Panel V: Bezpieczeństwo informacji – jak audyt może przygotować się do zmian?

1. ***Metoda analizy ryzyka w obszarze bezpieczeństwa informacji***
2. ***Sprawdzenia wg RODO w obecnej strukturze audytu w UMK***
3. ***Audyt bezpieczeństwa informacji po reorganizacji Zespołu audytu Wewnętrznego w UMK.***

Krzysztof Pakoński
Audytor Generalny
Urząd Miasta Krakowa

XV Samorządowe Forum Kapitału i Finansów – Katowice

Październik 2017

Zasoby, które obejmuje System Zarządzania Bezpieczeństwem Informacji w UMK

- kilkanaście budynków,
- setki pomieszczeń,
- ok. 2500 użytkowników i tyleż stacji roboczych,
- kilkadziesiąt serwerów wraz z oprogramowaniem systemowym i bazodanowym,
- kilkaset urządzeń sieciowych,
- paręset większych i mniejszych aplikacji „biznesowych”.

Używaniu każdego z tych kilkunastu tysięcy „elementów systemu ” towarzyszy ryzyko.
Racjonalne zarządzanie takim zasobem **bez** wykorzystania **analizy ryzyka** jest **trudne do wyobrażenia**.

Proces Zarządzania Ryzykiem w UMK

1. **Nośnikiem ryzyk operacyjnych** są **produkty** – celem organizacji jest efektywne dostarczanie dobrych produktów.
2. **Nośnikiem ryzyk w obszarze bezpieczeństwa informacji** są wspomniane wyżej **zasoby.**
3. **Ryzyka projektowe** dotyczą 3 kluczowych parametrów: wykonanie **zakresu** (ilość i jakość), dotrzymanie **terminów** i nieprzekroczenie **kosztów**.
4. **Ryzyka programów wieloletnich dotyczą** nieosiągnięcia zadeklarowanych w czasie **celów** (wyrażonych wskaźnikowo).
5. Ryzyka strategiczne to ogólne zagrożenia dla organizacji, które w długiej perspektywie mogą przynieść poważne negatywne skutki (np. niezdolność od generowania dostatecznej nadwyżki operacyjnej).

Metodyka analizy ryzyka w obszarze bezpieczeństwa informacji

1. **Dla oceny zagrożeń** realizacji **procesów** identyfikujemy zasoby przez nie używane i najsłabsze, **najgorzej zabezpieczone aktywo wyznaczy poziom ryzyka** dla procesu.
2. Każde aktywo (czasem ich grupa) ma **właściciel**a – on **odpowiada za**:
   - **ocenę ryzyka** wrodzonego
   - **ustalenie** właściwego poziomu **zabezpieczeń**
   - **określenie zasad** użytkowania aktywa z zastosowaniem w/w zabezpieczeń
3. **Użytkownik** aktywa **odpowiada za zastosowanie** ustalonych **zabezpieczeń**.

Metodyka analizy ryzyka w obszarze bezpieczeństwa informacji

1. **Dla** każdego **aktywa** ustalamy jego **wartość jako sumę**:.
   - Wpływu na **ciągłość działania** (ocena od **1 do 3**)
   - **Rodzaju** przetwarzanej **informacji** (ocena od **1 do 3**)
   - **Kosztu odtworzenia** zasobu(ocena od **1 do 3**)

   Przy czym ocena =1 – wartość niska; ocena =3 – wysoka.

   Zatem wartość aktywa może zawierać się w przedziale od 1 do 9.
2. Kolejno ocenie podlegają :
   - **Zagrożenie** (ryzyko wrodzone) od **1** (niskie) **do 3** (wysokie)
   - **Podatność** (słabość zabezpieczeń) gdzie **1** (wysoka) , **3** (niska)
   - **Prawdopodobieństwo incydentu** od **1**(niskie) **do 3** (wysokie)
3. **Miarą ryzyka** w/w zasobu jest **iloczyn** oszacowanej **wartości**

Metodyka analizy ryzyka w obszarze bezpieczeństwa informacji

1. **Maksymalna** „punktacja” dla ryzyka aktywa wynosi **243**.

