Opracowanie z cyklu „Polskie przepisy a COBIT® 5”

MAPOWANIE
minimalnych wymagań
dla systemów teleinformatycznych używanych przez podmioty realizujące zadania publiczne
na COBIT® 5

styczeń 2014
wersja 1.5

Opracowali:
Joanna Karczewska CISA
Wojciech Szyszka CISA, CISM
Łukasz Wilkosz CISA

Spis treści

Zastrzeżenie

Autorzy przygotowali to opracowanie przede wszystkim jako materiał szkoleniowy dla profesjonalistów zajmujących się nadzorem nad technologiami informatycznymi w firmie (GEIT), zapewnieniem, ryzykami i bezpieczeństwem IT. Autorzy nie twierdzą, że jakiekolwiek korzystanie z tego opracowania zapewni pozytywne wyniki. Opracowania nie należy traktować jako zawierającego właściwe informacje, procedury i testy bądź nie zawierającego innych informacji, procedur i testów, które mają na celu racjonalne osiągnięcie tych samych wyników. W ustalaniu stosowności jakiejkolwiek informacji, procedury lub testu, czytelnicy powinni polegać na swoim zawodowym osądzie określonych okoliczności związanych z GEIT, zapewnieniem, ryzykami i bezpieczeństwem, zaistniałych w danym środowisku systemów lub technologii informatycznych.

Wprowadzenie

Przekazujemy Państwu opracowanie, które pomoże ustalić i utrzymać zgodność z minimalnymi wymaganiami dla systemów teleinformatycznych, wymienionymi w rozdziale IV Rozporządzenia RM z dnia 12 kwietnia 2012 r. (Dz. U. poz 526 z roku 2012).

Rozporządzenie Rady Ministrów

Rozporządzenie z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych określa:

1) Krajowe Ramy Interoperacyjności;
2) minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej;
3) minimalne wymagania dla systemów teleinformatycznych, w tym:
   a) specyfikację formatów danych oraz protokołów komunikacyjnych i szyfrujących, które mają być stosowane w oprogramowaniu interfejsowym,
   b) sposoby zapewnienia bezpieczeństwa przy wymianie informacji,
   c) standardy techniczne zapewniające wymianę informacji z udziałem podmiotów publicznych z uwzględnieniem wymiany transgranicznej,
   d) sposoby zapewnienia dostępu do zasobów informacji podmiotów publicznych dla osób niepełnosprawnych.

W niniejszym opracowaniu uwagę skupiono na paragrafach 20 i 21 dotyczących minimalnych wymagań dla systemów teleinformatycznych używanych przez podmioty realizujące zadania publiczne, które należy projektować, wdrażać oraz eksploatować z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

Stowarzyszenie ISACA®

Stowarzyszenie ISACA® pomaga liderom biznesowym i informatycznym maksymalizować korzyści oraz zarządzać ryzykiem związanym z informacjami i technologiami. Liczy ponad 100 tysięcy członków i sympatyków w 180 krajach. Zostało założone w 1969 roku jako niezależne stowarzyszenie non-profit. ISACA jest rzecznikiem profesjonalistów zajmujących się bezpieczeństwem informacji, audytem, zarządzaniem ryzykiem i nadzorem. Ci profesjonaliści polegają na stowarzyszeniu ISACA jako na zaufanym źródle wiedzy, standardów i certyfikacji dotyczących informacji i technologii oraz społeczności. Liczące 200 oddziałów na całym świecie stowarzyszenie wspiera i poświadcza wiedzę i umiejętności kluczowe dla biznesu przyznając uznawane globalnie certyfikaty:

- Certified Information Systems Auditor™ (CISA®),
- Certified Information Security Manager® (CISM®),
- Certified in the Governance of Enterprise IT® (CGEIT®) oraz
- Certified in Risk and Information Systems Control™ (CRISC™).

ISACA także opracowało i stale aktualizuje biznesową metodykę COBIT®, która pomaga podmiotom ze wszystkich sektorów i o dowolnym położeniu geograficznym nadzorować i zarządzać swoimi informacjami i technologiami.

Metodyka COBIT® 5

COBIT 5 stanowi wszechstronną metodykę wspomagającą podmioty w osiąganiu celów związanych z nadzorem i zarządzaniem technologiami informatycznymi w firmie. Metodyka jest uniwersalna i przydatna dla podmiotów różnej wielkości, firm komercyjnych, organizacji not-for-profit oraz jednostek sektora finansów publicznych.
COBIT 5 pomaga podmiotom osiągać optymalną wartość z technologii informatycznych, ponieważ wskazuje, jak zachować równowagę pomiędzy uzyskiwaniem korzyści a optymalizacją poziomów ryzyka i wykorzystania zasobów.

Więcej informacji o ISACA i COBIT 5 można znaleźć na stronie www.isaca.org

Mapowanie

Tabela zawiera mapowanie wymogów zawartych w paragrafach 20 i 21 Rozporządzenia RM z dnia 12 kwietnia 2012 r. (Dz.U. poz.526 z roku 2012) na:

- punkty normy oraz cele stosowania zabezpieczeń i zabezpieczenia zdefiniowane w Polskiej Normie PN-ISO/IEC 27001 wymienionej w ustępie 3 paragrafu 20 Rozporządzenia,
- procesy i praktyki zarządcze oraz czynniki umożliwiające zdefiniowane w metodyce COBIT® 5,
- procesy i cele kontrolne zdefiniowane w metodyce COBIT® 4.1 (wcześniejszej wersji z roku 2007).

