PRIDE | Cloud Computing Services & Managed Services
+373 22 844-266 | office@pride.md | www.pride.global
MD-2004, Moldova, Chișinău, str. Columna 170 lit.“Ş”

Oferta Tehnică

RSISC

Digitally signed by Leu Alexei
Date: 2023.04.24 14:25:13 EEST
Reason: MoldSign Signature
Location: Moldova

Table of Contents

Introducere

În conformitate cu prevederile art.10 alin (1) al Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, Hotărârii Guvernului nr.482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică” (în continuare - STISC), în calitatea sa de Centru guvernamental de reacție la incidente de securitate cibernetică (în continuare - CERT Gov) și punct unic de contact și de raportare a incidentelor de securitate cibernetică pentru structurile de tip CERT departamentale ale Guvernului, asigură securitatea, inclusiv securitatea cibernetică, a resurselor și sistemelor informaționale de stat.

Una din atribuțiile STISC în calitate de CERT Gov este de a crea și pune în aplicare Registrul de stat al incidentelor de securitate cibernetică. De asemenea, conform pct.5 subpunctul 7) și 8) ale Măsurilor necesare pentru asigurarea securității cibernetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr. 482/2020, CERT Gov are atribuția de a oferi o platformă informațională de comunicare strategică cu entitățile publice precum și de a asigura evidența amenințărilor, vulnerabilităților și incidentelor de securitate cibernetice identificate sau raportate.

În prezent, pentru raportarea incidentelor de securitate cibernetică și alte date aferente acestora se utilizează procese semi-automatizate, ceea ce presupune numeroase riscuri privind: securitatea informației, integritatea datelor, istoricul modificărilor etc.

Incidentele raportate sunt documentate conform unui șablon predefinit (formular de raportare a incidentelor de securitate cibernetică) și sunt remise prin poșta electronică, fiind înregistrate manual întro bază de date în format MS Excel. Metoda actuală nu asigură realizarea unei analize comprehensive, care ar permite identificarea cauzelor și a ariilor expuse riscului de securitate. Înregistrarea și monitorizarea tuturor tipurilor de incidente de securitate cibernetică, ar îmbunătăți aspecte ce țin de: definiția, clasificarea, învățarea din incidente.

Astfel, apare necesitatea creării și implementării Sistemului Informațional Automatizat „Registrul de stat al incidentelor de securitate cibernetică” (în continuare - SIA RSISC). Prin aceasta se urmărește îmbunătățirea proceselor existente în cadrul CERT Gov, a modului de gestiune a incidentelor de securitate cibernetică, precum și furnizarea următoarelor beneficii:

- optimizarea proceselor de lucru și reducerea costurilor operaționale;
- regăsirea rapidă a datelor și documentelor relevante pentru procesele de lucru ale CERT Gov;
- consolidarea unei baze de date electronice aferentă incidentelor de securitate cibernetice;
- consolidarea unei baze de cunoștințe ce ar contribui la îmbunătățirea calității funcționării CERT Gov;
- înregistrarea și evidența totalității documentelor aferente incidentelor de securitate cibernetică;

- standardizarea datelor și acuratețea informațiilor gestionate în sistem;
- reducerea birocrației prin eliminarea treptată a evidențelor manuale;
- simplificarea procesului de introducere, modificare, actualizare a informațiilor aferente incidentelor de securitate cibernetică;
- centralizarea în format electronic a informațiilor cu privire la incidentele raportate de entitățile publice;
- asigurarea interoperabilității cu sisteme informatice ale entităților publice pentru schimbul bidirecțional de date.
- asigurarea schimbului de date cu privire la incidentele de securitate cibernetică, în format electronic, între CERT Gov și CERT departamentale, conform legislației;
- reducerea timpului mediu de raportare și răspuns la incidente de securitate cibernetică;
- asigurarea unui mediu operațional partajat, precum și a unei securități crescute a datelor electronice și informațiilor în cadrul și între entitățile publice.

Prezentul document prezintă o viziune conceptuală asupra ofertei tehnice propuse pentru a fi dezvoltată, implementată precum și asigurarea punerii in exploatare a Sistemului Informațional Automatizat „Registrul de stat al incidentelor de securitate cibernetică” incluzând aspecte privind scopul și obiectivele, principiile, caracteristicile de bază, funcționalitatea și arhitectura conceptuală, cerințele funcționale și nefuncționale ale sistemului informatic.

În acest sens este prezentată o descriere succintă a componentelor de bază ale viitoarei soluții accentuând principiile și particularitățile de implementare a funcționalităților și fluxurilor de lucru de care trebuie să se țină cont la elaborarea Sistemului Informațional Automatizat „Registrul de stat al incidentelor de securitate cibernetică”.

Descrierea Companiei

PRIDE SYSTEM SRL este o companie din Republica Moldova, fondată în anul 2013, specializată pe dezvoltarea de sisteme informatice, aplicații software, infrastructuri TIC, infrastructuri Cloud Computing, și prestare de servicii aferente domeniului.

Am obținut și ne mândrim cu o experiență vastă în dezvoltarea și livrarea de soluții informatice complexe, infrastructuri TIC reziliente și moderne, atât în sectorul privat și public.

Portofoliul nostru include un număr important de proiecte realizate în Republica Moldova, dar și peste hotarele țării, toate orientate pe satisfacerea și depășirea așteptărilor clienților, aplicarea inovațiilor, reducerea și optimizarea costurilor și atingerea criteriilor de calitate.

La ziua de astăzi suntem unul din dintre cei mai importanți și siguri furnizori, din Republica Moldova, de soluții TIC de tip: Infrastructură de bază, telecomunicații, securitate cibernetică, Virtualizare și Cloud Computing, Unified Communications & Collaboration, Business Intelligence, Software and Application development.

În direcția de dezvoltarea Sisteme informaționale activitatea PRIDE SYSTEM se bazează pe cele mai noi tehnologii și standarde:

Fron-end development:	HTML, CSS, JavaScript, React, React Native, Angular, Bootstrap, Vue.JS, TypeScript, Flutter, npm etc;
Back-end development:	ASP.NET Core, ASP.NET MVC, Node JS, Spring Boot, Symfony, Laravel, Ruby on Rails, AngularJS, Bootstrap, Gatsby, Django, Next.js
Other	WEB API, Elastic Search , Windows Service, SharePoint, Entity Framework Core etc.
RDBMS	Microsoft SQL Server, Azure SQL Database, PostgreSQL, MongoDB, OracleDB, MySQL, MariaDB, etc
Management	Waterfall, Agile, SCRUM **using**: Microsoft Project, Jira, Dev Azzure
DevOps	SVC (GitLab, GitHub), CI/CD (Azure, Bitbuket) Virtualization (Hyper-V, VMWare, Nutanix)
Monitoring	Prometheus, Kibana, Grafana, Zabbix SIEM Solutions (Microsoft Sentinel, Splunk, QRadar, FortiSiem, etc)

Cloud	Azure Services, Google Cloud, AWS, OnPremises solutions (Hyper-V, VMware, Nutanix, KVM)
Container	Kubernetes, Docker

Misiunea noastră: să asigurăm buna funcționare și dezvoltarea afacerilor clienților noștri. Scopul nostru este de a oferi clienților o calitate și o gamă completă de servicii proprii Cloud cât și a partenerilor tehnologici care să le permită să-și salveze propriul timp, bani și să gestioneze eficient afacerea.

Strategia noastră este de a anticipa nevoile clientului. Vedem clar perspectivele dezvoltării tehnologiei informației și înțelegem ce instrumente sunt necesare astăzi și mâine pentru ca clienții noștri să își desfășoare în mod eficient afacerea și în viața de zi cu zi. Creăm noi concepte tehnologice, prognozăm nevoile clienților și oferim tipuri avansate de echipamente și produse la prețuri rezonabile. Raportul preț-calitate este unul dintre avantajele noastre incontestabile.

Obiectivul nostru este creșterea cerințelor și așteptărilor clienților noștri. Soluțiile noastre au o valoare și nu un simplu preț!

Structura companiei este flexibilă, bazată pe direcții de business generate de soluțiile personalizate oferite partenerilor săi.

Echipa PRIDE SYSTEM este constituită de profesioniști calificați cu profil și expertiză într-o vastă gama de tehnologii (Full-Stack Development, Front-End Development, Back-End Development, Project management, Information security, Quality engineering, etc.), organizați într-o structură flexibilă și care să corespundă nivelului de performanță.

Portofoliu de proiect

n/o	Obiectul contractului	Beneficiar	Valoarea Proiectului	Perioada
1	Servicii de dezvoltare Full-Stack, software deployment, suport și mentenanță, administrare și găzduire SI **„Building management system (BMS) for Warehouse Automation and Pharmaceuticals Manufacturing”**	**SOPHARMACY MC SRL** str. Columna 170, Chișinău, MD-2004	3506032 MDL	36 luni
2	Servicii de dezvoltare Full-Stack, software deployment, suport și mentenanță, administrare și găzduire SI **„OTT/IPTV Platform for Live Streaming and Video on demand”**	**NGM COMPANY SRL** str. Arborilor 17/2, Chișinău, MD-2025	1470465 MDL	36 luni

3	Servicii de dezvoltare Full-Stack, software deployment, suport și mentenanță, administrare și găzduire SI **„Customer relationship management (CRM) system”**	BUSINESS LOGISTIC SRL str. Ismail 81/1 Chișinău	1633395 MDL	36 luni
4	Servicii de implementare software personalizat SI **„Healthcare patient management software and medical practice management (MPM)”**	CME SANCOS SRL bd. Moscova 16 Chișinău	1035424 MDL	36 luni
5	Servicii de implementare software personalizat SI **Document Management System (DMS)**	EXCELLENCE SRL str.Grenoble 23 Chișinău	550000 MDL	6 luni
6				
7				

Descrierea succintă a soluțiilor informatice similare:

Perioadă	Beneficiar	Scurtă descriere	Valoare	Rol
2020-2023 (on-going)	SOPHARMACY MC SRL **Project Name: Building management system (BMS)**	**Building management system (BMS)** for Warehouse Automation and Pharmaceuticals Manufacturing Proiectul a fost dezvoltat pentru satisfacerea necesităților clientului de monitorizare, control și automatizare a operațiunilor industriale, reinginerie a proceselor specifice activităților de business și anume aferente producerii eficiente (micșorând costurile de operare), păstrării (protejând bunurile și resursele fizice) și monitorizării produselor farmaceutice (garantând o funcționare sigură). **Funcționalitățile principale:** ✓ Production environment parameters ✓ Centralized management of various sensors and assets ✓ Dashboard for easy access to data ✓ Automated workflows **Activități**: • Business Analysis: Identifying business needs and requirements, studying current processes, and evaluating software options. • Regulatory Compliance: Ensuring that the BMS system complies with industry standards and regulatory requirements. • Facility Planning and Design: Designing and planning the physical space of the building to accommodate the BMS system's infrastructure. • System Architecture Design: Creating an architectural design and selecting technologies that align with the organization's needs and meet regulatory requirements. • HVAC and Refrigeration Control: Developing and integrating control systems to monitor and regulate HVAC and refrigeration systems. • Temperature and Humidity Control: Developing and integrating control systems to monitor and regulate temperature and humidity levels. • Power Monitoring and Control: Developing and integrating control systems to monitor and regulate power usage and quality.	>3,5 mln. MDL	Contractant unic

		• Access Control: Implementing access control systems to secure the facility and limit access to sensitive areas. • Fire and Life Safety: Developing and integrating systems to monitor and respond to fire and life safety emergencies. • Data Management and Analytics: Developing data management and analytics systems to monitor system performance and identify trends or issues. • Quality Assurance and Testing: Conducting comprehensive testing to ensure the BMS system is functioning correctly and meeting regulatory requirements. • Training and Support: Providing training and support to users to help them use the BMS system efficiently. • Maintenance and Updates: Ongoing maintenance		

Perioadă	Beneficiar	Scurtă descriere	Valoare	Rol
2020-2023 (on-going)	NGM COMPANY SRL **Project Name: OTT/IPTV Platform**	**OTT/IPTV Platformă pentru Live Streaming și Video on demand.** PRIDE SYSTEM a asigurat dezvoltarea (from scratch) a unei Serviciu pentru accesare și vizualizare conținut video și canale TV, în regim de timp-real (Live Streaming) și la solicitare (Video nn demand), în dependență de preferințele utilizatorilor. **Funcționalitățile principale:** ✓ Streaming Infrastructure ✓ Video Content Management ✓ Multilayer Analytics ✓ Secure Monetization ✓ Integrated Marketing Tools ✓ Pleasing User Experience ✓ ... **Activități**: • Business Analysis: Identifying business needs and requirements, analyzing the competition, and studying current market trends. • Content Strategy: Developing a content strategy that aligns with the platform's target audience and business objectives. • Technology and Architecture Design: Designing a technology and architecture plan to support the platform's functionality and performance goals.	>1,47 mln. MDL	Contractant unic

		• User Interface Design: Designing an easy-to-use interface for users to navigate and access content. • Video Encoding and Delivery: Establishing a video encoding and delivery infrastructure to ensure fast, high-quality video delivery to users. • Content Management: Developing a content management system to manage and organize video content. • Payment Processing: Integrating payment processing systems to enable users to purchase content or subscribe to the platform. • Analytics and Reporting: Implementing analytics and reporting tools to monitor user behavior and gather data on platform performance. • Multi-Platform Compatibility: Ensuring the platform is compatible with various devices, including smartphones, tablets, and smart TVs. • Quality Assurance and Testing: Conducting comprehensive testing to ensure the platform is functioning correctly. • Launch and Deployment: • Maintenance and Support: Providing ongoing maintenance and support		

Perioadă	Beneficiar	Scurtă descriere	Valoare	Rol
2020-2023 (on-going)	BUSINESS LOGISTIC SRL **Project Name: Customer relationship management (CRM) system**	Customer Relationship Management System pentru necesitățile de business ale beneficiarului. **Funcționalitățile principale:** • Contact management • Lead management • Reporting and analytics • Marketing • Pipeline management • Workflow automation • Document management • ... **Activități:** • Business Analysis: Identifying business needs and requirements, analyzing the competition, and studying current market trends. • Content Strategy: Developing a content strategy that aligns with the platform's target audience and business objectives. • Technology and Architecture Design: Designing a technology and architecture plan to support the platform's functionality and performance goals.	>1,63 mln MDL	Contractant unic

		• User Interface Design: Designing an easy-to-use interface for users to navigate and access content. • Video Encoding and Delivery: Establishing a video encoding and delivery infrastructure to ensure fast, high-quality video delivery to users. • Content Management: Developing a content management system to manage and organize video content. • Payment Processing: Integrating payment processing systems to enable users to purchase content or subscribe to the platform. • Analytics and Reporting: Implementing analytics and reporting tools to monitor user behavior and gather data on platform performance. • Multi-Platform Compatibility: Ensuring the platform is compatible with various devices, including smartphones, tablets, and smart TVs. • Quality Assurance and Testing: Conducting comprehensive testing to ensure the platform is functioning correctly and meeting business requirements. • Launch and Deployment: Deploying the platform to the production environment and launching it for public use. • Maintenance and Support: Providing ongoing maintenance.		

Perioadă	Beneficiar	Scurtă descriere	Valoare	Rol
2022	EXCELLENCE SRL **Project Name:** **Document Management System (DMS)**	Document management System (DMS) pentru necesitățile de business ale beneficiarului. **Funcționalitățile principale:** ✓ Centralized management ✓ Requirements for privacy protection compliance ✓ Revision security ✓ Group based authorisations ✓ Versioning ✓ Aarchiving ✓ Automated workflows ✓ ... **Activități:** • Business Analysis: Identifying business needs and requirements, studying current processes, and evaluating software options. • System Architecture Design: Creating an architectural design and selecting	>550 mii, MDL	

		technologies that align with the organization's needs. • Database Design: Defining data structures, tables, fields, and relationships that will store documents. • User Interface Design: Designing an easy-to-use interface for users to interact with the DMS system. • Application Development: Building and testing the DMS software application using the selected technologies. • Integration: Integrating the DMS system with other software applications, such as an ERP system or a CRM system. • Data Migration: Migrating data from the existing system to the new DMS software. • Customization: Adding new features and customizing the DMS software • Testing: Conducting comprehensive testing • Deployment: Deploying the DMS software to the production environment. • Training and Support • Maintenance: Ongoing maintenance and updates.		