2. Rejestr ryzyk operacyjnych **w UMK** stosuje skalę **od 1 do 7**:

KRYTYCZNE (ocena **7** lub punktacja w zakresie **121 - 243**) - wymaga możliwie szybkiej reakcji. Podjęcie działań nie powinno być odkładane

POWAŻNE (ocena **5 – 6** lub punktacja w zakresie **81 - 120**) - wymaga reakcji. Działania należy zaplanować, terminy mogą być odleglejsze

UMIARKOWANE (ocena **3 - 4** lub punktacja od **41 do 80**) - przeciwdziałanie wskazane, głównie tam, gdzie można uzyskać efekt bez istotnych nakładów.

NISKIE (ocena **1 - 2** lub punktacja poniżej **41**) – nie wymaga działań

Analiza ryzyka dla zapewnienia ciągłości działania

Prace „moderuje” Zespół Audytu Wewnętrznego mając do pomocy konsultanta zewnętrznego.

1. **Wyznaczenie procesów krytycznych**
   - funkcjonowanie centrum zarządzania kryzysowego
   - świadczenia i pomoc społeczna
   - możliwość dokonywania wypłat
2. **Ustalenie zasobów**, których te procesy używają
3. **Analiza zabezpieczeń**, aby wzmocnić je tam, gdzie racjonalnie możliwe.
4. **Określenie minimalnych wymagań** konfiguracyjnych
5. **Przygotowanie planów** przez właścicieli procesów
6. **Testy i doskonalenie** planów.

