Cuprins

Cuvânt-înainte 5
1. Introducere 9
2. Managementul riscului 13
3. Managementul riscului pentru sisteme informatice 18
3.1. Securitatea Informației 19
3.2. Metodă eficientă de protecție a datelor – Abordarea managementului securității prin managementul riscurilor 23
3.3. Construirea unui program de măsurare a performanțelor în securitatea informației 67
4. Metode şi standarde internaționale pentru managementul riscurilor 74
5. Managementul riscurilor IT 80
5.1. Procesul de management al riscurilor IT 81
5.2. Analiza de Risc 99
5.2.1. Etapele analizei de risc 100
5.2.2. Analiza Modurilor de Defectare şi a Efectelor lor (AMDE) – (Failure Mode and Effects Analysis – FMEA) 104
5.3. Aspecte specifice privind protecția datelor personale în contextul identificării şi evaluării riscului 116
5.3.1. Conceptul de 'date personale' 119
5.3.2. Stadiile supuse analizei de risc 123
5.3.3. Tipologii de prelucrare esențiale de analizat 125
5.3.4. Aspecte de analizat pentru orice flux de date 129
5.3.5. Metodologie pentru realizarea analizei de risc (DPIA) şi identificarea interesului legitim 148
5.4. Răspunsul la risc 154
5.4.1. Tipurile de răspuns la risc 155
5.4.2. Integrarea aspectelor de protecție a datelor în procesele existente de răspuns la risc 158
5.4.3. Corelarea răspunsului la risc între cerințele de protecție a datelor personale şi cele de securitate IT 160
5.4.4. Asigurarea unor abordări unitare în cadrul grupului 162
5.5. Monitorizarea riscurilor şi a răspunsului la riscuri 163
5.6. Implementarea controalelor în sistemele informatice 167

5.7. Integrarea procesului de management al riscurilor în procesele IT 177
5.7.1. Modelul de management prin procese şi adoptarea managementului de risc în IT 177
5.7.2. Îndeplinirea obligaţiilor de răspuns la solicitările persoanelor vizate şi a obligaţiilor referitoare la investigaţii (pentru protecţia datelor personale) 181
5.7.3. Analiza transferului datelor personale în contextul mai multor sisteme IT interne şi/sau externe 181
5.7.4. Integrarea protecţiei datelor în procesul de dezvoltare software 182
5.8. Riscuri specifice în cazul utilizării unei organizaţii terţe 189
6. Registrul Riscurilor 194
7. Rolul liniilor de apărare într-o organizaţie şi asigurarea conformităţii 203
7.1. Rolul liniilor de apărare într-o organizaţie 203
7.1.1. Prima Linie de Apărare – Managementul Operaţional 206
7.1.2. A doua linie de apărare – Funcţiile de conformitate şi managementul riscurilor 207
7.1.3. A treia linie de apărare – Auditul intern 208
7.1.4. Liniile de apărare pentru protecţia datelor personale 209
7.2. Asigurarea conformităţii 210
8. Standarde minime de risc informatic aliniate cu strategia afacerii şi cu apetitul definit pentru risc 216
9. Factorul uman 222
10. Reziliența – Strategii împotriva evenimentelor necunoscute sau cu un nivel ridicat de incertitudine 230
11. Concluzii 234
12. Termeni, definiţii 236

Bibliografie selectivă 240