Rodica BULAI,
Academia „Ştefan cel Mare”

ANALIZA ETAPELOR DE CREARE A UNUI SISTEM DE MANAGEMENT AL SECURITĂȚII INFORMAȚIEI

*An **Information Security Management System** (ISMS) is a system of management concerned with information security. The best known ISMS is described in ISO/IEC 27001 and ISO/IEC 27002.*

Informațiile sunt o resursă a organizației care, ca şi celelalte resurse importante de business, adaugă valoare organizației şi trebuie protejate ca atare. Un **Sistem de Management al Securității Informațiilor (SMSI)** este o abordare sistematică a gestionării informațiilor sensibile ale organizației în scopul protejării acestora.

Actualitatea creării SMSI reprezintă una dintre pietrele unghiulare, cu care se confruntă oricare organizație internațională (şi ar trebui să preocupe şi organizațiile naționale), una dintre cele mai prioritare sarcini al sistemului managerial de gestionare a organizațiilor.

Standardele ”ISO/IEC 27001:2005 (fost BS 7799-2) Sistemul de Management al Securității Informației” şi ”ISO/IEC 27002:2005/ Cor 1:2007 (fost BS 7799-1, ulterior, ISI/IEC 17799), Codul de practică pentru Managementul Securității Informației” sunt cele mai importante, până la ora actuală, în domeniul securității informației. Ele stabilesc un limbaj internațional comun pentru securitatea informației.

În anul 2003, Banca Națională a Republicii Moldova a fost prima din spațiul sovietic, care a început să implementeze în practică cerințele ISO 17799 şi BS 7799:2, obligând toate băncile să îndeplinească cerințele lui, creând SMSI pe baza standardului.

Un SMSI elaborat în conformitate cu cerințele standardului ISO/IEC 27001:2005 reprezintă un sistem complex care include atât mecanismele de gestionare, cât şi mecanismele de protecție a informației, figura 1. Modelul procesului de realizare a SMSI presupune un ciclu perpetuu de măsuri, şi anume: planificarea, realizarea, verificarea şi menținerea.

În etapa de planificare, se asigură evaluarea riscurilor securității informației, se propune un plan corespunzător de prelucrare a riscurilor. În etapa de realizare, sunt implementate deciziile luate în etapa de planificare. Etapele ulterioare, de verificare şi menținere, fortifică, redactează şi perfecționează deciziile privind securitatea informației, deja, luate şi implementate.

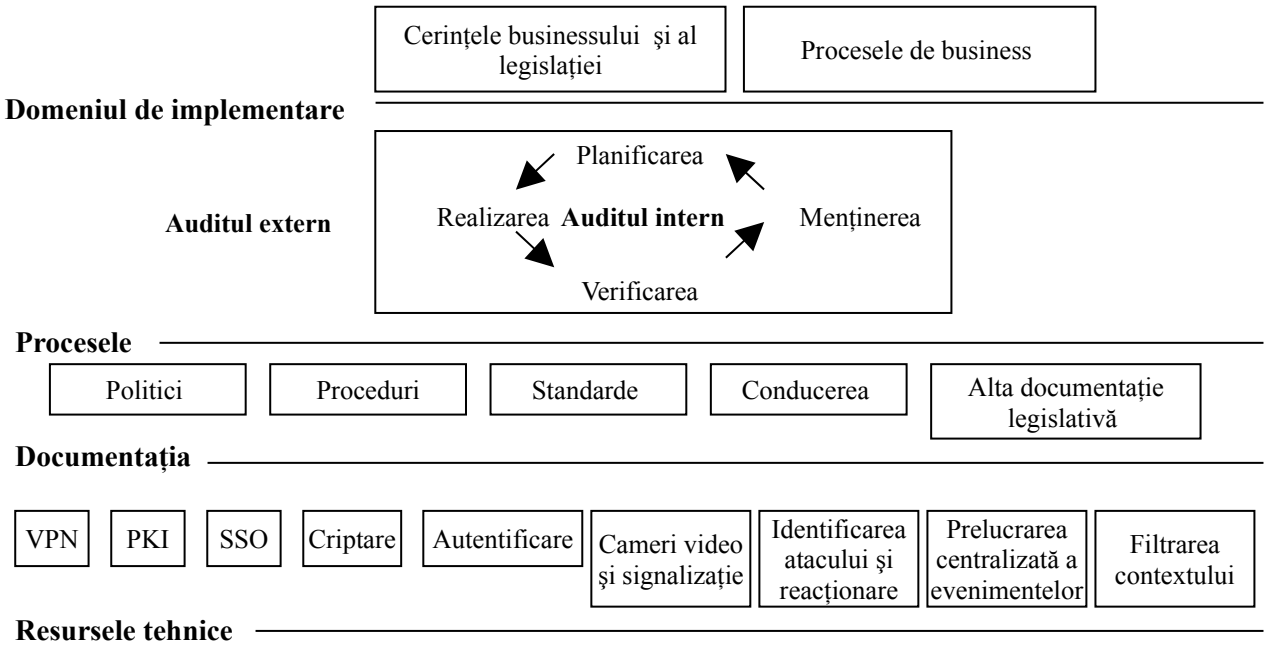

Figura 1. Sistemul de Management al Securității Informației

SMSI, care reprezintă un complex de măsuri organizaționale, programate, tehnice şi fizice,

trebuie să asigure integritatea, confidențialitatea, accesibilitatea şi autenticitatea resurselor informaționale.

