Raport privind analiza documentelor strategice existente la nivelul Centrului Național de Răspuns la Incidente de Securitate Cibernetică și a responsabilităților care decurg din monitorizarea acestora

Cod SIPOCA: 391 MYSMIS 116172
Contract nr. 24 din data 15.04.2020

Beneficiar: Autoritatea pentru Digitalizarea României (ADR) și
Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)
Țara: România

Proiect: Sistem integrat de management pentru o societate informațională performantă (SIMSIP)
Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020

Prestator:
Asocierea formată din ERNST & YOUNG SRL (România), în calitate de lider al asocierii și
PUBLIC RESEARCH SRL – Asociat
INITINVEST CONSULTING - Subcontractor

Informații document

Consultant:	ASOCIEREA FORMATĂ DIN ERNST & YOUNG SRL (ROMÂNIA) ÎN CALITATE DE LIDER AL ASOCIERII, (BUCHAREST TOWER CENTER, ETAJ 22, BD. ION MIHALACHE NR. 15-17, SECTOR 1 011171 BUCUREȘTI, ROMÂNIA) și PUBLIC RESEARCH SRL, INITINVEST CONSULTING - Subcontractor		
Denumirea proiectului:	Sistem integrat de management pentru o societate informațională performantă (SIMSIP)		
Lider de echipă:		**Versiune Document Nr:**	0.2
Etapă Implementare Proiect:		**Dată versiune document:**	15.07.2020
Metoda de revizuire a calității:	Revizuire de către Management		

Întocmit de către:

Nume	Rol	Data	Semnătura
Corina Homeuca	Expert cheie BSC	15.07.2020	
Carmen Adamescu	Expert cheie Coordonator de proiect	15.07.2020	
Adelina Peculea	Expert non- cheie	15.07.2020	
Andy Leoveanu	Expert non- cheie	15.07.2020	
Cristian Ghica	Expert non- cheie	15.07.2020	
Eduard Enache	Expert non- cheie	15.07.2020	
Vlad Lixandru	Expert non- cheie	15.07.2020	
Vlad Donciu	Expert non- cheie	15.07.2020	
Vlad Barbălată	Expert non- cheie	15.07.2020	
Monica Măroiu	Expert non- cheie	15.07.2020	
Roxana Popovici	Expert non- cheie	15.07.2020	

Lista de distribuție:

De la	Data	Telefon /Fax
Carmen Adamescu	15.07.2020	
Corina Homeuca	15.07.2020	

Către	Data	Tip acțiune
Monica Chiffa		Revizuire/Aprobare
Cristian Priboi		Revizuire

Tipuri de acțiune: Aprobare, Revizuire, Informare, Clasare, Acțiunea impusă, Participarea la ședință, altele (vă rugăm să specificați)

Istoric versiuni:

Ver. Nr.	Data Ver.	Revizuit de către	Descriere	Denumire fișier
0.1	30.06.2020	Corina Homeuca	Versiune preliminară	Livrabil A 6.1_Cert-RO
0.2	15.07.2020	Carmen Adamescu	Versiune finală	Livrabil A 6.1_Cert-RO

Cuprins

Lista abrevierilor

Abreviere	Explicație
ADR	Autoritatea pentru Digitalizarea României
BSC	Tablou de bord echilibrat pentru evaluarea performanței în engl. Balanced Scorecard
CAF	Cadrul Comun de Autoevaluare al Instituțiilor Publice
CERT-RO	Centrul Național de Răspuns la Incidente de Securitate Cibernetică
CSIRT	Computer Security Incident Response Team
FEIM	fundamentare, elaborare, implementare, monitorizare, evaluare
IL	Instrucțiuni de lucru
NIS	National Integrity System
MCSI	Ministerul Comunicațiilor și Societății Informaționale
MTIC	Ministerul Transporturilor, Infrastructurii și Comunicațiilor
ONRC	Oficiul Național Registrul Comerțului
PALG	Planul Anual de Lucru al Guvernului
PAIEMCAIP	Planul de acțiuni pentru implementarea etapizată a managementului calității în autorități și instituții publice 2016-2020
PAISPAAC	Planul integrat pentru simplificarea procedurilor administrative aplicabile cetățenilor
PO	Procedură operațională
PG	Program de guvernare
POCA	Programul Operațional Capacitate Administrativă
PS	Procedură de sistem
PSI	Plan strategic instituțional
PISNA	Planul de Integritate privind aplicarea SNA
ROF	Regulament de Organizare și Funcționare
ROI	Regulament de Ordine Interioară
SAT	Sistemului de Alertă Timpurie
SGG	Secretariatul General al Guvernului
SCAP	Strategia de Consolidarea a Administrației Publice 2014-2020
SNA	Strategia Națională Anticorupție 2016-2020
SNADR	Strategia Națională privind Agenda Digitală pentru România 2020
SPBR	Strategia privind mai Buna Reglementare 2014-2020
SCIM	Sistem de control intern managerial
UE	Uniunea Europeană

1 Introducere

Activitatea A6 din cadrul proiectului Sistem integrat de management pentru o societate informațională performantă (SIMSIP) are drept scop implementarea unui sistem de management al performanței în cadrul Autorității pentru Digitalizarea României (ADR) și Centrului Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO) bazat pe instrumentul Balanced Scorecard (BSC). Activitatea este structurată sub forma a 3 sub-activități:

1. Sub-activitatea A.6.1. - Analizarea strategiilor existente la nivelul celor două entități, precum și a responsabilităților ce decurg din monitorizarea acestora;
2. Sub-activitatea A.6.2. - Dezvoltarea sistemului de management al performanței BSC;
3. Sub-activitatea A.6.3. - Organizarea de evenimente pentru diseminarea și promovarea sistemului de management al performanței, împreună cu realizarea de pliante, manuale, organizarea de acțiuni de promovare, precum și diseminare a bunelor practici.

Prezentul raport reprezintă rezultatul sub-activității A.6.1 care a presupus analiza documentelor existente în cadrul CERT-RO. Informațiile relevante cu privire la responsabilitățile care decurg din analiza documentelor strategice existente au fost obținute printr-un exercițiu de colaborare cu structurile de specialitate din cadrul instituției. De asemenea, tot ca parte a acestei activități, au fost inventariate toate documentele strategice existente la nivelul Centrului Național de Răspuns la Incidente de Securitate Cibernetică.

Evaluarea sistematică a performanțelor, procedurilor și a proceselor în corelație cu resursele existente și mediul organizațional actual, caracterizate de schimbări permanente creează premise pentru proiectarea și implementarea unor decizii manageriale care să contribuie la îndeplinirea obiectivelor strategice și operaționale. În acest sens, îmbunătățirea procesului de management strategic reprezintă obiectivul principal al analizei realizate care urmărește evaluarea situației actuale a implementării managementului strategic la nivelul CERT-RO. Mai mult, această analiză, gândită ca un instrument de management, vizează **inventarierea tuturor „documentelor strategice”** existente în cadrul organizației, identificarea modului în care acestea sunt utilizate și formularea de recomandări privind îmbunătățirea procesului de management strategic. Pentru sectorul public, **managementul strategic se transpune prin decizii și acțiuni, urmărind formularea și implementarea de planuri proiectate pentru a realiza obiectivele organizaționale,** astfel încât să se asigure o viziune unitară și coerentă cu privire la administrarea serviciilor publice furnizate. În categoria „documentelor strategice” sunt avute în vedere documente precum strategiile, planurile de acțiuni, planurile de măsuri și nu numai.

Analiza este realizată din perspectiva metodelor utilizate, a resurselor alocate, a rolurilor și responsabilităților, a modului de derulare a procesului de planificare strategică (procese și fluxul acestora). În egală măsură, au fost avute în vedere procedurile interne, circuitul documentelor și analiza părților interesate implicate.

Analiza contribuie la atingerea obiectivelor specifice ale proiectului Sistem integrat de management pentru o societate informațională performantă (SIMSIP), cod SIPOCA 391,

cofinanțat prin Fondul Social European și Bugetul Național al României prin Programul Operațional Capacitate Administrativă 2014-2020, ce vizează având ca scop atingerea OS 1.1 al POCA – Dezvoltarea și introducerea de sisteme și standarde comune în administrația publică ce optimizează procesele decizionale orientate către cetățeni și mediul de afaceri, în concordanță cu Strategia pentru Consolidarea Administrației Publice (SCAP), prin dezvoltarea și implementarea setului de instrumente Cadrul Comun de Autoevaluare al Instituțiilor Publice (CAF) și BSC pentru furnizarea unor servicii de calitate recunoscute la nivel internațional.

Obiectivul general al proiectului este creșterea capacității administrative a ADR și CERT-RO pentru susținerea reformelor instituționale prin implementarea unui sistem unitar de management al calității (care să aibă la bază instrumentul CAF și standardul ISO 9001:2015) și al performanței (care sa aibă la bază BSC), precum și a unui sistem care să cuprindă proceduri și mecanisme pentru coordonare și consultare cu factorii interesați privind implementarea, monitorizarea și evaluarea politicilor și strategiilor pentru care CERT-RO este responsabil.

Procesul de analiză a fost unul iterativ și interactiv, iar informațiile utilizate au fost generate în contextul studierii documentelor, a prelucrării rezultatelor interviurilor desfășurate cu principalele părți interesate, precum și a rezultatelor obținute în urma aplicării unui chestionar cu scopul colectării punctelor de vedere ale unui grup mai mare de actori implicați în procesul de planificare strategică din cadrul CERT-RO. Concret, pentru realizarea analizei, sunt avute în vedere următoarele:

- realizarea analizei privind procedurile actuale de fundamentare, elaborare, implementare, monitorizare, evaluare a documentelor de planificare, cu implicarea echipei de experți și suportul permanent acordat de către structura și de echipa managerială din partea CERT-RO;
- diagnosticarea este realizată în baza metodologiei specifice, care îmbină metode și tehnici adecvate statutului de organizație nouă a CERT-RO;
- analiza realizată a avut în vedere obiectivele formulate;
- analiza conține o interpretare a rezultatelor în contextul realității existente;
- toate datele utilizate sunt adecvate obiectivelor și ipotezelor formulate;
- există suficiente date/probe înregistrate pentru a sprijini fiecare constatare;
- concluziile formulate se bazează strict pe constatări.

Informațiile obținute în cadrul activității de analiză urmează să fundamenteze proiectarea sistemului BSC, sistem care are drept scop facilitarea dezvoltării, aplicării și monitorizării documentelor de planificare strategică.

2 Sumar executiv

În contextul schimbărilor tehnologice, alinierii la directivele europene și a implementării unui sistem modern de management, planificarea și deciziile strategice devin cruciale pentru creșterea performanței organizaționale și a eficienței serviciilor oferite. Astfel, pornind de la beneficiile managementului schimbării organizaționale, considerăm că este important să sprijinim CERT-RO prin implementarea unui sistem de management strategic/sistem decizional axat pe criterii de performanță și orientat către creșterea calității serviciilor publice. De asemenea, se urmărește dezvoltarea capacității personalului de a utiliza unitar instrumentele managementului strategic bazat pe BSC în vederea îmbunătățirii comunicării organizaționale, cât și a monitorizării performanțelor acesteia plecând de la obiectivele strategice.

Analiza diagnostic cuprinsă în acest document a fost realizată cu scopul de a susține implementarea BSC în cadrul CERT-RO prin identificarea unor arii care pot fi îmbunătățire prin acesta. Realizarea acestei analize a presupus culegerea datelor, verificarea, sistematizarea și gruparea lor, inclusiv prin reprezentări grafice, apoi analiza, interpretarea și discutarea punctelor critice cu reprezentanții proceselor decizionale, respectiv operaționale astfel încât rezultatele obținute din analiza datelor să fie valorificate prin elaborarea unor recomandări.

Din punct de vedere metodologic, consultantul a utilizat o abordare mixtă, folosind diverse metode pentru a colecta și/ sau verifica/ triangula informațiile corespunzătoare. Strategia de colectare a datelor a combinat instrumente de cercetare diferite astfel încât să existe cât mai multe date pentru fundamentarea concluziilor finale. Datele relevante colectate au conținut informații cantitative și calitative.

Obiectivele fundamentale ale analizei au avut în vedere furnizarea unei imagini detaliată a procesului de management strategic desfășurat în cadrul CERT-RO cu mențiuni concrete despre fluxurile informaționale care sprijină de altfel procesele operaționale și de decizie, completată cu rezultate care arată implicarea CERT-RO în cadrul proceselor de elaborare/ implementare/ monitorizare/ evaluare a unor documente de planificare strategică. Analiza diagnostic realizată asupra CERT-RO expune atât aspecte pozitive, cât și practici care pot fi îmbunătățite în vederea implementării cu succes a unui instrument de management strategic care să asigure performanțe ridicate și să genereze direcții sustenabile de dezvoltare.

Rezultatele și concluziile cheie în urma analizei au în vedere:

- existența unui **proces managerial**, reflectat în ambele planuri, operațional și de decizie, riguros fundamentat pe o serie de analize din care sunt desprinse informații cu privire la inventarul factorilor interesați de activitatea CERT-RO, la elementele caracteristice mediului exterior și interior CERT-RO (de exemplu, Programul de Guvernare, strategii naționale, nevoile și interesele beneficiarilor de servicii, cadrul legislativ care reglementează organizarea și funcționarea entității etc.) și pe care le integrează ulterior în deciziile adoptate (inclusiv materializate în documente strategice) ținând cont și de riscurile identificate la nivelul entității;

- **desfășurarea procesului de management strategic** în parametri de funcționalitate cu o nevoie reală de implicare a CERT-RO în cadrul proceselor de elaborare/ implementare/ monitorizare/ evaluare a unor documente strategice;
- formarea permanentă a personalului, motivarea personalului și acoperirea deficitului de personal;
- atragerea de **surse de finanțare** pentru acoperirea necesarului de investiții din cadrul instituției;
- dezvoltarea, extinderea și actualizarea continuă a **sistemului de proceduri** de lucru, în conformitate cu cerințele actuale dar și cu riscurile de natură cibernetică;
- implementarea unui **sistem de măsurare a performanțelor** bazat pe criterii de dezvoltare continuă a instituției și pe obiective clare, formulate la toate nivelurile ierarhice și măsurate prin indicatori cheie ai performanței;
- intensificarea utilizării instrumentelor de **management al riscurilor** pentru o mai bună adaptabilitate la survenirea evenimentelor negative;
- elaborarea și implementarea unei **strategii de calitate** prin procese specifice managementului calității totale.

3 Cadrul general al analizei diagnostic

3.1 Metodologia

Din punct de vedere metodologic, analiza s-a realizat parcurgând următoarele etape:

Etapa 1: Analiza documentară preliminară

Aceasta este etapa de pregătire a diagnosticului în care au avut loc întâlniri între echipa de experți și reprezentanții CERT-RO prin care s-au definitivat instrumentele de lucru și acțiunile de parcurs. Scopul analizei documentare a fost acela de a evalua sursele de date, calitatea și volumul informațiilor existente și de a aprofunda cunoștințele și înțelegerea cu privire la strategiile evaluate. În această etapă s-au realizat:

- definirea problemelor supuse analizei și a obiectivelor de urmărit prin analiza-diagnostic;
- stabilirea exactă a rolurilor echipei de experți și a reprezentanților CERT-RO;
- stabilirea metodelor de abordare, a necesarului de materiale auxiliare (chestionare, fișe etc.);
- efectuarea unor investigații preliminare pentru stabilirea necesarului de date;
- stabilirea planului concret de acțiune;
- stabilirea indicatorilor de pornire;
- colectarea de date primare.

Această primă etapă s-a finalizat cu elaborarea unui grafic al acțiunilor și cu obținerea acordului din partea Beneficiarului privind modul de lucru, termenele propuse, persoanele implicate etc.

Detalierea metodologiei de analiză a avut în vedere clasificarea întrebărilor și criteriilor de evaluare, precum și indicarea tipurilor de analiză și a surselor de date primare și secundare. Pentru analiza procesului de management, întrebările și criteriile de evaluare, tipurile de analiză și sursele de date au fost structurate conform următoarei etapizări:

- Fundamentare a documentelor strategice;
- Elaborare / formulare;
- Implementare;
- Procesul de monitorizare și revizuire;
- Evaluare a documentelor strategice.

Elaborarea strategiei de colectare a datelor și a programului de lucru a fost realizată cu scopul de a asigura calitatea datelor și a informațiilor pentru obținerea cărora au fost utilizate următoarele instrumente de colectare a datelor care au facilitat triangularea informațiilor provenite din mai multe surse și formularea unui set de concluzii și recomandări robuste:

- Analiza documentară a documentelor relevante;
- Interviuri cu factorii interesați (stakeholderi) ai Strategiei de dezvoltare a TIC;
- Sondajul electronic în rândul beneficiarilor;
- Focus-grup cu factorii interesați.

Etapa 2: Detalierea instrumentelor de colectare a datelor

Analiza documentară/cercetare de birou – A fost realizată o analiză aprofundată a documentelor, informațiilor și datelor referitoare la documentele strategice existente și a planurilor de acțiune asociate. Scopul cercetării de birou este acela de a aprofunda înțelegerea cu privire la logica intervenției, de a analiza și determina progresul în implementare și a valida informațiile colectate din alte surse cu privire la lecțiile învățate și aspectele care afectează implementarea Strategiei/proiectelor, la data limită a evaluării.

Interviuri - au avut o importanță crescută pentru exercițiul de evaluare deoarece au permis colectarea de informații generale și specifice direct de la părțile implicate/responsabile în conceperea / implementarea strategiei care este supusă analizei. În cadrul interviurilor au fost adresate atât întrebări generale, cât și specifice privind implementarea strategiei, evoluția generală, bunele practici și lecții învățate. Modelul grilei de interviu utilizată poate fi consultat în Anexa dedesubt6.1 a prezentului raport.

Sondajul electronic – obiectivul sondajului a fost acela de a colecta informații/opinii de la un grup mare de persoane juridice și/sau fizice implicate în și/sau interesate de implementarea Strategiei. Chestionarul aplicat a cuprins un număr limitat de întrebări direct corelate cu întrebările incluse în cadrul general de evaluare. Sondajul a fost aplicat în rândul beneficiarilor (eșantion reprezentativ), prin intermediul emailului și a opțiunii Adobe Fișiere PDF Optimizate care a asigurat generarea, administrarea și procesarea automată a informațiilor. Modelul chestionarului aplicat poate fi consultat în Anexa 6.3 a prezentului raport.

Focus grup – prin intermediul acestui instrument s-au dezbătut aspectele care afectează implementarea proiectelor finanțate vis a vis de aranjamentele de implementare stabilite la nivelul Strategiei. De asemenea, un alt obiectiv al focus grupului a fost acela de a valida eventuale măsuri de îmbunătățire sugerate.

