Studiu privind standardele de certificare a securității cibernetice și analiză comparată

Proiect: Creșterea capacității autorităților competente din România, DNSC și RENAR conform Regulamentului European privind securitatea cibernetică 2019/881 (Cybersecurity Act)
Beneficiari: DNSC, RENAR și EY

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Cuprins

Tabel de figuri

Executive summary

Part 1. Presentation of the study

The National Cyber Security Directorate, the Accreditation Association of Romania and Ernst & Young, within the project "Increasing the capacity of the competent authorities in Romania DNSC and RENAR according to the European Regulation on Cybersecurity 2019/881 (Cybersecurity Act) developed the "Study on certification standards of cyber security and comparative analysis" in response to the need to increase the capacity of the competent authorities in Romania, DNSC and RENAR according to the Cybersecurity Act, with the aim of creating the optimal conditions for the adoption and implementation of the certification scheme of cyber security of ICT products, services and processes.

The objectives of the Study are:

- Need of implementation of a cyber security certification scheme in Romania.
- Analysis of the availability of implementing cyber security certification among entities (producers and users) from the public and private sector in Romania.
- Comparative analysis of Cybersecurity Act implementation practices at the level of some European Union member states with experience in terms of implementing its provisions.

The organizations involved in conducting the study are:

- National Cyber Security Directorate
- Accreditation Association from Romania
- Ernst & Young

The main results of the study are:

- Contribution to the fulfillment of the objective of the Directorate and Accreditation Association of Romania regarding the identification of the availability of implementation in Romania of the cyber security certification scheme, according to the Cybersecurity Act;
- The availability of alignment of the entities concerned regarding Romania's cyber security strategy, the financial and temporal implications related to the cyber security certification process for users and producers of products, services and processes in the field of information and communication technology.

Part 2. Current Affairs and Trends in Cyber Security Certification

Part 2.1. The European Cybersecurity Certification Framework

The European cybersecurity certification framework would establish an objective and standardized system of compliance with the level of trust specific to the evaluated products. Cyber security certification involves the formal assessment of ICT products, services and processes by an independent and accredited body against a defined set of criteria and standards, which can result in the issuance of a certificate indicating compliance. The certificates of conformity issued are recognized throughout the European Union. Cyber security certification system encourages developers to incorporate security specifications in the initial stages of product design and technical development (security by design).

To overcome the barriers within the single digital market and increase the transparency and comparability of ICT products, services and processes, with security elements, the European Union adopted the Cybersecurity Act. The document provides an integrated set of measures to support efforts to counter cyber-attacks and increase the cyber security trust at European level.

The Cybersecurity Act provides three levels of certification:

- products certified at the basic level must demonstrate the ability to minimize risks from known cyber incidents and attacks.
- products certified at the substantial level demonstrate the ability to minimize cyber security risks carried out by actors with limited capabilities and resources.
- products rated at the high level must demonstrate resistance to the latest cyber-attacks by actors with significant skills and resources.

At the European level, three certification schemes are being developed:

- Common Criteria based European candidate cybersecurity certification scheme,
- European Union Cybersecurity Certification Scheme for Cloud Services,
- European Union Cybersecurity Certification for 5G Networks.

Part 2.2. The standards required in cyber security certification

International standards have been developed to provide specific requirements for the establishment, implementation, maintenance and continuous improvement of an information security management system, for preserving confidentiality, integrity and availability of information by applying a risk management process that confers trust to stakeholders concerning proper management of risks.

The following standards are relevant for the certification activity in the field of cyber security of ICT products, services and processes:

- SR EN ISO/CEI 17065 Conformity assessment,
- SR EN ISO/CEI 17025 General requirements for the competence of testing and calibration laboratories, adopted in Romanian in March 2018.

Part 3. Romania's cybersecurity certification market

Part 3.1. Methodology

The market analysis carried out by Ernst &Young regarding the categories of ICT products, services and processes in Romania and the level of assurance of the cyber security certificate. The purpose of the analysis is to facilitate the adoption of the most effective decisions to transpose the Cybersecurity Act in Romania and includes:

- a desk research that led to the identification of the legislative framework;
- an online questionnaire, in Romanian, active between August 24 and September 30, 2022, which had as its target group a sample of approximately 300 IT certification laboratories, IT auditors, conformity assessment bodies, manufacturers, traders, distributors and public institutions identified as possible beneficiaries of products certified from cyber security perspective.

Part 3.2. National Cyber Security Normative Framework

The normative framework in the field of cyber security, in Romania, follows the provisions of European Union legislation and aims to update and expand the normative framework in the field of cyber security, by creating the national legislative framework for the transposition of the Cybersecurity Act.

Part 3.3. Objective and conclusions of the online questionnaire

The objective of the online questionnaire was to identify the categories of ICT products, services and processes present on the Romanian market, the level of assurance of the cyber security certificate and the obstacles encountered in the assurance process.

The need to increase the number of conformity assessment bodies in the field of cyber security as well as the number of cyber security testing laboratories was identified.

Part 3.4. Operationalization of the certification and monitoring structure in Romania

One of the main objectives of the Directorate is to create and develop the national certification framework in the field of cyber security, in cooperation with the institutions that have competences and responsibilities in the field.

According to Art.5(i) "National cybersecurity certification authority function", falls under the responsibility of the Directorate, which is the national body that ensures the mechanisms for the evaluation, certification and accreditation of products, services and processes in the field of cyber security, with the following roles and competences:

1. National Cyber Security Certification Authority for Civil Cyberspace. In this capacity, it certifies technologies, products and services from the point of view of cyber security;
2. Establishes norms, technical requirements, standards and procedures for the implementation of Cybersecurity Act;
3. Establishes and manages the National Register of Cyber Security Assets, Products and Services, hereinafter RNAPSSC;
4. Authorizes civilian laboratories for testing, evaluating and certifying cyber security of products and services;
5. Cooperates with national and international institutions in the field of standardization and accreditation of products, services and processes in the field of cyber security.

In accordance with the provisions of Art.5(q) "Evaluation and certification function", confers the following attributions:

1. Evaluates, tests and certifies cyber security products and services, for its own needs or at the request of institutions from SNAOPSN and/or the Government;
2. Establishes rules, prescriptions or characteristics for activities or their results in the field of cyber security, to ensure a unified approach at the national level in order to achieve a high common level of cyber security;
3. In collaboration with specialized bodies, participates in the development, approval and adoption of standards in the field of competence, which makes available to the public;
4. Participates in the work of national and international technical committees for the implementation of internationally accepted technical standards and specifications applicable to the security of networks and information systems, without imposing or discriminating in favor of the use of a certain type of technology.

Part 4. Comparative analysis of Cybersecurity Act implementation practices at the level of the Member States: France, Germany and the Netherlands

Part 4.1. France

French National Cyber Security Agency is a service with national competences and the role of conformity assessment body, a task carried out by the National Certification Center. This Center is the entity that certifies and issues the certificates. The main activities include reviewing the evaluation file sent by the sponsor and issuing a decision on the continuation of the evaluation activity. The sponsor has the task of managing the certification procedures from the side of the developer of the product subject to evaluation and certification.

The main duties of the National Certification Authority:

- Certification or public conformity assessment body that issues certificates at the high insurance level;
- Implementation of the European cyber security certification framework, including regulatory and external cooperation activities;
- Supervision - which includes the application of the controls established by the schemes, including the authorization and notification of conformity assessment bodies, monitoring of conformity assessment bodies, market surveillance for certificates issued in the form of self-assessments of conformity, handling complaints, providing support to the national body of accreditation, vulnerability management oversight and peer review.

Part 4.2. Germany

The national cybersecurity certification authority is the German Federal Office for Information Security. Thus, the Federal Office performs important certification, oversight management functions and is responsible for the following tasks:

- Monitoring and ensuring compliance with the rules within the European cyber security certification systems;
- Monitoring and ensuring compliance with manufacturers' obligations in the context of self-assessment of conformity;
- Supporting the national accreditation body in monitoring and supervising the activities of conformity assessment bodies and empowering them to grant authorization;
- Monitoring and supervision within European schemes;
- Monitoring relevant developments in the field of cyber security certification.

Part 4.3. Netherlands

The law adopting the Cybersecurity Act is at the draft stage. In the draft law, it is expected that the Ministry of Economy will be designated as the national cyber security certification authority and delegate this role to the Radiocommunications Agency of the Netherlands. At the same time, the draft law will designate an Accreditation Council as a national accreditation body, which will have the right to certify conformity assessment bodies.

The future law provides for the Netherlands Radiocommunication Agency to have additional responsibilities regarding the assessment of high-level certification. The law is to establish additional optional criteria for an assessment of the cyber security certification, supplementing the mandatory requirements set out in the Cybersecurity Act as well as procedures for legal protection that are in accordance with the Administrative Law. The law will also assign jurisdiction to the court, the Rotterdam Business Appeal Board, to be a specialized judicial tribunal in disputes regarding the approval or rejection of applications for cybersecurity certification.

Potential attributions of the National Cyber Security Center in the field of cyber security certification highlighted the following types of activities:

1. Supporting sets functions for the National Cyber Security Center that do not place it at the forefront, but only an advisory and support role for stakeholders,
2. Reacting which mostly includes functions where the National Cyber Security Center acts when requested, in response to an incident or a request,
3. Pro-active, when the National Cyber Security Center plays a central role in decision-making and initiatives.

Part 5. Conclusions

Part 5.1. At the European level, the cyber security certification framework is being developed and harmonized, being perceived as an opportunity to develop cyber security, within market representatives, from the perspective of creating a uniform legislative context regulated at the European Union level.

Part 5.2. In Romania, the cybersecurity certification process, involves the participation of two competent authorities:

a) Accreditation Association of Romania, according to European Regulation 765/2008, it is the only national accreditation body. In the cyber security certification activity, it has the role of developing/improving the accreditation programs and executing the accreditation of the conformity assessment bodies.

b) Directorate, according to GEO no. 104/2021, has the following tasks:

   1) Responsibility for authorization, notification and supervision of conformity assessment bodies,

   2) Supervising of suppliers, as well as management of complaint management,

   3) Ensuring compliance with the rules included in the European cyber security certification schemes,

   4) Supervising conformity of ICT products, processes and services with the certificates issued on the national territory,

   5) Monitoring compliance with the obligations of manufacturers or suppliers of products in the country, which carry out self-assessments of conformity, is particularly important,

   6) Providing assistance through expertise and relevant information to Accreditation Association of Romania in the activity of monitoring and supervising the activities carried out by conformity assessment bodies.

Sumar executiv

Partea 1. Fundamentarea studiului

Directoratul Național de Securitate Cibernetică, Asociația de Acreditare din România și Ernst & Young, în cadrul proiectului „Creșterea capacității autorităților competente din România DNSC și RENAR conform Regulamentului european privind securitatea cibernetică 2019/881 (Cybersecurity Act) a elaborat «Studiul privind standardele de certificare a securității cibernetice și analiză comparată» ca răspuns la necesitatea creșterii capacității autorităților competente din România, DNSC și RENAR conform Cybersecurity Act, având ca scop crearea condițiilor optime de adoptare și implementare a schemei de certificare a securității cibernetice a produselor, serviciilor și proceselor TIC.

Obiectivele Studiului sunt:

- Necesitatea implementării unei scheme de certificare a securității cibernetice în România.
- Analiza privind disponibilitatea de implementare a certificării securității cibernetice în rândul entităților (producători și utilizatori) din sectorul public și privat din România.
- Analiza comparată a practicilor de implementare a Cybersecurity Act la nivelul unor state membre ale Uniunii Europene cu experiență din punct de vedere al implementării prevederilor acestuia.

Organizațiile implicate în realizarea studiului sunt:

- Directoratul Național de Securitate Cibernetică
- Asociația de Acreditare din România
- Ernst & Young

Rezultatele principale ale studiului sunt:

- Contribuția la îndeplinirea obiectivului DNSC și RENAR referitor la identificarea disponibilității de implementare în România a schemei de certificare a securității cibernetice, conform Cybersecurity Act;
- Disponibilitatea de aliniere a entităților vizate privind strategia de securitate cibernetică a României, implicațiile financiare, precum și temporale aferente procesului de certificare a securității cibernetice pentru utilizatori și producători ai produselor, serviciilor și proceselor în domeniul tehnologiei informației și a comunicațiilor.

Partea 2. Elemente de actualitate și tendințe în certificarea securității cibernetice

Partea 2.1. Cadrul european de certificare a securității cibernetice

Cadrul european privind certificarea securității cibernetice ar urma să instituie un sistem obiectiv și standardizat de dovezi privind conformitatea cu nivelul de încredere specific produselor evaluate. Certificarea securității cibernetice presupune evaluarea formală a produselor, serviciilor și proceselor TIC de către un organism independent și acreditat în raport cu un set definit de criterii și standarde, din care poate rezulta eliberarea unui certificat indicând conformitatea. Certificatele de conformitate emise sunt recunoscute pe întreg teritoriul UE. Sistem de certificare de securitate cibernetică încurajează dezvoltatorii să încorporeze specificațiile de securitate în etapele inițiale ale proiectării și dezvoltării tehnice a produsului (security by design).

În vederea depășirii barierelor din cadrul pieței digitale unice și creșterea transparenței și comparabilității produselor, serviciilor și proceselor TIC, cu elemente de securitate, UE a adoptat Cybersecurity Act. Documentul prevede un set integrat de măsuri în vederea susținerii eforturilor de contracarare a atacurilor cibernetice și de creștere a posturii de securitate cibernetică la nivel european.

Cybersecurity Act prevede trei niveluri de certificare:

- produsele certificate la nivelul de bază trebuie să dovedească capacitatea de a minimaliza riscurile față de incidente și atacuri cibernetice cunoscute,
- produsele certificate la nivelul substanțial demonstrează capacitatea de a minimiza riscurile de securitate cibernetică desfășurate de actori cu capabilități și resurse limitate,
- produsele evaluate la nivelul ridicat trebuie să demonstreze rezistența la cele mai noi atacuri cibernetice desfășurate de actori cu aptitudini și resurse semnificative.

La nivel european sunt în proces de elaborare trei scheme de certificare:

- Common Criteria based European candidate cybersecurity certification scheme,
- European Union Cybersecurity Certification Scheme for Cloud Services,
- European Union Cybersecurity Certification for 5G Networks.

Partea 2.2. Principalele standarde implicate în certificarea securității cibernetice

Standardele internaționale au fost elaborate cu scopul de a furniza cerințe specifice pentru stabilirea, implementarea, mentenanța și îmbunătățirea continuă a unui sistem de management al securității informațiilor, pentru păstrarea confidențialității, integrității și disponibilității informațiilor prin aplicarea unui proces de management al riscului care să confere încredere părților interesate asupra faptului că riscurile sunt gestionate corespunzător.

Pentru activitatea de certificare în domeniul securității cibernetice a produselor, serviciilor și proceselor TIC, sunt relevante următoarele standarde:

- standardul SR EN ISO/CEI 17065 Evaluarea conformității;
- standardul SR EN ISO/CEI 17025 Cerințe generale pentru competența laboratoarelor de încercări și etalonări, adoptat în limba română în luna martie 2018.

Partea 3. Peisajul pieței de certificare a securității cibernetice din România

Partea 3.1. Metodologie

Studiul de piață realizat de EY cu privire la categoriile de produse, servicii și procese TIC din România și nivelul de asigurare al certificatului de securitate cibernetică.

Scopul acestui studiu este de a facilita adoptarea celor mai eficiente decizii pentru a transpune la nivelul României Cybersecurity Act si cuprinde:

- o cercetare de birou care a condus la identificarea cadrului legislativ;
- un chestionar online, în limba Română, activ în perioada 24 august- 30 septembrie 2022, care a avut ca grup țintă un eșantion de aproximativ 300 de laboratoare de certificare IT, auditori IT, organisme de evaluare a conformității, producători, comercianți, distribuitori și instituții publice ca posibili beneficiari ai produselor certificate din punct de vedere al securității cibernetice.

Partea 3.2. Cadrul normativ național privind securitatea cibernetică

Cadrul normativ în domeniul securității cibernetice, în România, urmează prevederile legislației de la nivelul UE și are ca obiectiv actualizarea și extinderea cadrului normativ în domeniul securității cibernetice, prin crearea cadrului legislativ național de transpunere a Cybersecurity Act.

Partea 3.3. Obiectivul și concluziile chestionarului online

Obiectivul chestionarului online a fost de identificarea categoriilor de produse, servicii și procese TIC prezente pe piața din România, nivelul de asigurare al certificatului de

securitate cibernetică și a obstacolelor întâmpinate în procesul de asigurare. A fost identificată nevoia de creștere a numărului de organisme de evaluare a conformității în domeniul securității cibernetice cât și a numărului de laboratoare de testare a securității cibernetice.

Partea 3.4. Operaționalizarea structurii de certificare și monitorizare din România

Unul din obiectivele principale ale DNSC este de a crea și dezvolta cadrul național de certificare în domeniul securității cibernetice, în cooperare cu instituțiile care au competențe și atribuții în domeniu.

Conform Art.5 lit. i "Funcția de autoritate națională de certificare privind securitatea cibernetică", îi revine Directoratului, care îndeplinește calitatea de organism național ce asigură mecanismele privind evaluarea, certificarea și acreditarea produselor, serviciilor și proceselor în domeniul securității cibernetice, cu următoarele roluri și competențe:

1. Autoritate națională de certificare în domeniul securității cibernetice pentru spațiul cibernetic civil. În această calitate, certifică din punctul de vedere al securității cibernetice tehnologii, produse și servicii;
2. Stabilește norme, cerințe tehnice, standarde și proceduri pentru implementarea Regulamentului (UE) 2019/881;
3. Înființează și gestionează Registrul Național al Activelor, Produselor și Serviciilor de Securitate Cibernetică, denumit în continuare RNAPSSC;
4. Autorizează laboratoarele civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor;
5. Cooperează cu instituțiile naționale și internaționale în domeniul standardizării și acreditarii produselor, serviciilor și proceselor în domeniul securității cibernetice.

În conformitate cu prevederile Art.5 lit q) "Funcția de evaluare și certificare", conferă următoarele atribuții:

5. Evaluează, testează și certifică produse și servicii de securitate cibernetică, pentru nevoi proprii sau la solicitarea instituțiilor din SNAOPSN și/sau a Guvernului;
6. Stabilește reguli, prescripții sau caracteristici pentru activități sau pentru rezultatele acestora din domeniul securității cibernetice, pentru asigurarea unei abordări unitare la nivel național în scopul realizării unui nivel comun ridicat al securității cibernetice;
7. În colaborare cu organismele specializate, participă la elaborarea, aprobarea și adoptarea de standarde în domeniul de competență, pe care le pune la dispoziția publicului;
8. Participă la lucrările comitetelor tehnice naționale și internaționale pentru punerea în aplicare a standardelor și specificațiilor tehnice acceptate la nivel internațional, aplicabile securității rețelelor și a sistemelor informatice, fără a impune sau discrimina în favoarea utilizării unui anumit tip de tehnologie.

Partea 4. Analiză comparată a practicilor de implementare a Cybersecurity Act la nivelul statelor membre: Franța, Germania și Olanda

Partea 4.1. Franța

Agenția Națională de Securitate Cibernetică Franceză este un serviciu cu competențe la nivel național și rol de organism de evaluare a conformității, sarcină efectuată prin Centrul Național de Certificare. Acest Centru este entitatea care certifică și emite certificatele. Principalele activități includ examinarea dosarului de evaluare trimis de sponsor și emiterea unei decizii cu privire la continuarea activității de evaluare. Sponsorul are sarcina de a gestiona procedurile de certificare din partea dezvoltatorului produsului supus evaluării și certificării.

Principalele atribuții ale Autorității naționale de certificare:

a) Certificare sau organism public de evaluare a conformității care emite certificate la nivelul de asigurare înalt;

b) Implementarea cadrului european de certificare a securității cibernetice, incluzând activitățile de reglementare și de cooperare externă;

c) Supraveghere - ce include aplicarea controalelor stabilite de scheme, inclusiv autorizarea și notificarea CAB-urilor, monitorizarea CAB-urilor, supravegherea pieței pentru certificatele emise sub forma unor auto-evaluări a conformității, gestionarea plângerilor, oferirea de sprijin către organismul național de acreditare, supravegherea gestionării vulnerabilităților și *peer review*.