Perioadă	Beneficiar	Scurtă descriere	Valoare	Rol
2020	CME SANCOS S.R.L. **Project name: Patient Management software (MPM)**	Healthcare patient management software and medical practice management (MPM) Cusomizarea și operaționalizarea aplicației software specializate pentru necesitățile de business a beneficiarului. **Printre principalele activități:** ✓ Automates appointment scheduling. ✓ Provides e-forms or intake forms for patients to fill before admission. ✓ Records interactions. ✓ Manages referrals. ✓ Allows payments. ✓ Maintains electronic records of your patients and their medical history.	>1,0 mil, MDL	Contractant unic

Printre clienții noștri:

Alte referințe (domeniile de activitate):

Servicii de Cloud Computing pentru companii în propriul Cloud PRIDE;

Dezvoltare de produse software:

- Dezvoltare SaaS
- Dezvoltare Cloud
- Dezvoltare Web
- Dezvoltare API și integrare software

Servicii de afaceri:

- Expertiză tehnică pentru tehnologia informației
- Auditul securității informației
- Gestionarea și optimizarea activelor software
- Instruire și certificare

Servicii de infrastructură:

- Sisteme informatice și rețele

- Sisteme de alimentare neîntreruptibile
- Supraveghere video și difuzare
- Securitate și control acces
- Automatizări industriale (IIoT, DCS/SCADA)

Servicii suport:

- Externalizare IT completă, încrucișată sau parțială
- Management integrat al infrastructurii IT bazat pe SLA;

Servicii de mentenanță și reparații pentru:

- Echipamente TIC
- Surse de alimentare neîntreruptibile
- Echipamente de supraveghere video
- Echipamente foto-video

Principiile de elaborare

Întru asigurarea obiectivelor înaintate sistemului informatic SIA RSISC, la proiectarea, realizarea și implementarea acestuia trebuie să se țină cont de următoarele principii generale:

- Principiul legalității: care presupune crearea și exploatarea sistemului informatic, în conformitate cu legislația națională în vigoare, a normelor și standardelor internaționale recunoscute în domeniu;

- Principiul responsabilității și conștientizării care constă în efortul continuu derulat de entitățile de drept public și privat în conștientizarea rolului și responsabilității individuale pentru atingerea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice

Principiul divizării arhitecturii pe nivele care constă în proiectarea și implementarea componentelor funcționale ale SIA RSISC în conformitate cu standardele de interfață dintre nivele;

- Principiul arhitecturii bazate pe servicii (SOA) care constă în distribuirea componentelor funcționale ale sistemului informatic în componente mai mici, distincte - numite servicii - care pot fi distribuite într-o rețea și pot fi utilizate împreună pentru a crea aplicații destinate implementării funcțiilor de business ale sistemului informatic. Aceste componente vor putea fi implementate fără dependențe reciproce rigide și vor interacționa prin interfețe externe implementate în bază de standarde deschise și independente de tehnologie. Acest fapt conferă flexibilitatea alegerii tehnologiilor și cicluri de viață independente pentru componentele SIA RSISC De asemenea, va permite părților interesate să selecteze opțiuni tehnologice alternative pentru capabilitățile de introducere și accesare date.

- Principiul reutilizării capabilităților existente care presupune că SIA RSISC va fi implementat prin reutilizarea la nivelul componentelor sale a capabilităților TIC curente la care are acces STISC. Dezvoltarea de noi capabilități specifice SIA RSISC se va face doar în cazul lipsei acestora în arhitectura TIC curentă a STISC (cu păstrarea arhitecturii SOA și asigurarea posibilității reutilizării acestor capabilități de alte sisteme informatice, unde e posibil). Acest fapt presupune utilizarea serviciilor de platformă guvernamentală, sau a soluțiilor de platformă implementate în cadrul STISC, pentru dezvoltarea componentelor ce formează SIA RSISC.

- Principiul alinierii la arhitectura TIC de scară largă a STISC care presupune că locul SIA RSISC în arhitectura TIC de scară largă este explicit delimitat în raport cu alte sisteme informatice ale STISC. SIA RSISC trebuie implementat cu aplicarea principiilor de arhitectură TIC stabilite de STISC și trebuie să fie capabil să interacționeze cu alte componente ale arhitecturii TIC. Principiile de arhitectură TIC sunt la rândul lor aliniate la principiile de arhitectură guvernamentală.

- Principiului modelului de date deschis și interoperabil care presupune că modelul de date susținut de SIA RSISC este documentat și comunicat către toți actorii interesați. SIA RSISC urmează a fi dezvoltat în baza standardelor acceptate în domeniu și aliniat la modelul de date guvernamental și departamental (adoptarea taxonomiei și semanticii deja existente la nivel național și departamental și îmbogățirea acesteia pentru a satisface necesitățile specifice domeniului asigurării securității informației).

- Principiul securității prin design care presupune proiectarea SIA RSISC în cunoștință de cauză cu privire la riscurile de securitate a informației ce pot afecta buna funcționare a sistemului informatic. Cerințele legale aplicabile pentru protecția datelor personale trebuie considerate la etapa de proiectare a SIA RSISC și implementate la etapa de dezvoltare. SIA RSISC va asigura accesarea controlată, transparentă și responsabilă a datelor.

- Principiul integrității, plenitudinii și veridicității datelor care presupune implementarea mecanismelor care permit păstrarea conținutului și interpretării univoce a datelor în condițiile unor influențe accidentale și eliminării fenomenelor de denaturare sau lichidare accidentală a acestora, furnizarea unui volum de date suficient executării funcțiilor de business al sistemului informatic și asigurarea unui grad înalt de corespundere a datelor cu starea reală a obiectelor pe care le reprezintă și care fac parte din SIA RSISC.

- Principiul accesibilității informației cu caracter public care presupune implementarea procedurilor de asigurare a accesului solicitanților la informația cu caracter public furnizată de soluția informatică.

Principiul expansibilității care stipulează posibilitatea extinderii și completării sistemului informatic cu noi funcții sau îmbunătățirea celor existente;

- Principiul de prioritate a primei persoane/a centrului unic care presupune existența unei persoane responsabile de rang înalt, cu drepturi suficiente pentru luarea deciziilor și coordonarea activităților în vederea creării și exploatării sistemului informatic;

- Principiul scalabilității care presupune asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării sistemului informatic;

- Principiul simplității și comodității utilizării care presupune proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor SIA RSISC, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție.

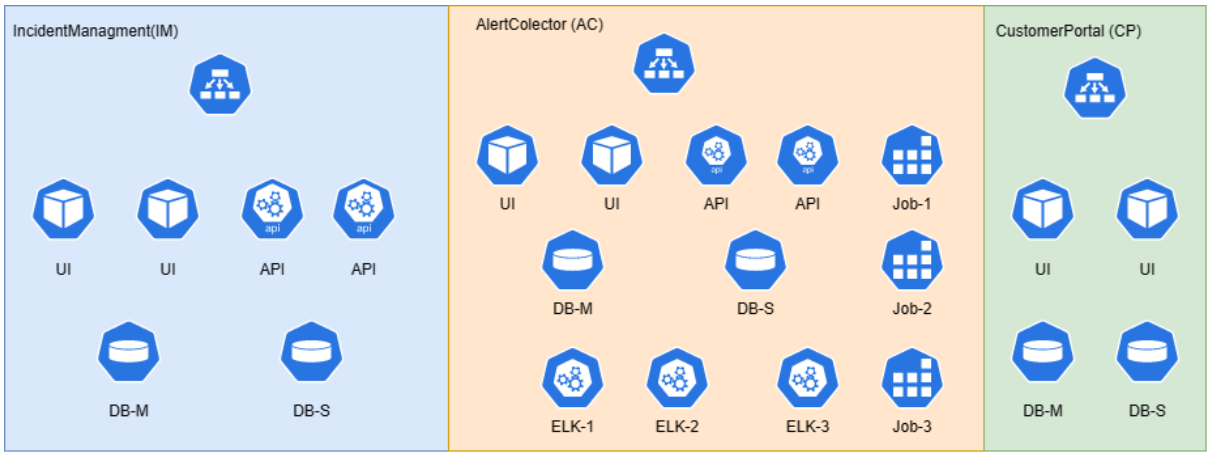
Arhitectura de nivel înalt a sistemului

Sistemul propus spre dezvoltare este compus din 3 componente majore, care interacționează intre ele si asigura funcționarea completa conform cerințelor funcționale si non-funcționale.

Sistemul este unul modular, bazat pe micro-servicii, scalabil atât pe orizontala cit si pe verticala.

Sistemul este propus, este unu Cloud-native, fără care restricții sau dependente hardware, ceea ce presupune câteva metode de desfășurare (deployment):

1. BareMetal
2. Infrastructura Virtuala
3. Docker-Composer
4. Kubernetes



Etapele de implementare

Activitățile de proiectare, dezvoltare, testare și implementare a a SIA RSISC o să fie realizate și vor cuprinde următoarele etape:

1. Etapa de elaborare a sistemului informatic - care va fi divizată în faze coordonate cu STISC după cum urmează:
   a. Furnizorul analizează termenii de referință, efectuează analiza de business și cu aprobarea STISC propune viziunea sa de dezvoltare a sistemului informatic prin intermediul unui Proiect tehnic (SRS și SDD) elaborat în termen de 1 lună calendaristică;
   b. Furnizorul dezvoltă codul program și integrează modulele dezvoltate într-o versiune prototip a SIA RSISC (se va face o primă prezentare părților demonstrând existenta tuturor funcționalităților descrise în prezentul caiet de sarcini) care ulterior va fi perfecționată până la semnarea acceptanței finale. Etapa în cauză nu va depăși 6 luni;
   c. Furnizorul efectuează activitățile de migrare și populare inițială cu date a SIA RSISC (1 lună calendaristică).
   d. Furnizorul testează sistemului în regim de laborator (testare internă) și pregătește documentația de însoțire (se prezintă funcționalitățile sistemului cu corectările și ajustările la obiecțiile făcute în sub-etapa precedentă, se prezintă setul documentației tehnice, etc.). Etapa în cauză va dura 3 săptămâni. Testarea va cuprinde obligatoriu următoarele etape:
      - vor fi verificate în comun totalitatea scenariilor de testare privind satisfacerea tuturor cerințelor funcționale ale sistemului informatic (functional testing, unit testing, integration testing); o asupra sistemului sunt aplicate scenarii de stress testing, load testing și security testing în vederea verificării gradului de corespundere a acestuia așteptărilor STISC și prevederilor prezentului caiet de sarcini;
      - în baza rezultatelor testării, în caz de necesitate, vor fi operate ajustările și modificărilor solicitate, pregătindu-se o versiune ameliorată a sistemului informatic.
   e. Furnizorul efectuează activitățile de desfășurare și configurare a celor 3 medii ale a SIA RSISC (Mediul de producție, Mediul de testare/instruire, Mediul de dezvoltare). Activitatea date va dura până la 1 săptămână.
2. Etapa de instruire va începe odată cu finisarea testelor de acceptanță și va cuprinde instruirea a 2 utilizatori cu rol Administrator de Sistem, 2 traineri pentru instruirea ulterioară a utilizatorilor autorizați și până la 30 utilizator autorizați cu toate rolurile configurate.
3. Etapa de stabilizare a SIA RSISC va începe odată cu aprobarea procesului verbal de acceptare de către STISC în varianta prezentată și semnarea actului de punere în producție a sistemului informatic. Această etapă va dura 3 luni pe parcursul căreia Furnizorul va asista STISC în exploatarea a SIA RSISC și va efectua activități de eliminare a erorilor/deficiențelor depistate precum și optimizări în parametrii de funcționare a SIA RSISC.
4. Darea în exploatare a sistemului începe odată cu semnarea actului de punere în exploatare a sistemului informatic și începere a exploatării acestuia.

Etapa de garanție mentenanță și suport este perioada în care Furnizorul își asumă obligațiunea față de STISC să-l asiste în menținerea capacității sistemului informatic de a presta servicii, precum și modificarea produsului informatic (eliminarea erorilor și optimizarea parametrilor de funcționare), păstrând integritatea lui. În cazul SIA RSISC sunt necesare 12 luni calendaristice de garanție, mentenanță și suport tehnic.

Metodologia de asigurare a serviciilor de garanție, mentenanță și suport

PRIDE SYSTEM deține o largă experiență în prestarea serviciilor de mentenanță și suport acumulată pe parcursul a peste 10 ani de activitate. Fiecare angajament nou pentru astfel de servicii a fost asumat asigurând o abordare de îmbunătățire continuă, atât în baza experienței instituționale, dar și celor mai bune practici din domeniu. O astfel de maturitate vine și să asigure un nivel excepțional de calitate și cea mai bună orientare spre satisfacția clienților noștri.

În continuare venim cu o descriere exhaustivă a unui model cadrul pentru serviciile de garanție, mentenanță și suport, dar care eventual va fi ajustat și aliniat la cerințele de business, funcționale și non-funcționale ale clientului.

Termeni și definiții, abrevieri

tehnologia informației (abreviat cel mai adesea din engleză „IT” și română „TI”) – este tehnologia necesară pentru prelucrarea (procurarea, procesarea, stocarea, convertirea și transmiterea) informației;

IT&C – tehnologia informației și a comunicațiilor;

externalizare IT (Outsourcing IT) – delegarea de către Beneficiar, a sarcinilor de administrare și/sau mentenanța şi suport IT&C către o companie licențiată/certificată din exterior;

sistem informatic – este un sistem care permite introducerea de date prin procedee manuale sau prin culegere automată de către sistem, stocarea acestora, prelucrarea lor și extragerea informației (rezultatelor) sub diverse forme. Componentele sistemului informatic sunt: echipamentele hardware, programele software, rețelele de calculatoare și utilizatorii;

echipament hardware – este partea fizică a unui sistem informatic, constituită din ansamblul de componente electrice, electronice și mecanice care împreună pot primi, prelucra, stoca și reda informații, sub diverse forme de semnale electrice, acustice sau optice;

program software – este partea logică a unui sistem informatic, constituită din ansamblul de programe soft incluzând procedurile lor de aplicare. Componența software include toată gama de produse de programare, uzual formată din sistem de operare, drivere și programe de aplicație cât și software-le înglobat în construcția de hardware - prin folosirea de circuite integrate preprogramate;

avarie – defecțiune hardware și/sau software a sistemului informatic care face imposibilă activitatea Beneficiarului (deex: server picat/blocat, rețeaua de transport de date/voce a căzut sau sunt pierderi de pachete, aplicație software blocată/virusată etc.);

intervenție la distanță – Prestatorul are în unele cazuri posibilitatea tehnică de a monitoriza funcționarea sistemului informatic, de a preveni accidentele tehnice și de a înlătura defecțiunile conectându-se de la distanță la sistemul informatic al Beneficiarului prin intermediul rețelei Internet, fără a fi nevoie de a se deplasa specialistul IT al Prestatorului la fața locului unde sa produs accidentul;

chemare – necesitatea deplasării specialistului IT al Prestatorului la fața locului, cînd este imposibilă intervenția la distanță;

revizie periodică – realizarea verificării tehnice periodice de întreținere a sistemul informatic deservit (de ex: verificarea integrității sistemului informatic deservit, verificarea parametrilor tehnici vulnerabili şi celor critici conform politicilor de securitate informațională, verificarea vizuală a componentelor electronice la uzură sau defecte exterioare care potențial pot crea o situație de avarie, inspecție vizuală asupra respectării de către Beneficiar al regulilor de exploatare prescrise de producătorul sistemului informatic).

acord scris – confirmare în formă scrisă ștampilată şi semnată de persoană autorizată, expediată prin e-mail, fax, direct sau poștă.

acord verbal – confirmare efectuată la telefon de persoană autorizată (cu condiția înregistrării apelului şi data efectuării acestuia).

zi – zi calendaristică; an – 365 de zile.

cont – denumire unică compusă dintr-un singur cuvânt sau mai multe prin asociere de litere și/sau cifre (de regulă prenume. nume angajat sau identic unui cont de email ca prenume.nume@company.com) la care se alătură o parolă (complexitate definită de Beneficiar conform politicelor de securitate ale sale) și care asigură accesul acestuia la sistemul informatic al Beneficiarului.

nivel agreat de servicii – set de parametri şi indicatori de performanță în baza cărora este măsurată calitatea prestării Serviciilor.

Principiul “cel mai bun efort” – situație în care Prestatorul va depune toată diligența în vederea prestării Serviciilor de cea mai înaltă calitate posibilă, dar fără a garanta conformarea la parametrii de calitate prevăzuți în prezentele Reguli.

Orele de lucru ale Prestatorlui – intervalul cuprins între orele 9:00 şi 18:00 de luni până vineri cu excepția zilelor oficial nelucrătoare. Prestarea *Serviciilor* legate de înlăturarea

problemelor tehnice in cazul unei avarii care a stopat total activitatea *Beneficiarului*, vor fi executate de *Prestator* conform programului de lucru ale *Beneficiarului*.

SSC – Serviciul Suport Clienți.

Elasticitate – capacitatea de a mări sau reduce cantitatea conturilor deservite, în funcție de necesități.

Scopul documentului

Scopul prezentelor *Reguli* este de a stabili modalitatea, particularitățile și nivelul de calitate la prestarea *Serviciilor mentenanță, deservire și suport*, dar și procesele de interacțiune a *Prestatorului* cu *Beneficiarul* în vederea prestării şi utilizării *Serviciilor,* precum şi responsabilitățile *Prestatorului* şi ale *Beneficiarului* în cadrul acestor procese.

Nivelul Serviciilor

1.1. Perioada de disponibilitate pentru *Serviciile* oferite de *Prestator* sunt clasificate în 3 categorii. Perioada garantată pentru nivelul agreat de disponibilitate a *Serviciilor* de tip:

- **Critic** – în regim NON-STOP, pentru cazurile de *avarie*;
- **Moderat** – în orele de lucru ale *Beneficiarului,* pentru intervențiile la distanță prin acord scris/verbal. În afara perioadei garantate, *Prestatorul* va asigura disponibilitatea *Serviciilor* în baza principiului „cel mai bun efort”;
- **Rezervat** – în *orele de lucru ale Prestatorlui* pentru *chemări* și *revizii periodice*. În afara perioadei garantate, *Prestatorul* va asigura disponibilitatea *Serviciilor* în baza principiului „cel mai bun efort”;

1.2. *Serviciile* sunt considerate disponibile și executate în următoarele scenarii:

- pentru cele **Critice** – dacă în decurs de 30 min din momentul depistării de către *Prestator* sau sesizării de către *Beneficiar* a cazului de *avarie*, a fost anunțați în scris și/sau verbal *Beneficiarului* termenii de restabilire a *sistemului informatic* aflat în gestiunea *Perestatorului* și restabilită activitatea *Beneficiarului* in decurs de 3 ore după depistarea/sesizarea cazului de *avarie* dacă este tehnic posibil;
- pentru cele **Moderate** – dacă în decurs de 3 ore lucrătoare după oferirea accesului la distanță către dispozitivul/serviciul reclamat a fost remediată defecțiunea sau a fost comunicat *Beneficiarului* de către *Prestator* prin acord scris/verbal termenii/condițiile necesare pentru a înlătura defecțiunea reclamată sau motivul imposibilității executării *Serviciilor*;
- pentru cele **Rezervate** – dacă în decurs de 8 ore lucrătoare din momentul înregistrării unei chemări *Serviciile* au fost executate și/sau efectuată după caz *revizia periodică* planificată și agreată de *Părți*.

