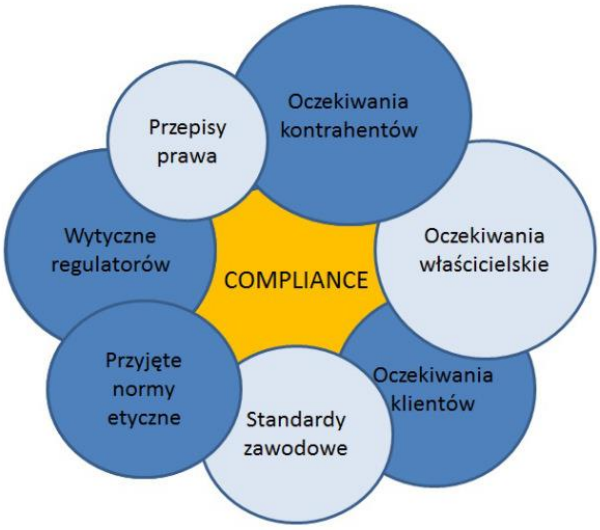
Norma ISO 19600 – próba standaryzacji zarządzania ryzykiem braku zgodności (compliance) - zagadnienia wstępne

Grzegorz Włodarczyk

Starszy ekspert ds. compliance

Od wielu lat obserwujemy na świecie (także w Polsce) gwałtowny wzrost znaczenia funkcji zarządzania ryzykiem braku zgodności, oraz samego zarządzania wskazanym ryzykiem czyli compliance. Compliance to funkcja w firmie, co do zasady o charakterze prewencyjnym[1], choć w ramach tzw. postępowań wyjaśniających (kwestie związane z incydentami braku zgodności) może działać także następczo, mająca na celu eliminowanie niezgodności (i zapobieganie potencjalnym niezgodnościom) z przepisami prawa powszechnie obowiązującego, wytycznymi, stanowiskami i rekomendacjami regulatorów, izb zawodowych, organizacji etc., także z zasadami postępowania, corporate governance czy w końcu zasadami etycznymi danej firmy[2](p. Rys. 1 - materie compliance – opracowanie własne autora).



[1] Tak Grynfelder J., Funkcja compliance, http://www.forumcompliance.com/4701.html.

[2] Por. Włodarczyk G., Kodeksy etyczne – zagadnienia wstępne.

Powstanie i gwałtowny rozwój funkcji compliance na świecie związany jest z dużymi aferami typu afera Enron'u czy kryzysami na rynkach (np. finansowym). Jako ich wynik powstały regulacje amerykańskie: Sorbanes – Oxley Act[3], The Foreign Corrupt Practices Act[4], oraz europejskie – np. Markets in Financial Instruments Directive (MiFID), które wprost, dla danych branż, czy typów przedsiębiorstw, wprowadziły obowiązek umiejscowienia w strukturach firmy jednostki ds. zapewnienia zgodności (compliance)[5].

Jako że, nie istnieje jedna ogólnoświatowa, ogólnorynkowa czy ogólnobranżowa regulacja dotycząca compliance, poszczególne branże, bądź to w ramach samoregulacji, bądź w ramach odrębnych przepisów prawa powszechnie obowiązującego, wprowadzają funkcję compliance do wewnętrznych porządków prawnych. Wydaje się, że w tej materii prym wiedzie sektor bankowy i kapitałowy – wystarczy spojrzeć tylko na dokumenty z ostatnich kilku lat, wprowadzające obowiązek posiadania jednostki ds. zapewnienia zgodności w strukturach firm.[6] Niestety pozostałe branże, poza sektorem finansowym, wypadają dość blado (pozytywne przejawy

[3] Dostępny w Biliotece Kongresu, http://www.loc.gov.

[4] PUBLIC LAW 95-213—DEC. 19, 1977.