Instrumentele metodologice sunt elaborate cu scopul de a sprijini echipa de proiect în colectarea informațiilor (fișa, chestionare, documente centralizatoare ale informațiilor analizate sau colectate, alte documente după caz). Au fost elaborate două tipuri de instrumente metodologice: **fișa de analiză și chestionarele.** Aceste chestionare au fost completate de către reprezentanții CERT-RO. Întrebările care compun chestionarul au fost elaborate cu scopul de a facilita culegerea datelor necesare pentru a putea răspunde obiectivelor cercetării, în cadrul chestionarului putând fi identificate atât întrebări închise precum și întrebări deschise, menite să colecteze o gamă cât mai largă a datelor colectate. Astfel, în cadrul chestionarului pot fi identificate întrebări închise, care presupun alegerea unei singure opțiuni din mai multe alternative posibile, dar și întrebări deschise care presupun obținerea unui răspuns diferit de cele indicate în cadrul întrebărilor închise, punându-se accentul pe percepția respondentului și opinia sa personală. Întrebările deschise sunt deosebit de utile în cazul unei cercetări exploratorii, cum este cea de față, ele servind, printre altele, la formularea ipotezelor cercetării și la identificarea unor idei noi.

3.1.1 Prezentarea CERT-RO și analiza provocărilor în implementarea BSC

Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO) este o instituție publică înființată în anul 2011 prin Hotărârea Guvernului nr. 494 din 11 mai 2011. CERT-RO reprezintă o structură independentă de expertiză și cercetare - dezvoltare în domeniul protecției infrastructurii cibernetice aflată până de curând sub coordonarea Ministerului Comunicațiilor și Societății Informaționale (MCSI) care, în urma reorganizării instituționale realizate ca urmare a Ordonanței de urgență a Guvernului nr. 68/2019, a fost desființat, toată activitatea în domeniul digital și structurile specializate în acest domeniu fiind preluate de Autoritatea pentru Digitalizarea României înființată prin Hotărârea Guvernului 89/2020.

Un alt document legislativ care reglementează activitatea CERT-RO este Legea nr. 362/2018, intrată în vigoare la data de 12 ianuarie 2019, privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice. Această lege transpune în legislația națională prevederile Directivei (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune care urmărește obiectivele Strategiei Europene de securitate cibernetică stabilite pentru pilonul National Integrity System (NIS).

În conformitate cu Legea nr. 362/2018, dar și cu Regulamentul de Organizare și Funcționare al instituției, CERT-RO funcționează în calitate de autoritate competentă în domeniu la nivel național, Punct național unic de contact, CSIRT (Computer Security Incident Response Team) național și instituție publică de expertiză și cercetare - dezvoltare în domeniul protecției infrastructurilor cibernetice. În funcție de calitățile pe care le îndeplinește conform legislației, CERT-RO are următoarele atribuții:

1. **Autoritate competentă la nivel național:**
   - Evidență – în acest sens identifică și ține evidența operatorilor de servicii esențiale și furnizorilor de servicii digitale;
   - Autorizare și atestare – în acest sens autorizează, revocă sau reînnoiește autorizarea echipelor CSIRT ce deservesc operatori de servicii esențiale ori furnizori de servicii digitale, precum și a formatorilor și furnizorilor de servicii de formare a echipelor CSIRT și auditorilor de securitate, respectiv eliberează, revocă sau reînnoiește atestatele auditorilor de securitate informatică care pot efectua audit în cadrul rețelelor și sistemelor informatice ce susțin servicii esențiale ori furnizează servicii digitale;
   - Control și monitorizare – în acest sens monitorizează aplicarea prevederilor Legii nr. 362/2018, cu modificările și completările ulterioare și verifică respectarea de către operatorii de servicii esențiale și furnizorii de servicii digitale a obligațiilor ce le revin conform Legii nr. 362/2018;
   - Reglementare tehnică – în acest sens elaborează și actualizează normele metodologice, tehnice, precum și regulamentele privind cerințele referitoare la înființarea, autorizarea și funcționarea echipelor CSIRT, desemnarea echipelor CSIRT sectoriale, cele referitoare la atestarea auditorilor calificați cu competențe în domeniul securității serviciilor esențiale și a serviciilor digitale, precum și normele referitoare la autorizarea formatorilor și furnizorilor de servicii de formare;

- Relaționare interinstituțională – în acest sens coordonează activitatea Grupului de lucru interinstituțional, prevăzut de art. 6 alin. (4) din Legea nr. 362/2018, și participă la Grupul de cooperare la nivelul Uniunii Europene constituit pentru a facilita cooperarea strategică și schimbul de informații între statele membre, pentru a consolida încrederea și în vederea obținerii unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană.

2. **Punct național unic de contact:**
   - Legătură internațională – în acest sens asigură legătură între autoritățile statului și autoritățile similare din alte state, Grupul de cooperare și rețeaua echipelor de răspuns la incidentele de securitate informatică;
   - Cooperare internă și internațională – în acest sens transmite la cererea autorităților sau a echipelor CSIRT, către punctele unice de contact din celelalte state membre, precum și la autoritățile prevăzute la art. 15 alin. (2) și art. 16 din Legea nr. 362/2018, cu modificările și completările ulterioare, notificările și cererile primite.
3. **CSIRT (Computer Security Incident Response Team) național:**
   - Monitorizare incidente – în acest sens monitorizează incidentele de securitate a rețelelor și sistemelor informatice la nivel național și emite avertizări timpurii, alerte și anunțuri și diseminează informațiile privind riscurile și incidentele către orice entitate de drept public sau privat căreia îi poate fi afectată securitatea rețelelor și sistemelor informatice;
   - Analiză impact incidente – în acest sens stabilește impactul la nivel național și transfrontalier al incidentelor și informează autoritățile relevante la nivel național, precum și autoritățile similare din alte state potențial afectate; elaborează analize dinamice de risc și de incident;
   - Răspuns la incidente de securitate – în acest sens asigură răspunsul la incidente în limitele legii; înființează, întreține și operează serviciul de alertare și cooperare cu operatorii de servicii esențiale și furnizorii de servicii digitale; participă la acțiuni comune în cadrul rețelei CSIRT la nivel european. completările ulterioare, cu privire la produsele și sistemele de securitate cibernetică care deservesc infrastructurile critice naționale și europene.
4. **Instituție publică de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice**
   - Analiză disfuncționalități tehnice – în acest sens analizează disfuncționalitățile procedurale și tehnice la nivelul infrastructurilor cibernetice, potrivit ariei de competență, și transmite instituțiilor sau autorităților publice ori altor persoane juridice de drept public sau privat aspectele de interes;
   - Elaborare politici publice – în acest sens asigură elaborarea și diseminarea politicilor publice de prevenire și contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competență;

- Cercetare-dezvoltare – în acest sens desfășoară activități de cercetare-dezvoltare în domeniu și elaborează proceduri și recomandări privind securitatea cibernetică, potrivit prevederilor legale privind cercetarea științifică și dezvoltarea tehnologică;
- Suport tehnic de specialitate – în acest sens asigură cadrul organizatoric și suportul tehnic necesar schimbului de informații dintre diverse echipe de tip CERT, utilizatori, autorități, producători de echipamente și soluții de securitate cibernetică, precum și furnizori de servicii în domeniu; organizează și desfășoară activități de instruire în domeniul securității cibernetice; asigură consultanță de specialitate autorităților publice responsabile, stabilite conform Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, aprobată cu modificări prin Legea nr.18/2011 cu modificările și completările ulterioare, cu privire la produsele și sistemele de securitate cibernetică care deservesc infrastructurile critice naționale și europene.

Pentru a evidenția modificările survenite în urma aplicării Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, în următorul tabel pot fi consultate noile atribuții ale CERT-RO care nu sunt surprinse în cadrul HG nr. 494/2011:

Noi atribuții ale CERT-RO ca urmare a Legii nr. 362/2018
Emitere de norme tehnice (securitate, notificare, audit, servicii CSIRT)
Identificarea și evidența OSE
Autorizare și acreditare (formatori, auditori, echipe CSIRT)
Primire de notificări privind incidentele de la agenți economici precum și de la autorități și echipe similare din celelalte state UE
Cooperare și coordonare (platforma de alertare și cooperare)
Coordonarea răspunsului la incidente la nivel național
Participarea în răspunsul comun la incidente la nivel european
Participarea în grupurile de cooperare NIS la nivel UE
Controlul respectării prevederilor legale și sancționare

Tabel 1 Noi atribuții ale CERT-RO ca urmare a Legii nr. 362/2018

În urma analizei actelor normative care reglementează activitatea CERT-RO, a reieșit faptul că instituția este responsabilă de punerea în aplicare a următoarelor strategii, regulamente și metodologii aflate în aria sa de competență, elaborate atât la nivel național, cât și la nivel european:

- Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (Directiva NIS);
- Strategia de securitate cibernetică a României, aprobată prin HG nr. 271/2013;

- Planul de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, aprobat prin HG nr. 271/2013; care se comunică direct instituțiilor interesate, având caracter clasificat potrivit legii.
- Normele metodologice de identificare a operatorilor de servicii esențiale și furnizorilor de servicii digitale, aprobate prin ORDIN 599/2019;
- Normele metodologice de organizare și funcționare a Registrului operatorilor de servicii esențiale, aprobate prin ORDIN 600/2019;
- Metodologie de stabilire a efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale, aprobată prin ORDIN 601/2019;
- Regulamente, proceduri şi norme proprii.

Conform legii 362/2018, în fiecare an CERT-RO, în calitate de punct unic de contact, elaborează un raport de sinteză care include numărul de notificări și natura incidentelor notificate, precum și acțiunile de remediere întreprinse.

CERT-RO în calitate de instituție publică de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice, în relația sa directă cu cetățenii, asigură elaborarea și diseminarea politicilor publice de prevenire și contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competență. Astfel CERT-RO promovează următoarele campanii de conștientizare și ghiduri de informare cu scopul de a încuraja utilizarea în siguranță a platformelor și serviciilor digitale de către toți cetățenii:

- Campania de conștientizare împotriva malware-ului pentru dispozitivele mobile;
- Campanie de prevenire a criminalității informatice în rândul tinerilor;
- Campanie de conștientizare înșelăciuni cu suport tehnic fals;
- Informarea despre NIS - legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;
- Divulgarea Coordonată a Vulnerabilităților (CVD) prin Serviciul de Raportare Vulnerabilități pus la dispoziție de către CERT-RO care este dedicat profesioniștilor în securitatea rețelelor și sistemelor informatice precum și cetățenilor care au identificat o vulnerabilitate ca utilizatori ai unui serviciu sau sistem informatic oferit publicului și doresc să o semnaleze spre remediere. Prezentul serviciu nu constituie sub nici o formă îndemn la comiterea de fapte penale pentru efectuarea de activități de ethical hacking (ex. teste de penetrare) sau alte tipuri de activități în legătură cu rețelele și sistemele informatice care nu le aparțin ori pentru care nu dețin dreptul de a le testa.
- Promovarea dezvoltării competențelor și a educației digitale a utilizatorilor, indiferent de pregătirea acestora prin programul online de mentorare în securitate cibernetică, desfășurat pe parcursul a 12 luni și promovat de CERT-RO și și Digital Nation;
- Numeroase ghiduri de informare printre care cele mai recente sunt: Noul normal după COVID-19 un ghid de siguranță, Recomandări pentru utilizare în siguranță a platformei Zoom sau Recomandări pentru angajați și angajatori în cazul telemuncii.

Strategia de securitate cibernetică a României numește, printre direcțiile sale de acțiune, **dezvoltarea capacităților naționale de management** al riscului în domeniul securității cibernetice și de reacție la incidente cibernetice în baza unui program național, inclusiv prin dezvoltarea entităților de tip CERT, atât în cadrul sectorului public, cât și în sectorul privat.

Capitolul 4 al strategiei de securitate cibernetică a României, ce descrie Sistemul național de securitate cibernetică, menționează ca atribuții ale CERT-RO - asigurarea elaborării și diseminării politicilor publice de prevenire și contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competență. În acest sens, în cadrul proiectului „Sistemul Național de Combatere a Criminalității Informatice Cyber Crime" al cărui beneficiar a fost, în anul 2014, Centrul Național de Răspuns la Incidente de Securitate Cibernetică a fost dezvoltată o serie de propuneri de politici publice după cum urmează:

- Propunere de politică publică privind extinderea Sistemului de Alertă Timpurie („SAT");
- Propunere de politică publică privind definirea statutului de furnizor de servicii de securitate cibernetică în vederea dezvoltării capacității de răspuns la incidentele de securitate;
- Propunere de politică publică privind înființarea și operaționalizarea unei unități specializate de tip „Patrulă cibernetică";
- Propunere de politică publică privind formarea de juriști cu specializare în domeniile drept informatic, probe digitale și criminalitate informatică;
- Propunere de politică publică privind formarea inițială și pregătirea profesională continuă a procurorilor și judecătorilor în domeniile: drept informatic, probe digitale și criminalitate informatică;
- Propunere de politică publică privind formarea inițială și pregătirea profesională continuă a polițiștilor în drept informatic, criminalitate informatică și probe / investigații digitale;
- Propunere de politică publică privind instruirea specifică a judecătorilor, procurorilor și polițiștilor prin exerciții și simulări integrate pe domeniile securitate cibernetică și criminalitate informatică;
- Propunere de politică publică privind definirea unui standard ocupațional și a unor criterii de competență de bază pentru personalul care operează și administrează infrastructuri de securitate informatică;
- Propunere de politică publică privind stabilirea unui program guvernamental de comunicare publică unitară în scopul prevenirii criminalității informatice;
- Propunere de politică publică privind îmbunătățirea educației pentru elevi și studenți în domeniul securității IT și prevenirea criminalității informatice. Pregătirea de competențe în domeniu. Creșterea gradului de siguranță a utilizării tehnologiei informației în școli și universități;
- Propunere de politică publică privind măsuri de protecție juridică a organizațiilor din mediul public și privat împotriva „amenințărilor din interior" privitoare la securitatea cibernetică;
- Propunere de politică publică privind incriminarea corespunzătoare a unor fapte din sfera criminalității informatice care au produs consecințe deosebit de grave . Circumstanță agravantă;

- Propunere de politică publică privind incriminarea distinctă în Codul Penal a faptei de furt de identitate;
- Propunere de politică publică privind clarificarea și armonizarea sensului unor noțiuni și expresii legate de domeniul informatic din Codul Penal și Codul de Procedură Penală.

3.2 Limitări privind analiza

3.2.1 Limitări metodologice

Pentru fiecare instrument utilizat pentru colectarea datelor au existat următoarele limitări metodologice care au fost depășite, în măsura în care a fost posibil, prin intermediul unor măsuri de prevenție asumate de către echipa de experți implicați în realizarea analizelor. Astfel, limitările metodologice specifice fiecărui instrument de colectare a datelor au fost:

- Analiza documentară de cele mai multe ori, oferă informații generale din sistemul de monitorizare/date privind procedurile și nu conduc la identificarea directă a bunelor practici sau informațiilor privind experiența practică.
- Interviurile online furnizează informații care pot fi afectate de gradul de subiectivism al intervievatului și intervievatorului.
- Sondajul electronic în rândul beneficiarilor este expus riscului privind rata de răspuns redusă; riscului privind primirea unor răspunsuri inexacte; gradul de reprezentare a factorilor interesați in cadrul eșantionului selectat poate fi insuficient; și procesarea dificilă a răspunsurilor la întrebările exploratorii și cu răspuns deschis.

3.2.2 Limitări sociale

În contextul actual de pandemie, toate întâlnirile și activitățile prevăzute pentru realizarea acestui livrabil au fost susținute online, prin utilizarea mijloacelor digitale. Măsurile de distanțare socială pentru limitarea răspândirii Covid-19 s-au impus în România începând cu Decretul Președintelui României nr. 195/16 Martie 2020 privind instituirea stării de urgență pe teritoriul României, care a intrat în vigoare în data de 16 martie 2020 data publicării în MO nr. 212. Apoi măsurile de distanțare socială au continuat să fie impuse într-o manieră mai puțin restrictivă, în starea de alertă instituită în data de 15 Mai 2020 prin Hotărârea Comitetului Național pentru Situații de Urgență și prelungită până în prezent, 15 iulie 2020.

4 Răspunsuri la întrebările de evaluare/ analiză

Analiza are la bază parcurgerea următoarelor etape principale:

Etapa 1 – Inițierea (în cadrul acestei etape au fost validate așteptările și ipotezele de lucru și a fost detaliată metodologia de evaluare pe baza înțelegerii contextului și logicii documentelor strategice existente):

- Stabilirea obiectivelor;
- Detalierea activităților – analiza documentară preliminară, metodologia analitică, strategia de colectare a datelor și programul de lucru.

Etapa 2 – Colectarea și analiza datelor (această etapă a presupus colectarea și analiza datelor prin aplicarea tehnicilor și instrumentelor de evaluare, conform metodologiei aprobate):

- Stabilirea obiectivelor;
- Detalierea activităților – descrierea instrumentelor de colectare a datelor, analiza detaliată a datelor colectate și prezentarea rezultatelor preliminare.

Etapa 3 – Raportare (în cadrul acestei etape au fost comunicate rezultatele analizei în conformitate cu formatele agreate și standardele de calitate aplicabile):

- Stabilirea obiectivelor;
- Detalierea activităților – întocmirea livrabilului final.

Pornind de la informațiile prezentate în secțiunile anterioare, subliniem rolul CERT-RO, ca autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice care asigură furnizarea de servicii esențiale ori furnizează servicii digitale având atribuții de reglementare, autorizare, atestare, monitorizare și control, cuprinzând în structura sa o echipă națională de răspuns la incidente de securitate informatică și un punct unic de contact la nivel național. Observăm de asemenea, specificul CERT-RO, care este o structură independentă de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice. Mai mult, CERT-RO este organismul principal de reglementare și gestionare a infrastructurii IT din România, cu atribuții de importanță strategică, raportate la următoarele puncte centrale:

- autoritate competentă la nivel național (evidență, autorizare și atestare, control și monitorizare, reglementare tehnică, relaționare inter-instituțională);
- punct național unic de contact (legătură internațională);
- echipă de răspuns la incidentele de securitate informatică (CSIRT);
- instituție publică de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice.

Pentru exercitarea atribuțiilor menționate mai sus, CERT-RO a formulat următoarele obiective generale:

- OG1 – Consolidarea rolului CERT-RO de autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, CSIRT național, punct unic de contact, precum și CERT național;
- OG2 – Încadrarea și pregătirea resursei umane a CERT-RO;

- OG3 – Îmbunătăţirea proceselor de gestionare şi reacţie la incidente de securitate cibernetică;
- OG4 – Atragerea de surse de finanţare;
- OG5 – SCIM.

Pentru a formula soluții și propuneri care să se regăsească în direcții viitoare strategice, a fost analizată situația actuală a fluxurilor informaționale/proceselor operaționale și de decizie, așa cum apar formalizate în diferite documente interne, respectiv externe. În acest sens, subliniem importanța fluxurilor informaționale de la nivelul CERT-RO, care trebuie să confere un real suport proceselor operaționale și de decizie. Observăm astfel, cum acestea sunt sprijinite de o bună comunicare intra și inter-organizațională, de existenţa unui sistem clar şi transparent de accesare a serviciilor publice, de utilizarea instrumentelor TIC, de ierarhizarea accesului la informații, de o corectă trasabilitate, de o soluționare operativă a incidentelor apărute în funcționarea sistemului informatic, de securitatea aplicațiilor utilizate în cadrul entității și de asistență tehnică a utilizatorilor aplicațiilor informatice.

