MODELS AND METHODS FOR GOVERNAMENTAL CYBER RISK MANGEMENT

MODELE ȘI METODE DE GESTIONARE A RISCURILOR CIBERALE GUVERNAMENTALE

Valeriu Cernei
Doctorand, Academia de Studii Economice a Moldovei
e-mail: valeriu.cernei@bsd.md

Abstract
The subject of cyber security risk management of state organizations is one that cannot lose its relevance given the fact of the continuous development of information technologies. The Republic of Moldova has demonstrated significant progress in the field of ICT, especially in the development of services for citizens, as well as to business and government to government, through the implementation of the interoperability platform. Thus, Cyber Security risk management processes and activities are to be carefully planned, implemented and monitored. The paper presents a generalized view of the approach and proposes certain tools and methods aiming to facilitate the implementation of a Government wize risk management process.

Keywords: *Risk Management, Cyber Security, Governement, ICT, KRI, approach*

JEL Classification: *C63, D81*

INTRODUCERE

Subiectul gestiunii riscurilor de securitate cibernetică este unul ce nu-și poate pierde actualitatea dat fiind faptul dezvoltării vertiginoase și continue a tehnologiilor informaționale. Apar noi vulnerabilități sau își modifică forma vulnerabilitățile vechi, și, prin urmare, se analizează noi riscuri inerente.

Domeniul gestiunii riscurilor TIC și a celor de Securitate cibernetică prezintă procese și activități ce trebuie cu o mare atenție planificate, realizate și monitorizate.

Conducătorii de toate nivele conștientizează faptul că procesul de gestiune a riscurilor, inclusiv a celor de Securitate cibernetică, reprezintă o sursă consistentă de informare cu scopul elaborării deciziilor corecte. Totodată, ei înțeleg, că procesul trebuie organizat și derulat cu o maximă responsabilitate și transparență, altfel, deciziile elaborate pot afecta negativ întreaga organizație.

Subiectul este de o și mai mare importanță odată cu orientarea serviciilor statale către cetățeni. Implementarea sistemelor informaționale ce au obiectivul de a ușura interacțiunea dintre stat si cetățeni, stat și persoane juridice, dintre instituțiile statului duce la faptul expunerii participanților unor riscuri inerente informaționale (TIC) și de Securitate cibernetică semnificative.

REZULTATELE CERCETĂRII

Republica Moldova, în ultimii 10 ani, a progresat semnificativ în digitizarea și automatizarea serviciilor pentru cetățeni și a activităților interne de colaborare inter-instituțională, inter-departamentală, s.a.m.d. Totodată, funcțiile de asigurare a securității cibernetică și analiza riscurilor, precum și cele de creștere a nivelului de conștientizare în domeniul securității cibernetice, nu au fost cumva tratate/dezvoltate și instituționalizate comensurabil, sau, dacă acest lucru s-a întâmplat, atunci activitățile respective au purtat un caracter sporadic, fără o coordonare consistentă și planificată la nivel statal.

Nivelul de maturitate a domeniului de Securitate al sectorului guvernamental a fost și este în continuare diferit: unele instituții alocă resurse și implementează mecanisme consistente de Securitate, altele, abordează subiectul superficial și cazual. Dacă ar fi să realizăm o grupare, atunci organizațiile guvernamentale ce posedă un nivel de maturitate sporit ar reprezenta mai puțin de 10 % din numărul total, inclusiv al instituțiile în care statul are calitate de fondator sau acționar.

Platforma interguvernamentală de comunicare (implementată de către Agenția pentru Guvernare Electronică) presupune că instituțiile de Statului sunt conectate și alimentează platforma cu date, astfel, fiind asigurate servicii dintr-o singură sursă pentru cetățeni. În acest caz, se poate admite obiectiv, că unele Instituții pot alimenta platforma cu date eronate/neveridice/etc, fapt ce implică riscuri de Securitate semnificative, inclusiv riscuri ce țin de protecția datelor cu caracter personal.

Autorul, pe parcursul ultimilor ani, a prestat servicii comerciale de audit al securității informaționale pentru mai multe Instituții de stat. O analiză generalizată a nivelului de maturitate a Instituțiilor statului din punct de vedere al securității cibernetice relevă mai multe concluzii, dintre care:

- Nivelul mediu de maturitate per instituții guvernamentale de nivel superior este evaluat ca fiind intre 1 si 2, pe o scara de la 0-5 (0-inexistent, 5 - optimizate).
- Funcția de ofițer de securitate cibernetică sau nu este instituită sau nu este completată (lipsa cadrelor în domeniu, necăutând la faptul instituirii specialităților corespunzătoare în cadrul instituțiilor de învățământ superior, licență și master).
- Doar câteva instituții au abordat subiectul securității informației într-un mod complex, prin adoptarea și implementarea unui sistem de management al securității cibernetice.