[5] W języku polskim określeń na jednostkę bądź osobę wykonującą zadania z zakresu zarządzania ryzykiem braku zgodności, czy ogólniej zapewnienia zgodności działalności przedsiębiorstwa z przepisami prawa etc. jest wiele – ja stosować będe zamiennie „jednostka ds. zapewnienia zgodności" oraz „compliance".

[6] Por. w szczególności: ISO 14001, OHSAS 18001, Komitet Bazylejski ds. Nadzoru Bankowego, Zgodność i funkcja zapewnienia zgodności w bankach, Kwiecień 2005, ESMA Europejski Urząd Nadzoru Giełd i Papierów Wartościowych) - Wytyczne w sprawie określonych aspektów wymogów dyrektywy MiFID dotyczących komórki ds. nadzoru zgodności z prawem, 25 czerwca 2012 r. | ESMA/2012/388, przepisy Rozporządzenia Ministra Finansów z dnia 24 września 2012 r. w sprawie określenia szczegółowych warunków technicznych i organizacyjnych dla firm inwestycyjnych, banków, o których mowa w art. 70 ust. 2 ustawy o obrocie instrumentami finansowymi, i banków powierniczych oraz warunków szacowania przez dom maklerski kapitału wewnętrznego (Dz. U. 0, poz.1072), Komisja Nadzoru Finansowego, Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach, 2012 r., Komisja Nadzoru Finansowego, Rekomendacja H dotycząca systemu kontroli wewnętrznej w bankach, 2011. Z ciekawych inicjatyw warto wskazać na podpisanie 20 maja 2014 r. porozumienia pomiędzy Komisją Nadzoru Finansowego, Giełdą Papierów Wartościowych w Warszawie S.A. oraz Centralnym Biurem Antykorpcyjnym „w zakresie organizacji szkoleń i warsztatów problemowych służących podnoszeniu kultury Compliance w spółkach notowanych na warszawskim parkiecie, z uwzględnieniem metodologii zapobiegania oraz wykrywania działań o charakterze korupcyjnym oraz działań niezgodnych z prawem rynku kapitałowego".

zwiększenia roli compliance można obserwować w firmach farmaceutycznych, telekomunikacyjnych, spółkach notowanych na giełdach, w sektorze chemicznym, energetycznym czy niekiedy budowlanym), w szczególności w sektor MŚP, gdzie funkcja compliance w zasadzie nie istnieje.

1. Norma ISO[7] 19600 – wprowadzenie

Norma ISO 19600[8] (ISO/DIS 19600 Compliance management systems - CMS) powstaje jako próba usystematyzowania kwestii zarządzania ryzykiem braku zgodności oraz stworzenia zunifikowanego systemu zarządzania ryzykiem braku zgodności, dedykowanego nie tylko dla potężnych korporacji, ale także dla firm z obszaru MŚP.

U źródeł powstania normy ISO 19600 leży inicjatywa australijska – w 2012 r. Australia zaproponowała rozpoczęcie prac nad normą ISO dotyczącą funkcji compliance, opartej na australijskim standardzie AS 8306.

Norma ISO 19600 co do zasady ma akcentować podejście do compliance sensu largo tj. chociażby rozumienie funkcji compliance jako funkcji doradczej, oraz równocześnie jako funkcji kontrolnej. To także patrzenie na compliance w sposób kompleksowy i zunifikowany w ramach przedsiębiorstwa – od wdrożenia założeń polityk, przez opiniowanie wewnętrznej dokumentacji i bieżącą pomoc pracownikom, przez szkolenia, aż po kontrolę i stałe ulepszanie systemu compliance. Jednocześnie norma ISO 19600 raczej ma na celu wskazanie konkretnych narzędzi, sformułowanie „miękkich" wytycznych, aniżeli stricte wprowadzenie ścisłych wymagań. Tego typu wytyczne, formułujące zalecenia, a nie wymagania, z perspektywy globalnej mogą znaleźć o wiele większe zastosowanie (jeśli ich przyjęcie miałoby być dobrowolne) w praktyce. Norma ISO 19600 powstaje jako swoisty „meta-standard"[9], określający na dużym poziomie ogólności podstawowe wytyczne dla funkcji compliance. Zaletą tak skonstruowanego „meta-standardu" jest połączenie w jednym dokumencie najważniejszych zasad

[7] International Organization for Standardization, czyli Międzynarodowa Organizacja Normalizacyjna to organizacja pozarządowa zrzeszająca krajowe organizacje normalizacyjne.

