KPMG
cutting through complexity

Wytyczne IT i ich skutki dla zakładów ubezpieczeń

Seminarium Podkomisji ds. Audytu i Kontroli Wewnętrznej
Polskiej Izby Ubezpieczeń

21 maja 2015

Paweł Skowroński

Wstęp

Istotność służb IT oraz systemów informatycznych we współczesnej Organizacji jest niepodważalna i nieprzerwanie rośnie na przestrzeni ostatnich lat. Pozycja służb IT w dużej mierze jest pochodną stopnia uzależnienia współczesnej instytucji od narzędzi informatycznych wspierających bieżącą realizację procesów. Obecnie bez automatyzacji procesów w systemach informatycznych organizacje nie mógłby realizować swej podstawowej działalności biznesowej.

Komisja Nadzoru Finansowego, wcześniej Główny Inspektorat Nadzoru Bankowego, dostrzega ogromny wpływ jaki IT ma na działanie banków. Od 1997 rok w sposób szczególny, za pośrednictwem Rekomendacji D, regulator przedstawiał bankom wytyczne dotyczące zarządzania ryzykami towarzyszącymi systemom informatycznym.

Z każdą kolejną wersją Rekomendacja D ewoluowała, kładąc akcenty na inne zagadnienia związane z systemami informatycznymi. Znowelizowana Rekomendacja D z dnia 8 stycznia 2013 Komisji Nadzoru Finansowego zawiera bardzo istotne zmiany w podejściu komisji do technologii informatycznych. Jednym z kluczowych obszarów gdzie Komisja dostrzega istotne ryzyka jest jakość danych, będących podstawą podejmowanych w organizacjach decyzji.

KNF widząc pozytywny wpływ rekomendacji na uporządkowanie procesów kontrolnych w bankach postanowił rozszerzyć zasięg jej obowiązywania o fundusze inwestycyjne oraz sektor ubezpieczeń wydając Wytyczne IT.

Źródło: http://www.knf.gov.pl/aktualnosci/2012/rekomendacja_d.html

Wytyczne IT – skutki dla zakładów

OPÓROPÓROPÓROPÓROPÓROPÓR

Wytyczne IT – skutki dla zakładów

TOP 5

- **Analiza ryzyka jako punkt wyjścia**
- **Zwiększenie rangi obszaru IT**
- **Konieczność istotnych zmian**
- **Wzrost wydatków na uzyskanie i zapewnienie zgodności regulacyjnej**
- **Rosnąca rola Audytu Wewnętrznego**

1. Analiza ryzyka jako punkt wyjścia

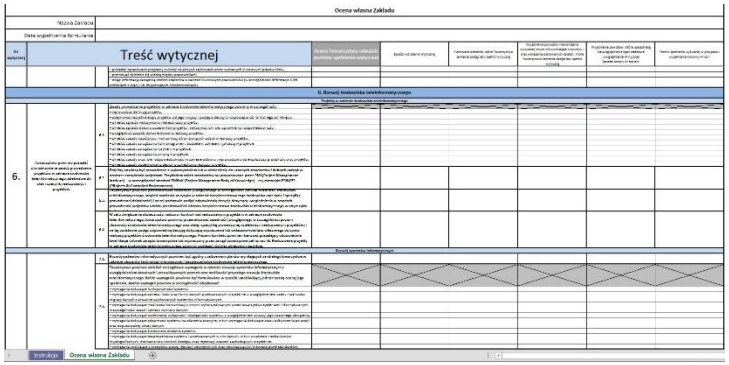
"Aby robić to, co dla Ciebie naprawdę ważne, musisz najpierw wiedzieć, co jest dla Ciebie naprawdę ważne.„