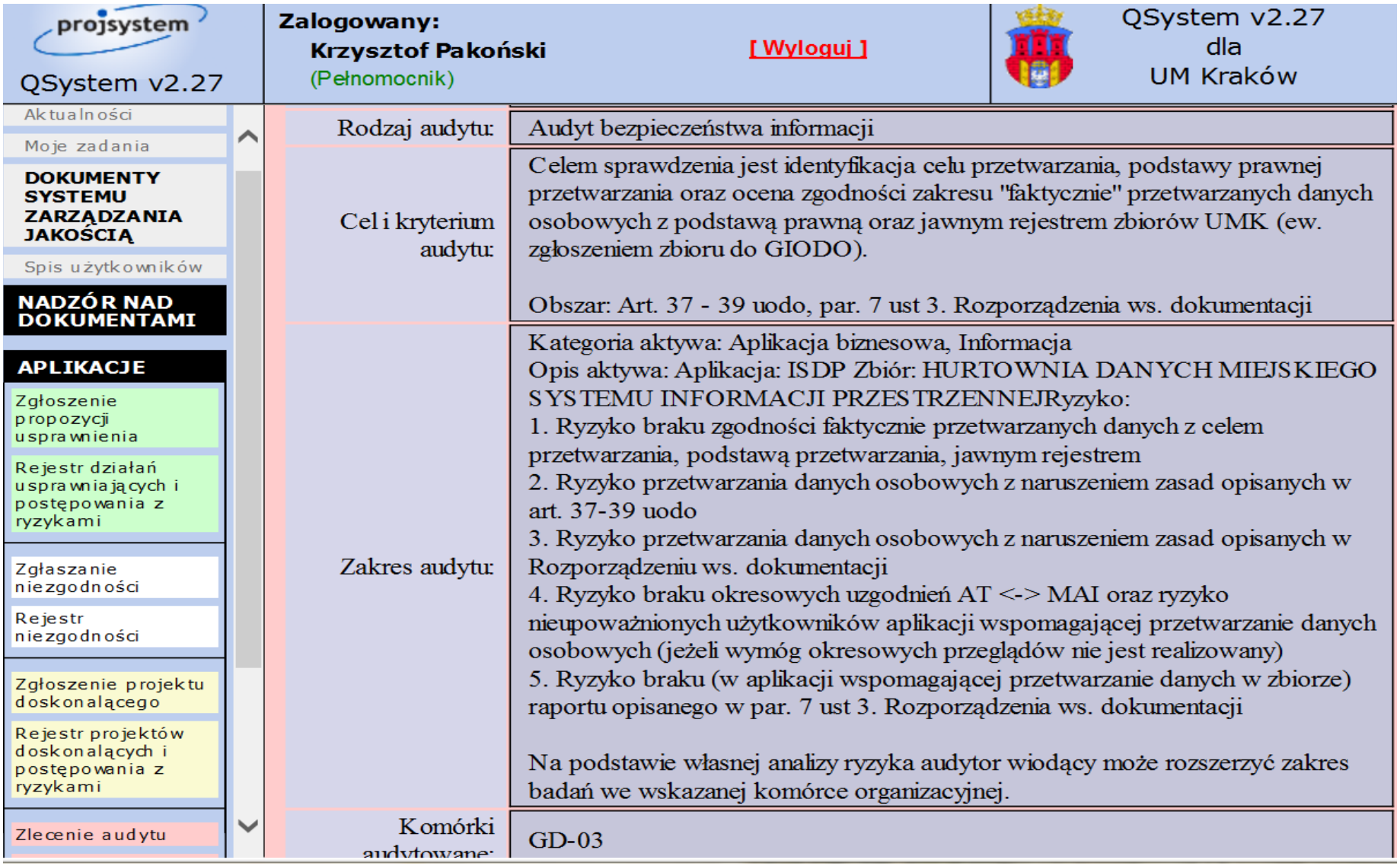
Czego nauczyliśmy się

1. **Zarządzanie ryzykiem** to konieczność i jedyna **racjonalna odpowiedź na zalew wymagań** i przepisów.
2. **Dobry proces ZR powinien** na czas **informować** najwyższe kierownictwo, **które ryzyka wymagają** jego zaangażowania.
3. **Aby organizacja osiągnęła dojrzałość** w zakresie analizowania i zarządzania ryzykiem **nie należy** zadań tych **powierzać zewnętrznym konsultantom.**
4. **Utopią jest** oczekiwanie, że można **skuteczny system zarządzania ryzykiem wprowadzić w ciągu roku** czy **dwóch**.
5. **Uporządkowanie obszaru bezpieczeństwa informacji to decyzja o charakterze strategicznym**, wymaga szkoleń, nakładów i wysiłku we wdrożenie zmian, a potem w utrzymanie systemu, ale nie można czekać, bo skala zagrożeń będzie rosła.

Organizacja audytu ochrony danych osobowych w UMK

- **SZBI** zgodny z normą 27001 i w jego ramach rocznie wykonujemy w UMK **kilkanaście zadań audytowych**.
- **Audyty spełniają wymagania** pkt.9.2 normy (plan, kryteria i zakres, wybór audytorów, raporty dla kierownictwa, dowody, dokumentacja)
- **Zlecenia audytów** przygotowuje Zespół Audytu Wewnętrznego, typując ryzyka do zbadania **na podstawie analizy ryzyka w UMK**.
- W praktyce **co najmniej połowa** tych zadań wyznaczana jest **dla** badania **ryzyk związanych** bezpośrednio lub pośrednio **z ochroną danych osobowych.**
- Szczegółowe **zadania w obszarze ochrony danych osobowych** typowane są z udziałem oraz na wniosek ABI'iego i **spełniają wymagania „sprawdzeń RODO"** wg &3 ust.2 pkt 1. Rozporządzenia MAC (11/2015).
- **Zadania te** umieszczane są **w planie audytów** obejmującym

Zlecenie audytu z zakresu ochrony danych osobowych w ramach planu audytu zgodności z ISO 27001 - przykład



Ocena wykonanego audytu SZBI - przykład

projsystem
QSystem v2.27

Zalogowany:
Krzysztof Pakoński
(Pełnomocnik)
[Wyloguj]

QSystem v2.27
dla
UM Kraków

- Aktualności
- Moje zadania
- **DOKUMENTY SYSTEMU ZARZĄDZANIA JAKOŚCIĄ**
- Spis użytkowników
- **NADZÓR NAD DOKUMENTAMI**
- **APLIKACJE**
- Zgłoszenie propozycji usprawnienia
- Rejestr działań usprawniających i postępowania z ryzykami
- Zgłaszanie niezgodności
- Rejestr niezgodności
- Zgłoszenie projektu doskonalącego
- Rejestr projektów doskonalących i postępowania z ryzykami

Nr niezgodności	Stwierdzone niezgodności	Pkt normy PN EN ISO9001/ISO27001
F2/000388	Ryzyko braku okresowych uzgodnień AT <-> MAI oraz ryzyko nieupoważnionych użytkowników aplikacji wspomagającej przetwarzanie danych osobowych	ISO9001: 7.5.2 , 7.5.3, ISO27001: A 8
F2/000389	Ryzyko przetwarzania danych osobowych z naruszeniem zasad opisanych w Rozporządzeniu ws. Dokumentacji	ISO27001: A15.12 , A15.11

Liczba niezgodności: **2**

Akceptacja audytu przez audytora generalnego i ocena

Ocena audytu: Ocena pozytywna, ryzyka zbadane. Klarownie zapisane ustalenia Trafnie wskazane niezgodności.