Partea 4.2. Germania

Autoritatea națională de certificare de securitate cibernetică este Oficiul Federal German pentru Securitatea Informațiilor. Așadar îndeplinește funcții importante de certificare, gestionare a supravegherii și răspunde de următoarele sarcini:

- Monitorizarea și asigurarea respectării normelor în cadrul sistemelor europene de certificare de securitate cibernetică;
- Monitorizarea și asigurarea respectării obligațiilor producătorilor în contextul autoevaluării conformității;
- Sprijinirea organismului național de acreditare în monitorizarea și supravegherea activităților organismelor de evaluare a conformității și împuternicirea de acordare a autorizației;
- Monitorizarea și supravegherea în cadrul schemelor europene;
- Monitorizarea evoluțiilor relevante în domeniul certificării de securitate cibernetică.

Partea 4.3. Olanda (Țările de Jos)

Legea adoptării Cybersecurity Act este la stadiul de proiect. În proiectul de lege este preconizat că va fi desemnat Ministerul Economiei ca fiind autoritatea națională de certificare pe securitate cibernetică și să delege acest rol Agenției de Radiocomunicații din Țările de Jos. Totodată proiectul de lege va desemna un Consiliul de Acreditare ca organism național de acreditare, care va avea dreptul de a atesta organismele de evaluare a conformității.

Viitoarea lege prevede ca Agenția de Radiocomunicații din Țările de Jos să aibă competențe suplimentare în ceea ce privește evaluarea certificării cu un nivel ridicat. Legea urmează să stabilească criterii opționale suplimentare pentru o evaluare a cererii de certificare de securitate cibernetică, completând cerințele obligatorii prevăzute în Cybersecurity Act cât și proceduri pentru protecție juridică care sunt în conformitate cu Legea administrativă. De asemenea legea va atribui competență instanței, Colegiului de apel pentru întreprinderi din

Rotterdam, pentru a fi un tribunal judiciar specializat în litigiile privind aprobarea sau respingerea cererilor de certificare de securitate cibernetică.

Potențiale atribuții ale Centrul național de securitate cibernetică în domeniul certificării securității cibernetice a evidențiat următoarele tipuri de activități:

1. De suport/de susținere stabilește funcții pentru Centrul național de securitate cibernetică care nu-l plasează în prim plan, ci doar un rol de consiliere și de sprijin pentru părțile interesate;
2. De reacție ce include în cea mai mare parte funcții în care Centrul național de securitate cibernetică acționează atunci când este solicitat, ca răspuns la un incident sau la o cerere;
3. Rolul pro activ, atunci când Centrul național de securitate cibernetică joacă un rol central în luarea deciziilor și inițiativelor.

Partea 5. Concluzii

Partea 5.1. La nivel european, cadrul de certificare a securității cibernetice este în dezvoltare și armonizare, fiind perceput ca o oportunitate de dezvoltare a securității cibernetice, în cadrul reprezentanților pieței, din perspectiva creării unui context legislativ uniform reglementat la nivelul Uniunii Europene.

Partea 5.2. În România, procesul de certificare a securității cibernetice, implică participarea a două autorități competente:

c) RENAR, conform Regulamentului European 765/2008 aceasta este unic organism național de acreditare. În activitatea de certificare a securității cibernetice are rolul de a dezvolta/perfecționa programele de acreditare și de a executa acreditarea organismelor de evaluare a conformității.

d) DNSC, conform OUG nr. 104/2021, are următoarele sarcini:

1. Responsabilitatea de autorizare, notificare și supraveghere a organismelor de evaluare a conformității;
2. Supravegherea furnizorilor, precum și gestionarea plângerilor;
3. Asigură respectarea normelor incluse în schemele europene de certificare a securității cibernetice;
4. Supravegherea conformității produselor, proceselor și serviciilor TIC cu certificatele eliberate pe teritoriul național;
5. Monitorizarea respectării obligațiilor producătorilor sau furnizorilor de produse din țară, care desfășoară autoevaluări ale conformității este deosebit de importantă;
6. Oferă asistență prin expertiză și informații relevante către RENAR în activitatea de monitorizare și supraveghere a activităților derulate de organismele de evaluare a conformității.

Acronime

ANSSI	Agenția Națională de Securitate Cibernetică Franceză
BSI	Oficiul Federal German pentru Securitatea Informațiilor
BSIG	Oficiul Federal pentru Securitatea Informațiilor
CAB/OEC	Organism de evaluare a conformității
CC	Criterii comune (*în Engl. Common criteria*)
CCN	Centrul Național de Certificare (*în franceză Centre de Certification National*)
CSA	Cybersecurity Act
CE	Comisia Europeană
CEF	Mecanismul pentru Interconectarea Europei (*în Engl. Connecting Europe Facility*)
CESTI	Centrul de Evaluare a Securității în Tehnologia Informației (*în franceză Centres d'évaluation de la sécurité des technologies de l'information*)
COFRAC	Comitatul Francez de Acreditare (*în Franceză Comité français d'accréditation*)
CEN	Comitetul European de Standardizare
DNSC	Directoratul Național de Securitate Cibernetică
eUICC	*în Engl. Universal Integrated Circuit Card*
ECCG	Grupul european pentru certificarea de securitate cibernetică
EUCC	Schema europeană de certificare a securității cibernetice (*în Engl. Common Criteria based European candidate cybersecurity certification scheme*)
EUCS	Schema europeană de certificare a securității cibernetice pentru serviciile de tip cloud (*în Engl. European Union Cybersecurity Certification Scheme for Cloud Services*)
EY	Ernst & Young
ENISA	Agenția Uniunii Europene pentru Securitate Cibernetică (*în Engl. European Union Agency for Cybersecurity*)
ETSI	Institutul European de Standarde în Telecomunicații
ISO	Organizația Internațională pentru Standardizare (*în Engl. International Organization for Standardization*)
ITSEF	Mecanismul pentru evaluarea securității tehnologiei informației (*în Engl. Information Technology Security Evaluation Facility*)
IEC	Comisia Electrotehnică Internațională (*în Engl. International Electrotechnical Commission*)
IoT	Internetul tuturor lucrurilor (*în Engl. Internet of things*)
ITU	**International Telecommunication Union**

IETF	Internet Engineering Task Force
IMM	Întreprinderi mici mijlocii
ISAC	Centrele de analiză și schimb de informații
MRA	Mutual Recognition Agreement
NCCA	Autoritate națională de certificare a securității cibernetice (*în Engl. National Commission for Certifying Agencies*)
NCSC	Centrul național de securitate cibernetică (*în Engl. National Cyber Security Center*)
NBV	Biroul Național pentru Securitate Conexiuni
NATO	Organizația Tratatului Atlanticului de Nord
NL	Regatul Țărilor de Jos
OEC	Organism de Evaluare a Conformității
OWASP	*în Engl. Open Web Application Security Project*
OUG	Ordonanța de urgență a Guvernului
RENAR	Asociația de Acreditare din România
Rva	Oficiul Național de Acreditare
SOGIS	*în Engl. Senior officials group information systems security*
SA	Schemă de acreditare
SEC	Schemă de evaluare a conformității
SGDSN	Secretariatul General pentru Apărare și Securitate Națională Francez
TIC	Tehnologia informației și telecomunicațiilor
UE	Uniunea Europeană (*în Engl. European Union*)
Wbni	Legea privind securitatea rețelelor și a sistemelor informatice
Wgmc	Legea privind cerințele de prelucrare și notificare a datelor
W3C	Consorțium World Wide Web

1. Introducere

Prezentul studiu, elaborat în cadrul proiectului „Creșterea capacității autorităților competente din România DNSC și RENAR conform Regulamentului european privind securitatea cibernetică 2019/881 (Cybersecurity Act)", continuă preocupările autorităților competente din România în domeniul creării condițiilor optime de adoptare și implementare a schemei de certificare a securității cibernetice a produselor, serviciilor și proceselor TIC. În cadrul studiului s-a avut în vedere analiza perspectivelor de implementare a unei scheme de certificare a securității cibernetice, pregătirea autorităților cu atribuții legale pentru implementarea activităților prevăzute de Cybersecurity Act (CSA), disponibilitatea de implementare a certificării securității cibernetice în rândul entităților (producători și utilizatori) din sectorul public și privat din România.

Studiul este structurat în trei secțiuni. Prima secțiune prezintă cadrul european de certificare a securității cibernetice, precum și standardele specifice de referință în domeniu. Această secțiune, cuprinde o serie de aspecte relevante privind procesul de certificare, standardele și autoritățile competente din România cu atribuții în aplicarea prevederilor Cybersecurity Act. Următoarea secțiune expune peisajul pieței de certificare a securității cibernetice în România, precum și particularitățile acesteia. Ultima secțiune cuprinde analiza comparată a practicilor de implementare a Cybersecurity Act la nivelul unor state membre ale Uniunii Europene (UE) mature din punct de vedere al implementării prevederilor acestuia.

Concluziile acestui studiu contribuie semnificativ la îndeplinirea obiectivului DNSC și RENAR referitor la identificarea disponibilității de implementare, în România a schemei de certificare a securității cibernetice, conform Cybersecurity Act. Studiul evidențiază disponibilitatea de aliniere a entităților vizate privind strategia de securitate cibernetică a României, implicațiile financiare, precum și temporale aferente procesului de certificare a securității cibernetice pentru utilizatori și producători ai produselor, serviciilor și proceselor în domeniul tehnologiei informației și a comunicațiilor (TIC).

2. Elemente de actualitate și tendințe în certificarea securității cibernetice

2.1. Cadrul european de certificare a securității cibernetice

„Dacă totul este conectat, totul poate fi atacat" este mesajul transmis de președinta Comisiei Europene (CE) Ursula Von Der Leyen în discursul cu privire la starea UE din 2021. Securitatea cibernetică este o componentă esențială atât pentru asigurarea continuității activităților economice, cât și pentru asigurarea apărării de factori maligni. În contextul dezvoltării digitalizării tuturor sectoarelor de activitate, nevoia creșterii eforturilor de asigurare a securității cibernetice este tot mai stringentă. În acest context piața soluțiilor TIC este fragmentată, complexă și diversă, crescând astfel dificultatea achiziționării produselor potrivite conform destinației de utilizare. La nivel european, există în prezent o diversitate de matrici cu privire la nivelul de securitate, aspect ce creează pe de-o parte confuzie la nivelul consumatorului și pe de altă parte creșterea costurilor de operare la nivelul dezvoltatorului și furnizorului. La nivel național, statele membre UE adoptă diverse reglementări, conducând la adâncirea fenomenului fragmentării pieței digitale unice și ridicând bariere întreprinderilor.

În vederea depășirii barierelor din cadrul pieței digitale unice și creșterea transparenței și comparabilității produselor, serviciilor și proceselor TIC, cu elemente de securitate, UE a adoptat Cybersecurity Act. Documentul prevede un set de măsuri în vederea susținerii eforturilor de contracarare a atacurilor cibernetice și de creștere a posturii de securitate cibernetică la nivel european. Cybersecurity Act cuprinde:

- un mandat permanent al Agenției Europene pentru Securitatea Cibernetică (ENISA), precum și extinderea resurselor alocate instituției în vederea atingerii obiectivelor și sarcinilor setate;
- cadrul european privind certificarea securității cibernetice pentru produse, servicii și procese TIC.

Cadrul european privind certificarea securității cibernetice ar urma să instituie un sistem obiectiv și standardizat de dovezi privind conformitatea cu nivelul de încredere specific produselor evaluate. Certificarea securității cibernetice presupune evaluarea formală a produselor, serviciilor și proceselor TIC de către un organism independent și acreditat în raport cu un set definit de criterii și standarde, care poate rezulta în eliberarea unui certificat indicând conformitatea. Certificatele emise sunt recunoscute pe întreg teritoriul UE. Acest sistem încurajează dezvoltatorii să incorporeze specificațiile de securitate în etapele inițiale ale proiectării și dezvoltării tehnice a produsului (*security by design*).

Beneficiile cadrului european de certificare a securității cibernetice includ creștea încrederii și securității în produse, servicii și procese TIC, acestea oferă transparență utilizatorilor cu privire la nivelul de conformitate cu cerințele declarate. Pentru utilizatori, certificarea contribuie la selectarea produselor, serviciilor și proceselor TIC conforme cu cerințele minime de securitate cibernetică. Pentru furnizori și dezvoltatori, recunoașterea certificatelor la nivel european facilitează extinderea activităților economice în tot spațiul pieței unice digitale.

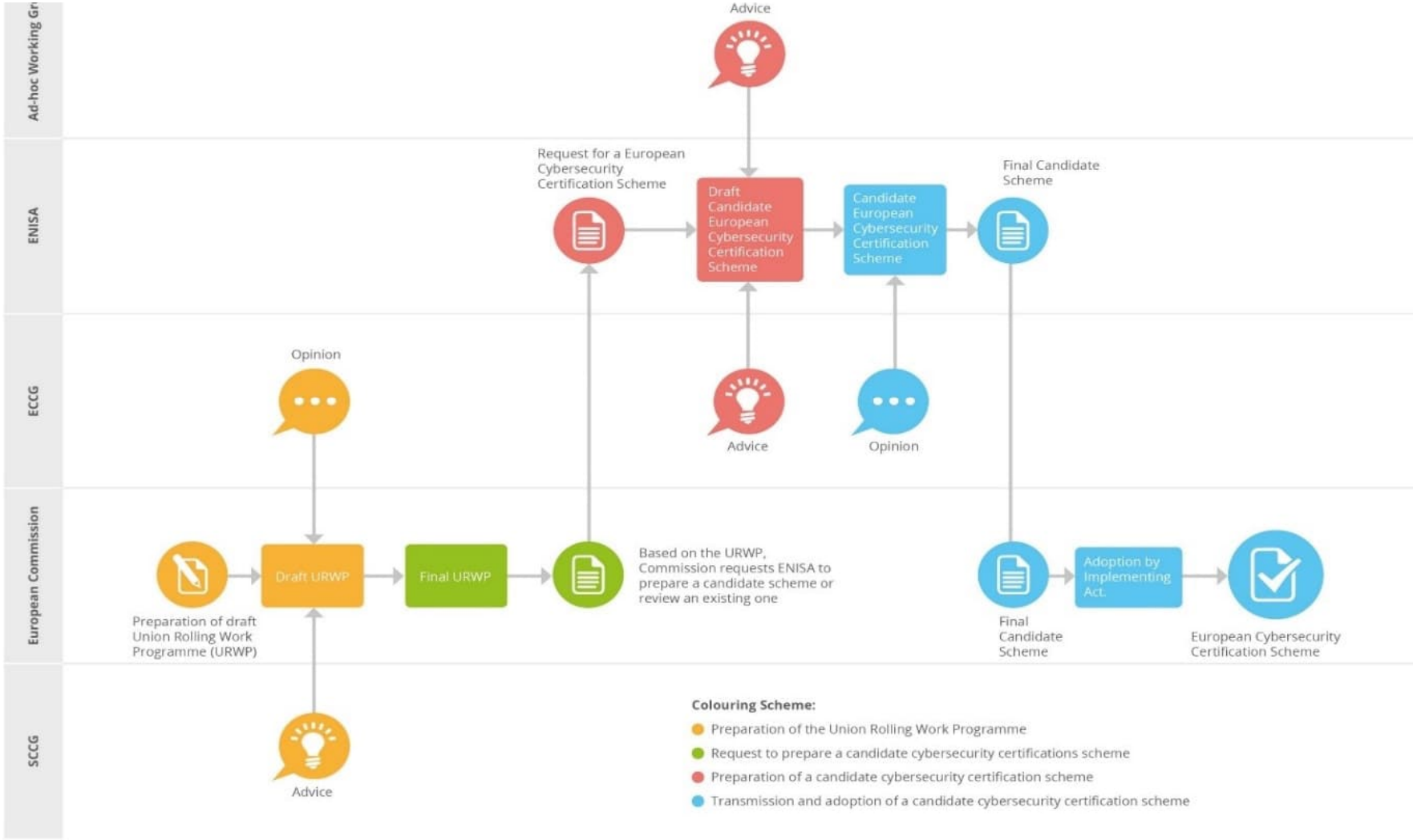
Cadrul european de certificare a securității cibernetice stabilește principalele cerințe orizontale pentru dezvoltarea schemelor de certificare a securității cibernetice. Procedura de dezvoltare a schemelor (Eroare! Fără sursă de referință.) se demarează cu o solicitare trimisă de Comisia Europeană către ENISA, iar aceasta din urmă pregătește o propunere consultându-se cu un grup de experți reuniți ad hoc, dar și cu Grupul European de Certificare a Securității Cibernetice (ECCG). Propunerea de schemă este trimisă Comisiei, care pregătește un regulament de implementare adoptat de un grup comitologic.

Noile scheme de certificare a securității cibernetice trebuie să atingă o serie de obiective de securitate cibernetică, care sunt aliniate cu practicile stabilite în industrie. Datele stocate, transmise sau prelucrate trebuie să fie disponibile, integre, confidențiale și autentice. Principalele obiective de securitate vizate de scheme se referă la controlul accesului, evaluarea vulnerabilităților, monitorizarea activității utilizatorului, reziliența cibernetică, securitate din faza proiectării și implementarea unui sistem de gestionare a actualizărilor (*patch management*).

Gradul de securitate al produselor, proceselor și serviciilor TIC certificate este indicat prin nivelurile de asigurare. Nivelul de asigurare este corespunzător nivelului riscului asociat cu utilizarea preconizată a unui produs, înțeles ca probabilitate și impact al unui incident. Cybersecurity Act prevede trei niveluri: de bază, substanțial și ridicat. Astfel:

- produsele certificate la nivelul de bază trebuie să dovedească capacitatea de a minimaliza riscurile față de incidente și atacuri cibernetice cunoscute. Evaluarea la acest nivel este limitată la analiza documentației tehnice.
- produsele certificate la nivelul substanțial demonstrează capacitatea de a minimiza riscurile de securitate cibernetică desfășurate de actori cu capabilități și resurse limitate. Procesul de evaluare presupune demonstrarea specificațiilor de securitate prin audituri, verificarea testelor funcționale și executarea unor teste de penetrare considerând atacurile cunoscute.
- produsele evaluate la nivelul ridicat trebuie să demonstreze rezistența la cele mai noi atacuri cibernetice desfășurate de actori cu aptitudini și resurse semnificative. Evaluarea produsului trebuie să identifice efectivitatea designului și operațiunilor la nivelul proprietăților proceselor și securității. Evaluarea produselor este efectuată printr-o analiză detaliată a cerințelor unor controale și executarea unor teste de penetrare de către un organism acreditat.

Figura 1: Procesul de dezvoltare a schemelor de certificare a securității cibernetice



Sursa: DNSC

Simultan cu realizarea acestui studiu (octombrie 2022), se definesc la nivel european trei scheme:

I. Common Criteria based European candidate cybersecurity certification scheme (EUCC)

EUCC este precursoarea schemei SOG-IS care permitea recunoașterea mutuală a certificatelor emise în câteva țări europene, preponderent vestice. Noua schemă europeană conferă un cadru pentru evaluarea produselor TIC generale și definește condițiile pentru promovarea produselor certificate la nivelul UE. EUCC este o schemă orizontală, prin acoperirea unei plaje largi de produse TIC. Perioada maximă de validitate a certificatelor este de cinci ani. Schema EUCC este bazată pe standardele Common Criteria (definite conform ISO/IEC 15408) și pe Metodologia Comună de Evaluare (definită conform ISO/IEC 18045). Certificarea în cadrul acestei scheme acoperă nivelurile de asigurare substanțial și înalt. Schema EUCC impune ca fiecare autoritate sau organism care emite certificate la nivelul de asigurare înalt să fie supusă unei evaluări periodice *inter pares*. La momentul realizării studiului, Comisia a trimis în vederea consultării membrilor ECCG propunerea de Regulament de Implementare a schemei EUCC. După această consultare, documentul va fi transmis unui grup comitologic (format în mare parte din aceiași experți precum ECCG) în vederea adoptării.