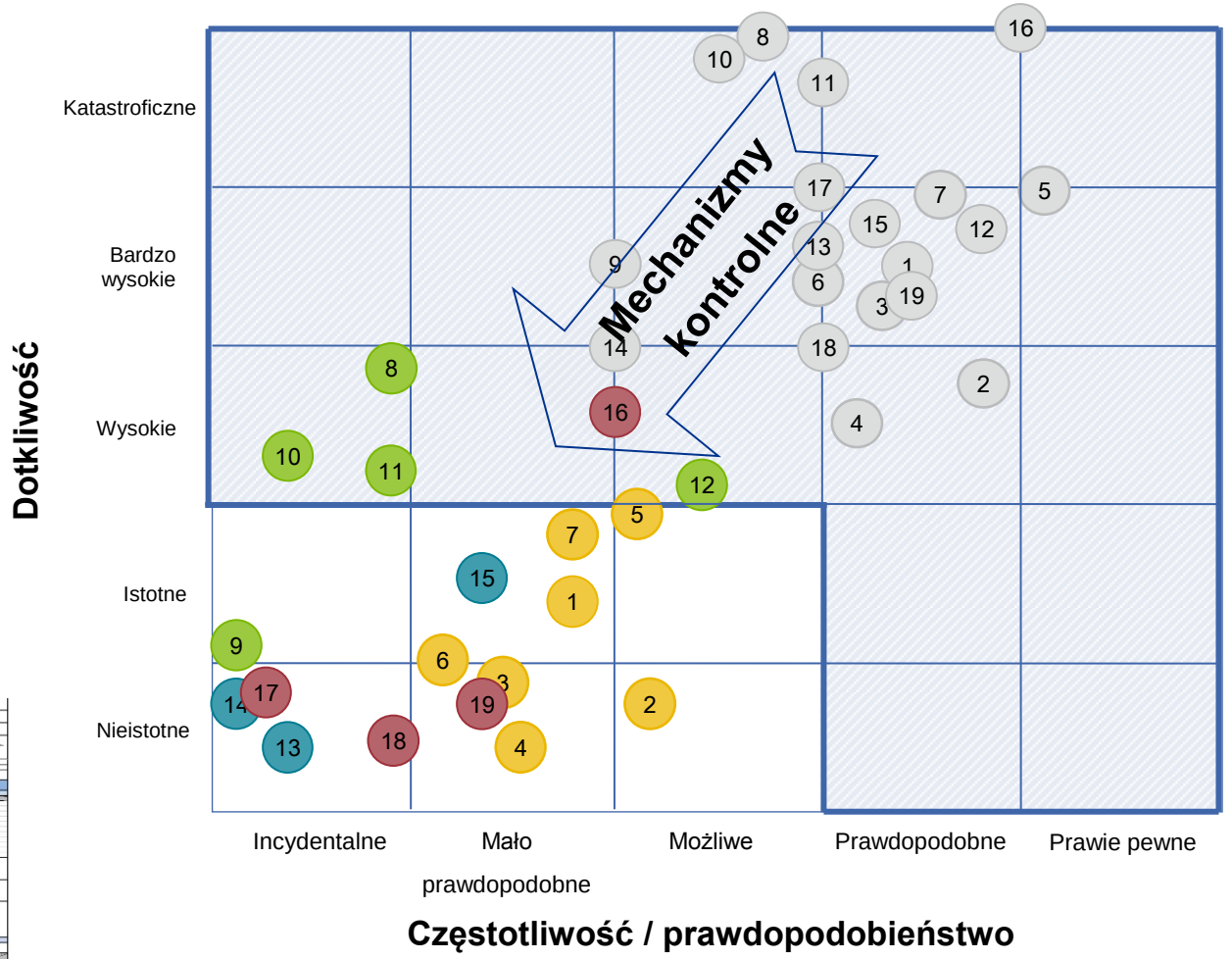
Dr. Ed Hallowell

1. Analiza ryzyka jako punkt wyjścia

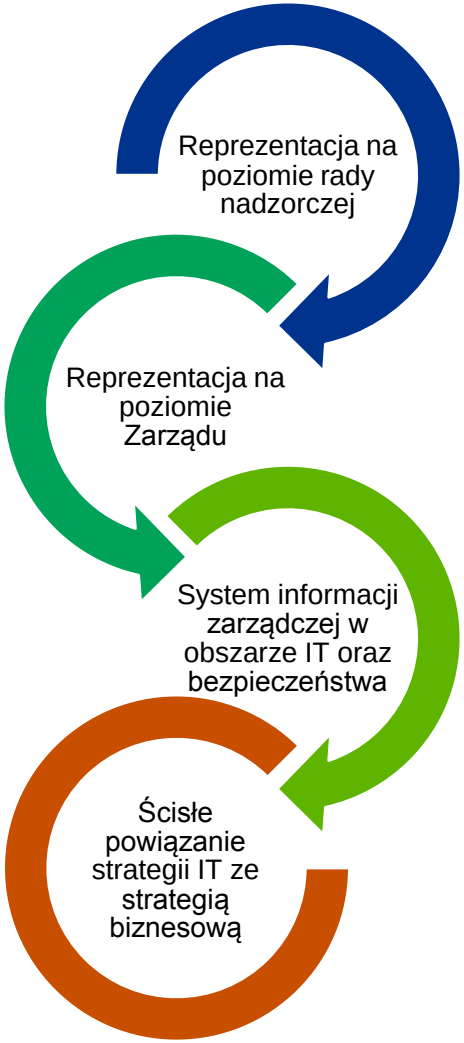
Czym jest zasada proporcjonalności?

- ❑ Powiązanie analizy ryzyka z profilem działalności i wykorzystywanymi technologiami
- ❑ Brak podejścia 0-1
- ❑ Każda decyzja o nieuzyskaniu pełnej zgodności poparta być musi uzasadnieniem (zasada comply or explain)





2. Zwiększenie rangi obszaru IT



Wytyczna 1 – Rada nadzorcza towarzystwa powinna nadzorować funkcjonowanie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, natomiast zarząd towarzystwa powinien zapewnić, aby powyższe obszary zarządzane były w sposób poprawny i efektywny.

Szczególną uwagę rada nadzorcza i zarząd towarzystwa powinni poświęcić w zakresie swoich kompetencji: **zarządzaniu bezpieczeństwem** środowiska teleinformatycznego oraz **ciągłością działania**, procesowi tworzenia i aktualizacji **strategii** w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, współpracy z zewnętrznymi **dostawcami** usług w zakresie środowiska teleinformatycznego i jego bezpieczeństwa, zapewnieniu adekwatnej struktury organizacyjnej oraz zasobów kadrowych w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, zarządzaniu jakością danych o kluczowym znaczeniu dla towarzystwa, zarządzaniu **elektronicznymi kanałami dostępu**.

Wytyczna 2 - W towarzystwie powinien funkcjonować sformalizowany system informacji zarządczej w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zapewniający każdemu z odbiorców informacji właściwy poziom wiedzy o tych obszarach.

"Strategia powinna wyrastać na błocie rynku, a nie w antyseptycznym środowisku wieży z kości słoniowej."

Al Ries, Jack Trout

2. Zwiększenie rangi obszaru IT
System Informacji Zarządczej - przykłady

Wskaźniki operacyjne

Wskaźniki operacyjne	Plan	Realizacja	Status	Tendencja	Szczegóły na stronie	Poprzedni okres
1. Inicjatywy					**3-5**	
Zaangażowanie pracowników w inicjatywy	97	98				78
Inicjatywy z przekroczonym planowanym czasem realizacji	97	98				78
2. Zarządzanie zmianami					**6-7**	
Liczba zmian zarejestrowanych	99	100				98
Liczba zmian pilnych zrealizowanych niezgodnie z SLA	100	100				98
Liczba zmian dopuszczonych warunkowo	100	100				98
Liczba zmian wycofanych	7	3				8
3. Współpraca z dostawcami zewnętrznymi					**8-9**	
Udział % zmian nierozwiązanych w terminie zgodnym z SLA - Dostawca A	810	810				820
Udział % zmian nierozwiązanych w terminie zgodnym z SLA - Dostawca B	120	120				90
Udział % zmian nierozwiązanych w terminie zgodnym z SLA - Dostawca C	20	20				17
Udział % zmian nierozwiązanych w terminie zgodnym z SLA - Dostawca D	20	20				19