Nivelul de accesibilitate

Serviciile contractate pot fi executate și la distanță prin intermediul rețelei Internet/Intranet.

Securitatea informației

Părțile acceptă de comun acord să coopereze în vederea gestiunii riscurilor de securitate a informației ce pot afecta *Serviciile* contractate şi/sau *sistemul informatic* aflat in gestiunea *Prestatorului* și care sunt dependente de serviciile *Prestatorului*.

În cadrul *Serviciilor*, *Prestatorul* asigură cu:

a. consultanță TIC și livrări de soluții tehnologice mature întru securizarea *sistemului informatic* aflat în gestiunea *Prestatorului* împotriva încălcări ale securității datelor / transmisiei de date ex-filtrare și prevenirea acestora, monitorizarea, detectarea și blocarea datelor *sensibile*. Următoarele date cu caracter personal sunt considerate „*sensibile*” și fac obiectul unor condiții de prelucrare speciale:
   - date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice;
   - apartenența la sindicate;
   - date genetice, datele biometrice prelucrate doar pentru identificare a unei ființe umane;
   - date privind sănătatea;
   - date privind viața sexuală sau orientarea sexuală a unei persoane.

b. consultanță IT&C și livrări de soluții tehnologice mature întru securizarea *sistemului informatic* aflat în gestiunea *Prestatorului* împotriva programelor software rău intenționat / dăunător;

c. consultanță IT&C și livrări de paravane de protecție menite să filtreze, să cripteze și/sau să intermedieze traficul de date;

d. accesul securizat (https) în sistemul Service Desk al *Prestatorului* de înregistrare a incidentelor și/sau interpelărilor *Beneficiarului*;

e. accesul la sistemul automat de actualizare a pachetelor de corecție pentru *sistemul informatic* aflat în gestiunea sa. În cazul unui incident care pune în pericol securitatea informației, *Partea* care a constatat producerea incidentului va notifica imediat cealaltă *Parte*, dacă şi aceasta poate fi afectată de incident. *Părțile* vor coordona măsurile care pot fi întreprinse pentru a diminua consecințele incidentului şi pentru a le lichida.

După soluționarea unui incident de securitate a informației, *Părţile* vor întocmi rapoarte individuale privind gestiunea incidentului. De comun acord, *Părţile* vor elabora un plan de acțiuni pentru prevenirea repetării unor incidente similare.

Lucrări de mentenanţă

Pentru menținerea nivelului agreat al *Serviciilor*, *Prestatorul* va efectua lucrări de mentenanța. Tipul lucrărilor de mentenanța şi angajamentele *Prestatorului* privind notificarea *Beneficiarului*, perioada şi durata acestor lucrări sunt coordonate și agreate cu Beneficiarul.

Tabelul 2. Lucrări de mentenanța

Tipul lucrărilor de mentenanţă	Notificarea Beneficiarului	Perioada şi durata lucrărilor
Lucrări curente	Cu 5 zile înainte	Sunt efectuate în afara programului de lucru. Durata acestor lucrări nu va depăși 6 ore.
Lucrări majore	Cu 10 zile înainte	Sunt efectuate în afara programului de lucru. Durata acestor lucrări nu va depăși 24 de ore.
Lucrări urgente, neefectuarea imediată a cărora poate duce la indisponibilitatea *Serviciilor* sau poate afecta funcționarea acestora	Notificarea imediat ce a apărut necesitatea inițierii lucrărilor	Po fi efectuate în orice perioadă. Durata acestora nu va depăși 3 ore. Rezultatele efectuării lucrărilor vor fi comunicate Beneficiarului la cerere.

În cazul în care lucrările de mentenanța vor afecta *Beneficiarul*, *Prestatorul* va coordona cu *Beneficiarul* intervalul în care pot fi efectuate acestea, cu excepția efectuării unor lucrări de mentenanța urgente.

Persoane responsabile

Prestatorul va desemna o persoană responsabilă de relația cu *Beneficiarul* (Manager Suport Clienți). *Prestatorul* va informa *Beneficiarul*, prin scrisoare oficială sau e-mail, despre persoana desemnată şi informația de contact a acesteia (numele, prenumele, funcția, număr de telefon, e-mail etc. Schimbarea persoanei responsabile se va face conform aceleiași proceduri. *Beneficiarul* va desemna una sau mai multe persoane responsabile de interacțiunea cu *Prestatorul*. *Beneficiarul* va informa *Prestatorul*, prin scrisoare oficială sau e-mail, în termen de maximum 72 ore, despre persoanele responsabile desemnate.

Serviciul Suport Clienţi

Prestatorul oferă suport *Beneficiarului* la utilizarea *Serviciilor*. În acest scop, *Prestatorul* va opera Serviciul Suport Clienţi (în continuare – ***“SSC”***). *Beneficiarul* va contacta *SSC* în următoarele scopuri:

- pentru a raporta un incident sau o problemă legată de utilizarea *Serviciilor*;
- pentru a solicita modificări în nivelul *Serviciilor* sau noi servicii de același tip;
- pentru a solicita realizarea anumitor activități şi acțiuni care, conform acestor *Reguli*, țin de responsabilitatea *Prestatorului*.

În cazul în care *Beneficiarul* întimpină dificultăți de orice natură la utilizarea *Serviciilor*, acesta va întreprinde, în ordinea indicată, următoarele:

- va consulta ghidurile utilizatorului pentru a fi sigur de corectitudinea acțiunilor sale şi a identifica posibilele soluții;
- va consulta altă informație pusă la dispoziție de *Prestator;*
- va apela *SSC*. *Prestatorul* oferă *Beneficiarului* posibilitatea de a contacta Serviciul Suport Clienți prin următoarele modalități:
  - transmiterea unei interpelări prin interfața web a sistemului Service Desk: https://helpdesk.pride.md
  - expedierea unui e-mail la adresa: support@pride.md;
  - efectuarea unui apel telefonic la numărul de telefon: +373 22 **844-266**. Modalitatea de contactare a *SSC* este selectată de *Beneficiar*, precum este stabilit în aceste *Reguli*. *Prestatorul* poate solicita *Beneficiarului* să utilizeze altă modalitate de contactare a *SSC*, în cazul în care acest fapt corespunde *Regulilor*. Programul de lucru al *SSC* este de la 9:00 pînă la 18:00, în zilele de lucru, conform legislației Republicii Moldova. Toate interpelările *Beneficiarului* vor fi înregistrate în Sistemul Service Desk. *Beneficiarul* va avea acces la informația relevantă pentru el din Sistemul Service Desk, inclusiv: solicitări de servicii, solicitări de informație, incidente înregistrate, rapoarte privind nivelul *Serviciilor*. *Beneficiarul* va accesa Sistemul Service Desk prin intermediul persoanelor responsabile desemnate conform prezentelor *Reguli*.

Implementarea şi prestarea Serviciilor

Reviziile periodice care necesită stoparea activității totale sau parțiale ale *Beneficiarului*, se vor efectua in baza unei programări preventive, care va fi adusă la cunoștința *Beneficiarului*, nu mai târziu de trei zile până la executarea acesteia.

În procesul furnizării *Serviciilor*, *Prestatorul*:

1. asigură livrarea *Serviciilor* în conformitate cu nivelul de *Servicii* stabilit şi agreat împreună cu beneficiarul;
2. elaborează, aprobă şi revizuiește:
   a. procedurile necesare administrării *sistemului informatic* aflat in gestiune;
   b. procedurile de evaluare a eficienței operării şi administrării *sistemului informatic* aflat in gestiune;
   c. procedurile de gestionare a riscurilor;
   d. procedurile de asigurare a securității *sistemului informatic* aflat in gestiune;
3. oferă suport metodologic *Beneficiarilor* în procesul de migrare a sistemelor informaționale şi/sau a datelor;
4. monitorizează utilizarea/disponibilitatea, evaluează capacitatea şi asigură buna funcționarea efectivă a *sistemului informatic* aflat in gestiune;

5. asigură controlul operării eficiente a *sistemului informatic* aflat in gestiune;
6. definește şi monitorizează indicatorii de performanță ai *Serviciilor* livrate;
7. asigură, în caz de necesitate, suportul tehnic *Beneficiarului*.

Accesarea *conturilor*

Accesarea conturilor se face în scop administrativ (acces administrativ) sau în scop de utilizare (acces utilizator). Accesul administrativ este destinat *Prestatorului* pentru gestionarea *sistemului informatic* (instalarea şi menținerea softului de sistem şi aplicativ). Accesul utilizator este destinat utilizării de către *Beneficiar* a *sistemului informatic* externalizat *Prestatorului*.

Regulile de accesare a conturilor la acordarea accesului sunt:

- accesarea *sistemului informatic* în scop administrativ se efectuează exclusiv din rețeaua *Prestatorului* sau a terților cărora *Beneficiarul* le-a dat acest drept;
- protocoalele utilizate pentru accesul administrativ trebuie să fie strict securizate, pentru a asigura confidențialitatea datelor transmise;
- accesul utilizator poate fi efectuat din rețeaua corporativă a *Beneficiarului* sau/şi din rețeaua publică Internet.

Beneficiarul poate modifica oricând regulile de acces utilizator pe *sistemele informatice* ale sale sau pe cele închiriate. În caz de necesitate, *Beneficiarul* poate solicita de la *Prestator* să facă modificări în regulile de acces la nivelul *Serviciilor* care sunt în gestiunea *Prestatorului*, plasând solicitările respective către *SSC* ale *Prestatorului* conform procedurilor descrise prezentele *Reguli*. *Prestatorul* va examina solicitările *Beneficiarului* şi, în caz de necesitate, îl va consulta în privința securității acceselor solicitate. În cazul în care accesele solicitate implică riscuri de securitate inacceptabile, *Prestatorul* poate respinge solicitările *Beneficiarului*. Altfel, *Prestatorul* va acorda accesele solicitate în maximum 48 ore lucrătoare. *Beneficiarul* este responsabilul exclusiv pentru accesele solicitate şi de modul în care va utiliza aceste accese.

Utilizarea Serviciilor

Beneficiarul decide în ce scop şi cum vor fi utilizate *Serviciile* livrate de *Prestator*. În acest sens, *Beneficiarul*:

1. coordonează, în comun acord cu *Prestatorul*, planul de optimizare/securizare a *sistemelor informaționale* şi/sau a datelor;
2. evaluează, în comun acord cu *Prestatorul* necesitățile proprii *Servicii*;
3. utilizează *sistemul informatic* în conformitate cu legislația în vigoare, inclusiv privind securitatea informației şi protecția datelor cu caracter personal;

În procesul utilizării *Serviciilor*, *Beneficiarul* trebuie să respecte următoarele reguli:

1. *Serviciile* vor fi utilizate în scopuri ce corespund legislației în vigoare;
2. *Serviciile* vor fi utilizate exclusiv în scopuri ce rezultă din necesitățile de activitate ale *Beneficiarului*;

3. *Serviciile* vor fi utilizate într-o manieră responsabilă şi securizată. *Beneficiarul* se va asigura că conștientizează riscurile de securitate aferente modului de utilizare a *Serviciilor* şi că le gestionează adecvat. Această informație poate fi solicitată şi comunicată *Presatorului*;
4. *Serviciile* nu vor fi utilizate în scopuri ce pot periclita imaginea *Beneficiarului* sau a *Prestatorului*;

Gestiunea incidentelor

Clasificarea incidentelor

Orice eveniment neplanificat care a afectat sau ar fi putut afecta disponibilitatea şi indicatorii de performanță ai *Serviciilor* este considerat incident aferent *Serviciilor*. *Prestatorul* şi *Beneficiarul* vor conlucra în vederea prevenirii incidentelor şi soluționării operative a acestora, pentru a minimiza impactul lor asupra *Serviciilor*. La stabilirea priorității în soluționarea unui incident se va ține cont de regulile stabilite în acest capitol.

Orice incident este privit sub două aspecte: nivelul impactului şi gradul de urgență. Nivelul impactului incidentului caracterizează consecințele produse asupra disponibilității şi performanței *Serviciilor*. Gradul de urgență al incidentului indică operativitatea cu care acesta trebuie soluționat, pentru a minimiza impactul lui asupra *Beneficiarului*. Prioritatea de escaladare şi soluționare a unui incident va fi în funcție de impactul şi urgență incidentului. Algoritmul aplicat pentru stabilirea priorității unui incident este prezentat în *tabelele 3-5*.

Tabelul 3. Stabilirea priorităţii de soluţionare a incidentelor

Gradul de urgenţă al incidentului	**Nivelul impactului incidentului**		
	Înalt	**Mediu**	**Redus**
Înalt	Critic	Înalt	Mediu
Mediu	Înalt	Mediu	Redus
Redus	Mediu	Redus	Neglijabil

Tabelul 4. Evaluarea urgenţei incidentului

Gradul de urgenţă	**Descrierea gradului de urgenţă**
Înalt	Un incident este calificat ca având gradul de urgență **Înalt** în unul sau mai multe din următoarele cazuri: • pagubele provocate de incident cresc extrem de rapid; • există activități şi operațiuni absolut necesare pentru afacerea *Beneficiarului* care trebuie efectuate imediat; • reacția imediată poate preveni riscuri legale majore şi de securitate (protecție) a informației.

Mediu	Un incident este calificat ca avînd gradul de urgență **Mediu** în unul sau mai multe din următoarele cazuri: • pagubele provocate de incident cresc considerabil în timp; • există activități şi operațiuni importante pentru afacerea *Beneficiarului* care trebuie să fie efectuate imediat; • reacția operativă poate preveni riscuri legale moderate şi de securitate a informației.
Redus	Un incident este calificat ca având gradul de urgență **Redus** în unul sau mai multe din următoarele cazuri: • pagubele provocate de incident cresc relativ încet în timp; • nu există activități şi operațiuni afectate care trebuie efectuate imediat; • nu există riscuri legale şi de securitate a informației semnificative.

Tabelul 5. Evaluarea impactului incidentului

Nivelul impactului	Descrierea nivelului impactului
Înalt	Un incident este calificat ca avînd nivelul impactului **Înalt** în unul sau mai multe din următoarele cazuri: • activitățile-cheie ale *Beneficiarului* sunt întrerupte; • incidentul este vizibil din exteriorul organizației *Beneficiarului* şi afectează utilizatorii externi, reputația şi imaginea *Beneficiarului*; • există riscuri legale şi financiare majore pentru *Beneficiar*; • s-au produs pierderi semnificative de informație foarte importantă din sistemele *Beneficiarului*.
Mediu	Un incident este calificat ca având nivelul impactului **Mediu** în unul sau mai multe din următoarele cazuri: • activitățile importante ale *Beneficiarului* sunt întrerupte sau activitățile-cheie sunt desfăşurate cu dificultate; • incidentul a afectat o parte din utilizatorii interni şi un număr nesemnificativ de utilizatori externi; • există riscuri legale şi financiare semnificative pentru *Beneficiar*; • s-au produs pierderi nesemnificative de informație din sistemele *Beneficiarului*.

Redus	Un incident este calificat ca având nivelul impactului **Redus** în unul sau mai multe din următoarele cazuri: • activitățile interne nesemnificative ale *Beneficiarului* sunt întrerupte sau activitățile importante se desfășoară cu dificultate; • incidentul a afectat doar o parte din utilizatorii interni ai *Beneficiarului*.

Raportarea şi soluţionarea incidentelor

Orice incident aferent *Serviciilor* este raportat de *Beneficiar* către *SSC* al *Prestatorului*, conform procedurilor stabilite în prezentele *Reguli*. *Prestatorul* va reacționa la incidentele raportate de *Beneficiar* în corespundere cu *Regulile* prezentate în *tabelul 6*. *Regulile* se aplică pentru perioada
programului de lucru al *Prestatorului*. În afara programului de lucru, soluționarea incidentelor se va baza pe principiul „*cel mai bun efort*”.

Tabelul 6. Soluţionarea incidentelor în funcţie de prioritatea lor

Prioritatea incidentului	Timpul de reacţie a Prestatorului	Timpul de soluţionare
Critică	5 minute	cel mult 2 ore
Înaltă	30 min	cel mult 4 ore
Medie	1 oră	cel mult 8 ore
Redusă	2 ore	până la începutul următoarei zile de lucru
Neglijabilă	4 ore	*“Cel mai bun efort”*

La raportarea unui incident, *Beneficiarul* evaluează nivelul impactului incidentului şi gradul de urgență în soluționarea acestuia, aplicând regulile stabilite. Ulterior este determinată prioritatea de soluţionare a incidentului conform regulilor stabilite.
SSC al *Prestatorului* poate contacta persoana care a raportat incidentul, pentru a preciza informația transmisă de *Beneficiar*. De comun acord cu aceasta, *Prestatorul* poate revizui nivelul impactului incidentului şi gradul de urgență în soluționarea lui. *Beneficiarul* are de asemenea posibilitatea ca ulterior să revizuiască clasificarea stabilită inițial. Necesitatea unei astfel de revizuiri este în funcție de promptitudinea şi eficiența soluționării incidentului.
Prestatorul va stabili cauza incidentului şi va identifica măsurile necesare pentru soluționarea lui. Pe parcursul soluționării incidentului, *Prestatorul* va oferi *Beneficiarului* informații cu privire la progresele în acest sens.
Persoanele responsabile ale *Prestatorului* pot solicita implicarea în gestiunea incidentului a persoanelor responsabile ale *Beneficiarului*. Conlucrarea este necesară în vederea diminuării impactului incidentului şi soluționării cât mai operative a acestuia.
Un incident se consideră soluționat atunci când *Serviciile* pentru *Beneficiar* sunt restabilite, la nivelul prevăzut în prezentele *Reguli*. În cazul în care *Beneficiarul* nu este mulțumit de calitatea soluționării incidentului, poate solicita lucrări repetate în vederea soluționării optime a incidentului. În caz contrar, incidentul se consideră rezolvat.
Toate incidentele raportate de *Beneficiar* sunt înregistrate de SSC. *Prestatorul* va utiliza informația privind incidentele produse în scopul îmbunătățirii calității *Serviciilor* şi neadmiterii repetării incidentelor.