În urma analizei instituționale realizate s-a determinat situația actuală a instituției și domeniile de acțiune viitoare. Astfel, în cele ce urmează vor fi prezentate concluziile analizei și modul în care acestea influențează atingerea obiectivelor.

Pentru **obiectivul general 1** (consolidarea rolului de autoritate competentă la nivel național), analiza a reliefat o structură organizațională funcțională și adecvată, beneficiind de un regulament de organizare și funcționare (ROF) și de o organigramă actualizată, completă și cunoscute de către angajații instituției precum și de o structură organizatorică capabilă să răspundă cerințelor la care este supusă. Structura organizațională este bazată pe relații ierarhice bine definite, ceea ce contribuie pozitiv la funcționalitatea ei, dar nu reflectă în totalitate relațiile de subordonare/coordonare. Acestea din urmă sunt reprezentate incorect din punct de vedere tehnic (de ex: există funcția de director adjunct, dar organigrama nu reprezintă clar compartimentele/serviciile din subordinea acestuia). De asemenea, sunt cunoscute și există o corelare cu cadrul legislativ și alte documente exterioare sistemului (program de guvernare, strategii naționale).

Tot între aspectele pozitive relevate de analiză menționăm abordarea corectă și unitară a problematicii eticii și integrității angajaților instituției. În acest sens, au fost apreciate pozitiv existența Codului de etică și faptul că întreg personalul cunoaște prevederile acestuia, existența avertizorului de integritate și organizarea activității de consiliere a personalului în probleme de etică.

Printre aspectele de îmbunătățit reliefate de studiu recomandăm elaborarea strategiei de dezvoltare a entității și a procedurii de monitorizare. Deoarece lipsesc bazele pentru formularea obiectivelor anuale și pentru măsurarea modului de atingere a obiectivelor și a performanțelor instituției. De asemenea, s-a identificat faptul că obiectivele formulate nu sunt revizuite în funcție de modificările aduse realizării activităților, într-o manieră procedural standardizată.

Printre aspectele de îmbunătățit legate de obiectivul general 1 (consolidarea rolului de autoritate competentă la nivel național) facem referire și la strategia de marketing și de promovare a serviciilor. În primul rând, eforturile de promovare a serviciilor CERT-RO ar trebui incluse în lista de obiective specifice, fiind cel mai potrivit să fie subordonate obiectivului general 1 (consolidarea rolului de autoritate competentă la nivel național). Analiza instituțională a reliefat existența unui sistem formalizat de promovare a serviciilor publice realizate, prin pagina de internet a instituției (http://cert.ro) care este funcțională și actualizată și a procedurilor de accesare a serviciilor publice, care sunt clare și disponibile în mod intuitiv.

De asemenea, analiza a reliefat comunicarea externă ca fiind adecvată scopului și obiectivelor instituției. Cu toate acestea, trebuie ridicată întrebarea referitoare la acuratețea afirmației precedente, în condițiile lipsei unei strategii de comunicare externă. Tot printre aspectele de îmbunătățit sistemului de comunicare se numără lipsa realizării unui sondaj în rândul beneficiarilor/grupului țintă și a măsurării satisfacției acestora, precum și a instrumentelor necesare realizării unei astfel de activități.

În ceea ce privește **obiectivul general 2** (încadrarea și pregătirea resursei umane a CERT-RO), s-a constatat o bună organizare a muncii prin acoperirea în totalitate a atribuțiilor și activităților prin sarcinile și fișele posturilor, precum și definirea sarcinilor, astfel încât să fie asigurată o bună colaborare între posturile de același nivel. În rândul aspectelor pozitive se numără și pregătirea adecvată a personalului în raport cu sarcinile și obligațiile curente ale posturilor.

Referitor la politica de personal și la managementul resurselor umane, au fost identificate următoarele puncte care necesită îmbunătățire:

- Personal insuficient;
- Lipsa unei strategii și a unui plan de dezvoltare profesională;
- Lipsa unui sistem de măsurare a performanței angajaților și;
- Lipsa unui sistem de motivare a personalului.

În acest sens, analiza arată faptul că întreg personalul participă la cursuri de formare profesională, dar în lipsa unei strategii și a unui plan de dezvoltare profesională, se pune problema eficienței și a eficacității acestor acțiuni, care sunt necorelate la nivel instituțional. De asemenea, trebuie menționat faptul că lipsa strategiei menționate anterior conduce în mod direct la nerealizarea în extenso a obiectivului specific 2.1.2 – pregătirea resursei umane prin cursuri în funcție de domeniul în care își desfășoară activitatea în cadrul CERT-RO.

Prin intermediul analizei instituționale s-a determinat faptul că personalul este evaluat cel puțin anual, dar nu în funcție de gradul de îndeplinire a criteriilor de performanță. Se ridică aici întrebarea, care sunt criteriile de evaluare a personalului în lipsa unui sistem de măsurare a performanței? De asemenea, cum poate fi asigurată o comunicare verticală și mai ales una orizontală adecvate, în condițiile în care planul de pregătire a personalului nu asigură dezvoltarea abilitaților de comunicare și de lucru în echipă?

Pentru **obiectivul general nr. 3** (îmbunătățirea proceselor) se observă o situație pozitivă. Astfel, a fost realizată alinierea la GDPR printr-un sistem care este funcțional, asigurând protecția datelor cu caracter personal prin regulament intern și prin implementarea de măsuri specifice organizației de protecție a datelor cu caracter personal. S-a determinat, de asemenea, existența registrului datelor cu caracter personal. Nu în ultimul rând, angajații cunosc normele de protecție a datelor cu caracter personal.

Din punct de vedere tehnic și procesual, instituția beneficiază de proceduri de lucru corecte, care descriu și stabilesc în mod just activitățile și responsabilitățile individuale. Asistența tehnică este asigurată, incidentele apărute sunt soluționate în mod operativ și securitate aplicațiilor este asigurată. Aici pot fi menționate trei observații care recomandăm să fie analizate:

- Cum se realizează controlul actualității registrului datelor cu caracter personal?
- De ce nu se ține registrul de intrări și ieșiri în mod digital?
- Sistemul de proceduri nu este complet (a se vedea aici observațiile de la obiectivul general nr. 5). Sunt acoperite de proceduri toate activitățile cu caracter tehnic?

Obiectivul general nr. 4 (atragere de surse de finanțare) este unul din obiectivele cheie ale planului de management și vizează finanțarea a trei proiecte aflate în desfășurare sau în planificare în cadrul CERT-RO. Dată fiind importanța unui proces de finanțare corect și adecvat, restrângerea acestui obiectiv la stricta finanțare a unor proiecte este inoportună în condițiile în care analiza instituțională a determinat următoarele:

- Nivel suboptim al investițiilor;
- Personal insuficient;
- Dotări tehnice și materiale / spațiu de lucru inadecvate.

Din aceste motive, considerăm oportună o abordare strategică a proceselor financiare din instituție, în locul abordării actuale punctuale pe obiective de investiție.

În final, **obiectivul general 5** (SCIM) este ultimul dintre obiectivele generale ale CERT-RO. Acest obiectiv are o formulare ambiguă, prin urmare recomandăm reformularea sa deoarece SCIM nu poate fi un obiectiv în sine, ci realizarea unei anumite activități sau atingerea unei anumite stări vis-a-vis de Sistemul de Control Intern Managerial. Existența SCIM, și a unui sistem de management a calității sunt apreciate ca demersuri pozitive, cu toate că ambele sisteme sunt incomplete. Dezvoltarea și perfecționarea ambelor sisteme ar trebui continuată, tot la nivel strategic. Printre aspectele de îmbunătățit descoperite de analiza instituțională se numără:

- Neacoperirea completă a tuturor activităților prin proceduri de lucru;
- Necesitatea introducerii unui sistem de măsurare a performanței bazat pe indicatori cheie a performanței care să măsoare realizarea obiectivelor din punct de vedere cantitativ, calitativ, al impactului si al rezultatului;
- Intensificarea eforturilor de identificare/analiză/gestionare a riscurilor;

- Dezvoltarea sistemului informatic al instituției astfel încât să furnizeze managementului rapoarte suficiente pentru luarea deciziilor eficiente și în cel mai scurt timp posibil;
- Dezvoltarea sistemului informatic al instituției astfel încât să permită monitorizarea realizării obiectivelor și a activităților în funcție de criteriile de performanță stabilite.

În concluzie, se observă necesitatea unei **abordări integrate la nivelul tuturor proceselor din cadrul CERT-RO**, precum și **elaborarea de strategii în domeniile cheie ale activității instituției**.

4.1 Inventar de strategii și documente strategice identificate la nivelul CERT-RO

4.1.1 Instrumente care vin din afara instituției

Strategia Națională Anticorupție 2016-2020 (SNA), a fost aprobată prin HG nr. 583/2016, împreună cu seturile de indicatori de performanță, riscurile asociate obiectivelor și măsurilor din strategie și sursele de verificare, inventarul măsurilor de transparență instituțională și de prevenire a corupției, a indicatorilor de evaluare, precum și standardele de publicare a informațiilor de interes public. Strategia a fost elaborată având în vedere concluziile evaluării realizate de Ministerul Justiției cu privire la implementarea Strategiei Naționale Anticorupție 2012-2015, precum și concluziile și recomandările raportului de evaluare independentă a impactului SNA 2012-2015.

Planul Anual de Lucru al Guvernului (PALG) - Secretariatul General al Guvernului coordonează procesul de elaborare și monitorizare a Planului Anual de Lucru al Guvernului. PALG reprezintă un calendar al proiectelor de documente de politici publice și al proiectelor de acte normative (legi și hotărâri ale Guvernului) cu impact semnificativ asupra economiei, societății, mediului și bugetului general consolidat, care necesită aprobarea Guvernului pentru anul în curs. Introdus la nivelul administrației publice centrale în anul 2014, PALG reprezintă unul dintre punctele care fac obiectul raportărilor către Comisia Europeană.

Strategia de Consolidare a Administrației Publice 2014-2020 (SCAP) - Prin HG nr. 909/2014 a fost aprobată Strategia pentru consolidarea administrației publice 2014-2020 și constituirea Comitetului național pentru coordonarea implementării SCAP, ținta fiind ca până în 2020 România să aibă o administrație publică eficientă și receptivă la nevoile societății. Strategia este un document integrat care are în vedere trei elemente cheie: necesitatea remedierii unor deficiențe structurale în funcționarea administrației publice; recomandările specifice de țară formulate de Comisia Europeană pentru anii 2013 și 2014 cu privire la administrația publică; necesitatea asigurării/pregătirii administrației publice pentru a îndeplini obligațiile asumate la nivel european în ceea ce privește o serie de ținte/obiective stabilite prin Strategia Europa 2020, Strategia pentru o reglementare mai bună.

Strategia privind mai Buna Reglementare 2014-2020 (SPBR) - Planul de acțiuni pentru implementarea SCAP a fost modificat și actualizat prin HG nr. 462/2017 – pentru modificarea anexei nr. 2 la HG nr. 909/2014 privind aprobarea Strategiei pentru consolidarea administrației publice 2014-2020 și constituirea Comitetului Național pentru Coordonarea Implementării Strategiei pentru Consolidarea Administrației Publice 2014-2020 și **pentru modificarea anexei la HG nr. 1076/2014 pentru aprobarea Strategiei privind mai buna reglementare 2014-2020**. SPBR își propune continuarea procesului de reducere a sarcinilor administrative prin simplificarea legislației aferente ultimelor domenii a căror măsurare s-a finalizat în 2014 prin utilizarea SCM: muncă (forță de muncă, legislația muncii, pensii și asigurări sociale, securitate și sănătate în muncă), sănătate (farma, autorizare și inspecție sanitară), educație, mediu (schimbări climatice, silvicultură) și justiție (registrul comerțului, profesii liberale).

Planul de acțiuni pentru implementarea etapizată a managementului calității în autorități și instituții publice 2016-2020 (PAIEMCAIP), răspunde subcriteriului condiționalității ex-ante prin care se solicită „Existența unui set de acțiuni care se referă la stabilirea sau utilizarea sistemelor de management al calității, deja stabilite, într-un mod durabil". Planul de acțiuni pentru implementarea etapizată a managementului calității se axează pe ideea de asumare a utilizării managementului calității la nivelul administrației publice centrale. În cadrul acestui plan Ministerul Justiției, Oficiul Național Registrul Comerțului (ONRC), ANP au atribuții privind menținerea/implementarea sistemului de management al calității.

Planul integrat pentru simplificarea procedurilor administrative aplicabile cetățenilor (PAISPAAC) a fost elaborat în contextul îndeplinirii, pentru segmentul cetățeni, a criteriului „Acțiuni integrate de simplificare și raționalizare a procedurilor administrative" al condiționalității ex-ante, subcriteriul „Existența unor acțiuni integrate de simplificare și raționalizare a procedurilor administrative, inclusiv soluții de e-guvernare" și contribuie la atingerea obiectivelor asumate prin Strategia pentru Consolidarea Administrației Publice 2014-2020 (SCAP 2014-2020). Pornind de la concluziile Analizei nevoilor și obiectivelor de simplificare și raționalizare a procedurilor administrative pentru cetățeni au fost identificate opt domenii de intervenție în vederea simplificării procedurilor administrative pentru cetățeni. Un domeniu îl reprezintă obținerea cetățeniei.

Strategia Națională privind Agenda Digitală pentru România 2020 (SNADR) aprobată prin HG nr. 245/2015. SNADR a fost dezvoltată pe baza programului Agenda Digitală pentru Europa 2020, aceasta fiind cadru de referință pentru dezvoltarea economiei digitale 2014 - 2020. Dintre cele 36 de evenimente de viață, 6 sunt în responsabilitatea ONRC.

4.1.2 Instrumente elaborate la nivelul CERT-RO

În cadrul CERT-RO, planificarea trebuie să se desfășoare urmând două direcții majore:

- Direcție strategică;
- Direcții operaționale.

Direcția strategică trebuie să derive din documente strategice aplicabile direct entității, care să urmărească o strategie de dezvoltare cu planuri de acțiune. Direcțiile operaționale CERT-RO urmăresc planificarea care derivă din următoarele instrumente, având la bază norme imperative sau inițiativele instituției:

- Planul anual de achiziții publice;
- Planul de integritate, elaborat în conformitate cu Strategia Națională Anticorupție 2016-2020, aprobată prin HG nr. 583/2016;
- Planul de asigurare a continuității și proceduri operaționale și de sistem, conform prevederilor OSGG nr. 600/2018;
- Planul de implementare a măsurilor de control pentru riscurile asociate funcțiilor sensibile – actualizare anuală;
- Programul de dezvoltare, conform OSGG nr. 600/2018;
- Planuri de implementare a proiectelor cu finanțare externă;

- Proceduri operaţionale şi de sistem;
- Codul de etică.

4.2 Analiza documentelor strategice identificate la nivelul CERT-RO

Aşa cum am precizat încă din secţiunile introductive, pentru evaluarea implementării instrumentelor de management strategic în cadrul CERT-RO s-a recurs la distribuirea unui sondaj electronic - chestionar completat de 9 angajați (a se vedea Anexa 6.3). Interpretarea răspunsurilor s-a făcut prin analizarea cu ajutorul instrumentarului statistic de bază, incluzând printre altele analize de corelare a informaţiilor oferite de către respondenţii selectaţi.

În ceea ce privește procedurile de elaborare a documentelor de planificare strategică, analiza procesului se concentrează pe următoarele paliere:

- Fundamentare, acoperită de de întrebările 6 și 14;
- Elaborarea propriu-zisă, acoperită de de întrebările 7 și 14;
- Implementare, acoperită de de întrebările 8 și 15;
- Monitorizarea și evaluarea, fiind acoperite de întrebările 9, 10 și 16.

Menţionăm de asemenea, că aceste paliere îşi regăsesc dimensiunile specifice şi în alte aprecieri ale respondenților pe baza întrebărilor 5, 11, 13, 17, 18 şi 27. Totodată, analiza realizată cuprinde în ansamblu, evaluarea progresului înregistrat de către CERT-RO cu privire la **instrumentele sistematice privind implementarea unui management strategic eficient şi responsabil care să conducă la îndeplinirea obiectivelor specifice şi generale.**

Înainte de a evalua propriu-zis modul de fundamentare a documentelor strategice, apreciem importanța acesteia în corelație cu celelalte paliere amintite sus. Mai mult, în figura de mai jos (figura 1), observăm un grad mare de colaborare între structuri, respectiv diferite componente ale sistemului implicate în cadrul proceselor de elaborare/ implementare/ monitorizare/ evaluare a unor documente de planificare strategică.