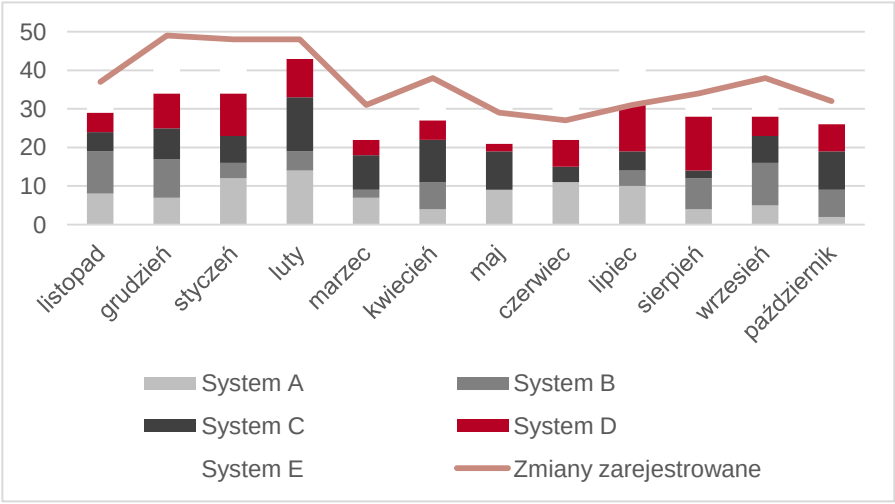
wartość ostrzegawcza
wartość bez zmian
wartość zrealizowana zgodnie z planem
spadek wartości wskaźnika względem poprzedniego okresu
wzrost wartości wskaźnika względem poprzedniego okresu

2. Zwiększenie rangi obszaru IT
System Informacji Zarządczej - przykłady

Liczba zmian zarejestrowanych i zamkniętych

W części opisowej powinny znaleźć się m.in. takie informacje jak:

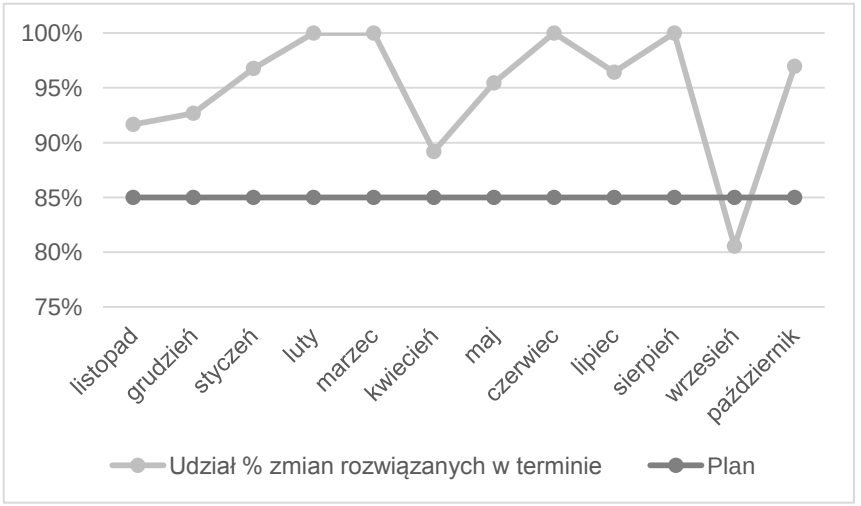
- Przyczyny znaczących odchyleń liczby zmian zarejestrowanych,
- Przyczyny odchyleń liczby zmian zarejestrowanych w danych systemach,
- Przyczyny odchyleń liczby zmian zamkniętych w stosunku do liczby zmian zarejestrowanych.



Zmiany pilne zrealizowane zgodnie z SLA

W części opisowej do tabeli powinny znaleźć się m.in. takie informacje jak:

- Analiza przyczyn odchyleń, dla których procent wdrożonych zmian pilnych jest niższy aniżeli poziom wyznaczony przez plan (np. jakich usług dotyczy, która grupa wsparcia była odpowiedzialna za wdrożenie zmiany, przyczyny niedotrzymania warunków SLA).

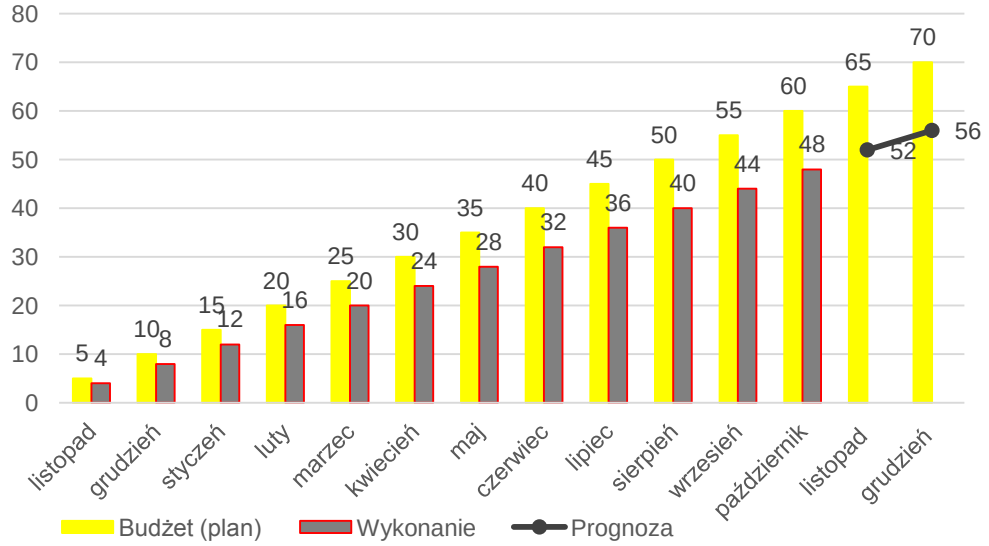


2. Zwiększenie rangi obszaru IT
System Informacji Zarządczej - przykłady

OPEX (Budżet IT)

W części opisowej powinny znaleźć się m.in. takie informacje jak:

