SPECIFICAŢII TEHNICE

Anexa nr. 22 la Documentația standard
aprobată prin Ordinul Ministrului Finanţelor nr. 115 din 15.09.2021

Numărul procedurii de achiziție: ***Licitație deschisă 21075656/ ocds-b3wdp1-MD-1678698721031***
Denumirea licitaţiei: ***Servicii de elaborare SIA „Registrul de stat al incidentelor de securitate cibernetică”***

Denumirea serviciilor	Denumirea modelului serviciului	Ţara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
Bunuri/servicii						
Lotul nr. 1: Servicii de elaborare SIA „Registrul de stat al incidentelor de securitate cibernetică” (SIA RSISC)	---	Republica Moldova	DSS	În conformitate cu Caietul de sarcini (Anexa nr. 21 din Documentația standard); Perioada de livrare: până la 10 luni din data semnării contractului; Termenul de garanție și suport: 12 luni de la punerea în producție a (SIA RSISC)	Conform descrierii soluției propuse anexate	**Moldova Standard**

Semnat:_____
Numele, Prenumele: Sîrbu Ion
În calitate de: Director
Ofertantul: DAAC Software Systems S.R.L.
Adresa: mun.Chișinau str.Calea Ieșilor 10

Digitally signed by Sîrbu Ion
Date: 2023.04.21 14:21:56 EEST
Reason: MoldSign Signature
Location: Moldova

OFERTA TEHNICĂ

Pentru dezvoltarea sistemului informațional automatizat
"REGISTRUL DE STAT AL INCIDENTELOR DE SECURITATE CIBERNETICĂ"

62-PB.001.01

"DAAC SYSTEM INTEGRATOR" SRL
2023

CUPRINS

1 Scopul

Implementarea unui Registru unic centralizat de stat pentru gestionarea incidentelor de securitate cibernetică (denumit în continuare **SIA RSISC)** are ca scop:

- crearea unei resurse informaționale de stat pentru acumularea, analiza și gestionarea informațiilor legate de incidentele de securitate cibernetică
- stabilirea unei proceduri unice de introducere online a datelor în SIA RSISC pe baza tehnologiilor moderne de acces la date.
- asigurarea creării unei baze de date a incidentelor de securitate cibernetică și a alertelor de securitate cibernetică de importanță națională pe baza unei structuri unitare a obiectelor de evidență, a metodelor de analiză și prelucrare a acestora
- asigurarea identificării automate a amenințărilor, vulnerabilităților și incidentelor de securitate cibernetică identificate sau raportate, a metodelor și tehnologiilor utilizate pentru atacuri și a celor mai bune practici de protecție a infrastructurii cibernetice.
- creșterea eficienței analizei riscurilor legate de amenințările cibernetice și a măsurilor de prevenire sau de reducere la minimum a efectelor negative prin menținerea sistematică a unei înregistrări centralizate unice, precum și prin analiza sistematică.
- accelerarea luării deciziilor de management de către funcționari prin crearea unei baze de cunoștințe (date de identificare, descrieri ale investigațiilor, decizii și acțiuni de prevenire și remediere a incidentelor cibernetice) prin reutilizarea acesteia
- notificarea în timp util a amenințărilor cibernetice identificate, a vulnerabilităților, a riscurilor de securitate cibernetică și a metodelor de prevenire sau de reducere la minimum a impactului acestora către autoritățile publice, întreprinderi și alte părți interesate
- furnizarea de statistici și analize actualizate, cu posibilitatea de a genera rapoarte în diverse configurații, inclusiv rapoarte analitice detaliate la nivel național în funcție de diferite criterii și intervale de timp
- furnizarea de informații generale utilizatorilor publici cu privire la securitatea cibernetică, la posibilele amenințări și la activitățile autorităților publice pentru a preveni și a minimiza consecințele acestora.

Înființarea SIA RSISC contribuie la realizarea următoarelor obiective

- Furnizarea de mecanisme de automatizare a proceselor de identificare, înregistrare, clasificare a incidentelor cibernetice

- Îmbunătățirea calității datelor (fiabilitate, promptitudine a raportării și plentitudine) privind incidentele de securitate cibernetică și alertele de securitate cibernetică.
- consolidarea setului de date electronice și a cunoștințelor legate de incidentele de securitate cibernetică prin standardizarea și structurarea informațiilor și a metodelor de procesare
- automatizarea procedurilor operaționale pentru diagnosticarea, analiza și gestionarea incidentelor de securitate cibernetică,
- oferirea de asistență persoanelor cu funcție de răspundere în luarea deciziilor și elaborarea măsurilor de protecție a infrastructurii cibernetice pe baza informațiilor acumulate și a datelor actualizate din sistemele externe, ceea ce va contribui la calitatea CERT Gov.
- reducerea timpului de înregistrare, analiză, documentare și luare a deciziilor privind incidentele de securitate cibernetică identificate
- detectarea automatizată a reapariților amenințărilor cibernetice
- automatizarea proceselor de monitorizare a alertelor și incidentelor de securitate cibernetică înregistrate, crearea și confirmarea rapoartelor de incident
- asigurarea punerii în aplicare a politicilor de prevenire și combatere a criminalității informatice
- asigurarea unei interacțiuni continue între CERT departamentale și CERT guvernamentale în ceea ce privește incidentele de securitate cibernetică și alte informații legate de securitatea cibernetică.
- organizarea interacțiunii cu sistemele informatice ale altor autorități și organizații publice pentru schimbul bidirecțional de date pe baza utilizării serviciilor guvernamentale furnizate de Agenția de Guvernare electronică sau furnizarea de interfețe standard pentru interacțiune.

2 Baza

Cerința Caiet de sarcini destinat elaborării Sistemului Informațional Automatizat „Registrul de stat al incidentelor de securitate cibernetică” от 13.03.2023.

3 Termeni și abrevieri

Autentificarea este procesul de potrivire a unui utilizator public al unui sistem cu identificatorul pe care acesta l-a numit.

Identificare - stabilirea identității unui utilizator public ca utilizator înregistrat în sistem și apoi acordarea drepturilor corespunzătoare atribuite acestuia
Serviciile web sunt aplicații autonome, modulare, distribuite, dinamice, care pot fi descrise, publicate, plasate și invocate în rețea. Ele nu sunt legate de o platformă sau de un limbaj de programare specific.
Depozitul de date (Warehouse) este un set de date orientate pe subiecte, integrate, istorice, nedistructibile, concepute pentru a sprijini procesul decizional de management.
Securitatea cibernetică este starea normală care rezultă dintr-un set complex de măsuri proactive și reactive care asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și permanența informațiilor în format electronic, a sistemelor și resurselor informatice, a serviciilor electronice publice și private.
Un incident de securitate cibernetică este un eveniment care a avut loc în spațiul cibernetic și ale cărui consecințe afectează securitatea cibernetică.
Riscurile de securitate cibernetică reprezintă probabilitatea ca o amenințare să se materializeze prin exploatarea unei anumite vulnerabilități specifice infrastructurilor cibernetice;
Un atac cibernetic este o acțiune ostilă desfășurată în spațiul cibernetic care poate afecta securitatea cibernetică;
Instituții publice - ministere, alte organe administrative centrale subordonate Guvernului, Cancelaria de Stat și structurile organizatorice din domeniile de competență ale acestora (organe administrative subordonate, servicii publice descentralizate și subordonate, precum și instituții publice și întreprinderi publice în care ministerul, Cancelaria de Stat sau un alt organ administrativ central are statut de fondator și organizații publice autonome înființate de Guvern;

ID este un identificator, un atribut unic al unui obiect de evidență care permite diferențierea unică a acestuia de alte obiecte, adică identificarea lui.
SIA - sistem informatic automatizat
BP – business proces
CV - ciclu de viață
AP - autoritate publică
DCD - depozit central de date (Warehouse)
SDE - semnătură digitală electronică

4 Destinație

Sistemul informațional automatizat "Registrul de stat al incidentelor de securitate cibernetică" este destinat pentru realizarea proceselor de înregistrare, întreținere și gestionare a incidentelor de securitate cibernetică înregistrate de către organele abilitate (CERT Gov, CERT-urile departamentale, serviciile speciale de racție din instituțiile de stat).
SIA RSISC este sistemul oficial de înregistrare și gestionare a incidentelor cibernetice la nivel guvernamental în Republica Moldova. Acesta este un instrument de sprijinire a activităților CERT Gov, oferind mijloacele tehnice pentru obținerea și schimbul de informații, cooperare și se caracterizează prin transparența activităților. Pe această bază, SIA RSISC va crea un Registru accesibil, actualizat, modern și sigur al incidentelor de securitate cibernetică.

SIA RSISC sprijină ciclul de viață al alertelor și incidentelor de securitate cibernetică: introducerea datelor, diagnosticarea, analiza riscurilor, procesarea, luarea deciziilor, implementarea politicilor și pregătirea documentelor pentru a preveni sau minimiza impactul negativ, stocarea, transmiterea informațiilor către alte entități și organizații colaboratoare, precum și furnizarea către părțile interesate a rapoartelor statistice și a informațiilor privind prezența și starea amenințărilor cibernetice și acțiunile întreprinse în legătură cu acestea.

Stocarea și prelucrarea informațiilor privind obiectele de evidență, înscrise în Registrul de Stat se realizează pe baza unor Dosare electronice generate automat.

Dosarele electronice de alertă și de incidente cibernetice conțin datele de identificare și datele descriptive ale raportului sau ale incidentului, parametrii de bază ai acestuia, manifestările, datele privind locurile de detectare sau de amenințare, entitatea care l-a înregistrat, rezultatele diagnosticului și ale analizei, deciziile luate și documentele pregătite pentru a contracara amenințările și a minimiza consecințele negative, precum și alte fișiere atașate de materiale și documente.

Pe parcursul ciclului de viață al gestionării incidentelor, datele din Dosarul incidentului cibernetic pot fi actualizate și pot fi adăugate informații suplimentare necesare. Pentru a accelera analiza, pregătirea documentelor de contracarare a amenințărilor și luarea deciziilor, SIA RSISC pune la dispoziția utilizatorilor responsabili materiale din baza de cunoștințe (descrieri și activități acumulate pe parcursul întregii perioade operaționale). Utilizatorul are posibilitatea de a le copia și de a modifica unele date, adică de a le actualiza la realitățile actuale.

Toate etapele de prelucrare a datelor Dosarului, stările trecute și persoanele care au luat măsuri cu privire la obiectele înregistrate sunt stocate în istoricul Dosarului. Dacă este necesar, se poate vizualiza întregul istoric al procesării unui Dosar de incident electronic.

Acțiunile de prelucrare a datelor de bază (editare) și acțiunile de luare a deciziilor sau de trimitere a mesajelor vor fi confirmate prin semnătura digitală electronică (SDE) a utilizatorului care a efectuat aceste acțiuni.

Documentele explicative sau de orientare (descrieri, politici, orientări, instrucțiuni etc.) pot fi atașate la elementele din dosarul electronic al incidentului, dacă este necesar, sub formă de fișiere electronice.

Sistemul de securitate SIA RSISC asigură stocarea de date despre toți utilizatorii sistemului, precum și gestionarea activităților, rolurilor, drepturilor și nivelurilor de acces ale acestora. SIA RSISC va permite, de asemenea, auditarea activităților utilizatorilor și a prelucrării datelor.

Toți utilizatorii înregistrați în SIA RSISC vor avea la dispoziție un birou privat, unde vor avea acces la datele și funcțiile sistemului în funcție de rolurile atribuite. Un tablou de bord personal va fi, de asemenea, pus la dispoziția utilizatorilor din biroul privat pentru vizualizarea informațiilor relevante, acces rapid la notificări și formulare legate de evenimentele și procesele de afaceri ale unui anumit rol.

Arhitectura SIA RSISC și ordinea de organizare a obiectelor informaționale permite, dacă este necesar, o extindere considerabilă a listei tipurilor de obiecte înregistrate (în Dosar), precum și modificarea ordinii de sprijinire a ciclului de viață și de prelucrare a obiectelor contabile.

SIA RSISC permite utilizatorilor (angajați ai structurilor autorizate) să efectueze căutări contextuale cu parametrii necesari în ceea ce privește obiectele contabile de bază (alerte, incidente, dosar, mesaj etc.) și documentele atașate acestora, să vizualizeze datele cazurilor și documentelor electronice, să gestioneze starea obiectelor de evidență, să ia decizii cu privire la acestea, să pregătească documente, să semneze datele și deciziile luate cu SDE, să verifice și să analizeze datele introduse, să verifice autenticitatea SDE, precum și să primească statisticile necesare. Toate acțiunile utilizatorii le pot efectua numai în limitele rolurilor, drepturilor și nivelurilor de acces date.
Informațiile privind datele, evenimentele și deciziile luate cu privire la Dosarele electronice și documentele anexate la acestea pot fi transmise organizațiilor și entităților autorizate relevante pentru alte acțiuni cu privire la acestea.

În timpul lucrului în SIA, va fi asigurată gestionarea drepturilor, accesului și activității utilizatorilor, iar toate acțiunile și evenimentele utilizatorilor din sistem vor fi înregistrate pentru analize ulterioare și luarea deciziilor de gestionare.

În cazul în care se înregistrează noi incidente, se iau decizii cu privire la acestea și se atribuie acțiuni sau apar alte evenimente definite în sistem (detectarea unor amenințări cibernetice repetate etc.), utilizatorii vor primi mesaje relevante (Notificare). Notificările vor fi, de asemenea, trimise utilizatorilor ca memento-uri pentru activitățile planificate și alte acțiuni necesare.

SIA RSISC va utiliza serviciile guvernamentale furnizate de Agenția de Guvernare electronică, cum ar fi: mCloud, mPass, mSign, mConnect, mLog, mNotify, mPower.

Pentru a obține date actualizate și pentru a verifica corectitudinea informațiilor, SIA RSISC va interacționa îndeaproape cu sistemele informatice automatizate ale entităților cooperante (definite prin Hotărârea de Guvern nr. 482/2020).
În plus, SIA RSISC poate furniza informații limitate privind resursele publice și a oferi servicii web pentru a interacționa cu alte sisteme informaționale.

RSISC va asigura lucrul asincrone a serviciilor și procesarea informațiilor 24 de ore din 24, 7 zile din 7.

RSISC va sprijini funcționarea în timp real a mai multor utilizatori.

5 Obiectele de evidență

Următoarele obiecte principale de evidență sunt definite în SIA RSISC:

- Avertisment privind securitatea cibernetică
- Incident de securitate cibernetică
- Dosarul incidentului
- Document (fișier generat sau atașat)
- Alerte
- Utilizator

Schema de organizare a obiectelor de informare și de utilizare a SIA RSISC este prezentată în figura 1.

Organizarea și interacțiunea obiectelor informaționale și elementelor în SIA RSISC

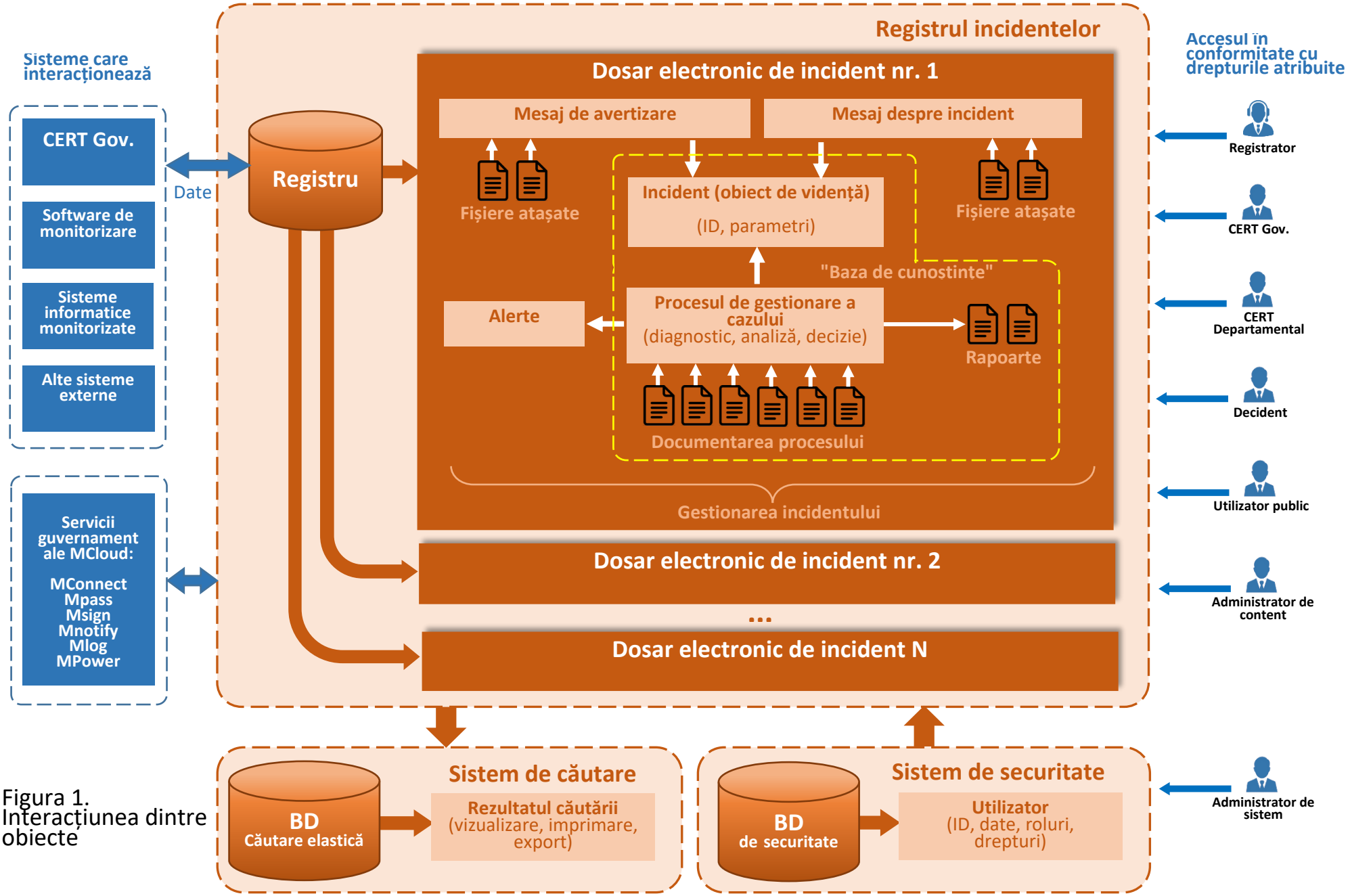

Figura 1. Interacțiunea dintre obiecte

Mesaj de incident/avertizare - un obiect generat de sistem atunci când se înregistrează un incident/avertizare (de către utilizator sau de către sistemele cooperante în mod automat), care conține informații de bază despre incidentul cibernetic, tipul, locația, ora, semnele de manifestare și alte informații, inclusiv fișiere atașate (capturi de ecran, descrieri, fragmente de cod etc.).

Dosar electronic de Incident - reprezintă un container electronic virtual care consolidează toate celelalte obiecte care descriu incidentul sau alerta curentă. Obiectul Dosar este creat automat de către sistem atunci când se raportează un nou incident sau o nouă alertă. Un Dosar este unic pentru Registru și se raportează la un incident ”unul la unu”, adică pentru fiecare incident se creează Dosarul "său".

Incident - identifică fără ambiguitate un Incident de securitate cibernetică înregistrat. Acesta conține toate datele despre evenimentul cibernetic curent (cine l-a înregistrat, unde a fost detectat, când), clasificarea, manifestările etc. La obiectul Incident pot fi atașate documente explicative (fișiere) - capturi de ecran, fragmente de cod, descriere etc.

De asemenea, descrie o Avertizare, adică probabilitatea ca o amenințare la adresa securității cibernetice să se materializeze, înregistrată în sistem. În acest caz, conține date privind comportamentul/ starea atipică a infrastructurii IT, manifestări externe etc.

Procesul de gestionare a dosarului - conține și descrie toate acțiunile care au fost efectuate în incidentul curent (investigație, diagnostic, analiză, decizii luate) și tehnicienii care au efectuat aceste acțiuni. Procesul de gestionare a dosarului poate fi însoțit de documente explicative (fișiere) - rezultatele studiului, descrierea impactului cibernetic, evaluarea riscurilor, deciziile luate și formulare pentru documentarea procesului de gestionare a dosarului.

Pe parcursul duratei de viață a sistemului, documentația elaborată a procesului de gestionare a dosarului se acumulează și formează o "bază de cunoștințe" pentru a face față amenințărilor și consecințelor neintenționate care au apărut. În acest fel, formularele/documentele dezvoltate o dată pot fi reutilizate pentru același tip de incidente în totalitate sau cu modificări minore.

Notificări - un obiect generat automat de sistem, care conține informații de bază despre incident/alertă, manifestările externe ale acestuia, posibilele consecințe etc. Acesta este conceput pentru a notifica utilizatorii și organizațiile cooperante cu privire la o amenințare cibernetică. Este trimis automat după înregistrare, decizie și atribuirea de acțiuni.

Utilizator - pentru fiecare utilizator înregistrat în sistem, se creează automat profilul acestuia, care conține date de identificare și informații despre utilizator. În plus, administratorul din profil gestionează activitatea și drepturile utilizatorului, atribuie roluri și drepturi suplimentare.

6 Domeniul de automatizare și structura a SIA RSISC

Din punct de vedere structural, SIA RSISC ar trebui să fie o soluție software autonomă, care comunică cu alte sisteme de informații prin intermediul serviciilor WEB și cu utilizatorii prin intermediul unei interfețe WEB.

SIA RSISC va pune la dispoziția utilizatorilor o interfață WEB accesibilă prin intermediul browserelor uzuale: MS Edge, Mozila FireFox, Opera, Google Chrome sau Safari.

Arhitectura RSISC va fi deschisă, ceea ce va permite dezvoltarea funcționalității sale în timp și va permite gestionarea diferitelor date electronice, precum și interoperabilitatea cu alte sisteme și module de informații.
De asemenea, va permite ca software-ul să fie scalabil, dacă este necesar, atât atunci când numărul de utilizatori crește, cât și atunci când crește cantitatea de informații gestionate.
Pentru a dezvolta cu succes componente pentru soluția actuală, SIA RSISC va utiliza soluții deschise, nepatentate, utilizate pentru aplicații WEB convenționale.

SIA RSISC este implementat în sistemul de stocare în cloud "mCloud" furnizat de Agenția de guvernare electronică.

Schema generală a SIA RSISC și interacțiunea elementelor între ele și cu alte sisteme este prezentată în figura 2.

Notă:
Această organigramă este doar un ghid pentru înțelegerea principiilor generale ale structurii și fluxului de informații RSISC SIA, dar nu prezintă interfețele cu utilizatorul sau mecanismele de interacțiune ale elementelor.

Structura SIA "Registrul de stat al incidentelor de securitate cibernetică"

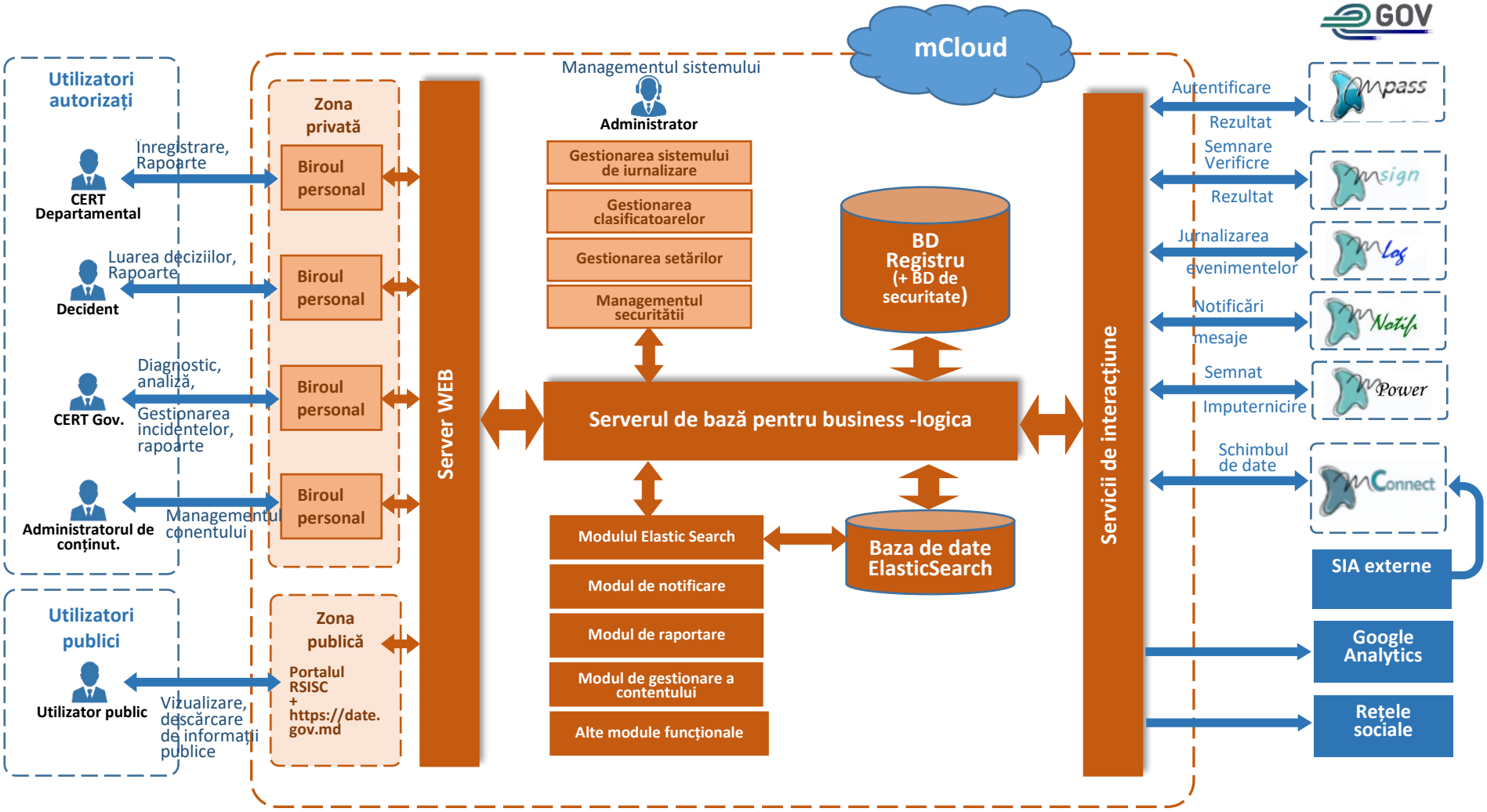

Figura 2: Structura SIA

Din punct de vedere structural, RSISC este conceput ca o soluție software de sine stătătoare, care interacționează cu alte sisteme informatice prin intermediul serviciilor WEB și cu utilizatorii prin intermediul unei interfețe WEB.

Arhitectura RSISC va permite ca funcționalitatea să crească în timp și să gestioneze diferite tipuri de date de intrare/ieșire (incidente, alerte de securitate cibernetică etc.).

- Arhitectura va utiliza soluții integrate, bazate pe cele mai bune practici din industria IT;
- Arhitectura sistemului va fi în mai multe niveluri cu delimitări foarte clare;
- Componentele sistemului vor fi relativ independente și vor interacționa între ele prin intermediul interfețelor selectate;
- Sistemul va avea posibilitatea să fie găzduită pe platforma guvernamentală MCloud;
- Acolo unde este posibil, modificările și parametrii sistemului nu vor influența asupra activității curente a sistemului, sesiunilor active, solicitări și altele;
- Arhitectura soluției software asigură un nivel înalt de accesibilitate la implementarea noilor versiuni, de asemenea, va avea posibilitatea de lansare concomitentă a mai multor exemplare;
- Modelul de date va fi descris și oferit beneficiarului în formatul convenit.

Din punct de vedere arhitectural, SIA RSISC reprezintă o structură standard din trei componente:

- BD
- serverul de aplicații (serverul de bază pentru business-logica)
- clientul subțire (serverul-web, aplicații-web)

precum și modulele auxiliare:

- servicii de interoperabilitate (pentru a permite comunicarea cu sistemele informatice externe)
- efectuarea căutării
- generarea de notificări
- generarea de rapoarte
- gestionarea contentului
- altele, care asigură funcționalitatea SIA RSISC

Serverul de aplicații furnizează logica de bază a RSISC și servește ca interfață între partea utilizatorului (client) și sistemele externe și baza de date a sistemului. Din punct de vedere funcțional, serverul de aplicații conține următoarele blocuri:

- blocul de asigurarea a business-logicii (toate funcționalitățile de bază ale SIA RSISC, și anume susținerea și gestionarea ciclului de viață al obiectelor de evidență, cererile de servicii web, asigurarea interacțiunii părții client cu baza

de date, gestionarea modulelor auxiliare, executarea verificărilor, selecțiile, gestionarea notificărilor, comunicarea cu sistemele externe etc.).
- blocul de securitate (gestionarea profilurilor, rolurilor, drepturilor și activităților utilizatorilor)
- blocul de jurnalizare (înregistrarea acțiunilor și evenimentelor utilizatorului în SIA RSISC, audit)
- blocul de gestionare a clasificatoarelor (întreținerea și actualizarea directoarelor și a clasificatorilor)
- blocul de gestionare a setărilor (gestionarea parametrilor, formularelor și șabloanelor comune SIA RSISC)

Din punct de vedere logic, baza de date este formată din două părți - Registrul propriu-zis (inclusiv informațiile de securitate) și baza de date Elastic Search.