FEIM: fundamentare, elaborare, implementare, monitorizare, evaluare

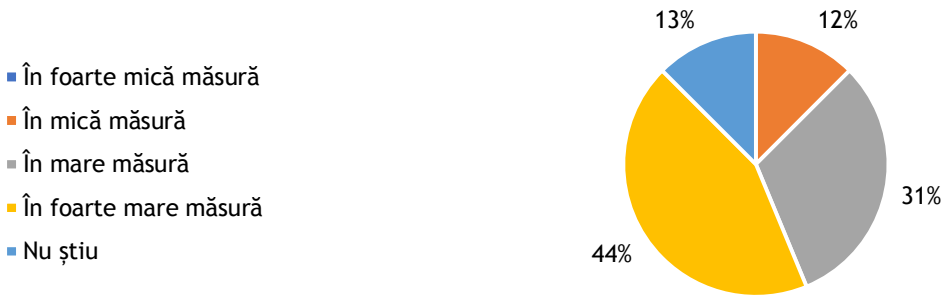

Figura 1: Funcționalitatea instrumentelor strategice prin colaborarea structurilor din cadrul CERT-RO

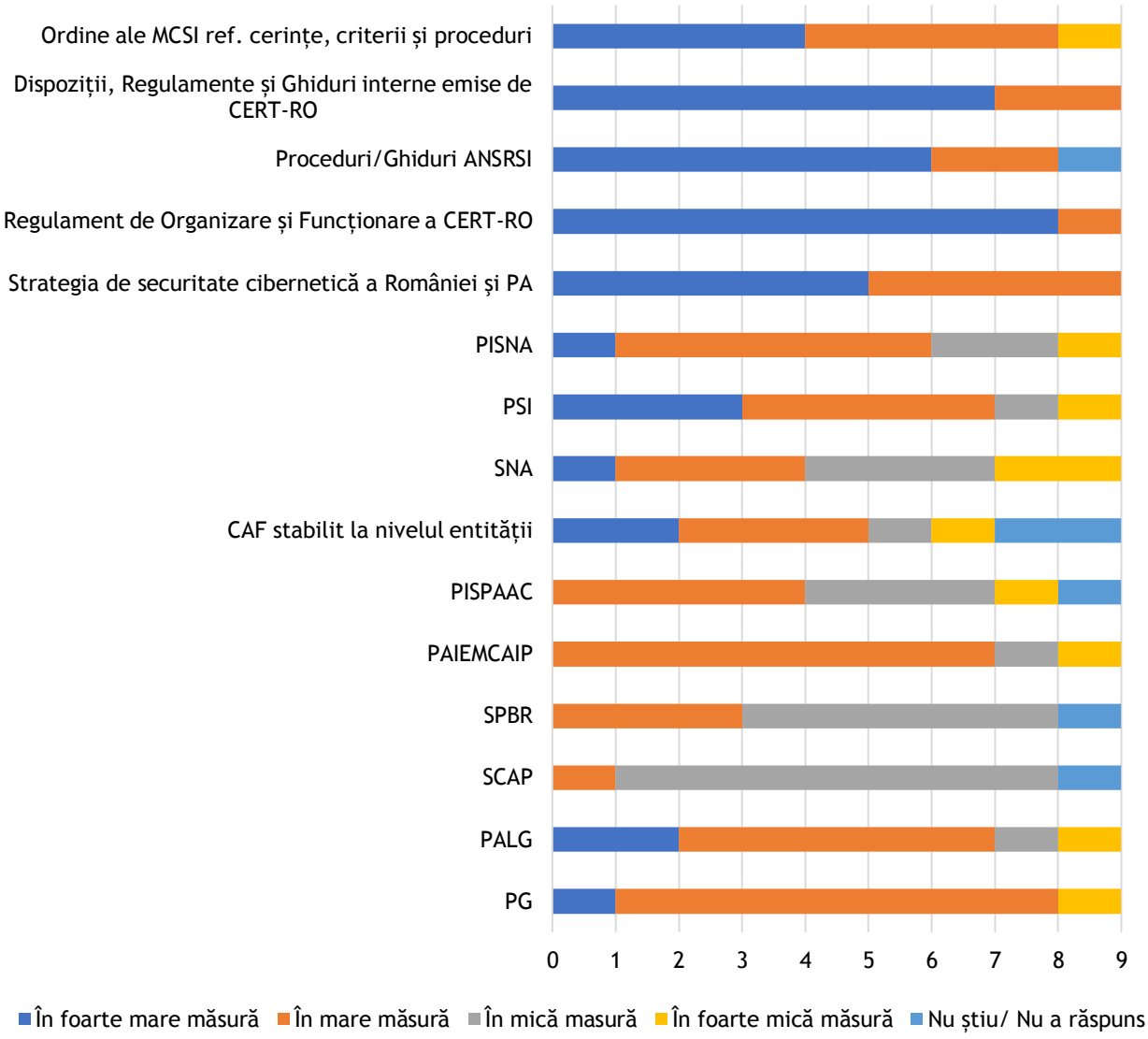

Figura 2: Influența instrumentelor strategice în cadrul CERT-RO în stabilirea obiectivelor, acțiunilor și responsabilităților

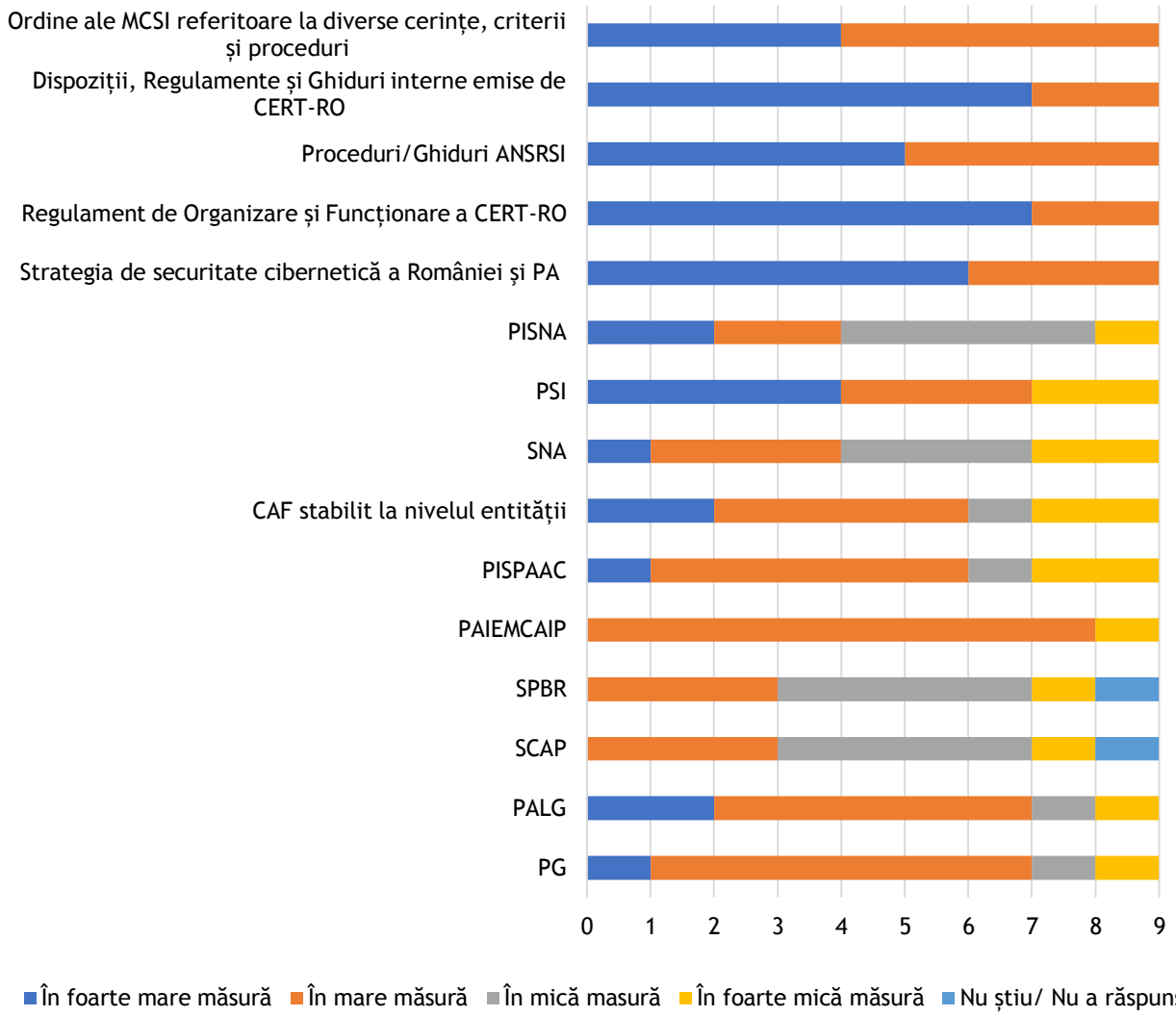

Figura 3: Utilitatea instrumentelor strategice pentru misiunea CERT-RO

Având în vedere răspunsurile transpuse în primele reprezentări grafice, prin aplicarea și evaluarea chestionarelor corelate cu interviurile și focus grupurile realizate cu factorii decidenți și responsabilii, observăm în cadrul CERT-RO, rolul major al documentelor strategice cum sunt **cele de importanță strategică națională** (Planul Anual de Lucru al Guvernului (PALG), Programul de Guvernare (PG), Strategia de Consolidare a Administrației Publice 2014-2020 (SCAP), Planul de acțiuni pentru implementarea etapizată a managementului calității în autorități si instituții publice 2016-2020 (PAIEMCAIP), Strategia Națională Anticorupție 2016-2020 (SNA)), precum și **documentele strategice interne** (Strategia de securitate cibernetică a României și Planul de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, Dispoziții, Regulamente și Ghiduri interne emise de CERT-RO, și altele precum Strategia de securitate cibernetică a UE, Directiva 2016/1148 privind NIS).

4.2.1 Fundamentarea documentelor strategice

Analiza modului de fundamentare a documentelor strategice a avut în vedere următoarele aspecte:

- Modul de identificare și colectare a nevoilor pe baza cărora au fost fundamentate documentele strategice, inclusiv metode de fundamentare și analiză folosite;
- Raportarea la alte documente (strategice) de nivel superior (ex. Program de guvernare, recomandări ale Comisiei Europene etc.);
- Modul de consultare cu părțile interesate și măsura în care propunerile acestora se regăsesc în documentele strategice.

Așa cum am observat și în partea introductivă a acestei analize asupra documentelor strategice, Întrebările 1 (Care dintre următoarele stabilesc pentru instituția dumneavoastră obiective, acțiuni și responsabilități?) și 2 (Cât de utile considerați că sunt aceste instrumente pentru misiunea instituției dumneavoastră?) pot fi analizate împreună. Astfel, din analizele vizuale și numerice a rezultatelor reiese faptul că misiunea, obiectivele, acțiunile și responsabilitățile sunt influențate mai puternic de factori interni, cum ar fi regulamentul de organizare și funcționare decât de factori externi, cum ar fi programul de guvernare sau diverse Ordine MCSI.

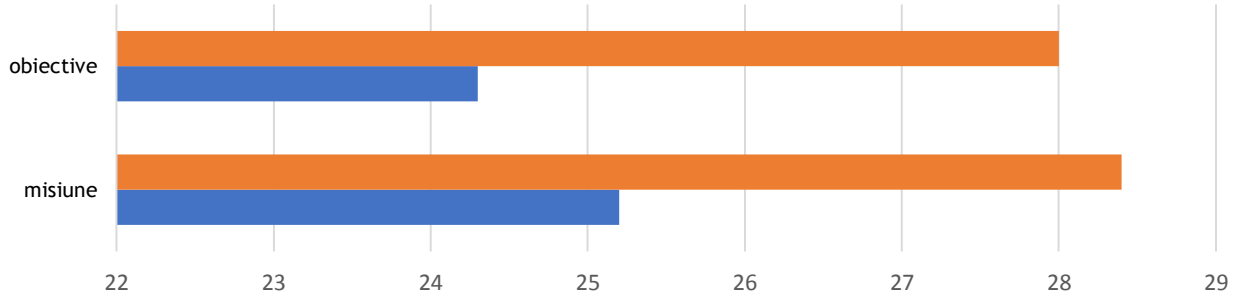

Figura 4: Importanța factorilor interni/externi asupra misiunii și obiectivelor CERT-RO

Figura 4 a fost creată în urma utilizării unei analize a mediilor ponderate, și reliefează influența mai puternică a factorilor interni aspra misiunii și obiectivelor instituției, decât a celor externi. Trebuie menționat aici faptul că, au fost luați în considerare de două ori mai mulți factori externi decât interni.

În procesul de fundamentare a documentelor strategice se acordă o importanță deosebită procesului de consultare a părților interesate, în speță partenerilor instituționali prin utilizarea unor proceduri specifice de lucru și se realizează corelarea cu alte documente strategice de nivel superior.

La nivelul CERT-RO modul în care factorii externi interacționează cu acest proces este determinat de relațiile dintre instituție și aceștia. Astfel, din răspunsurile oferite, se pot determina cu ușurință rolurile pe care părțile interesate le au în cadrul CERT-RO. Astfel, în procesul de fundamentare a documentelor strategice au fost identificate următoarele părți interesate (stakeholderi):

- Alte instituţii publice;
- Alte instituţii publice şi corelare cu documentele strategice;
- Mediul de afaceri;
- Mediul academic;
- Societatea civilă.

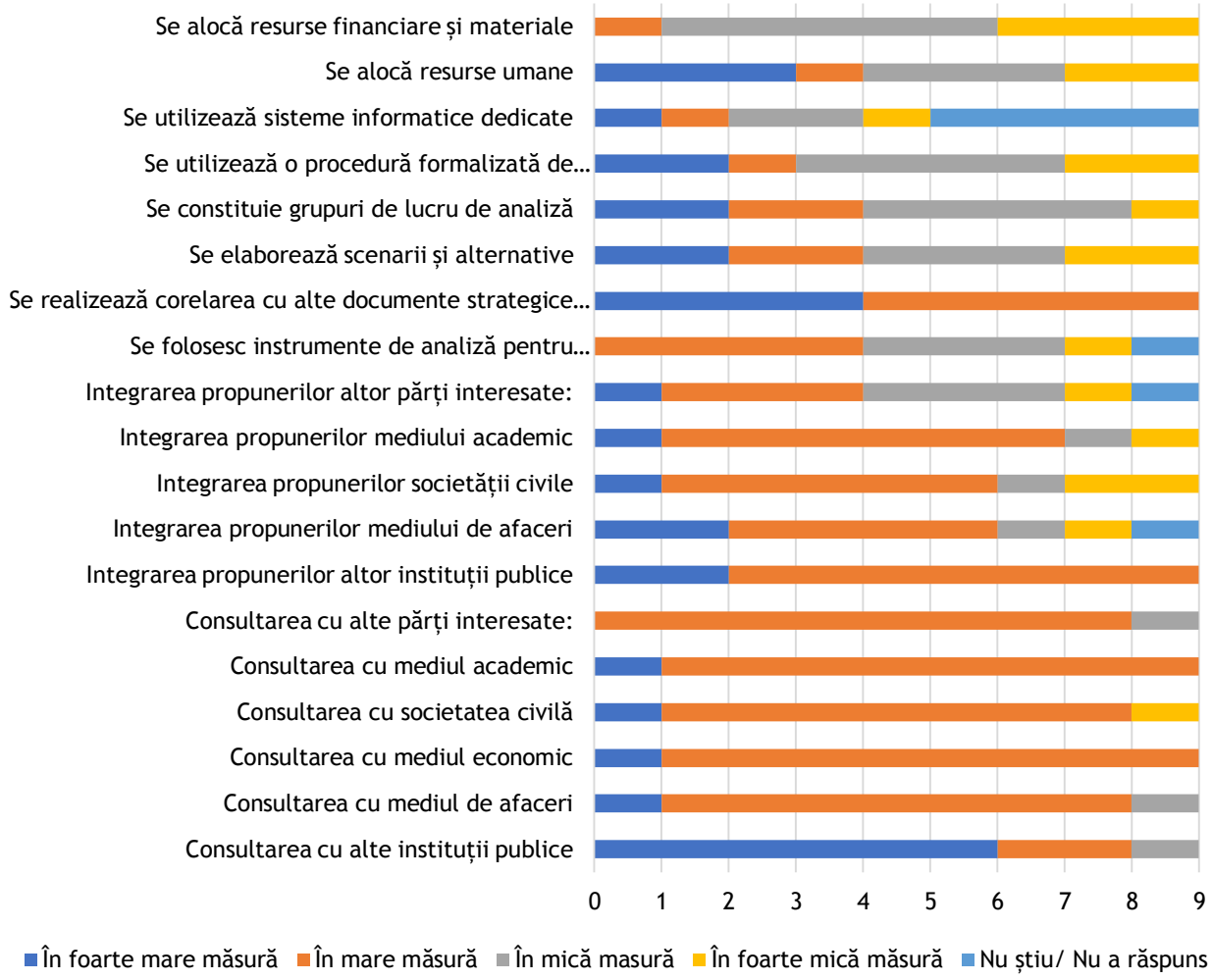

Figura 5: Procesul de fundamentare a elaborării documentelor de planificare strategică

Fundamentarea elaborării documentelor de planificare strategică este un proces complex, care influenţează în mod direct calitatea acestora, precum şi eficacitatea lor. Pentru mai multe detalii am prezentat mai sus şi imaginea de ansamblu în urma evaluărilor realizate pe baza aprecierii respondenţilor cu privire la acest proces de fundamentare a documentelor strategice din cadrul CERT-RO, întărit şi de o colaborare instituţională adecvată, aşa cum se vede în figura următoare.

Figura 6: Colaborare instituțională adecvată

4.2.2 Elaborarea documentelor strategice

Analiza privind elaborarea/formularea documentelor strategice a avut în vedere următoarele aspecte:

- Inițiatorul elaborării documentelor strategice și elementul generator al deciziei de elaborare;
- Conținutul documentelor;
- Pre-condițiile pe baza cărora sunt dezvoltate obiectivele sunt prevăzute în documente;
- Identificarea riscurilor și a strategiei pentru reducerea impactului riscurilor asupra rezultatelor;
- Formularea măsurilor a ținut cont de specificul organizației și de capacitatea de implementare a acesteia;
- Modul de adoptare/aprobare a documentelor strategice.

Documentele programatice au un **rol important în îndeplinirea misiunii CERT-RO**, fiind apreciate cu relevanță deosebită Strategia de securitate cibernetică a României şi Planul de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, Planul strategic instituțional, Programul de Guvernare, Planul Anual de Lucru al Guvernului, Strategia pentru Consolidarea Administrației Publice 2014-2020. Din prelucrarea chestionarelor, observăm că factorul principal în elaborarea documentelor strategice este tocmai nivelul superior şi obligațiile stabilite de acesta prin documente.

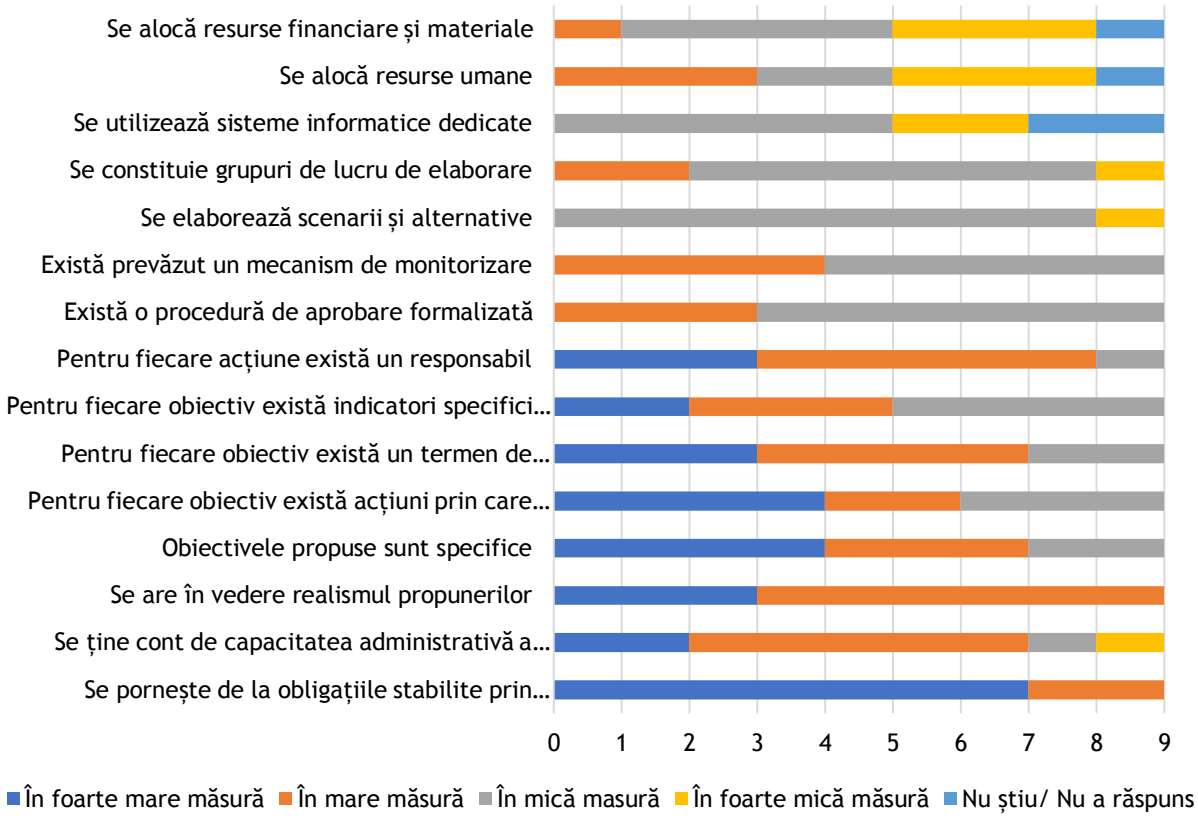

Figura 7: Aprecieri privind elaborarea documentelor strategice

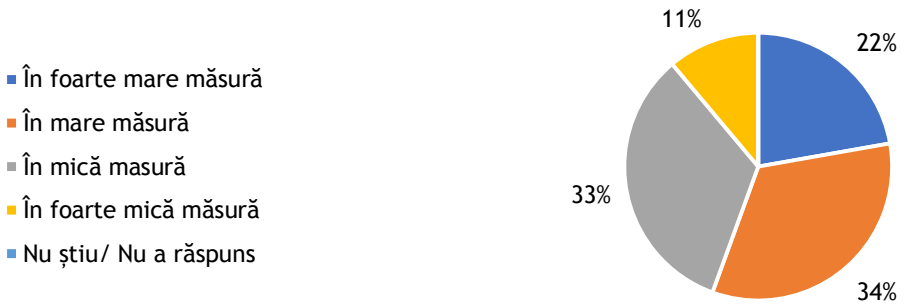

Figura 8: Colaborare internă adecvată

Din analiza activității de elaborare a documentelor strategice, la nivelul CERT-RO au fost identificate următoarele caracteristici ale acestei etape:

- normele imperative cuprinse în **documentele juridice de nivel superior** determină elaborarea altor documente la nivelul CERT-RO, care sunt aprobate prin respectarea unei **proceduri formalizate**, sub formă de acte juridice (decizii, hotărâre, ordin etc.);

- activitatea grupurilor de lucru este una riguroasă, în analizele elaborate fiind utilizate **tehnici și instrumente specifice de management**, observându-se și o colaborare internă adecvată (figura 8);
- procesul de elaborare se sprijină pe **o alocare adecvată de resurse umane și informatice**;
- documentele strategice elaborate cuprind obiective formalizate în sisteme categoriale ce vizează în general, toate nivelurile decizionale (nu în totalitate formalizate la nivelul posturilor), dar fără identificarea riscurilor și a activităților **legate de raportările monitorizării şi evaluării.**

4.2.3 Implementarea documentelor strategice

Analiza privind faza de implementare a documentelor strategice a avut în vedere următoarele aspecte:

- Definirea responsabilităților la nivelul intern al fiecărei instituții, al alocării resurselor prevăzute;
- Metode/modalități de implementare/asigurare a implementării măsurilor prevăzute în documentele strategice;
- Gradul în care implementarea strategiei a fost integrată în activitatea curentă a instituțiilor sau a reprezentat o activitate cu caracter excepțional.