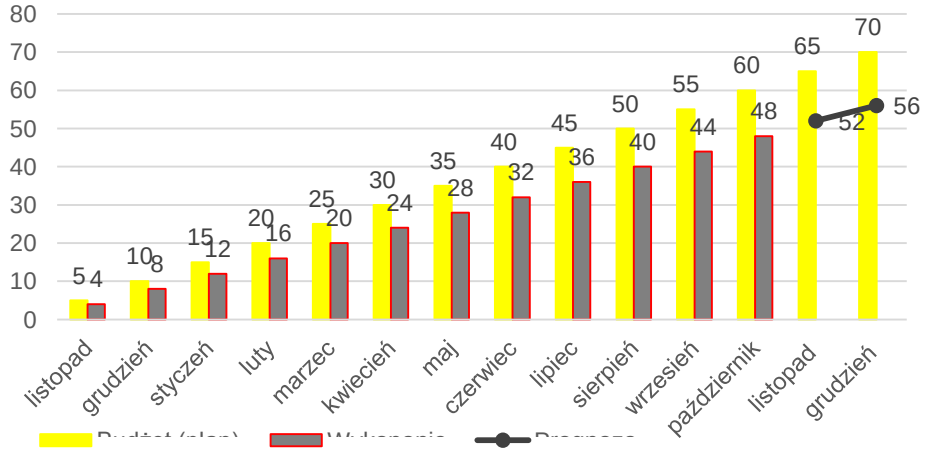
- Analiza trendu wykonania budżetu, czy jest poniżej / powyżej założonego planu,
- Wskazanie największych oszczędności / strat w porównaniu do planu budżetowego,
- Co spowodowało te oszczędności / straty (np. renegocjacje kontaktów z dostawcami zewnętrznymi),
- Wskazanie głównych grup kosztowych,
- Czy planowane jest wykorzystanie rezerwy, jeśli tak to, na jakim poziomie,
- Prognoza na przyszły okres.



CAPEX (Nakłady inwestycyjne)

W części opisowej powinny znaleźć się m.in. takie informacje jak:

- Analiza trendu wykonania budżetu, czy jest poniżej / powyżej założonego planu,
- Wskazanie inwestycji / projektów, które maja wpływ na wielkość tej pozycji (wraz z podaniem wartości).



Wskaźniki operacyjne (1/2)

Wskaźniki operacyjne	Plan	Realizacja	Status	Tendencja	Poprzedni wynik
1. Wskaźniki strategiczne					
Dostępność systemów krytycznych (%)	100%	90%			99%
Dostępność systemów strategicznych (%)	99%	100%			99%
Dostępność sieci LAN/WAN (%)	99%	100%			99%
Zajętość sieci LAN/WAN (%)	18%	16%			15%
	3	5			4,5
2. Zarządzanie projektami / inwestycjami / inicjatywami					
Zaangażowanie pracowników Pionu IT w projekty (rbh)	120	140			85
Suma wydatków Pionu IT na realizowane projekty (tys. PLN)	100	120			150
Udział Inicjatyw z przekroczonym planowanym czasem realizacji (%)	5%	4%			7%
3. Zarządzanie zmianami					
Liczba zmian zarejestrowanych	50	40			35
Udział zmian dopuszczonych warunkowo (%)	10%	7%			8%
Udział zmian wycofanych (%)	9%	6%			8%
Udział zmian pilnych zrealizowanych niezgodnie z SLA (%)	0%	5%			0%
4. Zarządzanie incydentami					
Liczba zarejestrowanych incydentów	25	23			30
Udział incydentów o priorytecie krytycznym (%)	4%	5%			5
Udział incydentów nierozwiązanych zgodnie z SLA (%)	0%	2%			0%
Średni czas realizacji incydentu o priorytecie krytycznym (h)	2	1,5			1,8

2. Zwiększenie rangi obszaru IT
System Informacji Zarządczej - przykłady

Dostępność krytycznych systemów

Średnia dostępność systemów w III kwartale roku 2014 wyniosła 99,73%. Średnia niedostępność w miesiącu 0:49:52.

Najniższą dostępność odnotował system A. Odnotowano 100% dostępność w przypadku 3 systemów.

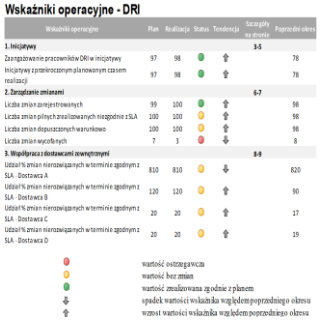
Przyczyny przekroczenia poziomu ostrzegawczego (komórki zaznaczone na żółto) oraz poziomu krytycznego (komórki zaznaczone na czerwono), w tym lista awarii, które miały wpływ na obniżenie dostępności poszczególnych systemów / usług.

Dostępność usługi (%)													
Nazwa systemu	Średnia 2013	2014 styczeń	2014 luty	2014 marzec	Średnia 1Q2014	2014 kwiecień	2014 maj	2014 czerwiec	Średnia 2Q2014	2014 lipiec	2014 sierpień	2014 wrzesień	Średnia 3Q2014
A	100,00%	99,99%	100,00%	100,00%	100,00%	99,98%	100,00%	100,00%	99,99%	99,99%	99,99%	99,99%	99,99%
B	100,00%	99,99%	100,00%	99,99%	99,99%	100,00%	99,97%	100,00%	99,99%	99,98%	99,98%	99,98%	99,98%
C	100,00%	100,00%	99,99%	99,99%	99,99%	99,98%	99,98%	99,99%	99,98%	99,87%	100,00%	100,00%	99,96%
D	100,00%	100,00%	99,96%	100,00%	99,99%	99,95%	98,86%	98,86%	99,22%	100,00%	99,96%	100,00%	99,99%
E	99,73%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
F	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
G	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,93%	100,00%	99,98%
H	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

KPMG

cutting through complexity™

3. Konieczność istotnych zmian



Wskaźniki operacyjne - DRI

Wskaźniki operacyjne	Plan	Realizacja	Status	Tendencja	Szczegóły na stronie	Poprzedni okres
1. Inicjatywy					3-5	
Zaangażowanie pracowników DRI w inicjatywy	97	98				78
Inicjatywy zrealizowanych planowanym czasem realizacji	97	98				78
2. Zarządzanie zmianami					6-7	
Liczba zmian zarejestrowanych	99	100				98
Liczba zmian pilnych zrealizowanych niezgodnie z SLA	100	100				98
Liczba zmian dopuszczonych warunkowo	100	100				98
Liczba zmian wycofanych	7	3				8
3. Współpraca z dostawcami zewnętrznymi					8-9	
Udział % zmian nierozwiązanych w terminie zgodnym z SLA - Dostawca A	810	810				820
Udział % zmian nierozwiązanych w terminie zgodnym z SLA - Dostawca B	120	120				90
Udział % zmian nierozwiązanych w terminie zgodnym z SLA - Dostawca C	20	20				17
Udział % zmian nierozwiązanych w terminie zgodnym z SLA - Dostawca D	20	20				19

wartość ostrzegawcza
wartość bez zmian
wartość zrealizowana zgodnie z planem
spadek wartości wskaźnika względem poprzedniego okresu
wzrost wartości wskaźnika względem poprzedniego okresu

Sformalizowany system informacji zarządczej

Bezpieczeństwo istotnym komponentem który trzeba zaadresować

Zarządzanie jakością danych

- Architektura danych
- Narzędzia EUC

Czy naprawdę musimy coś zmieniać?

