę prowadzonej działalności oraz poziom złożoności środowiska teleinformatycznego) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wykorzystania elektronicznego repozytorium w celu przeprowadzenia ww. inwentaryzacji i gromadzenia jej rezultatów.

8.2. Zakres i poziom szczegółowości powyższej inwentaryzacji powinny być uzależnione od skali działalności banku oraz określonej przez bank istotności poszczególnych grup danych (tj. danych dotyczących pewnego, określonego przez bank obszaru jego działalności). W przypadku istotnych grup danych bank powinien opracować ich szczegółową dokumentację, zawierającą modele tych danych, opisujące m.in. zależności pomiędzy ich poszczególnymi elementami oraz przepływy pomiędzy systemami informatycznymi, jak również posiadać odpowiednie zasady (polityki, standardy, procedury itp.) przetwarzania tych danych.

8.3. Do każdej zinwentaryzowanej grupy danych (lub jej podzbioru) powinien zostać przypisany podmiot (jednostka organizacyjna, rola, osoba itp.), który jest ostatecznie odpowiedzialny za jakość tych danych i nadzór nad nimi, w szczególności w zakresie zarządzania związanymi z nimi uprawnieniami i udziału w rozwoju systemów informatycznych, w których są one przetwarzane.

Data Governance w instytucjach finansowych

Sygnity

Zalecenia Komisji Nadzoru Finansowego

Zarządzanie jakością danych

8.4. W banku powinny obowiązywać sformalizowane zasady zarządzania jakością danych, których zakres i poziom szczegółowości powinny być uzależnione od skali i specyfiki działalności banku oraz określonej przez bank istotności poszczególnych grup danych. Niezależnie od przyjętej przez bank metodologii i nomenklatury w tym zakresie, zasady te powinny obejmować:

- okresowe dokonywanie oceny jakości danych,
- dokonywanie czyszczenia danych,
- identyfikację przyczyn błędów występujących w danych,
- bieżące monitorowanie jakości danych.

8.5. Dokonując okresowej oceny jakości danych, bank powinien w szczególności identyfikować błędy w danych oraz badać ich wpływ na swoją działalność. Bank powinien także upewniać się, że przetwarzane dane są odpowiednie z perspektywy zarządzania (w tym pomiaru) poszczególnymi rodzajami ryzyka, jak również zaspokajania potrzeb raportowych i analitycznych ich kluczowych odbiorców – to znaczy, czy i w jakim stopniu ewentualne podjęcie błędnych decyzji wynikać może z niskiej jakości danych stanowiących ich podstawę.

8.6. Dokonując czyszczenia danych (tj. zmiany danych ocenionych jako błędne w dane odpowiednie do potrzeb i celów ich użycia) – o ile działania te realizowane są w sposób zautomatyzowany – bank powinien przyłożyć szczególną uwagę do poprawnego skonstruowania algorytmów czyszczących. Niepoprawny algorytm poprawiając jedne dane może bowiem (poprzez efekty uboczne) spowodować pogorszenie jakości innych danych.

8.9. Projektując podejście do zarządzania jakością danych – w szczególności w przypadku braku wyodrębnionej jednostki organizacyjnej odpowiedzialnej za ten obszar – bank powinien zapewnić, aby zakresy odpowiedzialności i podział zadań w tym zakresie były jednoznacznie i precyzyjnie określone. Bank powinien również zapewnić zachowanie odpowiedniego stopnia poufności danych wykorzystywanych w procesie zarządzania jakością danych.

Data Governance w instytucjach finansowych

Sygnity

Zalecenia Komisji Nadzoru Finansowego

Zarządzanie jakością danych

8.11. Bank powinien tworzyć kulturę organizacyjną, w której kładzie się nacisk na zapewnianie odpowiedniej jakości danych wprowadzanych przez pracowników do systemów informatycznych.