Procesul de implementare a documentelor programatice de importanță națională, precum și a documentelor programatice stabilite la nivelul CERT-RO, are în vedere următoarele caracteristici (detaliate în reprezentările grafice ulterioare):

- etapa este una funcțională, integrată în activitatea curentă a instituției, programată cu ajutorul calendarelor de implementare, procedurată și însoțită de circuitele distincte ale documentelor;
- se elaborează planuri de implementare, fiind constituite de altfel şi grupuri de lucru;
- **reorganizarea structurală și procesuală a activității** a generat şi limitări în utilizarea unor sisteme informatice dedicate;
- în procesul de implementare este antrenat tot personalul CERT-RO, iar **responsabilitatea atingerii obiectivelor aparține întregului personal, nu doar managerilor sau celor ce au formulat obiectivele.**

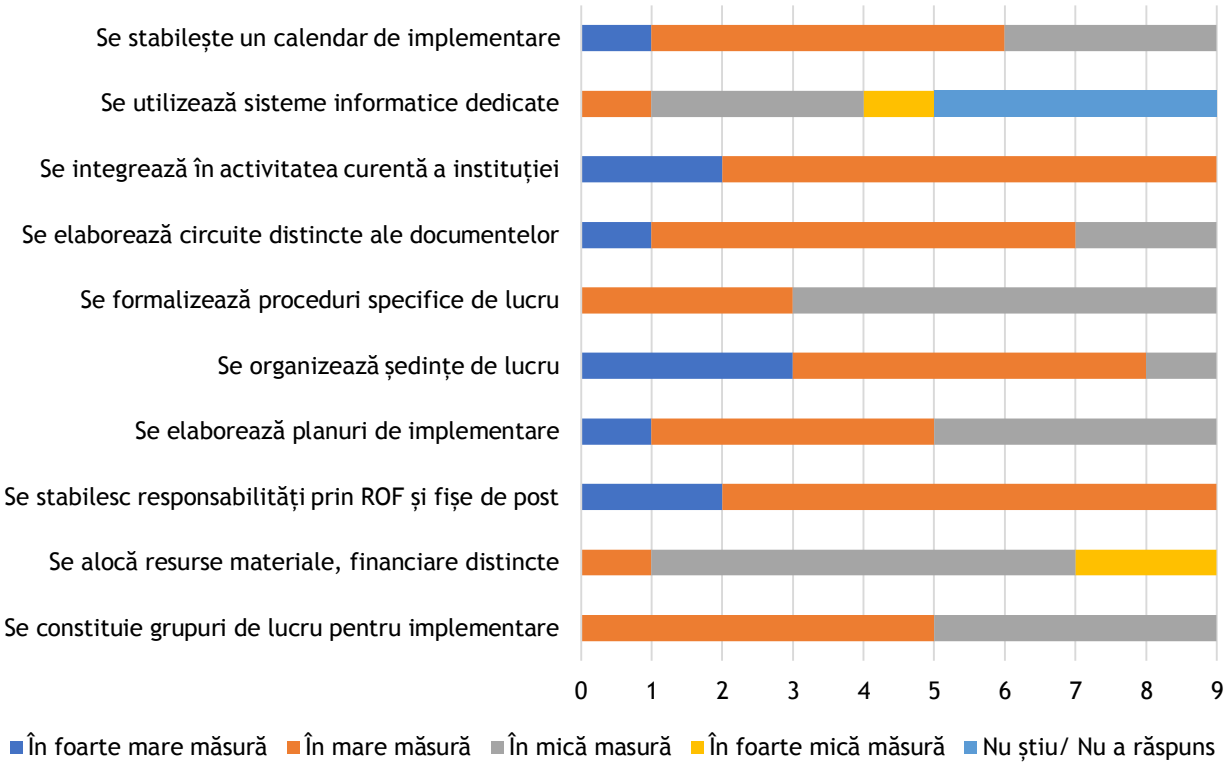

Figura 9: Implementarea documentelor strategice

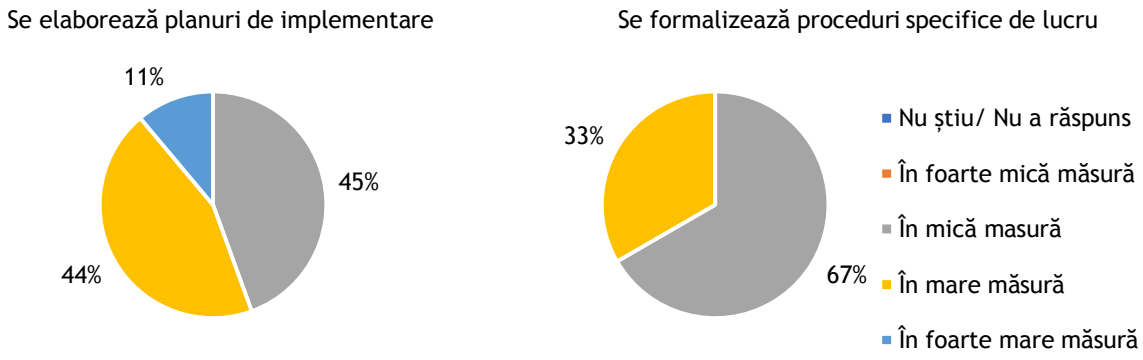

Figura 10: Elaborarea unor planuri de implementare, însă fără formalizarea unor proceduri de lucru

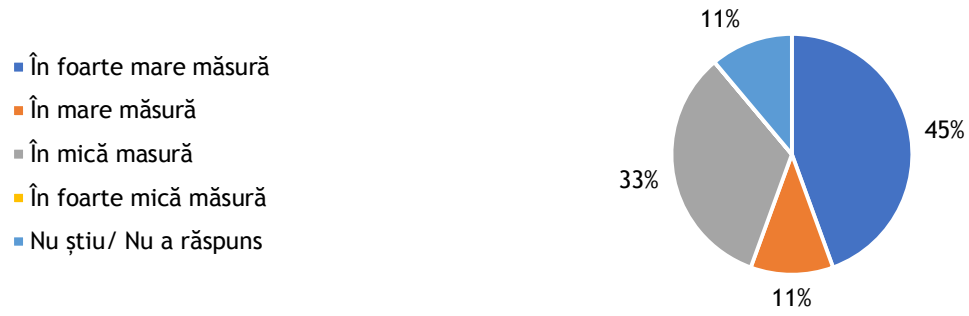

Figura 11: Utilitatea grupurilor de lucru

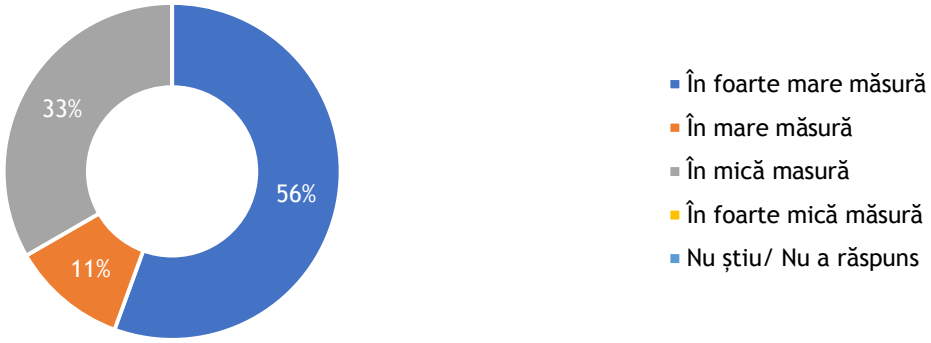

Figura 12: Cunoașterea obiectivelor la nivelul fiecărui angajat

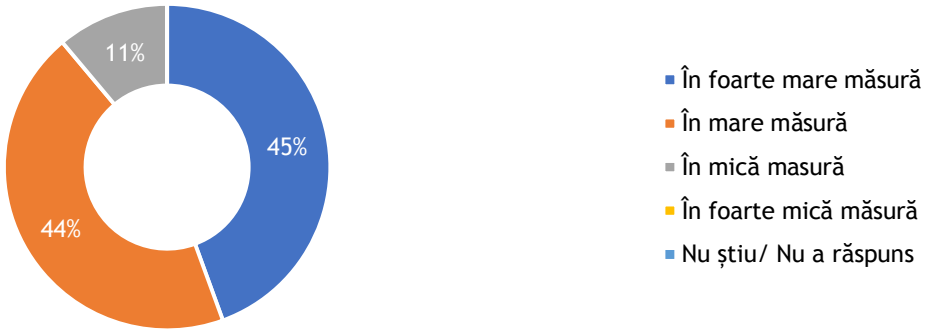

Figura 13: Corelarea activitățile curente ale angajaților cu obiectivele strategice ale instituției

De asemenea, respondenții apreciază că **principalele obstacole în procesul de implementare** a documentelor de planificare strategică de la nivelul CERT-RO, sunt: resursele financiare insuficiente, numărul redus de angajați, baze de date și sisteme informatice neadecvate sau inexistente, numărul mic de analize de impact existente, dinamica modificării programelor de guvernare (figura 14).

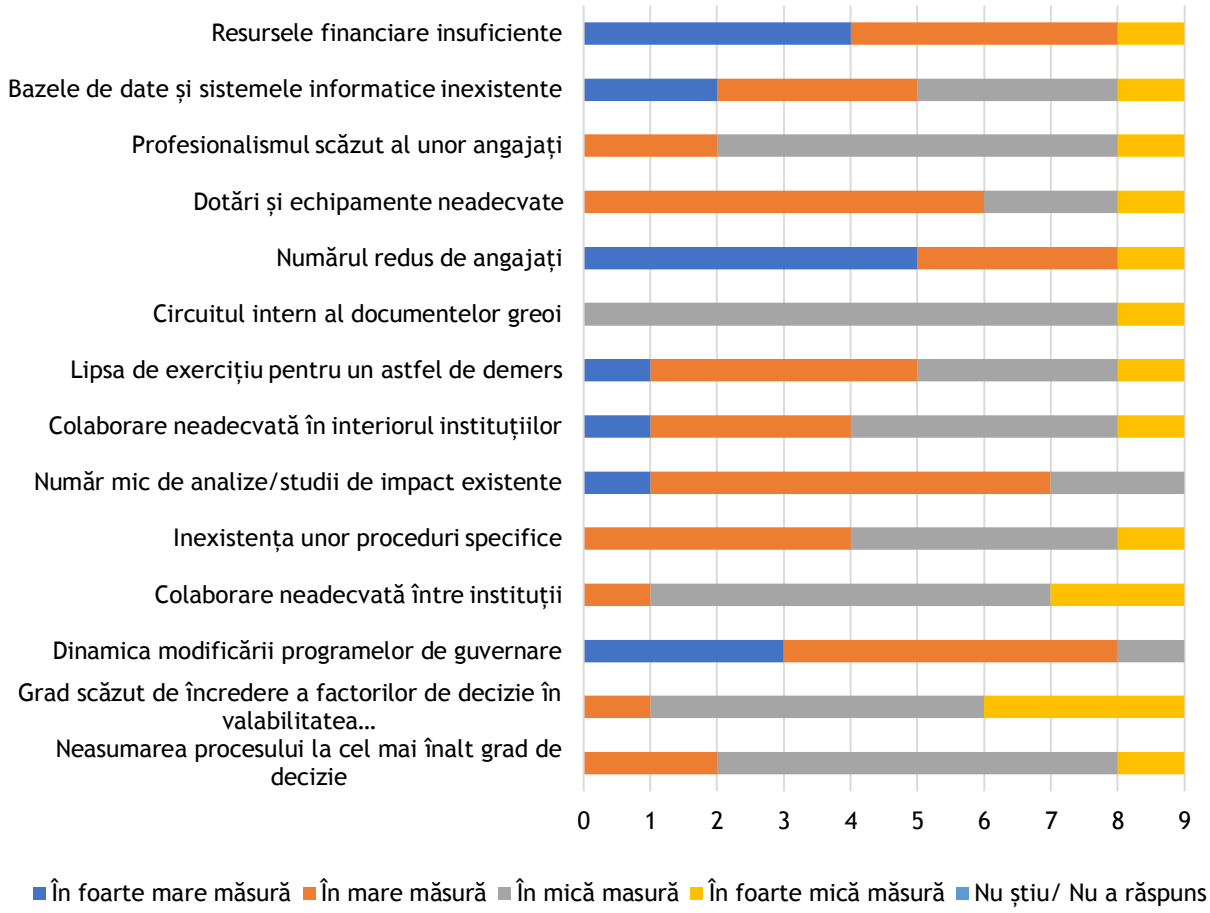

Figura 14: Obstacole în procesul de implementare a documentelor de planificare strategică în perioada 2014-2019

4.2.4 Monitorizarea și revizuirea documentelor strategice

Pentru monitorizarea și revizuirea documentelor strategice au fost analizate următoarele aspecte:

- Au fost definite/stabilite mecanisme de monitorizare;
- Existența revizuirilor, modul de fundamentare și adoptare a documentelor strategice revizuite;
- Implicarea factorilor interesați pentru asigurarea calității rezultatelor și capacitatea/instrumentele de autoevaluare utilizate.

În ceea ce privește procesul de monitorizare și revizuire a documentelor strategice au fost avute în vedere următoarele aspecte:

- activitatea de monitorizare și revizuire a documentelor de planificare strategică de la nivelul CERT-RO este realizată cu ajutorul grupurilor de lucru care organizează frecvent și ședințe de monitorizare;

- implicarea într-o măsură mai mică a factorilor interesați pentru asigurarea calității rezultatelor precum și capacitatea și instrumentele de autoevaluare utilizate;
- din perspectiva modului de organizare, responsabilitățile ce decurg din desfășurarea acestei activități sunt transpuse în Regulamentul de Organizare și funcționare, dar și la nivel de posturi;
- prin reprezentarea elementelor primordiale în procesul de monitorizare şi revizuire a documentelor strategice nu se regăsește elaborarea unor planuri și calendare de raportare, iar acestea nu sunt însoțite de proceduri și sisteme informatice dedicate, care să fie măsurate periodic (figura 15).

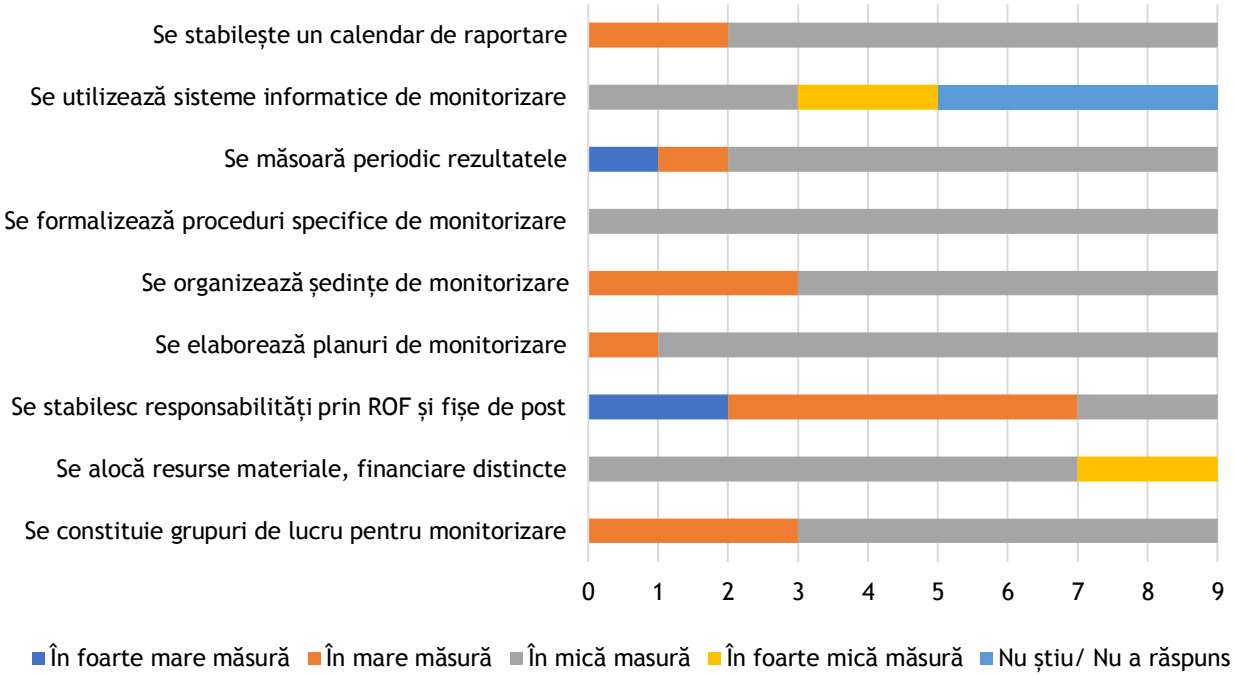

Figura 15: Elementele definitorii pentru monitorizarea și revizuirea documentelor de planificare strategică

Prelucrarea chestionarelor aplicate și a interviului realizat pe baza aspectelor evaluate şi incluse cuprins în fișa de analiză organizațională (Anexa 6.1) relevă faptul că activitatea de la nivelul CERT-RO este eficentă datorită stabilirii responsabilităților prin ROF şi fișe de post, așa cum evidențiază respondenții și influențează modul de asumare în vederea atingerii obiectivelor de către întregul personal.