3. Konieczność istotnych zmian
Bezpieczeństwo istotnym komponentem który trzeba zaadresować

Najistotniejsze wymogi bezpieczeństwa w wytycznych IT:

- Uwzględnienie kwestii bezpieczeństwa w strategii
- Uwzględnienie kwestii bezpieczeństwa w systemie informacji zarządczej
- Regularne przeprowadzanie testów penetracyjnych
- Standardy konfiguracyjne (w dużych zakładach)
- Sformalizowanie procesu zarzadzania incydentami
- Aktywna ochrona kluczowych zasobów informacyjnych
- Stosowanie adekwatnych zabezpieczeń do potrzeb i ryzyka

Zarządzanie ryzykiem bezpieczeństwa systemów informatycznych powinno być procesem ciągłym i sformalizowanym

3. Konieczność istotnych zmian
Bezpieczeństwo istotnym komponentem który trzeba zaadresować

Audyt wewnętrzny może wspierać cyberbezpieczeństwo poprzez:

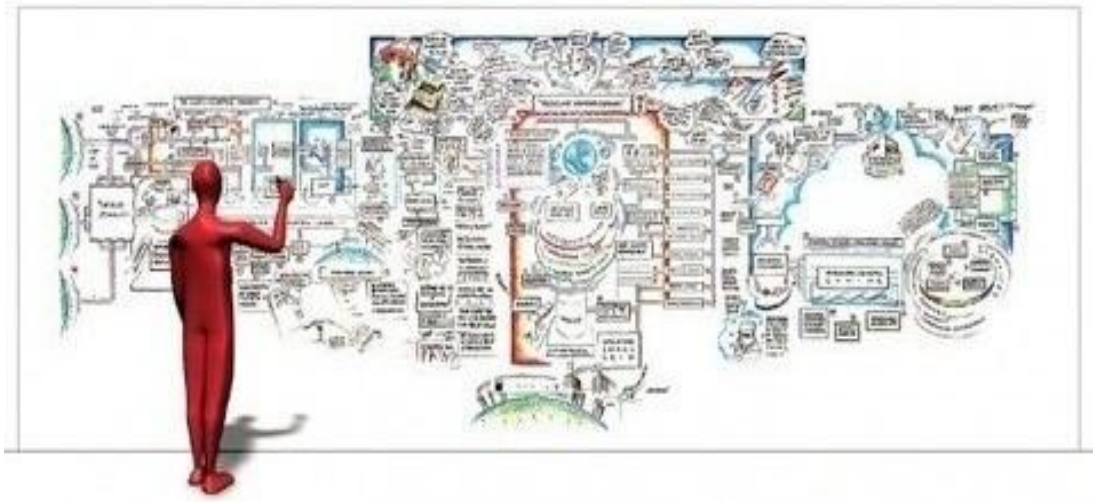
- Wsparcie w analizie ryzyka!,
- Na etapie nowych projektów poprzez weryfikację:
  - czy kwestie ochrony informacji poufnych są właściwie zaadresowane w umowach z wszystkimi stronami biorącymi udział w przedsięwzięciu (np. zewnętrzni doradcy / prawnicy),
  - czy zewnętrzni doradcy posiadają wdrożony i efektywny system zapewnienia bezpieczeństwa informacji na adekwatnym poziomie,
- Na etapie projektów technologicznych poprzez weryfikację (np. nowy system, platforma sprzedażowa):
  - czy na etapie definiowania wymagań, spisano wymagania w zakresie oczekiwanego poziomu bezpieczeństwa rozwiązań,
  - czy kompleksowa analiza ryzyka obejmująca poziom bezpieczeństwa całego rozwiązania została przeprowadzona,
  - czy w ramach procesu odbioru rozwiązania przewidziany jest etap testów bezpieczeństwa rozwiązań.
- W ramach audytu procesów operacyjnych IT weryfikacja sposobu zabezpieczeń technologicznych i organizacyjnych w obszarach takich jak Information Risk Management, Security Incident Management, Data Governance, Vendor Security Monitoring. W szczególności weryfikacja:
  - procesu identyfikacji kluczowych aktywów oraz adekwatności stosowanych zabezpieczeń
  - zasad bezpieczeństwa – czy są jasno określone, adekwatne do potrzeb i stosowane spójnie w całej organizacji (np. BYOD),
  - procesów monitorowania incydentów bezpieczeństwa,
  - adekwatność procesu szkoleń pracowniczych w zakresie bezpieczeństwa informatycznego,
  - technicznych aspektów bezpieczeństwa poprzez regularne audyty techniczne (np. testy penetracyjne danego obszaru).

3. Konieczność istotnych zmian
Zarządzanie Jakością Danych

Zarządzanie jakością danych jest ważne ponieważ informacja jest najwyższą wartością Organizacji.

Dostęp do informacji posiadającej takie atrybuty jak: dostępna, kompletna, rzetelna pozwoli na:

- budowę przewagi konkurencyjnej, chociażby poprzez lepsze wykorzystanie posiadanych informacji o swoich klientach,
- ograniczenie kosztów związanych z administracją danymi, zwłaszcza danymi stałymi,
- świadome zarządzanie ryzkiem podejmowanych decyzji.



3. Konieczność istotnych zmian
Zarządzanie Jakością Danych - Przyczyny

Jakość elektronicznych danych opiera się na procesie, który rozpoczyna się w momencie ich wprowadzenia lub ich wygenerowania w systemów źródłowych, a kończy się z chwilą wygenerowania finalnego produktu (np. raportu).