II. European Union Cybersecurity Certification Scheme for Cloud Services (EUCS)

EUCS permite certificarea securității cibernetice a serviciilor de tip cloud, pentru nivelurile de asigurare de bază, substanțial și înalt. Definirea și referințele pentru terminologie ,pentru serviciile eligibile și pentru certificarea în cadrul acestei scheme provin din standardele ISO/IEC 17788 și ISO/IEC 17000. Deși este diferită de schema EUCC, cele două scheme converg asupra organizării monitorizării conformității și a evaluărilor *inter pares*. Schema EUCS folosește unele principii care au fost definite pentru prima dată în schema EUCC.

III. European Union Cybersecurity Certification for 5G Networks (EU5G)

EU5G este cea mai nouă schemă, fiind încă în primele faze de dezvoltare la nivel de ENISA. Comisia a solicitat pregătirea acestei scheme pe baza Toolbox-ului 5G privind mitigarea riscurilor. Schema de certificare a securității cibernetice a rețelelor 5G va acoperi elementele schemei NESAS GSMA și profilurile de protecție pentru Universal Integrated Circuit Card (eUICC).

2.2. Principalele standarde necesare în certificarea securității cibernetice

Standardele internaționale au fost elaborate cu scopul de a furniza cerințe specifice pentru stabilirea, implementarea, mentenanța și îmbunătățirea continuă a unui sistem de management al securității informațiilor, pentru păstrarea confidențialității, integrității și disponibilității informațiilor prin aplicarea unui proces de management al riscului care să confere încredere părților interesate asupra faptului că riscurile sunt gestionate corespunzător.

Pe durata efectuării studiului au fost identificate standardele relevante pentru activitatea de securitate cibernetică și implicit activitatea subsecvente acesteia, certificarea de securitate cibernetică a produselor, serviciilor și proceselor TIC. Acestea sunt cuprinse în Anexa 1. O parte din standardele relevante identificate încă nu sunt traduse în limba română, acest lucru va fie realizat de către Asociația de Standardizare din România, la solicitarea autorităților competente și cu finanțarea corespunzătoare, în conformitate cu Programul de Standardizare Națională. Programul odată întocmit, va fi comunicat CE și statelor membre potrivit Regulamentului european de standardizare nr. 1025/2012.

În cadrul elaborării studiului am constat că, în general, accesibilitatea și gradul de implementare a standardelor europene și internaționale, la nivel național, crește odată cu adoptarea în limbile naționale ale statelor membre. Mai mult, doar standardele europene sau internaționale adoptate prin publicarea versiunii în limba română pot fi citate în reglementările tehnice naționale, potrivit art. 7 alin (3) coroborat cu art. 15 alin. (1) din

Legea nr. 163/2015 privind standardizarea națională. Iar standardele citate deja trebuie publicate în versiunea română în termen de 2 ani de la intrarea în vigoare a reglementării.

Pentru activitatea de certificare în domeniul securității cibernetice a produselor, serviciilor și proceselor TIC relevante sunt prevederile standardului SR EN ISO/CEI 17065 Evaluarea conformității. Cerințe pentru organisme care certifică produse, procese și servicii, adoptate în limba română în anul 2013 și standardul SR EN ISO/CEI 17025 Cerințe generale pentru competența laboratoarelor de încercări și etalonări, adoptat în limba română în luna martie 2018.

Standardul SR ISO 17025 a fost elaborat cu scopul de a promova încrederea în funcționarea laboratoarelor de evaluare și stipulează cerințe care să permită acestora să demonstreze că acționează competent, coerent și sunt capabile să genereze rezultate valide. Laboratoarele care îndeplinesc acest standard funcționează în acord cu principiile ISO 9001.

Conform standardului menționat, laboratorul vizat trebuie să planifice și să implementeze acțiuni care să trateze riscurile și oportunitățile. Abordarea atât a riscurilor cât și a oportunităților stabilește o bază pentru creșterea eficacității sistemului de management, pentru obținerea unor rezultate îmbunătățite și pentru minimalizarea efectelor negative. Utilizarea și implementarea prevederilor acestui standard va facilita cooperarea dintre laboratoare și autoritățile de acreditare, respectiv de evaluare a securității cibernetice, va asigura trasabilitatea evaluărilor de securitate cibernetică și va contribui la schimbul de informații și experiență și la armonizarea standardelor și a procedurilor. De asemenea, acceptarea rezultatelor între țări este facilitată dacă laboratoarele se conformează acestui document.

Organismele de evaluare a conformității (OEC/CAB), trebuie să implementeze cerințele cuprinse în standardul SR ISO 17065: 2013, cerințe pentru competența, funcționarea consecventă și imparțialitatea organismelor care certifică produse, procese și servicii. Conform standardului amintit mai sus, organismul de certificare trebuie să fie o entitate legală sau o parte definită a unei entități legale astfel încât entitatea legală să fie responsabilă legal pentru toate activitățile sale de certificare.

În conformitate cu prevederile OUG 104/2021, Directoratul Național de Securitate Cibernetică, îndeplinește funcția de autoritate națională de certificare privind securitatea cibernetică. În această calitate, certifică din punctul de vedere al securității cibernetice tehnologii, produse și servicii și autorizează laboratoarele civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice[1].

3. Peisajul pieței de certificare a securității cibernetice din România

3.1. Metodologie

EY, sprijinit de DNSC și RENAR, a realizat un studiu de piață cu privire la categoriile de produse, servicii și procese TIC din România și nivelul de asigurare al certificatului de securitate cibernetică. Scopul acestui studiu este de a facilita elaborarea de măsuri eficiente pentru a transpune la nivel național Cybersecurity Act.

Studiul de piață cuprinde:

- o cercetare de birou care a condus la identificarea cadrului legislativ;
- un chestionar online (Anexa I), în limba Română, activ în perioada 24 august- 30 septembrie 2022, care a avut ca grup țintă un eșantion de aproximativ 300 de laboratoare de certificare IT, auditori IT, organisme de evaluare a conformității, producători, comercianți, distribuitori și instituții publice.

[1] OUG 104/2022 privind înființarea Directoratului Național de Securitate Cibernetică, art. 5, lit. (i).

3.2. Cadrul normativ național privind securitatea cibernetică

În România, cadrul normativ în domeniul securității cibernetice urmează prevederile legislației de la nivelul UE prin:

- Legea 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, care creează cadrul juridic și instituțional de prevenire și răspuns la incidente;
- OUG 104/2021 privind înființarea DNSC, care stabilește guvernanța instituțională pentru îndeplinirea obligațiilor la nivel național;
- Legea 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice și de comunicații de interes național și condițiile implementării rețelelor 5G, care sporește securitatea lanțului de aprovizionare IT&C în domeniul comunicațiilor electronice de tip 5G prin implementarea unor măsuri recomandate în 5G Security Toolbox.

România urmărește actualizarea și extinderea cadrului normativ în domeniul securității cibernetice, prin adoptarea unei legi care să transpună la nivel național Cybersecurity Act.

3.3. Obiectivul și concluziile chestionarului online

Obiectivul chestionarului online a fost de identificarea categoriilor de produse, servicii și procese TIC prezente pe piața din România, nivelul de asigurare al certificatului de securitate cibernetică și a obstacolelor întâmpinate în procesul de asigurare.

Respondenții înregistrați sunt reprezentați 52% de companii private (Figura 2) dintre care majoritatea sunt producători TIC și organisme de evaluare a conformității (Figura 4), din regiunea București-Ilfov (Figura 3).

Figura 3: Respondenții pe categorii de organizații

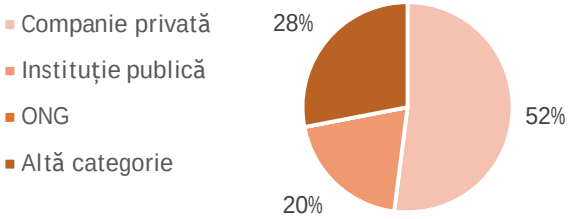
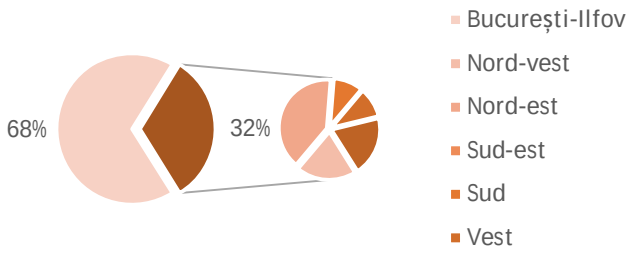
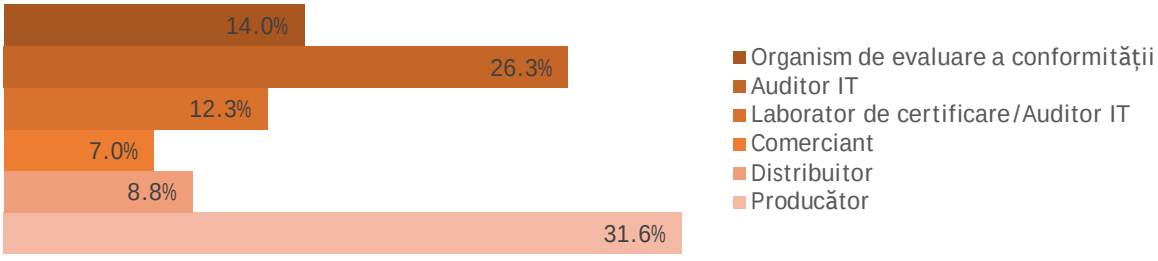


Figura 2: Respondenți pe regiuni la nivelul României



Sursa: EY

Figura 4: Respondenți pe categorii de organizații din domeniul TIC

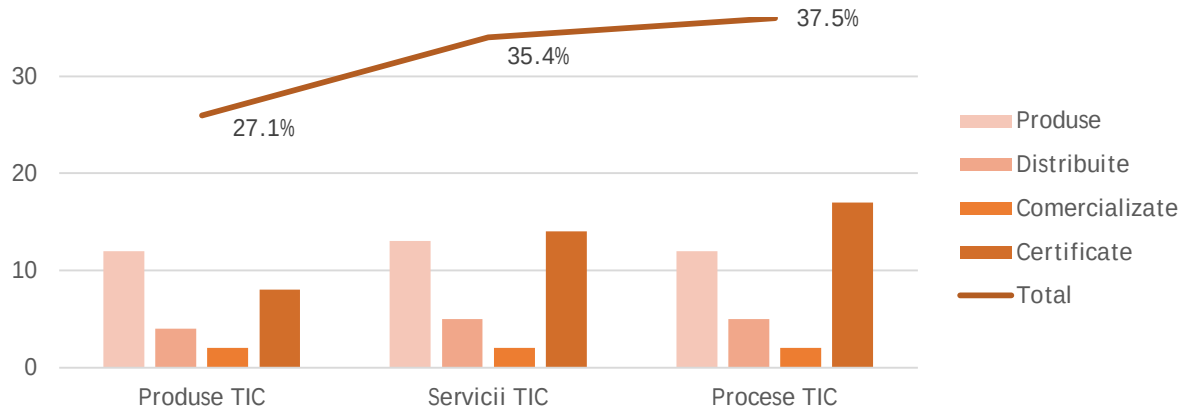


Sursa: EY

Din perspectiva categoriilor de produse, servicii sau procese TIC, respondenții chestionarului sunt echilibrați (Figura 5). În primul rând, am identificat faptul că majoritatea dintre produsele TIC, 56% fac parte din categoria de software TIC, urmată de hardware TIC 33% și materiale procesate 11%. În al doilea rând, serviciile TIC sunt mai echilibrat diseminate, astfel în ordine descrescătoare sunt reprezentate de stocarea informației 27%, transmiterea

informației 26%, prelucrarea informației 25%, extragerea informației 19% și software la comandă 3%. În ultimul rând, procesele TIC sunt de asemenea foarte diversificate pe piața din România, conceperea unui produs TIC/serviciu TIC 25%, dezvoltarea unui produs TIC/serviciu TIC 25%, întreținerea unui produs TIC/serviciu TIC 27%, furnizarea unui produs TIC/serviciu TIC 21% și certificarea sistemelor de management 1%.

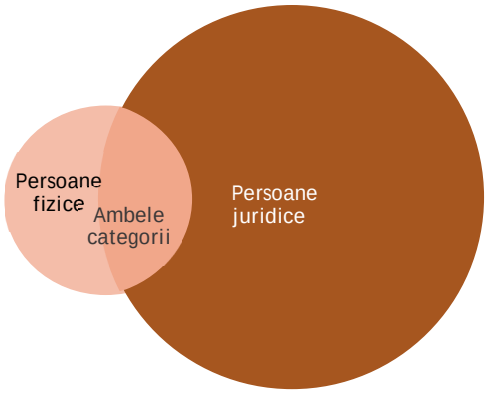
Figura 5: Respondenții din organizații care certifică, produce, distribuie și comercializează produse de securitate cibernetică



Sursa: EY

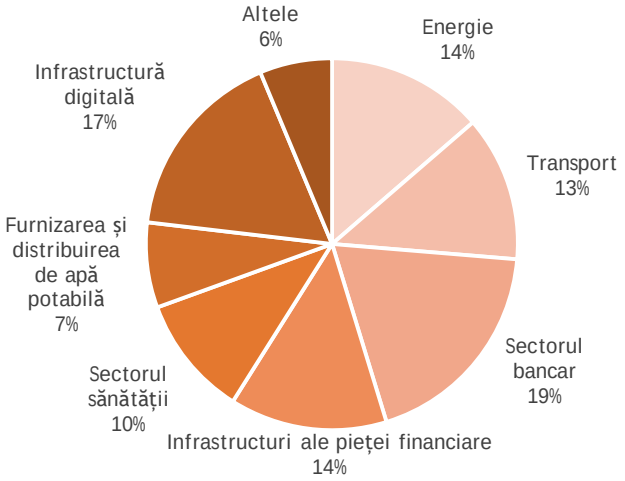
Categoriile de produse, servicii și procese TIC enumerate mai sus, sunt destinate în mare parte persoanelor juridice-56,25%, persoane fizice-18,75%, ambele categorii-25% (vezi Figura 6) și fac parte din sectoarele ilustrate în (Figura 7).

Figura 6: Destinația produselor/proceselor/ serviciilor TIC oferite de organizație



Sursa: EY

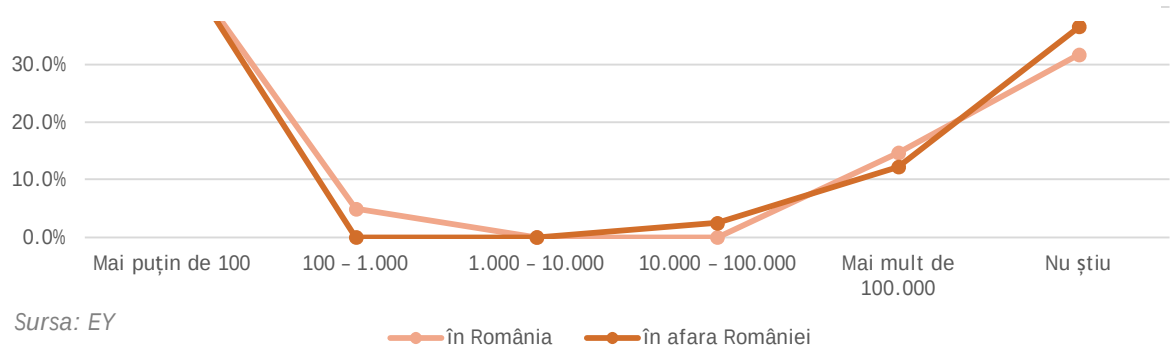
Figura 7: Categoriile de produse, servicii și procese TIC, pe sectoare de activitate



Sursa: EY

În prezent, produsele, serviciile și procesele TIC care sunt concepute, distribuite, comercializate în România sunt certificate în proporție de 66.4%. Regăsiți în figura de mai jos (Figura 8) și o estimare a volumului acestora în funcție de piața destinată.

Figura 8: Unități produse/ distribuite/ comercializate/ certificate în domeniul securității cibernetice, într-un an în România



Sursa: EY

Certificatele de securitate cibernetică pentru produsele, serviciile și procesele TIC utilizate în cadrul organizațiilor respondenților sunt obținute în mare parte intern, la sediul firmei din România, 42%. Iar majoritatea, 58% dintre acestea sunt standard la nivel național sau internațional (global, SUA) (Figura 9). La nivelul organizațiilor 52% din certificatele de securitate cibernetică utilizate sunt la nivelul standardelor (Figura 10).

Figura 10: Proveniența achizițiilor de produselor, proceselor și serviciilor TIC

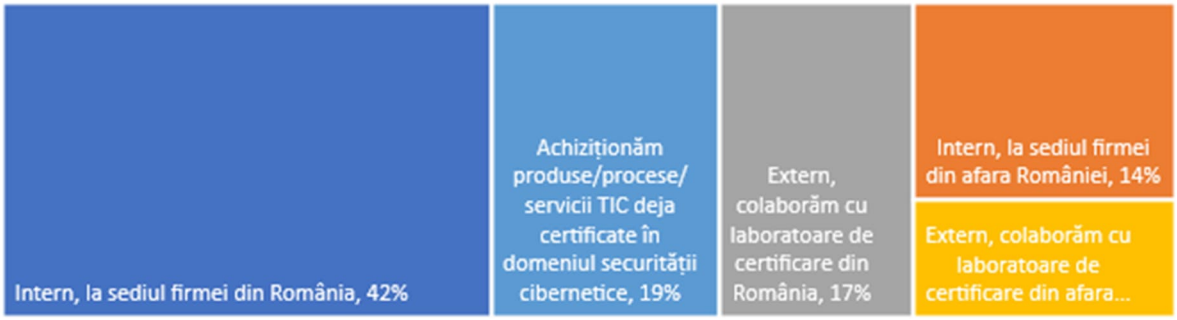
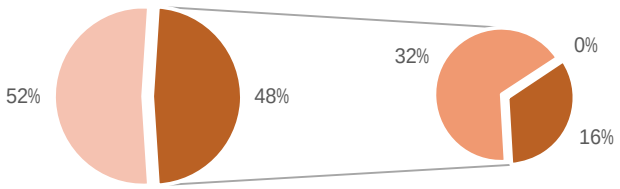


Figura 11: Nivelul de standardizare al certificatelor de securitate cibernetică utilizate în cadrul organizației

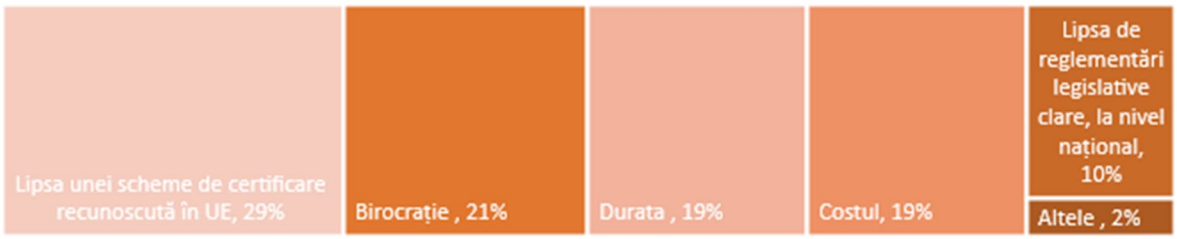


Sursa: EY

Da, toate ▪ Nu știu ▪ Nu ▪ Da, unele

În procesul de certificare, respondenții întâmpină provocări precum lipsa unei scheme de certificare în domeniul securității cibernetice, recunoscută la nivelul UE, lipsa de reglementări legislative clare, la nivelul României, birocrația, precum durata și costul emiterii unei astfel de certificări în condițiile date (Figura 11).

Figura 12: Provocări întâmpinate în procesul de certificare



Sursa: EY

Scala de măsurare a securității cibernetice definită în Cybersecurity act este în mare măsură apreciată ca fiind bine definită de către respondenți (Figura 12). 50% dintre ei consideră că scala poate fi îmbunătățită prin introducerea de elemente obiective, dezvoltarea părții calitative 38% și cantitative 12%. Conform înțelegerii respondenților, certificatele de securitate cibernetică, pe scala de măsurare, sunt apreciate ca fiind: la nivel ridicat 38%, de bază 34% și substanțial 28% (Figura 13).

