AUDYT BEZPIECZEŃSTWA INFORMACJI - ASPEKTY REGULACYJNE

Sławomir Kacprzak
Instytut Audytu Sektora Publicznego

Ministerstwo Finansów
26 marca 2013 r.

Przegląd zagadnień

1. Regulacje dotyczące bezpieczeństwa informacji
2. System zarządzania bezpieczeństwem informacji
3. Audyt w zakresie SZBI
4. Zarządzanie ryzykiem w zakresie SZBI

1

REGULACJE DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI

Wymogi prawne dotyczące zapewnienia bezpieczeństwa informacji

- ochrona informacji niejawnych
- ochrona danych osobowych
- informatyzacja działalności podmiotów realizujących zadania publiczne

Ochrona informacji niejawnych

- Przepisy o ochronie informacji niejawnych
  - Rozporządzenie PRM z dnia 20 lipca 2011r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

objęcie systemu teleinformatycznego procesem zarządzania ryzykiem dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym, zwanego dalej „zarządzaniem ryzykiem w systemie teleinformatycznym";

Dokumentacja bezpieczeństwa teleinformatycznego (inf. niejawne)

- szczególne wymagania bezpieczeństwa systemu teleinformatycznego
- procedury bezpiecznej eksploatacji
- Zabezpieczenia systemu teleinformatycznego - w oparciu o wyniki szacowania ryzyka
- Wątpliwości co do obowiązku audytu

Informacje niejawne c.d

§ 25. 3. W dokumencie szczególnych wymagań bezpieczeństwa zawiera się ponadto informacje o:

1) metodyce użytej w procesie szacowania ryzyka dla bezpieczeństwa informacji niejawnych oraz raport z tego procesu;

2) zastosowanych zabezpieczeniach;

3) ryzykach szczątkowych oraz deklaracji ich akceptacji;

16) audycie wewnętrznym;

17) zarządzaniu ryzykiem w systemie teleinformatycznym;

Przepisy o ochronie danych osobowych

- ROZPORZĄDZENIE MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

Dokumentacja opisująca sposób przetwarzania danych osobowych

- Polityka bezpieczeństwa
- Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
- Brak odniesienia do szacowania ryzyka
- Brak obowiązku audytu

Ustawa z 17 lutego 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne

Art. 2.

1. Z zastrzeżeniem ust. 2-4, przepisy ustawy stosuje się do realizujących zadania publiczne określone przez ustawy:
   1) organów administracji rządowej, organów kontroli państwowej i ochrony prawa, sądów, jednostek organizacyjnych prokuratury, a także jednostek samorządu terytorialnego i ich organów,
   2) jednostek budżetowych i samorządowych zakładów budżetowych,
   3) funduszy celowych,
   4) samodzielnych publicznych zakładów opieki zdrowotnej oraz spółek wykonujących działalność leczniczą w rozumieniu przepisów o działalności leczniczej,
   5) Zakładu Ubezpieczeń Społecznych, Kasy Rolniczego Ubezpieczenia Społecznego,
   6) Narodowego Funduszu Zdrowia,
   7) państwowych lub samorządowych osób prawnych utworzonych na podstawie odrębnych ustaw w celu realizacji zadań publicznych

   - zwanych dalej „podmiotami publicznymi".

Przepisów nie stosują

3. Przepisów ustawy nie stosuje się do przedsiębiorstw państwowych, spółek handlowych, służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154), Kancelarii Sejmu, Kancelarii Senatu, Kancelarii Prezydenta Rzeczypospolitej Polskiej oraz Narodowego Banku Polskiego, poza przypadkami gdy w związku z realizacją zadań przez te podmioty istnieje obowiązek przekazywania informacji do i od podmiotów niebędących organami administracji rządowej; w takich przypadkach stosuje się art. 13 ust. 2 pkt 1 niniejszej ustawy.