Przyczyny problemów z jakością danych

- Mnogość systemów źródłowych
- Ręczne wprowadzanie danych (często wielokrotne, w różnych systemach)
- Brak systemowych mechanizmów walidacji (lub luki w tych mechanizmach) danych wprowadzanych w trybie on-line
- Brak określonych struktur odpowiedzialnych za weryfikację danych
- Brak procedur dotyczących czyszczenia danych
- Niespójne definicje/słowniki danych pomiędzy systemami
- Brak systemowych mechanizmów (np. reguły walidacji) wspierających czyszczenie danych
- Niekreślona odpowiedzialność za jakość danych oraz ograniczone zaangażowanie biznesu w proces zarządzania danymi

Potencjalne ryzyka

- Niespójne (błędne) informacje na raportach końcowych
- Brak wiarygodności danych i raportów, co prowadzi do ograniczenia zaufania ze strony użytkowników, ogranicza korzystanie z systemów dostępnych sprawozdawczych i budowy własnych rozwiązań
- Brak podstaw, lub błędna założenia w procesie podejmowania decyzji

Dane stanowią aktywa całej Organizacji i cała Organizacja ponosi odpowiedzialność za ich jakość.

3. Konieczność istotnych zmian
Zarządzanie Jakością Danych - Korzyści

Dane istotne dla Organizacji będące również w zakresie Wytycznych IT / Solvency

Dane klienckie | **Polityki** | **Produkty** | **Ryzyka** | **Aktywa** | **Dane finansowe** | **Likwidacja szkód**

Przykładowe korzyści możliwe do osiągnięcia poprzez zwiększenie jakości danych

Zwiększenie sprzedaży

- **Możliwości sprzedażowe**
  - Możliwości sprzedaży produktów dodatkowych, tańszych lub droższych dzięki poprawionym / dokładniejszym profilom klientów
  - Lepsze dane dotyczące profilu ryzyka klienta pomagające w precyzyjnej wycenie produktów
- **Kampanie**
  - Kampanie oparte o profile zachowań Klientów

Ograniczenie kosztów

- **Identyfikacja nadużyć**
  - Lepsza jakość danych prowadząca do sprawniejszego systemu konroli wewnętrznej oraz identyfikacji nadużyć
  - Lepsze ukierunkowanie wysiłków na produkty o zwiększonym ryzyku
- **Koszty zarządzania danymi**
  - Ograncizenie kosztów wprowadzania danych i nadzoru nad ich jakością

Postrzeganie Klientów

- **Komunikacja**:
  - Bardziej precyzyjne komunikaty adresowane do właściwych klientów, we właściwym czasie oraz poprzez właściwe kanały komunikacyjne (e-mail, call center, bankowość internetowa i mobilna),
  - Lepsza ściągalność zaległości