Escaladarea incidentelor

În cazul în care un incident nu poate fi soluționat în timpul agreat, *Părţile* pot escalada incidentul la un nivel mai înalt de autoritate. *Părţile* vor stabili de comun acord formarea grupurilor mixte de lucru şi componența nominală a acestora, pentru a interveni în soluționarea operativă a incidentului.

Modificarea Serviciilor

Solicitarea de servicii suplimentare

Beneficiarul poate solicita, la un moment dat, *Servicii* suplimentare faţă de cele utilizate până atunci. În acest scop, *Beneficiarul* va plasa o solicitare de servicii suplimentare prin intermediul SSC al *Prestatorului*. *Presatorul* va examina solicitarea *Beneficiarului* şi, în termen de 8 ore lucrătoare, va confirma sau infirma posibilitatea acordării *Serviciilor* suplimentare. *Prestatorul* poate contacta *Beneficiarul* în vederea obţinerii unor informaţii relevante pentru serviciile solicitate. În cazul în care solicitarea *Beneficiarului* este acceptată, *Serviciile* suplimentare vor fi implementate conform regulilor stabilite.

Raportarea privind nivelul Serviciilor

Prestatorul optează pentru prestarea transparentă a *Serviciilor* către *Beneficiar*. În acest scop, *Prestatorul* va prezenta, cu regularitate, *Beneficiarului* rapoarte privind nivelul *Serviciilor*. Structura şi conţinutul acestor rapoarte sînt stabilite de *Prestator*. *Beneficiarul* poate formula propuneri cu referire la conţinutul rapoartelor de monitorizare a *Serviciilor* utilizate. Tipurile de rapoarte, conţinutul, destinaţia şi periodicitatea acestora sînt reflectate în *tabelul 7*.

Tabelul 7. Tipurile de rapoarte privind nivelul Serviciilor

Tipul raportului	Conţinutul	Destinaţia	Periodicitatea
Raport privind nivelul Serviciilor	Nivelul de disponibilitate a Serviciilor, întreruperile planificate, incidentele raportate, solicitările de suport	Raportul este prezentat în scopul asigurării transparenţei privind prestarea *Serviciilor* la nivelul agreat de *Prestator*	Trimestrial, în formă electronică. La solicitarea *Beneficiarului*, pe suport de hîrtie
Raport privind solicitările de modificare	Propunerile de modificare a Serviciilor	Raportul este prezentat în scopul asigurării transparenţei dezvoltării Serviciilor	Trimestrial, în formă electronică. La solicitarea *Beneficiarului*, pe suport de hîrtie

Suspendarea prestării Serviciilor

Prestarea *Serviciilor* poate fi suspendată temporar la solicitarea *Beneficiarului*, care adresează în acest sens o cerere oficială către *Prestator*. *Serviciile* pot fi suspendate de către *Prestator* din oficiu, cu notificarea prealabilă a *Beneficiarului*:

1. în caz de incidente de proporţii sau situaţii de criză, în scopul remedierii situaţiei şi repunerii sistemului în funcţiune;

2. în cazul în care continuarea prestării *Serviciilor* implică riscuri semnificative de securitate pentru resursele informaţionale de importanţă publică;
3. în cazul în care *Beneficiarul* nu-şi îndeplineşte obligaţiile sale

Comunicare şi reclamaţii

Comunicarea între *Părţi* este de preferat să se realizeze prin intermediul Sistemului Service Desk oferit de *Prestator*. *Beneficiarul* poate însă, la latitudinea sa, să contacteze prin email sau telefon Managerul Clienţi responsabil de interacţiunea cu *Beneficiarul*. De asemenea, el poate decide expedierea scrisorilor oficiale în adresa conducerii *Prestatorului*. Mesajele şi scrisorile expediate pot conţine: propuneri de îmbunătăţire a *Serviciilor*, propuneri de optimizare a comunicării între *Părţi*, reclamaţii privind nivelul *Serviciilor*, solicitări de informaţie etc.

Prestatorul poate, la rîndul său, să se adreseze către *Beneficiar* cu informaţii şi solicitări. Acestea pot fi adresate persoanelor responsabile ale *Beneficiarului* sau conducerii *Beneficiarului*. *Prestatorul* este în drept să solicite opinia şi feedback-ul *Beneficiarului* cu privire la *Serviciile* utilizate de *Beneficiar*. Această informaţie este solicitată în scopul îmbunătăţirii calităţii *Serviciilor* şi experienței *Beneficiarului* în utilizarea *Serviciilor*.

Complianța cu cerințele tehnice

Complianța cu cerințele funcționale ale facilităților de explorare a interfeței publice a SIA RSISC

ID	Obligativitate	Descrierea cerinței funcționale	Compliant
CF01.01.	M	Interfața Publică a SIA RSISC va furniza mecanism de navigare în categoriile de structură în scopul găsirii rapide a informației relevante.	Da
CF01.02.	M	Navigarea se va efectua prin intermediul meniului principal de navigare și interfața utilizator a Paginii Principale.	Da
CF01.03.	M	La accesarea mecanismului de navigare în categoriilor de structură, Interfața Publică a SIA RSISC tip va furniza un mecanism de navigare similar după principiile de utilizare unui director de căutare (unde arborele de structură corespunde structurii Paginii WEB).	Da
CF01.04.	M	Documentele de conținut vor fi amplasate în categoriile frunză ale arborelui de structură a Interfeței Publice a SIA RSISC.	Da
CF01.05.	M	Interfața Publică a SIA RSISC va afișa referințe de nivel pentru a arăta nivelul ierarhic compartimentului curent al Interfeței Publice.	Da
CF01.06.	M	Referințele de structură vor avea referințe hipertext care vor permite navigarea spre nivelele ierarhice superioare categoriei curente.	Da
CF01.07.	M	Interfața Publică a SIA RSISC trebuie să furnizeze mecanism de generare a conținutului textual în format A4 (optimizat pentru imprimare) și descărcare a documentelor plasate în conținut.	Da

CF01.08.	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 editoarelor WYSIWYG); • 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 Stat al Actelor Juridice (https://www.legis.md); • informație multimedia încărcată nemijlocit în SIA RSISC sau publicată prin intermediul resurselor externe (exemplu: Youtube, Rețele de socializare etc.).	Da
CF01.09.	M	Interfața publică a SIA RSISC va asigura acces la KPI și rapoarte statistice cu caracter public generate în baza datelor produse în cadrul fluxurilor de lucru aferente SIA RSISC.	Da
CF01.10.	M	Interfața Publică a SIA RSISC va furniza facilități de partajare a conținutului pe cele mai populare rețele de socializare (Facebook, Twitter, LinkedIn etc.).	Da
CF01.11.	M	Interfața public va furniza mecanism de feedback și contact prin intermediul cărora Internauții vor putea interacționa cu responsabilii din cadrul Centrului pentru Securitatea Cibernetică.	Da
CF01.11.	M	Toată informația statistică de interacțiune a Utilizatorilor Internet cu interfața publică a SIA RSISC va fi colectată prin intermediul API-ului expus de Google Analytics (Furnizorul va efectua toate activitățile de integrare a SIA RSISC cu Google Analytics).	Da
CF02.01.	M	SIA RSISC va livra utilizatorilor autorizați o soluție Dashboard prin intermediul căreia vor fi notificați asupra evenimentelor de business importante și accesa rapid detaliile acestora.	Da

CF02.02.	M	Pot fi enumerate următoarele categorii de evenimentele de business afișate în cadrul Dashboard-ului: • notificări de sistem; • notificări privind alertele de securitate cibernetică ce urmează a fi examinate; • notificări privind incidentele de securitate cibernetică ce urmează 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 așteaptă aprobare de la rolurile decidente (inclusiv alerte de întârziere); • notificări privind completarea fișei incidentului de securitate cibernetică cu noi documente sau formulare electronice; notificări privind evenimentele de trasabilitate a alertelor și incidentelor de securitate cibernetică; alte evenimente relevante.	Da
CF02.03.	M	Dashboard-ul utilizatorului SIA RSISC va afișa doar evenimente de business relevante rolurilor și drepturilor asignate utilizatorului autorizat.	Da
CF02.04.	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 utilizatorilor SIA RSISC și notificările dedicate exclusiv utilizator cu rol de Administrator de Sistem).	Da
CF02.05.	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.	Da
CF02.06.	M	SIA RSISC va afișa înregistrări detaliate ale Dashboard-ului în ferestre sau 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 fi procesate).	Da
CF02.07.	M	La accesarea referinței hipertext aferentă valorii agregate sau înregistrării detaliate a Dashboard-ului SIA RSISC va asigura accesul la informația de detaliu aferentă acestora sau funcționalitatea solicitată	Da

		(exemplu: formularul de evaluare a incidentului, formularul de escaladare a incidentului, formularul de introducere a rezultatelor soluționare incident etc.).	
CF02.08.	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 de securitate cibernetică perfectate curent); formulare electronice examinate spre aprobare.	Da
CF02.09.	D	SIA RSISC va oferi fiecărui utilizator autorizat funcționalitate de configurare individuală a aspectului și conținutului Dashboard-ului.	-
CF03.01.	M	SIA RSISC va furniza mecanism complex de căutare a datelor în întreg conținutul bazei de date.	Da
CF03.02.	M	SIA RSISC va furniza mecanism de căutare indexată a datelor utilizând Elastic Search.	Da
CF03.03.	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.	Da
CF03.04.	M	SIA RSISC va furniza un mecanism flexibil și performant de definire a criteriilor de căutare.	Da
CF03.05.	M	În calitate de criterii de căutare vor putea fi folosite: □ date aferente sistemului informatic sursă a alertei sau a incidentului de securitate cibernetică; • date de identificare a autorităților publice posesoare de sisteme informatice; • date aferente utilizatorilor autorizați care au procesat înregistrările bazei de date;	Da

		• date aferente sistemului de metadate specific alertelor sau incidentelor de securitate cibernetică; • date de detaliu a cazurilor de gestiune a incidentelor de securitate cibernetică; • date de detaliu ale alertelor raportate; • date de detaliu ale incidentelor raportate; • statutul înregistrărilor; alte categorii de date specifice.	
CF03.06.	M	În cazul formulări unor criterii de căutare prea largi, sau care necesită prea mult timp și resurse pentru execuție SIA RSISC nu va executa aceste interogări ci va solicita utilizatorului îngustarea domeniului de valori căutate.	Da
CF03.07.	M	Rezultatele căutării vor fi ordonate în funcție de relevanța rezultatului interogării de căutare, alfabetic sau dată creare/ultimă actualizare.	Da
CF03.08.	M	Utilizatorul va putea defini criterii de ordonare și grupare a conținutului listei cu rezultatele procesului de căutare.	Da
CF03.09.	M	SIA RSISC va oferi mecanism de paginare a rezultatelor căutării destinat evitării supraîncărcării exploratorului WEB și canalelor de transport date.	Da
CF03.10.	D	Înregistrările rezultatelor căutării vor fi marcate (culoare sau iconiță specifică) în funcție de natura sau statutul obiectului informațional găsit.	-
CF03.11.	M	SIA RSISC va furniza funcționalitate de afinare a căutării în rezultatele găsite.	Da
CF03.12.	M	• 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 documentului aferent evenimentului de business; • pentru alertele/incidentele de securitate raportate:	Da

		deschiderea cazului de gestiune a incidentului de securitate, schimbare statut al formularului alertei/incidentului raportat etc.	
CF03.13.	M	SIA RSISC va afișa în rezultatele căutării doar datele ce corespund domeniul de competență a utilizatorului autorizat, rolurilor și drepturile definite în profilul de utilizator autorizat al SIA RSISC.	Da
CF03.14.	M	SIA RSISC va restricționa accesul la detaliile rezultatelor găsite în cazul când utilizatorul care a declanșat procesul de căutare nu dispune de drepturi de acces la obiectele informaționale solicitate a fi accesate.	Da
CF03.15.	M	SIA RSISC va permite exportarea tabelului cu rezultatele căutării în format CSV sau PDF.	Da
CF04.01.	M	SIA RSISC va furniza utilizatorilor autorizați funcționalitate destinată Raportării alertelor și/sau incidentelor de securitate cibernetică.	Da
CF04.02.	M	Utilizatorii autorizați vor putea raporta prin intermediul CU04: • alerte de securitate cibernetică; incidente de securitate cibernetică.	Da
CF04.03.	M	Alertele de securitate cibernetică vor putea fi perfectate fie de utilizatorii autorizați (prin intermediul CU04), fie expediate automat de sisteme informatice externe (prin intermediul CU18).	Da
CF04.04.	M	Alerta și/sau incidentul se raportează conform formularului prezentat în Anexa 2.1.	Da
CF04.05.	D	Formularele de raportare a alertelor și/ sau incidentelor de securitate cibernetică perfectate prin intermediul CU04 vor fi afișate în baza configurațiilor definite prin intermediul CU13.	-
CF04.06.	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.	Da
CF04.07.	M	SIA RSISC va asigura acces utilizatorilor autorizați la lista de formulare de raportare a problemelor de securitate în funcție de rolurile deținute de aceștia și împuternicirilor furnizate de MPower.	Da
CF04.06.	M	Perfectarea formularului electronic destinat raportării - alertelor și/ sau incidentelor de securitate cibernetică se efectuează doar prin intermediul unor mecanisme exclusiv vizuale.	Da

CF04.07.	M	Formularul electronic destinat raportării - alertelor și/ sau incidentelor de securitate cibernetică va conține constrângeri și restricții de conținut în vederea limitării erorilor mecanice.	Da
CF04.08.	M	SIA RSISC va permite atașarea de fișiere la formularul electronic de raportare a - alertei și/ sau incidentului de securitate cibernetică (documente PDF, CSV, capturi ecran sau fișiere video etc.).	Da
CF04.09.	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.).	Da
CF04.10.	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.	Da
CF04.11.	M	SIA RSISC va asigura un mecanism de trasabilitate (păstrarea istoricului) de examinare a alertei și/sau incidentului de securitate cibernetică raportate.	Da
CF04.12.	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.	Da
CF04.13.	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.	Da
CF04.14.	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.	Da
CF04.1.01	M	SIA RSISC va furniza funcționalitate de raportare a alertelor de securitate cibernetică.	Da
CF04.1.02	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	-
CF04.1.03	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.	Da
CF04.1.04	M	Formularul alertei de securitate cibernetică poate avea mai multe stări	Da

		(statute) și tranziții, în funcție de configurările definite prin intermediul CU13.	
CF04.1.04	M	Conținutul unui formular al alertei de securitate cibernetică poate fi modificat doar în statutul de proiect (până la semnarea electronică a acestuia).	Da
CF04.1.06	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.	Da
CF04.1.07	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..	Da
CF04.1.08	M	În calitate de mecanism de notificare externă va fi utilizat serviciul guvernamental MNotify.	Da
CF04.2.01	M	SIA RSISC va furniza funcționalitate de raportare a incidentelor de securitate cibernetică.	Da
CF04.2.02	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.	-
CF04.2.03	M	Formularul incidentului de securitate cibernetică poate avea mai multe stări (statute) și tranziții, în funcție de configurările definite prin intermediul CU13.	Da
CF04.2.04	M	Conținutul unui formular al incidentului de securitate cibernetică poate fi modificat doar în statutul de proiect (până la semnarea electronică a acestuia).	Da
CF04.2.04	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.	Da
CF04.2.06	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.	Da
CF04.2.07	M	În calitate de mecanism de notificare externă va fi utilizat serviciul guvernamental MNotify.	Da
CF04.2.08	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.	Da

CF05.01.	M	SIA RSISC trebuie să fie în măsură să ofere un număr de documente, rapoarte statistice și ad-hoc, astfel încât să acopere toate necesitățile proceselor de business destinate asigurării securității informației și escaladare a incidentelor de securitate cibernetică (după caz).	Da
CF05.02.	D	Este binevenit ca la baza generării rapoartelor să stea o platformă dedicată destinată configurării generării dinamice a rapoartelor (exemplu: JasperReport).	-
CF05.03.	M	SIA RSISC trebuie să pună la dispoziția utilizatorilor un număr predefinit de documente/rapoarte configurabile și la necesitate să asigure producerea la necesitate a rapoartelor ad-hoc.	Da
CF05.04.	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 cum urmează: • Raportare alertă de securitate cibernetică; • Raportare incident de securitate cibernetică; • Raport de evaluare a alertei de securitate cibernetică raportate; • Raport de analiză a incidentului de securitate cibernetică raportat; • Raport de evaluare a incidentului de securitate cibernetică; • Raport privind escaladarea și comunicarea incidentului de securitate cibernetică; • Raport privind rezultatul soluționării incidentului de securitate cibernetică; • Raport privind cauzele incidentului de securitate cibernetică; • Raport de analiză follow-up; • Recipisă de recepționare a formularului de raportare a alertei și/sau incidentului de securitate cibernetică; • Notificare de sistem;	Da
CF05.05.	M	SIA RSISC va dispune de șabloane predefinite (redactabile) pentru fiecare tip de document generat necesar actualizării eventuale a regulilor de generare.	Da
CF05.06.	M	Furnizorul va implementa până la 20 documente ce urmează a fi generate de SIA RSISC, inclusiv cele expuse în CF05.04. Lista completă a documentelor urmează a fi identificată pe parcursul analizei de business.	Da