Figura 14: Scala privind importanța securității cibernetice

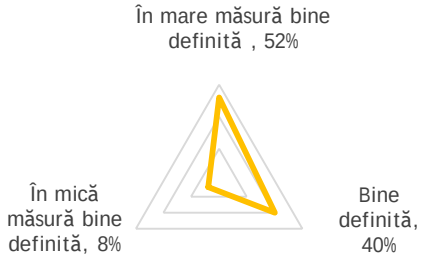
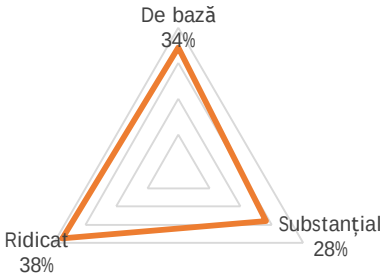


Figura 13: Nivelul de asigurare a certificatelor în domeniul securității cibernetice



Sursa: EY

Cu ajutorul chestionarului online a fost identificată nevoia de creștere atât a numărului de organisme de evaluare a conformității în domeniul securității cibernetice cât și de laboratoare care să desfășoare activități de certificare în domeniul securității cibernetice. 83% dintre respondenți consideră benefică creșterea numărului de organizații care să activeze ca organism de evaluare a conformității în domeniul securității cibernetice, iar 56% consideră organizația pe care o reprezintă ca fiind potrivită pentru rolul de organism de evaluare a conformității în domeniul securității cibernetice. 92% dintre respondenți consideră benefică creșterea numărului de laboratoare care să desfășoare activități de certificare în domeniul securității cibernetice, iar 33% consideră organizația pe care o reprezintă ca fiind potrivită pentru rolul de laborator de certificare în domeniul securității cibernetice.

Operaționalizarea structurii de certificare și monitorizare din România

În contextul Cybersecurity Act, CAB-ul public din cadrul Directoratului va putea activa privind certificarea pentru nivelul de asigurare înalt. Pentru nivelurile de asigurare de bază și substanțial se vor dezvolta organisme de evaluare a conformității private, astfel încât la nivelul autorității de certificare de securitate, activitatea se reduce la gestionarea procesului de certificare, generarea, semnarea și eliberarea certificatelor iar evaluarea de securitate propriu-zisă a produselor va fi realizată de laboratoarele private. Această măsură a fost introdusă în regulament pentru a se asigura că șeful CAB-ului nu influențează serviciul de supraveghere. Conform ISO 17065, CAB-ul din cadrul Directoratului va trebui să aibă competențe cu privire la modul de operare al laboratoarelor aflate în coordonare. Totodată EUCC menționează că organismul care certifică la nivelul înalt trebuie să satisfacă anumite cerințe legate de competența de evaluare a laboratorului din subordine.

Conform OUG 104/2021 unul din obiectivele principale ale DNSC este de a crea și dezvolta cadrul național de certificare în domeniul securității cibernetice, în cooperare cu instituțiile care au competențe și atribuții în domeniu. În acest scop Directoratul îndeplinește conform: Art.5 lit. i ”Funcția de autoritate națională de certificare privind securitatea cibernetică” având calitatea de organism național care asigură mecanismele naționale privind evaluarea, certificarea și acreditarea produselor, serviciilor și proceselor în domeniul securității cibernetice, cu următoarele roluri și competențe:

6. autoritate națională de certificare în domeniul securității cibernetice pentru spațiul cibernetic civil. În această calitate, certifică din punctul de vedere al securității cibernetice tehnologii, produse și servicii;

7. stabilește norme, cerințe tehnice, standarde și proceduri pentru implementarea Regulamentului (UE) 2019/881;
8. înființează și gestionează Registrul Național al Activelor, Produselor și Serviciilor de Securitate Cibernetică, denumit în continuare RNAPSSC;
9. autorizează laboratoarele civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice;
10. cooperează cu instituțiile naționale și internaționale în domeniul standardizării și acreditarii produselor, serviciilor și proceselor în domeniul securității cibernetice.

II) Art.5 lit q) ”Funcția de evaluare și certificare”

9. Evaluează, testează și certifică produse și servicii de securitate cibernetică, pentru nevoi proprii sau la solicitarea instituțiilor din SNAOPSN și/sau a Guvernului;
10. Stabilește reguli, prescripții sau caracteristici pentru activități sau pentru rezultatele acestora din domeniul securității cibernetice, pentru asigurarea unei abordări unitare la nivel național în scopul realizării unui nivel ridicat al securității cibernetice;
11. În colaborare cu organismele specializate, participă la elaborarea, aprobarea și adoptarea de standarde în domeniul de competență, pe care le pune la dispoziția publicului;
12. Participă la lucrările comitetelor tehnice naționale și internaționale pentru punerea în aplicare a standardelor și specificațiilor tehnice acceptate la nivel internațional, aplicabile securității rețelelor și a sistemelor informatice, fără a impune sau discrimina în favoarea utilizării unui anumit tip de tehnologie.

Totodată conform art. 18 din OUG 104/2021 privind înființarea DNSC funcționarea laboratoarelor civile autorizate ce efectuează activități de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice este condiționată de obținerea prealabilă a unei autorizații din partea DNSC, cu o perioadă de valabilitate de maxim 3 ani. Acordarea, prelungirea, suspendarea sau retragerea autorizației se efectuează în baza regulamentului de autorizare și verificare a laboratoarelor civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice, care este elaborat de DNSC și aprobat prin hotărâre a Guvernului.

Procedura obținerii autorizației de funcționare a laboratoarele este prevăzută în OUG 104/ 2021 art. 18 la alin. (2) - alin.(6). Conform art. 19 OUG 104/ 2021, DNSC exercită controlul activității desfășurate de către laboratoarele civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice și verifică îndeplinirea obligațiilor de către laboratoarele civile în baza regulamentului de autorizare și verificare, putând aplica sancțiuni contravenționale în cazuri cum ar fi: furnizarea de rapoarte sau certificate de testare, evaluare sau certificare de către laboratoare civile neautorizate sau fără autorizație valabilă, utilizarea titulaturii de laborator civil autorizat, fără o autorizație acordată de către DNSC, refuzul laboratorului civil de a se supune controlului declanșat de DNSC.

Astfel, în urma desemnării Directoratului ca NCCA, așa cum am prezentat prin OUG 104/2021 acesta își dorește să fie operațional începând cu adoptarea regulamentului de implementare a EUCC, după care va putea începe alături de RENAR pregătirea programului de acreditare și evaluarea CAB-urilor. Această colaborare este foarte importantă pentru a se asigura că laboratoarele și CAB-urile vor primi acreditarea în timp util. Principalele activități ca NCCA vor fi autorizarea și monitorizarea CAB-urilor care certifică la nivelul înalt și notificarea lor către Comisie (pentru toate nivelurile), precum și monitorizarea producătorilor și deținătorilor de certificare. Monitorizarea CAB va putea fi realizată prin audituri fizice, iar obiectivul principal va fi de a se asigura entitatea dispune de competențele tehnice și de management necesare, elemente care să asigure buna desfășurare a activităților de certificare. Monitorizarea nu va fi extinsă la laboratoare decât dacă există suspiciuni cu privire la activitatea neconformă a CAB-ului. Dar acest aspect este o excepție.

Totodată, trebuie avute în vedere prevederile Cybersecurity Act care stabilește separarea activităților de certificare de cele de supraveghere: "*Statele membre se asigură că activitățile autorităților naționale pentru certificarea europeană de securitate cibernetică în legătură cu emiterea certificatelor menționate la articolul 56 alin. (5) și litera (a) și alin. (6) sunt strict separate de activitățile de supraveghere menționate la prezentul articol și că activitățile respective se desfășoară în mod independent*." Acest aspect impune o serie de dificultăți, separarea trebuind făcută pe considerent de ordin bugetar dar și de putere decizională. Pentru acest motiv, în ianuarie 2022 a fost aprobată organigrama DNSC, astfel cum este stabilită în OUG 104/2021 art. 8 alin. 1 lit. i, fiind stabilite în cadrul Direcției Generale Reglementare și Control:

- Direcție Evaluare și Certificare Securitate Cibernetică tehnologii, produse și servicii, în cadrul căreia funcționează: Serviciul Evaluare și Certificare Servicii și Produse, Serviciul Evaluare Tehnologii Mobile, Serviciul Evaluare Internetul Obiectelor, Serviciul Evaluare Inteligență Artificială, Serviciul Evaluare Managementul Accesului și Identității, Serviciul Evaluare Tehnologii Emergente;
- Direcție Verificare și Control , în cadrul căreia funcționează: Serviciul Control, Serviciul Verificare și Monitorizare.

Prin urmare au fost separate cele două activități de certificare și de monitorizare/supraveghere în vederea îndeplinirii obligațiile legale așa cum sunt stabilite în Regulamentul (UE) 2019/88.

Nu în ultimul rând, în vederea demarării procedurii de acreditare a DNSC de către Asociația de Acreditare din România (RENAR), Directoratul va trebui să implementeze proceduri și elemente organizaționale care să integreze cele două standarde din domeniul evaluării conformității, și anume:

- SR EN ISO/CEI 17065: 2013 Cerințe pentru organisme care certifică produse, procese și servicii și
- SR EN ISO/CEI 17067: 2014, Principii fundamentale ale certificării produselor și linii directoare pentru schemele de certificare a produselor.

Aceste proceduri sunt necesare pentru a putea demonstra și imparțialitatea organismelor care certifică produsele, procesele și serviciile de securitate cibernetică. Trebuie menționat și faptul că în cadrul procesului de acreditare a Directoratului trebuie a se va avea în vedere și acreditarea OEC, sarcină efectuată prin Laboratorul DNSC.

Prin urmare, DNSC va autoriza și gestiona organismele de evaluare a conformității, se va ocupa de adoptarea, supravegherea și controlul schemelor europene de certificare implementate, de certificarea produselor, serviciilor și tehnologiilor pentru nivelul de asigurare înalt, precum și de gestionarea certificatelor de securitate cibernetică eliberare pentru nivelul de asigurare comun și substanțial.

4. Analiză comparată a practicilor de implementare a CSA la nivelul statelor membre mature

4.1. Bune practici identificate în Franța

Agenția Națională de Securitate Cibernetică Franceză (ANSSI) este un serviciu francez creat prin decret în iulie 2009[2]. Acest serviciu competent la nivel național este organizat pe lângă Secretariatul General pentru Apărare și Securitate Națională (SGDSN), autoritatea responsabilă cu asistența prim-ministrului în exercitarea atribuțiilor sale în materie de apărare și securitate națională. ANSSI înlocuiește Departamentul de Securitate a Sistemelor Informaționale Centrale, creat prin decret în iulie 2001. Astăzi, ANSSI are în continuare misiunea de a apăra sistemele informaționale ale statului, dar este responsabilă și de consilierea și sprijinirea administrațiilor și operatorilor privați de importanță vitală.

ANSSI se angajează să se asigure că administrațiile publice, serviciile publice și întreprinderile pot profita din plin de o digitalizare sigură și de încredere. Securitatea cibernetică este considerată în Franța o prioritate națională și una care îi privește acum pe fiecare dintre cetățenii săi. Rolul ANSSI este de a promova un răspuns coordonat, ambițios și proactiv la problemele de securitate cibernetică în Franța, de a conduce acțiuni de creștere a gradului de conștientizare, precum și de a răspândi viziunea și expertiza franceză și valorile europene în străinătate.

ANSSI este înființată prin Decretul nr. 2009-834 din 7 iulie 2009[3]. Articolul 2 privind înființarea ANSSI, însărcinează instituția, prin delegare de la Primul ministru, de a aproba centrele de evaluare și certificarea de securitate oferită de produsele și sistemele de tehnologie a informației prevăzute de Decretul nr. 2002-535 din 18 aprilie 2002[4]. Această prevedere desemnează ANSSI ca autoritatea națională privind certificarea în sistemele Common Criteria și SOG-IS. ANSSI este împărțită în patru departamente, respectiv Administrație, Expertiză, Operațiuni și Strategie (Eroare! Fără sursă de referință.14). Activitatea de certificare este plasată în Departamentul de Expertiză, în cadrul Diviziei Produse și Servicii de Securitate (PSS). Această Divizie este responsabilă cu îmbunătățirea, cantitativ și calitativ, și promovarea ofertei naționale a produselor și serviciilor de securitate. Obiectivul Diviziei de certificare este de a evalua produsele și de a crește transparența nivelului lor de securitate.

Decretul nr. 2002-535 din 18 aprilie 2002 stabilește principalele proceduri și direcții de organizare a sistemului național de certificare a securității cibernetice. Documentul stabilește principalele entități implicate în procesul de certificare, precum și procedurile-cadru pentru efectuarea evaluării și certificării. Acestea sunt Centrul Național de Certificare (*Centre de Certification National* – CCN) care activează în cadrul ANSSI, Centrele de Evaluare a Securității în Tehnologia Informației (*Centres d'évaluation de la sécurité des technologies de l'information* - CESTI), Comitatul Francez de Acreditare (*Comité français d'accréditation* - COFRAC), precum și dezvoltatorul și sponsorul (*commanditaire*) care solicită certificarea.

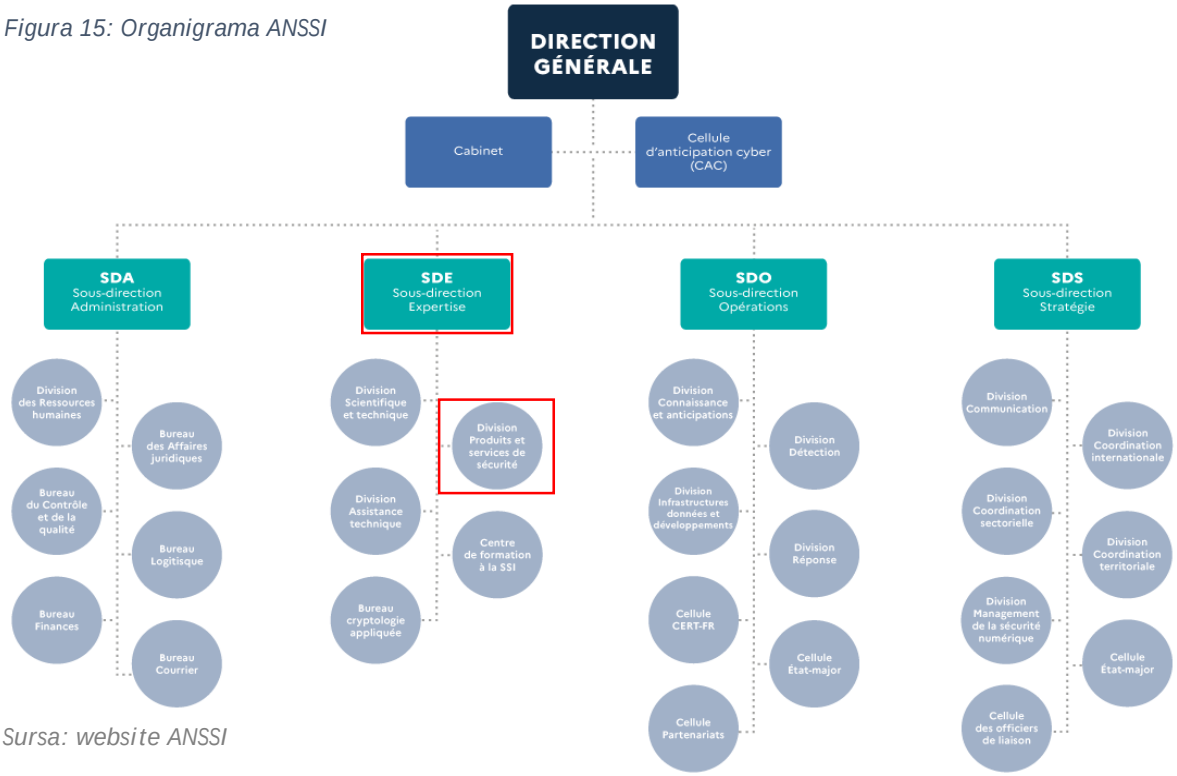
În primul rând, ANSSI are rolul de organism de evaluare a conformității (CAB), sarcină efectuată prin CCN. Acest Centru este entitatea care certifică și emite certificatele. Principalele activități includ examinarea dosarului de evaluare trimis de sponsor (*commanditaire*) și emiterea unei decizii cu privire la continuarea activității de evaluare. CCN are puterea de a respinge solicitarea de evaluare dacă obiectivele de securitate ale produsului nu sunt definite de manieră pertinentă a respecta procedurile și normele pentru demararea evaluării. Ulterior, după parcurgerea procedurilor de evaluare și emiterea

[2] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020828212
[3] Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020828212
[4] Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000412673/

raportului de evaluare de către laborator, ANSSI evaluează și validează raportul de evaluare și emite un raport de certificare care se poate concluziona cu emiterea unui certificat sau refuzul certificării. Certificatul este semnat de directorul general al ANSSI, atestând faptul că exemplarul de produs supus evaluării corespunde caracteristicilor de securitate specificate (Figura 15).

Managementul CCN-ului este format dintr-un șef tehnic și un manager al calității. Conducerea se ocupă de actualizarea sistemelor de management și de asigurarea unui nivel optim de calitate a activității. În aceeași organizație activează doi manageri însărcinați cu

Figura 15: Organigrama ANSSI



Sursa: website ANSSI

acordarea licențelor pentru laboratoare (ITSEF), precum și monitorizarea lor. În cadrul ANSSI, activitatea de certificare presupune doar gestionarea procesului de certificare, iar evaluarea propriu-zisă a produselor este realizată de laboratoarele private.

În contextul CSA, CAB-ul public din cadrul ANSSI își va continua activitatea privind certificarea la nivelul de asigurare înalt, iar pentru nivelurile de bază și substanțial se vor dezvolta organisme private. Activitatea ANSSI nu va fi foarte afectată de tranziția de la SOG-IS la CSA, majoritatea proceselor fiind compatibile, mai ales pentru nivelul de asigurare înalt. De asemenea, laboratoarele care activează în prezent își vor continua activitatea, fiind necesară însă acreditarea conform noilor criterii stabilite de CSA.

Centrele de Evaluare a Securității în Tehnologia Informației (*Centres d'évaluation de la sécurité des technologies de l'information* - CESTI)[5] efectuează evaluările ca o terță parte, independentă de dezvoltatorii de produse și de sponsori. Acestea trebuie să fie acreditate/evaluate de CCN și, ca atare, trebuie să respecte toate regulile schemei. Un CESTI este alcătuit dintr-o echipă de experți și manageri, cel mai adesea integrați într-o organizație cu vocație mai largă. Criteriile de acreditare impun o imparțialitate a CESTI față de alte activități ale organizației, precum cele de consultanță. Un CESTI trebuie să fie imparțial și independent de orice presiune din exterior. El nu trebuie în niciun caz implicat în dezvoltarea (inclusiv consilierea) și evaluarea aceluiași produs, dar pot oferi consultanță netintită. În procesul de certificare, centrele de evaluare au responsabilitatea redactării unui raport de evaluare, pe care îl trimit sponsorului și ANSSI.

[5] Centres d'évaluation, https://www.ssi.gouv.fr/administration/produits-certifies/cc/les-centres-devaluation/

Conform Decretului nr. 2002-535 din 18 aprilie 2002, centrele de evaluare pot funcționa sub umbrela schemei naționale de certificare a securității cibernetice doar dacă sunt autorizate de ANSSI.

Societatea care solicită această licențiere trebuie să facă dovada conformității față de criteriile de calitate, aptitudinile de aplicare a criteriilor de evaluare și metodologiei corespunzătoare, precum și competențe tehnice de coordonare a evaluării. Autorizarea este emisă de directorul general ANSSI, după consultarea comitetului director privind certificarea. Centrele de evaluare autorizate în afara teritoriului Franței, pe baza unor proceduri similare, sunt recunoscute ca autorizate de către directorul general ANSSI, luând în considerare opinia comitetului director privind certificarea. Există personal dedicat în cadrul ANSSI pentru autorizarea laboratoarelor care doresc să efectueze evaluări în contextul certificării. Atunci când laboratorul dorește să facă parte din schema de certificare, organizația trece prin procesul de obținere a licenței și mai târziu trebuie să îndeplinească anumite sarcini pentru a menține această licență. Personalul ANSSI desemnat are responsabilitatea de a monitoriza activitatea laboratorului și de a gestiona eventualele probleme care pot apărea în procesul de evaluare.