Totuşi, la crearea SMSI, este necesară luarea în considerare nu doar a regulilor enumerate mai sus, nu doar atingerea tuturor proprietăților resurselor informaționale, ci şi a specificului businessului. De exemplu, pentru sectorul bancar, scopul-cheie în direcția SI este asigurarea integrității informației financiare; pentru operatorii sectorului de telecomunicație – accesul la resursele informaționale, începând cu canalele de transmisie şi până la serverele comerciale; pentru companiile de stat, este importantă menținerea confidealității informațiilor etc. Acest lucru nu înseamnă că băncile nu iau în considerare accesibilitatea datelor sau că sectorul de stat nu are nevoie de menținerea integrității datelor.

Din aceste considerente, de la bun început, se iau în considerare aspectele critice cele mai importante şi specifice ale organizației şi prin crearea unei arhitecturi corecte, în final, poate fi obținut un SMSI eficient şi sigur.

În funcție de sfera şi specificul activității organizației, numărul de angajați şi aria activității care necesită a fi supusă procesului de securitate a informației, numărul etapelor şi detalizarea lor poate fi diferit. În general, ele cuprind: *luarea deciziei de creare a unui SMSI***,** *pregătirea pentru crearea SMSI* (organizarea grupului de lucru, asigurarea metodico-normativă, evidențierea sferei de activitate cuprinsă de SMSI, depistarea neconcordanțelor etc.), *analiza riscurilor* (identificarea tuturor activelor, determinarea valorii activelor identificate, identificarea amenințărilor şi vulnerabilităților pentru activele identificate, evaluarea riscurilor pentru posibilele cazuri de realizare a atacurilor informaționale în privința activelor identificate, alegerea criteriilor de reacționare la riscuri, pregătirea planului de prelucrare a riscurilor), *elaborarea politicii şi procedurilor SMSI***,** *implementarea şi exploatarea SMSI***.**

Prin implementarea SMSI se activează toate procedurile elaborate şi mecanismele, mijlocele de gestionare etc., figura 2.

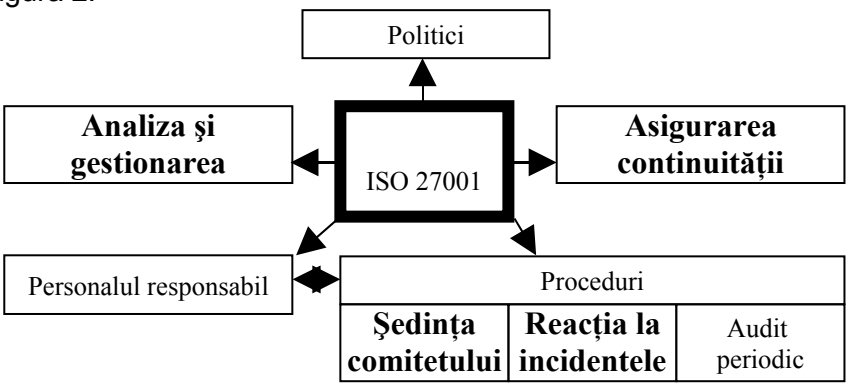

Figura 2. Mecanismele de bază ale SMSI

Cu toate că nu au regim de lege pentru organizații pe teritoriul republicii, implementarea standardelor ISO/IEC 27001:2005 şi ISO 27002:2005 fiind opțională, ele ar trebui luate în considerare de către toate organizațiile moldoveneşti.

Referințe bibliografice:

1. http://www.cadranpolitic.ro/ Cătălin ALBU, *Sistemul de Management al Securității Informației*.
2. http://www.InfoSecurity.ru/ Александр Астахов, *Как построить и сертифицировать систему управления информационной безопасностью?*
3. http://www.connect.ru/ Алексей Куканов, *Роль СУИБ в обеспечении информационной безопасности в объединенной генерирующей компании.*
4. http://www.jetinfo.ru/ Василий Носаков, *Создание комплексной системы управления информационной безопасностью.*
5. http://citcity.ru/ Юлия Хитькова, *Искусство войны, или Как построить эффективную СУИБ*.
6. http://barkas.org/sozdanie-suib.html *Построение Системы управления информационной безопасностью (СУИБ).*
7. http://www.conceptual-s.com/ *Система Управления Информационной Безопасностью (ISMS).*