CF05.07.	M	SIA RSISC va oferi un set de rapoarte ce urmează a fi generate în baza datelor 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 conține date 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 a datelor 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 filtrare posibile); • Liste de alerte conform tuturor modalităților de filtrare posibile); • Indicatori de performanță;	Da
CF05.08.	M	SIA RSISC va dispune de mecanism de definire a setului de rapoarte și date disponibile fiecărei categorii de utilizator, în funcție de rolurile și drepturile deținute.	Da
CF05.09.	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).	Da
CF05.10.	M	Implicit, documentele și rapoartele vor fi extrase în format PDF.	Da
CF05.11.	M	Furnizorul va implementa până la 20 categorii de rapoarte predefinite solicitate de beneficiar inclusiv cele specificate în CF05.07.	Da
CF05.12.	M	SIA RSISC va jurnaliza toate evenimentele de generare și imprimare a documentelor și rapoartelor statistice.	Da

CF06.01.	M	SIA RSISC va notifica automat orice utilizator autorizat în cazul înregistrării unui eveniment de business ce implică acțiunea utilizatorului sau care modifică statutul proceselor gestionate, monitorizate de acesta sau care-l vizează.	Da
CF06.02.	M	Utilizatorii autorizați vor recepționa notificări în Dashboard-ul personal.	Da
CF06.03.	M	O copie a notificării va fi expediată la adresa E-mail indicată în profilul utilizatorului autorizat din SIA RSISC.	Da
CF06.04.	M	Utilizatorul autorizat SIA RSISC va dispune de funcționalitate de configurare a preferințelor de recepționare a notificărilor (la adresa Email sau Dashboard).	Da
CF06.05.	M	SIA RSISC va expedia tot spectrul de notificări destinate utilizatorilor autorizați: • notificare cu privire la recepționarea unei alerte de securitate cibernetică raportate; • notificare cu privire la recepționarea unui incident de securitate cibernetică raportat; • notificare cu privire la deschiderea/actualizarea/închiderea cazurilor de gestiune a incidentelor de securitate cibernetică; • notificare cu privire la necesitatea implicării pe fluxurile de lucru a SIA RSISC; • notificare cu privire la întârzierea acțiunii utilizatorului (depășirea termenului limită de aprobare/respingere proiect de formular, perfectare formular aferent gestiunii incidentului de 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;	Da
CF06.06.	M	O notificare expediată stocată în Dashboard-ul utilizatorului autorizat va conține referință hipertext pentru a deschide formularul electronic relevat notificării.	Da
CF06.08.	M	Utilizatorii SIA RSISC vor recepționa notificărilor prin E-mail în format HTML sau Format Text îmbogățit.	Da
CF06.09.	M	Notificările externe (citite prin intermediul mijloacelor externe, în afara interfeței utilizator a SIA RSISC) vor fi	Da

		expediate prin intermediul serviciului de platformă MNotify.	
CF07.01.	M	SIA RSISC va furniza mecanism de procesare a alertelor de securitate cibernetică recepționate și înregistrate.	Da
CF07.02.	M	Alertele de securitate cibernetică vor parveni prin intermediul a 2 canale: expediate automat de către sistemele informatice; raportate de utilizatorii autorizați.	Da
CF07.03.	M	Procesarea alertei de securitate cibernetică presupune efectuarea următoarelor acțiuni puse la dispoziție de SIA RSISC: • analiza problemei; • perfectarea unui raport de analiză a alertei de securitate cibernetică; • schimbare statut alertă de securitate cibernetică (închiderea alertei în cazul în care se consideră ignorabilă); • asocierea alertei de securitate cibernetică unui incident de securitate cibernetică raportat.	Da
CF07.04.	M	Pentru alertele raportate de utilizatori autorizați (perfectate prin intermediul CU04.1) trebuie să fie completat un raport de analiză și răspuns la alertă (chiar dacă specialistul în securitatea informației nu depistează un careva pericol generat de alertă de securitate raportată).	Da
CF07.05.	M	Pentru alertele raportate de sistemele informatice nu este obligatorie completarea unui raport de analiză și răspuns la alertă. Pentru acestea este suficientă doar schimbarea statutului în cazul când specialistul de securitate nu atestă un pericol.	Da
CF07.06.	M	SIA RSISC va furniza funcționalitate de schimbare simultană a statutelor mai multor alerte de securitate raportate (valabil pentru alertele raportate automat de sistemele informatice).	Da
CF07.07.	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.	Da
CF07.08.	M	SIA RSISC va jurnaliza toate evenimentele de procesare a alertelor de securitate cibernetică raportate (inclusiv alternativ prin intermediul serviciului guvernamental MLog).	Da

CF08.01.	M	SIA RSISC va furniza funcționalitate destinată gestiunii cazurilor de gestiune a incidentelor de securitate cibernetică.	Da
CF08.02.	M	Gestiunea unui caz de gestiune a incidentului de securitate cibernetică presupune efectuarea următoarelor acțiuni: • deschidere/închidere/redeschidere caz de gestiune a incidentului de securitate cibernetică; • evaluarea incidentului de securitate cibernetică; • escaladarea incidentului de securitate cibernetică; • soluționarea incidentului de securitate cibernetică; investigarea cauzei producerii incidentului de securitate cibernetică.	Da
CF08.03.	M	SIA RSISC va permite, completarea electronică a conținutului fișei incidentului de securitate cibernetică de către Registrator precum și introducerea retroactivă a detaliilor incidentului de securitate cibernetică (cazul când reportatorul dispune de soft destinat documentării incidentului de securitate cibernetică și datele parvin automat prin intermediul CU18).	Da
CF08.04.	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 de securitate similare).	Da
CF08.05.	M	Formularele electronice de completare a fișei incidentului de securitate cibernetică vor fi afișate și validate în baza configurațiilor definite prin intermediul CU13.	Da
CF08.06.	M	Stările și tranzițiile prin care poate trece formularul electronic destinat documentării cazului de gestiune a incidentului de securitate cibernetică sunt configurate prin intermediul cazului de utilizare CU13.	Da
CF08.07.	M	Orice formular electronic destinat documentării procesului de gestiune a incidentului de securitate cibernetică va avea asociat un șablon de document care va fi configurat prin intermediul CU13 și extras prin intermediul CU05 în baza datelor conținute în formular.	Da
CF08.08.	M	Formularul electronic destinat documentării cazului de gestiune a incidentului de securitate cibernetică poate	Da

		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) sau din lista rezultatelor furnizate de CU03 (exemplu: inițierea cazului de gestiune a incidentului de securitate cibernetică în baza unor alerte sau incidente de securitate cibernetică anterior raportate).	
CF08.09.	M	SIA RSISC va asigura acces utilizatorilor autorizați la lista de formulare electronice destinate documentării cazului de gestiune a incidentului de securitate cibernetică în funcție de rolurile deținute de aceștia și împuternicirilor furnizate de MPower.	Da
CF08.10.	M	Perfectarea formularului electronic destinat documentării cazului de gestiune a incidentului de securitate cibernetică se efectuează doar prin intermediul unor mecanisme exclusiv vizuale.	Da
CF08.11.	M	Formularul electronic destinat documentării cazului de gestiune a incidentului de securitate cibernetică va conține constrângeri și restricții de conținut în vederea limitării erorilor mecanice.	Da
CF08.12.	M	SIA RSISC va dispune de capacități de calculare a unor valori agregate în baza datelor primare conținute (exemplu: totaluri, subtotaluri, cuantificări, calculare a unor indicatori generalizatori etc.)	Da
CF08.13.	M	SIA RSISC va permite atașarea de copii electronice a documentelor relevante la formularul electronic aferent cazului de gestiune a incidentului de securitate cibernetică.	Da
CF08.14.	M	SIA RSISC va furniza mecanism de verificare a plenitudinii sau corectitudinii perfectării formularului electronic de documentare a cazului de gestiune a incidentului de securitate cibernetică (obligativitate conținut date, corectitudine tip date inserate, integritate date introduse etc.).	Da
CF08.15.	M	Doar un formular electronic de documentare a cazului de gestiune a incidentului 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).	Da
CF08.16.	M	SIA RSISC va asigura mecanism de trasabilitate (păstrarea istoricului) la propagarea modificărilor în fișa incidentului de securitate cibernetică (toate evenimentele de adăugare, modificare, suprimare date, precum și vizualizare conținut dosar vor fi accesibile spre vizualizare).	Da

CF08.17.	M	SIA RSISC va furniza Registratorilor funcționalitate de semnare electronică a formularelor electronice de documentare a cazului de gestiune a incidentului de securitate cibernetică (dacă această obligativitate este inclusă configurațiile formularului definite prin intermediul CU12).	Da
CF08.18.	M	În calitate de mecanism de aplicare a semnăturii electronice va fi folosit serviciul guvernamental MSign.	Da
CF08.19.	M	SIA RSISC va jurnaliza toate evenimentele de gestiune a dosarului cazului de utilizare prin intermediul serviciului guvernamental MLog.	Da
CF08.1.01.	M	SIA RSISC va furniza funcționalitate de deschidere a unui caz de gestiune a incidentului de securitate cibernetică în baza: • alertelor de securitate cibernetică raportate prin intermediul CU04.1 • alertelor de securitate cibernetică recepționate prin intermediul CU18; • incidentelor de securitate cibernetică raportate prin intermediul CU04.2; Incidentelor de securitate cibernetică recepționate prin intermediul CU17.	Da
CF08.1.02.	M	Pentru deschiderea cazului de gestiune a evenimentului de securitate cibernetică este necesară: • Identificarea alertei sau incidentului de securitate cibernetică relevant; • completarea metadatelor aferente fișei de securitate cibernetică; • definirea persoanelor responsabile în documentarea și soluționarea incidentului de securitate cibernetică; • atașarea copiilor electronice și metadatelor asociate ale documentelor specifice deschiderii cazului de gestiune a incidentului de securitate cibernetică.	Da
CF08.1.03.	M	Unui dosar ai cazului de gestiune a incidentului de securitate cibernetică îi pot fi atașate mai multe alerte de securitate cibernetică sau incidente de securitate cibernetică raportate.	Da
CF08.1.04.	M	SIA RSISC va efectua o verificare a completitudinii dosarului și corectitudinii datelor introduse anterior deschiderii cazului de gestiune a incidentului de securitate cibernetică.	Da

CF08.1.05.	M	Registratorul va activa un buton specializat pentru deschiderea cazului în cazul când validarea CF08.1.04 a trecut cu succes.	Da
CF08.1.06.	M	Odată deschis cazul, SIA RSISC va notifica toți utilizatorii autorizați cazului și raportatorul/sursa alertei sau incidentului de securitate cibernetică (în cazul existenței adresei E-mail în profilul acestuia) asupra deschiderii unui nou caz de gestiune a incidentului de securitate cibernetică.	Da
CF08.1.07.	M	Un caz de gestiune a incidentului de securitate cibernetică poate trece în statut „Închis” în cazul în care toate procesele de evaluare, documentare și soluționare a incidentului de securitate cibernetică au fost finisate.	Da
CF08.1.08.	M	Registratorul va dispune de funcționalitate de închidere a cazului de gestiune a incidentului de securitate cibernetică (buton specializat pentru schimbarea statutului).	Da
CF08.1.09.	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 cibernetică va putea fi închis.	Da
CF08.1.08.	M	Cazurile de gestiune a incidentelor de securitate cibernetică incomplete sau care au depășit termenul limită de soluționare vor fi închise cu un statut special cu menționea cauzei închiderii cazului.	Da
CF08.1.08.	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 în profilul acestuia).	Da
CF08.1.08.	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.	Da
CF08.2.01.	M	SIA RSISC va furniza formular de documentare a incidentului de securitate cibernetică.	Da
CF08.2.02.	M	Conținutul formularului de documentare a incidentului de securitate cibernetică și fluxul de lucru aferent vor fi configurate prin intermediul CU12.	Da

CF08.2.03.	M	Documentarea unui incident de securitate cibernetică presupune colectarea și introducerea următoarelor categorii de date: • rezultatele analizei preliminare a incidentului de securitate cibernetică; • detaliile evenimentelor adverse (dacă există); • categoria incidentului; • tipul de impact al incidentului; • rezultatul evaluării primare a impactului și a rezultatelor produse de incidentul de securitate cibernetică; • rezultatul evaluării preliminare a urgenței soluționării incidentului de securitate cibernetică; • prioritatea de soluționare a incidentului de securitate cibernetică; • alte categorii de date relevante.	Da
CF08.2.04.	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.).	Da
CF08.2.05.	M	Un formular de documentare a incidentului de securitate cibernetică se consideră finisat în cazul în care este semnat de Registratorul care la completat.	Da
CF08.3.01.	M	SIA RSISC va furniza formular de comunicare și escaladare a incidentului de securitate cibernetică.	Da
CF08.3.02.	M	Conținutul formularului de comunicare și escaladare a incidentului de securitate cibernetică și fluxul de lucru aferent vor fi configurate prin intermediul CU12.	Da
CF08.3.03.	M	Escaladarea și comunicarea unui incident de securitate cibernetică presupune identificarea și introducerea următoarelor categorii de date: • echipa responsabilă de soluționarea incidentului de securitate cibernetică; • personalul responsabil de soluționare a incidentului de securitate cibernetică; • nivelele ierarhice implicate în escaladarea incidentului de securitate cibernetică; • instituțiile externe implicate în escaladarea incidentului de securitate cibernetică.	Da

		• nivelele ierarhice implicate în escaladarea incidentului de securitate cibernetică; • instituțiile externe implicate în escaladarea incidentului de securitate cibernetică.	
CF08.3.04.	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.).	Da
CF08.3.05.	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.	Da
CF08.3.06.	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 CF08.3.03) și va asigura acces la fișa incidentului de securitate cibernetică.	Da
CF08.4.01.	M	SIA RSISC va furniza toate formularele electronice necesare documentării procesului de soluționare a incidentului de securitate cibernetică.	Da
CF08.4.02.	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.	Da
CF08.4.03.	M	Documentarea procesului de soluționare a incidentului informatic presupune perfectarea formularelor electronice destinate documentării următoarelor etape de soluționare a incidentului de securitate cibernetică: • investigarea incidentului de securitate cibernetică; • izolarea resursei informatice afectate de incidentul de securitate cibernetică; • tratarea incidentului de securitate cibernetică; • recuperarea resursei informatice afectate de incidentul de securitate cibernetică; revizuirea și documentarea (inclusiv îmbunătățirea procedurilor existente, formularea recomandărilor, evaluarea eficacității măsurilor întreprinse etc.).	Da

CF08.4.04.	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).	Da
CF08.4.05.	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.	Da
CF08.4.06.	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 CF08.3.03) și va asigura acces la fișa incidentului de securitate cibernetică.	Da
CF08.5.01.	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.	Da
CF08.5.02.	M	Conținutul formularului electronic destinat analizei follow-up a incidentului de securitate cibernetică și fluxul de lucru aferent vor fi configurate prin intermediul CU12.	Da
CF08.5.03.	M	Analiza follow-up a unui incident de securitate cibernetică presupune identificarea și introducerea următoarelor categorii de date (o parte vor 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 a incidentului de securitate cibernetică; date privind indicatorii de performanță a proceselor de soluționare a incidentului de securitate cibernetică.	Da
CF08.5.04.	M	Raportul de analiză follow-up a incidentului de securitate cibernetică se perfectează conform șablonului inclus în anexa A1.3.	Da

CF08.5.05.	M	Formularul raportului de analiză follow-up a incidentului de securitate cibernetică va dispune de posibilitate de atașare a copiilor electronice ale documentelor.	Da
CF08.5.06.	M	Un formular de perfectare a raportului de analiză follow-up a incidentului de securitate cibernetică se consideră finisat în cazul în care este semnat de Registratorul care l-a completat.	Da
CF08.5.07.	M	Un formular de analiză follow-up nu poate fi perfectat dacă fișa incidentului de securitate cibernetică nu este complet (nu au fost finisate etapele definite de CU08.1-CU08.4) și reprezintă constrângerea de bază pentru închiderea unui caz de gestiune a incidentului de securitate cibernetică.	Da
CF09.01.	M	SIA RSISC va furniza actorilor autorizați (cu rol decident) mecanism de aprobare sau respingere a proiectelor de formulare perfectate de utilizatori autorizați (cu rol de Registrator) care necesită aprobare înainte de a fi salvate sau procesate.	Da
CF09.02.	M	Obligativitatea aprobării formularului electronic este configurată prin intermediul CU12 și va cuprinde setul de formulare perfectate prin intermediul CU08.	Da
CF09.03.	M	Lista completă a formularelor electronice care vor necesita aprobări din partea rolurilor decidente vor fi identificate în procesul analizei de business.	Da
CF09.04.	M	Aprobarea sau respingerea constă în perfectarea unei note, alegerea statutului (Aprobat sau Respins), confirmarea acestuia și aplicarea semnăturii electronice a utilizatorului cu rol decident.	Da
CF09.05.	M	Accesul la funcționalitatea de aprobare/respingere a proiectului va fi posibilă numai în cazul în care utilizatorul cu rol Decident dispune de asemenea împuternicire (verificarea se va face prin intermediul MPower).	Da
CF09.06.	M	SIA RSISC va utiliza serviciul de platformă MSign pentru aplicarea semnăturii electronice la Aprobarea/Respingerea formularului electronic.	Da
CF09.07.	M	În cazul aprobării formularului electronic, SIA RSISC va notifica toți utilizatorii relevanți acestuia privind evenimentul de aprobare/respingere.	Da