CSA nu menționează obligația de a autoriza laboratoarele. Această cerință este specificată doar pentru CAB-urile care certifică la nivelul înalt. În schimb, schemele pot adăuga astfel de cerințe. Schema EUCC menționează obligația CAB-ului de a aplica filtre laboratoarelor care evaluează la nivel înalt. Laboratoarele care evaluează la toate nivelurile sunt acreditate de COFRAC (Comité français d'accréditation). Laboratoarele trec printr-o formă de evaluare efectuată de CAB-ul public (care activează în subordinea ANSSI) pentru evaluarea conformității la nivel înalt. Pentru nivelurile de bază și substanțial, laboratoarele vor fi notificate de către ANSSI la Comisie, conform CSA. Conform ISO 17065, CAB-ul trebuie să aibă cunoștință cu privire la modul de operare al laboratoarelor aflate în coordonare și cărora le subcontractează partea de evaluare. ISO 17065 nu menționează că laboratoarele trebuie licențiate în nicio situație. În schimb, EUCC menționează că organismul care certifică la nivelul înalt trebuie să satisfacă anumite cerințe legate de competența de evaluare a laboratorului din subordine. ITSEF trebuie să demonstreze că are expertiza și experiența necesare pentru efectuarea activităților de testare (teste de penetrare), aplicarea metodologiei pentru determinarea rezistenței produsului împotriva atacurilor, precum și competențe tehnice pentru Smart Carduri și Dispozitive Hardware[6].

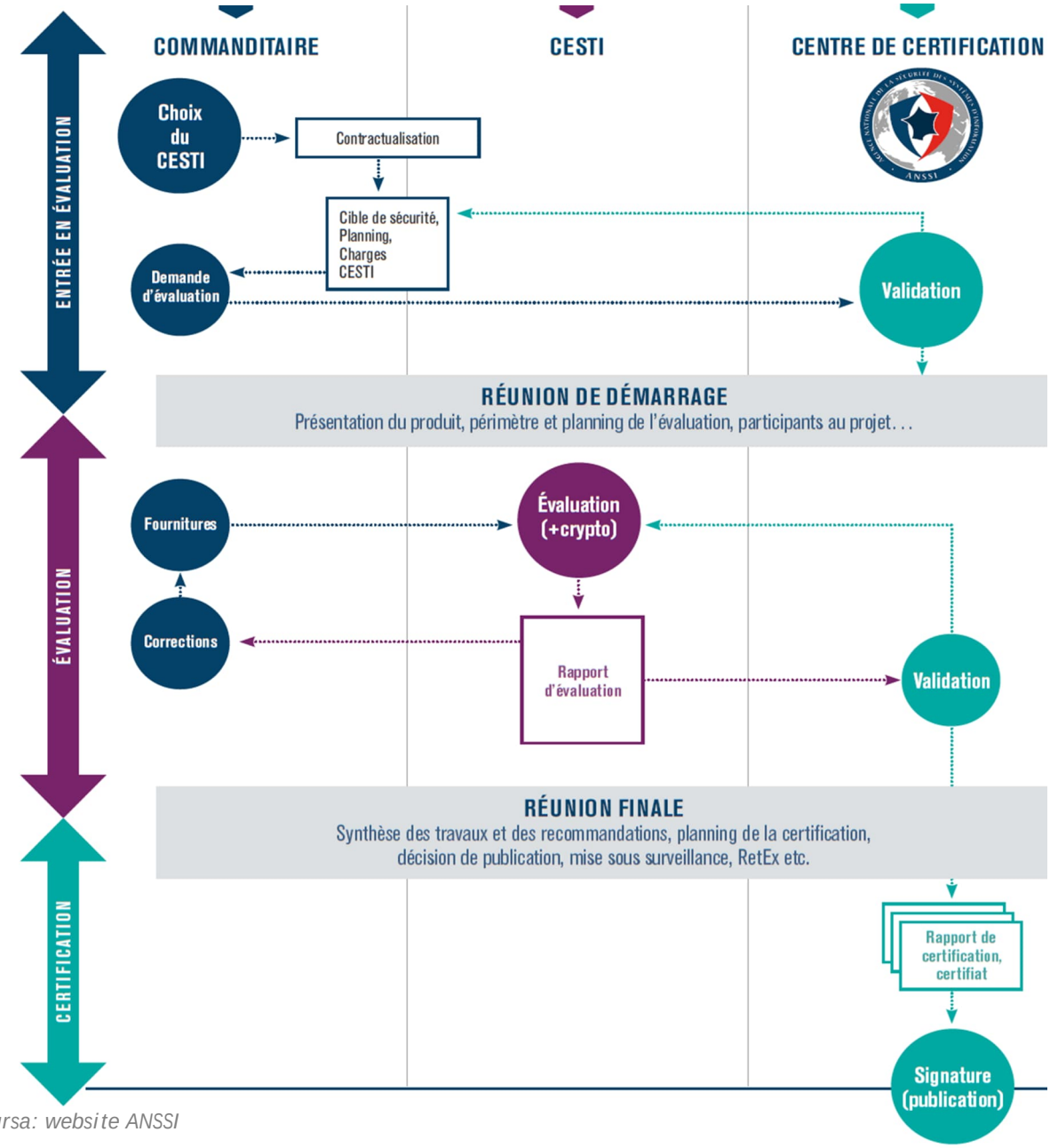
Sponsorul (*commanditaire*) are sarcina de a gestiona procedurile de certificare din partea dezvoltatorului produsului supus evaluării și certificării. Sponsorul solicită ANSSI certificarea prin prezentarea unui dosar de evaluare. Tot această entitate are responsabilitatea de a alege unul sau mai multe centre de evaluare (laboratoare de evaluare), acreditate conform legii. Selecția entității care urmează să efectueze evaluarea se face pe anumite criterii, inclusiv categoria de produs sau sistem de evaluat și obiectivele de securitate (pentru asigurarea domeniului de expertiză); condițiile de protejare a confidențialității informațiilor care vor fi prelucrate în cadrul evaluării; costul și condițiile de plată pentru evaluare; programul de lucru și termenele limită pentru evaluare. În vederea îndeplinirii sarcinilor centrului de evaluare și ANSSI, sponsorul are responsabilitatea de a pune la dispoziție toate informațiile necesare.

CSA, adoptat în iunie 2019, a dat fiecărui stat membru doi ani pentru a desemna autoritatea națională de certificare a securității cibernetice. ANSSI va fi autoritatea de certificare pentru Franța. Statele membre active anterior în domeniul certificării securității cibernetice, inclusiv Franța, trebuie să reformeze o parte din proceduri și elemente organizatorice.

[6] EUCC, pp. 23-24.

ANSSI se va ocupa de autorizarea și notificarea organismelor de evaluare a conformității, de controlul și supravegherea schemelor europene de certificare implementate, dar și, pentru fiecare schemă care o prevede, de eliberarea de certificate pentru nivelul de asigurare înalt.

Figura 16: Procedura de certificare a securității cibernetice în Franța înainte de CSA



Sursa: website ANSSI

ANSSI a fost desemnată NCCA în iunie 2021, dar temeiul juridic pentru activitatea NCCA este în curs de dezvoltare. Sistemul de sancțiuni trebuie să fie pus sub forma unei legi pentru a avea putere executorie. Această întârziere nu este încă problematică deoarece ne aflăm într-o perioadă de tranziție până la operaționalizarea primei scheme (un an după ce va fi adoptată de către grupul comitologic). Încă se lucrează la elaborarea unor proceduri interne, în așteptarea actului de punere în aplicare a EUCC.

NCCA va fi parțial operațională începând cu adoptarea regulamentului de implementare a EUCC. Apoi, va începe, de asemenea, să sprijine COFRAC în vederea pregătirii programului de acreditare și evaluarea CAB-urilor. Această colaborare este foarte importantă pentru a se asigura că laboratoarele și CAB-urile vor primi acreditarea în timp util în perioada de tranziție. În termen de un an de la adoptarea regulamentului de

implementare, vor începe autorizarea și notificarea CAB-urilor. Toate acestea sunt activități de supraveghere pe care NCCA trebuie să le efectueze.

Principalele activități ale NCCA sunt autorizarea și monitorizarea CAB-urilor care certifică la nivelul înalt și notificarea lor către Comisie (pentru toate nivelurile), precum și monitorizarea producătorilor și deținătorilor de certificare. Monitorizarea CAB va fi realizată prin audituri fizice, iar obiectivul principal va fi de a se asigura entitatea dispune de competențele tehnice și de management necesare, elemente care să asigure buna desfășurare a activităților de certificare. Monitorizarea nu va fi extinsă la laboratoare decât dacă există suspiciuni cu privire la activitatea neconformă a CAB-ului. Dar acest aspect este o excepție.

Procedurile de monitorizare a CAB diferă în funcție de durata de valabilitate a autorizării și acreditării inițiale. Dacă avem un proces în care autorizăm entitatea odată la 5 ani, va trebui să o monitorizăm mai des decât am face în scenariul autorizării la fiecare 2 ani sau 18 luni. Monitorizarea este o activitate suplimentară celor de acreditare și autorizare. Pentru auditurile periodice, se vor face eșantioane (5% din produsele certificate într-un an sau cel puțin un produs certificat pe an) sau reactiv pe baza plângerilor primite de CAB. Se vor investiga cazuri specifice, mai degrabă decât audituri periodice din oficiu. Trebuie să existe un echilibru între procesul formal de autorizare și monitorizare.

Monitorizarea CAB-urilor se va efectua pe baza specificațiilor fiecărei scheme. Cerințele vor fi adaptate în funcție de cerințele de notificare și nivelul de asigurare urmărit de fiecare CAB. Pentru EUCC, monitorizarea va fi efectuată de ANSSI pentru nivelul înalt și de COFRAC pentru substanțial. S-a ales această formă de împărțire a sarcinilor în vederea asigurării unei eficiențe în implementarea Regulamentului. ANSSI nu este o autoritate de supraveghere, prin urmare nu poate lua această sarcină pentru toată piața CAB-urilor. De reținut este faptul că supravegherea CAB-urilor care emit certificate la nivelul de asigurare înalt presupune monitorizarea unui alt departament din cadrul ANSSI. Separarea activității de certificare de cea de supraveghere este vitală pentru asigurarea unui standard ridicat al calității efectuării certificărilor.

Franța are în lucru o lege care descrie sistemul de penalizări în situațiile identificării neconformităților. Supravegherea se poate concluziona cu sesizarea unei neconformități. Pe baza rezultatelor investigării, penalizările vor fi aplicate de către un comitet de trei reprezentanți de la ministere diferite. Printre opțiunile prevăzute, sunt incluse retragerea autorizării atunci când nonconformitatea nu este corectată în intervalul de timp stabilit de ANSSI. Se poate aplica o amendă zilnică cel puțin egală cu 15 000 EUR de la momentul notificării deciziei până la remedierea problemei. Există și o penalizare financiară, aplicată proporțional cu nivelul de severitate al neconformității și impactul creat. Se poate aplica o amendă de 150 000 EUR și poate crește la 375 000 EUR în cazul unei încălcări repetate. În cazul unei companii mari, se aplică o amendă între 3% din profitul global anual din anul financiar precedent, până la 5% în cazul unei încălcări repetate.

1. Autoritatea națională de certificare implică patru categorii principale de activități. Prima este cea de certificare sau de CAB public care emite certificate la nivelul de asigurare înalt. Atribuțiile acestuia includ evaluarea conformității (prin evaluarea raportului de evaluare primit de la laborator), aprobarea și monitorizarea laboratorului (sau licențierea), gestionarea vulnerabilităților identificate la nivelul produselor certificate, precum și activitatea de evaluare *inter pares*. Practic, activitatea Centrului Național de Certificare (CCN), rămâne relativ neschimbată după perioada de tranziție la CSA. Aceste sarcini se pot și delega unui CAB privat prin aprobare prealabilă. Chiar dacă îi sunt delegate activitățile de certificare, Biroul de Calificări și Acorduri (BQA) din cadrul ANSSI va monitoriza delegarea, stabilește condițiile de delegare și efectuează evaluarea *inter pares*.
2. O altă componentă a activității de certificare este implementarea cadrului european de certificare a securității cibernetice, incluzând activitățile de reglementare și de cooperare externă. Pe de o parte, acest sub-departament participă la grupuri de lucru europene, inclusiv ECCG și subgrupurile acestuia, participarea în grupul ad hoc de la ENISA, monitorizarea evoluțiilor din domeniul standardizării și adaptarea legii naționale

în linie cu evoluțiile supranaționale. Pe de altă parte, tot această echipă se va ocupa de identificarea orientărilor CSA și de colaborare în vederea recunoașterii certificatelor.

3. A treia componentă este cea de supraveghere. Aceasta include aplicarea controalelor stabilite de scheme, inclusiv autorizarea și notificarea CAB-urilor, monitorizarea CAB-urilor, supravegherea pieței pentru certificatele emise sub forma unor auto-evaluări a conformității, gestionarea plângerilor, oferirea de sprijin către organismul național de acreditare, supravegherea gestionării vulnerabilităților și *peer review*. Totodată, această echipă se va ocupa și de consilierea privind gestionarea penalizărilor. Pe baza investigațiilor, aceștia vor adopta o decizie și vor informa comitetul însărcinat cu aplicarea sancțiunilor.
4. Ultima componentă este cea de întrunire a comitetului de aplicare a sancțiunilor. Legea privind sancțiunile este încă în lucru. Practic, acest comitet este format din reprezentanți de la trei ministere însărcinați cu analiza raportului de investigare emis de departamentul de supraveghere de la paragraful anterior și aplicarea sancțiunilor, după caz.

Cerința CSA de separare a activităților de certificare de cele de supraveghere impune o serie de dificultăți. Regulamentul menționează că separarea trebuie făcută pe considerente bugetare și putere decizională. Această cerință solicitată de CSA este dificil de implementat în contextul în care CAB-ul și partea de supraveghere activează sub același director general. Această măsură a fost introdusă în regulament pentru a se asigura că șeful CAB-ului nu influențează serviciul de supraveghere. ANSSI consideră că separarea bugetului este o cerință imposibil de implementat, deoarece cele două componente funcționează în cadrul ANSSI, care are un buget unitar pentru toată organizația. Pe de altă parte separarea pe considerente de putere decizională se poate gestiona. Componentele enumerate mai sus se vor distribui între departamentele mari ale instituției. Componenta de certificare și cea de implementare a cadrului european de certificare a securității cibernetice vor fi repartizate în Departamentul de Expertiză. Dilema pe care o au la acest moment este dificultatea identificării unui departament pentru activitățile de supraveghere. Activitatea de supraveghere ar putea fi repartizată în Departamentul de Strategie sau în unul nou. Francezii au luat în considerare și crearea unui nou departament, dar pentru moment nu este clar. Din același motiv dat anterior, într-un an de la punerea în aplicare a Regulamentului de implementare a EUCC, arhitectura instituțională va fi pregătită.

Nivelul de semnare al certificatelor eliberate de ANSSI (CAB-ul public) este în prezent la directorul general. Acest lucru s-ar putea schimba din cauza cerinței CSA de asigurare a independenței între activitățile de supraveghere și de certificare. Probabil această sarcină se va muta la nivelul șefului CAB-ului public. Amplasarea echipei de supraveghere este o altă dilemă de rezolvat. ANSSI consideră că supravegherea și activitatea de certificare nu ar trebui să fie separate în ceea ce privește organizarea și bugetul.

CSA nu limitează numărul de autorități naționale de certificare a securității cibernetice. De exemplu, ANSSI are în vedere desemnarea sarcinii de NCCA pentru schemele specializate către autoritățile sectoriale specializate. Delegarea activităților de supraveghere va depinde foarte mult de maturitatea autorităților sectoriale în cauză. Sunt multe autorități potențiale care ar putea prelua din activitățile de NCCA, deși au nevoie de o perioadă de tranziție în vederea înțelegerii problematicii securității cibernetice. În astfel de cazuri, ANSSI va co-acționa în rolul de NCCA cu entitățile sectoriale. Ulterior, acele autorități ar putea prelua întreg setul de sarcini.

4.2. Bune practici identificate în Germania

Oficiul Federal German pentru Securitatea Informațiilor (BSI) este autoritatea națională de certificare de securitate cibernetică (NCCA), în baza Legii privind securitatea IT 2.0, de creștere a securității sistemelor informatice. Sarcinile NCCA sunt stabilite conform Articolul 58 din Cybersecurity Act.

În calitate de NCCA, BSI îndeplinește funcții importante de certificare și gestionare a supravegherii. Aceste funcții sunt exercitate strict separat și independent unele de altele, în conformitate cu articolul 58 alineatul (4) CSA.

- **Which** supervision activities should be implemented in division SZ (Standardisation, Certification and Cybersecurity of Telecommunication Networks) **and how** should they be implemented?
  - Organisational separation to avoid personnel overlaps and conflict of interests (according to art. 58 para. 4 CSA)
  - Distribution of supervising and certifying responsibilities between the three branches within division SZ
  - also geographically with the new office in Freital/Saxony

Ca parte a activităților sale statutare de supraveghere, în conformitate cu prevederile art. 58 alin.7 CSA, NCCA răspunde de următoarele sarcini:

- Monitorizarea și asigurarea respectării normelor în cadrul sistemelor europene de certificare de securitate cibernetică;
- Monitorizarea și asigurarea respectării obligațiilor producătorilor în contextul autoevaluării conformității;
- Sprijinirea organismului național de acreditare în monitorizarea și supravegherea activităților organismelor de evaluare a conformității și împuternicirea de acordare a autorizației în temeiul articolului 9a din BSIG;
- Monitorizarea și supravegherea NCCA de certificare în BSI în cadrul schemelor europene;
- Monitorizarea evoluțiilor relevante în domeniul certificării de securitate cibernetică.

În îndeplinirea sarcinilor, conform prevederilor articolul 58 alineatul (8) al CSA, NCCA are competențe de a se asigura că toți deținătorii de certificate europene de securitate cibernetică, toți emitenții declarațiilor de conformitate ale UE și toate organismele de evaluare a conformității, respectă dispozițiile sistemelor europene de certificare de securitate cibernetică. De exemplu, NCCA pe componenta de supraveghere, poate:

- să solicite informațiile necesare;
- să efectueze investigații sub formă de audituri;
- să aibă acces în incintă;
- să revoce certificatele de securitate cibernetică
- să impună sancțiuni în temeiul articolului 65 CSA.

NCCA este centru (național) în peisajul european al certificărilor. Un alt domeniu de responsabilitate al NCCA, de supraveghere în cadrul BSI, este cooperarea cu Comisia Europeană, precum și cu NCCA din statele membre europene. În acest caz, atât participarea activă, cât și cea efectivă la Grupul european pentru certificarea de securitate cibernetică (ECCG) al Comisiei Europene, precum și schimbul și evaluarea reciprocă a NCCA europene între ele (articolul 59 din CSA) sunt definite ca sarcini.

NCCA trebuie să asigure fluxul de informații la nivel european. De exemplu, CSA solicită pregătirea unui raport anual care să fie trimis de toate statele membre ENISA și ECCG. În plus, NCCA trebuie să notifice Comisiei, prin intermediul mecanismului stabilit în articolul 61 CSA), pentru fiecare sistem european de certificare de securitate. cibernetică, organismele de evaluare a conformității desemnate pentru eliberarea certificatelor. Acestea sunt apoi enumerate în Jurnalul Oficial al Uniunii Europene la un an de la intrarea în vigoare a unui sistem european.

1. De ce există o separare a managementului certificării și al supravegherii în NCCA?[7]

"Statele membre se asigură că activitățile autorităților naționale pentru certificarea europeană de securitate cibernetică în legătură cu emiterea certificatelor menționate la articolul 56 alin. (5) și litera (a) și alin. (6) sunt strict separate de activitățile de supraveghere menționate la prezentul articol și că activitățile respective se desfășoară în mod independent."