8.12. Podejście banku do zarządzania jakością danych powinno uwzględniać szczególne uwarunkowania związane z ograniczoną kontrolą banku nad jakością danych pochodzących ze źródeł zewnętrznych (takich jak np. międzybankowe systemy wymiany informacji BIK, AMRON czy ZORO). Bank powinien podejmować działania mające na celu umożliwienie dokonania oceny jakości tych danych oraz jej poprawę, w szczególności poprzez wymaganie od dostawców danych zewnętrznych przedstawiania potwierdzenia odpowiedniej jakości danych (popartego wynikami niezależnego audytu zewnętrznego). Bank powinien również przykładać szczególną uwagę do jakości danych wprowadzanych przez niego do baz zewnętrznych.

8.12. Podejście towarzystwa do zarządzania jakością danych powinno uwzględniać szczególne uwarunkowania związane z ograniczoną kontrolą towarzystwa nad jakością danych pochodzących ze źródeł zewnętrznych (takich jak np. agenci, brokerzy, likwidatorzy szkód, operatorzy medyczni, Ośrodek Informacji Ubezpieczeniowego Funduszu Gwarancyjnego (OI UFG), Polskie Biuro Ubezpieczycieli Komunikacyjnych (PBUK)). Towarzystwo powinno podejmować działania mające na celu umożliwienie dokonania oceny jakości tych danych oraz jej poprawę, w szczególności poprzez wymaganie od dostawców danych zewnętrznych przedstawiania potwierdzenia odpowiedniej jakości danych (np. popartego wynikami niezależnego audytu zewnętrznego). Towarzystwo powinno również przykładać szczególną wagę do jakości danych wprowadzanych przez nie do baz zewnętrznych (np. UKNF, OI UFG, PBUK, Centralna Ewidencja Pojazdów i Kierowców).

8.13. W związku z tym, że jakość danych przetwarzanych w środowisku teleinformatycznym w istotny sposób wpływa na jakość zarządzania bankiem, a jednocześnie często odbiorcy tych danych nie mają bezpośredniego wpływu na ich jakość (np. w przypadku danych wprowadzanych w ramach obszaru sprzedaży, a następnie wykorzystywanych przez obszar ryzyka), bank powinien przeanalizować zasadność (uwzględniając w szczególności specyfikę swojej struktury organizacyjnej oraz realizowanych procesów przetwarzania danych) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wyznaczenia lub wskazania komitetu właściwego do spraw zarządzania jakością danych.

Data Governance – normy

Sygnity

PN-ISO/IEC 27001:2014-12

PN-ISO/IEC 27001 „Systemy zarządzania bezpieczeństwem informacji – Wymagania" to jedyna norma określająca wymagania dotyczące budowania systemów zarządzania bezpieczeństwem informacji (SZBI), a jednocześnie stanowiąca kryterium ich oceny. Norma ta została opracowana w celu zapewnienia wyboru adekwatnych i proporcjonalnych środków w obszarze bezpieczeństwa osobowego, fizycznego oraz informatycznego przy jednoczesnym zachowaniu zgodności z prawem.

Norma nie określa szczegółowych rozwiązań technicznych, lecz wskazuje obszary, które należy uregulować. Sposób zabezpieczenia tych obszarów zależy od samej organizacji i powinien być oparty na przeprowadzonej analizie ryzyka. Norma szeroko definiuje pojęcie bezpieczeństwa informacji, uwzględniając zagadnienia od rozwoju kompetencji personelu aż po środki techniczne służące ochronie przed włamaniami komputerowymi.

Wymogi określone w Normie Międzynarodowej są ogólne i mają zastosowanie do wszystkich organizacji, niezależnie od typu, wielkości i charakteru. Wyłączenie któregokolwiek z wymagań określonych w Rozdziałach 4 do 10 jest nieakceptowalne, w wypadku gdy organizacja deklaruje zgodność z niniejszą Normą Międzynarodową.

Norma PN-ISO/IEC 27001 pozwala kształtować system zarządzania bezpieczeństwem informacji w organizacji zgodnie z ustalonymi kryteriami – z jednej strony stanowiąc podstawy do jego budowania, z drugiej natomiast dając podstawy do certyfikacji tego systemu przez niezależną stronę trzecią.