7 Asigurarea software și hardware

Pentru a îndeplini cerințele sarcinii tehnice, SIA RSISC va fi desfășurată în 3 medii de operare:

- Mediu de producție;
- Mediu de testare/instruire;
- Mediu de dezvoltare.

Furnizarea de instrumente tehnice și software pentru aceste medii de operare este asigurată de furnizorul de infrastructură.

Licențele pentru software menționate în punctele 7.1.1.2, 7.1.2.2, 7.1.3.2, 7.2.1.2, 7.3.1.2, 7.3.1.2 care sunt desemnate în tabelele cu lista de software sunt furnizate de către solicitant și poartă mențiunea "Furnizat de către solicitant".

Implementarea complexului software și hardware în mediile de testare/instruire și de dezvoltare este asigurată de dezvoltatorul SIA RSISC, iar în mediul de producție de către dezvoltator împreună cu personalul solicitantului.

Platforma harware, formată din complexul tehnic de prelucrare și transportare a datelor, acesta fiind asigurat în sistemul MCloud.

Platforma MCloud ar trebui să ofere:

- Servere protejate redundant pentru hosting al bazelor de date, softului de sistem și softului funcțional (aplicații);

- Echipamente de comunicății pentru gormarea rețelelor locale LAN și organizarea comunicațiilor teritoriale WAN;
- Performanța optimă, pentru realizarea obiectivelor și asigurarea extinderii ulterioare a sistemului;
- Nivel corespunzător de securitate privind transportul de date.

7.1 Mediul de producție

Cerințele minime de configurare hardware pentru implementarea într-un mediu de producție, care trebuie să fie furnizate de furnizorul de infrastructură, sunt următoarele:

7.1.1 Server de aplicații

7.1.1.1 Parametrii tehnici minimi ai serverului

numărul de servere - 1 (*)

Numele parmetrului serverului	Valoare / descriere	Notă
Numărul fluxurilor de calcul al procesoarelor (buc.)	24	
Frecvența procesorului (GHz)	2,5	
Memoria RAM (GB)	128	
Spațiu liber pe disc (GB)	1000	
Capacitatea de transmisie a rețelei locale Mbit/s	1000	

(*) În cazul unei sarcini crescute a sistemului (dacă sunt instalate mai multe servere), echilibrarea sarcinii se va face cu Nginx. Configurația SIA RSISC va permite o scalare orizontală.

Echipamentele de server și de rețea trebuie să dispună de o sursă de alimentare neîntreruptă. Capacitatea UPS-ului trebuie să asigure funcționarea neîntreruptă a echipamentului în absența alimentării cu energie electrică timp de cel puțin 30 de minute. Vă recomandăm să monitorizați starea UPS-ului și să vă asigurați că serverele sunt oprite corect atunci când sunt deconectate.

7.1.1.2 Software

Pentru funcționarea SIA RSISC, pe server se instalează următoarele programe software:

Denumirea produsului software	Licența	Furnizrea

Microsoft Windows Server 2019, inclusiv IIS 10	Solicitantul alege orice tip de licență	Furnizat de către solicitant
ASP.NET Core Module/Hosting Bundle	MIT License	Furnizat de către solicitant
(*)Docker	Solicitantul alege orice tip de licență	Furnizat de către solicitant
(*)Nginx	Solicitantul alege orice tip de licență	Furnizat de către solicitant

(*) Notă: Solicitantul trebuie să implementeze și să configureze serviciile Docker, Docker Compose și să implementeze containerul cu balancer - Nginx

Pentru a asigura o performanță și o stabilitate optimă ale SIA RSISC, pe servere este interzis de a instala alte programe software, care nu sunt legate de funcționarea SIA RSISC.

7.1.2 Server de baze de date

7.1.2.1 Parametrii tehnici minimi ai serverului

numărul de servere - 1

Numele parmetrului serverului	Valoare / descriere	Notă
Numărul fluxurilor de calcul al procesoarelor (buc.)	12	
Frecvența procesorului (GHz)	2,5	
Frecvența procesorului (GHz)	32	
(*)Spațiu liber pe disc (GB)	2000	
Capacitatea de transmisie a rețelei locale Mbit/s	1000	

(*) Notă: Atunci când se procesează mai mult de 10 000 de incidente în SIA RSISC sau se primesc și se stochează mai mult de 100 000 000 de notificări anual este necesar de mărit spațiu pe disc.

Echipamentele de server și de rețea trebuie să dispună de o sursă de alimentare neîntreruptă. Capacitatea UPS-ului trebuie să asigure funcționarea neîntreruptă a echipamentului în absența alimentării cu energie electrică timp de cel puțin 30 de minute. Vă recomandăm să monitorizați starea UPS-ului și să vă asigurați că serverele sunt oprite corect atunci când sunt deconectate.

Ar trebui să se utilizeze masive de discuri cu toleranță la erori (RAID). Se recomandă să se asigure o resursă externă (rețea sau disc) pentru stocarea copiilor de rezervă ale bazei de date și a fișierelor SIA RSISC.

7.1.2.2 Software

Pe server este instalat următorul software:

Denumirea produsului software	Licența	Furnizrea

Microsoft Windows Server 2019, inclusiv Microsoft SQL Server Report Services	Standard Edition	Furnizat de către solicitant
SQL Server Management Studio	Additional software	Furnizat de către solicitant
Elastic Search	Free and open - Basic	Furnizat de către solicitant

Pentru a asigura o performanță și o stabilitate optime ale SIA RSISC, pe servere nu poate fi instalat niciun alt software care nu este legat de funcționarea SIA RSISC.

7.1.3 Server Hardbeat

Hardbeat va monitoriza în permanență funcționarea diferitelor noduri din sistem și va notifica administratorul în cazul unor defecțiuni ale elementelor.

7.1.3.1 Parametrii tehnici minimi ai serverului

numărul de servere - 1

Numele parmetrului serverului	Valoare / descriere	Notă
Numărul fluxurilor de calcul al procesoarelor (buc.)	12	
Frecvența procesorului (GHz)	2,5	
Frecvența procesorului (GHz)	32	
(*)Spațiu liber pe disc (GB)	600	
Capacitatea de transmisie a rețelei locale Mbit/s	100	

7.1.3.2 Software

Pentru a opera sistemul de monitorizare Hardbeat, următorul software este instalat pe server:

Denumirea produsului software	Licența	Furnizrea
Elastic HeartBeat	Free and open - Basic	Furnizat de către solicitant

7.2 Mediu de testare/instruire

Cerințele minime de configurare hardware pentru implementarea într-un mediu de testare/instruire, care trebuie să fie asigurat de furnizorul de infrastructură, sunt următoarele:

7.2.1 Server de aplicații și baze de date

7.2.1.1 Parametrii tehnici minimi ai serverului

numărul de servere - 1

Numele parmetrului serverului	Valoare / descriere	Notă
Numărul fluxurilor de calcul al procesoarelor (buc.)	24	
Frecvența procesorului (GHz)	2,5	
Frecvența procesorului (GHz)	128	
(*)Spațiu liber pe disc (GB)	2000	
Capacitatea de transmisie a rețelei locale Mbit/s	1000	

Echipamentele de server și de rețea trebuie să dispună de o sursă de alimentare neîntreruptă. Capacitatea UPS-ului trebuie să asigure funcționarea neîntreruptă a echipamentului în cazul unei pene de curent timp de cel puțin 10 minute.

7.2.1.2 Software

Pe server este instalat următorul software:

Denumirea produsului software	Licența	Furnizrea
Microsoft Windows Server 2019, inclusiv IIS 10	Solicitantul alege orice tip de licență	Furnizat de către solicitant
ASP.NET Core Module/Hosting Bundle	MIT License	Furnizat de către solicitant
(*)Docker	Solicitantul alege orice tip de licență	Furnizat de către solicitant
(*)Nginx	Solicitantul alege orice tip de licență	Furnizat de către solicitant
Microsoft SQL Server 2019, inclusiv Microsoft SQL Server Report Services	Standard Edition	Furnizat de către solicitant
SQL Server Management Studio	Additional software	Furnizat de către solicitant
Elastic Search	Free and open - Basic	Furnizat de către solicitant

(*) Notă: Solicitantul trebuie să implementeze și să configureze serviciile Docker, Docker Compose și să implementeze containerul cu balancer - Nginx

Pentru a îndeplini cerințele caietului de sarcini, pe server pot fi instalate produse software suplimentare pentru a testa RSISC SIA (software de scripting, teste de încărcare etc.), precum și pentru a demonstra sistemul prototip, materialele de instruire și documentele tehnice.

7.3 Mediu de dezvoltare

Cerințele minime de hardware pentru mediul de dezvoltare care urmează să fie asigurate de furnizorul de infrastructură sunt următoarele:

7.3.1 Server de dezvoltare

7.3.1.1 Parametrii tehnici minimi ai serverului

numărul de servere - 1

Numele parmetrului serverului	Valoare / descriere	Notă
Numărul fluxurilor de calcul al procesoarelor (buc.)	24	
Frecvența procesorului (GHz)	2,5	
Memoria RAM (GB)	32	
Spațiu liber pe disc (GB)	600	
Capacitatea de transmisie a rețelei locale Mbit/s	1000	

Echipamentele de server și de rețea trebuie să dispună de o sursă de alimentare neîntreruptă. Capacitatea UPS-ului trebuie să asigure funcționarea neîntreruptă a echipamentului în cazul unei pene de curent timp de cel puțin 10 minute.

7.3.1.2 Software

Pe server este instalat următorul software:

Denumirea produsului software	Licența	Furnizrea
Microsoft Windows Server 2019, inclusiv IIS 10	Solicitantul alege orice tip de licență	Furnizat de către solicitant
ASP.NET Core Module/Hosting Bundle	MIT License	Furnizat de către solicitant
Docker	Solicitantul alege orice tip de licență	Furnizat de către solicitant
Microsoft SQL Server 2019, inclusiv Microsoft SQL Server Report Services	Standard Edition	Furnizat de către solicitant
SQL Server Management Studio	Additional software	Furnizat de către solicitant
Elastic Search	Free and open - Basic	Furnizat de către solicitant
Microsoft Visual Studio Community 2022	Free to use	Furnizat de către solicitant
Kendo UI	Developer License	Furnizat de către solicitant
JQuery	MIT License	Furnizat de către solicitant
Bootstrap	free end product	Furnizat de către solicitant
(*)Umbraco	MIT License	Furnizat de către solicitant

(*) Notă: Platforma Umbraco va fi utilizată pentru a dezvolta și gestiona versiunea publică a portalului (SIA RSISC Public).

Pentru a îndeplini cerințele sarcinei tehnice, pe serverul de dezvoltare pot fi instalate produse software suplimentare pentru a permite dezvoltarea, integrarea, depanarea și testarea colectivă a SIA RSISC.

7.4 Cerințe recomandate pentru stațiile clienților

Echipament recomandat:

- sistem de operare: Windows 7/8/10;
- frecvența procesorului: cel puțin 2 GHz. Dual Core;
- memoria RAM: cel puțin 4 Gb;
- hard disk: cel puțin 15 Gb de spațiu liber pe disc;
- ecran: cel puțin 17", rezoluție 1920x1080 (rezoluție minimă: 1360x468).
- prezența unei cartele de rețea (conexiune la rețelele de date);

Software instalat

- Browsere web recomandate pentru SIA RSISC: MS Edge, Mozila FireFox, Opera, Google Chrome sau Safari;
- Pachetul MS Office instalat (MS Office versiunea 2003 sau o versiune superioară).

7.5 Stiva tehnologică

Soluția va fi dezvoltată utilizând ultimele versiuni ale următoarelor stive tehnologice:

- Limbaj de programare: C#
- Soluție ORM: Entity Framework Core.
- Cadrul web: ASP.NET MVC Core.
- SGBD: Microsoft SQL Server.
- Server de poștă: asigura de Benificiarului
- Organizarea căutării: Elastic Search
- Generarea de rapoarte: Microsoft Report Services
- Dezvoltarea și gestionarea mediului public: Umbraco
- Pentru dezvoltarea interfeței utilizatorilor: HTML, CSS, JavaScript, Jquery, Kendo UI, bootstrap

În procesul de dezvoltare a SIA RSISC poate fi propuse unii componente adiționale necesare pentru dezvoltarea și funcționalitatea adecvată a soluției în producție.

7.6 Software de schimbare a codului (de către beneficiar)

Software-ul necesar pentru a efectua modificări ale codului programului și pentru a-l recompila la nivel intern cu puterile proprii ale solicitantului:

- Microsoft Visual Studio Community 2022
- Microsoft SQL Server Developer 2019
- Kendo UI
- Umbraco

8 Etapele de implementare a SIA RSISC

Activitățile de proiectare, dezvoltare, testare și implementare a SIA RSISC vor fi realizate în conformitate cu cerințele Reglementării tehnice RT 38370656-002:2006 „Procesele ciclului de viață al software-ului”, aprobată prin ordinul Ministerului Tehnologiei Informației și Comunicațiilor nr.78/2006, pe baza experienței de mulți ani a DAAC System Integrator în implementarea unor astfel de sisteme.

Modelul ciclului de viață al sistemului software va consta din următoarele etape:

1. Etapa de dezvoltare a sistemului IT
2. Etapa de instruire
3. Etapa de stabilizare și punere în funcțiune a SIA RSISC
4. Etapa de suport de garanție

Toate activitățile și planul calendaristic pentru punerea în aplicare a fiecărei etape vor fi convenite cu Solicitantul.

8.1 Etapa 1. Dezvoltarea sistemului IT

Etapa va implica următoarele procese principale:

- dezvoltarea specificațiilor cerințelor și proiectarea structurală
- dezvoltare și integrare de software
- migrarea și completarea inițială a datelor
- testarea calificativă (inclusiv înlăturarea problemelor)
- implementarea sistemului în trei medii (dezvoltare, testare și instruire, producție)

În procesul de "Elaborare a specificațiilor privind cerințele și proiectare structurală" vor fi în mod suficient de detaliat clarificate cerințele solicitantului, nevoile, dorințele și așteptările părților interesate și va dezvolta o soluție de proiectare pentru implementare. Artefactele de ieșire ale acestui proces vor fi o Specificația cerințelor și Proiectul tehnic (SRS și SDD). Specificația cerințelor va fi aprobată de către Solicitant și va fi singurul criteriu de evaluare a produsului software în momentul acceptării.
De asemenea, se va elabora o soluție tehnică care să îndeplinească cerințele sistemului software. Se va elabora arhitectura sistemului software și diagrama structurală a acestuia cu asocierile dintre elemente, se vor defini interfețele externe sistemului și între componentele sistemului însuși. Artefactul de ieșire al acestui proces va fi un Proiect tehnic. Proiectul tehnic este aprobat de către dezvoltator.

Durata de realizare este de 1 lună.

În timpul procesului de "Dezvoltare și integrare software", codul software al elementelor sistemului va fi dezvoltat și modulele dezvoltate vor fi integrate în versiunea demo SIA RSISC. Prototipul SIA RSISC SIA și funcționalitatea acestuia vor fi demonstrate clientului. După demonstrație, SIA RSISC va fi perfecționat până la o versiune complet funcțională. Artefactul de ieșire al acestui proces va fi un prototip de sistem software.

Durata de implementare este de 6 luni.

În procesul de "Migrarea datelor și completarea inițială", se vor completa clasificatorii și directoarele. Datele pentru completarea clasificatorilor vor fi primite de la proprietarii acestora (surse primare), câmpurile vor fi completate, corectate sau adaptate, iar integritatea și coerența vor fi verificate. Artefactul de ieșire al acestui proces vor fi clasificatoarele și nomenclatoarele actualizate ale sistemului.

Timp de implementare - 1 lună

În procesul "testării calificative" a SIA RSISC, se va demonstra că caracteristicile și funcționalitatea produsului software îndeplinesc cerințele stipulate ale sistemului software, conform cărora produsul a fost implementat. Se vor efectua următoarele verificări:

- testarea funcțională a produsului software în conformitate cu scenariile convenite pentru conformitatea cu cerințele SRS și SDD
- teste de sarcină și de stres, simulând sarcini asupra produsului software mai mari decât vârfurile de sarcină ale procesului operațional
- comoditatea de utilizare a software-ului și ușurința de utilizare a interfeței utilizatorului

Pe baza rezultatelor testelor, se vor lua măsuri corective pentru a corecta neconformitățile. În această etapă se va pregăti, de asemenea, un set de documentație tehnică de sprijin și alte artefacte necesare.

Durata de implementare este de 3 săptămâni.

În timpul procesului "Implementarea în 3 medii" a SIA RSISC va fi implementat și configurat în 3 medii:

- Mediul de producție,
- Mediul de testare/instruire,
- Mediul de dezvoltare

Durata de implementare este de 1 săptămână.

8.2 Etapa 2: Instruirea

Etapa va implica următoarele procese principale:

- pregătirea materialelor de instruire
- efectuarea instruirii personalului solicitantului

În cadrul procesului „Pregătirea materialelor de instruire”, se va stabili ora desfășurăriii sesiunilor, se vor desemna persoanele pentru instruie și se vor repartiza în grupuri de instruire, va fi pregătit și aprobat planul calendaristic al cursurilor, vor fi elaborate materiale de instruire și vor fi întocmite certificate.

În procesul ”Instruirea personalului solicitantului” vor fi formate trei grupuri:

- 1 grup – 2 administratori de sistem
- 2 grup - 2 instructori (pentru instruirea ulterioară a altor utilizatori)
- 3 grup - 30 de utilizatori (pentru toate rolurile configurate)

Formatul desfășurării cursurilor este on-line. Solicitantul va trebui să ofere angajaților săi mijloace tehnice (pentru desfășurarea cursurilor on-line) și să asigure prezența acestora la cursuri.
Artefactele de ieșire ale acestui proces vor fi borderoul de admitere a persoanelor instruite și certificatele emise.

8.3 Etapa 3: Stabilizarea SIA RSISC

Etapa începe din momentul semnării actului de punere în exploatarea de producere a sistemului.

Etapa include acțiuni pentru începerea utilizării SIA RSISC. Această etapă trebuie să demonstreze pregătirea deplină a SIA RSISC, a infrastructurii solicitantului și a utilizatorilor pentru exploatarea de producere. În faza de stabilizare, furnizorul va acorda asistență și consultanță utilizatorilor, iar în caz de erori sau deficiențe (în cadrul specificației tehnice aprobate), va corecta și optimiza parametrii de funcționare ai SIA RSISC.
Artefactul de ieșire al acestei etape va fi Certificatul de punere în exploatare al SIA RSISC.
Timp de implementare - 3 luni.

8.4 Etapa 4: Suportul de garanție

Etapa începe din momentul semnării actului de punere în exploatarea de producere a sistemului.
Această etapă implică acțiuni de menținere a capacității sistemului software de a furniza serviciile necesare. În această etapă, produsul software este monitorizat, problemele sunt înregistrate pentru analiză în jurnalul de înregistrare a adresărilor și se iau măsuri preventive și corective. Pentru a elimina problemele, poate fi efectută o modificare (schimbare) a textului sau a setărilor software (în cadrul contractului și al cerințelor din specificația tehnică aprobată). Artefactele de ieșire din această etapă vor fi un jurnal de evidență a adresărilor, o versiune funcțională a SIA RSISC și documente justificative.

Durata de implementare este de 12 luni.

9 Planul preliminar al proiectului

9.1 Schema organizării lucrărilor

Structura activității de nivel înalt a proiectului este prezentată mai jos:

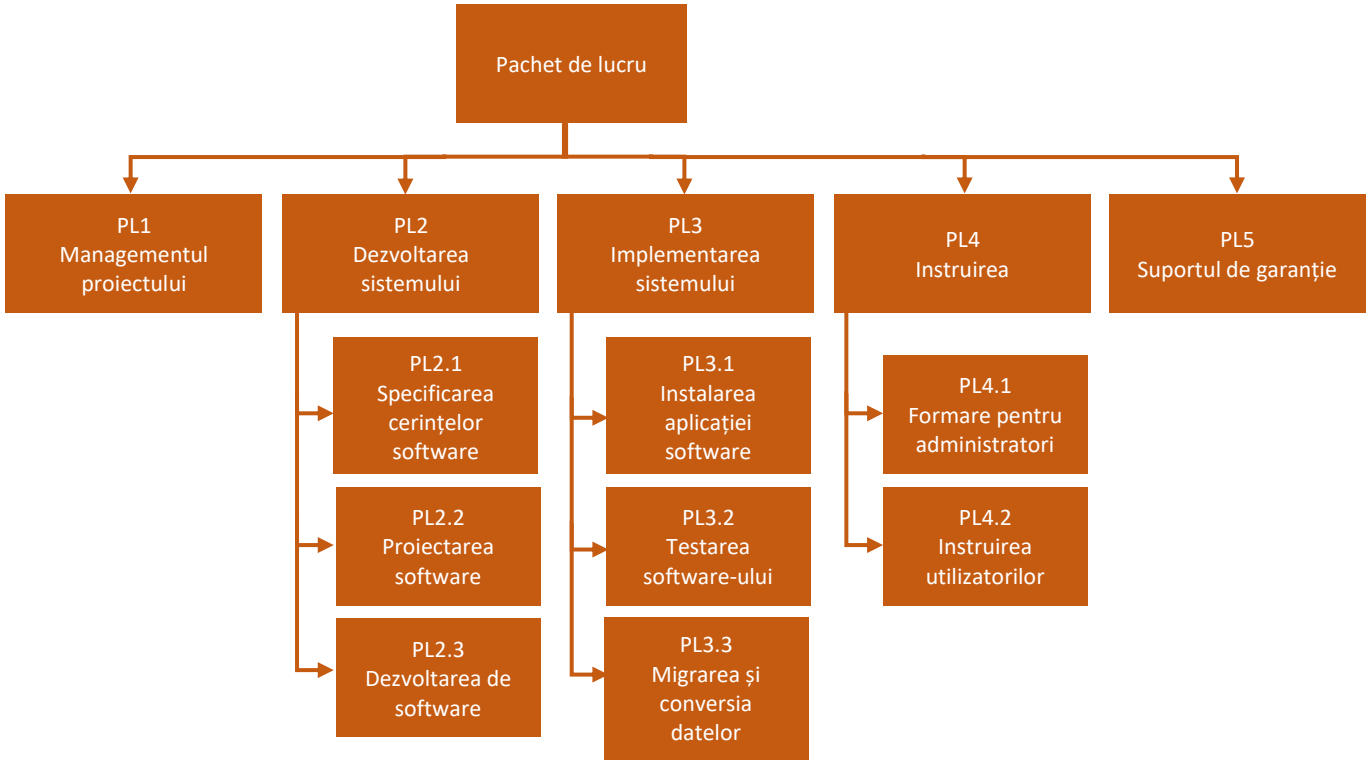

Figura 3: Modelul funcțional al sistemului

9.2 Etape de proiect

Următoarele servicii vor fi furnizate solicitantului pe durata implementării SIA RSISC:

Etapa	Nr.	Denumirea serviciului	Durata
Etapa 1: **Elaborarea sistemului informatic**	1	Elaborarea unei specificații a cerințelor software și proiectarea sistemului de bază	1 lună
	2	Dezvoltarea de software, inclusiv elaborarea de documentație tehnică	6 luni
	3	Migrarea datelor, inclusiv completarea inițială a datelor	1 lună
	4	Testare software	3 săptămâni
	5	Desfășurarea SIA RSISC	1 săptămână
Etapa 2: **Instruirea**	6	Instruirea personalului solicitantului	
Etapa 3: **Stabilizarea SIA RSISC**	7	Facilitarea și asistarea la punerea în funcțiune a sistemului	3 luni
Etapa 4: **Suportul de garanție**	8	Suport de garanție SIA RSISC, concometent cu etapa "Stabilizarea SIA RSISC "	12 luni

9.3 Managementul proiectelor

PL1 Managementul proiectelor

Activități	Activitățile de management de proiect sunt următoarele • Pregătirea unui plan de proiect. • Monitorizarea progresului proiectului și respectarea calendarului proiectului. • Desemnarea resurselor proiectului. • Monitorizarea implementării proiectului în limitele bugetului. • Participarea la întâlnirile cu solicitantul (întâlniri cu echipa de management, întâlniri lunare pe timpul lucrărilor și întâlniri tehnice, dacă este necesar). • Întocmirea rapoartelor lunare, trimestriale și finale. • Gestionarea problemelor. • Gestionarea riscurilor. • Instruirea personalului cu privire la procedurile care trebuie urmate în cadrul proiectului. • Asigurarea conformității cu procedurile stabilite.
Rezultatele obținute	• Un plan de proiect care să conțină următoarele capitole o Structura organizatorică detaliată a proiectului; o Planul de gestionare a proiectului; o Calendarul detaliat de punere în aplicare; o Un plan de proiectare, dezvoltare și implementare a software-ului aplicației; o Graficul detaliat de punere în aplicare; o Planul de instruire; o Planul realizării experimantale; o Planul de punere în funcțiune și acceptare operațională; o Planul de transfer/migrație a datelor; o Planul de coordonare și de rotație; o Plan de asistență tehnică; o Planificarea sarcinilor, a timpului și a resurselor; o Planul de realizare a implementării; o Plan de servicii de suport de garanție. • Rapoarte lunare privind lucrările efectuate. • Rapoarte trimestriale. • Raport final pe proiect.

9.4 Dezvoltarea sistemului

PL2.1 Specificarea cerințelor software

Descrierea lucrării	Conceptul sistemului, analiza, dezvoltarea și documentarea cerințelor tehnice detaliate pentru SIA RSISC.
Activități	• Definirea business-cerințelor de bază ale sistemului (realizarea de sondaje de opinie pentru utilizatori, colectarea de informații); • Analiza business-cerințelor esențiale identificate pentru sistem; • Elaborarea unei specificații a cerințelor software.

Rezultatele obținute	Specificația cerințelor software (SCS), conține următoarele informații în conformitate cu cerințele licitației și cu cerințele Regulamentului RM PT-38370656 - 002:2006 "Ciclul de viață al software-ului":
	• Introducere
	  ○ Scopul
	  ○ Volumul produsului
	  ○ Definiții și abrevieri
	  ○ Recomandări
	• Descrierea sistemului actual
	  ○ Structura organizatorică
	  ○ Model de date
	  ○ Model funcțional
	  ○ Probleme
	• Modelul logic al sistemului țintă
	  ○ Model de date (set de diagrame UML cu descrieri detaliate)
	  ○ Dicționar de date
	  ○ Model funcțional (un set de diagrame UML cu o descriere detaliată)
	• Descriere generală
	  ○ Funcțiile produsului
	  ○ Specificațiile utilizatorului
	  ○ Restricții generale
	  ○ Ipoteze și dependențe
	• Cerințe speciale
	  ○ Cerințe funcționale
	  ▪ Cerința funcțională 1
	  • Introducere
	  • Intrări
	  • Procesare (diagramă UML cu descriere detaliată)
	  • Ieșiri
	  ▪ Cerința funcțională 2
	  • Introducere
	  • Intrări
	  ▪ ...
	  ▪ Cerință funcțională n
	  ▪ ...
	  ▪ Interfețe externe
	  • Interfețe utilizator
	  • Interfețe hardware
	  • Interfețe software
	  • Interfețe de comunicare
	  ○ Cerințe de performanță și capacitate
	  ▪ Limite ale dezvoltării
	  • Conformitatea cu standardele
	  • Limite hardware
	  ▪ Atribute
	  • Simplitatea de utilizare
	  • Accesibilitate
	  • Transferabilitate/conversie
	  • Fiabilitate
	  ▪ Alte cerințe
	  • Specificațiile bazei de date

	• Securitate • Restabilirea performanței • Suport operațional • Distributiv • Instalare • Documentație • Instruire • Anexe

PL2.2 Proiectarea de software

Descrierea lucrului	Proiectarea funcționalității și a datelor SIA RSISC
Activități	• Arhitectura sistemului de design; • Proiectarea structurii bazei de date a sistemului; • Proiectarea componentelor structurii funcționale a sistemului; • Proiectarea interfeței utilizatorului; • Proiectarea interfețelor pentru schimbul cu alte sisteme și resurse; • Elaborarea unei descrieri a proiectării software.
Rezultatele obținute	Descrierea proiectului software (DPS), care conține informații în conformitate cu cerințele sarcinei tehnice și cu prevederile reglementărilor tehnice PM PT-38370656 - 002:2006 "Ciclul de viață al software-ului": • Introducere o Scopul o Termeni și abrevieri o Recomandări • Descriere detaliată a modelului (set de diagrame UML cu descrieri detaliate) o Descompunerea modulelor ▪ Modulul 1 Descriere ▪ Modulul 2 Descriere ▪ ... • Decompoziția datelor (set de diagrame UML cu descrieri detaliate) o Obiect de date 1 Descriere o Obiect de date 2 Descriere o ... • Descrierea dependenței (un set de diagrame UML cu o descriere detaliată) o Dependențe între module o Legături de date • Descrierea interfeței (set de diagrame UML cu o descriere detaliată) o Interfața modulului 1 o Modulul 1 Descriere o Modulul 2 Descriere... • Proiectare detaliată (set de diagrame UML cu descrieri detaliate) o Proiect de lucru al modulelor ▪ Modulul 1 detaliere ▪ Modulul 2 detaliere ▪ ...