În anul 2017 a fost aprobată HG 201 Cerințe minime de securitate cibernetică. Este de menționat că HG respectivă include expres cerințe privind gestiunea riscurilor cibernetice. Necăutând la faptul că procesul de gestiune a riscurilor de securitate este unul central implementării și menținerii unui sistem de management al securității informației, nicio instituție de stat nu a abordat subiectul într-un mod comprehensiv, fiind stabilit și urmat un proces în sensul larg.

Este evident că, în condițiile digitizării și centralizării serviciilor publice, este crucială o abordare centralizată și foarte bine coordonată a aspectelor de securitate a informației și, corespunzător, cele de gestiunea riscurilor cibernetice.

Pe lângă metodologia propriu-zisă ce trebuie dezvoltată, este necesar de a asigura un suport considerabil de implementare etapizată. Implementarea etapizată presupune crearea / validarea mediilor protejate și includerea graduală a unor medii informaționale adiționale, ca rezultat al activității de analiza a riscurilor și, ce este mai important, de tratare corespunzătoare a acestora.

Elaborarea unei metodologii de analiza a riscurilor cibernetice cu scopul de a fi adaptată și propusă spre implementare in instituțiile Statului este foarte importantă. Metodologia trebuie să vizeze evaluarea riscurilor, identificarea măsurilor de minimizare, planificarea activităților de tratare a riscurilor, aplicarea indicatorilor de corecție calculați în funcție de situația reală pentru perioadă analizată, etc. În sine, procesul de gestiune a riscurilor este interconectat și se alimentează cu informații și date rezultate din alte procese, cum ar fi gestiunea incidentelor, gestiunea schimbărilor, gestiunea continuității, s.a.m.d. Pentru a asigura un proces eficient de gestiunea riscurilor va fi necesar de a asigura și derularea eficientă a respectivelor procese.

Pornind de la axioma că ”tot ce nu poate fi măsurat, nu poate fi îmbunătățit”, nu mai puțin important este necesitatea dezvoltării unui sistem de parametrizare și raportare,

cu gruparea pe diferite resurse informaționale, după componentă, după sursă, nivelul riscului și altele.

Metodologia poate fi elaborată în baza instrumentelor MS Office: Excel și Word la prima etapă. Pentru a asigura maximum funcționalități utile și fezabile, instrumentele respective pot fi create și ținând cont de rezultatele analizelor instrumentelor de Risc Management existente pe piață, care prezintă mai multe neajunsuri cum ar fi rigiditatea de configurare adaptare, efort sporit de localizare, complexitatea, lipsa specialiștilor si, nu în ultimul rând, prețul sporit de achiziție și licențiere.

Din punct de vedere al abordării activităților, acestea trebuie structurate în mai multe etape, atât practice cât și de cercetare, rezultatul reprezentând instrumente fezabile și concluzii relevante - rezultat al activităților analitice. Astfel, se conturează câteva etape de realizare ce sunt prezentate în continuare:

- **Evaluarea situației privind gestiunea riscurilor la nivel statal**. Activitatea presupune organizarea unei serii de ședințe și întâlniri cu persoane cheie din cadrul organizațiilor statale. Pentru a asigura rezultate cât mai relevante, este necesar de a selecta organizații de nivel 1 (Ministere și Agenții de stat), nivel 2 (Agenții și Companii fondate sau administrate de către structuri guvernamentale de nivel 1) si chiar 3 (Agenții și organizații subordonate celor de nivel 2). Pentru a asigura că selecția și, corespunzător, rezultatele sunt relevante, va fi necesar de a elabora criteriile de selecție a instituțiilor. Un criteriu evident la momentul scrierii curentului referat poate fi nivelul organizației conform HG201 privind cerințele minime de securitate cibernetică, precum și cantitatea de date furnizate către platforma guvernamentală.
- **Analiza bazei legale privind gestiunea riscurilor TIC și de securitate cibernetică a Republicii Moldova.** Respectiva activitate presupune analiza detaliată a cadrului legal în domeniu. Ca rezultat vor fi înaintate recomandări de îmbunătățire a bazei normative și legale statale
- **Evaluarea situației privind gestiunea riscurilor de securitate cibernetică în instituțiile comerciale**. Autorul își propune să realizeze o analiza a mediului comercial din punct de vedere al proceselor aferente gestiunii riscurilor de securitate.
- **Analiza comparativă stat versus comercial în R. Moldova.** Analiza comparativă in raport cu un sistem de referință precum și cu mediul comercial, poate oferi o înțelegere mai bună a situației curente precum și facilita selectarea strategiei de implementare a proceselor aferente securității informației, specific gestiunii riscurilor de securitate.
- **Analiza principalelor instrumente de gestiune a riscurilor existente la nivel local și internațional**. Pe piață există o multitudine de soluții ce, parțial sau integral, automatizează activitățile aferente gestiunii riscurilor. Acestea reprezintă instrumente valoroase si complexe. Totodată, în R. Moldova nu au fost identificate cazuri de implementare a astfel de sisteme. În scopul lucrării, analiza respectivelor sisteme va avea o valoare semnificativă din punct de vedere al organizării proceselor și a funcționalităților specifice. Totodată va fi realizată analiza comparativă a diferitor metodologii de analiza a riscurilor calitative și relevarea aspectelor de localizare
- **Elaborarea metodologiei de gestiunea riscurilor la nivel de Instituții de Stat.** Este considerat că, aderarea la o metodă cantitativă a riscurilor, va fi mult prea greoaie de implementat și menținut, în special în situația lipsei de experți în domeniu. Cunoștințele și experiența acumulată de-a lungul anilor vor fi sistematizate, dezvoltate și îmbogățite cu rezultatele cercetării aspectelor specifice cu scopul elaborării unei metodologii viabile, ușor de implementat și menținut.
- **Elaborarea conceptului de implementare graduală a metodologiei la nivel statal**. Metodologia elaborată urmează să stea la baza conceptului de implementare graduală.

După cum a fost specificat anterior, se recomandă a asigura o abordare etapizată de implementare, fapt ce presupune crearea a cel puțin 3 zone de implementare: zona securizată, zona tampon, zona cu risc înalt. Instituțiile de stat vor fi grupate conform unor criterii elaborate și pre-aprobate. Ulterior, fiecare instituție va trebui să satisfacă anumite cerințe pentru a fi atribuite zonei cu nivel de securizare mai înalt. Totodată, va fi necesar de a stabili principiile de monitorizare a modului de menținere a nivelului curent.

- **Elaborarea instrumentarului de înregistrare, calcul și evidența a riscurilor informaționale/cibernetice.** În cadrul activității respective autorul își propune a sistematiza cunoștințele acumulate în rezultatul cercetării și a elabora instrumentele de automatizare a procesului. În scopul lucrării procesul urmează a fi automatizat cu ajutorul instrumentelor MS Excel și MS Word. Ulterior, odată ce metodologia va fi implementată și ajustată conform situației reale, aceasta urmează a fi automatizată in baza tehnologiilor moderne.
- **Propunerea unui program de studiu prind gestiunea riscurilor cibernetice utilizând tehnici neformale de educare în domeniu**. Autorul își propune a elabora un curs de studiu, ce urmează a fi propus instituțiilor de învățământ. Acest lucru este important pentru a asigura experți pregătiți de a menține procesele de gestiune a riscurilor în instituțiile de stat.

Rezultatele cercetării pot avea un impact semnificativ în procesul de consolidare cibernetică a statului. Efectul va fi unul benefic pentru fiecare dintre instituțiile statale, comerciale, precum și instituțiile de învățământ.

CONCLUZII

Procesul de gestiune a riscurilor reprezintă unul dintre instrumentele cheie în elaborarea deciziilor. În condițiile curente și cele viitoare, când tehnologiile se dezvoltă cu o progresie geometrică, este crucial de a asigura, pentru analiza, informație relevantă și actuală. Un proces de gestiune a riscurilor consistent ne permite, nu doar să anticipam potențialele evenimente nedorite, dar și să învățăm din experiența anterioară, analizând și contrapunând diferiți indicatori de risc.

BIBLIOGRAFIE

1. ISO 31000, *Risk management – Guidelines*
2. HOTĂRÎRE Nr. 201 din 28.03.2017 privind *Cerințe minime obligatorii de securitate cibernetică*
3. Levi Gundert, The Risk Business (2020) - *What CISOs Need to Know About Risk-Based Cybersecurity*
4. Лившиц Илья Иосифович (2018) *Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами*
5. Ванюрихин Ф.Г. (2019), *Модели и методы динамического управления рисками предприятий.*