3. Konieczność istotnych zmian
Zarządzanie Jakością Danych - Wymogi

Wymogi Wytycznych IT odnośnie jakości danych

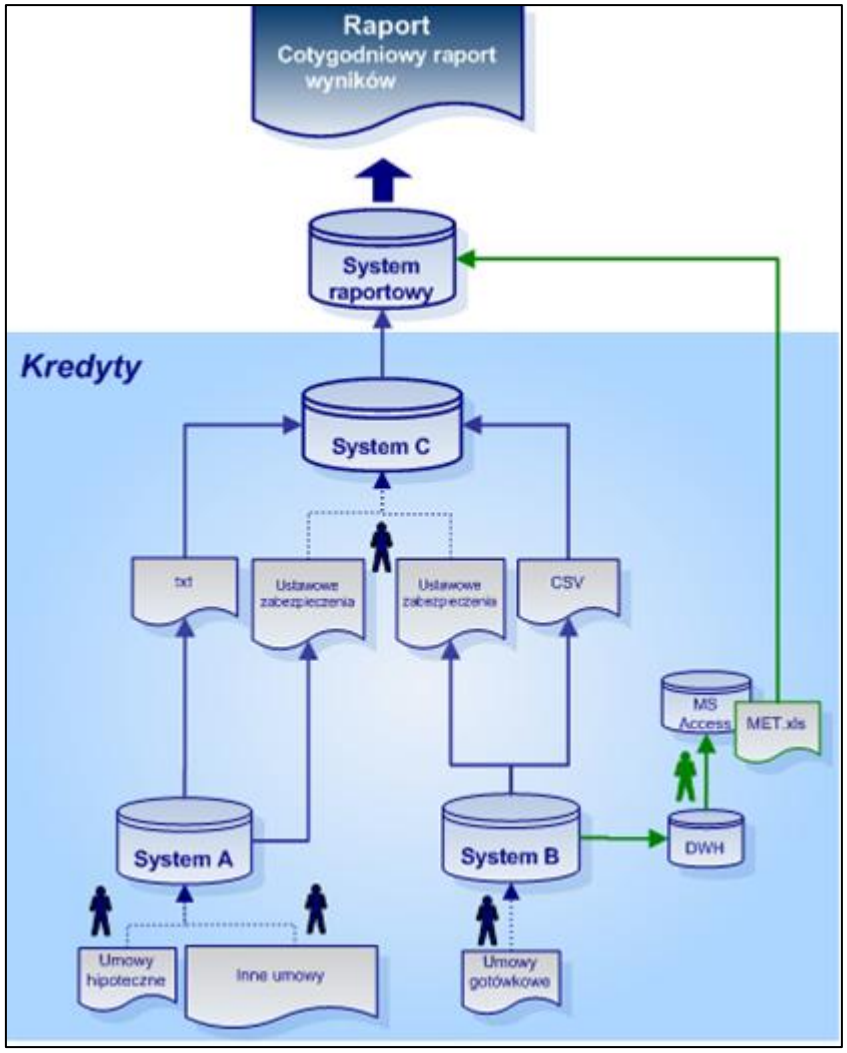
Niezbędne elementy

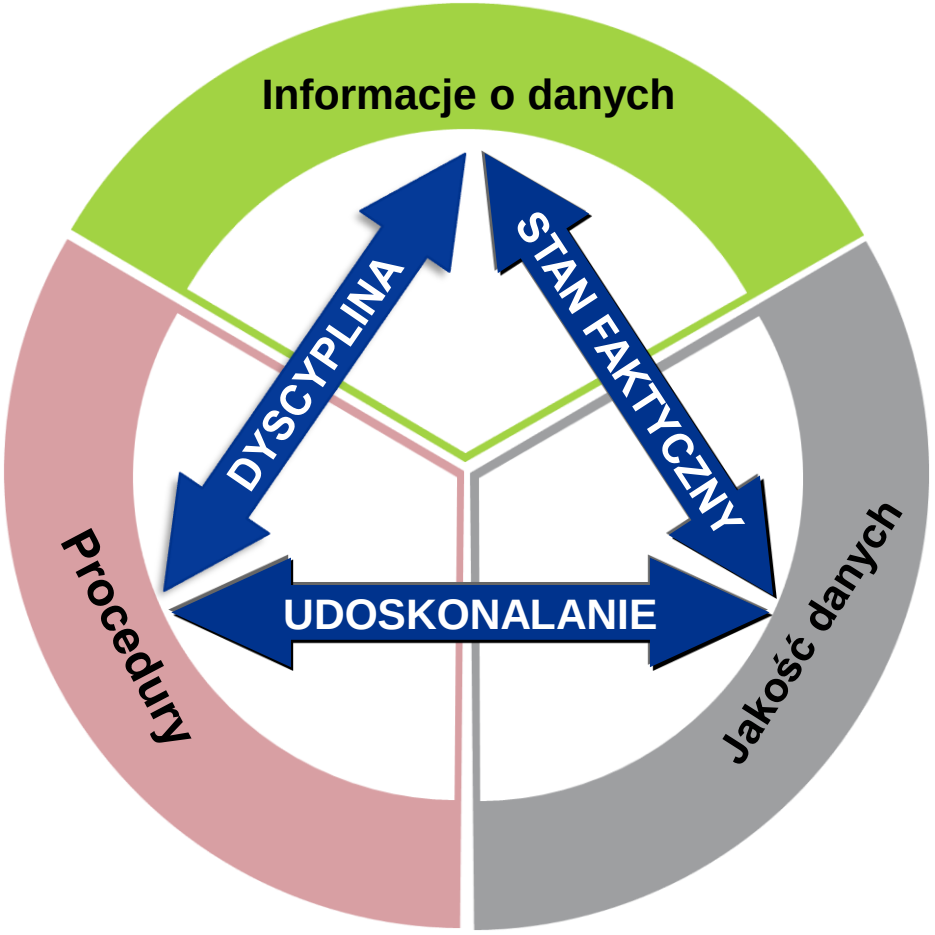
→ Zatwierdzona, pisemna **Polityka Zarządzania Danymi**	→ **Struktury i proces zarządzania danymi** → Jasno zdefiniowane **role i odpowiedzialność** za dane	→ Własny **pomysł na zarządzanie jakością danych** → Opisana **Architektura Danych**	→ **Słownik danych** specyfikujący źródła, charakterystyki oraz wykorzystanie danych	→ Zdefiniowany i wdrożony **proces oceny jakości danych** oraz proces **raportowania jakości danych**

Co to oznacza?

Organizacja musi określić cel do którego dąży w odniesieniu do problematyki jakości danych. Niezbędna jest jasna i klarowna wizja w tym zakresie.	**Niezbędne jest zdefiniowanie kto i za co jest odpowiedzialny, nie tylko na poziomie strategicznym, ale również na poziomie operacyjnym.**	**Niezbędne jest określenie co tak naprawdę oznacza wysoka jakość danych w Organizacji oraz jak to osiągnąć w określonym horyzoncie czasowym.**	**Niezbędne jest jasne zdefiniowanie poszczególnych kategorii danych, wskazanie gdzie się znajdują, kto ich używa, jaka jest ich jakość oraz upewnienie się, że definicje te są spójne.**	**Organizacja musi regularnie oceniać jakość danych i wdrażać działania naprawcze.**

3. Konieczność istotnych zmian
Zarządzanie Jakością Danych – Podejście?





3. Konieczność istotnych zmian
Zarządzanie Jakością Danych – Ilustracja efektów

CEO DASHBOARD

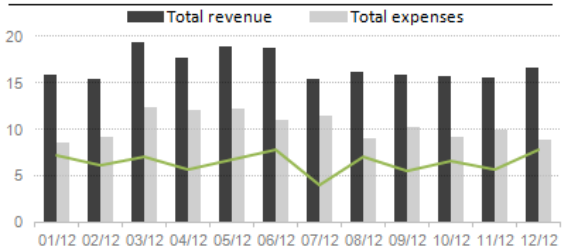
CEO | FINANCE | FINANCE DPT. | PRODUCT | IT | DISTRIBUTION | MAIN MENU

DQ: ✓

Key Metrics [YTD, in MEUR where possible]

Last 12 months	Metric	Actual	Plan	% of YTD Plan	YtY
●	Total revenue	202	230	88%	5%
●	Total expenses	125	100	125%	12%
●	Operating profit	78	130	60%	-5%
●	Loans volume	1 934	2 500	77%	23%
●	Deposit volume	3 078	3 500	88%	-15%
	No. of active clients [M]	0,96	1,05	91%	12%
●	No. of dormant client [M]	0,30	0,25	120%	-5%
	Customer satisfaction index	0,90	0,90	100%	7%
●	Share price [€]	19,55	25,00	78%	-10%
	Market capitalization	1 955	2 000	98%	-3%

Net profit trend [YTD, in MEUR]



Financial Perspective

Total revenue by division [YTD, in MEUR]

Last 12 months	Metric	Actual	Plan	% of target	YtY
●	Retail	75	100	75%	5%
●	SME	34	30	113%	12%
	Corporate	114	125	91%	-5%
	Subsidiaries	22	20	109%	23%
●	Financial markets	130	150	87%	-15%

Risk, debt and liquidity

Metric	Actual	YtY
RAROC	15%	↑
Capital adequacy ratio	14%	
Tier 1 capital ratio	12%	↓
Debt-to-equity ratio	1,30	
Interest coverage ratio	0,75	↓
Liquidity coverage ratio	1,50	
Net stable funding ratio	120%	↑

Internal Perspective

Last 12 months	Metric	Actual	Plan	% of target	YtY
●	Time-to-open current account	0:35	0:30	117%	7%
	Time-to-open savings account	0:42	0:45	93%	-5%
	Loan approval time	6 days	6 days	100%	0%
●	Average call wait time	0:03	0:02	150%	24%
	Clients reaching operator rate	0,89	0,90	99%	-3%
	ELB availability rate	0,97	0,99	98%	1%
	IT support availability rate	0,95	0,95	100%	-2%
	Satisfied SLA rate	0,92	0,95	97%	2%