	○ Proiectarea datelor ▪ Obiect de date 1 detaliere ▪ Obiect de date 2 detaliere ▪ ... • Destributiv (set de diagrame UML cu descrieri detaliate) ○ Descrierea programelor auxiliare ○ Pachet de instalare • Note • Anexe

PL2.3 Dezvoltarea de software

Descrierea lucrului	Pe baza specificației cerințelor software (SRS) și a proiectului tehnic al software-ului (SDD), se va elabora SIA RSISC.
Activități	• Dezvoltarea efectivă a codului (codificare), depanarea și testarea internă a software-ului aplicației SIA RSISC utilizând instrumente și metode corespunzătoare în conformitate cu SRS și SDD aprobate. • Elaborarea manualului de instalare și configurare pentru sistemul de aplicații; • Elaborarea Ghidului utilizatorului; • Elaborarea unui plan pentru testarea funcțională, de stres și de rezistență.
Rezultatele obținute	• Module executabile ale software-ului de aplicație; • Planul de testare funcțională, de încărcare și de stres conține scenarii de testare funcțională și specificații pentru testarea de încărcare și de stres; • Ghidul de instalare și configurare pentru sistemul de aplicații, care conține: ○ Introducere; ○ Terminologie și abrevieri; ○ Cerințe privind echipamentul; ○ Complect de instalare. Modulele suplimentare, bibliotecile și producătorii terți necesari și versiunea acceptabilă a acestora; ○ Instrucțiuni de instalare; ○ Descriere a setărilor necesare; ○ Lista mesajelor și acțiunilor cheie. • Ghidul utilizatorului, care conține: ○ Instrucțiuni pentru utilizator, care conțin o introducere, o descriere a interacțiunii utilizatorului cu sistemul și o descriere a tuturor scenariilor de utilizare a sistemului; ○ Scopul și descrierea sistemului; ○ Caracteristici de intrare/ieșire; ○ Modele de documente de intrare și exemple pentru toate formatele de intrare (forme vizuale); ○ Modele ale tuturor documentelor de ieșire (formulare, rapoarte sau prezentări); ○ Instrucțiuni pentru introducerea datelor; ○ Link-uri către toate documentele sau manualele destinate utilizatorilor; ○ O descriere a limitelor sistemului;

	○ O descriere a tuturor situațiilor eronate, care pot apărea și a modului de reacție.

9.5 Implementarea sistemului

PL3.1 Instalarea software-ului pro-aplicație

Descrierea lucrului	Configurarea, instalarea și testarea componentelor software SIA RSISC în infrastructura pusă la dispoziție de către solicitant
Activități	• Extragerea componentelor software din mediul de dezvoltare; • Instalarea modulelor în mediul de producție; • Configurarea modulului de autentificare; • Configurarea datelor și a parametrilor sistemului; • Asigurarea securității (atribuirea de roluri corespunzătoare utilizatorilor); • Verificarea instalării software-ului (efectuarea de interogări specifice asupra bazelor de date pentru a determina caracterul complet al migrării); • Executarea scenariilor indicative/reprezentative; • Configurarea bazei de date și a serverelor de aplicații (numărul de sesiuni, parametrii de paralelism etc.); • Implementarea bazei de date fizice (dimensiunea și dispunerea discurilor, indexarea etc.)
Rezultatele obținute	Instalarea verificată a componentelor software SIA RSISC în infrastructura solicitantului

PL3.2 Testarea software

Descrierea postului	Testarea funcțională, de încărcare și de stres SIA RSISC.
Activități	• Instruirea utilizatorilor în domeniul testării funcționale; • Pregătirea scenariilor de testare • Pregătirea datelor și a materialelor pentru testare • Efectuarea de teste funcționale ale software-ului SIA RSISC; • Efectuarea testelor de încărcare a software-ului SIA RSISC • Efectuarea testelor de stres SIA RSISC • Analiza rezultatelor testelor; • Corectarea erorilor; • Configurarea platformei de operare SIA RSISC.
Rezultatele obținute	• Protocolul privind rezultatele testelor SIA RSISC; • Cod software corectat; • Actul de acceptare SIA RSISC .

PL3.2 Migrarea și conversia datelor

Descrierea lucrului	Realizarea umplerii inițiale a directoarelor și clasificatoarelor SIA RSISC, conversia datelor din surse primare (dacă este necesar) .
Activități	• Obținerea accesului la sursele primare de clasificatoare și directoare; • Începerea procedurii de completare inițială a metadatelor; • Conversia datelor, dacă este necesar;

	• Verificarea integrității și coerenței metadatelor; • Verificarea mecanismelor de actualizare automată a datelor clasificatoarelor;
Rezultatele obținute	• Completarea metadatelor SIA RSISC;

9.6 Instruirea

PL4.1 Instruirea pentru administratori

Descrierea lucrului	Planificarea, organizarea și efectuarea instruirii pentru administratorii sistemului dezvoltat vor face parte din acest pachet de lucru.
Activități	• Pregătirea unui plan de instruire detaliat; • Pregătirea materialelor de instruire; • Desfășurarea cursurilor de instruire în conformitate cu planul de instruire pregătit. Pentru mai multe informații, consultați secțiunea ”Planul de instruire” din prezentul document.
Rezultatele obținute	• Planul de instruire, astfel cum este descris în secțiunea "Planul de instruire" din prezentul document. • Materiale didactice. • Borderoul de punctaj a instruirii administratorilor

PL4.2 Instruirea utilizatorilor

Descrierea lucrului	Planificarea, organizarea și desfășurarea instruirii utilizatorilor vor fi realizate în cadrul pachetului de lucru.
Activități	• Pregătirea unui plan de instruire detaliat (actualizarea materialelor de instruire); • Pregătirea materialelor de instruire; • Desfășurarea cursurilor de instruire în conformitate cu planul de instruire pregătit. Pentru mai multe informații, consultați secțiunea ”Planul de instruire” din acest document.
Rezultatele obținute	• Planul de instruire, așa cum este descris în "**Ошибка! Источник ссылки не найден.**" din prezentul document. • Materiale didactice. • Borderoul de punctaj a instruirii utilizatorilor.

9.7 Garanție

Descrierea lucrului	Descrierea metodologiei Furnizorului pentru asigurarea cerințelor de suport de garanție a sistemului în conformitate cu Contractul și cu Cerințele tehnice.
Activități	• Asistență tehnică; • Serviciul de garanție; • Asistență pentru utilizatori/ linie fierbinte pentru utilizatori; • Consultanță tehnică. Pentru mai multe informații, consultați secțiunea "Planul de asistență tehnică a sistemului" din prezentul document.

Rezultatele obținute	Servicii de garanție

10 Personalul implicat în proiect

Personalul companiei DAAC SYSTEM INTEGRATOR S.R.L., care este responsabil pentru dezvoltarea și livrarea sistemului țintă, în general corespunde cerintelor stabilite.

Echipa de lucru va fi formată din personal cheie și non-cheie.

10.1 Personalul cheie implicat în proiect

Nr.	Rolul	Calificări	Nume
1	Manager de proiect	• Elaborarea de documente organizaționale și de management • Organizarea lucrărilor • Definirea unei strategii de implementare • Organizarea comunicării cu solicitantul • Determinarea cerințelor de resurse • Identificarea riscurilor • Organizarea unui sistem de gestionare a cerințelor • Elaborarea unui plan și a unui calendar de gestionare a proiectului • Coordonarea și aprobarea proiectului tehnic • Monitorizarea punerii în aplicare a planului • Analiza rezultatelor testelor • Pregătirea și aprobarea documentelor de predare a SIA RSISC către solicitant.	Sirbi I.
2	System Architect / Business Analyst	• Dezvoltarea funcționării SIA • Construirea unui model de business-procese automatizate • Definirea business - entităților, a obiectelor din sistem și a rolurilor • Definirea arhitecturii sistemului software și a interacțiunii acestuia cu alte sisteme • Determinarea limitelor necesare • Elaborarea limitelor proiectului și a cerințelor de calificare • Elaborarea unui proiect tehnic	Paprotkii I.
3	Dezvoltator / Administrator Bază de date	• Elaborarea de clase • Identificarea asociațiilor dintre clase (obiecte) • Dezvoltarea artefactelor • Dezvoltarea de baze de date • Dezvoltarea de mecanisme de conversie (transfer) a datelor • Transfer de date • Administrarea SGBD	Ustica A.
4	Software Developer / Integration Expert	• Dezvoltarea unui sistem software • Dezvoltarea de convertoare de date • Efectuarea de teste interne	Surcov V.

5	Software Developer / DevOps Expert	• Planificarea integrării elementelor sistemului de programe • Integrarea și asamblarea sistemului, definirea dependențelor • Analiza conflictelor din cod • Identificarea și fixarea relizelor, înregistrarea versiei • Desfășurarea și lansarea SIA RSISC pentru testare și într-un mediu de lucru • Automatizarea proceselor de implementare a sistemului • Pregătirea pachetului de distribuție	Anisimov G.
6	Software Tester	• Verificarea calității codului • Efectuarea de teste funcționale • Efectuarea testelor de încărcare • Efectuarea de teste de interfață a utilizatorului	Caldare A.
7	Trainer	• Pregătirea unui plan de instruire • Pregătirea materialelor de instruire și a testelor • Desfășurarea de sesiuni de instruire a personalului • Analiza rezultatelor procesului de instruire	Ciobanu A.

10.2 Personalul non-cheie implicat în proiect

Nr.	Rolul	Funcții principale	Nume
1	Designer	• Dezvoltarea formelor vizuale • Dezvoltarea prototipului SIA RSISC	Oleinic A.

Pentru fiecare membru al echipei sunt anexate CV-uri, care confirmă calificările și experiența.

11 Metodologia de dezvoltare a software-ului

Metodologia care urmează să fie utilizată pentru dezvoltarea SIA RSISC este exprimată în termeni de metodologie de dezvoltare a sistemului bazată pe procese. Un proces este un set coerent de sarcini legate între ele care au ca rezultat unul sau mai multe rezultate cheie. Elementele interfeței cu utilizatorul vor fi conforme la nivelul A cu cerințele Instrucțiunii privind accesibilitatea conținutului web (WCAG) 2.0. Metodologia de dezvoltare a software-ului pentru SIA RSISC include următoarele procese pentru a realiza activitățile de dezvoltare și a furniza rezultatele corespunzătoare:

11.1 Analiza cerințelor pentru software

Acest proces asigură o înțelegere clară a cerințelor și așteptărilor Solicitantului în ceea ce privește software-ul aplicației. Este un set de activități care se desfășoară periodic:

- Colectarea documentației existente. Materialul colectat include o listă de forme și documente vizuale, cum ar fi:
    - Toate legile, actele legislative și alte documente relevante în vigoare, publicate și care reglementează aplicarea SIA RSISC;
    - Toate instrucțiunile interne relevante, descrierile și regulile business-proceselor;
    - Toate șabloanele de formulare, rapoarte și documente de ieșire utilizate în business-procesele relevante, cu descrierea atributelor și a regulilor de generare și validare a acestora.
    - Acțiunile, sarcinile și domeniile de responsabilitate ale utilizatorilor.
- Interviurile și întâlnirile de clarificare cu membrii cheie ai echipei de proiect a solicitantului permit sistematizarea informațiilor colectate pentru o mai bună înțelegere atât de către echipa de proiect a furnizorului, cât și de către cea a solicitantului, și pentru a fi utilizate în elaborarea specificațiilor privind cerințele software;
- Activitatea de elaborare a unei specificații software permite definirea funcționalității sistemului care satisface business-cerințele organizației. Specificația cerințelor de software (SRS) conține următoarele informații în conformitate atât cu cerințele Sarcina tehnică, cât și cu cerințele Regulamentului RM PT-38370656 - 002:2006 "Ciclul de viață al software-ului"

În acest fel, business-cerințele sunt convertite în specificații software detaliate. Pe baza unor întâlniri succesive, cerințele de sistem detaliate propuse sunt verificate și aprobate de către oficialii solicitantului.

11.2 Proiectarea software-ului și codificarea efectivă

Acest proces constă în următoarele activități:

- Elaborarea unei specificații tehnice de proiectare a software-ului (SDS) care oferă o idee clară despre modul în care sistemul software va fi structurat pentru a îndeplini cerințele definite în SRS. SDD este o traducere a cerințelor într-o descriere a structurii software, a componentelor software, a interfețelor și a datelor necesare pentru faza de implementare. SDD conține informații structurate în conformitate cu cerințele din Sarcina tehnică și din Regulamentul RM PT-38370656 - 002:2006 ”Ciclul de viață al software-ului.”
- Crearea de exemplare fizice ale bazelor de date. Rezultatul este baza de date Registrului Data Warehouse și baza de date de căutare ElasticSearch, inclusiv indexarea eficientă și securitatea obiectelor bazei de date;
- Proiectarea, asamblarea modulelor de aplicații software. Aceasta este partea principală a procesului de dezvoltare a aplicațiilor pentru utilizatori. Ajută dezvoltatorii să proiecteze aplicația și să creeze codul de lucru pentru aplicație în conformitate cu orientările SRS și SDD.
- Testarea internă a modulelor software ale aplicației va include toate activitățile necesare pentru a livra un produs software care să îndeplinească așteptările clienților. În timpul perioadei de testare, versiunea aplicației în curs de dezvoltare este supusă următoarelor niveluri de testare:
    - Testarea unitară testează funcționalitatea unei anumite funcții (document, raport, interfață utilizator, proces etc.) a aplicației;
    - Testarea integrării identifică defectele din interfețele și interacțiunile dintre modulele integrate;
    - Testarea sistemului verifică sistemul complet integrat pentru a se asigura că acesta îndeplinește cerințele.

Testatorii întocmesc rapoarte privind testarea și stabilesc dacă software-ul testat este pregătit pentru lansare. De asemenea, se va elabora un plan de testare calificativă cu scenarii de testare funcțională, de încărcare și de stres.

- Versiunea "Release candidate" a software-ului de aplicație dezvoltat, este gata pentru testarea funcțională și acceptarea de către solicitant în timpul procedurii de acceptare a instalației.
- Elaborarea documentației a software-ului de aplicație, inclusiv:
    - Ghid de instalare și configurare a sistemului de aplicații
    - Ghid de utilizare care descrie funcțiile pentru diferitele roluri de utilizator și oferă informații explicative.
    - Ghid al administratorului care descrie funcțiile destinate configurării și funcționării fără probleme a sistemului

11.3 Implementarea software-ului de aplicație și testarea calificativă

Rezultatul cu succes al acestui proces este software-ul de aplicație instalat, gata de testare și de implementare ulterioară pentru funcționare. Rezultatele furnizate după finalizarea cu succes a acestui proces sunt: pachetul de instalare a software-ului aplicației și documentația sistemului.
Pe parcursul acestui proces trebuie să se parcurgă următoarele acțiuni:

- Instalarea și configurarea SIA RSISC într-un mediu de testare calificativă;
- Instruirea utilizatorilor în materie de testare;
- Testarea funcțională, de încărcare și de stres a aplicației software;
- Corectarea erorilor;
- Eliberarea versiunii finale a software-ului aplicației.

Principalul document de verificare este Certificatul de instalare, semnat de solicitant, ceea ce înseamnă că caracteristicile funcționale și de sarcină ale aplicației software îndeplinesc cerințele și așteptările solicitantului și sunt pregătite pentru implementarea ulterioară.
Toate testele vor avea loc în mediul de testare, în prezența reprezentanților managerului solicitantului și a altor funcționari desemnați. Membrii echipei de dezvoltare a furnizorului vor participa, de asemenea, și îi vor asista pe utilizatorii echipei de testare calificativă la efectuarea testelor de acceptare. În tabelul următor este prezentat un rezumat al rolurilor și responsabilităților membrilor echipei de testare funcțională implicați în testarea pre-pilot.

Roluri	Responsabilități
Manager de proiect	Managerul de proiect va fi responsabil pentru executarea cu succes a testelor funcționale și de încărcare. Sarcinile sale vor consta în planificarea, organizarea, gestionarea și controlul testării funcționale.
Grupul de testare claificativă	Testerii vor testa modulele dezvoltate. Aceștia vor fi responsabili de executarea scenariilor de testare în conformitate cu instrucțiunile descrise în procedurile de testare și de raportarea rezultatelor testelor prin completarea jurnalelor de execuție a testelor.

Inițial, toți testerii vor primi formulare de scenariu (Test Case). Un model al unui astfel de formular este prezentat în tabelul următor:

Proiect	SIA RSISC
Tester	…
Secțiune	…
Data	…
Scenariu de testare #	…

Temă	…				
Business rol	…				
Funcționalitate	…				
Dependențe între cazuri	…				
Pas #	Descrierea pașii/acțiuni	A trecut cu succes	Nu a trecut testul	Blocat	Comentarii
1.					
2.					
3.					
4.					
OUTPUTS Sunt specificate toate ieșirile prezise generate de execuția scenariului de testare. Ieșirile includ toate mesajele (de exemplu, mesaje de eroare etc.) generate de sistem, ceea ce se traduce prin parcurgerea tuturor rutinelor de gestionare a excepțiilor.					

Testarea se va realiza prin succesiunea de pași, stabilită de procedurile de testare din Planul de testare (funcționalitatea sistemului este testată cu ajutorul unui set de proceduri de testare, constând în unul sau mai multe scenarii de testare). Rezultatele testului vor fi prezentate în raportul privind scenariul de testare:

№	Funcția business/punctul din Sarcina Tehnică	Scenariul (Pașii) de testare	Rezultatul executării reușite	Rezultatul
1.				
2.				
3.				
4.				

Protocolul va fi prezentat echipei de dezvoltare pentru analiza și rezolvarea problemelor identificate.

Defectele descoperite în timpul testelor calificative vor fi predate echipei de dezvoltare a furnizorului. Toate defectele rămase deschise la sfârșitul testelor calificative vor fi corectate în versiunea finală a aplicației, care va fi utilizată în etapa de implementare.

Clasificarea defectelor în funcție de gradul de criticitate (1, 2, 3 și 4) se definește după cum se arată în tabelul următor:

Criticitate	Clasificare	Funcționalitate	Impactul asupra sistemului
1	Critic (defect de blocare)	S-a făcut o greșeală gravă; nu există nicio soluție de ocolire.	Testul nu poate fi evaluat în continuare. Încheierea anormală a programului, erori numerice sau cerințe neîndeplinite, erori de nivel de criticitate 1.
2	Înalt (defect grav)	A apărut o eroare gravă, dar există o soluție software pentru a o înlătura.	O finalizare anormală care poate fi ocolită prin alte intrări ale utilizatorului, mici erori în rezultatele finale sau eșecuri minore în punerea în aplicare a cerințelor sunt clasificate ca fiind de nivelul 2 de criticitate.
3	Mediu (defect minor)	O omisiune nesemnificativă sau un defect nesemnificativ de funcționalitate.	Un format de raport incorect sau o vizualizare sau o problemă incorectă este clasificată ca o eroare cosmetică, la fel ca și deficiențele care îngreunează utilizarea software-ului, dar care nu încalcă cerințele și specificațiile.
4	Scăzut (defect enervant)	A fost detectată o eroare "cosmetică".	Nu afectează componenta (componentele) relevantă (relevante).

Criteriile pentru finalizarea cu succes a testării funcționale sunt următoarele:

- Defecte de nivel de criticitate 1 - lipsesc.
- Defecte de nivel de criticitate 2 - lipsesc.

Orice defecte rămase deschise la sfârșitul testelor calificative vor fi corectate înainte ca versiunea finală a aplicației să fie lansată.

Echipa de testare calificativă poate efectua, de asemenea, teste de cercetare (testare specială). Acesta este un proces creativ, intuitiv, care implică proiectarea testelor și rularea lor simultană. Această abordare nu necesită prea multă planificare prealabilă și permite o documentare limitată a scopului testului. Această abordare se bazează în principal pe abilitățile și cunoștințele testerului care efectuează testul.

12 Planul de instruire

12.1 Metoda de instruire

Grupul nr. 1, până la 30 de utilizatori (roluri: Registrator, CERT GOV, CERT Departamental, Decident) vor fi instruiți lucrului în SIA RSISC.

Grupul nr. 2 format din 2 administratori (roluri: Administrator de conent, Administrator de sistem) va fi instruit în diverse sarcini și proceduri administrative, precum și în detaliile implementării modulelor de sistem.

Grupul nr. 3, format din 2 instructori, va fi instruit cu privire la toate funcțiile oferite de sistem.

Durata instruirii fiecărui grup va fi stabilită de comun acord cu solicitantul.

Toate training-urile vor fi dotate cu materialele didactice necesare în funcție de cursurile de instruite oferite.

Metoda preferată de instruire va fi - traininguri on-line. Solicitantul este responsabil pentru furnizarea mijloacelor tehnice necesare pentru participarea la cursurile de instruire on-line.

12.2 Condiții prealabile

Toți utilizatorii care urmează să fie instruiți, trebuie să posede cunoștințe de bază în domeniul lucrului la calculator înainte de a participa la cursurile relevante.

Toți utilizatorii vor fi familiarizați cu business-procesele din domeniul, pe care au fost desemnați să îl studieze.

12.3 Specificațiile cursului

Planul de instruire detaliat furnizat include următoarele:

- Specificarea instalațiilor și echipamentelor necesare pentru fiecare curs. În special, vor fi evaluate următoarele elemente:
  - Materiale didactice;
  - Resurse informatice (hardware și periferice - sistem de operare / rețea / software de aplicație).
- Programul cursului

Această secțiune a planului prezintă o matrice a orarului cursurilor. Informațiile necesare trebuie incluse într-un tabel cu următoarea structură:

Codul cursului	Codul clasei	Locație/ încăpere	Data de începere a cursului	Data de încheiere a cursului	Număr de participanți	Ora de începere	Data creării clasei	Trainer

Tabelul trebuie completat de traineri.

12.4 Orarul cursurilor

Această secțiune prezintă o matrice pentru fiecare curs, care va include orarul de participare la fiecare curs. Fiecare clasă este identificată prin codul cursului, denumirea și durata acestuia. Informațiile solicitate trebuie incluse într-un tabel cu următoarea structură:

Codul clasei	Locație / încăpere	Data de începere a cursurilor	Persoana instruită	Date de contact ale persoanei instruite

Tabelul trebuie completat de către traineri, cu excepția datelor referitoare la cursanți, care trebuie furnizate de către solicitant.
După finalizarea cursurilor de instruire, managerul de proiect ar trebui să elibereze un formular al certificatului de instruire într-o perioadă rezonabilă (până la 5 zile) ca dovadă că sesiunile de instruire planificate au avut loc efectiv.

13 Plan de suport tehnică de garanție pentru sistem

SIA RSISC este acoperit de servicii de suport și asistență tehnică de garanție timp de 12 luni de la acceptare, în conformitate cu cerințele standardului național SM ISO/CEI 14764:2005 - Tehnologii informaționale.

13.1 Suport software

Garanția acoperă toate modulele care au fost dezvoltate și livrate în sistemul informatic vizat.
Durata perioadei de asistență în garanție va fi de 12 luni. Condițiile și volumul lucrărilor pentru perioadele de asistență suplimentare vor fi convenite de părți pentru fiecare an suplimentar.
Furnizorul oferă asistență pentru utilizator și pentru funcționalitatea SIA RSISC. Acest sprijin constă în următoarele grupuri de activități:

- Asistență tehnică;
- Serviciul de garanție;
- Asistență pentru utilizatori/linie fierbinte;

Furnizorul garantează următoarele servicii de garanție pentru software-ul dezvoltat și livrat pentru o perioadă de 12 luni de la data acceptării, fără costuri suplimentare:

- Corectarea erorilor (modificările produsului software după livrare pentru a remedia problemele/erorile detectate);
- Livrarea de actualizări (modificarea produsului software după livrare, atunci când sunt detectate și corectate erori ascunse în produsul software înainte ca acestea să devină erori valide);
- Lucrul serviciului ServiceDesk în zilele lucrătoare 5/8 (răspuns la orice apel la serviciul de asistență al furnizorului în timpul zilei de lucru);
- Consultări la ”linia fierbinte” de asistență IT a furnizorului prin telefon sau e-mail 5/8;
- Vizită la fața locului, dacă este necesar, în următoarea zi lucrătoare;

13.1.1 Procese de suport software

Toate incidentele sunt prelucrate în conformitate cu următorul proces:

5. Solicitantul va înființa un serviciu de suport IT pentru utilizatorii finali
6. Furnizorul va organiza serviciul de suport IT pentru solicitant.
7. Utilizatorul final informează personalul de asistență IT al solicitantului, personal, prin telefon sau e-mail, cu privire la orice problemă sau defecțiune a sistemului sau solicită asistență.
8. Personalul de asistență IT al solicitantului încearcă să rezolve problema. În cazul în care problema este rezolvată, incidentul este închis.
9. În cazul în care personalul de asistență IT al solicitantului nu poate rezolva problema și dacă aceasta este legată de operabilitatea sistemului implementat ca parte a proiectului vizat, problema este transmisă echipei de asistență a furnizorului de prim nivel pentru investigații suplimentare și acțiuni corective.
10. Personalul de suport al furnizorului:
    a. Utilizând experiența sa în înlăturarea defecțiunilor și cunoștințele sale despre sistemul concret, încearcă să găsească o soluție la problemă sau să determine cât mai exact posibil cauza problemei.

b. Informează personalul de asistență IT al solicitantului cu privire la starea unei probleme specifice, precum și cu privire la starea întregului sistem.

11. În cazul în care personalul de asistență al furnizorului nu poate rezolva problema, acesta o va trimite la echipa de asistență de nivel secundar corespunzătoare.

12. Inginerii echipei de asistență de nivel 2 informează personalul de asistență IT al solicitantului cu privire la acțiunile lor și la rezultatele/statutul problemei pentru care au fost desemnați să o rezolve.

13. Echipa de asistență de nivel 2 are acces la toate instrumentele necesare pentru rezolvarea problemelor (software de sistem, software de aplicații, upgrade-uri, actualizări etc.).

14. În cazul în care problema nu poate fi rezolvată de la distanță, inginerii echipei de asistență de nivel 2, cu toate informațiile necesare, se vor deplasa la fața locului și vor rezolva problema (configurarea aplicației, instalarea actualizărilor) și, dacă este necesar, vor colecta toate informațiile necesare pentru a actualiza aplicația.

15. Serviciul de asistență tehnică al furnizorului menține o bază de date pentru a urmări și monitoriza toate incidentele.

13.1.2 Condițiile de acordare a serviciilor de garanție pentru suport

1. Solicitantul formează și expediază solicitarea către Prestator. Prestatorul recepționează Solicitările numai de la o persoană responsabilă desemnată din partea Solicitantului. Solicitările nu trebuie să fie duplicate și cerințele din solicitare trebuie descrise detaliat.

2. Timpul de reacție și execuție – vezi Termenii de reacție. Reacția este faptul expedierii mesajului de confirmare către Solicitant privind înregistrarea acestei Solicitări. Timpul maximal pentru soluționarea unei probleme poate fi majorat în dependență de complexitatea problemei.

3. Graficul standard pentru prestarea serviciilor în zilele lucrătoare de la 9:00 până la 18:00.

4. Prestatorul oferă Solicitantului posibilitatea de a-l contacta prin următoarele modalități (enumerate în ordinea descreșterii preferinței):

- expedierea de e-mail la adresa SSC ServiceDesk@dsi.md ;
- apel telefonic la numărul corporativ al SSC - 22 509 777;
- utilizarea sistemului de gestiune a solicitărilor (Service Desk) al Prestatorului.

5. Toate solicitările sunt înregistrate în sistemul informațional al Prestatorului - ServiceDesk. Datele privind solicitarea înregistrată sunt expediate Prestatorului prin e-mail. Lista de solicitări deschise cu statutele actualizate sunt expediate Solicitantului la cerere.

6. La închiderea solicitării Beneficiarului se expediază un mesaj. Solicitantul trebuie să verifice rezultatul.

7. Pentru fiecare cerere se stabilește nivel de prioritate (Low, Medium, High) si nivel de criticitate. Acești indicatori sunt determinați de către Solicitant la momentul depunerii cererii. Prioritatea se acordă cererilor cu nivelul de criticitate « High », printre cererile cu un nivel de criticitate, se acordă prioritate cererilor cu nivelul de prioritate « High ».

8. Dacă cerințele nu sunt clare sau nu sunt suficient de detaliate, sau sunt specificate cerințe prea generale (de exemplu," de a adăuga o nouă coloană Subdiviziune la toate rapoartele" – în acest caz nu este specificat în ce rapoarte trebuie să fie adăugate și care sunt regulile de completare a acestei coloane), atunci solicitarea este reîntoarsă Solicitantului pentru completări de clarificare și detaliere cerințe, iar această solicitare este suspendată. Pentru solicitările la care nu se recepționează clarificări și explicații mai mult de 5 zile lucrătoare, Prestatorul va expedia Solicitantului un aviz privind închiderea solicitării timp de 3 zile. Astfel de solicitări se închid după 3 zile de la data notificării.

9. Modalități de prestarea serviciilor de mentenanță: remote acces prin instrumente de tip VPN sau RDP sau alte instrumente, consultații prin telefon sau email.