În BSI, această separare este asigurată de locația NCCA de supraveghere și de certificarea NCCA în diferite ministere ale departamentului SZ- Standardizare și certificare. Structurile respective lucrează independent unul de celălalt.

2. Ce certificate eliberează NCCA de certificare în BSI[8]*?*

Prin derogare de la alineatul (4), în cazuri justificate în mod corespunzător, un sistem european de certificare de securitate cibernetică poate prevede ca un certificat european de securitate cibernetică emis în cadrul sistemului respectiv să fie întocmit numai de un organism public. Un astfel de organism este unul dintre următoarele:

(a) o autoritate națională de certificare de securitate cibernetică menționată la articolul 58 alineatul (1); [...]

Articolul 56 alin (6) CSA

În cazul în care un sistem european de certificare de securitate cibernetică menționat la articolul 49 necesită un nivel de asigurare "ridicat", certificatul european de securitate cibernetică în temeiul sistemului respectiv poate fi emis numai de o autoritate națională de certificare de securitate cibernetică sau, în următoarele cazuri, de un organism de evaluare a conformității:

(a) în cazul în care autoritatea națională de certificare de securitate cibernetică și-a dat anterior acordul pentru fiecare certificat european individual de securitate cibernetică emis de un organism de evaluare a conformității;

(b) în cazul în care autoritatea națională de certificare de securitate cibernetică a delegat anterior, în general, sarcina de a emite astfel de certificate europene de securitate cibernetică unui organism de evaluare a conformității.

Pe baza CSA, BSI, în calitate de autoritate națională pentru certificarea de securitate cibernetică, eliberează certificatele pentru nivelul de asigurare "ridicat", astfel cum este definit la articolul 52 alineatul (7) din CSA și precizat în sistemele europene respective de certificare de securitate cibernetică în temeiul articolului 54 din CSA.

3. Ce supraveghează mai exact NCCA[9]*?*

Autoritățile naționale de certificare de securitate cibernetică:

(a) monitorizează și asigură respectarea normelor din cadrul sistemelor europene de certificare de securitate cibernetică menționate la articolul 54 alineatul (1) litera (j), în vederea urmăririi conformității produselor TIC, a serviciilor TIC și a proceselor TIC cu cerințele certificatelor europene de securitate cibernetică emise pe teritoriile lor respective, în cooperare cu alte autorități competente de supraveghere a pieței;

(b) monitorizează și asigură respectarea obligațiilor producătorilor sau furnizorilor de produse TIC, servicii TIC sau procese TIC stabilite pe teritoriul lor care efectuează autoevaluarea conformității, în special obligațiile producătorilor sau furnizorilor respectivi în temeiul articolului 53 alineatele (2) și (3) și a sistemului european de certificare de securitate cibernetică relevant;

[7] Art. 58 alin. (4) CSA
[8] Art. 56 alin (5) CSA
[9] Art. 58 alin. (7) CSA

(c) fără a aduce atingere articolului 60 alineatul (3), asistă în mod activ organismele naționale de acreditare în monitorizarea și supravegherea activităților de evaluare a conformității în sensul prezentului regulament;

(d) supravegherea activităților entităților din sectorul public menționate la articolul 56 alineatul (5).

Art.9a din Legea privind Oficiul Federal pentru Securitatea Informațiilor

"Oficiul Federal este autoritatea națională pentru certificarea de securitate cibernetică în sensul articolului 58 alineatul (1) din Regulamentul (UE) 2019/881. La cerere, Oficiul Federal poate autoriza organismele de evaluare a conformității care își desfășoară activitatea în domeniul de aplicare al Regulamentului (UE) 2019/881 și al secțiunii 9 din prezentul act să ia măsuri, și anume să acționeze în cazul în care sunt îndeplinite cerințele sistemului european relevant de certificare de securitate cibernetică în temeiul articolului 54 din Regulamentul (UE) 2019/881 sau al secțiunii 9 din prezentul act. Fără acordarea autorizației de către Oficiul Federal, organismele de evaluare a conformității nu pot acționa în domeniul de aplicare al Regulamentului (UE) 2019/881."

Sarcinile de supraveghere ale NCCA sunt prevăzute la articolul 58 din CSA și includ, în special, respectarea cerințelor sistemelor europene de certificare de securitate cibernetică. În acest sens, articolul 9a din BSIG prevede că BSI, în calitate de autoritate națională de supraveghere, este responsabilă de acordarea permiselor, fără de care organismele naționale de evaluare a conformității nu pot acționa în cadrul certificării europene de securitate cibernetică. În ceea ce privește supravegherea pieței, sunt verificați, de asemenea, producătorii care emit o declarație de conformitate UE, așa-numita declarație pe proprie răspundere a producătorului pentru nivelul de asigurare "*scăzut*"/de bază.

4. Există alte certificate europene de securitate cibernetică care nu sunt emise de BSI ca NCCA?

"Organismele de evaluare a conformității menționate la articolul 60 eliberează un certificat european de securitate cibernetică menționat la prezentul articol cu un nivel de asigurare "scăzut" sau "mediu" pe baza criteriilor stabilite în sistemul european de certificare de securitate cibernetică adoptat de Comisie în temeiul articolului 49."[10]

BSI în calitate de NCCA care certifică, nu eliberează certificate europene de securitate cibernetică pentru nivelurile de asigurare "scăzute"/de bază și "medii"/substanțiale. Nivelul de asigurare "scăzut"/de bază poate fi emis de producătorii sau furnizorii de produse, servicii și procese TIC cu risc scăzut în cadrul unei autoevaluări a conformității la nivelul UE, în conformitate cu articolul 53 din CSA.

Nivelul de asigurare "mediu"/substanțial este evaluat de organismele private de evaluare a conformității în concordanță cu articolul 60 din CSA pentru a determina dacă produsele TIC, serviciile și procesele TIC reduc la minimum riscurile cunoscute de securitate cibernetică, riscul de incidente de securitate cibernetică și atacuri cibernetice din partea actorilor cu competențe și resurse limitate.

5. Cum se asigură NCCA, autoritate de supraveghere, că certificatele care nu sunt emise prin intermediul BSI în calitate de NCCA, respectă cerințele sistemelor europene de certificare de securitate cibernetică?

În conformitate cu articolul 58 alineatul (8) din CSA și articolul 9a din Legea privind Oficiul Federal pentru Securitatea Informațiilor (BSIG*), BSI, în calitate de NCCA-autoritate de supraveghere, are competențe extinse de a monitoriza și de a asigura respectarea reglementărilor în cadrul sistemelor europene de certificare de securitate cibernetică.*

Acestea includ:

- furnizarea de informații (articolul 58 alineatul (8) litera (a) din CSA coroborat cu articolul 9a alineatul (3) din BSIG);

[10] Articolul 56 din CSA.

- investigații sub formă de audituri (articolul 58 alineatul (8) litera (b) din CSA coroborat cu articolul 9a alineatul (4) din BSIG);
- accesul în sediile organismelor de evaluare a conformității și ale titularilor de certificate europene de securitate cibernetică (articolul 58 alineatul (8) litera (d) din CSA coroborat cu articolul 9a alineatul (5) din BSIG);
- posibilitatea de revocare a certificatelor europene de securitate cibernetică (articolul 58 alineatul (8) litera (e) din CSA coroborat cu articolul 9a alineatul (6) din BSIG);
- luarea măsurilor corespunzătoare și, dacă este necesar, a sancțiunilor (articolul 58 alineatul (8) litera (c) și f) CSA coroborat cu articolul 14 alineatele (2), (3), (4), (5) din BSIG0.

6. Cine poate fi contactat în cazul în care se suspectează încălcări ale CSA sau ale sistemelor europene de certificare de securitate cibernetică?

Autoritățile naționale de certificare de securitate cibernetică:

"Tratarea plângerilor depuse de persoane fizice sau juridice cu privire la certificatele europene de securitate cibernetică emise de autoritatea națională de certificare de securitate cibernetică sau la certificatele europene de securitate cibernetică emise de organismele de evaluare a conformității în concordanță cu articolul 56 alineatul (6) sau în legătură cu declarațiile de conformitate sunt prezentate în acord cu articolul 53 și o anchetă corespunzătoare a obiectului plângerii și informează reclamantul cu privire la evoluția și rezultatul investigației într-un termen rezonabil"[11].

În cadrul BSI, NCCA autoritate de supraveghere se ocupă de plângerile primite.

7. Cine poate raporta o astfel de presupusă încălcare către autoritatea națională competentă?

Articolul 63 alin. (1) CSA

"Persoanele fizice și juridice au dreptul de a depune o plângere la emitentul unui certificat european de securitate cibernetică sau, în cazul în care plângerea este îndreptată împotriva unui certificat european de securitate cibernetică emis de un organism de evaluare a conformității în concordanță cu articolul 56 alineatul (6), la autoritatea națională competentă pentru certificarea de securitate cibernetică."

8. Ce se întâmplă după un astfel de raport?

Articolul 63 CSA

Alin. (2) Autoritatea sau organismul la care a fost depusă plângerea informează reclamantul cu privire la evoluția procedurii și de decizia luată și informează totodată reclamantul cu privire la posibilitatea unei căi de atac eficiente în temeiul art.i 64.

În calitate de NCCA de supraveghere, BSI are competențe extinse în temeiul articolului 58 alineatul (8) din CSA și al articolului 9a din Legea privind Oficiul Federal pentru Securitatea Informațiilor (BSIG), de a monitoriza și de a asigura respectarea reglementărilor în cadrul sistemelor europene de certificare de securitate cibernetică. Acestea includ:

- furnizarea de informații (articolul 58 alineatul (8) litera (a) din CSA coroborat cu articolul 9a alineatul (3) din BSIG);
- investigații sub formă de audituri (articolul 58 alineatul (8) litera (b) din CSA coroborat cu articolul 9a alineatul (4) din BSIG);
- accesul în sediile organismelor de evaluare a conformității și ale titularilor de certificate europene de securitate cibernetică (articolul 58 alineatul (8) litera (d) din CSA coroborat cu articolul 9a alineatul (5) din BSIG);
- posibila revocare a certificatelor europene de securitate cibernetică (articolul 58 alineatul (8) litera (e) din CSA coroborat cu articolul 9a alineatul (6) din BSIG);

[11] Articolul 58 Alin. (7), Litera (f) CSA.

- luarea măsurilor și sancțiunilor corespunzătoare (articolul 58 alineatul (8) litera (c), f) CSA coroborat cu articolul 14 alineatele (2), (3), (4), (5) din BSIG).

9. Există deja dispoziții privind amenzile?

La articolul 14 alineatul (2) nr.10, (3), (4), (5) din Legea privind Oficiul Federal pentru Securitatea Informațiilor (BSIG), au fost definite următoarele sancțiuni administrative:

- organismele de evaluare a conformității care acționează fără acordarea autorității/ permisiunii de către BSI în conformitate cu articolul 9a alineatul (2) teza 2din BSIG;
- producătorii sau furnizorii care nu oferă informații sau sunt incorecte/incomplete, ori nu transmit informații în termen de o lună în registrul online cu lacune de securitate, făcute publice în temeiul articolului 55 alineatul (1) din CSA,
- detectarea unei deficiențe de securitate sau a unor nereguli în temeiul articolului 56 alineatul (8) teza 1 CSA cu privire la care nu sunt furnizate informații, nu complet sau nu imediat

În aceste cazuri, se poate aplica o amendă de până la 500 000 EUR

10. Pentru ce rapoarte nu este responsabilă NCCA ca autoritate de supraveghere din cadrul BSI?

În conformitate cu articolul 58 alineatul (7) din CSA, autoritățile naționale de certificare de securitate cibernetică din statele membre europene sunt responsabile numai pentru certificatele europene de securitate cibernetică emise pe teritoriile lor.

4.3. BRegatul Țărilor de Jos (NL)

4.3.1. Cadrul juridic privind securitatea cibernetică în Țările de Jos și mandatul NCSC

Pentru a pune în aplicare Directiva europeană privind securitatea rețelelor și a informației în legislația olandeză a fost introdusă în anul 2018 Legea privind securitatea rețelelor și a sistemelor informatice (Wbni). Wbni a înlocuit Legea privind cerințele de prelucrare și notificare a datelor(Wgmc).

Wbni codifică și alocă competențele, drepturile și obligațiile CSIRT-ului național și ale CSIRT-urilor sectoriale privind notificarea și coordonarea răspunsurilor la amenințările și incidentele cibernetice. Când un incident de securitate cibernetică apare la un operator de servicii esențiale, aceștia au obligația de a notifica NCSC în calitate de punct central de contact. Furnizorii de servicii digitale trebuie să notifice Ministerul Economiei (Agenția de Telecomunicații) prin intermediul CSIRT-DSP.

Modelul olandez este unul descentralizat, prin care mai multe agenții și ministere au competențe în domeniul securității cibernetice. NCSC din Țările de Jos este parte integrantă din Ministerul Justiției și Securității, iar sarcinile sale decurg în principal din Directiva NIS și din legislația de punere în aplicare a acesteia cum ar fi: punct unic de contact, CSIRT național, punct de sprijin pentru operatorii de servicii esențiale de a lua măsurile necesare pentru a asigura sau a restabili continuitatea serviciilor, centru de analiză tehnică și cercetare privind amenințările și incidentele cibernetice pentru a proteja sau a restabili continuitatea serviciilor și pentru a informa actorii relevanți cu privire la amenințările și incidentele cibernetice, . Printre alți actori cu competențe în domeniu se numără Agenția Națională de Radiotelecomunicații, Serviciul General de Informații și Securitate, Biroul Național pentru Conexiuni de Securitate, Serviciul militar de informații și securitate, precum și Centrul de încredere digitală.

Autoritățile sectoriale specifice sunt, de asemenea, numite în Wbni:

- Centrul olandez bancar este desemnat ca autoritate responsabilă pentru securitatea cibernetică în sectorul bancar și financiar;
- Ministerul Infrastructurii este autoritatea competentă pentru securitatea cibernetică în transportul și distribuția apei;

- Ministerul Sănătății este responsabilă pentru securitatea cibernetică în sectorul sănătății.

4.3.2. Adoptarea legii privind certificarea securității cibernetice în NL

Organismele naționale cu competențe în domeniul certificării și acreditării

Legea adoptării CSA (Uitvoeringswet Cyberbeveiligingsverordening) este la stadiul proiect. Prin proiectul de lege este preconizat că va fi desemnat Ministerul Economiei ca fiind autoritatea națională de certificare pe securitate cibernetică și să delege acest rol Agenției de Radiocomunicații din Țările de Jos. Totodată proiectul de lege va desemna un Consiliul de Acreditare ca organism național de acreditare, care va avea dreptul de a atesta organismele de evaluare a conformității.

Viitoarea lege prevede ca Agenția de Radiocomunicații din Țările de Jos să aibă competențe suplimentare în ceea ce privește evaluarea certificării cu un nivel ridicat. Legea urmează să stabilească criterii opționale suplimentare pentru o evaluare a cererii de certificare de securitate cibernetică, completând cerințele obligatorii prevăzute în CSA cât și proceduri pentru protecție juridică care sunt în conformitate cu Legea administrativă (Awb). De asemenea legea va atribui competență instanței, Colegiului de apel pentru întreprinderi din Rotterdam, pentru a fi un tribunal judiciar specializat în litigiile privind aprobarea sau respingerea cererilor de certificare de securitate cibernetică.

După cum s-a menționat, Agenția de Radiotelecomunicații (Agentschap Telecom) va fi desemnată pentru a îndeplini rolul de Autoritate Națională de Certificare pe Securitate Cibernetică (NCCA) pentru certificarea de securitate cibernetică din Țările de Jos. I se vor acorda competențele de a solicita orice informații necesare de la organismele de evaluare a conformității, de a efectua audituri, de a lua măsuri adecvate în conformitate cu dreptul intern pentru a se asigura că organismele de evaluare a conformității respectă sistemul european de securitate cibernetică. Pentru a-și exercita competențele, Agenția de Radiotelecomunicații poate impune sancțiunile prevăzute în capitolul 5 din Legea administrativă (Awb), inclusiv o penalitate forfetară, penalități periodice sau alte penalități, cu titlu cominatoriu.

Alături de Agenția de Radiotelecomunicații un rol important în materie de securitate cibernetică îl joacă și Serviciul General de Informații și Securitate al Ministerului Afacerilor Interne prin Biroul Național pentru Securitate Conexiuni (NBV). NBV ajută la evaluarea și dezvoltarea de produse de securitate cibernetică sigure, dar are și rolul în dezvoltarea standardelor de securitate cibernetică cât și un rol potențial în domeniul certificării. În plus, o parte din NBV, Autoritatea Națională de Distribuție, este singura responsabilă pentru înregistrarea și distribuirea de dispozitive criptografice. NBV are competențe de a evalua deținătorii de dispozitive criptografice în numele NATO cât și rol de supraveghere a schemei de certificare privind securitatea informatică din NL.

Există o gamă largă de organisme de certificare și laboratoare de testare care operează în Țările de Jos. Organismele de evaluare a conformității sunt acreditate oficial de Oficiul Național de Acreditare (Rva) în domeniul securității informațiilor.

Parteneriatele public-privat joacă un rol substanțial în peisajul olandez în ceea ce privește certificare în domeniul securității cibernetice. Un exemplu este reprezentat de Centrele de analiză și schimb de informații (ISAC).

CSA adoptă un model centralizat, prin care Comisia Europeană și ENISA joacă un rol central în elaborarea și adoptarea certificării în domeniul securității cibernetice. În faza de punere în aplicare a CSA, actorii naționali din statele membre preiau evaluările, acordarea de certificări și sunt totodată responsabili de supraveghere. La nivel național autoritățile din statele membre trebuie să evalueze modul în care se poziționează în noul peisaj și să identifice domeniile în care să își îmbunătățească și să își actualizeze rolul atât la nivel național, cât și la nivelul UE.

În NL există numeroase organisme de evaluare a conformității care operează la nivel internațional. Activitățile acestora la nivel multinațional influențează poziționarea

organismelor de evaluare a conformității, care nu urmăresc doar evoluțiile locale dar au și interesul de a-și consolida relațiile guvernamentale nu doar în Țările de Jos, ci și la nivel transfrontalier.

Organismele de certificare din Țările de Jos sunt orientate către piața locală, dar adesea acestea sunt ramificații ale unui grup mai mare de organisme de certificare, fie sub forma unei rețele, fie aparținând aceluiași grup de societăți, cu birouri și sedii în diferite state membre sau chiar în întreaga lume. Acest lucru are desigur impact și ridică o serie de probleme, cum ar fi faptul că, standardele și sistemele de certificare preferate sunt cele internaționale sau europene. Există, desigur, excepții, atunci când este nevoie de un standard național, cum ar fi cum ar fi, de exemplu, NEN 7510 privind securitatea informațiilor în sectorul asistenței medicale, care este un standard utilizat pe scară largă.

Rolul standardizării în domeniul certificării securității cibernetice și organisme cu competență în domeniul standardizării

Cercetarea și practica au arătat că standardizarea și evaluarea conformității sunt instrumente valoroase pentru îmbunătățirea securității cibernetice. Standardele codifică și adună cunoștințele și cele mai bune practici ale actorilor importanți din domeniul securității cibernetice. Certificarea de către organismele acreditate de evaluare a conformității oferă potențialul unui audit independent efectuat de o terță parte (CAB) și o atestare fiabilă a nivelului de securitate a produselor și proceselor unei organizații.

Există o varietate de organizații care au obiect de activitate elaborarea de standarde printre care și cele de securitate cibernetică. Formal organismele de standardizare, cum ar fi organizația olandeză de standardizare (NEN), CEN, CENELEC și ETSI la nivelul UE, precum și ISO, IEC, și ITU la nivel internațional, lucrează în paralel cu o varietate de organizații, forumuri industriale și consorții precum OASIS, OWASP, W3C, IETF și altele. NEN este activă în elaborarea standardelor naționale în domeniul de securitate a informațiilor și securitate cibernetică.