[8] Tekst projektu normy dostępny do kupienia na stronie www ISO http://www.iso.org.

[9] Tzw. HLS – High Level Structure.

wynikających ze standardów i dobrych praktyk sektorowych, standardów rodzajowych, wytycznych rodzajowych, standardów dokumentacyjnych etc.

Jedną z najważniejszych wartości normy ISO 19600 jest przyjęcie założenia, znanego chociażby z wytycznych ESMA, czy bardziej generalnie ustawodawstwa MiFID, tj. przyjęcia swoistej zasady proporcjonalności przy wdrożeniu normy. Zasada proporcjonalności pozwala przedsiębiorstwom (np. MŚP) dostosować się, przy dołożeniu należytej staranności, w sposób proporcjonalny do założeń normy ISO 19600 (co do zasady bez obniżania standardów). Jest to o tyle logiczne, że o ile standardy, czy wytyczne mogą być tożsame tak dla dużych korporacji, jak i dla np. MŚP, to już konkretne wymogi strukturalne już nie zawsze, gdyż mogłoby to prowadzić bądź do obniżenia standardów dla dużych korporacji („równanie w dół"), bądź to do nadmiernego obciążenia obowiązkami MŚP („równanie w górę"). Wydaje się, że zasada proporcjonalności rozwiązuje wskazane problemy.

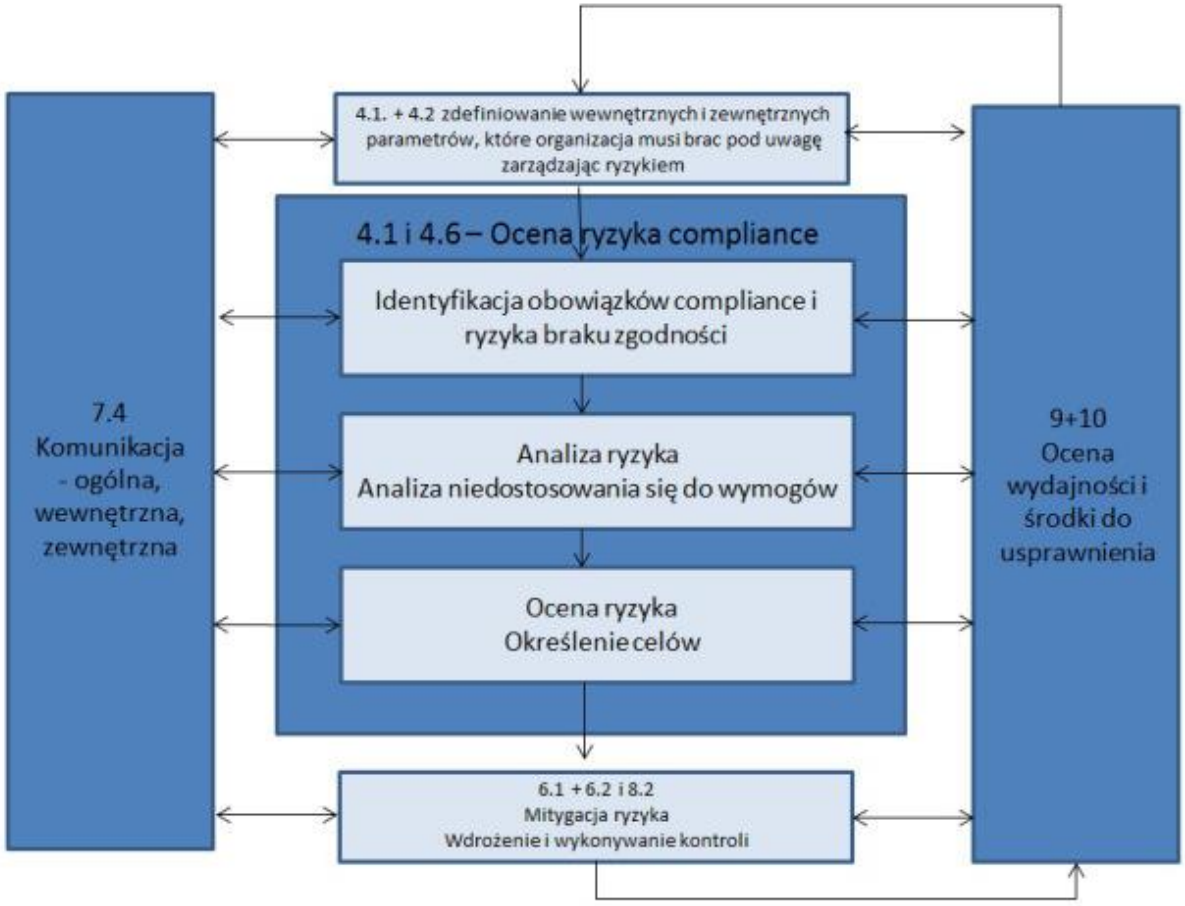
2. Zalety Normy ISO 19600:

- Czerpanie z najlepszych ogólnoświatowych wzorców.
- Kompleksowe ujęcie kwestii compliance.
- Konstrukcja na zasadach „meta-standardu".
- Zasada proporcjonalności.
- Podejście oparte na analizie ryzyka.

Co do zasady CMS w normie ISO 19600 oparte jest o podejście oparte na analizie ryzyka, co zresztą wydaje się obecnie być jednym słusznym spojrzeniem na compliance. Co ciekawe norma ISO 19600 sięga po znaną już i sprawdzoną metodykę zarządzania ryzykiem, określoną w normie ISO 31000[10] (p. Rys. - CMS oparty na analizie ryzyka – za. Bleker S., Hortensius D., ISO 19600: The development of a global standard on compliance management). Tego typu podejście do funkcji compliance jest charakterystyczne dla (w zależności od metody klasyfikacji) tzw. dojrzałego bądź bardzo dojrzałego systemu compliance, zatem widać, że założenia normy ISO 19600 wpisują się w światowe trendy związane z zarządzaniem ryzykiem braku zgodności. Zarządzanie ryzykiem braku zgodności oparte jest w normie ISO 19600 na kompleksowej ocenie ryzyka compliance, która znowuż polega na identyfikacji wszelkich obowiązków compliance -