13.1.3 Termenii de reactive

Neconcordanță	Descriere	Timp max. de reacție/timp max. pentru soluționare o singură problemă (ore de lucru, zile)
Înaltă (*)	Probleme, ce au influentă înaltă asupra asigurării funcționalității Sistemului. Astfel de neconcordanțe pot conduce la restricționarea utilizării a unei părți a Sistemului.	Timp max. de reacție: 8 ore. Timp max. pentru soluționare o singură problemă: 8 ore
Medie *	Probleme ce țin de dereglările funcționalității Sistemului și, care pot fi soluționate fără riscul pierderii de date sau prejudicierea funcționalității Sistemului.	Timp max. de reacție: 2 zile. Timp max. pentru soluționare o singură problemă: 2 zile

Mică *	Probleme cu impact mic sau foarte mic asupra funcționalității Sistemului. De exemplu, probleme legate de afișarea mesajelor sau modificări în documentație.	Timp max. de reacție: 3 zile. Timp max. pentru soluționare o singură problemă: 3 zile

(*) - în cazuri exceptionale Timpul maximal pentru soluționarea unei singure probleme poate fi extins cu notificarea solicitantului. Timpul maximal pentru soluționarea unei singure probleme nu include durata acțiunilor și operațiunilor, desfășurate de către solicitant de partea sa pentru a înlătura problema, inclusiv timpul de reacție al solicitantului la întrebări de clarificare.

14 Funcțiile SIA RSISC

Reieșind din scopul și destinația SIA RSISC, poate fi demonstrat modelul funcțional:

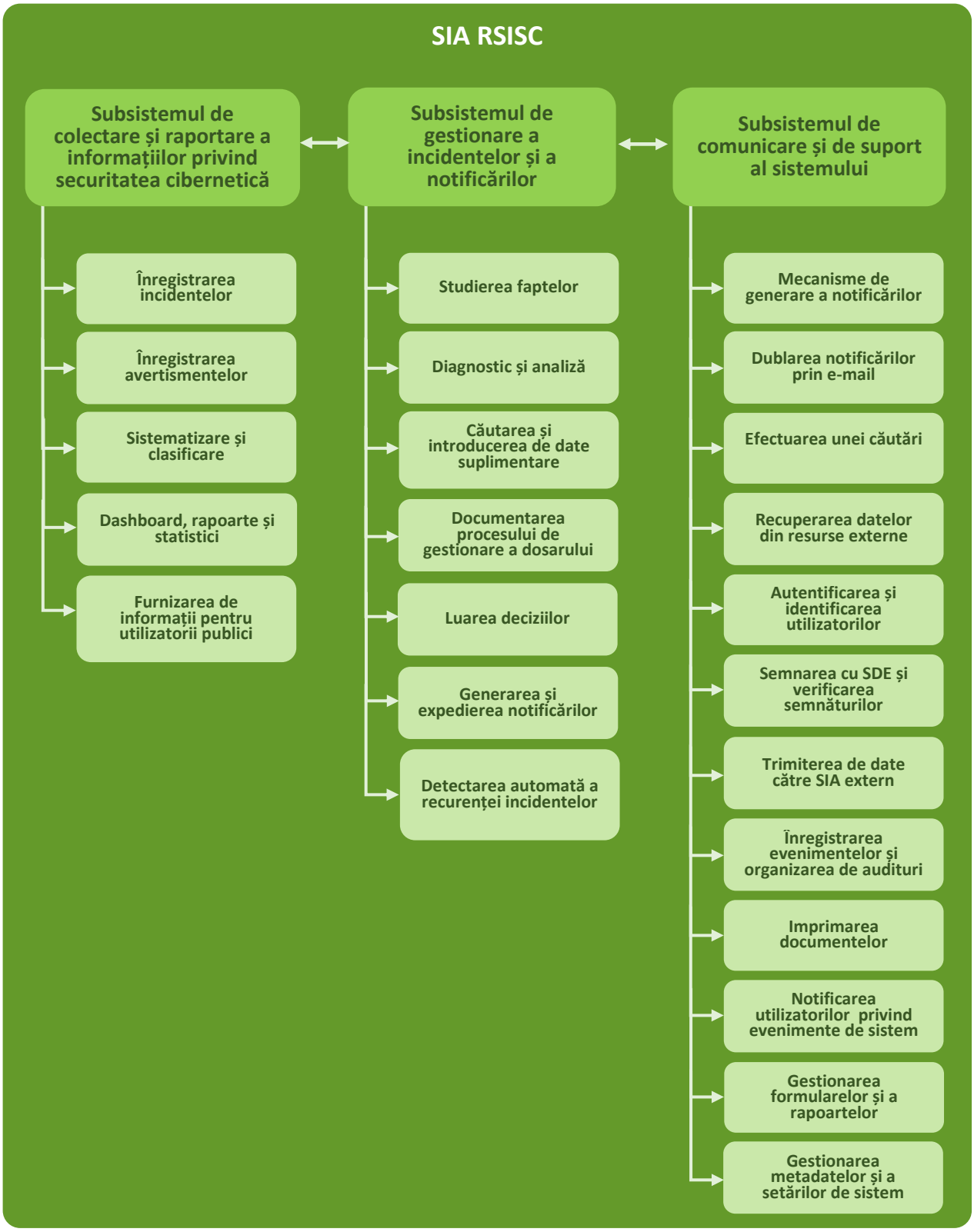

Figura 4: Modelul funcțional al sistemului

Din punct de vedere logic, modelul funcțional este alcătuit din trei subsisteme:

Subsistemul de colectare și raportare a informațiilor privind securitatea cibernetică (răspunde în timp real la incidentele cibernetice) - asigură colectarea și sistematizarea informațiilor privind incidentele cibernetice, evaluarea preliminară a acestora și furnizarea de informații publicului și utilizatorilor înregistrați.
Registratorul poate completa Dosarul incidentului cu informații obținute din diverse surse.
Pentru a accelera procesarea informațiilor, SIA RSISC vă permite să căutați în "baza de cunoștințe" aceleași incidente sau incidente similare și să folosiți activitatea anterioară.
Subsistemul asigură generarea și recepționarea diferitelor rapoarte statistice și analitice pentru beneficiarii sistemului. De asemenea, Dashboard-ul cu date actualizate din Registru este vizualizat în permanență în accesibilitate.
Subsistemul de gestionare a incidentelor și notificărilor - asigură activitățile de bază ale ciclului de viață pentru un obiect de incident cibernetic înregistrat, cum ar fi: studierea faptelor, diagnosticarea, detectarea factorilor dăunători, analiza aprofundată a condițiilor prealabile și a structurii amenințărilor, precum și pregătirea documentației și aprobarea deciziilor. Toate datele, constatările și deciziile primite sunt înregistrate într-un Registru. Pe baza acestor date, persoanele responsabile formulează recomandări menite să minimizeze efectele negative ale incidentului cibernetic.
SIA RSISC permite reutilizarea datelor dezvoltate anterior din "baza de cunoștințe", permițând în același timp ajustări și actualizări.
Pe această bază, SIA RSISC generează o alertă. Tehnicienii pot corecta alertele și pot atașa documentele și materialele necesare.
În plus, toate datele privind incidentele cibernetice și toate informațiile generate sunt disponibile pentru unitățile CERT, CERT Govs și autoritățile competente. Nivelul de acces al beneficiarilor SIA RSISC este stabilit în conformitate cu Regulamentul privind realizarea "Registrului de stat al incidentelor de securitate cibernetică". Pentru utilizatorii publici sunt disponibile informațiile refritoare.

Subsistemul de comunicare și de suport al sistemului este un grup de funcții care asigură gestionarea utilizatorilor, organizează accesul acestora la funcționalitatea SIA RSISC în conformitate cu rolurile și drepturile atribuite, organizează auditul funcționării sistemului și al acțiunilor utilizatorilor, furnizează mecanisme de notificare pentru părțile interesate, semnează documente cu SDE și efectuează căutări de informații în toate datele din Registru.
În plus, RSISC generează și trimite memento-uri cu privire la termenele limită pentru acțiunile planificate.
Subsistemul asigură, de asemenea, interacțiunea cu sistemele informatice externe (prin intermediul serviciilor guvernamentale) privind răspândirea informațiilor de securitate cibernetică, inclusiv rezultatele analizei incidentelor de securitate

cibernetică, soluțiile și acțiunile recomandate, în conformitate cu prevederile acordurilor de cooperare.

Modelul funcțional este implementat prin intermediul cazurilor de utilizare, prezentate în diagrama (figura 5):

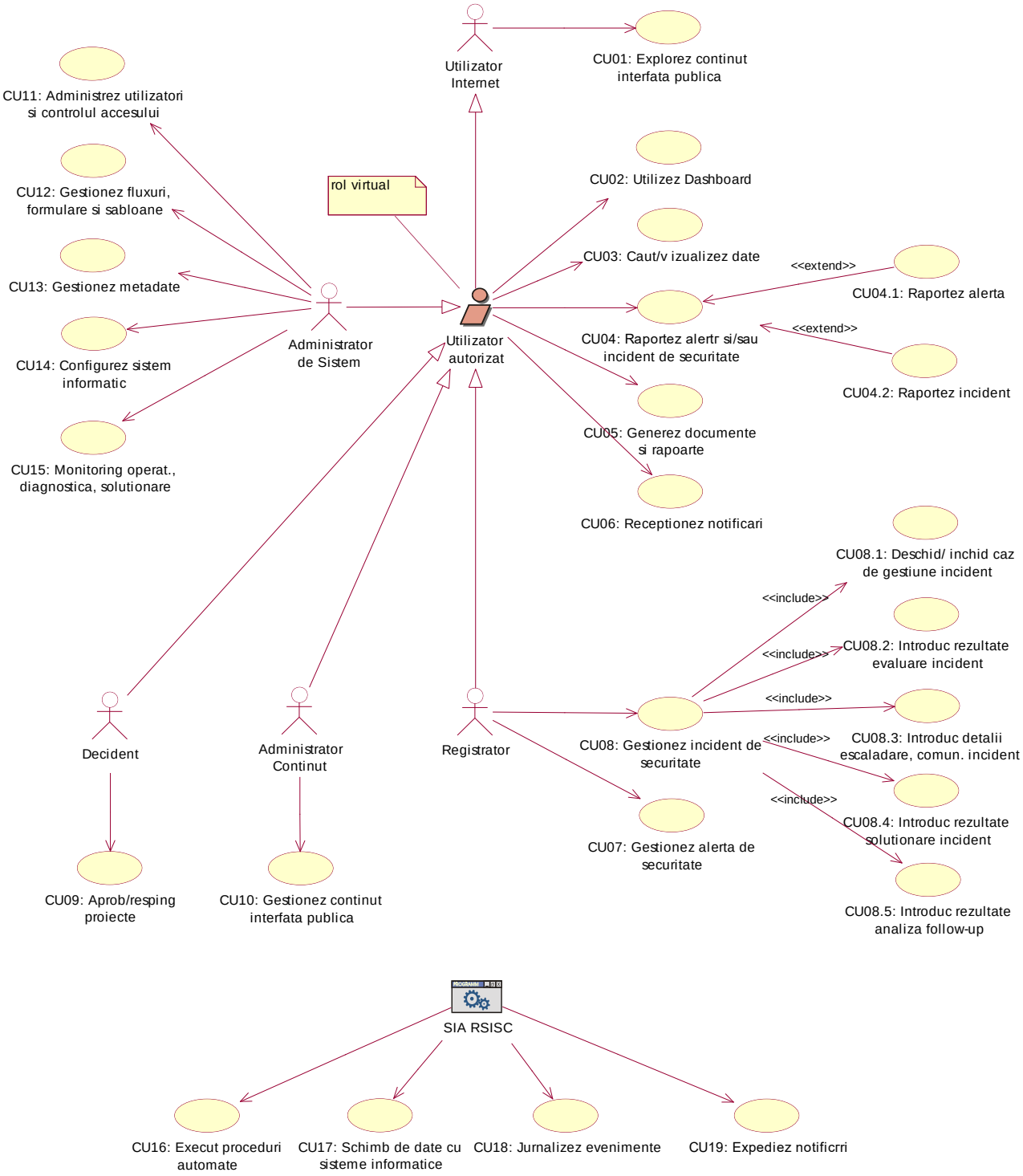

Figura 5. Funcționalitatea SIA RSISC

15 Cerințe funcționale

Soluția tehnică propusă implementează cerințele CAIETULUI DE SARCINI destinat elaborării Sistemului Informațional Automatizat „Registrul de stat al incidentelor de securitate cibernetică”, după cum urmează:

15.1 CU01: Explorez conținut interfață publică

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
CF 01.01.	M	Interfața Publică a SIA RSISC va furniza mecanism de navigare în categoriile de structură în scopul găsirii rapide a informației relevante.	Corespunde
CF 01.02.	M	Navigarea se va efectua prin intermediul meniului principal denavigare și interfața utilizator a Paginii Principale.	Corespunde
CF 01.03.	M	La accesarea mecanismului de navigare în categoriilor de structură, Interfața Publică a SIA RSISC tip va furniza un mecanism de navigaresimilar după principiile de utilizare unui director de căutare (unde arborele de structură corespunde structurii Paginii WEB).	Corespunde
CF 01.04.	M	Documentele de conținut vor fi amplasate în categoriile frunză alearborelui de structură a Interfeței Publice a SIA RSISC.	Corespunde
CF 01.05.	M	Interfața Publică a SIA RSISC va afișa referințe de nivel pentru a arătanivelul ierarhic compartimentului curent al Interfeței Publice.	Corespunde
CF 01.06.	M	Referințele de structură vor avea referințe hipertext care vor permitenavigarea spre nivelele ierarhice superioare categoriei curente.	Corespunde
CF 01.07.	M	Interfața Publică a SIA RSISC trebuie să furnizeze mecanism degenerare a conținutului textual în format A4 (optimizat pentruimprimare) și descărcare a documentelor plasate în conținut.	Corespunde
CF 01.08.	M	Interfața publică a SIA RSISC va asigura acces la o bază de cunoștințe prin intermediul căreia se vor accesa următoarele categorii de date și facilități funcționale: • documente în format HTML (redactate cu ajutorul editoarelorWYSIWYG); • ghiduri/instrucțiuni încărcate în format PDF, DOC/DOCX,PPT/PPTX etc.; • documente de politici cu privire la securitatea informației; • recomandări cu privire la securitatea informației; • răspuns la întrebările frecvente (F.A.Q.); • referințe la cadrul legal în vigoare conținut în Registrul de Statal Actelor Juridice (https://www.legis.md);	Corespunde

		• informație multimedia încărcată nemijlocit în SIA RSISC sau publicată prin intermediul resurselor externe (exemplu: Youtube, Rețele de socializare etc.).	
CF 01.09.	M	Interfața publică a SIA RSISC va asigura acces la KPI și rapoarte statistice cu caracter public generate în baza datelor produse în cadrulfluxurilor de lucru aferente SIA RSISC.	Corespunde Solicitantul trebuie să furnizeze indicatori cheie de performanță
CF 01.10.	M	Interfața Publică a SIA RSISC va furniza facilități de partajare a conținutului pe cele mai populare rețele de socializare (Facebook,Twitter, LinkedIn etc.).	Corespunde
CF 01.11.	M	Interfața public va furniza mecanism de feedback și contact prin intermediul cărora Internauții vor putea interacționa cu responsabiliidin cadrul Centrului pentru Securitatea Cibernetică.	Corespunde
CF 01.11.	M	Toată informația statistică de interacțiune a Utilizatorilor Internet cuinterfața publică a SIA RSISC va fi colectată prin intermediul API-ului expus de Google Analytics (Furnizorul va efectua toate activitățile deintegrare a SIA RSISC cu Google Analytics).	Corespunde

15.2 CU02: Utilizez Dashboard

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
CF 02.01.	M	SIA RSISC va livra utilizatorilor autorizați o soluție Dashboard prin intermediul căreia vor fi notificați asupra evenimentelor de businessimportante și accesa rapid detaliile acestora.	Corespunde
CF 02.02.	M	Pot fi enumerate următoarele categorii de evenimentele de businessafișate în cadrul Dashboard-ului: • notificări de sistem; • notificări privind alertele de securitate cibernetică ce urmeazăa fi examinate; • notificări privind incidentele de securitate cibernetică ceurmează a fi gestionate; • notificări privind necesitatea implicării utilizatorului în activitățile fluxurilor de lucru ale SIA RSISC (inclusiv alerte de întârziere); • notificări privind formulare sau documente care așteaptăaprobare de la rolurile decidente (inclusiv alerte de întârziere); • notificări privind completarea fișei incidentului de securitatecibernetică cu noi documente sau formulare electronice; • notificări privind evenimentele de trasabilitate a alertelor șiincidentelor de securitate cibernetică; • alte evenimente relevante.	Corespunde

CF 02.03.	M	Dashboard-ul utilizatorului SIA RSISC va afișa doar evenimente debusiness relevante rolurilor și drepturilor asignate utilizatorului autorizat.	Corespunde
CF 02.04.	M	Dashboard-ul utilizatorului cu rol Administrator de Sistem va afișa toate evenimente de business aferente funcționalității SIA RSISC (totalitatea notificărilor afișate în Dashboard-ul tuturor utilizatorilorSIA RSISC și notificările dedicate exclusiv utilizator cu rol de Administrator de Sistem).	Corespunde
CF 02.05.	M	Dashboard-ul va grupa evenimentele de business afișându-le sub formă de indicatori cu valori agregate (exemplu: Notificări de sistem necitite -14; Alerte de securitate noi - 45, Incidente de securitate noi –6, Cazuri curente de gestiune a incidentelor - 8, Formulare expediate spre aprobare - 8 etc.) care vor conține referință hipertext de accesare a detaliilor.	Corespunde
CF 02.06.	M	SIA RSISC va afișa înregistrări detaliate ale Dashboard-ului în ferestresau zone specializate pe pagina principală a interfeței utilizatorului autorizat care la rândul lor vor dispune de referință hipertext de accesare directă a detaliilor (*exemplu: lista alertelor ce urmează a fiprocesate*).	Corespunde
CF 02.07.	M	La accesarea referinței hipertext aferentă valorii agregate sau înregistrării detaliate a Dashboard-ului SIA RSISC va asigura accesul lainformația de detaliu aferentă acestora sau funcționalitatea solicitată (*exemplu: formularul de evaluare a incidentului, formularul de escaladare a incidentului, formularul de introducere a rezultatelor soluționare incident etc.*).	Corespunde
CF 02.08.	M	Dashboard-ul SIA RSISC va conține o zonă specializată (favorite) în care utilizatorul și va plasa referințe la informația de conținut la care lucrează. Acestea pot fi de 3 tipuri: • cazuri de gestiune a incidentelor de securitate cibernetică deschise/închise; • formulare electronice perfectate (evenimente de business aferente cazurilor de gestiune a alertelor sau incidentelor desecuritate cibernetică perfectate curent); • formulare electronice examinate spre aprobare.	Corespunde
CF 02.09.	D	SIA RSISC va oferi fiecărui utilizator autorizat funcționalitate de configurare individuală a aspectului și conținutului Dashboard-ului.	Corespunde Va fi realizat în cazul, dacă acceptarea SIA RSISC va fi efectuată înainte de termenul stabilit

15.3 CU03: Caut/vizualizez date

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
CF 03.01.	M	SIA RSISC va furniza mecanism complex de căutare a datelor în întregconținutul bazei de date.	Corespunde
CF 03.02.	M	SIA RSISC va furniza mecanism de căutare	Corespunde

		indexată a datelor utilizândElastic Search.	
CF 03.03.	M	SIA RSISC va permite definirea următoarelor ținte de căutare(rezultatul căutării va afișa lista de): • autorități publice posesoare de sisteme informatice; • utilizatori autorități; • alerte raportate; • incidente raportate; • cazuri de gestiune a incidentelor; • formulare ale cazurilor de gestiune a incidentelor de securitate cibernetică • alte ținte specifice.	Corespunde
CF 03.04.	M	SIA RSISC va furniza un mecanism flexibil și performant de definire acriteriilor de căutare.	Corespunde
CF 03.05.	M	În calitate de criterii de căutare vor putea fi folosite: • date aferente sistemului informatic sursă a alertei sau aincidentului de securitate cibernetică; • date de identificare a autorităților publice posesoare desisteme informatice; • date aferente utilizatorilor autorizați care au procesat înregistrările bazei de date; • date aferente sistemului de metadate specific alertelor sauincidentelor de securitate cibernetică; • date de detaliu a cazurilor de gestiune a incidentelor desecuritate cibernetică; • date de detaliu ale alertelor raportate; • date de detaliu ale incidentelor raportate; • statutul înregistrărilor; • alte categorii de date specifice.	Corespunde
CF 03.06.	M	În cazul formulări unor criterii de căutare prea largi, sau care necesităprea mult timp și resurse pentru execuție SIA RSISC nu va executa aceste interogări ci va solicita utilizatorului îngustarea domeniului devalori căutate.	Corespunde
CF 03.07.	M	Rezultatele căutării vor fi ordonate în funcție de relevanța rezultatuluiinterogării de căutare, alfabetic sau dată creare/ultimă actualizare.	Corespunde
CF 03.08.	M	Utilizatorul va putea defini criterii de ordonare și grupare aconținutului listei cu rezultatele procesului de căutare.	Gruparea poate fi efectuată în funcție de tipul obiectului informațional sau de date
CF 03.09.	M	SIA RSISC va oferi mecanism de paginare a rezultatelor căutării destinat evitării supraîncărcării exploratorului WEB și canalelor detransport date.	Corespunde
CF 03.10.	D	Înregistrările rezultatelor căutării vor fi marcate (culoare sau iconițăspecifică) în funcție de natura sau statutul obiectului informaționalgăsit.	Această cerință poate supraîncărca grav sistemul. Va fi realizat în cazul, dacă acceptarea SIA RSISC va fi

			efectuată înainte de termenul stabilit
CF 03.11.	M	SIA RSISC va furniza funcționalitate de afinare a căutării în rezultatelegăsite.	Corespunde
CF 03.12.	M	SIA RSISC va permite declanșarea unor procese asupra rezultatelorgăsite sau a unui grup de rezultate găsite și marcate cum ar fi: • selectare înregistrări ale rezultatului căutării; • vizualizare detalii înregistrări găsite; • semnare electronică multiplă; • suprimare multiplă; • pentru utilizatorii găsiți: vizualizarea profilului utilizatorului, vizualizarea cazurilor de gestiune a incidentelor de securitateaferente utilizatorului, vizualizarea formularelor aferente cazului de gestiune a incidentului de securitate, vizualizarea alertelor de securitate raportate/ procesate, vizualizarea incidentelor de securitate raportate/procesate etc.; • pentru dosarele cazurilor de gestiune a incidentelor de securitate: accesare conținut dosar caz de gestiune incident de securitate, generarea fișei cazului de gestiune a incidentului de securitate etc.; • pentru evenimentele de business ale cazurilor de gestiune a incidentelor de securitate: vizualizarea documentului aferent evenimentului, accesarea formularului electronic de perfectare a evenimentului de business, aprobarea/respingerea formularului, generarea documentuluiaferent evenimentului de business; • pentru alertele/incidentele de securitate raportate: deschiderea cazului de gestiune a incidentului de securitate, schimbare statut al formularului alertei/incidentului raportatetc. • alte acțiuni relevante.	Corespunde
CF 03.13.	M	SIA RSISC va afișa în rezultatele căutării doar datele ce corespunddomeniul de competență a utilizatorului autorizat, rolurilor și drepturile definite în profilul de utilizator autorizat al SIA RSISC.	Corespunde
CF 03.14.	M	SIA RSISC va restricționa accesul la detaliile rezultatelor găsite în cazulcând utilizatorul care a declanșat procesul de căutare nu dispune de drepturi de acces la obiectele informaționale solicitate a fi accesate.	Corespunde
CF 03.15.	M	SIA RSISC va permite exportarea tabelului cu rezultatele căutării înformat CSV sau PDF.	Corespunde

15.4 CU04: Raportez alertă sau incident de securitate cibernetică

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
CF 04.01.	M	SIA RSISC va furniza utilizatorilor autorizați funcționalitate destinatăRaportării alertelor și/sau incidentelor de securitate cibernetică.	Corespunde
CF 04.02.	M	Utilizatorii autorizați vor putea raporta prin intermediul CU04: • alerte de securitate cibernetică; • incidente de securitate cibernetică.	Corespunde
CF 04.03.	M	Alertele de securitate cibernetică vor putea fi perfectate fie de utilizatorii autorizați (prin intermediul CU04), fie expediate automatde sisteme informatice externe (prin intermediul CU18).	Corespunde
CF 04.04.	M	Alerta și/sau incidentul se raportează conform formularului prezentatîn Anexa 2.1.	Corespunde
CF 04.05.	D	Formularele de raportare a alertelor și/ sau incidentelor de securitatecibernetică perfectate prin intermediul CU04 vor fi afișate în baza configurațiilor definite prin intermediul CU13.	Corespunde Va fi realizat în cazul, dacă acceptarea SIA RSISC va fi efectuată înainte de termenul stabilit
CF 04.06.	M	Stările și tranzițiile prin care poate formularele de raportare a - alertelor și/ sau incidentelor de securitate cibernetică perfectate prin intermediul CU04 sunt configurate prin intermediul cazului de utilizare CU13.	Corespunde
CF 04.07.	M	SIA RSISC va asigura acces utilizatorilor autorizați la lista de formularede raportare a problemelor de securitate în funcție de rolurile deținute de aceștia și împuternicirilor furnizate de MPower.	Corespunde
CF 04.06.	M	Perfectarea formularului electronic destinat raportării - alertelor și/sau incidentelor de securitate cibernetică se efectuează doar prin intermediul unor mecanisme exclusiv vizuale.	Corespunde
CF 04.07.	M	Formularul electronic destinat raportării - alertelor și/ sau incidentelorde securitate cibernetică va conține constrângeri și restricții de conținut în vederea limitării erorilor mecanice.	Corespunde
CF 04.08.	M	SIA RSISC va permite atașarea de fișiere la formularul electronic deraportare a - alertei și/ sau incidentului de securitate cibernetică (documente PDF, CSV, capturi ecran sau fișiere video etc.).	Corespunde
CF 04.09.	M	SIA RSISC va furniza mecanism de verificare a plenitudinii sau corectitudinii perfectării formularului electronic de raportare a - alertelor și/ sau incidentelor de securitate cibernetică (obligativitate conținut date, corectitudine tip date inserate, integritate date introduse etc.).	Corespunde
CF 04.10.	M	Doar un formular electronic de raportare a alertei și/sau incidentului de securitate cibernetică care a trecut cu succes procedura de verificare a corectitudinii perfectării va putea fi expediat spre examinare.	Corespunde
CF 04.11.	M	SIA RSISC va asigura un mecanism de trasabilitate (păstrarea istoricului) de examinare a alertei și/sau incidentului de securitate cibernetică raportate.	mecanismul de urmărire (stocare istorică) va efectua stocarea (și vizualizarea) tuturor evenimentelor (inclusiv statutele) de procesare a obiectului informațional

CF 04.12.	M	SIA RSISC nu va permite suprimarea niciunui formular de raportare a alertei și/sau incidentului de securitate cibernetică expediat spre examinare, în examinare sau procesat ci doar anularea acestuia.	Corespunde
CF 04.13.	M	Un formular de raportare a alertei și/sau incidentului de securitate cibernetică expediat prin intermediul CU04 trebuie semnat electronic de expeditor anterior expedierii spre examinare.	Corespunde
CF 04.14.	M	În calitate de mecanism de semnare electronică a formularului de raportare a alertei și/sau incidentului de securitate cibernetică va fi utilizat serviciul guvernamental MSign.	Corespunde
CF 04.1.01	M	SIA RSISC va furniza funcționalitate de raportare a alertelor de securitate cibernetică.	Corespunde
CF 04.1.02	I	O alertă de securitate reprezintă o notificare a unei activități anomalice, ce poate servi ca un indiciu de vulnerabilitate cu risc înalt de exploatare în scopul producerii unui incident de securitate cibernetică	Corespunde
CF 04.1.03	M	O alertă de securitate cibernetică poate fi expediată, de asemenea, în mod automat de către sistemele informatice unde este atestată. Aceste alerte sunt recepționate prin intermediul CU18.	Corespunde
CF 04.1.04	M	Formularul alertei de securitate cibernetică poate avea mai multe stări (statute) și tranziții, în funcție de configurările definite prin intermediul CU13.	Corespunde
CF 04.1.04	M	Conținutul unui formular al alertei de securitate cibernetică poate fi modificat doar în statutul de proiect (până la semnarea electronică a acestuia).	Corespunde
CF 04.1.06	M	SI RISC va păstra proiectul de alertă de securitate cibernetică o perioadă determinată de timp (definită prin intermediul CU15), după care proiectul de alertă va fi suprimat, autorul fiind notificat în prealabil.	Corespunde
CF 04.1.07	M	În momentul în care, alerta va fi expediată spre examinare SIA RSISC va notifica expeditorul și utilizatorul responsabil de procesare a alertei privind recepționarea acesteia..	Corespunde
CF 04.1.08	M	În calitate de mecanism de notificare externă va fi utilizat serviciul guvernamental MNotify.	Corespunde
CF 04.2.01	M	SIA RSISC va furniza funcționalitate de raportare a incidentelor de securitate cibernetică.	Corespunde
CF 04.2.02	I	Un incident de securitate este un eveniment (acțiune ce perturbă activitatea normală) , care poate indica faptul că sistemele sau datele unei entități au fost compromise sau că măsurile de securitate cibernetică adoptate pentru a le proteja au eșuat.	Corespunde
CF 04.2.03	M	Formularul incidentului de securitate cibernetică poate avea mai multe stări (statute) și tranziții, în funcție de configurările definite prin intermediul CU13.	Corespunde
CF 04.2.04	M	Conținutul unui formular al incidentului de securitate cibernetică poate fi modificat doar în statutul de proiect (până la semnarea electronică a acestuia).	Corespunde
CF 04.2.04	M	SI RISC va păstra proiectul de incident de securitate cibernetică o perioadă determinată de timp (definită prin intermediul CU15), după care formularul incidentului de securitate cibernetică în statut proiect va fi suprimat, autorul fiind notificat în prealabil.	Corespunde