Learning & Growth Perspective

Metric	Actual	YtY
No. of FTE	7500	↓
FTE fluctuation	4%	
Personnel cost	32	
MDs on training	1 232	
MDs on CSR	765	↑
Desired employer rank	7	↓

Client Perspective

Metric	Retail	YtY	SME	YtY	Corporate	YtY
No. of clients [M]	0,92	6%	0,24	-14%	0,15	7%
Net additions [M]	0,05		-0,03	↓	0,01	
Attrition rate	5,13%	↑	3,25%		3,83%	↑
Client value	€ 234	3%	€ 1 678	4%	€ 5 432	2%

External Perspective

Metric	Actual	YtY
Market share	31%	↑
Market share loans	35%	
Market share deposits	28%	
Credit rating (S&P)	AA	

Data as of: 31.08.2012
Last report run: 16.10.2012 18:00:00
Printed by ZDENDEME at: 17.10.2012 14:00:00

Report ID: CEO
Designer: MARTKOPE/Reporting
Garant: KLARJANA/Finance

KPMG

4. Wzrost wydatków na uzyskanie i zapewnienie zgodności regulacyjnej

Audyt i zapewnienie zgodności kosztuje ;)

- Siły własne (dobra znajomość organizacji lecz brak czasu oraz doświadczenia w wybranych obszarach)

  vs

  wsparcie zewnętrznych doradców (czas, doświadczenie lecz średnia znajomość organizacji i koszt wsparcia).

  Przykładem mogą być:
  - Audyt luki i powdrożeniowy Wytycznych IT
  - Audyt wybranych obszarów wymagających specyficznych kompetencji (DRP, BCP, zarządzanie tożsamością, architektura, etc.)
  - testy penetracyjne (9.21).

Etatyzacja w kontekście rozdziału obowiązków pomiędzy administratorów baz danych, aplikacji i developerów

- 5.1 Struktura organizacyjna w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego pozwalała na efektywną realizację celów towarzystwa w tych obszarach, odpowiednio do skali i profilu działalności towarzystwa oraz stopnia złożoności środowiska teleinformatycznego.
- 5.2 Podział obowiązków powinien minimalizować ryzyko błędów i nadużyć w procesach i systemach. Organizacja powinna wprowadzić separację obowiązków np. w zakresie administrowania sieciami informatycznymi, administrowania baz danych oraz aplikacji, funkcji kontrolnych.
- 5.9 Plan sukcesji kluczowych pracowników

Edukacja pracowników Organizacji w zakresie technologii informatycznych oraz ich bezpieczeństwa powinna być procesem ciągłym

- Służby IT:
  5.6 Towarzystwo powinno zapewnić, aby zarówno liczebność, jak i poziom wiedzy i kwalifikacji pracowników obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego pozwalały na bezpieczną i poprawną eksploatację całości środowiska teleinformatycznego.
  W obszarze IT powinna istnieć mapa kompetencji pracowników pozwalająca na planowy rozwój kompetencji i identyfikację kluczowych zasobów
- 12.4 Pozostali pracownicy powinni być również wspierani przez szkolenia z zakresu bezpieczeństwa

5. Rosnąca rola Audytu Wewnętrznego

Zasadnym wydaje się by audyt wewnętrzny uczestniczył w procesie uzyskiwania zgodności z Wytycznymi IT jako:

- niezależny konsultant / opiniodawca planów naprawczych,
- niezależny audytor oceniający uzyskany stopień zgodności (ostatni kwartał 2016 lub pierwszy kwartał 2017).

Wytyczne IT wymagają by audyt był prowadzony

Regularnie w oparciu o analizę ryzyka	• 22.3 Audyt obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinien być przeprowadzany regularnie oraz każdorazowo po wprowadzeniu zmian mogących znacząco wpłynąć na poziom bezpieczeństwa środowiska teleinformatycznego.
Przez audytorów o właściwych kompetencjach	• 22.2 Osoby odpowiedzialne za przeprowadzanie audytów obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny posiadać odpowiednie kwalifikacje. Audyty powinny być przeprowadzane z wykorzystaniem uznanych standardów międzynarodowych i dobrych praktyk w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego.

Uwaga: Sourcing zasobów jest dozwolony, a nawet zalecany (22.4)

5. Rosnąca rola Audytu Wewnętrznego

Więc w jakich obszarach zasadne jest specjalistyczne wsparcie:

#	Wytyczne IT	Wymagana obecność audytora IT	Możliwa realizacja bez wiedzy IT (zalecana obecność audytora IT lub podstawowa wiedza w badanym obszarze)
1	Odpowiedzialność zarządu i rady nadzorczej za obszar technologii informacyjnej i bezpieczeństwa		TAK
2	System informacji zarządczej w obszarze IT		TAK częściowo
3	Strategia IT oraz strategia bezpieczeństwa teleinformatycznego	TAK	
4	Współpraca IT z Biznesem pozwalająca na wykorzystanie potencjału IT	TAK	
5	Zasoby ludzkie IT	TAK	
6	Zarządzanie projektami IT		TAK częściowo
7	Rozwój systemów IT	TAK	
8	Zarządzanie architekturą i modelem danymi	TAK	
9	Infrastruktura IT (architektura, wydajność, pojemność)	TAK	
10	Współpraca z dostawcami		TAK
11	Dostęp logiczny i fizyczny do informacji	TAK	
12	Ochrona antywirusowa	TAK	
13	Wsparcie użytkowników końcowych		TAK częściowo
14	Kwalifikacja personelu IT	TAK	
15	Planowanie Ciągłości Działania	TAK częściowo (DRP)	TAK częściowo (BCP)
16	Zarządzanie tożsamością klientów	TAK	
17	Oprogramowanie użytkownika końcowego (również End user computing)		TAK częściowo
18	Zarządzanie bezpieczeństwem	TAK	
19	Klasyfikacja systemów i informacji		TAK
20	Zarządzanie incydentami i problemami	TAK	
21	Zgodność regulacyjna i prawna		TAK
22	Regularny audyt IT	TAK	

Pytania

cutting through complexity™

Kontakt:

Paweł Skowroński
Starszy Menadżer
Risk Consulting

T: +48 664 718 627
pskowronski@kpmg.pl