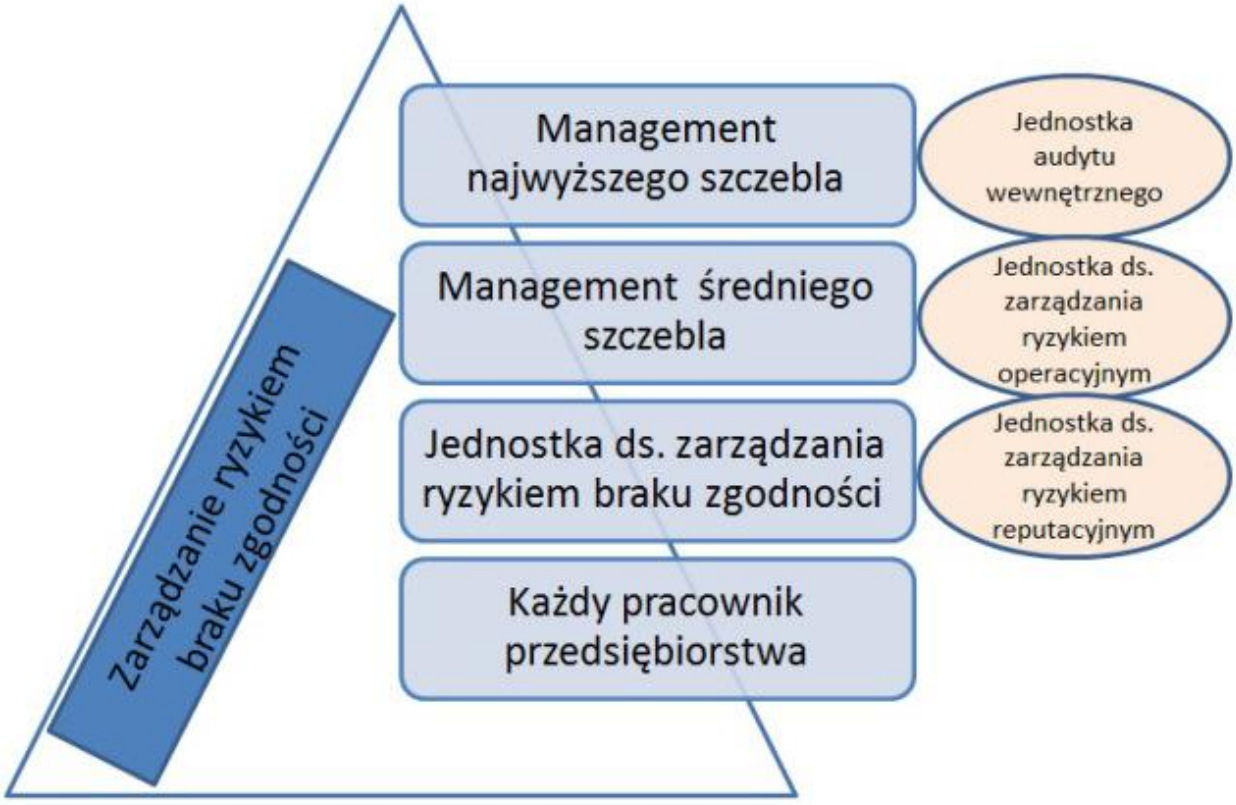
[10] PN-ISO 31000:2012 - wersja polska, Zarządzanie ryzykiem - Zasady i wytyczne.

przez analizę ryzyka, ocenę ryzyka, kontrolę zgodności, aż po wnioski i ustalenia związane z zapewnieniem zgodności, oraz ew. wnioski uzupełniające, mające na celu usprawnienie systemu compliance w przedsiębiorstwie.



Norma ISO 19600, jak wskazano powyżej, konstytuuje pełny standard zarządzania ryzykiem braku zgodności w przedsiębiorstwie. Skupia się zarówno na kwestiach stricte związanych z jednostką ds. zapewnienia zgodności, ale także na kwestiach odpowiedzialności każdego pracownika za zarządzanie ryzkiem braku zgodności, oraz na tak istotnej materii jak odpowiedzialność za compliance funkcji najwyższych w przedsiębiorstwie – managerów najwyższego i średniego szczebla. Model zarządzania ryzykiem braku zgodności i odpowiedzialności za compliance pokazuje Rys. 3 – Modelowa struktura zarządzania ryzykiem braku zgodności - opracowanie własne autora. Bardzo ważne jest współdziałanie wszystkich

„szczebli" struktury w organizacji, bez niego bowiem nie istnieje efektywne zarządzanie ryzykiem braku zgodności.



Norma ISO 19600 będzie na pewno cennym i kompleksowym materiałem pozwalającym na organizację funkcji compliance w przedsiębiorstwie. Będzie także zapewne novum dla sektora MŚP, czy innych przedsiębiorstw, które do tej pory systemu compliance nie wdrażały (dla firm o dojrzałym compliance – banków, firm inwestycyjnych, norma ISO 19600 zapewne nie wniesie nic nowego do wewnętrznego systemu zarządzania ryzykiem braku zgodności, aczkolwiek być może będzie przydatna celem usystematyzowania wszelkich odchyleń od modelowej struktury).