Certyfikacja na zgodność z PN-ISO/IEC 27001 oznacza, że organizacja:

- określiła wymagania dotyczące bezpieczeństwa przetwarzanych przez nią informacji,
- skutecznie wdrożyła odpowiednie zabezpieczenia,
- w sposób profesjonalny i procesowy zarządza bezpieczeństwem swoich zasobów informacyjnych oraz informacji powierzanych przez klientów, pracowników, partnerów handlowych i inne strony zainteresowane,
- jest świadoma konsekwencji utraty lub naruszenia bezpieczeństwa informacji,
- demonstruje swoją wiarygodność jako partnera biznesowego.

2 grudnia 2014 roku PN-ISO/IEC 27001:2007 została wycofana i zastąpiona normą PN-ISO/IEC 27001:2014-12

Data Governance – normy

Sygnity

Przykłady zaleceń normy ISO 27001

10.7.3	Procedury postępowania z inform
16	Zaleca się wdrożenie procedur po przechowywania w celu ochrony i ujawnieniem lub niewłaściwym uż
16.1	Czy sporządzona została procedura post przekazywania informacji zgodnie z jej kl
16.2	Czy procedura postępowania, przetwarz zgodnie z jej klasyfikacją określa sposób ich poziome klasyfikacji?
16.3	Czy został ograniczony dostęp do inform personelu?
16.4	Czy utrzymywany jest formalny rejestr au
16.5	Czy określone zostały mechanizmy kontr wejściowych?
16.6	Czy określone zostały mechanizmy kontr zakończenia przetwarzania?
16.7	Czy określone zostały mechanizmy kontr
16.8	Czy rozpowszechnianie danych jest ograniczone do minimum?
16.9	Czy wszystkie kopie nośnika informacji zawierają oznaczenie autoryzowanych odbiorców?
16.10	Czy dane oczekujące na wyjściu są chronione zgodnie z ich poziomem wrażliwości?
16.11	Czy listy dystrybucyjne nośników oraz autoryzowanych odbiorców są regularnie przeglądane?

10.8.5	Biznesowe systemy informacyjne
10	Zaleca się opracowanie i wdrożenie polityk i procedur dla ochrony informacji związanych z połączeniami między biznesowymi systemami informacyjnymi.
10.1	Czy zostały opracowane i wdrożone polityki i procedury dla ochrony informacji związanych z połączeniami między biznesowymi systemami informacyjnymi?
10.2	Czy określone zostały znane podatności systemów administracyjnych i księgowych, w których informacje są współużytkowane przez różne części organizacji?
10.3	Czy określona została podatność informacji w biznesowych systemach informacyjnych (np.. Nagrywanie rozmów telefonicznych lub konferencyjnych, poufność rozmów, przechowywanie faksów, otwieranie i dystrybucja poczty)?
10.4	Czy określone zostały polityki i wdrożone odpowiednie zabezpieczenia dla zarządzania współużytkowaniem informacji?
10.5	Czy dostęp do kalendarzy spotkań personelu jest ograniczony (w szczególności personelu pracującego nad wrażliwymi projektami)?
10.6	Czy określone zostały kategorie personelu, wykonawców lub partnerów biznesowych, którzy mogą korzystać z systemów, oraz lokalizacji, z których takich dostęp może być zrealizowany?
10.7	Czy dla biznesowych systemów informacyjnych został określone wymagania na wypadek konieczności ich odtworzenia?
10.8	Czy dla biznesowych systemów informacyjnych został określony sposób tworzenie i przechowywania kopii zapasowych?

Data Governance - podsumowanie

Sygnity

- DG - porządkuje proces przetwarzania danych:
  - Ocena źródeł danych
  - Weryfikacja ich poprawności
  - Bezpieczeństwo przetwarzania
  - Obniżanie ryzyka utraty reputacji
  - Racjonalizacja kosztów przetwarzania danych
- Zgodność z przepisami prawa:
  - Szczególne np. rekomendacje / wytyczne KNF
  - Ustawa o Ochronie Danych Osobowych
  - Zgodność z normami

Dziękuję