NEN participă în comitetele tehnice ale organizațiilor europene de standardizare active în domeniu, cum ar fi Comitetul tehnic mixt CEN/CLC/JTC 13 privind securitatea cibernetică și protecția datelor, precum și la nivel internațional în organizații de standardizare, cum ar fi ISO și IEC.

Consiliul Național de Acreditare (Raad voor Accreditatie) joacă un rol important, mai ales că CSA stabilește acreditarea obligatorie pentru organismele de certificare care intenționează să ofere servicii privind sistemele europene de certificare de securitate cibernetică. Organismul național de acreditare va furniza acreditarea în acord cu schemele de certificare stabilite conform CSA. Dincolo de organizațiile formale de standardizare recunoscute de legislația Uniunii, există inițiative și platforme în domeniul standardizării.

În NL funcționează Forumul de standardizare (Forum Standaardisatie), care vizează promovarea interoperabilității și a independenței furnizorilor prin utilizarea unor standarde deschise în zona digitală privind schimbul de date din sectorul public. Un alt exemplu este Platforma pentru standarde de internet (Platform Internetstandaarden), care promovează specificațiile pentru procese și infrastructuri digitale sigure într-o serie de domenii precum sănătatea, confidențialitatea, inteligența artificială și guvernanța internetului.

NL este un lider în digitalizarea societății, folosind infrastructura digitală pentru comunicare între cetățeni și guvern, pentru a oferi asistență medicală și educație și pentru a spori flexibilitatea și mobilitatea la locul de muncă. Pentru a consolida reziliența societății digitale olandeze, guvernul olandez a decis să întărească legislația privind poziția pe care o ocupă NCSC și a fost separat de organizația-mamă – Coordonatorul Național pentru Terorism și Securitate, pentru a deveni o organizație de sine stătătoare. Există în continuare legături strânse între cele două organizații, deoarece un nivel ridicat de cooperare între cele două instituții trebuie să existe și sunt importante pentru a proteja societatea olandeză de amenințările on-și offline.

Datorită numeroaselor aspecte ale securității digitale, peisajul olandez al securității cibernetice este complex și fragmentat fiind implicați mai mulți actori care se concentrează pe diferite aspecte ale rezilienței digitale.

Externalizarea procesului de evaluare a certificării securității cibernetice vs folosirea resurselor interne

Externalizarea procesului de evaluare a certificării nu este unul neobișnuit în NL, existând organizații mici, dar cu expertiză în evaluări tehnice complexe și licențiate, dotate cu laboratoare care efectuează teste de penetrare cât și alte teste de securitate cibernetică. Multe dintre organismele de evaluare a conformității din Țările de Jos aparțin unor organizații care oferă consultanță privind securitatea cibernetică, dar iau măsuri împotriva unor posibile conflicte de interes, cum ar fi separarea unităților și a personalului care lucrează în domeniul consultanței și cei care lucrează la evaluare și certificare în diferite entități juridice. Obligații privind luarea de măsuri în ceea ce privește imparțialitatea, decurg din standardul ISO/IEC 17065 care stă la baza acreditării organismelor de evaluare a conformității.

Atingerea unui nivel ridicat de securitate cibernetică la un produs, sistem sau serviciu este unul dintre factorii evidenți ai securității cibernetice. Demonstrarea unei evaluări de către un organism de certificare independent adaugă încredere și fiabilitate.

În ceea ce privește infrastructurile critice, operatorii de servicii esențiale din Țările de Jos solicită certificarea furnizorilor lor, care provine dintr-o obligație de diligență a OSE impusă de Legea Wbni. Cu toate acestea, certificarea nu este obligatorie, ci doar o preferință.

Strategia națională de securitate cibernetică

În Țările de Jos, Strategia națională de securitate cibernetică (NCSA) a stabilit obiectivele securității cibernetice pentru următorii ani, astfel încât NL să fie avangarda hardware-ului și software-ului securizat. Pentru a atinge un astfel de obiectiv, NCSA recunoaște că standardizarea și certificarea aduc o contribuție importantă la securitatea digitală a hardware-ului și software-ului. Astfel NCSA are în vedere opțiunea de certificare obligatorie pentru anumite grupe de produse pe termen scurt și respectarea treptată a unui tip de sigiliu de tip marcă CE pentru toate produsele conectate la internet pe termen lung.

Organismele de evaluare a conformității

În NL, organismele de evaluare a conformității sunt în favoarea certificării obligatorii, nu numai din punct de vedere comercial, dar și pentru că, în opinia lor, aceasta va armoniza și va crește nivelul de securitate al produselor, sistemelor sau serviciilor.

Organismele de evaluare a conformității și Institutul olandez de standardizare nu sunt parteneri direcți cu NCSC. Experții în standardizare din cadrul NEN recunosc importanța participării NCSC în Comitetele de standardizare ale NEN. În ciuda faptului că nu au o colaborare formală în acest moment, dar recunosc că participarea NCSC la comitetele de standardizare permite NCSC să reprezinte interesele sale.

Organismele de evaluare a conformității sunt interesate să colaboreze cu autoritățile olandeze privind schimbul de informații, sensibilizarea și publicarea de informații despre entitățile certificate.

În Țările de Jos nu numai standardele formale elaborate de organismele de standardizare recunoscute sunt utilizate ca bază pentru certificare. De asemenea, specificațiile elaborate de anumiți furnizori acționează ca standarde de conformitate și pot impune propriile lor condițiile pentru partenerii respectivi. O certificare pe un standard recunoscut necesită o documentație extinsă în plus față de testare, și astfel vor crește costurile totale pentru obținerea certificării. Prin urmare, unele organisme de evaluare a conformității optează pentru a oferi servicii de certificare și pentru standarde non-formale, atunci când, de exemplu, un client are activități cu risc scăzut, este un start-up sau o întreprindere mică mijlocie (IMM).

Standardele de securitate cibernetică utilizate în evaluarea conformității se referă la produse, sisteme de management și servicii. Deși există standarde sectoriale specifice adoptate de organizații, un exemplu caracteristic fiind sectorul bancar, cele mai frecvente sunt generice, neutre din punct de vedere sectorial. Există însă inițiative de elaborare a unei specificații sectoriale specifice pe baza unei standardul generic. Un astfel de standard este NEN 7510, care este adaptarea anului 27001 la informațiile din sectorul sănătății.

De departe, cel mai frecvent utilizat standard de către organismele de evaluare a conformității și clienții acestora este standardul ISO/CEI 27001 privind managementul securității informațiilor.

ISO/IEC 15408 este un standard internațional utilizat pentru evaluarea securității IT. Criteriile comune, permit unui dezvoltator de produse să adapteze o evaluare la nevoile de securitate ale produsului său, prin alegerea unei Evaluation Assurance Level.

Seria de standarde IEC 62443 oferă un cadru pentru abordarea vulnerabilităților de securitate în automatizarea industrială și de control (IACS). Standardele sunt aplicabile în toate sectoarele. Seria IEC 62443 adoptă un domeniu de aplicare destul de larg inclusiv securitatea calculatoarelor, rețelelor, sistemelor de operare, aplicațiilor și a altor sisteme programabile. Standardele acoperă, de asemenea, SCADA care sunt utilizate în mod obișnuit de organizațiile care se ocupă de infrastructuri critice.

Organismele de evaluare a conformității, inclusiv laboratoarele de testare din NL oferă servicii pe baza standardelor și specificațiilor mai sus amintite.

Rolul NSCC în domeniul certificării securității cibernetice

Un inventar al rolurilor potențiale ale NCSC în domeniul certificării securității cibernetice a evidențiat următoarele tipuri de activități:

4. Rolul de suport/de susținere stabilește funcții pentru NCSC care nu-l plasează în prim plan, ci doar un rol de consiliere și de sprijin pentru părțile interesate;
5. Rolul de reacție ce include în cea mai mare parte funcții în care NCSC acționează atunci când este solicitat, ca răspuns la un incident sau la o cerere;
6. Rolul pro activ, atunci când NCSC joacă un rol central în luarea deciziilor și inițiativelor.

Aceste 3 roluri de bază ale NCSC urmează a fi divizate după cum urmează:

- Rolul 1: Facilitator al schimbului de cunoștințe (rol de suport/susținere);
- Rolul 2: Sensibilizare și formare (rol de suport/susținere);
- Rolul 3: Furnizarea de asistență autorității naționale de certificare de securitate cibernetică în îndeplinirea sarcinilor sale (rol de susținere/reacție);
- Rolul 4: Furnizarea de cunoștințe și expertiză în timpul acreditării organismelor de certificare (rol reacție);
- Rolul 5: Contribuie la dezvoltarea standardelor și certificărilor (rol reacție);
- Rolul 6: Dezvoltarea propriei scheme (rol pro activ).

Rolul 1 - Facilitator al schimbului de cunoștințe (rol de susținere)

NCSC joacă în prezent un rol de a oferi o platformă de colaborare în materie de securitate cibernetică. Acest rol se realizează în principal prin intermediul centrelor de schimb și analiză a informațiilor (ISAC). În timp ce NCSC este secretariatul, ISAC-urile reprezintă o responsabilitate comună cu participanții din industrie (pentru organizarea de reuniuni etc.), furnizând astfel un model de guvernanță structurat, dar flexibil. Se preconizează o creștere a rolului NCSC de facilitare a schimbului de informații, a bunelor practici și a instrumentelor de securitate cibernetică. NCSC ar putea servi drept platformă de informare cu privire la noile evoluții și actualizări privind standardele și certificările în materie de securitate cibernetică obținute de la partenerii săi.

În afară de sectoarele vitale, organizații precum organismele de standardizare, organismele de evaluare a conformității și organismul național de acreditare ar beneficia, de asemenea, de tipul de cunoștințe obținute în cadrul diferitelor colaborări ale NCSC.

În mod informal, acest rol poate fi văzut ca un exercițiu de consolidare a capacităților în ceea ce privește evaluarea conformității în domeniul securității cibernetice în Țările de Jos.

Rolul 2 - Sensibilizare și formare (rol de susținere)

Valoarea adăugată a certificării în domeniul securității cibernetice nu este întotdeauna clară pentru piață. Organismele de certificare au arătat faptul că principalul factor care determină o companie să fie certificată este o obligație impusă prin lege. Acest lucru arată clar că beneficiile legate de încredere, fiabilitate, diligență, responsabilitate și, în primul rând, creșterea securității nivelului de securitate a produsului, procesului sau a serviciului certificat, verificat printr-un audit independent efectuat de o terță parte, sunt de cele mai multe ori supravegheate.

Motive pentru care nu se adoptă noi standarde este faptul că acestea sunt relativ recente, costul implementării și al certificării ulterioare sunt relativ ridicate iar raportul cost/beneficiu este unul neclar.

NCSC poate atenua unii dintre acești factori prin creșterea conștientizării și furnizării de informații neutre cu privire la beneficiile anumitor certificări pentru diferite sectoare și poate contribui astfel la adoptarea certificărilor europene în materie de securitate cibernetică.

În acest rol, NCSC poate instrui companiile stabilite în Țările de Jos cu privire la impactul sistemelor europene de certificare a securității cibernetice în fiecare sector de activitate și la modul în care trebuie să te adaptezi la peisajul complex al standardelor din acest domeniu.

Rolul 3 - Furnizarea de asistență autorității naționale de certificare de securitate cibernetică în îndeplinirea sarcinilor sale (rol de susținere/reacție)

Ministerul Economiei va fi autoritatea competentă de certificare în domeniul securității cibernetice, care va delega sarcina Agenției de Radiocomunicații (AT). Deși AT are o experiență îndelungată în materie de supraveghere în domeniul pieței telecomunicațiilor, certificarea securității cibernetice este un domeniu relativ nou și neexplorat pentru AT. În plus, certificarea prin CSA este, de asemenea, relevantă pentru sectoarele și domeniile de aplicare în care AT sau alte agenții au puțină experiență.

NCSC, datorită implicării sale puternice în gestionarea incidentelor, se află în poziția unică de a obține informații valoroase din teren care ar putea fi relevante și pentru certificare, deoarece poate oferi perspective în domenii pentru care ar putea fi elaborate standarde și cele mai bune practici, sau poate stabili care sunt deficiențele unui sistem de certificare existent. Acesta poate aduce informații pentru toate sectoarele vitale (în timp ce AT în prezent are doar o imagine de ansamblu asupra sectoarelor energiei și telecomunicațiilor) și pentru mai mulți parteneri. În plus, NCSC are un tip de relație cu partenerii săi, care diferă de rolul de supraveghere pe care AT îl are în prezent pentru sectorul energetic și al telecomunicațiilor.

NCSC, după cum s-a menționat anterior, este perceput ca un partener de încredere disponibil pentru a-și asista partenerii.

Rolul 4 - Furnizarea de cunoștințe și expertiză în timpul acreditării organismelor de certificare (rol reactiv)

CSA obligă organismele și autoritățile de certificare să obțină acreditarea pentru serviciile lor de certificare. Acreditarea va fi realizată de organismul național de acreditare (RvA) în conformitate cu Regulamentul 765/2008 atât cu resurse interne, cât și externe pentru efectuarea evaluărilor.

RvA pe baza expertizei interne îi permite să aprecieze dacă un organism de evaluare a conformității este competent să efectueze o activitate specifică de analiză a conformității. Expertiza internă nu este neapărat necesară în ceea ce privește criteriile specifice certificării de securitate cibernetică. În domenii care necesită un nivel ridicat de cunoștințe de specialitate, RvA adesea colaborează cu experți independenți care efectuează evaluări în numele său.

NCSC poate colabora cu RvA, în funcție de necesități, furnizând experți pentru a asista RvA în evaluările sale de acreditare. Această colaborare nu trebuie confundată cu supravegherea activității stabilite în articolului 58 alineatul (7) litera (c) CSA, care prevede că autoritatea națională de certificare de securitate cibernetică are competența de "asistarea și sprijinirea activă a organismelor naționale de acreditare în monitorizarea și supravegherea activităților organismelor de evaluare a conformității".

Rolul propus se referă la asistarea RvA în efectuarea evaluărilor cu privire la aspectul dacă un organism de certificare îndeplinește cerințele, în special cele referitoare la expertiza în materie de securitate cibernetică, pentru a primi acreditarea.

Rolul 5 - Contribuția la dezvoltarea standardelor și certificărilor (rol reactiv)

Monitorizarea evoluțiilor și schimbul de cunoștințe pot contribui la adoptarea unei forme mai active în cadrul acestui domeniu. Acest lucru se realizează prin contribuția activă la dezvoltarea standardelor și sistemelor de certificare. În ceea ce privește standardizarea, cât și certificarea, expertiza NCSC este valoroasă prin prisma activităților naționale, europene și internaționale. Elaborarea sau oferirea de consultanță de specialitate și de feedback, va putea conduce la creșterea calității standardelor și a sistemelor, dar va oferi și informații NCSC -ului cu privire la evoluții în acest domeniu, aspecte ce vor consolida profilul său.

NCSC participă la Comitetul pentru securitatea informațiilor, securitate cibernetică și confidențialitate al NEN. Cu toate acestea, participarea ar putea fi făcută într-o manieră mai sistematică, cu o agendă pentru a:

a) identifica noi teme/elemente de standardizare pe baza cartografierii nevoilor partenerilor NCSC;

b)comunica contribuția la activitățile existente ale CEN-CLC/JTC 13 "Securitatea cibernetică și protecția datelor și ISO ISO/IEC JTC 1/SC 27 "Securitatea informațiilor, securitatea cibernetică și protecția vieții private".

Rolul 6 - Dezvoltarea propriei scheme (rol pro-activ)

Schimbul de informații între părțile interesate necesită un anumit nivel de încredere.

În timp ce există deja mecanisme care să asigure schimbul de informații între părțile de interesate din cadrul ISAC-urilor, cu ajutorul protocolului *Traffic Light*, extinderea colaborării și a informațiilor ar necesita modalități mai avansate de consolidare a încrederii. O soluție posibilă pentru NCSC este crearea propriului său sistem de încredere pentru a oferi garanții de tipul expertiză, confidențialitate și valoare adăugată grupului de parteneri.

Un rol potențial pro activ al NCSC este acela de a-și dezvolta propriul său sistem de securitate cibernetică pentru produse și sisteme. Acest lucru ar putea implica fie dezvoltarea unui "standard" intern, pe baza unei combinații de standarde existente.

Eticheta de securitate cibernetică a NCSC-NL ar fi voluntară, iar scopul ar consta în ajutorul acordat partenerilor săi să navigheze prin jungla de standarde și de a sprijini securitatea lanțului de aprovizionare și colaborările internaționale.

5. Concluzii

Cadrul european de certificare a securității cibernetice aflat în curs de dezvoltare și armonizare, este perceput ca o oportunitate de dezvoltare a securității cibernetice, de către reprezentanții pieței, din perspectiva creării unui context legislativ uniform reglementat la nivelul UE.

Procesul de certificare a securității cibernetice în România implică participarea a două autorități competente la nivel național. Prima autoritate este RENAR, conform Regulamentului European 765/2008 aceasta:

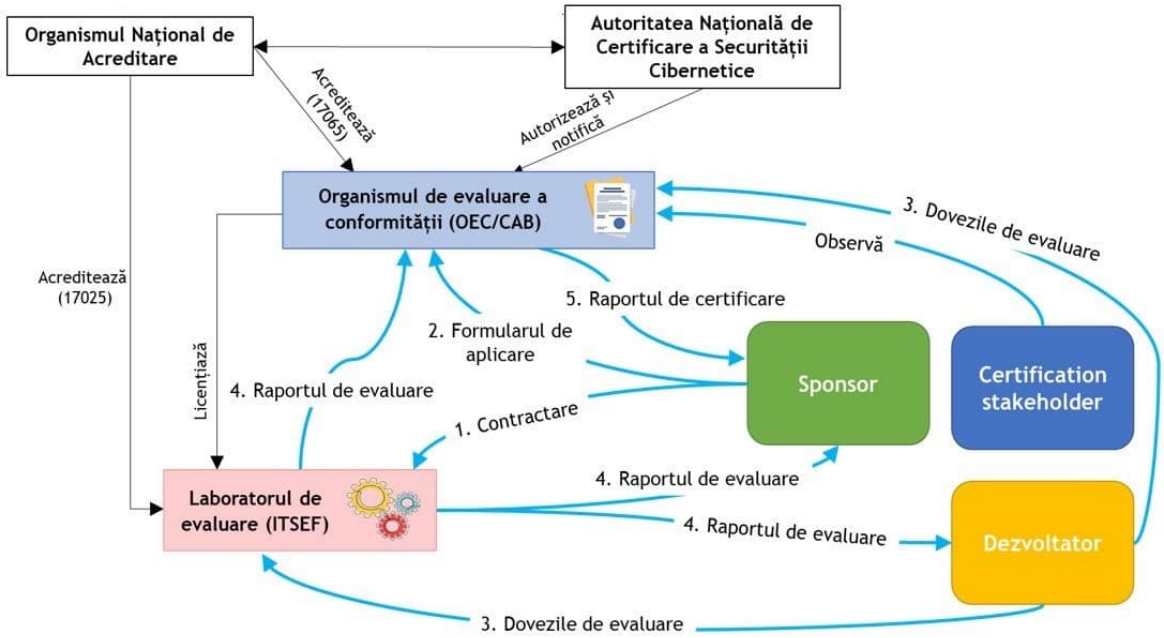
- este unic organism național de acreditare

- în ecuația de certificare a securității cibernetice are rolul de a dezvolta/perfecționa programele de acreditare și de a executa acreditarea organismelor de evaluare a conformității CAB (Figura 17: Schema NCSC).

A doua autoritate este DNSC, conform OUG nr. 104/2021 are responsabilitatea de autorizare, notificare și supraveghere a CAB-urilor, funcția de supraveghere a furnizorilor, precum și de gestionare a plângerilor.

Pentru a fi asigurată imparțialitatea, Regulamentul UE 881/2019 prevede ca activitatea de emitere a certificatelor de securitate cibernetică să fie delimitată de autoritatea de monitorizare/supraveghere din punct de vedere organizațional, buget, structură legală și putere decizională.