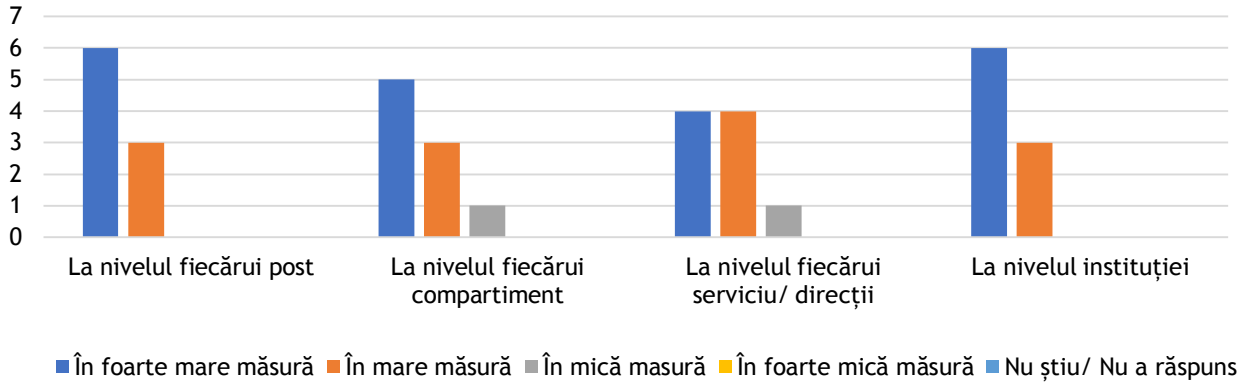

Figura 16: Existența unui set de obiective asumate, formalizate în diferite documente, pentru fiecare nivel decizional

Observăm că, respondenții evidențiază aceleași **obstacole în procesul de monitorizare/ evaluare** a documentelor de planificare strategică de la nivelul CERT-RO, așa cum au fost prezentate și în etapa de implementare (figura 17) - resursa umană insuficientă și numărul scăzut de analize/studii de impact. Astfel, așa cum am dezvoltat și în secțiunile anterioare, observăm și aici lipsa resurselor materiale și financiare. Procesul de evaluare nu este planificat, sau formalizat.

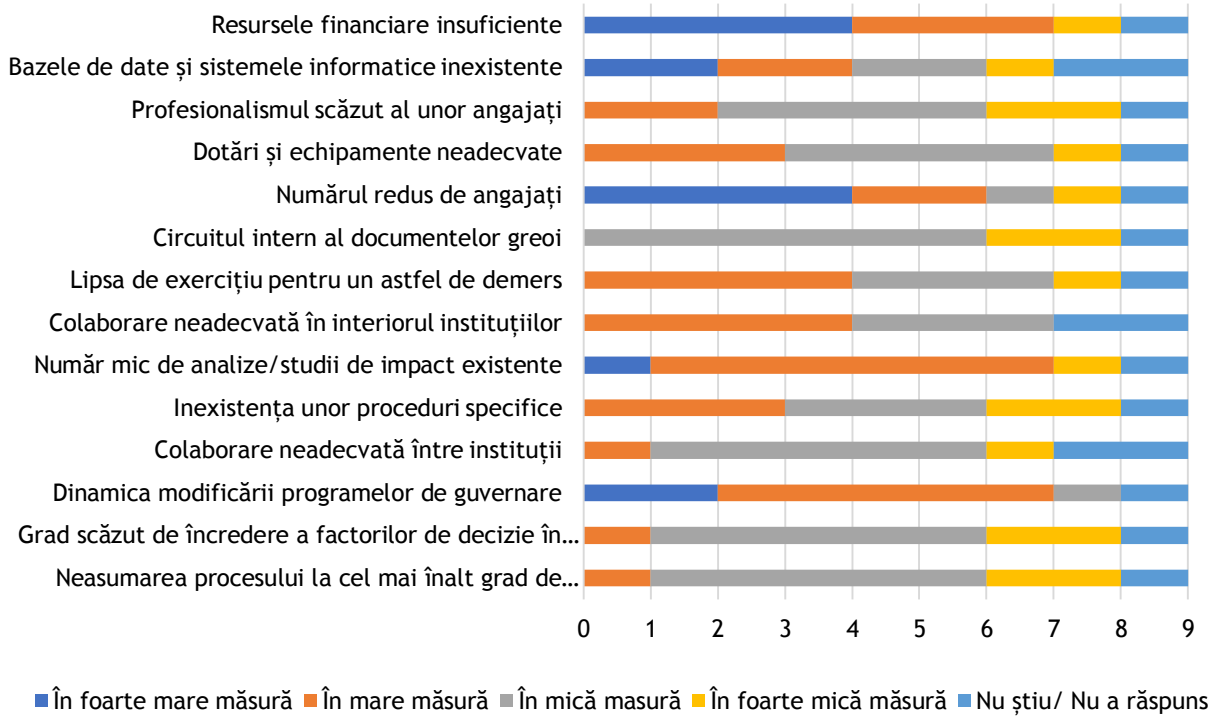

Figura 17: Obstacole în procesul de monitorizare/evaluare a documentelor de planificare strategică în perioada 2014-2019

4.2.5 Evaluarea documentelor strategice

Pentru analiza privind evaluarea documentelor strategice au fost luate în considerare următoarele aspecte:

- Existența evaluărilor intermediare ale documentelor strategice, modul de realizare (intern/extern), metode de evaluare folosite, responsabili, efectele/acțiunile realizate în urma evaluărilor;
- Existența evaluărilor post implementare, modul lor de realizare (intern/extern), metode de evaluare folosite, responsabili, utilizarea concluziilor evaluării;
- Rolul compartimentelor din fiecare instituție în procesul de fundamentare/ elaborare/ adoptare a documentelor strategice menționate, probleme constatate.

Succesul realizării şi implementării documentelor strategice se măsoară prin intermediul indicatorilor de performanţă, **evaluându-se gradul de atingere a obiectivelor propuse**. Indicatorii de performanţă se formulează pentru fiecare obiectiv strategic, pentru perioada de acţiune a strategiei, cu accent pe toate elementele strategiei, inclusiv aspecte financiare şi organizaționale.

Activitatea de evaluare a documentelor de planificare strategică de la nivelul CERT-RO este apreciată ca fiind funcţională într-o măsură mai mică (figura 18). **Aceste considerente pot influenţa negativ atingerea obiectivelor sau pot genera riscuri privind termenele de finalizare.**

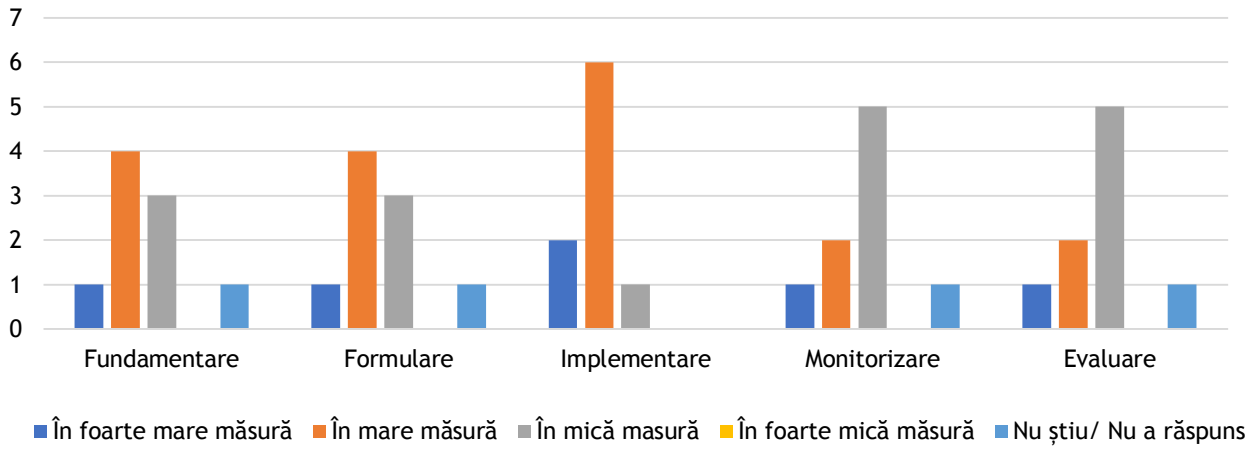

Figura 18: Aprecieri privind evaluarea documentelor de planificare strategică în perioada 2014-2019. Funcționalitatea procesului de evaluare

Din perspectiva respondenților la chestionar (Figura 19), principalele riscuri privind procesul de elaborare/ implementare/ monitorizare/ evaluare a documentelor de planificare strategică de la nivelul IGSU în perioada 2019 – 2020, sunt resursele insuficiente (umane și financiare), instrumentele IT necorelate și managementul relațiilor interne, dar și interguvernamentale, influențate și de instabilitatea legislativă.

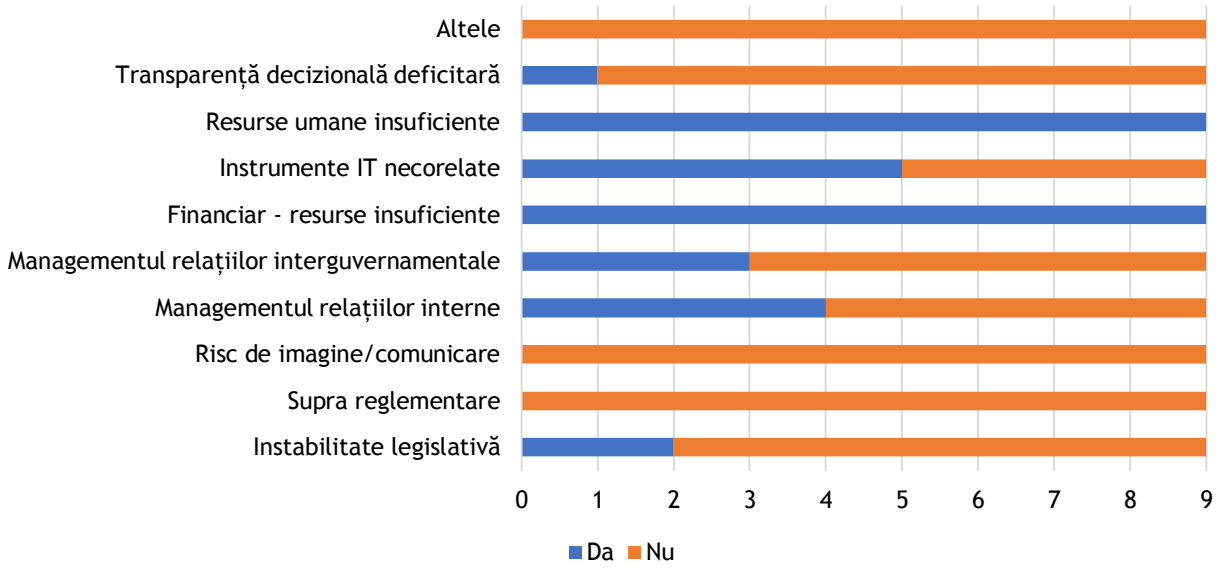

Figura 19: Existența unui set de obiective asumate, formalizate în diferite documente, pentru fiecare nivel decizional

Pentru întârzierile sau amânările termenelor prevăzute în diferite documente de planificare strategică,(întrebarea 19) respondenții au identificat următoarele cauze:

- Lipsa deprinderilor personalului în ceea ce privește lucrul în echipă;
- Lipsa unui proces detaliat de luare a deciziilor;
- Slaba coordonare dintre departamente și;
- Blocajele birocratice.

Răspunsurile sunt în concordanță cu analiza instituțională, unde sunt menționate mai multe din aspectele identificate în chestionar. Cu toate acestea, respondenții indică în unanimitate responsabilitatea întregului personal pentru atingerea obiectivelor instituției (întrebarea 20).

Deși analiza, în linii generale, arată existența răspunderii în rândul întregului personal, cauzele întârzierilor identificate mai sus indică existența unei probleme mult mai complexă, și anume importanța inventarierii obiectivelor și identificarea cauzelor neatingerii lor, acolo unde este cazul. Mai mult, este recomandat să se observe manifestarea directă a managementului participativ și să se desemneze responsabilități pentru luarea deciziilor și răspundere pentru procese/activități direct proprietarilor de procese/șefilor de activități.

În continuare au fost identificate următoarele variante a documentelor de planificare strategică viitoare (întrebarea 24):

- Finalizarea implementării Legii nr. 362/2018, respectiv adoptarea legislației secundare în sensul în care este stabilită prin dispozițiile actului normativ menționat anterior;
- Obținerea alocațiilor bugetare pentru asigurarea disponibilității resurselor necesare finalizării demersului precizat anterior;
- Implementarea standardelor ISO din familiile 27000, 14000, 17025;
- Dezvoltarea relațiilor de cooperare cu mediul universitar, academic al cercetării-dezvoltării și inovării;
- Actualizarea strategiei de securitate cibernetică națională;
- Recrutarea de personal;
- Adaptarea instituției la dinamica evoluțiilor internaționale;
- Eficientizarea actului de conducere, și;
- Fluidizarea fluxurilor relaționale interne.

Pentru realizarea acestor puncte sunt propuse următoarele acțiuni (întrebarea 25):

- Realizarea planului strategic al instituției pornind de la strategia de securitate cibernetică a UE pentru perioada 2021-2027, de la strategia națională de securitate cibernetică, directivele UE în domeniu mai ales în domeniul NIS și armonizarea acestor documente cu obiectivele stabilite CERT-RO prin legislația națională care îi reglementează domeniul de activitate;
- Asigurarea bugetului prin planuri/programe bugetare multianuale;
- Corelarea procesului de planificare intern cu planificarea de la nivel UE, respectiv pe 7 ani;
- Introducerea în planul cu principalele activități al instituției a costurilor necesare îndeplinirii fiecărei acțiuni/măsuri în concordanță cu bugetul alocat;
- Corelarea planului anual de achiziții publice cu ciclul de planificare bugetară multianuală și obiectivele cuprinse în planul cu principalele activități;
- Acțiuni de implementare/monitorizare/evaluare/documentare;
- Implicarea mai profundă a zonei tehnice în procesul de fundamentare a obiectivelor strategice ale organizației;
- Stabilirea unor etape clare de îndeplinire a obiectivelor propuse;
- Organizarea unor evaluări de etapă pentru inducerea corecțiilor necesare obiectivelor stabilite;
- Transmiterea periodică a feedback-ului către personalul de execuție.

5 Concluzii și recomandări

Fluxurile informaţionale au la bază informaţii strategice şi operative cu rol de a asigura conexiunea informaţională dintre sistemul decizional (de conducere) şi cel operaţional (de execuţie). La nivelul Centrului Național de Răspuns la Incidente de Securitate Cibernetică procesul de management strategic se desfășoară în parametri de funcționalitate optimă fiind fundamentat pe o colaborare strânsă a diferitelor componente implicate în acest proces.

Corelând analiza documentației cu evaluarea fluxurilor informaționale existente la nivelul Centrului Național de Răspuns la Incidente de Securitate Cibernetică, prin raportare la procese, proceduri şi resurse implicate, concluzionăm astfel:

- apreciem existența unei implicări organizaționale eficiente, însă prin analiza proceselor operaționale și de decizie, precum și a fluxurilor informaționale au fost identificate și o serie de puncte de îmbunătățire, așa cum au fost ele prezentate detaliat în secțiunea de analiză;
- analiza diagnostic relevă un set de riscuri cu care se confruntă CERT-RO în procesul de planificare strategică asociate instrumentelor strategice, managementului resurselor umane, lipsei resurselor umane și a resurselor financiare, precum și aspectele de îmbunătățit în ceea ce privește documentele strategice operaționale și de decizie;
- se observă posibilitatea de îmbunătățire a procesului de fundamentare prin implicarea unor specialişti pe domenii de lucru în cazul fundamentării documentelor strategice;
- raţionalizarea fluxurilor informaţionale cu implicări pe toate componentele devine o necesitate prin care resursele, procesele, structurile şi procedurile au rol de suport în **consolidarea rolului de autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice.**
- se observă necesitatea unei **abordări integrate** la nivelul tuturor proceselor din cadrul CERT-RO, precum și la nivelul de elaborare a strategiilor în domeniile cheie ale activității instituției.

Direcțiile ulterioare de dezvoltare este recomandat să se focuseze pe domeniile de îmbunătățire reliefate de analiza diagnostic, în special în ceea ce privește elaborarea strategiilor care guvernează activitățile cheie ale CERT-RO și corelarea lor cu obiectivele și scopurile enunțate, dar și cu strategiile dezvoltate la nivel național și european. Aceste demersuri se pot concretiza prin:

- Elaborarea **strategiei pentru dezvoltarea resurselor umane** orientate spre formarea permanentă a personalului, motivarea personalului și acoperirea deficitului de personal;
- Implementarea unui **sistem de măsurare a performanțelor** bazat pe criterii de dezvoltare continuă a instituției și pe obiective clare, formulate la toate nivelurile ierarhice și măsurate prin indicatori cheie ai performanței;
- Elaborarea, revizuirea și implementarea unei **strategii de comunicare, marketing și promovare** a instituției;

- Atragerea de **surse de finanțare** pentru acoperirea necesarului de investiții din cadrul instituției;
- Dezvoltarea, extinderea și actualizarea continuă a **sistemului de proceduri** de lucru, în conformitate cu cerințele actuale dar și cu riscurile de natură cibernetică;
- Intensificarea utilizării instrumentelor de **management al riscurilor** pentru o mai bună adaptabilitate la survenirea evenimentelor negative;
- Formularea și implementarea unei **strategii de calitate** prin procese specifice managementului calității și sistemului de control intern managerial.

Toate aspectele enumerate mai sus se vor corela în toate privințele cu **strategia de dezvoltare** pe termen lung a instituției și vor deveni parte integrată a acesteia. De asemenea, strategia de dezvoltare trebuie corelată cu strategiile naționale și cu cerințele și standardele europene aplicabile, asigurându-se astfel bazele pentru dezvoltarea durabilă a CERT-RO în condiții de cooperare instituțională.