4. Przepisów rozdziału 4 nie stosuje się do jednostek badawczo-rozwojowych, uczelni publicznych, Polskiej Akademii Nauk i tworzonych przez nią jednostek organizacyjnych, Rzecznika Praw Obywatelskich, Trybunału Konstytucyjnego, Sądu Najwyższego, sądów administracyjnych, Najwyższej Izby Kontroli, Krajowej Rady Radiofonii i Telewizji, Krajowego Biura Wyborczego, Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, Generalnego Inspektora Ochrony Danych Osobowych, Komisji Nadzoru Finansowego oraz Generalnego Inspektora Informacji Finansowej.

Systemy teleinformatyczne – Rozdział 3

- Art. 13. ust. 1 ustawy:
- Podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności.

Regulacje dot. bezpieczeństwa informacji

Kontrola - art. 25

Kontroli działania systemów teleinformatycznych, używanych do realizacji zadań publicznych dokonuje:

a) w JST – właściwy wojewoda

b) w podmiotach publicznych podległych lub nadzorowanych przez organy administracji rządowej - organ administracji rządowej nadzorujący dany podmiot publiczny,

c) w podmiotach publicznych niewymienionych w lit. a i b - minister właściwy do spraw informatyzacji

Kontrola - uprawnienia

- Audytor systemu zarządzania bezpieczeństwem informacji według normy PN ISO/IEC 27001
- Audytor systemu zarządzania usługami informatycznymi według normy PN ISO/IEC 20000
- Audytor systemu zarządzania jakością według normy PN ISO/IEC 9001
- Certified Information System Auditor (CISA).
- Certified in the Governance of Enterprise IT (CGEIT).
- Certified Internal Auditor (CIA).
- Certified Information Systems Security Professional (CISSP).
- Europejski Certyfikat Umiejętności Zawodowych Informatyka — EUCIP Professional specjalizacja Audytor Systemów Informacyjnych.
- Systems Security Certified Practitioner (SSCP).

2

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Przepisy wykonawcze

- Rozp. RM z 16 maja 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

Rozdział IV - Minimalne wymagania dla systemów teleinformatycznych

- § 20. 1. Podmiot realizujący zadania publiczne:
  - opracowuje i ustanawia,
  - wdraża i eksploatuje,
  - monitoruje i przegląda
  - utrzymuje i doskonali
- system zarządzania bezpieczeństwem informacji zapewniający:
  - poufność, dostępność i integralność informacji
- z uwzględnieniem takich atrybutów, jak:
  - autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

2. Zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie

- przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy
- zapewnienia aktualizacji regulacji wewnętrznych
- utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania
- posiadania, adekwatności i aktualności uprawnień,
- szkolenia osób zaangażowanych w proces przetwarzania informacji

Zapewnienie przez kierownictwo…. c.d.

- zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość
- zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych
- zawierania w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji
- bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zapewnienie przez kierownictwo…. c.d.

- 7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
  - a) monitorowanie dostępu do informacji,
  - b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
  - c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
- 9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie

Zapewnienie przez kierownictwo…. c.d.

12) Odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa

Spełnienie wymagań

- Jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001,
- a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie
  - PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń
  - PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem
  - PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania
- Czy oznacza to obowiązek wdrożenia tych norm?

Ważne! – przydałby się audyt!

- § 22. Systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia należy dostosować do wymagań określonych w § 19, nie później niż w terminie 3 lat od dnia wejścia w życie niniejszego rozporządzenia (30 maja 2015)
- § 23. Systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia na podstawie dotychczas obowiązujących przepisów należy dostosować do wymagań, o których mowa w rozdziale IV rozporządzenia, nie później niż w dniu ich pierwszej istotnej modernizacji przypadającej po wejściu w życie rozporządzenia.

System zarządzania bezpieczeństwem informacji wg PN-ISO 27001

- Ta część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji
- UWAGA: System zarządzania zawiera strukturę organizacyjną, polityki, planowane działania, zakresy odpowiedzialności, zasady, procedury, procesy i zasoby.

