

SPIS TREŚCI

Wstęp	7
Rozdział 1. Bezpieczeństwo informacji	11
1. Znaczenie informacji	11
1.1. Definicja informacji	13
1.2. Cykl życia informacji	17
2. Istota bezpieczeństwa informacji	19
2.1. Poufność	22
2.2. Integralność	27
2.3. Dostępność	27
3. Incydenty związane z bezpieczeństwem informacji	28
4. Elementy bezpieczeństwa informacji	33
4.1. Zasoby w ISMS	35
4.2. Zagrożenia związane z bezpieczeństwem informacji	36
4.3. Podatności informacji	37
4.4. Następstwa incydentów	39
4.5. Ryzyko	39
4.6. Zabezpieczenia w ISMS	40
5. Wymagania prawne dotyczące bezpieczeństwa informacji	43
5.1. Konstytucja Rzeczypospolitej Polskiej	45
5.2. Ustawa o ochronie danych osobowych	46
5.3. Ustawa o rachunkowości	47
5.4. Kodeks pracy	48
5.5. Ustawa o zwalczaniu nieuczciwej konkurencji	48
5.6. Regulacje dotyczące zarządzania ciągłością działania	49
6. Korzyści z ochrony informacji	49
Rozdział 2. Systemowe zarządzanie bezpieczeństwem informacji	55
1. Historia systemowego zarządzania bezpieczeństwem informacji	55
1.1. Polskie edycje norm dotyczących zarządzania bezpieczeństwem informacji	59
2. ISO 27001, COBIT, ITIL oraz ISO 20000	60
2.1. COBIT	60
2.2. ITIL	64
2.3. ISO 20000	66
2.4. ISO 31000	67

3. Koncepcja systemu zarządzania bezpieczeństwem informacji	71
4. Planowanie i polityka bezpieczeństwa informacji	75
5. Odpowiedzialność i uprawnienia – role w ISMS	80
6. Dokumentacja w systemie zarządzania bezpieczeństwem informacji . .	83
7. Audyt systemu zarządzania bezpieczeństwem informacji	90
7.1. Istota audytu ISMS	91
7.2. Cele audytu i zakresy odpowiedzialności	93
7.3. Etapy działań audytowych	94
8. Certyfikacja systemów zarządzania bezpieczeństwem informacji	106
9. Integracja ISMS z innymi systemami zarządzania	113
Rozdział 3. Interpretacja wymagań normy ISO/IEC 27001:2005	117
1. Ustanowienie i zarządzanie ISMS	119
2. Wdrożenie i stosowanie ISMS	127
3. Monitorowanie i przegląd ISMS	129
4. Utrzymanie i doskonalenie ISMS	130
5. Dokumentacja w systemie zarządzania bezpieczeństwem informacji . .	131
6. Odpowiedzialność kierownictwa w systemie zarządzania bezpieczeństwem informacji	134
7. Zarządzanie zasobami w ISMS	135
8. Wewnętrzne audyty ISMS	136
9. Przeglądy ISMS realizowane przez kierownictwo	137
10. Doskonalenie ISMS	138
11. Interpretacja zabezpieczeń wymaganych przez ISO/IEC 27001:2005 . .	139
Rozdział 4. Proces szacowania ryzyka bezpieczeństwa informacji	205
1. Wdrażanie systemu zarządzania bezpieczeństwem informacji (ISO/IEC 27001:2005)	209
2. Wdrożenie i eksploatacja ISMS	222
3. Monitorowanie i przegląd ISMS	223
4. Utrzymanie i doskonalenie ISMS	226
4.1. Identyfikacja informacji i zagrożeń	227
4.2. Klasyfikacja informacji	229
4.3. Szacowanie ryzyka	231
4.4. Postępowanie z ryzykiem (plan minimalizacji ryzyka)	231
4.5. Plan ciągłości działania	232
5. Charakterystyka metod szacowania ryzyka bezpieczeństwa informacji – koncepcje i zastosowania	236
5.1. Ogólna charakterystyka metod szacowania ryzyka bezpieczeństwa informacji	236

5.2. Wytyczne do szacowania ryzyka określone w ISO/IEC 27001:2005	238
5.3. Szacowanie ryzyka według ISO/IEC TR 13335-3	239
5.4. Metoda OCTAVE	244
5.5. Analiza skutków potencjalnych błędów – FMEA	245
5.6. Metoda CRAMM	246
5.7. Metoda COBRA	246
5.8. Metoda MARION	247
5.9. Metoda MEHARI	247
5.10. Standardy ISACA	248
5.11. Metody autorskie	250
6. Przykłady narzędzi szacowania ryzyka o charakterze otwartym	250
7. Przykład wykorzystania oprogramowania do zarządzania ryzykiem	251
 Rozdział 5. Wdrożenie, utrzymanie i rozwój ISMS w organizacji – analiza przypadku	257
1. Zarządzanie projektem	257
1.1. Opis przedsiębiorstwa, branża, zakres działania	257
1.2. Struktura i organizacja projektu wdrożeniowego	258
1.3. Szacowanie ryzyka bezpieczeństwa informacji w przedsiębiorstwie – prezentacja metody	260
2. Systemowe zarządzanie bezpieczeństwem informacji na podstawie analizy ryzyka	288
3. Raport z szacowania ryzyka bezpieczeństwa informacji	290
4. Plany ciągłości działania	292
5. Dokumentacja systemu ISMS	294
 Zakończenie	297
 Załączniki	299
1. Lista sprawdzająca ISMS	299
2. Klasyfikacja informacji (na przykładzie przedsiębiorstwa z branży energetycznej)	313
3. Deklaracja stosowania (na przykładzie przedsiębiorstwa z branży energetycznej)	341
4. Polityka bezpieczeństwa informacji (przykład)	355
5. Dokumentacja ISMS (przykład). Księga procesu: Zarządzanie bezpieczeń- stwem informacji	370
5.1. Procedura: Klasyfikacja informacji i szacowanie ryzyka	375
5.2. Procedura: Utrzymanie czystych biurków i pulpitów	393
5.3. Procedura: Opatrywanie informacji opisem	398
5.4. Procedura: Postępowanie z informacją zgodnie ze schematem klasyfikacyjnym	400

5.5. Procedura: Zgłaszanie przypadków naruszenia bezpieczeństwa . . .	404
5.6. Procedura: Wejścia i wyjścia pracowników i osób trzecich	408
5.7. Procedura: Zarządzanie incydentami – organizacja systemu Incydent	419
5.8. Procedura: Zgłaszanie niewłaściwego funkcjonowania oprogramowania	422
5.9. Procedura: Zgłaszanie słabości systemu bezpieczeństwa	424
5.10. Procedura: Ochrona danych	426
Spis literatury	429
Spis tabel	439
Spis rysunków	440
Spis przykładów	443