CF 04.2.06	M	În momentul în care cazul incidentului de securitate cibernetică va fi expediat spre examinare, SIA RSISC va notifica expeditorul și utilizatorul responsabil de procesare a incidentului privind recepționarea acestuia.	Corespunde
CF 04.2.07	M	În calitate de mecanism de notificare externă va fi utilizat serviciul guvernamental MNotify.	Corespunde
CF 04.2.08	M	Un formular de raportare a incidentului de securitate cibernetică va avea asociat un caz gestiune a incidentului de securitate cibernetică care va conține istoricul și evenimentele de trasabilitate a acestuia.	Corespunde

15.5 CU05: Generez documente și rapoarte

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
CF 05.01.	M	SIA RSISC trebuie să fie în măsură să ofere un număr de documente,rapoarte statistice și ad-hoc, astfel încât să acopere toate necesitățileproceselor de business destinate asigurării securității informației și escaladare a incidentelor de securitate cibernetică (după caz).	Corespunde
CF 05.02.	D	Este binevenit ca la baza generării rapoartelor să stea o platformădedicată destinată configurării generării dinamice a rapoartelor (*exemplu: JasperReport*).	Corespunde Va fi realizat în cazul, dacă acceptarea SIA RSISC va fi efectuată înainte de termenul stabilit
CF 05.03.	M	SIA RSISC trebuie să pună la dispoziția utilizatorilor un număr predefinit de documente/rapoarte configurabile și la necesitate săasigure producerea la necesitate a rapoartelor ad-hoc.	Corespunde
CF 05.04.	M	SIA RSISC va oferi un set de documente ce urmează a fi generate în baza datelor stocate în baza de date a sistemului informatic după cumurmează: • Raportare alertă de securitate cibernetică; • Raportare incident de securitate cibernetică; • Raport de evaluare a alertei de securitate ciberneticăraportate; • Raport de analiză a incidentului de securitate ciberneticăraportat; • Raport de evaluare a incidentului de securitate cibernetică; • Raport privind escaladarea și comunicarea incidentului de securitate cibernetică; • Raport privind rezultatul soluționării incidentului de securitatecibernetică; • Raport privind cauzele incidentului de securitate cibernetică; • Raport de analiză follow-up; • Recipisă de recepționare a formularului de raportare a alerteișsau incidentului de securitate cibernetică; • Notificare de sistem;	Corespunde

		Alte documente relevante.	
CF 05.05.	M	SIA RSISC va dispune de șabloane predefinite (redactabile) pentrufiecare tip de document generat necesar actualizării eventuale aregulilor de generare.	Corespunde
CF 05.06.	M	Furnizorul va implementa până la 20 documente ce urmează a fi generate de SIA RSISC, inclusiv cele expuse în CF 05.04. Lista completăa documentelor urmează a fi identificată pe parcursul analizei de business.	Corespunde
CF 05.07.	M	SIA RSISC va oferi un set de rapoarte ce urmează a fi generate în bazadatelor stocate în baza de date a sistemului informatic după cum urmează: • Raportul de performanță al SIA RSISC (date statistice privind conținutul curent al SIA RSISC) cu diferite principii de agregare (conform AP, conform sistemelor informatice, conform tipurilor de alerte/incidente, conform priorității, conform impactului, conform statutului curent al alertelor și/sau incidentelor, etc.); • Raport de performanță a utilizatorului autorizat, care conținedate statistice și detalii privind cazurile de gestiune a incidentelor nou deschise, cazuri în curs de operare, cazuri închise pe perioadă determinată de timp cu un grad diferit de agregare; • Fișa dosarului cazului de gestiune a incidentelor (o sinteză adatelor din toate formularele cazului de gestiune a incidentului); • Raport privind cazurile de gestiune a incidentelor (conform subdiviziunilor, conform perioadei de timp, conform clasificatoarelor incidentelor, conform rezultatului escaladării,conform sursei etc.); • Liste de incidente (conform tuturor modalităților de filtrareposibile); • Liste de alerte conform tuturor modalităților de filtrareposibile); • Indicatori de performanță; • Alte rapoarte relevante.	Corespunde Vor fi elaborate până la 20 de rapoarte predefinite, bazate pe datele stocate în SIA RSISC.
CF 05.08.	M	SIA RSISC va dispune de mecanism de definire a setului de rapoarte șidate disponibile fiecărei categorii de utilizator, în funcție de rolurile și drepturile deținute.	Corespunde
CF 05.09.	M	Un utilizator care vizualizează un document sau raport în cadrul sistemului, trebuie să-l poată exporta într-un fișier extern redactabil(XLS/XLSX și DOCX).	Corespunde
CF 05.10.	M	Implicit, documentele și rapoartele vor fi extrase în format PDF.	Corespunde
CF 05.11.	M	Furnizorul va implementa până la 20 categorii de rapoarte predefinitesolicitate de beneficiar inclusiv cele specificate în CF 05.07.	Corespunde

CF 05.12.	M	SIA RSISC va jurnaliza toate evenimentele de generare și imprimare adocumentelor și rapoartelor statistice.	Corespunde

15.6 CU06: Recepționez notificări

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
CF 06.01.	M	SIA RSISC va notifica automat orice utilizator autorizat în cazulînregistrării unui eveniment de business ce implică acțiunea utilizatorului sau care modifică statutul proceselor gestionate,monitorizate de acesta sau care-l vizează.	Corespunde
CF 06.02.	M	Utilizatorii autorizați vor recepționa notificări în Dashboard-ulpersonal.	Corespunde
CF 06.03.	M	O copie a notificării va fi expediată la adresa E-mail indicată în profilulutilizatorului autorizat din SIA RSISC.	Corespunde
CF 06.04.	M	Utilizatorul autorizat SIA RSISC va dispune de funcționalitate de configurare a preferințelor de recepționare a notificărilor (la adresa E-mail sau Dashboard).	Corespunde
CF 06.05.	M	SIA RSISC va expedia tot spectrul de notificări destinate utilizatorilorautorizați: • notificare cu privire la recepționarea unei alerte de securitatecibernetică raportate; • notificare cu privire la recepționarea unui incident de securitate cibernetică raportat; • notificare cu privire la deschiderea/actualizarea/închid erea cazurilor de gestiune a incidentelor de securitate cibernetică; • notificare cu privire la necesitatea implicării pe fluxurile delucru a SIA RSISC; • notificare cu privire la întârzierea acțiunii utilizatorului (depășirea termenului limită de aprobare/respingere proiect de formular, perfectare formular aferent gestiunii incidentuluide securitate cibernetică etc.); • notificare cu privire la aprobarea/respingerea proiectelor de formulare electronice de către rolurile decidente; • notificare cu privire la problemele de funcționare a SIA RSISC; • alte notificări relevante.	Corespunde
CF 06.06.	M	O notificare expediată stocată în Dashboard-ul utilizatorului autorizatva conține referință hipertext pentru a deschide formularul electronicrelevat notificării.	Corespunde
CF 06.08.	M	Utilizatorii SIA RSISC vor recepționa notificărilor prin E-mail în formatHTML sau Format Text îmbogățit.	Corespunde

CF 06.09.	M	Notificările externe (citite prin intermediul mijloacelor externe, în afara interfeței utilizator a SIA RSISC) vor fi expediate prin intermediul serviciului de platformă MNotify.	Corespunde

15.7 CU07: Gestionez alertă de securitate cibernetică

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
CF 07.01.	M	SIA RSISC va furniza mecanism de procesare a alertelor de securitatecibernetică recepționate și înregistrate.	Corespunde
CF 07.02.	M	Alertele de securitate cibernetică vor parveni prin intermediul a 2canale: • expediate automat de către sistemele informatice; • raportate de utilizatorii autorizați.	Corespunde
CF 07.03.	M	Procesarea alertei de securitate cibernetică presupune efectuareaurmătoarelor acțiuni puse la dispoziție de SIA RSISC: • analiza problemei; • perfectarea unui raport de analiză a alertei de securitatecibernetică; • schimbare statut alertă de securitate cibernetică (închidereaalertei în cazul în care se consideră ignorabilă); • asocierea alertei de securitate cibernetică unui incident desecuritate cibernetică raportat.	Corespunde
CF 07.04.	M	Pentru alertele raportate de utilizatori autorizați (perfectate prin intermediul CU04.1) trebuie să fie completat un raport de analiză șirăspuns la alertă (chiar dacă specialistul în securitatea informației nu depistează un careva pericol generat de alertă de securitate raportată).	Corespunde
CF 07.05.	M	Pentru alertele raportate de sistemele informatice nu este obligatorie completarea unui raport de analiză și răspuns la alertă. Pentru acesteaeste suficientă doar schimbarea statutului în cazul când specialistul de securitate nu atestă un pericol.	Corespunde
CF 07.06.	M	SIA RSISC va furniza funcționalitate de schimbare simultană a statutelor mai multor alerte de securitate raportate (valabil pentrualertele raportate automat de sistemele informatice).	Corespunde
CF 07.07.	M	SIA RSISC va notifica raportatorii de alerte de securitate cibernetică privind orice evenimente de trasabilitate aacestora. În calitate de mecanism de notificare va fi utilizat serviciul guvernamental MNotify.	Corespunde
CF 07.08.	M	SIA RSISC va jurnaliza toate evenimentele de procesare a alertelor desecuritate cibernetică raportate (inclusiv alternativ prin intermediul serviciului guvernamental MLog).	Corespunde

15.8 CU08: Gestionez incident de securitate cibernetică

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
CF 08.01.	M	SIA RSISC va furniza funcționalitate destinată gestiunii cazurilor degestiune a incidentelor de securitate cibernetică.	Corespunde
CF 08.02.	M	Gestiunea unui caz de gestiune a incidentului de securitate cibernetică presupune efectuarea următoarelor acțiuni: • deschidere/închidere/redeschidere caz de gestiune aincidentului de securitate cibernetică; • evaluarea incidentului de securitate cibernetică; • escaladarea incidentului de securitate cibernetică; • soluționarea incidentului de securitate cibernetică; • investigarea cauzei producerii incidentului de securitatecibernetică.	Corespunde
CF 08.03.	M	SIA RSISC va permite, completarea electronică a conținutului fișei incidentului de securitate cibernetică de către Registrator precum șiintroducerea retroactivă a detaliilor incidentului de securitate cibernetică (cazul când raportatorul dispune de soft destinat documentării incidentului de securitate cibernetică și datele parvinautomat prin intermediul CU18).	Corespunde
CF 08.04.	M	SIA RSISC va permite completarea automată a unor formulare electronice aferente cazului de gestiune a incidentului de securitate cibernetică utilizând datele altor cazuri de gestiune a incidentelor de securitate completate în prealabil (exemplu: în cazul unor incidente desecuritate similare).	Corespunde
CF 08.05.	M	Formularele electronice de completare a fișei incidentului de securitate cibernetică vor fi afișate și validate în baza configurațiilordefinite prin intermediul CU13.	Corespunde
CF 08.06.	M	Stările și tranzițiile prin care poate trece formularul electronic destinatdocumentării cazului de gestiune a incidentului de securitate cibernetică sunt configurate prin intermediul cazului de utilizare CU13.	Corespunde
CF 08.07.	M	Orice formular electronic destinat documentării procesului de gestiune a incidentului de securitate cibernetică va avea asociat unșablon de document care va fi configurat prin intermediul CU13 șiextras prin intermediul CU05 în baza datelor conținute în formular.	Corespunde
CF 08.08.	M	Formularul electronic destinat documentării cazului de gestiune a incidentului de securitate cibernetică poate fi accesat explicit din opțiunile de meniu, apelat din fișa incidentului de securitate cibernetică (cu completare prealabilă automată a datelor care pot fi extrase din conținutul dosarului cazului de gestiune a incidentului) saudin lista rezultatelor furnizate de CU03 (exemplu: inițierea cazului de gestiune a incidentului de securitate cibernetică în baza unor	Corespunde

		alerte sau incidente de securitate cibernetică anterior raportate).	
CF 08.09.	M	SIA RSISC va asigura acces utilizatorilor autorizați la lista de formulareelectronice destinate documentării cazului de gestiune a incidentului de securitate cibernetică în funcție de rolurile deținute de aceștia și împuternicirilor furnizate de MPower.	Corespunde
CF 08.10.	M	Perfectarea formularului electronic destinat documentării cazului degestiune a incidentului de securitate cibernetică se efectuează doar prin intermediul unor mecanisme exclusiv vizuale.	Corespunde
CF 08.11.	M	Formularul electronic destinat documentării cazului de gestiune aincidentului de securitate cibernetică va conține constrângeri și restricții de conținut în vederea limitării erorilor mecanice.	Corespunde
CF 08.12.	M	SIA RSISC va dispune de capacități de calculare a unor valori agregateîn baza datelor primare conținute (exemplu: totaluri, subtotaluri, cuantificări, calculare a unor indicatori generalizatori etc.)	Corespunde
CF 08.13.	M	SIA RSISC va permite atașarea de copii electronice a documentelorrelevante la formularul electronic aferent cazului de gestiune a incidentului de securitate cibernetică.	Corespunde
CF 08.14.	M	SIA RSISC va furniza mecanism de verificare a plenitudinii sau corectitudinii perfectării formularului electronic de documentare acazului de gestiune a incidentului de securitate cibernetică (obligativitate conținut date, corectitudine tip date inserate, integritate date introduse etc.).	Corespunde
CF 08.15.	M	Doar un formular electronic de documentare a cazului de gestiune aincidentului de securitate cibernetică care a trecut cu succes procedura de verificare a corectitudinii perfectării va putea trece în statutul final sau expediat spre aprobare Decidentului (în cazul când formularul necesită aprobare).	Corespunde
CF 08.16.	M	SIA RSISC va asigura mecanism de trasabilitate (păstrarea istoricului) lapropagarea modificărilor în fișa incidentului de securitate cibernetică (toate evenimentele de adăugare, modificare, suprimare date, precum și vizualizare conținut dosar vor fi accesibile spre vizualizare).	mecanismul de urmărire (stocare istorică) va efectua stocarea (și vizualizarea) tuturor evenimentelor (inclusiv statutele) de procesare a obiectului informațional
CF 08.17.	M	SIA RSISC va furniza Registratorilor funcționalitate de semnare electronică a formularelor electronice de documentare a cazului degestiune a incidentului de securitate cibernetică (dacă această obligativitate este inclusă configurațiile formularului definite prin intermediul CU12).	Corespunde
CF 08.18.	M	În calitate de mecanism de aplicare a semnăturii electronice va fifolosit serviciul guvernamental MSign.	Corespunde
CF 08.19.	M	SIA RSISC va jurnaliza toate evenimentele de gestiune a dosarului cazului de utilizare prin intermediul serviciului guvernamental MLog.	Corespunde
CF 08.1.01.	M	SIA RSISC va furniza funcționalitate de deschidere a unui caz degestiune a incidentului de securitate cibernetică în baza: • alertelor de securitate cibernetică raportate prin intermediulCU04.1 • alertelor de securitate cibernetică recepționate prinintermediul	Corespunde

		CU18; • incidentelor de securitate cibernetică raportate prin intermediul CU04.2; • Incidentelor de securitate cibernetică recepționate prinintermediul CU17.	
CF 08.1.02.	M	Pentru deschiderea cazului de gestiune a evenimentului de securitatecibernetică este necesară: • Identificarea alertei sau incidentului de securitate ciberneticărelevant; • completarea metadatelor aferente fișei de securitatecibernetică; • definirea persoanelor responsabile în documentarea șisoluționarea incidentului de securitate cibernetică; • atașarea copiilor electronice și metadatelor asociate ale documentelor specifice deschiderii cazului de gestiune aincidentului de securitate cibernetică.	Corespunde
CF 08.1.03.	M	Unui dosar ai cazului de gestiune a incidentului de securitate cibernetică îi pot fi atașate mai multe alerte de securitate ciberneticăsau incidente de securitate cibernetică raportate.	Corespunde. În cazul în care mai multe alerte sau incidente de securitate cibernetică provin din mai multe surse diferite
CF 08.1.04.	M	SIA RSISC va efectua o verificare a completitudinii dosarului și corectitudinii datelor introduse anterior deschiderii cazului degestiune a incidentului de securitate cibernetică.	Corespunde
CF 08.1.05.	M	Registratorul va activa un buton specializat pentru deschiderea cazuluiîn cazul când validarea CF 08.1.04 a trecut cu succes.	Corespunde
CF 08.1.06.	M	Odată deschis cazul, SIA RSISC va notifica toți utilizatorii autorizațicazului și raportatorul/sursa alertei sau incidentului de securitatecibernetică (în cazul existenței adresei E-mail în profilul acestuia) asupra deschiderii unui nou caz de gestiune a incidentului de securitate cibernetică.	Corespunde
CF 08.1.07.	M	Un caz de gestiune a incidentului de securitate cibernetică poate treceîn statut „Închis” în cazul în care toate procesele de evaluare, documentare și soluționare a incidentului de securitate cibernetică au fost finisate.	Corespunde
CF 08.1.08.	M	Registratorul va dispune de funcționalitate de închidere a cazului degestiune a incidentului de securitate cibernetică (buton specializat pentru schimbarea statutului).	Corespunde
CF 08.1.09.	M	SIA RSISC va efectua o verificare a plenitudinii dosarului cazului de gestiune a incidentului de securitate cibernetică și doar în cazul lipsei problemelor cazul de gestiune a incidentului de securitate ciberneticăva putea fi închis.	Corespunde
CF 08.1.08.	M	Cazurile de gestiune a incidentelor de securitate cibernetică incomplete sau care au depășit termenul	Corespunde

		limită de soluționare vor fiînchise cu un statut special cu mențiunea cauzei închiderii cazului.	
CF 08.1.08.	M	Odată închis cazul de gestiune a incidentului de securitate cibernetică,SIA RSISC va notifica toți utilizatorii autorizați cazului și raportatorul incidentului de securitate cibernetică (dacă există E-mail de contact înprofilul acestuia).	Corespunde
CF 08.1.08.	M	Toate evenimentele de business aferente fișei incidentului de securitate cibernetică trebuie jurnalizate exhaustiv prin intermediul mijloacelor proprii ale SIA RSISC și în paralel prin intermediul serviciului de platformă MLog.	Corespunde
CF 08.2.01.	M	SIA RSISC va furniza formular de documentare a incidentului desecuritate cibernetică.	Corespunde
CF 08.2.02.	M	Conținutul formularului de documentare a incidentului de securitate cibernetică și fluxul de lucru aferent vor fi configurate prin intermediulCU12.	Corespunde
CF 08.2.03.	M	Documentarea unui incident de securitate cibernetică presupunecolectarea și introducerea următoarelor categorii de date: • rezultatele analizei preliminare a incidentului de securitatecibernetică; • detaliile evenimentelor adverse (dacă există); • categoria incidentului; • tipul de impact al incidentului; • rezultatul evaluării primare a impactului și a rezultatelorproduse de incidentul de securitate cibernetică; • rezultatul evaluării preliminare a urgenței soluționăriiincidentului de securitate cibernetică; • prioritatea de soluționare a incidentului de securitate cibernetică; • alte categorii de date relevante.	Corespunde
CF 08.2.04.	M	Formularul de documentare primară a incidentului de securitate cibernetică va dispune de posibilitate de atașare a copiilor electronice ale documentelor (exemplu: fișiere log, capturi de ecran, seturi de date specifice etc.).	Corespunde
CF 08.2.05.	M	Un formular de documentare a incidentului de securitate cibernetică se consideră finisat în cazul în care este semnat de Registratorul care l- a completat.	Corespunde
CF 08.3.01.	M	SIA RSISC va furniza formular de comunicare și escaladare a incidentului de securitate cibernetică.	Corespunde
CF 08.3.02.	M	Conținutul formularului de comunicare și escaladare a incidentului de securitate cibernetică și fluxul de lucru aferent vor fi configurate prin intermediul CU12.	Corespunde
CF 08.3.03.	M	Escaladarea și comunicarea unui incident de securitate cibernetică presupune identificarea și introducerea următoarelor categorii dedate: • echipa responsabilă de soluționarea incidentului de securitatecibernetică; • personalul responsabil de soluționare a incidentului de securitate cibernetică; • nivelele ierarhice implicate în	Corespunde

		escaladarea incidentului desecuritate cibernetică; • instituțiile externe implicate în escaladarea incidentului desecuritate cibernetică.	
CF 08.3.04.	M	Formularul de escaladare și documentare a incidentului de securitate cibernetică va dispune de posibilitate de atașare a copiilor electronice ale documentelor (exemplu: contracte prestări servicii, acorduri SLA, planuri de continuitate etc.).	Corespunde
CF 08.3.05.	M	Un formular de escaladare și comunicare a incidentului de securitate cibernetică se consideră finisat în cazul în care este semnat de Registratorul care l-a completat.	Corespunde
CF 08.3.06.	M	Odată finisat și semnat formularul electronic destinat escaladării și comunicării incidentului de securitate cibernetică, SIA RSISC va notifica toți actorii care urmează a fi implicați în procesul de soluționare a incidentului (introduși prin intermediul CF 08.3.03) și va asigura acces la fișa incidentului de securitate cibernetică.	Corespunde
CF 08.4.01.	M	SIA RSISC va furniza toate formularele electronice necesare documentării procesului de soluționare a incidentului de securitate cibernetică.	Corespunde
CF 08.4.02.	M	Conținutul formularelor electronice destinate documentării măsurilor de soluționare a incidentului de securitate cibernetică și fluxurile de lucru aferente vor fi configurate prin intermediul CU12.	Corespunde
CF 08.4.03.	M	Documentarea procesului de soluționare a incidentului informaticpresupune perfectarea formularelor electronice destinate documentării următoarelor etape de soluționare a incidentului desecuritate cibernetică: • investigarea incidentului de securitate cibernetică; • izolarea resursei informatice afectate de incidentul desecuritate cibernetică; • tratarea incidentului de securitate cibernetică; • recuperarea resursei informatice afectate de incidentul desecuritate cibernetică; • revizuirea și documentarea (inclusiv îmbunătățirea procedurilor existente, formularea recomandărilor, evaluarea eficacității măsurilor întreprinse etc.).	Corespunde
CF 08.4.04.	M	Formularele electronice destinate documentării procesului de soluționare a incidentului de securitate cibernetică va dispune de posibilitate de atașare a copiilor electronice ale documentelor (utilizate în calitate de dovezi pentru acțiunile întreprinse).	Corespunde
CF 08.4.05.	M	Un formular de documentare a procesului de soluționare a incidentului de securitate cibernetică se consideră finisat în cazul în care este semnat de Registratorul care l-a completat.	Corespunde
CF 08.4.06.	M	Odată finisat și semnat formularul electronic destinat escaladării și comunicării incidentului de securitate	Corespunde

		cibernetică, SIA RSISC va notifica toți actorii care urmează a fi implicați în procesul de soluționare a incidentului (introduși prin intermediul CF 08.3.03) și va asigura acces la fișa incidentului de securitate cibernetică.	
CF 08.5.01.	M	SIA RSISC va furniza formularele electronic destinat introducerii rezultatelor analizei follow-up a incidentului de securitate cibernetică destinat investigării eficienței tratării incidentului de securitate cibernetică și documentării lecțiilor învățate.	Corespunde
CF 08.5.02.	M	Conținutul formularului electronic destinat analizei follow-up a incidentului de securitate cibernetică și fluxul de lucru aferent vor fi configurate prin intermediul CU12.	Corespunde
CF 08.5.03.	M	Analiza follow-up a unui incident de securitate cibernetică presupuneidentificarea și introducerea următoarelor categorii de date (o partevor fi preluate din formularele deja perfectate a cazului de gestiune a incidentului de securitate cibernetică): • datele de identificare a incidentului de securitate cibernetică; • datele de clasificare a incidentului de securitate cibernetică; • obiectivele analizei follow-up; • date privind timpul de reacție per fiecare fază de gestiune aincidentului de securitate cibernetică; • date privind indicatorii de performanță a proceselor desoluționare a incidentului de securitate cibernetică.	Corespunde
CF 08.5.04.	M	Raportul de analiză follow-up a incidentului de securitate ciberneticăse perfectează conform șablonului inclus în anexa A1.3.	Corespunde
CF 08.5.05.	M	Formularul raportului de analiză follow-up a incidentului de securitatecibernetică va dispune de posibilitate de atașare a copiilor electroniceale documentelor.	Corespunde
CF 08.5.06.	M	Un formular de perfectare a raportului de analiză follow-up a incidentului de securitate cibernetică se consideră finisat în cazul încare este semnat de Registratorul care l-a completat.	Corespunde
CF 08.5.07.	M	Un formular de analiză follow-up nu poate fi perfectat dacă fișa incidentului de securitate cibernetică nu este complet (nu au fostfinisate etapele definite de CU08.1-CU08.4) și reprezintă constrângerea de bază pentru închiderea unui caz de gestiune aincidentului de securitate cibernetică.	Corespunde

15.9 CU09: Aprob/resping proiecte

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
CF 09.01.	M	SIA RSISC va furniza actorilor autorizați (cu rol decident) mecanism deaprobare sau respingere a proiectelor de formulare perfectate de utilizatori autorizați (cu rol de Registrator) care necesită aprobare înainte de a fi salvate sau procesate.	Corespunde

CF 09.02.	M	Obligativitatea aprobării formularului electronic este configurată prinintermediul CU12 și va cuprinde setul de formulare perfectate prin intermediul CU08.	Corespunde
CF 09.03.	M	Lista completă a formularelor electronice care vor necesita aprobări din partea rolurilor decidente vor fi identificate în procesul analizei debusiness.	Corespunde
CF 09.04.	M	Aprobarea sau respingerea constă în perfectarea unei note, alegereastatutului (Aprobat sau Respins), confirmarea acestuia și aplicarea semnăturii electronice a utilizatorului cu rol decident.	Corespunde
CF 09.05.	M	Accesul la funcționalitatea de aprobare/respingere a proiectului va fiposibilă numai în cazul în care utilizatorul cu rol Decident dispune deasemenea împuternicire (verificarea se va face prin intermediul MPower).	Corespunde
CF 09.06.	M	SIA RSISC va utiliza serviciul de platformă MSign pentru aplicareasemnăturii electronice la Aprobarea/Respingerea formularului electronic.	Corespunde
CF 09.07.	M	În cazul aprobării formularului electronic, SIA RSISC va notifica toțiutilizatorii relevanți acestuia privind evenimentul de aprobare/respingere.	Corespunde
CF 09.08.	M	În cazul respingerii formularului electronic, fluxul de lucru va trece automat la etapa precedentă (va întoarce spre reperfectare formularul utilizatorului care l-a expediat spre aprobare) și va notificatoți utilizatorii relevanți.	Corespunde
CF 09.09.	M	În momentul în care un formular este expediat spre aprobare acestanu poate fi modificat decât de decidentul care trebuie să-l aprobe cuaplicarea repetată a semnăturii electronice.	Corespunde
CF 09.10.	M	SIA RSISC va jurnaliza toate evenimentelor de aprobare/respingere aproiectelor de formulare electronice.	Corespunde

15.10 CU10: Gestionez conținut interfață publică

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
CF 10.01.	M	SIA RSISC va furniza un mecanism de gestiune a interfeței publicedestinate accesării de către utilizatori anonimi.	Corespunde
CF 10.02.	M	Mecanismul de gestiune a interfeței publice destinate accesării de către utilizatori anonimi și candidați trebuie să furnizeze următoarele funcționalități: • gestiunea meniului de navigare; • configurarea paginii principale; • gestiunea informației de conținut (noutăți, F.A.Q., publicații,informație multimedia); • gestiunea materialelor instructiv metodice; • gestiunea studiilor de caz.	Corespunde
CF 10.03.	M	SIA RSISC va furniza un mecanism de gestiune a structurii conținutuluiinterfeței publice în baza căreia va fi afișat meniul de navigare.	Corespunde
CF 10.04.	I	Structura interfeței publice a SIA RSISC reprezintă un arbore cunelimitat în nivele ierarhice frunzele căruia conțin informația deconținut.	Corespunde