Ustanowienie SZBI wg PN-ISO 27001

- Zdefiniować zakres i granice SZBI
- Zdefiniować politykę SZBI
- Zdefiniować podejście do szacowania ryzyka w organizacji
- Określić ryzyka
- Analizować i oceniać ryzyka
- Zidentyfikować i ocenić warianty postępowania z ryzykiem
- Wybrać cele stosowania zabezpieczeń i zabezpieczenia jako środki postępowania z ryzykiem
- Uzyskać akceptację kierownictwa dla proponowanych ryzyk szczątkowych
- Uzyskać autoryzację kierownictwa do wdrażania i eksploatacji SZBI
- Przygotować deklarację stosowania

3

Audyt w zakresie SZBI

SZBI a system kontroli zarządczej

- System zarządzania bezpieczeństwem informacji stanowi część systemu kontroli zarządczej
- Wskazówki w Standardach KZ są zbieżne z przepisami rozporządzenia RM (procedury, szkolenia, zarządzanie ryzykiem, mechanizmy informatyczne itp.)
- Audyt wewnętrzny jest działalnością niezależną i obiektywną, której celem jest wspieranie ministra kierującego działem lub kierownika jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej oraz czynności doradcze.

Wewnętrzne audyty SZBI (27001)

- W zaplanowanych odstępach czasu
- Przeprowadzane przez organizację lub w imieniu organizacji na potrzeby wewnętrzne
- Program audytu – na podstawie analizy ryzyka
- Obiektywność i bezstronność
- Audytorzy nie powinni audytować swojej pracy
- Wymagania dotyczące planowania i przeprowadzania audytów – zdefiniowane w udokumentowanej procedurze
- Kierownictwo odpowiada za wdrożenia zaleceń
- Działania poaudytowe (czynności sprawdzające)

Zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji

- Nie rzadziej niż raz na rok
- Czy audytorzy wewnętrzni (UFP) mogą przeprowadzać audyty BI?
- Czy potrzebne są szczególne uprawnienia formalne do przeprowadzania audytów BI?
- Czy audyt BI polega na badaniu zgodności z odpowiednią normą? Czy wdrożenie normy jest obowiązkowe?
- Czy wdrożenie i certyfikacja SZBI uwalnia audytorów wewnętrznych (UFP) od audytów BI?
- Jaką politykę przyjąć z punktu widzenia KAW?
- Co z jednostkami, w których nie ma KAW?
- pytania

4

ZARZĄDZANIE RYZYKIEM W ZAKRESIE SZBI

Proces zarządzania ryzykiem w BI wg PN-ISO 27005

- Ustanawianie kontekstu
- Szacowanie ryzyka
- Postępowanie z ryzykiem
- Akceptowanie ryzyka
- Informowanie o ryzyku
- Monitorowanie i przegląd ryzyka
- schemat

Identyfikowanie ryzyka

- Identyfikowanie aktywów (wszystko, co ma wartość dla organizacji) przykład
- Identyfikowanie zagrożeń (potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji) przykład
- Identyfikowanie istniejących zabezpieczeń
- Identyfikowanie podatności (słabość aktywu lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie) przykład
- Identyfikowanie następstw (jakie może spowodować dla aktywów utrata poufności, integralności i dostępności) np. utrata skuteczności, pogorszenie warunków działania, straty, utrata reputacji, zniszczenie

Estymacja ryzyka

- Wybór metody (jakościowa, ilościowa)
- Szacowanie następstw
- Szacowanie prawdopodobieństwa incydentu
  - (pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji)
- Poziom estymacji ryzyka (istotność ryzyka)
- przykład

Ocena ryzyka

- Kryteria oceny ryzyka (polityka bezpieczeństwa informacji)
- Czy podjąć działanie?
- Priorytety dla postępowania z ryzykiem, z uwzględnieniem estymowanych poziomów ryzyk

Dziękuję za uwagę

Sławomir Kacprzak
s.kacprzak@inasp.pl
606 648 448