CF09.08.	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 notifica toți utilizatorii relevanți.	Da
CF09.09.	M	În momentul în care un formular este expediat spre aprobare acesta nu poate fi modificat decât de decidentul care trebuie să-l aprobe cu aplicarea repetată a semnăturii electronice.	Da
CF09.10.	M	SIA RSISC va jurnaliza toate evenimentelor de aprobare/respingere a proiectelor de formulare electronice.	Da
CF 10.01.	M	SIA RSISC va furniza un mecanism de gestiune a interfeței publice destinate accesării de către utilizatori anonimi.	Da
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.	Da
CF 10.03.	M	SIA RSISC va furniza un mecanism de gestiune a structurii conținutului interfeței publice în baza căreia va fi afișat meniul de navigare.	Da
CF 10.04.	I	Structura interfeței publice a SIA RSISC reprezintă un arbore cu nelimitat în nivele ierarhice frunzele căruia conțin informația de conținut.	-
CF 10.05.	M	SIA RSISC va furniza funcționalitate de reorganizare a arborelui de structură a interfeței publice (mutare subcategorie dintr-o categorie în alta, ascundere/ștergere categorii ale arborelui de structură, redenumire a categoriilor arborelui de structură etc.).	Da
CF 10.06.	M	Pentru categoriile de structură a arborelui de structură se va putea defini: • informație de conținut (adăugare/modificare/ștergere informație de conținut);	Da

		• URL de acces la modulele interfeței publice sau accesare a resurselor externe; Subcategorii subordonate.	
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.	Da
CF 10.08.	M	SIA RSISC va furniza un mecanism de gestiune a paginii principale a interfeței publice.	Da
CF 10.09.	I	Pagina principală reprezintă un mecanism de acces rapid la serviciile și facilitățile interfeței publice.	-
CF 10.10.	M	Pentru pagina principală a interfeței publice a SIA RSISC trebuie să existe următoarele facilități de configurare: • definire aspect de prezentare a informației (număr de culoare afișate, compartimente și ordinea lor de afișare pe Pagina Principale); • configurarea blocurilor cu informații extrase din conținutul informațional al interfeței publice; • configurarea zonelor cu bannere de acces la serviciile SIA RSISC, resurse STISC sau externe; • configurarea accesului la serviciile electronice accesibile prin intermediul SIA RSISC; • gestiunea informației plasate în subsolul Paginii Principale și a interfeței publice.	Da
CF 10.11.	M	SIA RSISC va dispune de funcționalitate de configurare a accesului la serviciile electronice oferite prin intermediul interfeței publice.	Da
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.	Da
CF 10.13.	M	Serviciile electronice integrate în interfața publică a SIA RSISC vor putea fie accesate la URL-uri permanente.	Da
CF 10.14.	M	SIA RSISC va dispune de funcționalitate de gestiune a conținutului informațional prin intermediul unor facilități specifice Sistemelor de Gestiune a	Da

		Conținutului care va furniza următoarele funcționalități: • redactarea și publicarea documentelor prin intermediul editoarelor WYSIWYG; • încărcarea de fișiere și imagini în conținutul documentelor publicate 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.	Da
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.	Da
CF 10.17.	M	SIA RSISC va furniza funcționalități de definire și gestiune a structurii bazei de cunoștințe.	Da
CF 10.18.	M	SIA RSISC trebuie să fie capabil să plaseze (și afișeze ulterior în interfața publică) următoarele tipuri de conținut în baza de cunoștințe: (materiale instructiv-metodice) • documente în format HTML (redactate cu ajutorul editoarelor WYSIWYG); • ghiduri/instrucțiuni încărcate în format PDF, DOC/DOCX, PPT/PPTX etc. • referințe la cadrul legal în vigoare conținut în Registrul de Stat al Actelor Juridice (https://www.legis.md); • informație multimedia încărcată nemijlocit în cadrul SIA RSISC sau publicată prin intermediul resurselor externe (exemplu: Youtube, Rețele de socializare etc.); studii de caz, extrase în baza dosarelor cazurilor de gestiune a incidentelor de securitate.	Da

CF 11.01.	M	SIA RSISC va furniza funcționalitate de definire și gestiune dinamică a utilizatorilor, rolurilor și drepturilor de acces a acestora.	Da
CF 11.02.	M	Fiecare utilizator autorizat va dispune de un profil cu următoarele categorii 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, MPass etc.); • cont activ/dezactivat; • perioadă de valabilitate a accesului; • rolurile utilizatorului; drepturi particulare de acces la interfața utilizator și date;	Da
CF 11.03.	M	SIA RSISC va conține o categorie implicită de utilizatori creată de Furnizor și credențiale pentru acesta sunt remise la livrare pentru categoria de super administrator.	Da
CF 11.04.	M	SIA RSISC trebuie să asigure accesul la unele funcționalități specifice doar 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;	Da
CF 11.05.	M	Gestionarea utilizatorilor precum si a rolurilor atribuite in sistem se va efectua prin intermediul MPass.	Da
CF 11.06.	M	SIA RSISC va furniza mecanism de definire pentru utilizatori a drepturilor de acces la date în funcție categoriile sau tipurile de alerte/incidente, arealul geografic, categorii specific de date etc. ținându-se cont de atribuțiile de serviciu a utilizatorul autorizat.	Da
CF 11.07.	M	SIA RSISC va furniza utilizatorilor autorizați funcționalități de modificare și restabilire a parolei de acces.	Da

CF 11.08.	M	SAI SPM va asigura protecție parolelor utilizatorilor autorizați. Metoda de protecție utilizată trebuie să asigure imposibilitatea interceptării, deducerii și recuperare a parolei de acces.	Da
CF 11.09.	M	SIA RSISC va permite blocarea/deblocarea accesului utilizatorului.	Da
CF 11.10.	M	Comunicarea între dispozitivul utilizatorului și serverul aplicație a SIA RSISC trebuie să fie criptată (utilizând protocolul SSL/TLS).	Da
CF 11.11.	M	SIA RSISC trebuie să fie capabil să configureze numărul de sesiuni paralele posibile de a fi inițiate de același utilizator.	Da
CF 11.12.	M	SIA RSISC trebuie să fie capabil să configureze perioada de inactivitate a utilizatorului după care sesiunea urmează a fi închisă în mod automat.	Da
CF 11.13.	M	SIA RSISC trebuie să prevină orice posibilitate de preluare neautorizată a sesiunilor active inițiate de utilizatorii autorizați	Da
CF 11.14.	M	SIA RSISC va permite blocarea sesiunii la cererea utilizatorului sau automat la expirarea sesiunii utilizatorului.	Da
CF 11.15.	M	Un Profil de utilizator autorizat poate fi eliminat fizic doar în cazul când nu există evenimente jurnalizate sau înregistrări aferente acestuia.	Da
CF 11.16.	M	SIA RSISC trebuie să furnizeze un mecanism de gestiune granulară a drepturilor de acces la obiectele sale și a acțiunilor posibile asupra acestora (alerte de securitate cibernetică raportate, incidente de securitate cibernetică raportate, cazuri de gestiune a incidentelor de securitate cibernetică , formulare electronice, meniuri, funcționalități, rapoarte, acțiuni de adăugare/vizualizare/actualizare/ștergere date etc.).	Da
CF 11.17.	M	Metoda de autorizare a utilizatorilor SIA RSISC trebuie să se bazeze pe principiul „*tot ce nu este permis este interzis*”.	Da
CF 11.18.	M	SIA RSISC va furniza funcționalitate de definire a grupurilor și rolurilor utilizatorilor și facilități de asociere a utilizatorilor la grupuri și roluri.	Da
CF 11.19.	M	Un rol este definit prin denumire generică, descriere succintă și statutul de activ/dezactivat. Rolurile	Da

		dezactivate nu vor fi afișate la configurarea drepturilor de acces la resursele aplicației sau a drepturile utilizatorilor.	
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 modalității de acces a acestora).	Da
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 cu unul sau mai multe grupuri și roluri, iar drepturile de acces ale utilizatorului sunt determinate cumulativ.	Da
CF 11.22.	M	SIA RSISC trebuie să permită acordarea drepturilor de acces în baza regulilor 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 sau context*).	Da
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.	Da
CF 11.24.	M	SIA RSISC va furniza mecanism de înregistrare a componentelor interfeței utilizator (resurselor) în scopul asigurării unui mecanism de definire 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 a căreia este suficientă pentru configurarea drepturilor de acces, tranzițiilor fluxurilor de lucru și acțiunilor accesibile utilizatorilor.	Da
CF 11.25.	M	SIA RSISC va permite configurarea ierarhiei componentelor interfeței utilizator, la nivelul rădăcină fiind modulele de bază ale aplicației iar nivelele subordonate nu vor fi limitate în adâncime, ierarhia fiind determinată de arhitectura acestora.	Da
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)	Da

		rolurile care au acces la componenta interfeței utilizator sau acțiunile ce pot fi întreprinse.	
CF 11.27.	M	Orice componentă a interfeței utilizator SIA RSISC va conține date privind, statutele prin care pot trece datele gestionate prin intermediul componentei, tranzițiile de parcurgere a statutelor componentei (configurare fluxuri de lucru).	Da
CF 11.28.	M	SIA RSISC va permite definirea permisiunilor aferente acțiunilor (evenimentelor de business) disponibile utilizatorilor cu acces la componentele interfeței utilizator. Vor fi configurate următoarele categorii de acțiuni disponibile utilizatorilor: • vizualizare înregistrări; • adăugare înregistrări; • modificare înregistrări; • eliminarea înregistrări; • tranziție flux de lucru; alte acțiuni relevante.	Da
CF 11.29.	M	SIA RSISC trebui să permită atribuirea temporară a drepturilor deținute de un utilizator către alt utilizator. Această atribuire trebuie făcută 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.	Da
CF 11.30.	D	SIA RSISC trebuie să permită separarea activităților administrative (*exemplu: Administratorul 1 face modificările și Administratorul 2 le confirmă*).	-
CF 11.31.	M	SIA RSISC trebuie să furnizeze facilități pentru vizualizare și generarea de 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.	Da
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 cibernetică și a cazurilor de gestiune a incidentelor de securitate cibernetică.	Da

CF 12.02.	M	Gestiunea fluxurilor de lucru trebuie să se poată realiza folosind interfața grafică a sistemului informatic în care utilizatorul lucrează în mod obișnuit.	Da
CF 12.03.	M	Fluxurile de lucru vor fi definite prin specificarea stărilor în care poate trece 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.	Da
CF 12.04.	M	Un flux de lucru va fi implementat ca o colecție de activități prin care trece un formular electronic perfectat în cadrul proceselor de business ce se desfășoară secvențial.	Da
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.	Da
CF 12.06.	D	Un flux de lucru trebuie să poată avea asociat un coordonator (supervizor). Coordonatorul trebuie să poată primi mesajele de avertizare (notificări) generate de rularea fluxului respectiv. Utilizatorul care lansează un formular spre procesare pe un flux de lucru trebuie să poată specifica cine este supervizorul fluxului.	
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.	Da
CF 12.08.	M	SIA RSISC va oferi un mecanism de configurare a formularelor electronice utilizate în interfața utilizator destinată raportării alertelor de securitate cibernetică și cazurile e gestiune a incidentelor de securitate.	Da
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 modificarea aspectului și conținutului documentului extras).	Da
CF 12.10.	D	Este binevenit ca șabloanele de documente și rapoarte să fie configurate prin intermediul unei platforme de	

		configurare și generare a rapoartelor (*Exemplu: JasperReports*,	
CF 12.11.	M	Toate șabloanele de documente și rapoarte configurate prin intermediul CF 12.09 – CF 12.10 vor fi utilizate la generarea rapoartelor/documentelor prin intermediul CU05 și CU15.	Da
CF 12.12.	M	Dezvoltatorul va configura la cererea Beneficiarului până la 20 șabloane de documente și 20 șabloane de rapoarte ce urmează a fi generate de SIA RSISC.	Da
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 a alertelor de securitate cibernetică și a gestiunii incidentelor de securitate cibernetică.	Da
CF 13.02.	M	Următoarele categorii de metadate urmează a fi utilizate în cadrul SIA RSISC: • **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** (valorile cărora 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, metadate de 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.).	Da
CF 13.03.	M	Furnizorul trebuie să implementeze mecanism destinat actualizării automate a metadatelor (dacă acestea există) necesare implementării schimbului de date cu sisteme informatice externe.	Da
CF 13.04.	M	SIA RSISC va furniza mecanism de export și import a clasificatoarelor din interfața utilizator în format XML	Da

		sau CSV. Drepturile de import și export vor fi atribuite utilizatorilor cu rolul de Administrator de Sistem.	
CF 13.05.	M	Pentru clasificatoarele oficiale, internaționale și cele furnizate de sistemele informatice externe cu care efectuează schimbul reciproc de date vor fi limitate drepturile de modificare a valorilor prin intermediul facilităților SIA RSISC.	Da
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).	Da
CF 13.07.	M	SIA RSISC va furniza funcționalitate de gestiune a valorilor textuale a clasificatoarelor/nomenclatoarelor altor categorii de metadate în 3 versiuni lingvistice: Română, Engleză și Rusă.	Da
CF 13.08.	M	SIA RSISC va furniza funcționalitate de gestiune a etichetelor și mesajelor interfeței utilizator în 3 versiuni lingvistice: Română, Engleză și Rusă.	Da
CF 13.09.	M	SIA RSISC nu va permite eliminare unei categorii de metadate dacă aceasta este utilizată cel puțin într-o înregistrare a bazei de date.	Da
CF 13.10.	M	SIA RSISC va oferi mecanism de versionare a valorilor metadatelor și stabilite a intervalului de timp aferent validității valorilor metadator.	Da
CF 14.01.	M	SIA RSISC va dispune de facilități de configurare a strategiilor de jurnalizare a evenimentelor de business.	Da
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 sau platforme specializate (*exemplu: utilizarea generatoarelor de rapoarte*).	Da
CF 14.03.	D	SIA RSISC trebuie să permită adăugarea și configurarea unor noi rapoarte.	
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.	Da

CF 14.05.	M	SIA RSISC va dispune de funcționalitate de definire a termenului de valabilitate a formularelor electronice aflate în statut „Proiect” după care pot fi suprimate automat.	Da
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. SIA RSISC trebuie să permită adăugarea și configurarea de job-uri noi precum și modificarea parametrilor de funcționare a job-urilor existente.	Da
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 facilităților de interoperabilitate).	Da
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 de interfața utilizator fără a fi necesară compilarea și/sau desfășurarea repetată a codului sursă sau intervenții directe în conținutul bazei de date.	Da
CF 15.01.	M	SIA RSISC va avea încorporat un serviciu Heartbeat care va comunica periodic statutul curent de funcționare a sistemului informatic.	Da
CF 15.02.	M	SIA RSISC trebuie să conțină mecanisme de monitorizare a gradului de încărcare și statutul curent al tuturor componentelor cheie (Furnizorul trebuie să furnizeze soluție software de monitorizare a performanței SIA RSISC).	Da
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 cel așteptat*).	Da
CF 15.04.	M	Furnizorul trebuie să asigure facilități de administrare a SIA RSISC după 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.	Da