CF 10.05.	M	SIA RSISC va furniza funcționalitate de reorganizare a arborelui de structură a interfeței publice (mutare subcategorie dintr-o categorie înalta, ascundere/ștergere categorii ale arborelui de structură, redenumire a categoriilor arborelui de structură etc.).	Corespunde
CF 10.06.	M	Pentru categoriile de structură a arborelui de structură se va puteadefini: • informație de conținut (adăugare/modificare/ștergere informație de conținut); • URL de acces la modulele interfeței publice sau accesare aresurselor externe; • Subcategorii subordonate.	Corespunde
CF 10.07.	M	SIA RSISC nu va permite suprimarea unei categorii de structură dacă conține cel puțin un document de conținut sau categorie subordonată.	Corespunde
CF 10.08.	M	SIA RSISC va furniza un mecanism de gestiune a paginii principale a interfeței publice.	Corespunde
CF 10.09.	I	Pagina principală reprezintă un mecanism de acces rapid la serviciile și facilitățile interfeței publice.	Corespunde
CF 10.10.	M	Pentru pagina principală a interfeței publice a SIA RSISC trebuie săexiste următoarele facilități de configurare: • definire aspect de prezentare a informației (număr de culoareafișate, compartimente și ordinea lor de afișare pe Pagina Principale); • configurarea blocurilor cu informații extrase din conținutulinformațional al interfeței publice; • configurarea zonelor cu bannere de acces la serviciile SIARSISC, resurse STISC sau externe; • configurarea accesului la serviciile electronice accesibile prinintermediul SIA RSISC; • gestiunea informației plasate în subsolul Paginii Principale și ainterfeței publice.	Corespunde
CF 10.11.	M	SIA RSISC va dispune de funcționalitate de configurare a accesului la serviciile electronice oferite prin intermediul interfeței publice.	Corespunde
CF 10.12.	M	Serviciile electronice furnizate de SIA RSISC (exemplu: raportare alertă/incident) vor fi implementate prin intermediul unor module dedicate interfața cărora va fi posibilă a fi integrată în paginile interfeței publice a SIA RSISC.	Corespunde
CF 10.13.	M	Serviciile electronice integrate în interfața publică a SIA RSISC vor putea fie accesate la URL-uri permanente.	Corespunde
CF 10.14.	M	SIA RSISC va dispune de funcționalitate de gestiune a conținutului informațional prin intermediul unor facilități specifice Sistemelor deGestiune a Conținutului care va furniza următoarele funcționalități: • redactarea și publicarea documentelor prin intermediul editoarelor WYSIWYG;	Corespunde

		• încărcarea de fișiere și imagini în conținutul documentelorpublicate sau atașarea lor acestor documente; • încărcarea și publicarea informației multimedia (video); • publicarea informației multimedia din surse externe(exemplu: Youtube).	
CF 10.15.	M	Toate documentele de conținut și metadatele atașate acestora publicate prin intermediul interfeței publice a SIA RSISC trebuie să corespundă rigorilor Hotărârii Guvernului nr. 188 din 03.04.2012 privind paginile oficiale ale autorităților administrației publice în rețeaua Internet.	Corespunde
CF 10.16.	M	SIA RSISC va furniza funcționalități pentru gestiunea unei baze de cunoștințe care să conțină informații instructiv metodice în domeniul gestiunii incidentelor de securitate.	Corespunde
CF 10.17.	M	SIA RSISC va furniza funcționalități de definire și gestiune a structurii bazei de cunoștințe.	Corespunde
CF 10.18.	M	SIA RSISC trebuie să fie capabil să plaseze (și afișeze ulterior ininterfața publică) următoarele tipuri de conținut în baza de cunoștințe: (materiale instructiv-metodice) • documente în format HTML (redactate cu ajutorul editoarelorWYSIWYG); • ghiduri/instrucțiuni încărcate în format PDF, DOC/DOCX,PPT/PPTX etc. • referințe la cadrul legal în vigoare conținut în Registrul de Statal Actelor Juridice (https://www.legis.md); • informație multimedia încărcată nemijlocit în cadrul SIA RSISCsau publicată prin intermediul resurselor externe (exemplu: Youtube, Rețele de socializare etc.); • studii de caz, extrase în baza dosarelor cazurilor de gestiune aincidentelor de securitate.	Corespunde

15.11 CU11: Administrez utilizatori și controlul accesului

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
CF 11.01.	M	SIA RSISC va furniza funcționalitate de definire și gestiune dinamică autilizatorilor, rolurilor și drepturilor de acces a acestora.	Corespunde
CF 11.02.	M	Fiecare utilizator autorizat va dispune de un profil cu următoarelecategorii de date: • nume utilizator; • prenume utilizator; • adresă E-mail de contact; • număr telefon de contact; • login de acces; • parolă de acces; • strategie de autentificare (utilizator+parolă,	Corespunde

		MPass etc.); • cont activ/dezactivat; • perioadă de valabilitate a accesului; • rolurile utilizatorului; • drepturi particulare de acces la interfața utilizator și date; • alte date relevante.	
CF 11.03.	M	SIA RSISC va conține o categorie implicită de utilizatori creată de Furnizor și credențialele pentru acesta sunt remise la livrare pentrucategoria de superadministrator.	Corespunde
CF 11.04.	M	SIA RSISC trebuie să asigure accesul la unele funcționalități specificedoar după autentificarea și autorizarea utilizatorului. SIA RSISC va asigura suport pentru următoarele alternative de autentificare a utilizatorilor: • semnătură electronică (prin intermediul serviciului MPass); • login și parolă;	Corespunde
CF 11.05.	M	Gestionarea utilizatorilor precum si a rolurilor atribuite in sistem se vaefectua prin intermediul MPass.	Corespunde
CF 11.06.	M	SIA RSISC va furniza mecanism de definire pentru utilizatori a drepturilor de acces la date în funcție categoriile sau tipurile dealerte/incidente, arealul geografic, categorii specific de date etc.ținându-se cont de atribuțiile de serviciu a utilizatorul autorizat.	Corespunde
CF 11.07.	M	SIA RSISC va furniza utilizatorilor autorizați funcționalități demodificare și restabilire a parolei de acces.	Corespunde
CF 11.08.	M	SAI SPM va asigura protecție parolelor utilizatorilor autorizați. Metodade protecție utilizată trebuie să asigure imposibilitatea interceptării, deducerii și recuperare a parolei de acces.	Corespunde
CF 11.09.	M	SIA RSISC va permite blocarea/deblocarea accesului utilizatorului.	Corespunde
CF 11.10.	M	Comunicarea între dispozitivul utilizatorului și serverul aplicație a SIARSISC trebuie să fie criptată (utilizând protocolul SSL/TLS).	Corespunde
CF 11.11.	M	SIA RSISC trebuie să fie capabil să configureze numărul de sesiuniparalele posibile de a fi inițiate de același utilizator.	Corespunde
CF 11.12.	M	SIA RSISC trebuie să fie capabil să configureze perioada de inactivitatea utilizatorului după care sesiunea urmează a fi închisă în mod automat.	Corespunde
CF 11.13.	M	SIA RSISC trebuie să prevină orice posibilitate de preluare neautorizată a sesiunilor active inițiate de utilizatorii autorizați	Corespunde
CF 11.14.	M	SIA RSISC va permite blocarea sesiunii la cererea utilizatorului sauautomat la expirarea sesiunii utilizatorului.	Corespunde
CF 11.15.	M	Un Profil de utilizator autorizat poate fi eliminat fizic doar în cazulcând nu există evenimente jurnalizate sau înregistrări aferente acestuia.	Corespunde
CF 11.16.	M	SIA RSISC trebuie să furnizeze un mecanism de gestiune granulară adrepturilor de acces la obiectele sale și a acțiunilor posibile asupra acestora (alerte de securitate cibernetică raportate, incidente de securitate cibernetică raportate, cazuri de	Corespunde

		gestiune a incidentelor de securitate cibernetică , formulare electronice, meniuri, funcționalități, rapoarte, acțiuni de adăugare/vizualizare/actualizare/ștergere date etc.).	
CF 11.17.	M	Metoda de autorizare a utilizatorilor SIA RSISC trebuie să se bazeze peprincipiul „*tot ce nu este permis este interzis*”.	Corespunde
CF 11.18.	M	SIA RSISC va furniza funcționalitate de definire a grupurilor și rolurilorutilizatorilor și facilități de asociere a utilizatorilor la grupuri și roluri.	SIA RSISC va oferi posibilitatea de a defini rolurile utilizatorilor (drepturi și niveluri de acces), precum și mijloacele de a atribui roluri unor utilizatori specifici.
CF 11.19.	M	Un rol este definit prin denumire generică, descriere succintă și statutul de activ/dezactivat. Rolurile dezactivate nu vor fi afișate laconfigurarea drepturilor de acces la resursele aplicației sau a drepturile utilizatorilor.	Corespunde
CF 11.20.	M	Odată introdus și activat, rolul va fi disponibil de a fi utilizat în modulele de gestiune a utilizatorilor (atașarea de roluri utilizatorilor) și gestiune a componentelor SIA RSISC (atașarea rolurilor care au acces la componentele interfeței utilizator și configurarea modalitățiide acces a acestora).	Corespunde
CF 11.21.	M	SIA RSISC trebuie să permită acordarea drepturilor de acces a la nivel de utilizator explicit, grup sau rol. Un grup de utilizatori poate cuprinde mai multe subgrupuri/roluri. Un utilizator poate fi asociat cuunul sau mai multe grupuri și roluri, iar drepturile de acces ale utilizatorului sunt determinate cumulativ.	Utilizatorilor li se vor atribui roluri. Fiecare rol va avea un set de drepturi și niveluri definite de acces la date și funcții. Unui utilizator i se pot atribui mai multe roluri, iar drepturile totale vor fi definite ca fiind suma drepturilor fiecărui rol atribuit (comutativ).
CF 11.22.	M	SIA RSISC trebuie să permită acordarea drepturilor de acces în bazaregulilor de afaceri (*exemplu: o înregistrare poate fi modificată doar atunci când utilizatorul este autorul acestuia sau când acțiunea de modificare este efectuată într-o anumită perioadă de timp, stare saucontext*).	Corespunde
CF 11.23.	M	Un rol nu va putea fi suprimat dacă acesta este atașat măcar unui utilizator sau unei componente ale interfeței utilizator a SIA RSISC.	Corespunde
CF 11.24.	M	SIA RSISC va furniza mecanism de înregistrare a componentelor interfeței utilizator (resurselor) în scopul asigurării unui mecanism dedefinire a drepturilor de acces a utilizatorilor la interfața utilizator. Prin componentă se înțelege orice entitate modulară a aplicației (formular, meniu, opțiune de meniu, câmp etc.) gradul de detaliere acăreia este suficientă pentru configurarea drepturilor de acces, tranzițiilor fluxurilor de lucru și acțiunilor accesibile utilizatorilor.	Pentru fiecare rol, în funcție de drepturile sale, va fi predefinită o listă de elemente ale formei (câmpuri, butoane, meniuri, etc.), la care rolul respectiv va avea acces.
CF 11.25.	M	SIA RSISC va permite configurarea ierarhiei componentelor interfețeiutilizator, la nivelul rădăcină fiind modulele de bază ale aplicației iar nivelele subordonate nu vor fi limitate în adâncime, ierarhia fiind determinată de arhitectura acestora.	Ierarhia elementelor interfeței utilizatorului va fi definită la etapa de dezvoltare a SIA RSISC. Schimbarea ierarhiei create anterior va necesita o

			modificare a codului formei vizuale
CF 11.26.	M	Orice componentă a interfeței utilizator SIA RSISC va conține date privind denumire generică, descriere succintă, acțiunile disponibile utilizatorilor (evenimentele de business pe care le pot genera) rolurilecare au acces la componenta interfeței utilizator sau acțiunile ce pot fiîntreprinse.	Datele enumerate vor fi descrise în Ghidul utilizatorului și în ajutorul pentru forma specifică..
CF 11.27.	M	Orice componentă a interfeței utilizator SIA RSISC va conține dateprivind, statutele prin care pot trece datele gestionate prin intermediul componentei, tranzițiile de parcurgere a statutelor componentei (configurare fluxuri de lucru).	Toate procesele de lucru în SIA RSISC, acțiunile utilizatorilor și accesul la forme (și la elemente) vor fi predefinite. Vor fi configurate drepturile rolurilor. Rolurile vor fi apoi atribuite unor utilizatori specifici.
CF 11.28.	M	SIA RSISC va permite definirea permisiunilor aferente acțiunilor(evenimentelor de business) disponibile utilizatorilor cu acces lacomponentele interfeței utilizator. Vor fi configurate următoarele categorii de acțiuni disponibileutilizatorilor: • vizualizare înregistrări; • adăugare înregistrări; • modificare înregistrări; • eliminarea înregistrări; • tranziție flux de lucru; • alte acțiuni relevante.	Setările specificate vor fi efectuate la nivelul drepturilor de rol.
CF 11.29.	M	SIA RSISC trebui să permită atribuirea temporară a drepturilor deținute de un utilizator către alt utilizator. Această atribuire trebuiefăcută prin păstrarea sau suspendarea drepturilor deținute de utilizatorul căruia i se atribuie temporar drepturile. Aceste împuterniciri urmează a fi definite/verificate prin intermediul serviciului de platformă MPower.	Corespunde
CF 11.30.	D	SIA RSISC trebuie să permită separarea activităților administrative (*exemplu: Administratorul 1 face modificările și Administratorul 2 leconfirmă*).	Corespunde
CF 11.31.	M	SIA RSISC trebuie să furnizeze facilități pentru vizualizare și generareade rapoarte cu privire la drepturile de acces configurate. Generarea unor asemenea rapoarte trebuie efectuată în funcție de cel puțin următoarele criterii: grup de utilizatori/rol, login, proprietăți,acțiuni permise.	Corespunde

15.12 CU12: Gestionez fluxuri, formulare și șabloane

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
CF 12.01.	M	SIA RSISC va dispune de mecanism de gestiune a resurselor program(module, formulare electronice, opțiuni de meniu, butoane etc.) pentru configurarea fluxurilor de lucru și definirea regulilor de procesare a acestora pentru toate scenariile aferente proceselor de raportare a alertelor sau incidentelor de securitate	Toate procesele de lucru în SIA RSISC, acțiunile utilizatorilor și accesul la forme (și la elemente) vor fi predefinite.

		cibernetică și a cazurilor de gestiune a incidentelor de securitate cibernetică.	Toate formele și modelul lor vor fi prestabilite și aprobate de către solicitant. SIA RSISC se consideră un mecanism bazat pe roluri. Fiecare rol va avea propriul set de drepturi. Rolurile vor fi atribuite unor utilizatori specifici. Drepturile rolurilor vor fi configurabile (acces la date: vizualizare, ștergere, editare, acces la forme și vizualizarea elementelor formei etc.).
CF 12.02.	M	Gestiunea fluxurilor de lucru trebuie să se poată realiza folosind interfața grafică a sistemului informatic în care utilizatorul lucrează înmod obișnuit.	
CF 12.03.	M	Fluxurile de lucru vor fi definite prin specificarea stărilor în care poatetrece un formular electronic și pașii de procesare (etapele sau tranzițiile de evoluție a fluxului de lucru și acțiunile ce pot fi făcute în starea concretă a formularului) realizați de utilizatori cu roluri specifice.	
CF 12.04.	M	Un flux de lucru va fi implementat ca o colecție de activități prin caretrece un formular electronic perfectat în cadrul proceselor de business ce se desfășoară secvențial.	Busines-procesele vor fi definite ca un set de activități repetitive, legate logic (sau o secvență a acestora) pe care actorii din sistem le pot efectua. Toate busines-procesele de afaceri din cadrul SIA RSISC vor fi definite în prealabil.
CF 12.05.	M	Numărul de pași ce pot fi incluși într-un flux nu trebuie să fie limitat.În așa fel soluția informatică va fi adaptabilă modificărilor metodologiei de lucru cu documentele procesate în cadrul procedurilor de gestiune a cazurilor de gestiune a incidentelor de securitate cibernetică.	Numărul de acțiuni incluse într-un busines-proces este nelimitat. Pentru a adapta busines-procesul la cerințele modificate, va fi necesară modificarea codului.
CF 12.06.	D	Un flux de lucru trebuie să poată avea asociat un coordonator (supervizor). Coordonatorul trebuie să poată primi mesajele deavertizare (notificări) generate de rularea fluxului respectiv. Utilizatorul care lansează un formular spre procesare pe un flux delucru trebuie să poată specifica cine este supervizorul fluxului.	Atunci când apar anumite evenimente în SIA RSISC (când sunt executate anumite business-procese), persoana desemnată (coordonatorul BP) va primi mesajul/notificarea corespunzătoare. Utilizatorul care inițiază mesajul poate specifica destinatarul.
CF 12.07.	M	Furnizorul va configura fluxurile de procesare a formularelor electronice destinate perfectării tuturor evenimentelor de business aferente proceselor de raportare a alertelor de securitate cibernetică și cazurilor de gestiune a incidentelor de securitate cibernetică.	Fluxurile de procesare a formularelor electronice asociate cu procesele de raportare a alertelor de securitate cibernetică și de gestionare a incidentelor de securitate cibernetică vor fi configurate de către furnizor. Toate formele și modelul lor vor fi prestabilite și aprobate de către solicitant.
CF 12.08.	M	SIA RSISC va oferi un mecanism de configurare a formularelor electronice utilizate în interfața utilizator destinată raportării alertelorde securitate cibernetică și cazurile e gestiune a incidentelor de securitate.	SIA RSISC va furniza mecanisme pentru configurarea textului static în șabloanele notificărilor.
CF 12.09.	M	SIA RSISC va oferi mecanisme de configurare a șabloanelor de documente (și rapoartelor) aferente proceselor de business implementate (șabloanele vor avea o structură bine definită care va permite	Corespunde

		modificarea aspectului și conținutului documentului extras).	
CF 12.10.	D	Este binevenit ca șabloanele de documente și rapoarte să fie configurate prin intermediul unei platforme de configurare șigenerare a rapoartelor (*Exemplu: JasperReports,*	Corespunde
CF 12.11.	M	Toate șabloanele de documente și rapoarte configurate prinintermediul CF 12.09 – CF 12.10 vor fi utilizate la generarearapoartelor/documentelor prin intermediul CU05 și CU15.	Corespunde
CF 12.12.	M	Dezvoltatorul va configura la cererea Beneficiarului până la 20 șabloane de documente și 20 șabloane de rapoarte ce urmează a figenerate de SIA RSISC.	Corespunde

15.13 CU13: Gestionez metadate

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
CF 13.01.	M	SIA RSISC va furniza mecanism de gestiune a nomenclatoarelor, clasificatoarelor ce conțin totalitatea metadatelor destinate configurării sistemului informatic și gestiunii proceselor de raportare aalertelor de securitate cibernetică și a gestiunii incidentelor de securitate cibernetică.	Corespunde
CF 13.02.	M	Următoarele categorii de metadate urmează a fi utilizate în cadrul SIARSISC: • **Clasificatoare Internaționale**, valorile cărora sunt standardizate și acceptate la nivel internațional (exemplu: Clasificatorul Internațional al Unităților de Măsură – SI, clasificatorul țărilor etc.); • **Clasificatoare oficiale naționale** (exemplu: Clasificatorului Unităților Administrativ-Teritoriale al Republicii Moldova etc.); • **Clasificatoare/nomenclatoare de interoperabilitate** (valorilecărora sunt utilizate pentru implementarea schimbului de date cu sisteme informatice terțe); • **Clasificatoare/nomenclatoare interne** (exemplu: variabile de sistem, parametri ai interfeței utilizator, parametri de configurare a sistemului informatic și proceselor implementate în cadrul sistemului informatic, roluri, metadatede trafic telecomunicațional, categorii de incidente, tipuri de impact, nivelul impactului, urgența soluționării incidentului, prioritățile de soluționare a incidentelor, nivele ierarhice de escaladare a incidentelor, surse de date etc.).	Corespunde
CF 13.03.	M	Furnizorul trebuie să implementeze mecanism destinat actualizării automate a metadatelor (dacă acestea există) necesare implementăriischimbului de date cu sisteme informatice externe.	Corespunde, dar sistemele externe ar trebui să dispună de mecanisme gata pregătite pentru a furniza date modificate
CF 13.04.	M	SIA RSISC va furniza mecanism de export și import a clasificatoarelor din interfața utilizator în format XML	Corespunde

		sau CSV. Drepturile de import și export vor fi atribuite utilizatorilor cu rolul de Administrator deSistem.	
CF 13.05.	M	Pentru clasificatoarele oficiale, internaționale și cele furnizate de sistemele informatice externe cu care efectuează schimbul reciproc dedate vor fi limitate drepturile de modificare a valorilor prin intermediul facilităților SIA RSISC.	Corespunde
CF 13.06.	M	Pentru sistemul de clasificatoare/nomenclatoare și metadate interne,SIA RSISC va livra mecanism de definire și administrare dinamică a acestora (trebuie să fie posibilă adăugarea dinamică a categoriilor de nomenclatoare/clasificatoare și a conținutului acestora).	Corespunde
CF 13.07.	M	SIA RSISC va furniza funcționalitate de gestiune a valorilor textuale aclasificatoarelor/nomenclatoarelor altor categorii de metadate în 3versiuni lingvistice: Română, Engleză și Rusă.	Corespunde
CF 13.08.	M	SIA RSISC va furniza funcționalitate de gestiune a etichetelor șimesajelor interfeței utilizator în 3 versiuni lingvistice: Română,Engleză și Rusă.	Corespunde
CF 13.09.	M	SIA RSISC nu va permite eliminare unei categorii de metadate dacăaceasta este utilizată cel puțin într-o înregistrare a bazei de date.	Corespunde
CF 13.10.	M	SIA RSISC va oferi mecanism de versionare a valorilor metadatelor șistabilite a intervalului de timp aferent validității valorilor metadator.	Corespunde

15.14 CU14: Configurez sistem informatic

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
CF 14.01.	M	SIA RSISC va dispune de facilități de configurare a strategiilor dejurnalizare a evenimentelor de business.	Corespunde
CF 14.02.	M	SIA RSISC va dispune de facilități de configurare a rapoartelor existente (*exemplu: ajustarea seturilor de date, reformatarea rapoartelor etc.*) modificând fișierele șabloanelor implementate sauplatforme specializate (*exemplu: utilizarea generatoarelor de rapoarte*).	Corespunde
CF 14.03.	D	SIA RSISC trebuie să permită adăugarea și configurarea unor noirapoarte.	Corespunde
CF 14.04.	M	SIA RSISC trebuie să dispună de facilități pentru a configura rapoartelor ce urmează a fi generate periodic automat. Generarea automată este specifică pentru rapoartele complexe care necesită un timp îndelungat de procesare a datelor. Rapoartele generate automat vor fi stocate în sistem (pentru a fi accesate de utilizatorii autorizați) sau trimise la adrese e-mail sau utilizatori concreți.	Corespunde
CF 14.05.	M	SIA RSISC va dispune de funcționalitate de definire a termenului devalabilitate a formularelor electronice aflate în statut „Proiect” dupăcare pot fi suprimate automat.	Corespunde
CF 14.06.	M	SIA RSISC trebuie dispună de funcționalități destinate configurării job-urilor care trebuie să ruleze automat în funcție de parametrii de timp sau producerea anumitor evenimente de business.	Corespunde Toate sarcinile, care urmează să fie efectuate conform orarului, trebuie definite în prealabil și

		SIA RSISC trebuie să permită adăugarea și configurarea de job-uri noiprecum și modificarea parametrilor de funcționare a job-urilor existente.	implementate la etapa de proiectare a sistemului.
CF 14.07.	M	SIA RSISC va furniza funcționalitate de import manual a datelor primare în baza unor fișiere tipizate cu structură predefinită. Această funcționalitate urmează a fi utilizate pentru sincronizarea în regim manual cu sursele de date oficiale (în cazul inaccesibilității facilitățilorde interoperabilitate).	Corespunde
CF 14.08.	M	Datele potențial variabile ale SIA RSISC (parametrii de funcționare, valorile constantelor, căile de acces la fișiere/date, parametrii de integrare cu sisteme informatice externe, metadatele specifice etc.) trebuie să poată fi configurabile prin intermediul facilităților oferite deinterfața utilizator fără a fi necesară compilarea și/sau desfășurarea repetată a codului sursă sau intervenții directe în conținutul bazei de date.	Corespunde

15.15 CU15: Monitoring operațional, diagnostică și soluționare problem

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
CF 15.01.	M	SIA RSISC va avea încorporat un serviciu Heartbeat care va comunicaperiodic statutul curent de funcționare a sistemului informatic.	Corespunde
CF 15.02.	M	SIA RSISC trebuie să conțină mecanisme de monitorizare a gradului deîncărcare și statutul curent al tuturor componentelor cheie (Furnizorultrebuie să furnizeze soluție software de monitorizare a performanței SIA RSISC).	Având în vedere faptul că sistemul țintă ar trebui plasat în MCloud, se vor utiliza soluții standard gata, pentru a monitoriza volumul de lucru și starea componentelor existente în MCloud. Pentru arhitectura Microsoft monitorizarea încărcării se va efectua pe containere (serviciul HealthCheck).
CF 15.03.	M	SIA RSISC trebuie să expedieze notificări rolurilor relevante în cazul când performanța componentelor sale este în degradare (*exemplu: timpul de răspuns la unele interogări este mai mare decât celașteptat*).	Corespunde
CF 15.04.	M	Furnizorul trebuie să asigure facilități de administrare a SIA RSISCdupă cum urmează: • startarea componentelor SIA RSISC; • oprirea componentelor SIA RSISC; • restartarea componentelor SIA RSISC; • generarea copiilor de rezervă; • restabilirea datelor în baza copiilor de rezervă; • împrospătarea memoriei operaționale.	Corespunde
CF 15.05.	M	Mijloacele care implementează funcțiile de administrare a SIA RSISC pot fi implementate folosind comenzile și facilitățile software-ului de platformă,	Sistemul va fi administrat prin intermediul unor

		fără a fi nevoie de implementarea unei interfețe grafice dedicate.	instrumente de administrare standard.
CF 15.06.	M	Furnizorul trebuie să enumere mijloacele care trebuie utilizate pentru depanarea problemelor tehnice de funcționare a SIA RSISC.	Mijloace care trebuie utilizate pentru a remedia problemele tehnice în funcționarea SIA RSISC: • Microsoft Visual Studio Community 2022 - pentru a remedia erorile din codul sursă al aplicației SIA RSISC • SQL Server Management Studio - pentru restaurarea bazei de date din backup, gestionarea sql job • IIS - pentru a reporni aplicația web și serviciile SIA RSISC. • Docker - pentru a actualiza aplicația SIA RSISC
CF 15.07.	M	SIA RSISC trebuie să fie în măsură să ofere un număr de rapoarte de management, de statistică și ad-hoc, astfel încât rolurile administrative să poată monitoriza activitatea și statutul sistemului.	Corespunde
CF 15.08.	I	Rapoartele gestionate prin intermediul CU15 sunt destinate funcțiilor de audit informatic și nu include rapoarte aferente evenimentelor de business specifice CU05.	Corespunde
CF 15.09.	M	Această raportare este necesară în cadrul întregului sistem, incluzând: • nomenclatoarele și clasificatoarele; • înregistrările bazei de date; • activitatea utilizatorului; • permisiunile de acces și securitate.	Corespunde
CF 15.10.	M	Rapoartele vor fi generate în baza următoarelor categorii de evenimente jurnalizate: • autentificare cu succes a utilizatorilor; • autentificare nereușită a utilizatorilor; • notificări expediate; • acțiuni asupra datelor (accesare, adăugare, modificare,eliminare).	Corespunde
CF 15.11.	M	SIA RSISC va permite extragerea agregată a rapoartelor sau detaliereaacestora per utilizator concret, subdiviziune centrală sau teritorială a STISC sau a unor grupuri de utilizatori.	Corespunde
CF 15.12.	M	Un utilizator care vizualizează un raport în cadrul sistemului, trebuiesă-l poată exporta în format PDF sau într-un fișier extern redactabil (XLS/XLSX, CSV, DOC/DOCX).	Corespunde
CF 15.13.	M	Furnizorul va implementa până la 10 rapoarte predefinite ale auditului informatic solicitate de STISC. Rapoartele de audit care pot fi generateprin intermediul mijloacelor de sistem nu vor fi implementate în interfața utilizator a SIA RSISC.	Corespunde
CF 15.14.	D	Pentru extragerea rapoartelor și statisticilor de sistem relevante CU15este binevenită utilizarea unei platforme dedicate configurării și generării rapoartelor.	Corespunde Va fi realizat în cazul, dacă acceptarea SIA RSISC va fi

			efectuată înainte de termenul stabilit

15.16 CU16: Execut proceduri automate

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
CF 16.01.	M	SIA RSISC va furniza funcționalitate de lansare a procedurilorautomate destinate funcționării în bune condiții a sistemuluiinformatic.	Corespunde
CF 16.02.	M	Momentul de timp și periodicitatea lansării spre execuție a procedurilor automate este configurat prin intermediul CF 14.05.	Corespunde
CF 16.03.	M	SIA RSISC va livra mecanism de generare automată a copiilor de rezervă (conform unor reguli prestabilite) în baza cărora să fie posibilărestabilirea funcționalității sistemului informatic în cazul producerii unor incidente de securitate.	Corespunde
CF 16.04.	M	SIA RSISC va livra mecanism de arhivare a datelor vechi și inutile proceselor de business curente ale STISC și eliminare a acestora de peplatforma de producție.	Corespunde
CF 16.05.	M	SIA RSISC va declanșa în mod automat procedurile de schimb reciprocde date cu sisteme informatice externe definite prin intermediul CU17.	Corespunde
CF 16.06.	M	SIA RSISC va șterge automat formularele electronice aflate în statut „Proiect” care au depășit termenul limită de aflare în acest statutconfigurat prin intermediul CU14.	Corespunde
CF 16.07.	M	SIA RSISC va fi capabil să efectueze periodic și planificat (în orele desolicitare minimă a SIA RSISC) calculele preliminare ale indicatorilornecesari generării în timp util a rapoartelor statistice complexe.	Corespunde
CF 16.08.	M	SIA RSISC identifica automat și expedia notificările ce trebuie expediate utilizatorilor autorizați ca urmare a unor evenimente debusiness (*exemplu: întârzieri în executarea sarcinilor*).	Corespunde
CF 16.09.	M	SIA RSISC trebuie să furnizeze interfață de vizualizare a statutuluicurent al procedurile executate automat în curs de procesare.	Corespunde
CF 16.10.	M	SIA RSISC trebuie să furnizeze facilități de gestiune a procedurilor automate planificate: • startarea manuală a procedurii automate; • oprirea din execuție a procedurii automate; • redemararea procedurii automate oprite anterior; • anularea executării procedurii automate.	Corespunde
CF 16.11.	M	SIA RSISC va publica periodic în cadrul interfeței publice și Partalului Datelor Deschise rapoarte și KPI cu caracter public produse în cadrulproceselor de business implementate.	Corespunde
CF 16.12.	M	Toate evenimente aferente funcționării procedurilor automate definite prin intermediul cerințelor funcționale CF 16.03 - CF 16.11trebuie jurnalizate.	Corespunde
CF 16.13.	M	SIA RSISC trebuie să furnizeze facilități de corelare, in baza dateloracumulate, precum si cele disponibile public (ipReputation,DomainReputation,BotNets,etc) precum si stabilirea gradului de risc in baza mai multor criterii.	Corespunde Determinarea gradului de risc se va face pe baza unor

			criterii care urmează să fie stabilite de către solicitant.
CF 16.14.	M	SIA RSISC trebuie să furnizeze facilități de identificare si ridicarea gradului de risc in baza clasificatoarelor precum si corelarea acestoracu MITRE ATT&CK®.	Corespunde