6 Anexe

6.1 Fișa de analiză organizațională CERT-RO

6.2 Minute ale întâlnirilor realizate prin intermediul platformei online Microsoft Teams

MINUTA ÎNTÂLNIRII pentru realizarea Sub-activității 6.1

Client:	Autoritatea pentru Digitalizarea României (ADR) și Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)		
Contract:	Contract de achiziție servicii nr. 24 din 15.04.2020	**Redactat de:**	Nume: Nesrin Regep Data: 11.05.2020
		Revizuit de:	Nume: Vlad Barbălată Data: 11.05.2020

Titlu proiect	**Sistem integrat de management pentru o societate informațională performantă (SIMSIP) cod SIPOCA 391**		
Subiect	**Întâlnire pentru realizarea Sub-activității 6.1**		
Data	11.05.2020	**Locație**	Microsoft Teams
Ora de începere	11h00	**Ora de încheiere**	12h00
Lista de prezență	-	**Prezentare PowerPoint**	-

Persoane prezente în cadrul întâlnirii
Următoarele persoane au fost prezente în cadrul întâlnirii: ► Din partea Beneficiarului: Cristian PRIBOI, CERT-RO ► Din partea Prestatorului: Vlad Barbălată, EY Dragoș Crețu, EY Vlad Donciu, EY Corina HOMEUCA, Initinvest

Persoane prezente în cadrul întâlnirii
Subiecte de discuție

Întâlnirea are ca scop alinierea abordării de realizare a activității A6 din cadrul proiectului SCIM între Prestator și CERT-RO, în calitate de Beneficiar.

Dna. Homeuca, expert cheie BSC a început prin prezentarea BSC și a rolului important pe care îl vor avea colegii CERT-RO din departamentul Control Intern Managerial mai ales în furnizarea documentelor care trebuie evaluate și detaliază:

- indicatori scorecard: learning & growth (HR, skills, knowledge); procese interne (al doilea palier);
- politica de instruire; CERT-RO nu are o structură dedicată de training. În funcție de proiect, au existat cursuri pentru jurnaliști, pentru top management de la instituții publice.
- SCIM: politici, planuri de acțiune, enumerare proceduri (atât de sistem cât și operaționale);
- scop principal: de a diminua riscurile cibernetice și de a conștientiza clienții/beneficiarii;
- e nevoie de: procese interne (SCIM); resurse umane; PR, comunicare strategică.

Dl. Priboi a sugerat că ar fi util să primească inițial o cerere de informații ca să poată pregăti împreună cu colegii din cadrul altor departamente documentele de interes, iar după ce le transmite Prestatorului să organizeze de comun acord întâlniri de clarificare unde se consideră necesar. Este posibil să întâmpinăm o mică problemă pe partea de strategie deoarece CERT-RO are un raport pe care îl prezintă anual CSAT iar acesta este clasificat. Pe baza lui se stabilesc direcțiile strategice. Intră sub incidența ORNIS (sunt informații în timp real).

Dna. Homeuca agreează această abordare menționând faptul că ideal ar fi în etapa a doua, pentru dezvoltarea indicatorilor să se faciliteze o colaborare mai activă și din partea Beneficiarului. Este important să înțelegem cum o să fie de folos pentru beneficiar acest proiect pentru a putea alinia așteptările.

Dl. Priboi a reiterat schimbările majore la nivelul CERT-RO menționate și în cadrul întâlnirii de inițiere, tranziția la autoritate pentru operatorii de servicii esențiale și furnizorii de servicii digitale (addendum conform directivei NIS). În prezent CERT-RO are organigrama de peste 130 de oameni, buget pentru 39, iar actualmente 36 angajați. Când CERT RO va avea rol de autoritate, la sursele de finanțare vor fi incluse și venituri din amenzile pentru neconformitate.

Beneficiul principal al legislației de facto (addendum conform directivei NIS) este obligativitatea raportării către CERT RO (în momentul unui incident, CERT RO trebuie notificat în timp real ca apoi să poată accesa sursele comune de informații); proiect pe Horizon 2020 pentru acces la informații de *threat intelligence* cu parteneriatul a diferite laboratoare de cercetare. HG-urile pentru legislația subsecventă care va stabili pragurile de la care se vor aplica și cuantumurile de amenzi sun încă în lucru. Iar cea mai benefică activitate viitoare va fi creșterea personalului.

În concluzie primul pas în urma acestei ședințe va fi solicitarea documentelor strategice aprobate la nivelul CERT RO, în vigoare, care vizează alocarea resurselor, a rolurilor și responsabilităților, a modului de derulare a procesului de planificare strategică (procese și fluxul acestora, proceduri interne, circuitul documentelor, părți interesate implicate etc) precum:

- Strategii

Persoane prezente în cadrul întâlnirii
▶ Planuri de acțiune ▶ Planuri de masuri ▶ Planuri de formare ▶ Instrucțiuni de lucru (IL) ▶ Proceduri de proces (PP) ▶ Politici interne ▶ Proceduri (operaționale / de sistem) ▶ Planuri de comunicare cu cetățenii ▶ Organigrama actualizată a CERT-RO

În cadrul întâlnirii au fost discutate și convenite următoarele acțiuni:

#	Acțiune	Responsabil	Termen
1	Organizarea și participare la întâlnirea - SCIM (Eliza Ciurea)	Prestator și Beneficiar	14.05.2020
2	Organizarea și participare la întâlnirea - Juridic (Mihai Guranda) în care se va discuta despre obiectivele și direcțiile strategice ce țin de adaptarea cadrului administrativ.	Prestator și Beneficiar	18.05.2020
3	Organizarea și participare la întâlnirea PR – Mihai Rotariu	Prestator și Beneficiar	TBD

MINUTA ÎNTÂLNIRII pentru realizarea Sub-activității 6.1

Client:	Autoritatea pentru Digitalizarea României (ADR) și Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)		
Contract:	Contract de achiziție servicii nr. 24 din 15.04.2020	**Redactat de:**	Nume: Nesrin Regep Data: 14.05.2020
		Revizuit de:	Nume: Vlad Barbălată Data: 14.05.2020

Titlu proiect	**Sistem integrat de management pentru o societate informațională performantă (SIMSIP) cod SIPOCA 391**		
Subiect	**Întâlnire pentru realizarea Sub-activității 6.1**		
Data	14.05.2020	**Locație**	Microsoft Teams
Ora de începere	11h00	**Ora de încheiere**	12h00
Lista de prezență	-	**Prezentare PowerPoint**	-

Persoane prezente în cadrul întâlnirii
Următoarele persoane au fost prezente în cadrul întâlnirii: ► Din partea Beneficiarului: Cristian PRIBOI, CERT-RO Eliza Ciurea, CERT-RO SCIM ► Din partea Prestatorului: Vlad Barbălată, EY Dragoș Crețu, EY Vlad Donciu, EY Corina HOMEUCA, Initinvest

Subiecte de discuție
În cadrul întâlnirii s-au discutat următoarele aspecte: ▶ Confirmarea întâlnirii la nivel înalt între Prestator și conducerea CERT-RO și ADR; ▶ Faptul că pentru completarea formularului inițial vor fi responsabili dl. Cristian Priboi și încă o persoană din cadrul CERT-RO; ▶ Formularul nr 2 pentru identificarea obiectivelor va fi adresat către 1/2 persoane din fiecare departament; ▶ Pentru întâlnirea cu reprezentantul din cadrul departamentului juridic, trebuie identificată legislația aplicabilă (in afară de legea 362 cu care Prestatorul este deja familiar).

În cadrul întâlnirii au fost discutate și convenite următoarele acțiuni:

#	Acțiune	Responsabil	Termen
1	Organizarea și participare la întâlnirea - Juridic (Mihai Guranda) în care se va discuta despre obiectivele și direcțiile strategice ce țin de adaptarea cadrului administrativ.	Prestator și Beneficiar	18.05.2020

MINUTA ÎNTÂLNIRII pentru realizarea Sub-activității 6.1

Client:	Autoritatea pentru Digitalizarea României (ADR) și Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)		
Contract:	Contract de achiziție servicii nr. 24 din 15.04.2020	**Redactat de:**	Nume: Nesrin Regep Data: 18.05.2020
		Revizuit de:	Nume: Vlad Barbălată Data: 18.05.2020

Titlu proiect	**Sistem integrat de management pentru o societate informațională performantă (SIMSIP) cod SIPOCA 391**		
Subiect	**Întâlnire pentru realizarea Sub-activității 6.1**		
Data	18.05.2020	**Locație**	Microsoft Teams
Ora de începere	14h00	**Ora de încheiere**	15h00
Lista de prezență	-	**Prezentare PowerPoint**	-

Persoane prezente în cadrul întâlnirii
Următoarele persoane au fost prezente în cadrul întâlnirii: ► Din partea Beneficiarului: Cristian PRIBOI, CERT-RO Mihai Guranda, CERT-RO Juridic Eliza Ciurea, CERT-RO SCIM ► Din partea Prestatorului: Vlad Barbălată, EY Dragoș Crețu, EY Vlad Donciu, EY Corina HOMEUCA, Initinvest

Subiecte de discuție
Întâlnirea are ca scop alinierea abordării pentru realizarea activității A6 din cadrul proiectului SCIM între Prestator și CERT-RO, în calitate de Beneficiar. Dl. Priboi a început întâlnirea cu mențiunea că nu au fost încă demarate acțiuni legate de SIMSIP, încă sunt în faza de clarificare a procedurilor. Faptic în prezent în cadrul CERT-RO sunt 40 de angajați pe vechea organigramă, fiind deja și organigrama nouă elaborată în varianta extinsă de 140 angajați. CH: Introducerea instrumentelor BSC și CAF implică analiza mai multor documente: strategii, politici, planuri de acțiune, proceduri, cadru legislativ etc. Prima etapă a proiectului este colectarea și analiza atât a conformității cu standardele de management cât și a necesității dezvoltării anumitor spețe. Aplicația informatică care va susține metodologia BSC dezvoltată se va implementa în cadrul unui proiect distinct. Așadar ce documente se utilizează la nivelul CERT-RO pentru definirea strategiei, viziunii? Răspuns: Strategia la nivelul CERT RO se bazează pe un plan de activitate anual elaborat de conducerea CERT-RO împreună cu un comitet de coordonare (compus din membrii CSAT). Aceștia au 2 întâlniri anuale. Planul de activitate prevede activități ce se vor desfășura în anul următor (cf. ordinului SGG 600/2018), acesta conține și o zonă de obiective specifice. CH: BSC în general se bazează pe un plan pe termen mai lung (3 ani) dar în acest caz va adapta specificităților proiectului actual. Colegul nostru Dragoș Crețu a transmis un pe email cu documentele necesare primei etape, pentru a putea supune aprobării conducerii. Oricum la nivel de legislație au fost identificate Strategia Națională Anticorupție și Legea 362 (directiva NIS). Răspuns: Când vom răspunde la cererea de informații vom include și linkuri către legislația care guvernează activitățile. Din ianuarie 2020 CERT RO se află în ordinea SGG, vă vom trimite transformarea instituțională a CERT RO. Dna. Homeuca a prezentat formularul de analiză (https://initinvest.ro/bsc-fisa/) care are ca termen de completare - aproximativ o săptămână. CH: Este utilă crearea unei echipe care să completeze formularul pentru a se asigura cunoștințe pe toate zonele studiate în analiza documentelor. Ne va ajuta să înțelegem ce trebuie îmbunătățit, din perspectiva internă a CERT RO. Fișa se adresează întregii instituții și se completează o singură dată (completată în echipă la nivelul organizației de către stakeholderii care cunosc în detaliu organizația). Răspuns: În ceea ce privește comunicarea cu cetățenii, există o procedură de comunicare, și anume OUG 97 (ordonanța petițiilor) și legea accesului la informații de interes public. CERT-RO nu are angajați funcționari publici, ci personal contractual (la momentul actual). CH: Pentru analiza premergătoare obiectivele se vor stabili împreună, apoi vom avea nevoie de o altă analiză completată de aproximativ 2 persoane de la fiecare departament din cadrul instituției. Răspuns: Se poate trimite o listă cu proceduri din care să alegem cele necesare unei analize mai în detaliu. Momentan sunt în total undeva la 30 de proceduri (nu toate actualizate).

Subiecte de discuție
CH: Ne trebuie politicile mai ales în acest moment. Răspuns: Nu sunt diferențiate foarte mult politicile de proceduri. CH: În prima etapă mai mapăm ce ține de obiective, procedurile de sistem. Răspuns: În zona de HR se face un referat de necesitate prin care se propune un angajat care să participe la un anumit curs deoarece sunt limite bugetare accentuate pe zona de cursuri (justificare pentru lipsa unei proceduri legate de cursuri/certificări). Aceleași limitări se aplică și pe zona de capacity planning pentru achiziții tehnologie. Trasabilitatea e bună, dar cum se va mitiga setarea obiectivelor între diferitele niveluri din organizație? CH: Prin negociere. Conform best practices din proiecte anterioare, unul dintre aspectele identificate e lipsa vizibilității la nivel de top management. Răspuns: Top management, adică director general numit politic de către PM la recomandarea SGG și directorii adjuncți numiți de către instituțiile care fac parte din comitetul de coordonare (MAI, MApN, structuri de inteligență). Încercam să finalizăm colectarea documentelor pe 25.05 (luni), însă ținând cont că se lucrează și remote e greu să ne luăm un angajament ferm în numele colegilor. CH: Recapitulare documente necesare în prima etapă sunt tot ce ține de obiective, organigrama finală extinsă, ROF, legislația etc. Răspuns: Trebuie cerut acordul de la conducere privind diseminarea informațiilor. Este utilă minuta întâlnirii pentru a avea consens asupra informațiilor cerute. Oorganizatoric, au fost probleme cu linkul de Microsoft Teams. A retrimis dl. Priboi un link si abia apoi a funcționat. Dragoș Crețu: Rămâne de stabilit o discuție și cu colegii din CERT-RO pe zona de PR / Comunicare. Vom transmite către dl. Priboi propunerile de planificare a întâlnirii.

În cadrul întâlnirii au fost discutate și convenite următoarele acțiuni:

#	Acțiune	Responsabil	Termen
1	Organizarea și participare la întâlnirea PR – Mihai Rotariu	Prestator și Beneficiar	TBD

MINUTA ÎNTÂLNIRII pentru realizarea Sub-activității 6.1

Client:	Autoritatea pentru Digitalizarea României (ADR) și Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)		
Contract:	Contract de achiziție servicii nr. 24 din 15.04.2020	**Redactat de:**	Nume: Nesrin Regep Data: 21.05.2020
		Revizuit de:	Nume: Vlad Barbălată Data: 21.05.2020

Titlu proiect	**Sistem integrat de management pentru o societate informațională performantă (SIMSIP) cod SIPOCA 391**		
Subiect	**Întâlnire pentru realizarea Sub-activității 6.1**		
Data	21.05.2020	**Locație**	Microsoft Teams
Ora de începere	15h30	**Ora de încheiere**	16h30
Lista de prezență	-	**Prezentare PowerPoint**	Realizată de Adelina Peculea

Persoane prezente în cadrul întâlnirii
Următoarele persoane au fost prezente în cadrul întâlnirii: ► Din partea Beneficiarului: Cristian PRIBOI, CERT-RO Mihai Rotariu, CERT-RO Comunicare ► Din partea Prestatorului: Vlad Barbălată, EY Dragoș Crețu, EY Vlad Donciu, EY Corina HOMEUCA, Initinvest Adelina Dumitrescu, Inititvest

Subiecte de discuție
Întâlnirea are ca scop alinierea abordării pentru realizarea activității A6 din cadrul proiectului SCIM între Prestator și CERT-RO, în calitate de Beneficiar. CH: Așa cum a fost înștiințat deja dl. Priboi pentru prima etapă a proiectului BSC sunt necesare mai multe documente și strategii de comunicare, planuri de acțiune pentru a realiza analiza pe 4 paliere de analiză: financiară (eficiență costuri), formare și dezvoltare, procesele interne și satisfacția cetățeanului în raport cu organizația. AP: Înainte de a stabili indicatorii, trebuie făcută o analiza preliminară a ceea ce înseamnă management strategic la nivel CERT-RO. Astfel, sunt necesare o serie de documente care să descrie: viziune, misiune, valori, direcții strategice. Răspuns: Se lucrează la o strategie de comunicare în conformitate cu viziunea noului manager al instituției. Nu avem planuri de acțiune pe partea de comunicare, dar vom verifica și reveni cu un răspuns ferm. CH: Avem vizibilitate momentan doar la strategia de securitate cibernetică a României. Răspuns: Privitor și la implementarea legii 362 (directiva NIS) se lucrează mult pe zona de awareness pentru cybersecurity (activitatea BAU); răspunsul la incidente de securitate cibernetică (există și un call center în acest sens). Referitor la documente interne legate de zona de strategie de comunicare (planul / strategia de comunicare) aceasta va fi trimisă în momentul în care va ieși din stadiul de draft. Nu există o procedură clară pentru că în prezent dl. Rotariu este singurul care se ocupă de această zonă. Mărirea organizației conform noii organigrame la 140 de angajați se va realiza prin concurs de angajare, când starea de fapt o va permite. Nu există momentan buget pentru mai mult decât cei 39 de angajați (37 de facto). Vom căuta și propuneri mai vechi referitoare la zona de comunicare pe site-ul vechi care a fost migrat acum câțiva ani. CP: Pentru documente, trebuie să existe un flux clar al transmiterii acestora (trebuie cerute explicit pe mail, pentru că și un draft când părăsește CERT RO devine document oficial). Răspuns: Fiecare lider de departament ar trebui să aibă planuri de acțiune, trebuie verificat cu aceștia. Pentru orice informație trebuie să ne consultăm cu managementul instituției pentru obținerea aprobărilor Referitor la planul strategic instituțional la nivelul ministerului ne interesăm dacă există la nivelul guvernului o strategie pentru CERT RO. CP: Chestionarul (fișa de analiză) e în lucru în cadrul instituției, rămâne de planificat o discuție pentru mâine (vineri) la ora 10 pentru a confirma dacă se pot transmite până luni documentele cerute prin RFI. Dragoș Crețu va retrimite RFI-ul transmis anterior și către celelalte departamente, prezentarea de azi de la Adelina Peculea și o prezentare scurtă din care reies beneficiile proiectului. Mai ar fi necesare câteva întâlniri pentru a clarifica o serie de aspecte privind:

Subiecte de discuție
1. adoptarea internă a masurilor impuse de GDPR (679/2016), din punct de vedere tehnic, organizatoric (altele măsuri decât cele incluse în procedura de protecția datelor primită deja) a. conștientizarea angajaților privind GDPR, b. clauze incluse/anexate in/la fișa de post), c. inclusiv, dacă există proceduri de privacy by design/by default 2. modul de implementare, respectiv monitorizare a strategiilor (in general, daca se organizeaza un grup de lucru, exista un responsabil etc)

În cadrul întâlnirii au fost discutate și convenite următoarele acțiuni:

#	Acțiune	Responsabil	Termen
1	Organizarea și participare la întâlnirea cu managementul CERT-RO Director Gen., Dir. Gen Adj, Director Tehnic, dar si sefi de departamente). In acest sens, ar dori sa stie daca se pot loga doar cu link (eventual si cu cod) in Teams ca sa nu mai trimita adresele de email (stiu ca exista aceasta posibilitate, dar trebuie configurat de admin-ul vostru).	Prestator și Beneficiar	TBD

MINUTA ÎNTÂLNIRII pentru realizarea Sub-activității 6.1

Client:	Autoritatea pentru Digitalizarea României (ADR) și Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)		
Contract:	Contract de achiziție servicii nr. 24 din 15.04.2020	**Redactat de:**	Nume: Nesrin Regep Data: 28.05.2020
		Revizuit de:	Nume: Vlad Barbălată Data: 28.05.2020