CF 15.05.	M	Mijloacele care implementează funcțiile de administrare a SIA RSISC pot fi implementate folosind comenzile și facilitățile software-ului de platformă, fără a fi nevoie de implementarea unei interfețe grafice dedicate.	Da
CF 15.06.	M	Furnizorul trebuie să enumere mijloacele care trebuie utilizate pentru depanarea problemelor tehnice de funcționare a SIA RSISC.	Da
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.	Da
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.	
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.	Da
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).	Da
CF 15.11.	M	SIA RSISC va permite extragerea agregată a rapoartelor sau detalierea acestora per utilizator concret, subdiviziune centrală sau teritorială a STISC sau a unor grupuri de utilizatori.	Da
CF 15.12.	M	Un utilizator care vizualizează un raport în cadrul sistemului, trebuie să-l poată exporta în format PDF sau într-un fișier extern redactabil (XLS/XLSX, CSV, DOC/DOCX).	Da
CF 15.13.	M	Furnizorul va implementa până la 10 rapoarte predefinite ale auditului informatic solicitate de STISC. Rapoartele de audit care pot fi generate prin intermediul mijloacelor de sistem nu vor fi implementate în interfața utilizator a SIA RSISC.	Da
CF 15.14.	D	Pentru extragerea rapoartelor și statisticilor de sistem relevante CU15 este binevenită utilizarea unei	

		platforme dedicate configurării și generării rapoartelor.	
CF 16.01.	M	SIA RSISC va furniza funcționalitate de lansare a procedurilor automate destinate funcționării în bune condiții a sistemului informatic.	Da
CF 16.02.	M	Momentul de timp și periodicitatea lansării spre execuție a procedurilor automate este configurat prin intermediul CF 14.05.	Da
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 posibilă restabilirea funcționalității sistemului informatic în cazul producerii unor incidente de securitate.	Da
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 pe platforma de producție.	Da
CF 16.05.	M	SIA RSISC va declanșa în mod automat procedurile de schimb reciproc de date cu sisteme informatice externe definite prin intermediul CU17.	Da
CF 16.06.	M	SIA RSISC va șterge automat formularele electronice aflate în statut „Proiect” care au depășit termenul limită de aflare în acest statut configurat prin intermediul CU14.	Da
CF 16.07.	M	SIA RSISC va fi capabil să efectueze periodic și planificat (în orele de solicitare minimă a SIA RSISC) calculele preliminare ale indicatorilor necesari generării în timp util a rapoartelor statistice complexe.	Da
CF 16.08.	M	SIA RSISC identifica automat și expedia notificările ce trebuie expediate utilizatorilor autorizați ca urmare a unor evenimente de business (*exemplu: întârzieri în executarea sarcinilor*).	Da
CF 16.09.	M	SIA RSISC trebuie să furnizeze interfață de vizualizare a statutului curent al procedurile executate automat în curs de procesare.	Da
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.	Da
CF 16.11.	M	SIA RSISC va publica periodic în cadrul interfeței publice și Partalului Datelor Deschise rapoarte și KPI	Da

		cu caracter public produse în cadrul proceselor de business implementate.	
CF 16.12.	M	Toate evenimente aferente funcționării procedurilor automate definite prin intermediul cerințelor funcționale CF 16.03 - CF 16.11 trebuie jurnalizate.	Da
CF 16.13.	M	SIA RSISC trebuie să furnizeze facilități de corelare, in baza datelor acumulate, precum si cele disponibile public (ipReputation,DomainReputation,BotNets,etc) precum si stabilirea gradului de risc in baza mai multor criterii.	Da
CF 16.14.	M	SIA RSISC trebuie să furnizeze facilități de identificare si ridicarea gradului de risc in baza clasificatoarelor precum si corelarea acestora cu MITRE ATT&CK®.	Da
CF 17.01.	M	SIA RSISC trebuie să fie dezvoltat în baza unei arhitecturi capabile să implementeze facilități de interoperabilitate cu sisteme informatice externe.	Da
CF 17.02.	M	SIA RSISC va efectua schimb de date cu sistemele informatice externe prin intermediul API-urilor expuse de acestea (cazul sistemelor informatice neguvernamentale) și platforma de interoperabilitate a MConnect (pentru cazul sistemelor informatice ale AP).	Da
CF 17.03.	M	Interacțiunea SIA RSISC cu sistemele informatice interne ale STISC în cazul 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.	Da
CF 17.04.	M	SIA RSISC trebuie să fie capabil a se integra cu următoarele servicii de guvernamentale: • MPass - pentru autentificare și controlul accesului utilizatorilor; • MSign - pentru aplicarea semnăturii electronice în cadrul proceselor de business ale SIA RSISC; • MLog - pentru jurnalizarea evenimentelor de business critice; • MNotify - pentru notificarea utilizatorilor autorizați; • MPower - pentru verificarea împuternicirilor de reprezentare a utilizatorilor necesare autorizării acțiunilor acestora; PDGD - pentru publicarea seturilor publice de date produse în cadrul fluxurilor de lucru ale SIA RSISC.	Da
CF 17.05.	M	SIA RSISC se va integra prin intermediul platformei guvernamentale MConnect cu următoarele sisteme	Da

		informatice pentru recepționarea datelor aferente alertelor și incidentelor de securitate: • Sisteme informatice ale AP - care vor expedia în mod automat alerte 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 considerate cu risc major asupra securității informației;; Soluții informatice destinate gestiunii incidentelor de securitate cibernetică - pentru preluarea automatizată a datelor aferente alertelor și e a incidentelor de securitate cibernetică.	
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 datelor recepționate.	Da
CF 17.07.	M	SIA RSISC se va integra cu Google Analytics în scopul expedierii datelor statistice privind exploatarea Interfeței Publice.	Da
CF 17.08.	M	SIA RSISC se va integra cu rețele de socializare (LinkedIn, Facebook și Twitter) în scopul publicării informației de conținut a interfeței publice SIA RSISC.	Da
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 intermediul mecanismului de jurnalizare intern a SIA RSISC și serviciului de platformă MLog.	Da
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.	Da
CF 17.11.	M	Sistemul va include adaptoare la cheie pentru urmatoarele surse de date(Fortinet,ShadaowServer,Barracuda Spam, si WAF, Nginx, WangGuard)	Da

CF 17.12.	M	Sistemul va permite importarea, periodica, din diferite surse publice, IpReputation, botnet, etc.	Da
CF 18.01.	M	SIA RSISC va conține mecanism de jurnalizare a tuturor evenimentelor de business aferente utilizării sale.	Da
CF 18.02.	M	Administratorul de Sistem va putea configura strategiile de jurnalizare aferente 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 guvernamental MLog).	Da
CF 18.03.	M	SIA RSISC va furniza Administratorilor de Sistem mecanism de căutare, filtrare și vizualizare a detaliilor evenimentelor jurnalizate.	Da
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 SIA RSISC; • schimbul de date cu sisteme informatice externe; • generare/accesare raport; • interogări la baza de date; alte evenimente de business specifice.	Da
CF 18.05.	M	Evenimentele jurnalizate vor salva următoarele categorii de date (în funcție 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.).	Da
CF 18.06.	M	SIA RSISC va jurnaliza exhaustiv toate evenimentele de business produse.	Da

CF 18.07.	M	SIA RSISC va jurnaliza în paralel evenimentele de business critice prin intermediul serviciul guvernamental de jurnalizare MLog.	Da
CF 18.08.	M	SIA RSISC va furniza funcționalitate de definire a evenimentelor de business critice care urmează a fi jurnalizate în paralel prin intermediul serviciului de platformă MLog.	Da
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.	Da
CF 19.02.	M	SIA RSISC va notifica utilizatorii relevanți la producerea unui eveniment de business specific activității lor.	Da
CF 19.03.	M	Notificarea va conține referință de accesare a înregistrării/formularului electronic relevant evenimentului de business care a generat notificarea (valabil pentru notificările stocate în Dashboard-ul utilizatorului).	Da
CF 19.04.	M	Utilizatorii autorizați (indiferent de rolurile de care dispun) vor putea să-și configureze preferințele mijloacelor de notificare.	Da
CF 19.05.	M	Toate categoriile de utilizatori autorizați vor primi notificări privind evenimentele 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.*).	Da
CF 19.06.	M	Administratorul de Sistem va dispune de funcționalitate de perfectare și expediere notificări utilizatorilor expliciți sau grupurilor de utilizatori.	Da
CF 19.07.	M	SIA RSISC va notifica Administratorul de Sistem asupra oricăror probleme ce afectează performanța și disponibilitatea sistemului informatic.	Da
CF 19.08.	M	SIA RSISC va notifica utilizatorii care recepționează notificările prin mijloace externe prin intermediul serviciului guvernamental de notificare MNotify.	Da
GEN 001	M	SIA RSISC trebuie să fie dezvoltat în baza metodologiei Agile.	Da

GEN 002	M	Toate interfețele utilizator și conținutul bazei de date vor fi perfectate în limba română cu utilizarea diacriticelor românești.	Da
GEN 003	M	Interfața utilizator al interfeței publice a SIA RSISC și valorile metadatelor textuale (clasificatoare, nomenclatoare etc.) trebuie să fie accesibile în limbile română, engleză și rusă.	Da
GEN 004	M	Datele bazei de date a SIA RSISC urmează a fi stocate în format unicode (*exemplu: utilizând UTF-8*).	Da
GEN 005	M	Elementele interfeței utilizator trebuie să se conformeze la Nivel A cu cerințele *Web Content Accessibility Guidelines (WCAG) 2.0.*	Da
GEN 006	M	Interfața utilizatori pentru utilizatorii autorizați ai SIA RSISC va fi optimizată rezoluției 1360x768 cu evitarea apariției barelor de defilare pentru interfețele utilizator prezentate de soluția informatică.	Da
GEN 007	M	SIA RSISC va furniza interfață publică adaptabilă (va livra interfață responsivă) în funcție de dispozitivul utilizat de acesta (*notebook, netbook, calculator desktop, smartphone, tabletă etc.*)	Da
GEN 008	M	Interfața Publică va genera paginile de conținut ținând cont de cele mai bune practici de optimizare SEO.	Da
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 de natura informației căutate utilizatorul va utiliza aceeași metodă de interogare și regăsire a datelor pentru orișicare compartiment al interfeței utilizator a produsului informatic.	Da
GEN 010	M	Interfața utilizator a sistemului informatic trebuie să asigure căutarea, filtrarea și vizualizarea înregistrărilor ce corespund criteriului de căutare prezentate utilizatorilor în funcție de drepturile lor de acces.	Da
GEN 011	M	Conținutul oricărui tabel cu rezultate ale căutării trebuie să poată fi exportat fie în format XLS, CSV și PDF.	Da
GEN 012	M	Arhitectura SIA RSISC va fi concepută integrat, dezvoltată cu aplicarea celor mai bune practici în domeniu (exemplu: principii de arhitectură și arhitecturi de referință aliniate TOGAF 9.1).	Da
GEN 013	M	Arhitectura completă SIA RSISC va fi coordonată în prealabil cu STISC.	Da

GEN 014	M	Arhitectura SIA RSISC trebuie să asigure utilizarea rațională și balansată a resurselor de procesare.	Da
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 logicii de business și nivelul de date*).	Da
GEN 016	M	SIA RSISC trebuie să ofere interfețe web de interacțiune cu sisteme informatice ale STISC și ale altor autorități publice ale Republicii Moldova prin intermediul microserviciilor și MCloud.	Da
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.	Da
GEN 018	M	Informația potențial variabilă (*exemplu: diferiți parametri, căi de stocare a 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.	Da
PER 001	M	Timpul mediu de răspuns al serverului nu va depăși 3 secunde la încărcătura nominală a sistemului.	Da
PER 002	M	SIA RSISC trebuie sa fie capabil să permită activitatea a cel puțin 200 utilizatori autorizați.	Da
PER 003	M	SIA RSISC va permite activitatea concurentă a cel puțin 150 utilizatori autorizați și deservirea concomitentă a cel puțin 100 interogări fără a afecta performanța de funcționare.	Da
PER 004	M	Interfața publică a SIA RSISC trebuie sa fie capabilă sa deservească accesul anual a peste 500000 utilizatori anonimi.	Da
PER 005	M	Interfața publică a SIA RSISC trebuie să fie capabilă să deservească cel puțin 500 utilizatori anonimi concurenți și 300 interogări paralele.	Da
PER 006	M	SIA RSISC trebuie să fie capabil să recepționeze, proceseze și stocheze anual datele a peste 100 000 000 alerte și peste și peste 10 000 incidente de securitate.	Da
PER 007	M	Anterior livrării SIA RSISC vor fi efectuate totalitatea testelor de performanță și securitate.	Da
PER 008	M	Testarea performanței va include minim doua componente: testarea încărcăturii sistemului (*load testing*) și testarea comportamentului sistemului la solicitări mari (*stress testing*).	Da

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 noduri server și efectuare balansare a încărcării).	Da
SR 002	D	SIA RSISC va putea fi configurat pentru scalare automată la nivelul componentelor cheie (lag sensitive). Scalarea sistemului se va face atât în sus, cât și în jos.	
SR 003	M	SIA RSISC trebuie să dețină posibilitatea de a deservi un număr nelimitat de tranzacții, cu condiția alocării corespunzătoare a resurselor de procesare și stocare date. Resursele vor fi alocate pe orizontală (alocare noi servere, fără creșterea performanței pe serverele existente).	Da
SHC 001	M	SIA RSISC trebuie să poată fi instalat atât pe servere dedicate, cât și pe soluții de virtualizare (SIA RSISC trebuie să fie conform cerințelor de desfășurare a sistemelor informatice pe platforma guvernamentală tehnologică comună MCloud).	Da
SHC 002	M	Este necesară demonstrarea capacității de virtualizare prin livrarea către STISC a unei imagini a sistemului ce poate fi încărcată și devine funcțională cu configurări minime pe una din soluțiile de virtualizare existente pe piață.	Da
SHC 003	M	Furnizorul va demonstra posibilitatea instalării și operării SIA RSISC în infrastructura MCloud.	Da
SHC 004	M	SIA RSISC trebuie să poată fi accesat pe canale de comunicații de cel puțin 512Kbps.	Da
SHC 005	M	SIA RSISC trebuie să fie dezvoltat în baza următoarelor tehnologii: • Microsoft Windows Server 2019 (în calitate de sistem de operare); • IIS 10 (în calitate de server WEB); • Microsoft SQL Server 2019 Standard Edition (în calitate de SGBD); • Elastic Search (în calitate de motor de căutare indexată a datelor și 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 de rapoarte);	Da

		• Angular JS, React JS sau Knockout JS (în calitate de framework destinat implementării interfeței utilizator); Nginx (în calitate de soluție pentru balansor)	
SHC 006	M	Furnizorul va indica explicit în ofertă platforma software în baza căreia urmează a fi dezvoltat SIA RSISC și platforma software necesară exploatării acestuia.	Da
SHC 007	M	Tehnologiile propuse de Furnizor trebuie să fie accesibile pentru cel puțin 3 companii specializate în dezvoltarea soluțiilor software care activează pe piața locală a Republicii Moldova	Da
SHC 008	M	SIA RSISC va utiliza standarde deschise pentru formate și protocoale de comunicare.	Da
SHC 009	M	Serviciile expuse către public de SIA RSISC vor fi tehnologic neutre (Sistem de Operare, explorator Internet etc.).	Da
SHC 010	M	Produsul program generic recomandat pentru operarea și interacțiunea cu SIA RSISC reprezintă exploratorul WEB.	Da
SHC 011	M	Sistemul va fi compatibil cu cel puțin 2 cele mai recente versiuni ale următoarelor exploratoare Web: *MS Internet Explorer/MS Edge, Mozilla Firefox, Google Chrome*, *Safari* și *Opera*.	Da
SHC 012	M	Compatibilitatea cu exploratorul WEB *MS Internet Explorer/MS Edge* este obligatorie.	Da
SHC 013	D	SIA RSISC va încorpora un serviciu Heart-beat care va comunica periodic starea normală de lucru a sistemului.	
SHC 014	M	Sistemul va include mijloace configurabile de jurnalizare tehnică (logging).	Da
SHC 015	M	Sistemul trebuie să fie capabil să producă cel puțin următoarele nivele de jurnalizare tehnică: *info*; *warning*; *critic*; *error*.	Da
SHC 016	M	Dezvoltatorul va enumera mijloacele ce vor fi utilizate la depanarea tehnică a sistemului.	Da
SHC 017	M	Furnizorul va pregăti mijloace ce facilitează funcțiile de administrare a sistemului: • startarea componentelor sistemului; • stoparea componentelor sistemului; • restartarea componentelor sistemului, • crearea copiei de rezervă a bazei de date,	Da

		• restaurarea datelor de pe copia de rezervă indicată, împrospătarea memoriei operaționale a sistemului.	
SHC 018	M	SIA RSISC va opera în rețele TCP/IP și în special HTTPS.	Da
SHC 019	M	SIA RSISC va utiliza XML în calitate de mijloc principal pentru integrarea datelor.	Da
SHC 020	M	Furnizorul va sugera alte servicii de rețea și utilitare necesare pentru operarea sistemului.	Da
LIC 001	I	STISC va asigură următoarele medii de operare pentru SIA RSISC: • Mediul de producție; • Mediul de testare/instruire; Mediul de dezvoltare.	
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 la dispoziție de STISC. Aici sunt incluse următoarele: sisteme de operare, sisteme de gestiune baze de date, biblioteci software, utilitare și alt soft de sistem.	Da
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*).	Da
LIC 004	M	Cantitatea licențelor oferite trebuie să permită accesarea API-urilor expuse de SIA RSISC de orice aplicație și sistem extern.	Da
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.	Da
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.	Da

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.	Da
INT 001	I	Toate interfețele expuse de SIA RSISC trebuie să fie bazate pe standarde deschise. Toate fluxurile de mesaje între SIA RSISC și entități externe se vor realiza cu utilizarea standardelor deschise.	
INT 002	M	SIA RSISC va deține capabilități de implementare a interfețelor prin intermediul MConnect.	Da
INT 003	M	SIA RSISC va deține capabilități de integrare cu sistemele informatice ale AP din Republica Moldova în vederea recepționării automate a datelor referitoare la alertele înregistrate pe parcursul exploatării lor.	Da
INT 004	M	SIA RSISC va deține capabilități de integrare cu sistemele informatice ale AP din Republica Moldova destinate gestiunii incidentelor de securitate în vederea recepționării datelor referitoare la incidentele de securitate gestionate în cadrul AP.	Da
INT 005	M	SIA RSISC se va integra cu platforma de interoperabilitate MConnect pentru a consuma date din sisteme informatice externe (exemplu: extragerea datelor din registre de stat).	Da
INT 006	M	SIA RSISC se va integra cu serviciul guvernamental MPass pentru implementarea mecanismului de autentificare a utilizatorilor prin intermediul semnăturii electronice sau mobile.	Da
INT 007	M	SIA RSISC se va integra cu serviciul guvernamental MSign pentru implementarea infrastructurii de utilizare a semnăturii electronice.	Da
INT 008	M	SIA RSISC se va integra cu serviciul guvernamental MLog pentru jurnalizarea evenimentelor de business critice.	Da
INT 009	M	SIA RSISC se va integra cu serviciul guvernamental MNotify pentru implementarea mecanismului de notificare a utilizatorilor.	Da
INT 010	M	SIA RSISC se va integra cu serviciul guvernamental MPower pentru verificarea împuternicirilor utilizatorilor autoriza de a efectua acțiuni specifice în cadrul interfeței utilizator.	Da
INT 011	M	SIA RSISC se va integra cu serviciul guvernamental Portalul Datelor Deschise (https://date.gov.md) pentru publicarea datelor deschise produse în cadrul fluxurilor de lucru implementate.	Da