15.17 CU17: Schimb de date cu sisteme externe

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
CF 17.01.	M	SIA RSISC trebuie să fie dezvoltat în baza unei arhitecturi capabile săimplementeze facilități de interoperabilitate cu sisteme informaticeexterne.	Corespunde
CF 17.02.	M	SIA RSISC va efectua schimb de date cu sistemele informatice externeprin intermediul API-urilor expuse de acestea (cazul sistemelor informatice neguvernamentale) și platforma de interoperabilitate a MConnect (pentru cazul sistemelor informatice ale AP).	Corespunde
CF 17.03.	M	Interacțiunea SIA RSISC cu sistemele informatice interne ale STISC încazul în care serviciile de furnizate/recepționate a datelor nu sunt solicitate de sisteme informatice ale altor AP din Republica Moldova vor fi implementate prin intermediul microserviciilor.	Corespunde
CF 17.04.	M	SIA RSISC trebuie să fie capabil a se integra cu următoarele servicii de guvernamentale: • MPass - pentru autentificare și controlul accesuluiutilizatorilor; • MSign - pentru aplicarea semnăturii electronice în cadrulproceselor de business ale SIA RSISC; • MLog - pentru jurnalizarea evenimentelor de business critice; • MNotify - pentru notificarea utilizatorilor autorizați; • MPower - pentru verificarea împuternicirilor de reprezentarea utilizatorilor necesare autorizării acțiunilor acestora; • PDGD - pentru publicarea seturilor publice de date produse încadrul fluxurilor de lucru ale SIA RSISC.	Corespunde
CF 17.05.	M	SIA RSISC se va integra prin intermediul platformei guvernamentale MConnect cu următoarele sisteme informatice pentru recepționarea datelor aferente alertelor și incidentelor de securitate: • Sisteme informatice ale AP - care vor expedia în mod automatalerte de securitate cibernetică în cazul producerii unor evenimente considerate cu risc major asupra securității informației; • Soluțiilor software de monitorizare a infrastructurii TIC a AP -care vor expedia în mod automat alerte de securitate cibernetică în cazul producerii unor evenimente consideratecu risc major asupra securității informației;;	Corespunde

		• Soluții informatice destinate gestiunii incidentelor de securitate cibernetică - pentru preluarea automatizată adatelor aferente alertelor și e a incidentelor de securitatecibernetică.	
CF 17.06.	M	La recepționarea datelor de la soluții informatice ale AP utilizate pentru gestiunea incidentelor de securitate cibernetică SIA RSISC va crea automat evenimentele de raportare a alertelor și incidentelor de securitate cibernetică și va crea în mod automat cazurile de gestiune a incidentelor cu completarea formularelor relevante în baza datelorrecepționate.	Corespunde
CF 17.07.	M	SIA RSISC se va integra cu Google Analytics în scopul expedierii datelorstatistice privind exploatarea Interfeței Publice.	Corespunde
CF 17.08.	M	SIA RSISC se va integra cu rețele de socializare (LinkedIn, Facebook șiTwitter) în scopul publicării informației de conținut a interfeței publice SIA RSISC.	Corespunde
CF 17.09.	M	Toate evenimentele de schimb de date cu sisteme informatice externe prin intermediul procedurilor descrise de cerințele funcționale CF 17.04 - CF 17.06 vor fi jurnalizate prin intermediulmecanismului de jurnalizare intern a SIA RSISC și serviciului de platformă MLog.	Corespunde
CF 17.10.	M	Sistemul va permite importarea automatizata (prin intermediul adaptoarelor), din diferite surse de date (csv,xls,sql), prin diferite protocoale(soap,rest,syslog) cu posibilitatea ajustarii parametrilor pentru fiecare sursa de date intr-un mod dinamic si individual.	Pentru importuri (prin intermediul adaptoarelor), toate sursele de date și protocoalele de comunicare trebuie să fie definite în prealabil la etapa de dezvoltare. Configurarea se va face la etapa de implementare.
CF 17.11.	M	Sistemul va include adaptoare la cheie pentru urmatoarele surse de date (Fortinet, ShadaowServer, Barracuda Spam, si WAF, Nginx, WangGuard)	Corespunde Adaptoarele gata pentru conectarea la SIA RSISC vor fi furnizate de către solicitant.
CF 17.12.	M	Sistemul va permite importarea, periodica, din diferite surse publice, IpReputation, botnet, etc.	Corespunde Solicitantul va stabili lista surselor publice din care sunt necesare importurile.

15.18 CU18: Jurnalizez evenimente

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
CF 18.01.	M	SIA RSISC va conține mecanism de jurnalizare a tuturor evenimentelorde business aferente utilizării sale.	Corespunde
CF 18.02.	M	Administratorul de Sistem va putea configura strategiile de jurnalizareaferente evenimentelor de business produse de SIA RSISC prin intermediul cazului de utilizare CU12 și CU15 (inclusiv care evenimente vor fi jurnalizate doar prin intermediul mecanismelor interne și care suplimentar prin intermediul serviciului guvernamentalMLog).	Corespunde

CF 18.03.	M	SIA RSISC va furniza Administratorilor de Sistem mecanism de căutare,filtrare și vizualizare a detaliilor evenimentelor jurnalizate.	Corespunde
CF 18.04.	M	Vor fi jurnalizate următoarele categorii de evenimente: • autentificare utilizator; • deconectare utilizator; • adăugare/modificare/eliminare/accesare înregistrare; • evenimente de business specifice fluxurilor de lucru ale SIARSISC; • schimbul de date cu sisteme informatice externe; • generare/accesare raport; • interogări la baza de date; • alte evenimente de business specifice.	Corespunde
CF 18.05.	M	Evenimentele jurnalizate vor salva următoarele categorii de date (înfuncție de natura evenimentului jurnalizat: • identificatorul utilizatorului care a generat evenimentul; • categoria evenimentului jurnalizat; • momentul jurnalizării evenimentului; • modulul SIA RSISC care a generat evenimentul de business; • înregistrarea afectată de evenimentul de business; • acțiunea efectuată de utilizator (exemplu: detaliile modificării,datele adăugate etc.).	Corespunde
CF 18.06.	M	SIA RSISC va jurnaliza exhaustiv toate evenimentele de businessproduse.	Corespunde
CF 18.07.	M	SIA RSISC va jurnaliza în paralel evenimentele de business critice prinintermediul serviciul guvernamental de jurnalizare MLog.	Corespunde
CF 18.08.	M	SIA RSISC va furniza funcționalitate de definire a evenimentelor debusiness critice care urmează a fi jurnalizate în paralel prin intermediul serviciului de platformă MLog.	Corespunde

15.19 CU19: Expediez notificări

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
CF 19.01.	M	În funcție de utilizator (datele de configurare a profilului acestuia),funcționalitatea de notificare a utilizatorilor va aplica una din 3 strategii de notificare: • notificare prin E-mail; • notificare în Dashboard-ul utilizatorului autorizat; • ambele categorii de mai sus.	Corespunde
CF 19.02.	M	SIA RSISC va notifica utilizatorii relevanți la producerea unuieveniment de business specific activității lor.	Corespunde
CF 19.03.	M	Notificarea va conține referință de accesare a înregistrării/formularului electronic relevant evenimentului de business care a generat notificarea	Corespunde

		(valabil pentru notificările stocateîn Dashboard-ul utilizatorului).	
CF 19.04.	M	Utilizatorii autorizați (indiferent de rolurile de care dispun) vor puteasă-și configureze preferințele mijloacelor de notificare.	Corespunde
CF 19.05.	M	Toate categoriile de utilizatori autorizați vor primi notificări privindevenimentele de business aferente obligațiilor sale de serviciu (*exemplu: necesitate procesare alertă sau incident de securitate* cibernetică *raportate, necesitatea escaladării incidentului de securitate* cibernetică*, necesitate aprobare proiecte de formulare electronice, întârziere în executarea atribuțiilor de serviciu etc.*).	Corespunde
CF 19.06.	M	Administratorul de Sistem va dispune de funcționalitate de perfectareși expediere notificări utilizatorilor expliciți sau grupurilor de utilizatori.	Corespunde
CF 19.07.	M	SIA RSISC va notifica Administratorul de Sistem asupra oricăror probleme ce afectează performanța și disponibilitatea sistemuluiinformatic.	Corespunde
CF 19.08.	M	SIA RSISC va notifica utilizatorii care recepționează notificările prinmijloace externe prin intermediul serviciului guvernamental de notificare MNotify.	Corespunde

16 Cerințe nefuncționale

16.1 Cerințe generale ale sistemului informatic

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
GEN 001	M	SIA RSISC trebuie să fie dezvoltat în baza metodologiei Agile.	Furnizorul satisface cerința
GEN 002	M	Toate interfețele utilizator și conținutul bazei de date vor fi perfectate înlimba română cu utilizarea diacriticelor românești.	Corespunde
GEN 003	M	Interfața utilizator al interfeței publice a SIA RSISC și valorile metadatelortextuale (clasificatoare, nomenclatoare etc.) trebuie să fie accesibile în limbile română, engleză și rusă.	Corespunde
GEN 004	M	Datele bazei de date a SIA RSISC urmează a fi stocate în format unicode(*exemplu: utilizând UTF-8*).	Corespunde
GEN 005	M	Elementele interfeței utilizator trebuie să se conformeze la Nivel A cucerințele *Web Content Accessibility Guidelines (WCAG) 2.0.*	Soluția propusă susține dispozițiile și principiile de creare a web-contentului accesibil pentru un număr maximal de utilizatori diferiți
GEN 006	M	Interfața utilizatori pentru utilizatorii autorizați ai SIA RSISC va fi optimizată rezoluției 1360x768 cu evitarea apariției barelor de defilarepentru interfețele utilizator prezentate de soluția informatică.	Corespunde
GEN 007	M	SIA RSISC va furniza interfață publică adaptabilă (va livra interfațăresponsivă) în funcție de dispozitivul utilizat de acesta (*notebook,netbook, calculator desktop, smartphone, tabletă etc.*)	Corespunde
GEN 008	M	Interfața Publică va genera paginile de conținut ținând cont de cele mai bune practici de optimizare SEO.	Corespunde Se va realiza o optimizare internă și externă

GEN 009	M	Procedurile de căutare a datelor vor fi implementate prin intermediul unor căutări simple (specificarea unor șiruri de căutare) sau a unor căutări de complexitate mai ridicată, prin intermediul cărora se poate realiza o filtrare mai exact a informației (formulare QBE). Indiferent denatura informației căutate utilizatorul va utiliza aceeași metodă de interogare și regăsire a datelor pentru orișicare compartiment al interfeței utilizator a produsului informatic.	În calitate de limbaj de interogare pentru Elastic Search se va folosi limbajul ESQL.
GEN 010	M	Interfața utilizator a sistemului informatic trebuie să asigure căutarea, filtrarea și vizualizarea înregistrărilor ce corespund criteriului de căutareprezentate utilizatorilor în funcție de drepturile lor de acces.	Corespunde
GEN 011	M	Conținutul oricărui tabel cu rezultate ale căutării trebuie să poată fiexportat fie în format XLS, CSV și PDF.	Soluția propusă va exporta datele din tabelul cu rezultatele căutării în format XLS și PDF.
GEN 012	M	Arhitectura SIA RSISC va fi concepută integrat, dezvoltată cu aplicareacelor mai bune practici în domeniu (exemplu: principii de arhitectură și arhitecturi de referință aliniate TOGAF 9.1).	Soluția propusă va utiliza un framework universal în domeniul proiectării arhitecturii IT, care oferă îndrumări metodice privind stabilirea și utilizarea practicilor de proiectare a arhitecturii.
GEN 013	M	Arhitectura completă SIA RSISC va fi coordonată în prealabil cu STISC.	Corespunde
GEN 014	M	Arhitectura SIA RSISC trebuie să asigure utilizarea rațională și balansată aresurselor de procesare.	Corespunde
GEN 015	M	SIA RSISC va fi dezvoltat în baza unei arhitecturi SOA multi-nivel (cel puțin 3 nivele arhitecturale (*exemplu: nivelul de prezentare, nivelul logiciide business și nivelul de date*).	Corespunde
GEN 016	M	SIA RSISC trebuie să ofere interfețe web de interacțiune cu sisteme informatice ale STISC și ale altor autorități publice ale Republicii Moldovaprin intermediul microserviciilor și MCloud.	Corespunde
GEN 017	M	SIA RSISC va fi optimizat în transferul minim de date între calculatorul client și server, punându-se accent pe evitarea la maximum a cererilor inutile, implementarea AJAX cu JSON, solicitării la minim a resurselor server necesare procedurilor de autentificare, autorizare și jurnalizare.	Corespunde
GEN 018	M	Informația potențial variabilă (*exemplu: diferiți parametri, căi de stocarea datelor, cai de conexiune cu servicii externe, clasificatoare etc.*) va fi configurabilă și NU va necesita recompilarea soluției sau intervenții directe în baza de date.	Corespunde

16.2 Cerințele de performanță a sistemului informatics

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
PER 001	M	Timpul mediu de răspuns al serverului nu va depăși 3 secunde laîncărcătura nominală a sistemului.	Corespunde
PER 002	M	SIA RSISC trebuie sa fie capabil să permită activitatea a cel puțin 200 utilizatori autorizați.	Corespunde

PER 003	M	SIA RSISC va permite activitatea concurentă a cel puțin 150 utilizatoriautorizați și deservirea concomitentă a cel puțin 100 interogări fără aafecta performanța de funcționare.	Corespunde
PER 004	M	Interfața publică a SIA RSISC trebuie sa fie capabilă sa deserveascăaccesul anual a peste 500000 utilizatori anonimi.	Corespunde
PER 005	M	Interfața publică a SIA RSISC trebuie să fie capabilă să deservească celpuțin 500 utilizatori anonimi concurenți și 300 interogări paralele.	Corespunde
PER 006	M	SIA RSISC trebuie să fie capabil să recepționeze, proceseze și stochezeanual datele a peste 100 000 000 alerte și peste și peste 10 000 incidente de securitate.	Corespunde
PER 007	M	Anterior livrării SIA RSISC vor fi efectuate totalitatea testelor deperformanță și securitate.	Corespunde
PER 008	M	Testarea performanței va include minim doua componente: testareaîncărcăturii sistemului (*load testing*) și testarea comportamentului sistemului la solicitări mari (*stress testing*).	Corespunde

16.3 Cerințele de scalabilitate a sistemului informatics

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
SR 001	M	SIA RSISC va permite creșterea capacității de procesare fără a întrerupe funcționarea sa. În acest scop, sistemul va suporta extinderea pe orizontală a capacității de procesare (exemplu: adăugarea de noi noduriserver și efectuare balansare a încărcării).	Corespunde
SR 002	D	SIA RSISC va putea fi configurat pentru scalare automată la nivelul componentelor cheie (lag sensitive). Scalarea sistemului se va face atâtîn sus, cât și în jos.	Corespunde Va fi realizat în cazul, dacă acceptarea SIA RSISC va fi efectuată înainte de termenul stabilit
SR 003	M	SIA RSISC trebuie să dețină posibilitatea de a deservi un număr nelimitatde tranzacții, cu condiția alocării corespunzătoare a resurselor de procesare și stocare date. Resursele vor fi alocate pe orizontală (alocarenoi servere, fără creșterea performanței pe serverele existente).	Corespunde

16.4 Cerințe software, hardware și canale de comunicație

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
SHC 001	M	SIA RSISC trebuie să poată fi instalat atât pe servere dedicate, cât și pesoluții de virtualizare (SIA RSISC trebuie să fie conform cerințelor de desfășurare a sistemelor informatice pe platforma guvernamentală tehnologică comună MCloud).	Corespunde
SHC 002	M	Este necesară demonstrarea capacității de virtualizare prin livrarea cătreSTISC a unei imagini a sistemului ce poate fi încărcată și devine funcțională cu configurări minime pe una din soluțiile de virtualizare existente pe piață.	Corespunde
SHC 003	M	Furnizorul va demonstra posibilitatea instalării și operării SIA RSISC îninfrastructura MCloud.	Corespunde
SHC 004	M	SIA RSISC trebuie să poată fi accesat pe canale de comunicații de celpuțin 512Kbps.	Corespunde

SHC 005	M	SIA RSISC trebuie să fie dezvoltat în baza următoarelor tehnologii: • Microsoft Windows Server 2019 (în calitate de sistem deoperare); • IIS 10 (în calitate de server WEB); • Microsoft SQL Server 2019 Standard Edition (în calitate deSGBD); • Elastic Search (în calitate de motor de căutare indexată a datelorși soluție de stocare/gestiune a alertelor); • ASP.NET Core (în calitate de framework de dezvoltare); • Entity Framework (în calitate de soluție ORM); • Microsoft SQL Server Report Services (în calitate de generator derapoarte); • Angular JS, React JS sau Knockout JS (în calitate de frameworkdestinat implementării interfeței utilizator); • Nginx (în calitate de soluție pentru balansor)	Corespunde
SHC 006	M	Furnizorul va indica explicit în ofertă platforma software în baza căreiaurmează a fi dezvoltat SIA RSISC și platforma software necesară exploatării acestuia.	Pentru sugestii privind platforma tehnologică, a se vedea secțiunea 7.
SHC 007	M	Tehnologiile propuse de Furnizor trebuie să fie accesibile pentru celpuțin 3 companii specializate în dezvoltarea soluțiilor software careactivează pe piața locală a Republicii Moldova	Tehnologiile furnizate de furnizor vor fi general acceptate în practica internațională de dezvoltare a sistemelor informatice.
SHC 008	M	SIA RSISC va utiliza standarde deschise pentru formate și protocoale decomunicare.	Corespunde
SHC 009	M	Serviciile expuse către public de SIA RSISC vor fi tehnologic neutre(Sistem de Operare, explorator Internet etc.).	Corespunde
SHC 010	M	Produsul program generic recomandat pentru operarea și interacțiuneacu SIA RSISC reprezintă exploratorul WEB.	Corespunde
SHC 011	M	Sistemul va fi compatibil cu cel puțin 2 cele mai recente versiuni ale următoarelor exploratoare Web: *MS Internet Explorer/MS Edge, MozillaFirefox, Google Chrome*, *Safari* și *Opera*.	Corespunde
SHC 012	M	Compatibilitatea cu exploratorul WEB *MS Internet Explorer/MS Edge* este obligatorie.	Corespunde
SHC 013	D	SIA RSISC va încorpora un serviciu Heart-beat care va comunica periodicstarea normală de lucru a sistemului.	Corespunde Pentru o propunere privind utilizarea tehnologiei Heartbeat, a se vedea secțiunea 7.
SHC 014	M	Sistemul va include mijloace configurabile de jurnalizare tehnică(logging).	Corespunde
SHC 015	M	Sistemul trebuie să fie capabil să producă cel puțin următoarele nivelede jurnalizare tehnică: *info*; *warning*; *critic*; *error*.	Corespunde
SHC 016	M	Dezvoltatorul va enumera mijloacele ce vor fi utilizate la depanareatehnică a sistemului.	Instrumente pentru depanarea tehnică: • Microsoft Visual Studio Community 2022 - pentru remedierea erorilor din

			codul sursă al aplicației SIA RSISC • SQL Server Management Studio - pentru restaurarea bazei de date din backup, gestionarea sql job • IIS - pentru a reporni aplicația web și serviciile SIA RSISC. • Docker - pentru a actualiza aplicația SIA RSISC
SHC 017	M	Furnizorul va pregăti mijloace ce facilitează funcțiile de administrare asistemului: • startarea componentelor sistemului; • stoparea componentelor sistemului; • restartarea componentelor sistemului, • crearea copiei de rezervă a bazei de date, • restaurarea datelor de pe copia de rezervă indicată, • împrospătarea memoriei operaționale a sistemului.	Furnizorul satisface cerința
SHC 018	M	SIA RSISC va opera în rețele TCP/IP și în special HTTPS.	Corespunde
SHC 019	M	SIA RSISC va utiliza XML în calitate de mijloc principal pentru integrareadatelor.	Corespunde
SHC 020	M	Furnizorul va sugera alte servicii de rețea și utilitare necesare pentruoperarea sistemului.	Furnizorul satisface cerința

16.5 Cerințe de licențiere și proprietate intelectuală

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
LIC 001	I	STISC va asigură următoarele medii de operare pentru SIA RSISC: • Mediul de producție; • Mediul de testare/instruire; • Mediul de dezvoltare.	Furnizorul satisface cerința
LIC 002	M	Furnizorul va include în oferta sa financiară licențele pentru toate produsele soft de tip COTS (diferite de cele menționate în SHC 005), necesare implementării și exploatării SIA RSISC în cele trei medii puse ladispoziție de STISC. Aici sunt incluse următoarele: sisteme de operare, sisteme de gestiunebaze de date, biblioteci software, utilitare și alt soft de sistem.	Pentru implementarea și expluatarea SIA RSISC, trebuie instalat software-ul descris în secțiunea 7. De asemenea, se descrie și modul de acordare a licenței pentru acesta.
LIC 003	M	Cantitatea licențelor oferite trebuie să permită accesarea și utilizarea SIA RSISC (în orice mediu în care funcționează) de cel puțin 200 de utilizatori autorizați nominali, precum și nelimitat de utilizatori anonimi și sisteme externe. Nu vor exista restricții cu privire la numărul de documente, tranzacții sau mod de accesare a SIA RSISC (exemplu: limitări la accesare concurentă).	Furnizorul satisface cerința Numărul de utilizatori care se conectează la SIA RSISC (în fiecare mediu) este limitat de numărul de licențe software furnizate de solicitant.
LIC 004	M	Cantitatea licențelor oferite trebuie să permită accesarea API-urilor expuse de SIA RSISC de orice	Numărul de sisteme externe conectate la SIA RSISC (în

		aplicație și sistem extern.	fiecare mediu) este limitat de numărul de licențe software furnizate de solicitant.
LIC 005	M	Furnizorul va transmite către STISC toate drepturile asupra dezvoltărilor, ajustărilor, configurărilor și personalizărilor efectuate pentru implementarea SIA RSISC conform cerințelor. Acestea pot fi aferente produselor soft terțe licențiate sau pot fi componente elaborate în cadrul proiectului.	Furnizorul satisface cerința
LIC 006	M	Orice date stocate în cadrul bazelor de date aferente SIA RSISC sunt proprietatea STISC. Accesul la aceste date pe întreaga perioada de contractare a furnizorului, cât și după, este subiect al cerințelor și clauzelor de confidențialitate a informației.	Furnizorul satisface cerința
LIC 007	M	Furnizorul va prezenta modelul său de licențiere propus pentru SIA RSISC care trebuie să corespundă cerințelor LIPR 001 – LIPR 006. Furnizorul va descrie modelul de licențiere propus, argumentând de ce acesta este cel optim pentru STISC. Va prezenta o analiză comparativă cu alte modele de licențiere oferite de obicei pentru soluția ofertată.	Informații privind acordarea licențelor sunt furnizate în secțiunea 7

16.6 Cerințe de interoperabilitate

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
INT 001	I	Toate interfețele expuse de SIA RSISC trebuie să fie bazate pe standardedeschise. Toate fluxurile de mesaje între SIA RSISC și entități externe se vor realiza cu utilizarea standardelor deschise.	Corespunde
INT 002	M	SIA RSISC va deține capabilități de implementare a interfețelor prinintermediul MConnect.	Corespunde
INT 003	M	SIA RSISC va deține capabilități de integrare cu sistemele informatice aleAP din Republica Moldova în vederea recepționării automate a datelor referitoare la alertele înregistrate pe parcursul exploatării lor.	Corespunde
INT 004	M	SIA RSISC va deține capabilități de integrare cu sistemele informatice aleAP din Republica Moldova destinate gestiunii incidentelor de securitate în vederea recepționării datelor referitoare la incidentele de securitategestionate în cadrul AP.	Corespunde
INT 005	M	SIA RSISC se va integra cu platforma de interoperabilitate MConnectpentru a consuma date din sisteme informatice externe (exemplu: extragerea datelor din registre de stat).	Corespunde
INT 006	M	SIA RSISC se va integra cu serviciul guvernamental MPass pentruimplementarea mecanismului de autentificare a utilizatorilor prinintermediul semnăturii electronice sau mobile.	Corespunde
INT 007	M	SIA RSISC se va integra cu serviciul guvernamental MSign pentru implementarea infrastructurii de utilizare a semnăturii electronice.	Corespunde

INT 008	M	SIA RSISC se va integra cu serviciul guvernamental MLog pentrujurnalizarea evenimentelor de business critice.	Corespunde
INT 009	M	SIA RSISC se va integra cu serviciul guvernamental MNotify pentruimplementarea mecanismului de notificare a utilizatorilor.	Corespunde
INT 010	M	SIA RSISC se va integra cu serviciul guvernamental MPower pentru verificarea împuternicirilor utilizatorilor autoriza de a efectua acțiunispecifice în cadrul interfeței utilizator.	Corespunde
INT 011	M	SIA RSISC se va integra cu serviciul guvernamental Portalul DatelorDeschise (https://date.gov.md) pentru publicarea datelor deschiseproduse în cadrul fluxurilor de lucru implementate.	Corespunde
INT 012	M	Toate interfețele furnizate de SIA RSISC vor interacționa cu aplicațiileexterne instantaneu sau programat prin intermediul unor job-uri specializate.	Corespunde
INT 013	M	Interfața publică a SIA RSISC se va integra cu Google Analytics și cele maiimportante rețele de socializare (LinkedIn, Facebook și Twitter) în vederea expedierii statisticilor de vizitare a conținutului public și publicării conținutului public pe rețelele de socializare.	Corespunde
INT 014	D	SIA RSISC va deține capabilități de definire a noilor interfețe standard pentru accesarea tuturor funcțiilor de business cheie ale sistemului (*exemplu: generare documente, generare tranzacții, accesare informații despre entitățile de business stocate în cadrul SIA RSISC*).	Corespunde Va fi realizat în cazul, dacă acceptarea SIA RSISC va fi efectuată înainte de termenul stabilit
INT 015	D	Interfețele respective trebuie să permită gestiunea entităților debusiness cu aplicarea tuturor regulilor de business relevante și cuutilizarea tuturor proprietăților aferente entităților de business.	Corespunde Va fi realizat în cazul, dacă acceptarea SIA RSISC va fi efectuată înainte de termenul stabilit
INT 016	D	SIA RSISC va deține capabilități de definire a noilor interfețe pentru accesarea sistemelor externe cu utilizarea standardelor deschise. Aceste interfețe vor fi accesibile pentru apelare în cadrul funcțiilor sistemului, laimplementarea funcționalităților SIA RSISC.	După realizarea și punerea în exploatare a SIA RSISC, interfețele noi pentru interconectarea cu sistemele externe vor fi dezvoltate în cadrul lucrărilor de finalizare a sistemului.
INT 017	M	SIA RSISC va deține interfețe standard pentru exportul datelor în cadrulinstrumentelor de tipul Data Warehouse.	Corespunde