Rozporządzenie	27001	COBIT 5	Czynnik umożliwiający	COBIT 4.1
§ 20. 2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez **zapewnienie przez kierownictwo podmiotu publicznego** warunków umożliwiających realizację i egzekwowanie następujących działań:				
1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;	pkt 5.2.1c A.5.1 A.15	APO01.01 APO01.04 APO01.07 APO02 APO04.02 APO13	1. Zasady, polityki i metodyki 3. Struktury organizacyjne	DS5.1 DS5.2
2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;	A.7	APO01.06 APO03 BAI09.01 BAI09.03 BAI09.05 BAI10.01-04	5. Informacje 6. Usługi, infrastruktura i aplikacje	DS9.1
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;	pkt 4.2.1d pkt 4.2.1e pkt 4.2.1f A.6.2.1	EDM03 APO12	5. Informacje	PO9 ME4.5
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;	A.11	APO01.02 APO01.06 DSS06.03	6. Usługi, infrastruktura i aplikacje 7. Ludzie, umiejętności i kompetencje	DS5.3 DS5.4
5) **bezzwłocznej zmiany uprawnień**, w przypadku zmiany zadań osób, o których mowa w pkt 4;	A.8.3.3 A.11	DSS05.04 DSS05.05 DSS06.03	6. Usługi, infrastruktura i aplikacje 7. Ludzie, umiejętności i kompetencje	DS5.3 DS5.4

Rozporządzenie	27001	COBIT 5	Czynnik umożliwiający	COBIT 4.1
6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;	pkt 5.2.2 A.8.2.2	APO07.03	4. Kultura, etyka i postępowanie 5. Informacje 7. Ludzie, umiejętności i kompetencje	PO7.4 AI7.1 DS7
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;	A.10	DSS05.01 DSS05.02 DSS05.07	5. Informacje 6. Usługi, infrastruktura i aplikacje	DS5.5 DS5.7 DS5.10 DS5.11 ME2
8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;	A.9.2.5 A.10 A.11.7	APO13.02 DSS05.01 DSS05.02	1. Zasady, polityki i metodyki	DS5.10 DS5.11
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;	A.10 A.11	DSS05.01 DSS05.02 DSS05.07	5. Informacje 6. Usługi, infrastruktura i aplikacje	DS5.4, DS5.5 DS5.10 DS5.11 DS12
10) zawierania w umowach serwisowych podpisanych ze **stronami trzecimi** zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;	A.6.2.3	APO09.03 APO10.01 APO10.03 APO10.05 DSS01.02	6. Usługi, infrastruktura i aplikacje	DS2.1 DS2.4

Rozporządzenie	27001	COBIT 5	Czynnik umożliwiający	COBIT 4.1
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;	A.7.1 A.7.2 A.9.1 A.9.2	APO13.02 DSS05.03 DSS05.05	1. Zasady, polityki i metodyki 4. Kultura, etyka i postępowanie 5. Informacje 6. Usługi, infrastruktura i aplikacje	DS5.2 DS12
12) zapewnienia 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;	A.9 A.10 A.12.6	APO01.08 DSS04.07 DSS05.01-03 DSS05.07	5. Informacje 6. Usługi, infrastruktura i aplikacje	DS5.2 DS5.4 DS5.5 DS5.8 DS5.10 DS5.11 DS11.5 AI6 AI2 (dla a) DS4 (dla b) DS10 (dla g) ME3 (dla h)
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;	A.13	DSS02.01-03 DSS02.05	1. Zasady, polityki i metodyki 5. Informacje 6. Usługi, infrastruktura i aplikacje	DS8

Rozporządzenie	27001	COBIT 5	Czynnik umożliwiający	COBIT 4.1
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.	pkt 4.2.3e pkt 4.2.3f pkt 6 pkt 7 A.6.1.8 A.15.3	MEA02.05 MEA02.06 MEA02.08	5. Informacje	ME2.5
§ 21. 1. Rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w **dziennikach systemów** (logach).				
2. W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.	A.10.10 A.12.4	DSS01.03 DSS05.07 DSS06.05	5. Informacje 6. Usługi, infrastruktura i aplikacje	DS5.5 DS9.3 DS13.3
3. Poza informacjami wymienionymi w ust. 2 mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka.	A.10.10 A.12.4	DSS01.03 DSS05.07 DSS06.05	5. Informacje 6. Usługi, infrastruktura i aplikacje	DS5.5 ME1.1 ME1.2 ME1.3

Rozporządzenie	27001	COBIT 5	Czynnik umożliwiający	COBIT 4.1
4. Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata. 5. Zapisy dzienników systemów mogą być składowane na zewnętrznych informatycznych nośnikach danych w warunkach zapewniających bezpieczeństwo informacji. W uzasadnionych przypadkach dzienniki systemów mogą być prowadzone na nośniku papierowym.	A.10.5	DSS04.07	6. Usługi, infrastruktura i aplikacje	DS11

Bibliografia

Wydane przez ISACA

- COBIT 5
- COBIT 5: Enabling Processes
- COBIT 5 Enabling Information
- COBIT 5 Implementation
- COBIT 5 for Information Security
- COBIT 5 for Assurance
- COBIT 5 for Risk
- COBIT Assessment Programme

dostępne na stronie www.isaca.org/COBIT/Pages/Product-Family.aspx

Wydane przez Polski Komitet Normalizacyjny

- PN-ISO/IEC 27001:2007P „Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji – Wymagania”

dostępne na stronie www.pkn.pl