INT 012	M	Toate interfețele furnizate de SIA RSISC vor interacționa cu aplicațiile externe instantaneu sau programat prin intermediul unor job-uri specializate.	Da
INT 013	M	Interfața publică a SIA RSISC se va integra cu Google Analytics și cele mai importante rețele de socializare (LinkedIn, Facebook și Twitter) în vederea expedierii statisticilor de vizitare a conținutului public și publicării conținutului public pe rețelele de socializare.	Da
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*).	
INT 015	D	Interfețele respective trebuie să permită gestiunea entităților de business cu aplicarea tuturor regulilor de business relevante și cu utilizarea tuturor proprietăților aferente entităților de business.	
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, la implementarea funcționalităților SIA RSISC.	
INT 017	M	SIA RSISC va deține interfețe standard pentru exportul datelor în cadrul instrumentelor de tipul Data Warehouse.	Da
MIG 001.	M	STISC va pregăti și livra seturile de date și metadate necesare populării cu date primare a SIA RSISC. Formatul datelor migrate va fi convenit de comun acord cu Dezvoltatorul.	Da
MIG 002.	M	Dezvoltatorul va trebuie să convertească valori specifice ale metadatelor aferente seturilor de date externe conform sistemului de metadate statistice al STISC.	Da
MIG 003.	M	Dezvoltatorul va include în oferta tehnică abordarea sa privind procedura de implementare a procedurii de migrare și populare inițială a bazei de date.	Da
MIG 004.	M	Dezvoltatorul trebuie să furnizeze mecanism care va asigura popularea automatizată 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.	Da
MIG 005.	M	Pe parcursul implementării procedurii de migrare și populare a datelor Furnizorul este responsabil pentru:	Da

		• definirea metodologiei utilizate în procesul de migrare și populare a datelor; • elaborarea planurilor detaliate de migrare și populare a datelor; • furnizarea mecanismelor software destinate migrării și populării datelor; • 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 (în cazul 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 fi migrate și populare; • popularea bazei de date a SIA RSISC în baza seturilor de date furnizate de STISC; identificarea și soluționarea excepțiilor/erorilor pe parcursul procesului de migrare și populare a datelor.	
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 și populate; • 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 de SIA RSISC dar care 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 a procesului de migrare și populare a datelor); planul de livrare a mecanismului de migrare și populare a datelor.	Da

MIG 007.	M	Furnizorul trebuie să pregătească și livreze planul detailat al migrării și populării inițiale cu date a SIA RSISC (strategia de migrare și conversie a datelor). Acest plan trebuie să fie aliniat planului de implementare a SIA RSISC.	Da
MIG 008.	M	Furnizorul trebuie să livreze către STISC soluție software destinată automatizării proceselor de migrare și populare inițială cu date a SIA RSISC.	Da
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. Datele nu vor părăsi niciodată infrastructura TIC a STISC.	Da
MIG 010.	M	În procesul migrării Furnizorul se va confirma politicii de securitate a STISC.	Da
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 fi semnat între Furnizor și STISC).	Da
SEC 014	M	SIA RSISC va permite accesarea funcțiilor sale doar după autentificarea cu succes 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).	Da
SEC 015	M	SIA RSISC va permite utilizatorilor mecanism de schimbare și restabilire a parolelor individuale.	Da
SEC 016	M	SIA RSISC va permite înregistrarea utilizatorilor și a informației de profil aferentă acestora (*exemplu: login, parolă, nume, prenume, IDNP, Email etc.*).	Da
SEC 017	M	Parolele utilizatorilor trebuie să fie protejate. Metoda de protejare a parolelor trebuie să asigure imposibilitatea interceptării, deducerii sau recuperării acestora (algoritm de criptare unidirecțională).	Da
SEC 018	D	SIA RSISC va permite aplicarea diferențiată a politicilor de utilizare a parolelor pentru diferite grupuri de utilizatori.	
SEC 019	M	SIA RSISC va permite blocarea, dezactivarea sau suspendarea conturilor utilizatorilor la nivel de aplicație.	Da
SEC 020	D	SIA RSISC va permite aplicarea diferențiată a metodelor de autentificare, în funcție de rolurile	-

		deținute de utilizatori și componentele funcționale accesate	
SEC 021	M	SIA RSISC va permite setarea numărului de conexiuni simultane ce pot fi inițiate de un utilizator.	Da
SEC 022	M	SIA RSISC va permite setarea timpului de expirare a sesiunilor utilizatorilor autorizați în caz de inactivitate (valoarea implicită este de 15 minute).	Da
SEC 023	M	SIA RSISC va deține mecanisme eficiente de prevenire a preluării neautorizate a sesiunilor active inițiate de utilizatorii autorizați.	Da
SEC 024	M	Sesiunea de lucru în SIA RSISC va fi blocată la solicitarea utilizatorului sau automat, la expirarea timpului rezervat sesiunii.	Da
SEC 025	M	SIA RSISC va permite gestiunea granulară a drepturilor de acces la toate obiectele sale și acțiunile posibile asupra acestora (*exemplu: formulare electronice, meniuri, rapoarte, acțiuni de creare/vizualizare/actualizare/ eliminare etc.*).	Da
SEC 026	M	Metoda de autorizare în cadrul sistemului se va baza pe principiul „*este interzis tot ce nu este explicit permis*”.	Da
SEC 027	M	SIA RSISC va permite definirea de grupuri de utilizatori și roluri și asocierea utilizatorilor la aceste grupe și roluri.	Da
SEC 028	M	SIA RSISC va permite acordarea drepturilor de acces la nivel de utilizator explicit, 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.	Da
SEC 029	M	SIA RSISC va permite acordarea drepturilor de acces bazate pe reguli de business (exemplu: modificarea înregistrării doar dacă utilizatorul este autor sau dacă operațiunea se face într-un anumit interval de timp, stare sau context).	Da
SEC 030	M	SIA RSISC va permite atribuirea temporară a drepturilor deținute de un utilizator către un alt utilizator. Atribuirea va putea fi efectuată cu păstrarea sau suspendarea drepturilor deținute de utilizatorul către care se deleagă drepturile.	Da
SEC 031	D	SIA RSISC va permite segregarea activităților administrative (exemplu: Administratorul 1 modifică, Administratorul 2 confirmă).	
SEC 032	M	SIA RSISC va furniza vizualizări și rapoarte privind drepturile de acces configurate. Acestea vor putea fi parametrizate în funcție de cel puțin următoarele	Da

		criterii: grup de utilizatori/roluri, login utilizator, acțiuni admise etc.	
SEC 033	M	SIA RSISC va deține capabilități de autentificare și autorizare a utilizatorilor prin intermediul atât a mecanismelor interne, cât și prin intermediul serviciului de platformă MPass.	Da
SEC 034	M	SIA RSISC va autoriza accesul utilizatorilor la compartimentele interfeței utilizator și date după verificarea împuternicirilor acestora prin intermediul MPower.	Da
SEC 035	M	SIA RSISC va deține mecanisme adecvate pentru a preveni manipularea datelor de intrare (date de intrare parvenite de la utilizatorii autorizați, date de intrare parvenite de la aplicații externe).	Da
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*).	Da
SEC 037	M	SIA RSISC va efectua validarea completă și independentă a datelor pe partea de nivelul de prezentare, nivelul logicii de business, nivelul de date, în scopul asigurării integrității, completitudinii și corectitudinii datelor.	Da
SEC 038	M	Toate afișările de date în cadrul SIA RSISC trebuie să fie însoțite de un marcaj de securitate, conform unui clasificator stabilit în acest sens în cadrul SIA RSISC.	Da
SEC 039	M	Datele confidențiale nu vor fi stocate și accesate nesecurizat în cadrul SIA RSISC (*exemplu: fișiere log, caching etc.*).	Da
SEC 040	M	SIA RSISC va deține mecanisme de protejare adițională a datelor deosebit de confidențiale (exemplu: afișarea mascată a datelor, stocarea datelor în formă criptată, autentificarea repetată sau utilizând mijloace suplimentare a utilizatorului etc.).	Da
SEC 041	M	SIA RSISC va deține proceduri de rutină pentru verificarea și detectarea posibilelor coruperi a relațiilor de integritate a datelor.	Da
SEC 042	M	SIA RSISC va deține mecanisme adecvate pentru a preveni manipularea datelor stocate în cadrul aplicației.	Da
SEC 043	M	SIA RSISC va deține componente de audit ce vor colecta și gestiona centralizat înregistrările de audit la nivelul fiecărui modul al sistemului informatic.	Da

SEC 044	M	Componenta de audit va permite configurarea granulară a politicilor de audit.	Da
SEC 045	M	SIA RSISC va permite stabilirea politicilor de audit la nivel de componentă funcțională/compartiment al interfeței utilizator, categorii de date și la nivel de eveniment jurnalizat.	Da
SEC 046	M	SIA RSISC va permite stabilirea caracteristicilor specifice evenimentelor ce trebuie să fie jurnalizate (exemplu: produse într-un anumit interval de timp, aflate într-un anumit statut sau care tranzitează un anumit statut etc.).	Da
SEC 047	M	SIA RSISC va permite auditarea oricărui eveniment, la nivelul oricărui obiect sau entitate de business din cadrul sistemului informatic.	Da
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.	Da
SEC 049	M	Înregistrările de audit nu vor conține date confidențiale (exemplu: parole introduse la încercările eșuate de autentificare).	Da
SEC 050	M	Erorile ce pot apărea la jurnalizarea înregistrărilor de audit nu trebuie să afecteze funcționarea normală a sistemului informatic.	Da
SEC 051	M	Componenta de audit va utiliza ceasul de sistem setat la nivelul sistemului de operare al serverului aplicație în care rulează funcționalitatea de jurnalizare a evenimentelor.	Da
SEC 052	M	Componenta de audit va deține un mecanism de arhivare a înregistrărilor de audit istorice. Procesul de arhivare va putea fi parametrizat (frecvența, vechime date, format arhivare, destinație etc.).	Da
SEC 053	M	SIA RSISC va putea genera automat notificări către persoanele responsabile la producerea anumitor evenimente de securitate, conform configurațiilor setate.	Da
SEC 054	M	SIA RSISC va permite fixarea versiunilor istorice ale datelor, ce vor fi considerate deosebit de senzitive.	Da

SEC 055	M	Activitățile de schimbare stări și responsabili înregistrări vor fi jurnalizate.	Da
SEC 056	M	SIA RSISC va deține instrumente comode pentru accesarea și procesarea evenimentelor jurnalizate, inclusiv filtrarea înregistrărilor de audit după orice câmp deținut și exportul acestora în format uzual. Instrumentele de audit ale sistemului informatic vor putea fi utilizate și în scopul importului arhivelor cu fișiere de audit pentru activități de analiză ocazionale.	Da
SEC 057	M	SIA RSISC va deține mecanisme sigure de protejare a integrității datelor de audit înregistrate.	Da
SEC 058	M	Evenimentele de business critice trebuie jurnalizate în paralel prin intermediul serviciului guvernamental de jurnalizare MLog.	Da
SEC 059	M	SIA RSISC va furniza mecanism de configurare a evenimentelor de business care vor fi jurnalizate în paralel prin intermediul serviciului MLog.	Da
SEC 060	M	SIA RSISC va înregistra centralizat toate excepțiile și erorile generate de componentele sale funcționale.	Da
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 identificator unic al erorii, pentru a facilita implicarea serviciilor de suport.	Da
SEC 062	M	SIA RSISC va deține instrumentele necesare pentru analiza și procesarea înregistrărilor aferente excepțiilor și erorilor.	Da
SEC 063	M	SIA RSISC va putea genera automat notificări către persoanele responsabile la producerea anumitor erori în funcționarea componentelor sale funcționale.	Da
SEC 064	M	SIA RSISC va avea implementate instrumente pentru executarea procedurilor de generare automată a copiilor de rezervă și gestiune a copiilor de rezervă istorice.	Da
SEC 065	M	SIA RSISC trebuie să dețină mecanisme de asigurare a integrității datelor în cazul căderilor la nivelul oricăror componente.	Da
SEC 066	M	SIA RSISC trebuie să dețină mecanisme de restabilire operativă a disponibilității și accesibilității în cazul unor incidente de continuitate.	Da

SEC 067	M	Arhitectura SIA RSISC trebuie să fie rezistentă la căderi de componente și să nu dețină puncte singulare de cădere (SPOF).	Da
SEC 068	M	SIA RSISC trebuie să dețină mecanisme de asigurare a integrității datelor în cazul unor căderi accidentale la nivelul oricăror componente ale sale.	Da
SEC 069	M	SIA RSISC trebuie să dețină mecanisme de restabilire operativă a disponibilității și accesibilității în cazul unor incidente de continuitate.	Da
DEP 001	M	SIA RSISC trebuie să capabil a fi instalat pe servere dedicate și în medii virtualizate.	Da
DEP 002	M	SIA RSISC trebuie să capabil să fie desfășurat și să funcționeze pe o infrastructură containerizată (*exemplu: Docker Engine, Kubernetes*).	Da
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.	Da
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.	Da
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.*).	Da
DEP 006	M	Mecanismul de desfășurare a SIA RSISC trebuie să fie capabil să gestioneze conținutul containerului.	Da
DEP 007	M	Mecanismul de desfășurare a SIA RSISC trebuie să fie capabil să adauge noi componente în conținutul containerului.	Da
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.	Da
DEP 009	M	Pentru desfășurarea SIA RSISC este necesar ca mecanismul de desfășurare să furnizeze flux de lucru pentru compilarea codului sau registrelor.	Da

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.	Da
DEP 011	M	Mediul de producție al SIA RSISC trebuie să poată fi actualizat automat cu posibilități de intervenție manuală (*exemplu: aprobare build manual*).	Da
DEP 012	M	Dezvoltatorul va livra către STISC toate instrumentarele și scripturile necesare desfășurării automatizate a SIA RSISC.	Da
DOC 001	M	Furnizorul va pregăti și publica materiale de ghidare interactivă incluse în interfața utilizator a SIA RSISC.	Da
DOC 002	M	Furnizorul va pregăti și livra manualul utilizatorului în limba Română.	Da
DOC 003	M	Furnizorul va pregăti și livra ghidul administratorului în limba Română.	Da
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, configurarea aplicației, proceduri de disaster recovery).	Da
DOC 005	M	Furnizorul va pregăti și livra proiectul tehnic al sistemului informatic livrat în baza căruia vor fi efectuate totalitatea activităților de dezvoltare/acceptanță a sistemului informatic (SRS și SDD).	Da
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 modelul logic și fizic al datelor).	Da
DOC 007	M	Furnizorul va pregăti și livra documentația API-urilor consumate și expuse pentru integrare cu sistemele informatice externe.	Da
DOC 008	M	Furnizorul va livra totalitatea instrucțiunilor necesare bunei exploatări a SIA RSISC și soluționare a unor eventuale probleme tehnice.	Da

DOC 009	M	Furnizorul va livra codul sursă pentru aplicațiile și componentele dezvoltate în cadrul proiectului cu comentariile necesare înțelegerii codului program.	Da
DOC 010	M	Furnizorul va livra documentația de instruire pentru toate rolurile de utilizatori ai SIA RSISC.	Da
GMS 001	M	Dezvoltatorul va oferi garanție și suport tehnic pe parcursul a 12 luni după acceptanța finală a SIA RSISC.	Da
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.	Da
GMS 003	M	Dezvoltatorul va pune la dispoziția STISC un serviciu Help Desk disponibil în toate zilele lucrătoare ale anului.	Da
GMS 004	M	Utilizatorii STISC vor putea apela serviciul Help Desk la un număr de telefon național (care corespunde numerotării telefonice a Republicii Moldova).	Da
GMS 005	M	Limba de comunicare cu serviciul Help Desk – română sau rusă.	Da
GMS 006	M	Utilizatorii STISC vor putea semnala alternativ problemele tehnice apărute prin mecanism de ticketing, Email sau mesaje instant.	Da
GMS 007	M	Furnizorul va asigura suport de documentare a problemelor tehnice și trasabilitatea acestora pentru Beneficiar.	Da
GMS 008	M	Termenul limită de răspuns și remediere a problemelor tehnice raportate nu va depăși 8 ore de la semnalarea acestora.	Da
GMS 009	M	În cazul unor probleme de complexitate majoră, termenul de soluționare a acestora nu va depăși 72 ore.	Da
GMS 010	M	Dezvoltatorul va demonstra capabilitatea de asigurare a suportului tehnic post livrare în conformitate cu cerințele GMS 001-GMS 009.	Da
GMS 011	M	Orice eroare program depistată pe parcursul perioadei de garanție va fi remediată de Dezvoltator gratuit și în termen util.	Da
GMS 012	M	În cazul apariției unor solicitări adăugătoare de implementare, acestea vor face obiectul unui	Da

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

DEL 015	M	Furnizorul urmează să efectueze activități de instruire destinate trainerilor STISC care vor putea instrui în continuare toate categoriile de utilizatori a SIA RSISC.	Da
DEL 016	M	Furnizorul urmează să efectueze activități de instruire tuturor categoriilor de utilizatori autorizați și utilizatorilor cu rol administrator de sistem.	Da
DEL 017	M	Furnizorul urmează să furnizez servicii de asistență tehnică pe perioada de pilotare a SIA RSISC.	Da
DEL 018	M	Furnizorul va asista STISC în activitățile de testarea de acceptare a SIA RSISC.	Da
DEL 019	M	Furnizorul urmează să furnizeze servicii de asistare a STISC în procesele de punere a SIA RSISC în producție.	Da
DEL 020	M	Furnizorul urmează să elimine toate deficiențele și erorile ale SIA RSISC identificate pe perioada de pilotare și la testarea de acceptare.	Da
DEL 021	M	Furnizorul urmează să asigure suport tehnic post implementare (după punerea sistemului în producție) pentru o perioadă de 12 luni, inclusiv mentenanță corectivă, adaptivă și preventivă, în conformitate cu *SM ISO/CEI 14764:2015 - Ingineria software. Procesele ciclului de viață al software-ului. Mentenanță*.	Da