Kryteria oceny:

	Nazwa kryterium	Waga	Ocena
1.	Ocena prezentacji i zakresu badań	1.00	3
2.	Klarowność i odpowiedniość ustaleń	1.00	3
3.	Trafność spostrzeżeń, wniosków oraz ustaleń	1.00	2
4.	Prawidłowość przywołania punktu z Normy	1.00	1
5.	Wnioski, których wartość oceniamy jako dodaną	1.00	0
	OCENA KOŃCOWA:		**9.00**

Podpis audytora generalnego: Krzysztof Pakoński

Organizacja audytu wewnętrznego w GMK po reorganizacji (początek 2018)

1. Audyt wewnętrzny w GMK wykonywany będzie przez **Zespół Audytu Wewnętrznego** (ZA) **podległy** bezpośrednio **Prezydentowi Miasta** i usytuowany w Magistracie.
2. Zespołem Kieruje Dyrektor Audytu Wewnętrznego GMK (DA).
3. Ponadto w Zespole zatrudnionych będzie docelowo:
   - **trzech koordynatorów**:
     - **d/s. audytu w obszarze informatyki, bezpieczeństwa informacji i ochrony danych osobowych**
     - d/s. audytu finansowego
     - d/s. audytu organizacji, procedur i efektywności
   - asystent ds. organizacji i koordynacji
   - dziesięciu audytorów i asystentów audytu.
4. Zespół planem audytu obejmował będzie UMK oraz jednostki

Podstawowe obowiązki zreorganizowanego ZA

- Niezależna ocena ryzyka na poziomie gminy oraz jednostek objętych audytem
- Przygotowanie planu audytu wewnętrznego obejmującego wszystkie jednostki objęte audytem
- Wykonywanie zadań audytowych oraz analiz zaplanowanych w poszczególnych jednostkach oraz zadań doraźnych zlecanych przez PMK bezpośrednio lub na wniosek kierowników MJO
- Wykonywanie zadań „grupowych” , czyli zadań o tej samej tematyce i wg tego samego programu w wielu jednostkach
- **Koordynacja**, wyznaczanie ryzyk do badań i ocena raportów **audytu ISO 9001 i 27001 (w tym sprawdzenia RODO) w UMK**
- **Wykonywanie „sprawdzeń RODO” w jednostkach**
- Przygotowanie każdorocznie sprawozdania z wykonania planu

Organizacja audytu wewnętrznego w GMK - 2018

1. **ZA** (korzystając z dokumentacji dotyczącej zarządzania ryzykiem tworzonej w MJO) **pod koniec roku dokona** własnej, niezależnej **oceny ryzyka** i na jej podstawie oraz w konsultacji z kierownikami MJO **przygotuje plan audytu** na kolejny rok.
2. Plan obejmował będzie:
   - **zadania indywidualne** w jednostkach oraz
   - **zadania grupowe** (w kilku jednostkach wg jednego programu)
3. Zadania będą wykonywali wskazani przez DA audytorzy z pomocą asystentów audytu.
4. **Koordynację merytoryczną** i nadzór nad jakością **sprawować będą koordynatorzy** odpowiednio do zakresu zadania

Szacunkowe roczne ilości zadań/badań w GMK

Lp	Jednostka	Zadania AW indyw.	Zadania AW grup.	Sprawdzenia RODO	Zad ISO 9001	Łącznie działania koordynowane w ZA
		Ilość zadań	Ilość badań	Ilość sprawdzeń	Ilość zad. w koordynacji	Ilość zadań lub badań
1	UMK	12	2	12	18	44
2	ZIKIT	4	2	4		10
3	ZEO	4	2	4		10
4	ZBK	3	2	4		9
5	MOPS	3	2	4		9
6	ZIS	2	2	3		7
7	ZCK	2	2	3		7
8	ZIM	2	2	2		6
9	ZZM	3	2	2		7
10	SMMK	2	2	3		7
	Razem MJO	**25**	**18**	**29**	**0**	**72**
	Razem GMK	**37**	**20**	**41**	**18**	**116**