Titlu proiect	**Sistem integrat de management pentru o societate informațională performantă (SIMSIP) cod SIPOCA 391**		
Subiect	**Întâlnire pentru realizarea Sub-activității 6.1**		
Data	28.05.2020	**Locație**	Microsoft Teams
Ora de începere	11h00	**Ora de încheiere**	12h00
Lista de prezență	-	**Prezentare PowerPoint**	-

Persoane prezente în cadrul întâlnirii
Următoarele persoane au fost prezente în cadrul întâlnirii: ► Din partea Beneficiarului: Cristian PRIBOI, CERT-RO ► Din partea Prestatorului: Vlad Barbălată, EY Dragoș Crețu, EY Vlad Donciu, EY Corina HOMEUCA, Initinvest

Subiecte de discuție
Întâlnirea are ca scop alinierea abordării pentru realizarea activității A6 din cadrul proiectului SCIM între Prestator și CERT-RO, în calitate de Beneficiar. S-au discutat punctual modificările realizate la formularul prezentat în cadrul unei ședințe anterioară. Pentru ca utilizarea formularului să fie mai facilă Prestatorul pune la dispoziție două variante, dintre care CERT-RO va putea alege: 1. Format **PDF**, care poate fi completat și parțial, salvat și apoi circulat între respondenți. Rubrica Observații, deși pare mică, are nr. nelimitat de caractere. La final, când este completat integral, se apasă și butonul trimite ca să fie înregistrat și în sistemul Prestatorului 2. Formularul **online în care a fost introdus** un câmp de email astfel încât cel care completează, chiar si parțial, va primi pe email formularul completat în format PDF, pentru a fi circulat și celorlalți participanți. La final poate prestatorul să integreze toate răspunsurile, în condițiile în care Beneficiarul furnizează variantele completate parțial și, în cazul în care există dubluri (același câmp completat de mai mulți respondenți diferiți)să fie transmisă varianta finală. Datele de acces sunt :https://initinvest.ro/bsc-fisa/ și parola: SIMSIP-BSC@391Init

În cadrul întâlnirii au fost discutate și convenite următoarele acțiuni:

#	Acțiune	Responsabil	Termen
1	Comunicarea formatului ales pentru chestionar	Beneficiar	TBD

MINUTA ÎNTÂLNIRII pentru realizarea Sub-activității 6.1

Client:	Autoritatea pentru Digitalizarea României (ADR) și Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)		
Contract:	Contract de achiziție servicii nr. 24 din 15.04.2020	**Redactat de:**	Nume: Nesrin Regep Data: 26.06.2020
		Revizuit de:	Nume: Vlad Barbălată Data: 26.06.2020

Titlu proiect	**Sistem integrat de management pentru o societate informațională performantă (SIMSIP) cod SIPOCA 391**		
Subiect	**Întâlnire pentru realizarea Sub-activității 6.1**		
Data	26.06.2020	**Locație**	Microsoft Teams
Ora de începere	11h00	**Ora de încheiere**	12h00
Lista de prezență	-	**Prezentare PowerPoint**	-

Persoane prezente în cadrul întâlnirii
Următoarele persoane au fost prezente în cadrul întâlnirii: ► Din partea Beneficiarului: Cristian PRIBOI, CERT-RO Eliza Ciurea, CERT-RO SCIM Mihai Guranda, CERT-RO Juridic ► Din partea Prestatorului: Vlad Barbălată, EY Nesrin REGEP, EY Corina HOMEUCA, Initinvest

Subiecte de discuție
CH: Ați avut disponibilitate să vă uitați pe Chestionarul de analiză la nivelul organizației, funcționează ok? Răspuns: Chestionarul a fost testat este în regulă, acesta va fi transmis astăzi către toți potențialii respondenți din cadrul CERT-RO. CH: Revin cu rugămintea să menționați faptul că după completare acesta trebuie salvat ca optimized PDF, foarte important pentru prelucrarea răspunsurilor. Întâlnirea are ca scop clarificarea unor aspecte ce au reieșit în urma studierii de către Prestator a documentelor/procedurilor transmise de către CERT-RO. CH: Cum se realizează diseminarea ultimelor versiuni ale procedurilor, din documentele studiate am observat și unele versiuni actualizate de proceduri? Răspuns: Comunicarea se realizează pe email către echipă, dar ca prezentare inițial șefii de departament pun în discuție actualizarea și dacă sunt întrebări sau sunt necesare clarificări acestea sunt adresate șefului ierarhic superior și sunt circulate tot pe email o dată cu actualizarea. CH: Fiecare departament elaborează procedurile sale pe domeniul de activitate și apoi sunt avizate de SCIM? Răspuns: Într-adevăr de la începutul anului 2020 acesta este procesul, însă înainte nu erau verificările/validările SCIM, se elaborau procedurile și apoi se trecea direct la etapa de implementare. CH: Am văzut că există un registru GDPR la nivelul instituției, unde este acesta la DPO sau la departamentul Juridic? Răspuns: Registrul este la DPO însă nu știm exact cum este împărțită responsabilitatea de actualizare a acestuia, ar fi mai în regulă să răspundă DPO-ul la întâlnirea programată luni pentru a păstrăm un echilibru în comunicare. CH: Instruirile obligatorii prin lege, cum ar fi GDPR, SSM se organizează în cadrul CERT-RO? Răspuns: Da. CH: ROF și fișele posturilor acoperă în totalitate atribuțiile, sarcinile și activitățile desfășurate, dar clauzele de confidențialitate sunt de asemenea incluse? Răspuns: La angajare Lucian Crețu a distribuit un acord de confidențialitate, anexă la fișa postului. CH: Care este procesul de implementare a unui proiect? Răspuns: În primul rând se stabilește o echipă de implementare a proiectului prin decizie, apoi la finele lunii se face raportul de activitate pentru fiecare persoana și se plătesc orele alocate pe proiect, pentru cele cu finanțare UE. Proiectele interne nu se plătesc, se alocă un responsabil/ mai mulți responsabili și având în vedere că se atribuie sarcini deja stipulate în fișa postului nu e plătit suplimentar.

Subiecte de discuție
CH: Obiectivele de atins pe baza atribuțiilor din fișa postului sunt deja prevăzute, însă la un obiectiv nou care se mapează pe atribuțiile deja existente cum se procedează cine inițiază procesul? Răspuns: Ca și proiecte lucrările vin repartizate de conducere pe firul ierarhic iar setul nou de atribuții le executăm ca atare. Directorul general (DG) și DG Adjunct desemnează departamentul/departamentele responsabil/-e apoi fiecare șef de departament nominalizează responsabilii de implementare și așa se formează echipele de implementare. CH: Am constata că există multe proceduri dar și așa rămân activități neacoperite. Există și alte proceduri interne? Răspuns: Nu există alte proceduri interne în afară de cele transmise. Implementarea activităților care nu sunt transpuse în proceduri depinde de la caz la caz, pe partea de comunicare de exemplu departamentul de analiză cooperare are descrisă în fișa postului activitatea de promovare CERT-RO și realizează acest lucru cu aprobare din partea conducerii. Deci nu există efectiv o procedură internă ci activitățile sunt distribuite prin fișa postului care revine persoanei în cauză. CH: Ce se întâmplă dacă trebuie îndeplinită o acțiune nouă pe care o persoană nu o poate îndeplini deoarece nu are competențele necesare? Răspuns: Se poate face un referat de necesitate pentru a parcurge cursuri de formare pentru a dobândi noi competențe, urmând ca acestea să se aprobe în limita bugetului alocat pentru formare. Când s-a făcut noua mapare ROF prin hotărâre CSAT anul trecut, activitățile/acțiunile/competențele s-au stabilit așa cum se procedează de obicei, proporțional în funcție de gradația pe care o are angajatul. CH: În ce mod cu și ce frecvență se realizează evaluarea personalului? Am constatat din documentele transmise faptul că obiectivele și atribuțiile există, dar indicatori? Puteți furniza câteva exemple de indicatori? Răspuns: Indicatorii sunt prevăzuți în fișa postului. Ex. abilitatea de a analiza evalua și propune măsuri de evaluare a procedurilor. Se lucrează la HR la o nouă procedura de evaluare/cuantificare. O să organizăm o întâlnire cu colega de la HR, care în această săptămână este în concediu, ea vă va putea răspunde mai concret la întrebare și poate detalia procedura de evaluare a personalului. CH: În evaluarea personalului trebuie prevăzuți și indicatori de implementare a Strategiei – obiective-acțiuni - (BSC prevede împărțirea pe 4 paliere: financiar, dezvoltarea personalului, evaluarea satisfacției clienților/beneficiarilor) Răspuns: Nu există în prezent metode de măsurare a satisfacției beneficiarilor – ar trebui să existe o corelare între indicatorii de performanță a managementului și satisfacția beneficiarilor. Activitățile legate de CSIRT nu sunt încă operaționalizate. Legea 362 / 2018 e relativ nouă și este încă în stadiu de implementare. Multe texte din lege unde s-ar putea verifica gradul de mulțumire, nu se pot realiza încă pana nu se va operaționaliza Referitor la Planul SNSC: Comitetul de coordonare din care face parte și CERT-RO (gradul de mulțumire este evaluat prin niște instrumente stabilite prin lege). CH: Am observat faptul că CERT-RO are atribuții de implementare și monitorizare a strategiilor, dar ce ne puteți împărtăși despre rolul în etapa de elaborare?

Subiecte de discuție
Răspuns: Avem un rol activ consultativ în etapa de elaborare strategii ca membru COSC. Înainte de 2020 strategia de securitate cibernetică o elabora MCSI, iar acum intră în atribuțiile SGG. Și înainte se solicita punctul de vedere al CERT-RO însă acum implicarea este mai mare. CH: Există vreun proces de monitorizare a implementării strategiei? Răspuns: Odată ce se adoptă cadrul legislativ pentru implementarea strategiei și obiectivele și măsurile care trebuie luate de fiecare instituție întocmite la nivel SGG. Noi elaborăm propuneri venim cu proiecte și o parte pot fi și adoptate și transpuse ca atare, Participăm la discuții și ne susținem punctul de vedere. Cel mult CSAT ar putea verifica implementarea ex-post. CERT-RO are abilitatea de a controla post implementare ceea ce se întâmplă, atribuțiile intră în partea de monitorizare. Planul de activitate CSAT suntem obligați prin lege să îl implementăm, iar dacă apar obstacole sau propuneri de îmbunătățire când vine comitetul de coordonare și se constată nivelul de implementare al obiectivelor se mai poate discuta pe obiectiv în sine. Comitetul de coordonare este compus din reprezentanți SRI, STS, SIE, MAI, MapN, MAE conform art. 15 alin. 2 din Legea 362. CH: Am constatat faptul că sistemul de relații ierarhice este bine definit in ROF, dar organigrama nu respectă standardul, nu sunt repartizate clar relațiile de subordonare. Ar trebui poate să fie mai clară mai detaliată, vom reveni cu câteva recomandări punctuale în acest sens.

În cadrul întâlnirii au fost discutate și convenite următoarele acțiuni:

#	Acțiune	Responsabil	Termen
1	Organizarea și participare la întâlnirea DPO	Prestator și Beneficiar	29.06.2020

MINUTA ÎNTÂLNIRII pentru realizarea Sub-activității 6.1

Client:	Autoritatea pentru Digitalizarea României (ADR) și Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)		
Contract:	Contract de achiziție servicii nr. 24 din 15.04.2020	**Redactat de:**	Nume: Nesrin Regep Data: 29.06.2020
		Revizuit de:	Nume: Vlad Barbălată Data: 29.06.2020

Titlu proiect	**Sistem integrat de management pentru o societate informațională performantă (SIMSIP) cod SIPOCA 391**		
Subiect	**Întâlnire pentru realizarea Sub-activității 6.1**		
Data	29.06.2020	**Locație**	Microsoft Teams
Ora de începere	12h00	**Ora de încheiere**	13h00
Lista de prezență	-	**Prezentare PowerPoint**	-

Persoane prezente în cadrul întâlnirii
Următoarele persoane au fost prezente în cadrul întâlnirii: ► Din partea Beneficiarului: Cristian PRIBOI, CERT-RO Lucian CREȚU, DPO CERT-RO ► Din partea Prestatorului: Nesrin REGEP, EY Corina HOMEUCA, Initinvest

Subiecte de discuție
Demersurile realizate în cadrul acestei activități au ca obiectiv final dezvoltarea unui soft care vă va ajuta să treceți prin pașii de elaborare, implementare, monitorizare și evaluare a oricărei strategi sau plan național. Practic softul vă va ajuta să urmăriți îndeplinirea pe bază de obiectiv și indicatori. CH: În această etapă trebuie să identificăm și dacă implementarea unui nou proiect pe zona de protecție a datelor are nevoie de acțiuni suplimentare de urmărire a activităților. Am analizat documentele primite, am văzut că există o procedură. DPO: În prezent avem 2 politici aprobate de conducerea instituției pentru implementarea la nivelul CERT-RO, referitoare la reglementarea politicii de cookie a paginii web și politica privind implementarea GDPR care conform regulamentului suntem obligați să o publicăm. Noi suntem instituție publică și în același timp o autoritate care are contact foarte restrâns cu persoanele fizice, în 2 situații: - concursuri de încadrare când colectăm datele cu caracter personal conform legii art 6 alin. c și e - semnalarea de incidente prin email sau call-center când mai colectăm date cu caracter personal de la diverse persoane, însă acesta nu e obiectivul de activitate al CERT-RO. În call center sunt preluate apelurile de la persoanele respective și se dau indicații referitoare la instituțiile pe care trebuie sa le contacteze, nu le reținem datele personale. Alertele de la white hackers când sună la call-center li se aduce la cunoștință mesajul privitor la politica de înregistrare a convorbirii și faptul că continuarea apelului reprezintă acordul. Pentru prelucrarea datelor ale personalului instituției utilizăm programul REVISAL în care sunt introduse toate datele, protecția datelor e asigurată de lege și firma care a dezvoltat programul și proiectul respectiv. În cazul contractului nostru, există acordul de confidențialitate. Orice contract dintre instituții și firme are protecția GDPR iar politica de confidențialitate e altceva. Confidențialul are 2 aspecte generic și concret (nivel secret) nu face obiectul unei astfel de activități. Confidențialul folosit de instituții de drept privat se referă la date cu caracter secret care ar produce prejudiciu firmelor respective. În instituțiile publice aceste date nu sunt cotate ca fiind clasificate ci sunt fie considerate secret de serviciu sau neclasificate nedestinate publicității. CH: În cazul autorităților publice sunt date cu caracter secret și altele. Orice altceva necesită autorizare pentru a fi dat publicității și pentru a implementa principiul transparenței. DPO: În procesul de implementare BSC se poate implementa o politică mai ales pe comunicare. CH: Toți angajații vor fi în sistem. DPO: Toți angajații sunt avizați să acceseze informații clasificate secret de stat, ceilalți sunt avizați pentru manipularea de informații clasificate secret de serviciu. Angajații au semnat angajament de confidențialitate conform legii 585 anexa 3.

Subiecte de discuție
CH: Pentru datele cu caracter personal ale angajaților în funcție de dreptul de acces se utilizează pseudonimizarea? DPO: Majoritatea calculatoarelor care prelucrează date cu caracter personal au acces limitat, maxim 2 utilizatori. Pseudominizarea o face firma. Alt calculator care prelucrează avizul persoanelor la informații clasificate mijloc de calcul acreditat, se află într-o zonă securizată și cu nr de persoane limitat cu prelucrarea doar avizată. În altă parte nu se mai stochează decât pe server REVISAL, nu se stochează IP-urile care oricum sunt dinamice. CH: Din punct de vedere al securității cibernetice nu m-am gândit ca ar fi o problemă privitor la măsurile implementate, regulament și atribuții ANSPDPC etc. CP: Prin rigoarea internă respectam regulile GDPR înainte, aceste măsuri reglementate sunt mult mai relaxate decât ce implementăm noi. DPO: Avem puține stații de lucru care procesează date, iar persoanele autorizate își desfășoară activitatea în principiul necesității. CH: Sunt toți angajații conștientizați și de exemplu din punct de vedere al securității documentelor fizice etc. DPO: Între altele prelucrăm și secrete de stat, planurile de pregătire sunt realizate lunar. Teme de pregătire pe intranet transmise periodic. Există 2 persoane acreditate DPO cu atribuții duse prin cumul de atribuții. E foarte greu de organizat forme de pregătire internă din cauza regulilor de conectare. CH: Instruiri interne sunt necesare deoarece vulnerabilitatea organizației sunt oamenii pentru că sunt cel mai greu de controlat. DPO: Consider că cea mai mare oportunitate a unei organizații este omul. Toți angajații au certificate eliberate de ORNISS. A îți pierde avizul este echivalent cu pierderea locului de muncă, cu consecințe chiar în plan penal în funcție de gravitate. Avem o procedură pentru gestionarea datelor cu caracter personal din 2016, dar nu mai e de actualitate. Dpdv a ceea ce reprezintă SCIM la noi au fost dificultăți din trecut care au dus la implementare mai mult sau mai puțin. Numărul mic de angajați si numărul mare de sarcini fac ca anumite sarcini extra să nu fie realizate dacă au caracter opțional. Implementarea legii cum ar trebui, uneori este foarte dificil de realizat, ca să respecți una trebuie să încalci alta. Suntem o instituție mică cu responsabilități multe și într-un an am trecut prin 3 modificări majore: coordonare MCSI, coordonare MTIC apoi coordonarea primului ministru și alocați la bugetul SGG. Aceste schimbări au afectat modul de alocare a resurselor bugetare. CH: Recomandăm conștientizarea periodică a angajaților privitor la chestiuni interne, cum ar fi unde se găsesc informații despre GDPR, testare anuală de cunoștințe online. Clarificăm faptul că BSC va ajunge la nivel de KPI pe 4 paliere, dar nu este instrument de evaluare a angajatului. Al 5-lea palier este responsabilitate socială.

Subiecte de discuție
DPO: Se poate dezvolta și al 5-lea palier la nivelul CERT-RO deoarece sunt situații în care lucrăm în week-end, organizăm cursuri pentru copii, jurnaliști despre managementul situațiilor de criză/urgență etc. Conform legii o autoritatea poate fi subordonată parlamentului, ministerului sau premierului în funcție de nivelul de reglementare. ANCOM e subordonat parlamentului ața acum prevăd reglementările UE în domeniu, ca să poată amenda operatorii de pe piață nu putea fi în subordinea guvernului care emite legile respective, altfel se crea monopol (emit-controlez-amendez). ADR și CERT-RO sunt subordonate premierului. CP: Confirmăm faptul ca dl. Lucian Crețu este reprezentant BSC și CAF în cadrul CERT-RO iar chestionarele necesare pentru finalizarea analizei vor fi transmise miercuri. După finalizarea livrabilului aferent 6.1 se va organiza o întâlnire la sediul CERT-RO.

În cadrul întâlnirii au fost discutate și convenite următoarele acțiuni:

#	Acțiune	Responsabil	Termen
1	Transmiterea chestionarelor completate	Beneficiar	1.07.2020

6.3 Chestionare de analiză la nivelul organizației CERT-RO