16.7 Cerințe de migrare și populare a datelor

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
MIG 001.	M	STISC va pregăti și livra seturile de date și metadate necesare populăriicu date primare a SIA RSISC. Formatul datelor migrate va fi convenit decomun acord cu Dezvoltatorul.	Corespunde
MIG 002.	M	Dezvoltatorul va trebuie să convertească valori specifice ale metadateloraferente seturilor de date	Dezvoltatorul satisface cerința

		externe conform sistemului de metadate statistice al STISC.	
MIG 003.	M	Dezvoltatorul va include în oferta tehnică abordarea sa privind procedura de implementare a procedurii de migrare și populare inițială abazei de date.	Dezvoltatorul satisface cerința
MIG 004.	M	Dezvoltatorul trebuie să furnizeze mecanism care va asigura populareaautomatizată a bazei de date a SIA RSISC cu metadatele relevante (nomenclatoare, clasificatoare, variabile de diferită natură etc.) și seturile de date primare furnizate de STISC în vederea consolidării stocului de date inițial al SIA RSISC.	Dezvoltatorul satisface cerința
MIG 005.	M	Pe parcursul implementării procedurii de migrare și populare a datelorFurnizorul este responsabil pentru: • definirea metodologiei utilizate în procesul de migrare șipopulare a datelor; • elaborarea planurilor detaliate de migrare și populare a datelor; • furnizarea mecanismelor software destinate migrării și populăriidatelor; • definirea cerințelor de calitate către seturile de date destinate migrării/populării și procesarea lor prin intermediul mecanismelor de migrare și populare elaborate; • maparea valorii metadatelor recepționate din surse externe (încazul divergențelor); • definirea criteriilor de reconciliere a datelor migrate și populate; • participarea în procesul de curățare și îmbogățire a datelor; • verificarea și validarea calității seturilor de date ce urmează a fimigrate și populare; • popularea bazei de date a SIA RSISC în baza seturilor de datefurnizate de STISC; • identificarea și soluționarea excepțiilor/erorilor pe parcursulprocesului de migrare și populare a datelor.	Dezvoltatorul satisface cerința
MIG 006.	M	Furnizorul trebuie să propună către STISC metodologia de migrare și populare a datelor. Metodologia de migrare și populare a datelor trebuie să conțină următoarele elemente: • metodologia de pregătire a datelor ce urmează a fi migrate șipopulate; • metodologia de mapare a datelor migrate și populate; • metodologie de curățare și îmbogățire a datelor migrate/populate și asigurare a calității lor; • metodologia completării valorii datelor solicitate obligatoriu deSIA RSISC dar care	Dezvoltatorul satisface cerința

		lipsesc în seturile de date furnizate; • procedura automatizată de migrare și populare a datelor; • principiile de reconciliere a datelor migrate și populate; • planul de recuperare în caz de eșec (pentru fiecare etapă aprocesului de migrare și populare a datelor); • planul de livrare a mecanismului de migrare și populare adatelor.	
MIG 007.	M	Furnizorul trebuie să pregătească și livreze planul detailat al migrării șipopulării inițiale cu date a SIA RSISC (strategia de migrare și conversie a datelor). Acest plan trebuie să fie aliniat planului de implementare a SIARSISC.	Dezvoltatorul satisface cerința
MIG 008.	M	Furnizorul trebuie să livreze către STISC soluție software destinată automatizării proceselor de migrare și populare inițială cu date a SIARSISC.	Dezvoltatorul satisface cerința
MIG 009.	M	Toate activitățile de migrare și populare inițială a SIA RSISC cu date trebuie să fie efectuate în mediul de operare controlat de STISC. Datelenu vor părăsi niciodată infrastructura TIC a STISC.	Corespunde
MIG 010.	M	În procesul migrării Furnizorul se va confirma politicii de securitate aSTISC.	Corespunde
MIG 011.	M	Furnizorul va demonstra corectitudinea instrumentarului de migrare și populare inițială cu date a SIA RSISC specialiștilor STISC (un act de acceptanță a migrării și populării inițiale cu date a SIA RSISC urmează a fisemnat între Furnizor și STISC).	Dezvoltatorul satisface cerința

16.8 Cerințe de asigurare a securității informaționale

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
SEC 001	M	Arhitectura SIA RSISC trebuie să fie concepută prin aplicarea uneiabordări de tipul *„Security by design”* (securitate prin design).	Corespunde
SEC 002	M	Arhitectura de securitate a SIA RSISC trebuie să fie documentată la niveltehnic. Documentația va conține: • descrierea modelului de securitate implementat; • componentele prezente; • rolul fiecărei componente din punct de vedere al securității	Corespunde
SEC 003	M	Documentația va conține, de asemenea, specificațiile privind plasarea lanivel de rețea a componentelor SIA RSISC și recomandările Furnizorului privind regulile de acces la nivel de rețea necesar a fi setate de STISC în vederea accesului securizat la toate componentele sistemului (*exemplu:matrice de comunicare între servicii*).	Furnizorul satisface cerința
SEC 004	M	Toate procesele de sistem aferente componentelor SIA RSISC vor rula cuprivilegii minime necesare executării sarcinilor atribuite.	Corespunde

SEC 005	M	Toate credențialele de acces utilizate de SIA RSISC trebuie să fie configurabile în interfețele administrative. SIA RSISC nu va conținecredențiale de acces hard-coded.	Toate datele de evidență pentru accesul la SIA RSISC trebuie să fie definite în etapa de elaborare a SIA RSISC.
SEC 006	M	SIA RSISC nu va conține credențiale de acces stocate la nivelul componentelor sale (în baza de date, fișiere de configurație) în formădeschisă.	Corespunde
SEC 007	M	Toate interfețele expuse ale SIA RSISC vor fi accesate cu aplicareametodelor sigure de autentificare (*exemplu: certificate X.509*).	Corespunde Atunci când se utilizează serviciul MPass, acesta va prelua aceste funcții
SEC 008	M	Accesul la funcțiile oferite utilizatorilor neautentificați (interfața publicăfurnizată de SIA RSISC) trebuie să fie controlat cu mijloace de protecție contra suprasolicitării (*exemplu: CAPTCHA, RECAPTCA etc.)*.	Corespunde
SEC 009	M	Conținutul câmpurilor din formularele completate de către utilizatori trebuie să fie validat în mod obligatoriu atât pe calculatorul client cât șipe server până la stocarea în baza de date.	Corespunde
SEC 010	M	SIA RSISC va fi securizat pentru OWASP Top 10 vulnerabilities (2017).	Soluția propusă va fi protejată împotriva a 10 probleme de bază, legate de securitatea aplicațiilor web
SEC 011	M	SIA RSISC va asigura confidențialitatea datelor transmise-recepționate pecanalele de comunicație.	Corespunde
SEC 012	M	Acțiunile utilizatorilor trebuie să fie înregistrate în jurnale electronice.	Corespunde
SEC 013	D	SIA RSISC va emite un semnal periodic care indică starea sa funcțională.	Corespunde
SEC 014	M	SIA RSISC va permite accesarea funcțiilor sale doar după autentificarea cusucces a utilizatorului, oferind suport pentru cel puțin următoarele metode de autentificare: • în bază de login și parolă; • în bază de soluție LDAP; • autentificarea prin intermediul semnăturii electronice sau mobile(MPass).	Corespunde
SEC 015	M	SIA RSISC va permite utilizatorilor mecanism de schimbare și restabilire aparolelor individuale.	Corespunde
SEC 016	M	SIA RSISC va permite înregistrarea utilizatorilor și a informației de profilaferentă acestora (*exemplu: login, parolă, nume, prenume, IDNP, Emailetc.*).	Corespunde
SEC 017	M	Parolele utilizatorilor trebuie să fie protejate. Metoda de protejare a parolelor trebuie să asigure imposibilitatea interceptării, deducerii saurecuperării acestora (algoritm de criptare unidirecțională).	Corespunde
SEC 018	D	SIA RSISC va permite aplicarea diferențiată a politicilor de utilizare aparolelor pentru diferite grupuri de utilizatori.	Politica privind parolele va fi uniformă pentru toate rolurile din SIA RSISC.
SEC 019	M	SIA RSISC va permite blocarea, dezactivarea sau suspendarea conturilorutilizatorilor la nivel de aplicație.	Corespunde
SEC 020	D	SIA RSISC va permite aplicarea diferențiată a metodelor de autentificare,în funcție de rolurile deținute de utilizatori și componentele funcționale accesate	Corespunde

SEC 021	M	SIA RSISC va permite setarea numărului de conexiuni simultane ce pot fiinițiate de un utilizator.	Corespunde
SEC 022	M	SIA RSISC va permite setarea timpului de expirare a sesiunilor utilizatorilor autorizați în caz de inactivitate (valoarea implicită este de 15minute).	Corespunde
SEC 023	M	SIA RSISC va deține mecanisme eficiente de prevenire a preluăriineautorizate a sesiunilor active inițiate de utilizatorii autorizați.	Corespunde
SEC 024	M	Sesiunea de lucru în SIA RSISC va fi blocată la solicitarea utilizatorului sauautomat, la expirarea timpului rezervat sesiunii.	Corespunde
SEC 025	M	SIA RSISC va permite gestiunea granulară a drepturilor de acces la toateobiectele sale și acțiunile posibile asupra acestora (*exemplu: formulare electronice, meniuri, rapoarte, acțiuni de creare/vizualizare/actualizare/eliminare etc.*).	Corespunde Setările se vor face la nivelul drepturilor de rol. Fiecare rol va avea propriul set de drepturi. Rolurile vor fi atribuite utilizatorilor specifici. Drepturile rolurilor vor fi configurabile (acces la date: vizualizare, ștergere, editare, acces la forme și vizualizarea elementelor formei etc.).
SEC 026	M	Metoda de autorizare în cadrul sistemului se va baza pe principiul „*esteinterzis tot ce nu este explicit permis*”.	Corespunde
SEC 027	M	SIA RSISC va permite definirea de grupuri de utilizatori și roluri șiasocierea utilizatorilor la aceste grupe și roluri.	SIA RSISC va permite definirea rolurilor în SIA RSISC și atribuirea acestor roluri unor utilizatori specifici.
SEC 028	M	SIA RSISC va permite acordarea drepturilor de acces la nivel de utilizatorexplicit, grup și rol. Un grup de utilizatori va putea conține mai multe subgrupuri/roluri. Un utilizator poate fi asociat unuia sau mai multor grupuri și roluri, drepturile sale de acces fiind determinate cumulativ.	SIA RSISC va permite atribuirea de roluri utilizatorilor. Rolurile definesc drepturile de acces la datele și funcțiile SIA RSISC. Unui utilizator i se pot atribui mai multe roluri, în acest caz acesta va avea suma drepturilor fiecărui rol.
SEC 029	M	SIA RSISC va permite acordarea drepturilor de acces bazate pe reguli debusiness (exemplu: modificarea înregistrării doar dacă utilizatorul este autor sau dacă operațiunea se face într-un anumit interval de timp, staresau context).	Corespunde
SEC 030	M	SIA RSISC va permite atribuirea temporară a drepturilor deținute de unutilizator către un alt utilizator. Atribuirea va putea fi efectuată cu păstrarea sau suspendarea drepturilor deținute de utilizatorul către carese deleagă drepturile.	Corespunde
SEC 031	D	SIA RSISC va permite segregarea activităților administrative (exemplu:Administratorul 1 modifică, Administratorul 2 confirmă).	Corespunde
SEC 032	M	SIA RSISC va furniza vizualizări și rapoarte privind drepturile de acces configurate. Acestea vor putea fi parametrizate în funcție de cel puținurmătoarele criterii: grup de utilizatori/roluri, login utilizator, acțiuni admise etc.	Corespunde

SEC 033	M	SIA RSISC va deține capabilități de autentificare și autorizare a utilizatorilor prin intermediul atât a mecanismelor interne, cât și prinintermediul serviciului de platformă MPass.	Corespunde
SEC 034	M	SIA RSISC va autoriza accesul utilizatorilor la compartimentele interfețeiutilizator și date după verificarea împuternicirilor acestora prin intermediul MPower.	Corespunde
SEC 035	M	SIA RSISC va deține mecanisme adecvate pentru a preveni manipulareadatelor de intrare (date de intrare parvenite de la utilizatorii autorizați,date de intrare parvenite de la aplicații externe).	Corespunde
SEC 036	M	Toate acțiunile de modificare date critice și sensibile în cadrul SIA RSISC vor fi efectuate prin intermediul formularelor și documentelor specializate, conform fluxului de lucru stabilit pentru aceste categorii de documente (*exemplu: corectarea datelor incidentelor documentate*).	Corespunde
SEC 037	M	SIA RSISC va efectua validarea completă și independentă a datelor pepartea de nivelul de prezentare, nivelul logicii de business, nivelul dedate, în scopul asigurării integrității, completitudinii și corectitudinii datelor.	Corespunde
SEC 038	M	Toate afișările de date în cadrul SIA RSISC trebuie să fie însoțite de unmarcaj de securitate, conform unui clasificator stabilit în acest sens încadrul SIA RSISC.	Corespunde Solicitantul trebuie să furnizeze forma marcajului de securitate și să descrie metodele de aplicare înainte de etapa de elaborare.
SEC 039	M	Datele confidențiale nu vor fi stocate și accesate nesecurizat în cadrul SIARSISC (*exemplu: fișiere log, caching etc.*).	Corespunde
SEC 040	M	SIA RSISC va deține mecanisme de protejare adițională a datelor deosebitde confidențiale (exemplu: afișarea mascată a datelor, stocarea datelor în formă criptată, autentificarea repetată sau utilizând mijloace suplimentare a utilizatorului etc.).	Corespunde
SEC 041	M	SIA RSISC va deține proceduri de rutină pentru verificarea și detectareaposibilelor coruperi a relațiilor de integritate a datelor.	Corespunde
SEC 042	M	SIA RSISC va deține mecanisme adecvate pentru a preveni manipulareadatelor stocate în cadrul aplicației.	Corespunde
SEC 043	M	SIA RSISC va deține componente de audit ce vor colecta și gestiona centralizat înregistrările de audit la nivelul fiecărui modul al sistemuluiinformatic.	Corespunde
SEC 044	M	Componenta de audit va permite configurarea granulară a politicilor deaudit.	Corespunde
SEC 045	M	SIA RSISC va permite stabilirea politicilor de audit la nivel de componentăfuncțională/compartiment al interfeței utilizator, categorii de date și la nivel de eveniment jurnalizat.	Corespunde
SEC 046	M	SIA RSISC va permite stabilirea caracteristicilor specifice evenimentelor ce trebuie să fie jurnalizate (exemplu: produse într-un anumit interval detimp, aflate într-un anumit statut sau care tranzitează un anumit statut etc.).	Corespunde

SEC 047	M	SIA RSISC va permite auditarea oricărui eveniment, la nivelul oricăruiobiect sau entitate de business din cadrul sistemului informatic.	Corespunde
SEC 048	M	Fiecare înregistrare de audit va conține cel puțin: • momentul în timp al producerii evenimentului; • subiectul evenimentului (identificatorul utilizatorului); • obiectul sau entitatea afectată; • evenimentul produs; • adresa IP de unde s-a inițiat evenimentul.	Corespunde
SEC 049	M	Înregistrările de audit nu vor conține date confidențiale (exemplu: paroleintroduse la încercările eșuate de autentificare).	Corespunde
SEC 050	M	Erorile ce pot apărea la jurnalizarea înregistrărilor de audit nu trebuie săafecteze funcționarea normală a sistemului informatic.	Corespunde
SEC 051	M	Componenta de audit va utiliza ceasul de sistem setat la nivelulsistemului de operare al serverului aplicație în care rulează funcționalitatea de jurnalizare a evenimentelor.	Corespunde
SEC 052	M	Componenta de audit va deține un mecanism de arhivare a înregistrărilorde audit istorice. Procesul de arhivare va putea fi parametrizat (frecvența, vechime date, format arhivare, destinație etc.).	Corespunde
SEC 053	M	SIA RSISC va putea genera automat notificări către persoanele responsabile la producerea anumitor evenimente de securitate, conformconfigurațiilor setate.	Corespunde
SEC 054	M	SIA RSISC va permite fixarea versiunilor istorice ale datelor, ce vor ficonsiderate deosebit de senzitive.	Corespunde
SEC 055	M	Activitățile de schimbare stări și responsabili înregistrări vor fi jurnalizate.	Corespunde
SEC 056	M	SIA RSISC va deține instrumente comode pentru accesarea și procesareaevenimentelor jurnalizate, inclusiv filtrarea înregistrărilor de audit după orice câmp deținut și exportul acestora în format uzual. Instrumentele deaudit ale sistemului informatic vor putea fi utilizate și în scopul importului arhivelor cu fișiere de audit pentru activități de analiză ocazionale.	Corespunde
SEC 057	M	SIA RSISC va deține mecanisme sigure de protejare a integrității datelorde audit înregistrate.	Corespunde
SEC 058	M	Evenimentele de business critice trebuie jurnalizate în paralel prinintermediul serviciului guvernamental de jurnalizare MLog.	Corespunde
SEC 059	M	SIA RSISC va furniza mecanism de configurare a evenimentelor de business care vor fi jurnalizate în paralel prin intermediul serviciului MLog	Corespunde
SEC 060	M	SIA RSISC va înregistra centralizat toate excepțiile și erorile generate decomponentele sale funcționale.	Corespunde
SEC 061	M	La producerea unei erori, SIA RSISC va afișa utilizatorului un mesaj de eroare generic. Acesta poate conține un cod de eroare și un identificatorunic al erorii, pentru a facilita implicarea serviciilor de suport.	Corespunde

SEC 062	M	SIA RSISC va deține instrumentele necesare pentru analiza și procesareaînregistrărilor aferente excepțiilor și erorilor.	Corespunde
SEC 063	M	SIA RSISC va putea genera automat notificări către persoaneleresponsabile la producerea anumitor erori în funcționarea componentelor sale funcționale.	Corespunde
SEC 064	M	SIA RSISC va avea implementate instrumente pentru executarea procedurilor de generare automată a copiilor de rezervă și gestiune acopiilor de rezervă istorice.	Corespunde
SEC 065	M	SIA RSISC trebuie să dețină mecanisme de asigurare a integrității datelorîn cazul căderilor la nivelul oricăror componente.	Corespunde
SEC 066	M	SIA RSISC trebuie să dețină mecanisme de restabilire operativă a disponibilității și accesibilității în cazul unor incidente de continuitate.	Corespunde
SEC 067	M	Arhitectura SIA RSISC trebuie să fie rezistentă la căderi de componente și să nu dețină puncte singulare de cădere (SPOF).	Soluția propusă va fi protejată de SPOF. Se va utiliza atât echipament de exces (servere), cât și copierea datelor și monitorizarea sistemelor separate.
SEC 068	M	SIA RSISC trebuie să dețină mecanisme de asigurare a integrității datelorîn cazul unor căderi accidentale la nivelul oricăror componente ale sale.	Corespunde
SEC 069	M	SIA RSISC trebuie să dețină mecanisme de restabilire operativă a disponibilității și accesibilității în cazul unor incidente de continuitate.	Corespunde

16.9 Cerințele de desfășurare a sistemului informatics

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
DEP 001	M	SIA RSISC trebuie să capabil a fi instalat pe servere dedicate și în medii virtualizate.	Corespunde
DEP 002	M	SIA RSISC trebuie să capabil să fie desfășurat și să funcționeze pe o infrastructură containerizată (exemplu: Docker Engine, Kubernetes).	Corespunde, Clientul trebuie să furnizeze infrastructura containerizată instalată și configurată, precum și să asigure administrarea acestei infrastructuri
DEP 003	M	SIA RSISC trebuie să capabilă să inițieze desfășurarea pe mai multe medii simultan (exemplu: de dezvoltare, de testare, de producție) inițiate de la zero.	Corespunde
DEP 004	M	Desfășurarea SIA RSISC trebuie să fie efectuată prin intermediul unor instrumentare specializate ce asigură automatizarea procesului de creare a imaginilor docker, actualizarea acestora,versionarea, desfășurarea.	Corespunde
DEP 005	M	Mecanismul de desfășurare a SIA RSISC trebuie să fie capabil să definească componenta containerului ce urmează a fi actualizată (*exemplu: versiune nouă a softului de platformă, modul funcțional actualizat, etc*.).	Corespunde
DEP 006	M	Mecanismul de desfășurare a SIA RSISC trebuie să fie capabil să gestioneze conținutul containerului.	Corespunde

DEP 007	M	Mecanismul de desfășurare a SIA RSISC trebuie să fie capabil să adauge noi componente în conținutul containerului.	Corespunde
DEP 008	M	Pentru desfășurarea SIA RSISC este necesar ca mecanismul de desfășurare să poată specifica în ce cluster (server dedicat sau cloud) trebuie să fie efectuată desfășurarea.	Corespunde
DEP 009	M	Pentru desfășurarea SIA RSISC este necesar ca mecanismul de desfășurare să furnizeze flux de lucru pentru compilarea codului sau registrelor.	Corespunde
DEP 010	M	Mecanismul de desfășurare a SIA RSISC trebuie să furnizeze funcționalități de livrare a soluției informatice și efectuare de acțiuni terțe (exemplu: instalarea pachetelor adiționale, configurare notificări etc.) utilizând instrumentare existente.	Corespunde
DEP 011	M	Mediul de producție al SIA RSISC trebuie să poată fi actualizat automat cu posibilități de intervenție manuală (*exemplu: aprobarebuild manual*).	Corespunde
DEP 012	M	Dezvoltatorul va livra către STISC toate instrumentarele șiscripturile necesare desfășurării automatizate a SIA RSISC.	Corespunde

16.10 Cerințe de documentare a sistemului informatics

ID	Obligativitate	Descrierea cerinței funcționale	Propunerea
DOC 001	M	Furnizorul va pregăti și publica materiale de ghidare interactivă incluse îninterfața utilizator a SIA RSISC.	Furnizorul satisface cerința
DOC 002	M	Furnizorul va pregăti și livra manualul utilizatorului în limba Română.	Furnizorul satisface cerința
DOC 003	M	Furnizorul va pregăti și livra ghidul administratorului în limba Română.	Furnizorul satisface cerința
DOC 004	M	Furnizorul va pregăti și livra ghidul de instalare si configurare a sistemului(care să includă cel puțin compilarea codului, instalarea aplicației, cerințe hardware și software, descrierea și configurarea platformei, configurareaaplicației, proceduri de disaster recovery).	Furnizorul satisface cerința
DOC 005	M	Furnizorul va pregăti și livra proiectul tehnic al sistemului informaticlivrat în baza căruia vor fi efectuate totalitatea activităților de dezvoltare/acceptanță a sistemului informatic (SRS și SDD).	Furnizorul satisface cerința
DOC 006	M	Furnizorul va pregăti și livra documentația de Arhitectură a sistemului cu descrierea modelelor în limbajul UML, care să includă un nivel de detaliere suficient al arhitecturii în mai multe secționări (inclusiv modelullogic și fizic al datelor).	Furnizorul satisface cerința
DOC 007	M	Furnizorul va pregăti și livra documentația API-urilor consumate șiexpuse pentru integrare cu sistemele informatice externe.	Furnizorul satisface cerința
DOC 008	M	Furnizorul va livra totalitatea instrucțiunilor necesare bunei exploatări aSIA RSISC și soluționare a unor eventuale probleme tehnice.	Furnizorul satisface cerința
DOC 009	M	Furnizorul va livra codul sursă pentru aplicațiile și componentele dezvoltate în cadrul proiectului cu comentariile necesare înțelegeriicodului program.	Furnizorul satisface cerința

DOC 010	M	Furnizorul va livra documentația de instruire pentru toate rolurile deutilizatori ai SIA RSISC.	Furnizorul satisface cerința

16.11 Cerințe de garanție, mentenanță și suport tehnic al sistemului informatics

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
GMS 001	M	Dezvoltatorul va oferi garanție și suport tehnic pe parcursul a 12 lunidupă acceptanța finală a SIA RSISC.	Furnizorul satisface cerința
GMS 002	M	Garanția și suportul tehnic va corespunde standardului național SM ISO/CEI 14764:2015 - Ingineria software. Procesele ciclului de viață al software-ului. Mentenanță.	Furnizorul satisface cerința
GMS 003	M	Dezvoltatorul va pune la dispoziția STISC un serviciu Help Desk disponibil în toate zilele lucrătoare ale anului.	Furnizorul satisface cerința
GMS 004	M	Utilizatorii STISC vor putea apela serviciul Help Desk la un număr detelefon național (care corespunde numerotării telefonice a RepubliciiMoldova).	Furnizorul satisface cerința
GMS 005	M	Limba de comunicare cu serviciul Help Desk – română sau rusă.	Furnizorul satisface cerința
GMS 006	M	Utilizatorii STISC vor putea semnala alternativ problemele tehniceapărute prin mecanism de ticketing, Email sau mesaje instant.	Furnizorul satisface cerința
GMS 007	M	Furnizorul va asigura suport de documentare a problemelor tehnice șitrasabilitatea acestora pentru Beneficiar.	Furnizorul satisface cerința
GMS 008	M	Termenul limită de răspuns și remediere a problemelor tehnice raportatenu va depăși 8 ore de la semnalarea acestora.	Furnizorul satisface cerința
GMS 009	M	În cazul unor probleme de complexitate majoră, termenul de soluționarea acestora nu va depăși 72 ore.	Furnizorul satisface cerința
GMS 010	M	Dezvoltatorul va demonstra capabilitatea de asigurare a suportuluitehnic post livrare în conformitate cu cerințele GMS 001-GMS 009.	Furnizorul satisface cerința
GMS 011	M	Orice eroare program depistată pe parcursul perioadei de garanție va firemediată de Dezvoltator gratuit și în termen util.	Furnizorul satisface cerința
GMS 012	M	În cazul apariției unor solicitări adăugătoare de implementare, acesteavor face obiectul unui amendament la contract și plată a contravalorii serviciilor.	Furnizorul satisface cerința
GMS 013	M	Furnizorul și STISC vor semna un SLA care va specifica în detalii principiilede prestare a serviciilor de garanție, mentenanță și suport.	Furnizorul satisface cerința

17 Produsul final și componentele livrate

17.1 Lista livrabilelor de proiect

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea

DEL 001	M	Codul sursă complet al modulelor și componentelor necesare compilăriiprodusului program livrat.	Furnizorul satisface cerința
DEL 002	M	Soluția software de migrare și populare primară a datelor în SIA RSISC.	Furnizorul satisface cerința
DEL 003	M	Produsul final împachetat pentru instalare facilă în mediul tehnologicpropus (inclusiv scripturile de deployment automatizat).	Furnizorul satisface cerința
DEL 004	M	Documente și rapoarte aferente proceselor de management al proiectului de proiectare, dezvoltare și implementare a SIA RSISC.	Furnizorul satisface cerința
DEL 005	M	Proiectul Tehnic (SRS+SDD).	Furnizorul satisface cerința
DEL 006	M	Documentul privind desfășurarea și configurarea SIA RSISC.	Furnizorul satisface cerința
DEL 007	M	Manualul Utilizatorului.	Furnizorul satisface cerința
DEL 008	M	Manualul Administratorului (inclusiv planul de contingență).	Furnizorul satisface cerința
DEL 009	M	Ghidul de înlăturare a defecțiunilor și activităților de mentenanță curentăa SIA RSISC.	Furnizorul satisface cerința
DEL 010	M	Totalitatea materialelor aferente instruirii utilizatorilor SIA RSISC.	Furnizorul satisface cerința
DEL 011	M	Specificațiile tehnice pentru interfețele consumate și publicate de SIARSISC.	Furnizorul satisface cerința
DEL 012	M	Planul de testare și rezultatele testării interne (funcționale, de integrare,de performanță, de încărcare, de securitate).	Furnizorul satisface cerința
DEL 013	M	Acord SLA semnat cu STISC pentru perioada de mentenanță, garanție șisuport.	Furnizorul satisface cerința
DEL 014	M	Toate artefactele urmează a fi livrate pe suport electronic (DVD+-R).	Furnizorul satisface cerința

17.2 Serviciile de transfer de cunoștințe aferente artefactelor livrate

ID	Obliga-tivitate	Descrierea cerinței funcționale	Propunerea
DEL 015	M	Furnizorul urmează să efectueze activități de instruire destinate trainerilor STISC care vor putea instrui în continuare toate categoriile deutilizatori a SIA RSISC.	Furnizorul satisface cerința
DEL 016	M	Furnizorul urmează să efectueze activități de instruire tuturor categoriilor de utilizatori autorizați și utilizatorilor cu rol administrator desistem.	Furnizorul satisface cerința
DEL 017	M	Furnizorul urmează să furnizez servicii de asistență tehnică pe perioadade pilotare a SIA RSISC.	Furnizorul satisface cerința
DEL 018	M	Furnizorul va asista STISC în activitățile de testarea de acceptare a SIARSISC.	Furnizorul satisface cerința
DEL 019	M	Furnizorul urmează să furnizeze servicii de asistare a STISC în proceselede punere a SIA RSISC în producție.	Furnizorul satisface cerința
DEL 020	M	Furnizorul urmează să elimine toate deficiențele și erorile ale SIA RSISCidentificate pe perioada de pilotare și la testarea de acceptare.	Furnizorul satisface cerința
DEL 021	M	Furnizorul urmează să asigure suport tehnic post implementare (dupăpunerea sistemului în producție) pentru o perioadă de 12 luni, inclusivmentenanță corectivă, adaptivă și preventivă, în conformitate cu *SM ISO/CEI 14764:2015 - Ingineria software. Procesele ciclului de viață alsoftware-ului. Mentenanță*.	Furnizorul satisface cerința