Figura 17: Schema NCSC



Sursa: DNSC

În calitate de autoritate națională de certificare a securității cibernetice, DNSC una dintre activitățile principale este de supraveghere și de asigurare a respectării normelor incluse în schemele europene de certificare a securității cibernetice, iar cea mai complexă este monitorizarea conformității produselor, proceselor și serviciilor TIC cu certificatele eliberate pe teritoriul național. De asemenea, responsabilitatea de a monitoriza respectarea obligațiilor producătorilor sau furnizorilor de produse din țară, care desfășoară autoevaluări ale conformității este deosebit de importantă. DNSC oferă asistență prin expertiză și informații relevante către RENAR în activitatea de monitorizare și supraveghere a activităților derulate de organismele de evaluare a conformității.

Directoratul va avea responsabilitatea de a monitoriza și supraveghea activitățile organismelor publice de evaluare a conformității, care desfășoară activitatea pentru nivelul de asigurare *ridicat*. Monitorizarea și supravegherea pentru celelalte două niveluri este realizată de RENAR. Același raționament se aplică și autorizării organismelor de evaluare a conformității, DNSC acoperind entitățile care efectuează activități pentru nivelul de asigurare *ridicat*, iar RENAR va aborda celelalte niveluri.

Gestionarea plângerilor este o activitate importantă a autorității competente, deoarece devine elementul declanșator pentru activitățile de monitorizare. Cybersecurity Act nu este foarte explicit în ceea ce privește responsabilitatea de gestionare a plângerilor.

Plângerile se pot referi la probleme de acreditare a organismelor de evaluare a conformității, de autorizare sau certificare a produselor, serviciilor sau proceselor. În situația în care plângerea este legată de acreditare, RENAR este organismul care soluționează plângerea în conformitate cu Regulamentul (CE) nr. 765/2008, iar în cazul în care plângerea este legată de autorizare, DNSC sau CAB-urile (după caz) vor analiza, monitoriza și soluționa plângerea. În cazul în care plângerea este legată de autorizare, DNSC sau CAB-urile (după caz) vor analiza și soluționa plângerea.

Tot în Figura 17, este ilustrat faptul că organismul de evaluare a conformității (CAB) evaluează laboratoarele, supraveghează procesul de evaluare a produselor, iar pe baza *Rapoartelor de evaluare* emite certificatele. Laboratorul de testare a securității cibernetice (ITSEF) execută evaluările și elaborează rapoartele de evaluare. *Certification stakeholde*r este un utilizator de importanță deosebită care are un set de cerințe specifice cu privire la produsul pentru care se solicită certificarea de securitate cibernetică. Acesta poate fi o federație de bănci, o autoritate administrativă centrală, o companie multinațională etc. Sponsorul este cel care solicită certificarea prin completarea și transmiterea formularului de aplicare către OEC, gestionează întreg procesul de certificare, finanțează certificarea și va deține în final certificatul de securitate cibernetică. Uneori, *certification stakeholder*, sponsorul și producătorul pot fi aceeași entitate.

Procesul de certificare de securitate cibernetică începe cu contactarea directă a laboratorului, prin selecția (dintr-o listă de laboratoare evaluate) de către Sponsor și trimiterea unui formular de solicitare a certificării către CAB (Figura 17, săgețile de culoare albastră). După finalizarea procedurilor de contractare, Dezvoltatorul trimite informațiile specifice pentru evaluare către laboratorul de evaluare (ITSEF) și CAB. La finalizarea activității de evaluare, laboratorul trimite *Raportul de evaluare* către Producător, Sponsor și CAB. După finalizarea analizei, CAB-ul emite un Raport de certificare și Certificatul de securitate cibernetică pe care le trimite Sponsorului. Procesul de certificare poate dura de la 6 luni, la 2 ani sau mai mult, în funcție de complexitatea produsului, serviciului sau procesului pentru care se solicită certificarea.

Odată emise, certificatele de securitate cibernetică, sunt publicate pe site-ul Autorității Naționale de Certificare a Securității Cibernetice pe categorii de produse, servicii și procese, împreună cu nivelul de certificare (comun, substanțial, ridicat).

Tot din conținutul studiului rezultă și faptul că dezvoltarea, precum și adoptarea standardelor relevante care definesc cerințele comune pentru asigurarea unui nivel de securitate rezonabil al produselor, serviciilor și proceselor constituie o prioritate la nivelul autorităților competente naționale. De asemenea, dezvoltarea și efectuarea de teste și analize în vederea certificării de securitate cibernetică, duce la creșterea încrederii utilizatorilor în aceste produse, servicii și procese și odată cu aceasta, disponibilitatea acestora de a le utiliza. Prin urmare procesul de certificare de securitate cibernetică este considerat un beneficiu și din perspectiva optimizării duratei unor misiuni de auditare din punct de vedere al securității cibernetice a rețelelor și sistemelor informatice.

Crearea unui context legislativ uniform la nivel european este de asemenea considerat a constitui o oportunitate de extindere a portofoliului de clienți cât și perspectiva accesării a noi piețe. Astfel, dezvoltatorii de produse, servicii și tehnologii ce vor fi certificate din punct de vedere al securității cibernetice vor avea posibilitatea să-și vândă produsele certificate în toate țările UE și astfel să își extindă portofoliul de clienți.

În stabilirea orizontului de timp necesar operaționalizării autorităților competente pentru realizarea certificării de securitate cibernetică în România este necesar să se țină seama de necesitatea resursei umane înalt calificate în domeniu, a resursei umane și dotărilor specifice în cadrul laboratoarelor testare a securității cibernetice, de realizarea unor analize de risc aprofundate, având în vedere domeniile de utilizare și importanța produselor certificate în cadrul ecosistemului.

În prezent, în România, domeniul securității cibernetice are ca principale reglementări specifice de referință Regulamentul UE 881/2019 respectiv OUG nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică aprobată cu Legea nr. 11/2022. Conform acestor reglementări entitățile cu rol determinant în dezvoltarea, menținerea și îmbunătățirea infrastructurii în domeniul securității cibernetice sunt:

A. Directoratul Național de Securitate Cibernetică – autoritatea națională competentă în domeniul securității cibernetice având responsabilități privind:
   - autorizarea, notificarea și supravegherea organismelor de evaluare a conformității (OEC) – (a se vedea Figura nr. 17),
   - supravegherea furnizorilor de produse, servicii și tehnologii de securitate cibernetică,
   - tratarea plângerilor consumatorilor de produse, servicii și tehnologii de securitate cibernetică.

B. Asociația de Acreditare din România – RENAR, organismul național de acreditare din România care asigură dezvoltarea schemelor specifice de evaluare a conformității și realizează acreditarea OEC din domeniul securității cibernetice (a se vedea Figura nr. 17).

Ținând seama de practicile existente în unele state membre ale UE (Germania, Franța, Olanda), cu experiență anterioară relevantă în domeniul securității cibernetice, dar și de prevederile reglementările aplicabile considerăm că:

Directoratul Național de Securitate Cibernetică trebuie să-și operaționalizeze structurile organizatorice pentru aplicarea prevederilor OUG nr. 104/2021 pentru a putea să aplica schemele europene de certificare de securitate și Regulamentul UE 881/2019.

RENAR trebuie să dezvolte schemele specifice de evaluare a conformității din domeniul securității cibernetice. Acest lucru va fi posibil numai după aprobarea și publicarea pe web-site-ul ENISA a documentelor de referință pentru schemele precizate în prezentul studiu.

6. Anexa I

Chestionar privind standardele de certificare a securității cibernetice

În cadrul proiectului Consolidarea capacității Directoratului Național de Securitate Cibernetică (DNSC) și Asociației de Acreditare din România (RENAR) în conformitate cu Regulamentul privind securitatea cibernetică (UE) 2019/881, pentru implementarea schemei de certificare a securității cibernetice, finanțat de Uniunea Europeană, reprezentată de Agenția Executivă pentru Domeniile Sănătății și Digital (En-HaDEA) prin Mecanismul pentru Interconectarea Europei (En-CEF), ne-am propus realizarea unui Studiu privind standardele de certificare a securității cibernetice și analiză comparată.

Scopul proiectului este consolidarea capacității celor două autorități naționale competente printr-un program multidimensional care include:

- sesiuni de instruire pentru personal,
- campanii de conștientizare și clarificare desfășurate la nivel național,
- studiu și analiză comparată, privind „standardele de certificare a securității cibernetice”,
- evaluare: „inventarierea așa cum este”,
- studiu privind pregătirea României pentru implementarea schemelor de certificare a securității cibernetice în conformitate cu Regulamentul european privind securitatea cibernetică.

Vă invităm să participați la realizarea studiului prin completarea unui chestionar online ce colectează informații utile pentru analiza pieței din România privitor la standardele de certificare a securității cibernetice utilizate. Datele colectate nu vor permite identificarea fiecărui respondent, ci se vor interpreta agregat și anonimizat la nivel central.

Înainte de a începe completarea chestionarului, vă informăm următoarele:

1. Completarea chestionarului se face exclusiv online, până la data de 9 septembrie 2022.
2. Durata estimată de completare de 10 minute.
3. Chestionarul se poate completa de mai multe ori. Răspunsurile vor fi salvate doar după apăsarea butonului ”Trimite”. Completarea chestionarului se poate întrerupe pe parcurs și relua ulterior prin accesarea link-ului (utilizând același dispozitiv de pe care a fost inițiată conexiunea), în cazul în care chestionarul nu a fost finalizat.
4. Pentru a parcurge setul de întrebări, apăsați butonul "Înainte". Pentru a vă întoarce la întrebările anterioare, apăsați butonul "Înapoi" din partea de jos a paginii.
5. Dacă întâmpinați dificultăți de natură tehnică în completarea și transmiterea chestionarului, vă rugăm să ne contactați la adresa nesrin.regep@ro.ey.com

Pentru mai multe informații despre proiect, vă rog să ne contactați la adresa: nesrin.regep@ro.ey.com

Vă mulțumim pentru colaborare!

Datele dumneavoastră cu caracter personal vor fi păstrate de către Ernst & Young până la finalizarea relației contractuale cu Comisia Europeană, după care vor fi distruse iremediabil. Având în vedere scopurile și mijlocele prelucrării datelor cu caracter personal indicate mai sus, aveți următoarele drepturi: dreptul la informare, dreptul de acces la date, dreptul la rectificarea datelor, dreptul la restricționarea prelucrării, dreptul de a vă adresa justiției sau Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal. Aveți dreptul de a vă retrage în orice moment consimțământul acordat. Retragerea consimțământului nu afectează legalitatea prelucrării efectuate înainte de retragerea acestuia. Pentru mai multe detalii referitoare la felul în care sunt prelucrate datele dumneavoastră cu caracter personal, precum și modul de exercitare a drepturilor, vă rugăm să consultați politica de confidențialitate la adresa https://www.ey.com/en_gl/privacy-statement sau să contactați Ernst & Young SRL la adresa Bvd. Ion Mihalache nr. 15-17, etaj 22, Bucharest Tower Center, București Romania, e-mail: gdpr@ro.ey.com.

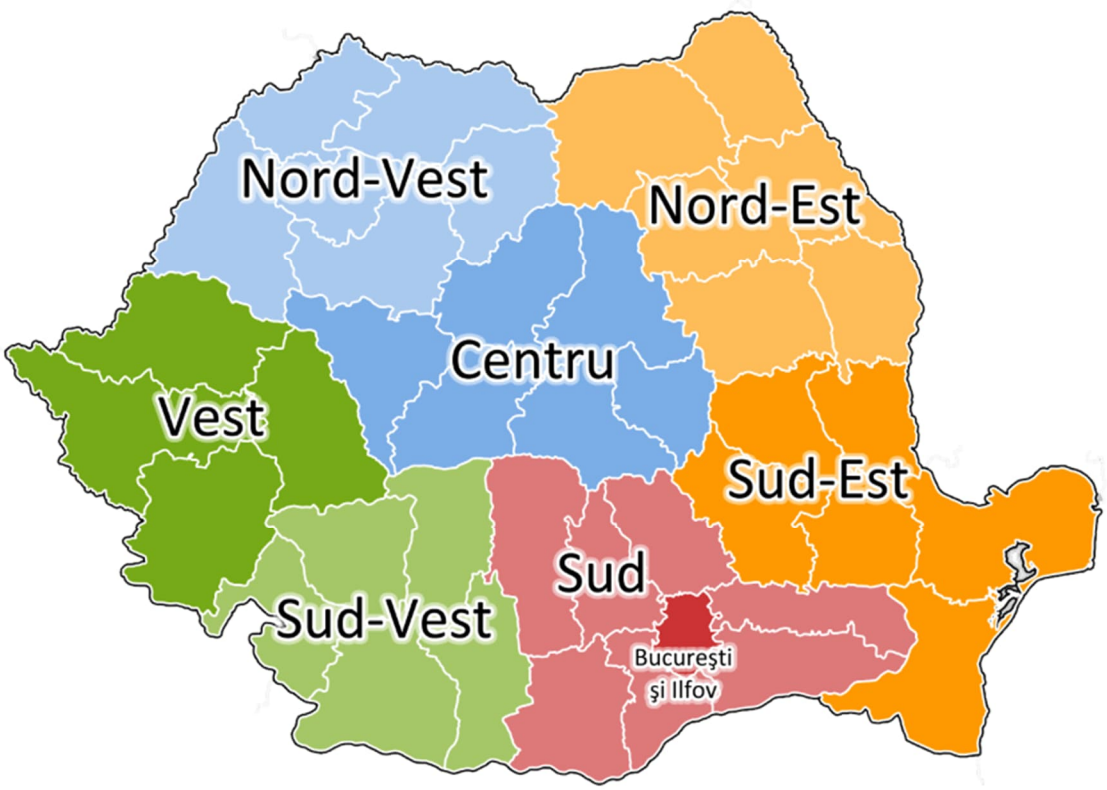
A. Întrebări introductive

1. În care din următoarele categorii se încadrează organizația pe care o reprezentați?
   a. Companie privată
   b. Instituție publică
   c. ONG
   d. Altă categorie *(vă rog specificați)*

2. În care din următoarele categorii din domeniul TIC se încadrează organizația pe care o reprezentați? *(răspuns multiplu)*
   a. Producător de produse/servicii/procese TIC
   b. Distribuitor de produse/servicii/procese TIC
   c. Comerciant de produse/servicii/procese TIC
   d. Laborator de certificare în domeniul securității cibernetice/Auditor IT
   e. Auditor IT
   f. Organism de evaluare a conformității

3. Care este țara de origine a firmei pe care o reprezentați?
   a. România
   b. Străinătate *(vă rog specificați)*

4. Care este regiunea din care face parte organizația pe care o reprezentați? (pentru cine selectează a la AQ3)



   a. Vest
   b. Nord-vest
   c. Nord-est
   d. Sud-est
   e. Sud
   f. București-Ilfov
   g. Sud-vest
   h. Centru

5. Care este aria geografică în care operează organizația pe care o reprezentați? (*răspuns multiplu)*
   a. În România
   b. În UE (excluzând România)
   c. În afara UE

6. Vă rog să completați numele firmei pe care o reprezentați și website: *(opțional)*

B. Categoriile de produse, servicii, procese

1. Ce anume produce/ distribuie/ comercializează/ certifică organizația pe care o reprezentați? *(răspuns multiplu)*
   Produs TIC = un element sau un grup de elemente al unei rețele sau al unui sistem informatic
   Serviciu TIC = un serviciu care constă integral sau preponderent în transmiterea, stocarea, extragerea sau prelucrarea informației prin intermediul rețelelor și al sistemelor informatice
   Proces TIC = un set de activități desfășurate pentru a concepe, a dezvolta, a furniza sau a întreține un produs TIC sau un serviciu TIC
   a. Produse TIC
   b. Servicii TIC
   c. Procese TIC

2. Ce categorii de produse TIC dezvoltați/ distribuiți/ comercializați/ certificați în domeniul securității cibernetice? *(răspuns multiplu)* (pentru cine selectează a la BQ1)
   a. TIC software (ex. servicii de e-mail, platforme pentru munca colaborativă)
   b. TIC hardware (ex. telefon mobil, monitor, hard drive)
   c. Materiale procesate (ex. soluție pentru curățarea monitorului)
   d. Altele *(vă rog specificați)*

3. Ce categorii de servicii TIC dezvoltați/ distribuiți/ comercializați/ certificați în domeniul securității cibernetice? *(răspuns multiplu)* (pentru cine selectează b la BQ1)
   a. Transmiterea informației (ex. call centre, desfășurare sesiuni de instruire)
   b. Stocarea informației (ex. intranet, arhivare, back-up)
   c. Prelucrarea informației (ex. analiză chestionar online, AI)
   d. Extragerea informației (ex. căutare online)
   e. Altele *(vă rog specificați)*

4. Ce categorii de procese TIC dezvoltați/ distribuiți/ comercializați/ certificați în domeniul securității cibernetice? *(răspuns multiplu)* (pentru cine selectează c la BQ1)
   a. Conceperea unui produs TIC/serviciu TIC
   b. Dezvoltarea unui produs TIC/serviciu TIC
   c. Furnizarea unui produs TIC/serviciu TIC
   d. Întreținerea unui produs TIC/serviciu TIC
   e. Altele *(vă rog specificați)*

5. Vă rog exemplificați: (pentru cine selectează d la BQ2 și e la BQ3,BQ4)

6. Cărei categorii de utilizatori îi sunt destinate cu preponderență produsele/ procesele/ serviciile TIC oferite de organizația pe care o reprezentați?
   a. Persoane fizice
   b. Persoane juridice (ex. organizații, întreprinderi, instituții publice)
   c. Ambele categorii

7. În ce sector activează cu preponderență utilizatorii produselor/proceselor/serviciilor TIC oferite de organizația pe care o reprezentați? *(răspuns multiplu)* (pentru cine selectează b,c la BQ6)
   a. Energie
   b. Transport
   c. Sectorul bancar
   d. Infrastructuri ale pieței financiare
   e. Sectorul sănătății
   f. Furnizarea și distribuirea de apă potabilă
   g. Infrastructură digitală
   h. Altele *(vă rog specificați)*

8. În ce măsură sunt certificate în domeniul securității cibernetice produsele/procesele/serviciile TIC produse/distribuite/comercializate de organizația pe care o reprezentați? (pentru cine selectează a,b,c la AQ2)

   0_10_20_30_40_50_60_70_80_90_100 *(roller)*

C. Cantități produse/servicii/procese TIC
   1. Câte unități produceți/ distribuiți/ comercializați/ certificați în domeniul securității cibernetice, într-un an în România?
      a. Mai puțin de 100
      b. 100 – 1.000
      c. 1.000 – 10.000
      d. 10.000 – 100.000
      e. Mai mult de 100.000
      f. Nu știu

   2. Câte unități produceți/ distribuiți/ comercializați/ certificați în domeniul securității cibernetice, într-un an în afara României?
      a. Mai puțin de 100
      b. 100 – 1.000
      c. 1.000 – 10.000
      d. 10.000 – 100.000
      e. Mai mult de 100.000
      f. Nu știu

D. Nivel de asigurare al certificatului de securitate cibernetică
   1. Vă este cunoscut faptul că există multiple scheme de certificare în domeniul securității cibernetice pentru aceleași categorii de produse/procese/servicii TIC? *Ex. EUCC, Franța-ANSSI, Germania-BSI, Italia-OCSI*
      a. Da (*vă rog exemplificați*)
      b. Nu

   2. Cum obțineți certificatele de securitate cibernetică pentru produsele/ procesele/ serviciile TIC utilizate în cadrul organizației pe care o reprezentați? *(răspuns multiplu)*
      a. Intern, la sediul firmei din România
      b. Intern, la sediul firmei din afara României
      c. Extern, colaborăm cu laboratoare de certificare din România
      d. Extern, colaborăm cu laboratoare de certificare din afara României
      e. Achiziționăm produse/procese/servicii TIC deja certificate în domeniul securității cibernetice

   3. Care este denumirea certificatelor de securitate cibernetică utilizate în cadrul organizației pe care o reprezentați?

4. În care din următoarele categorii se încadrează certificatele de securitate cibernetică utilizate în cadrul organizației pe care o reprezentați? *(răspuns multiplu)*
   a. Produse TIC
   b. Servicii Cloud
   c. Rețele 5G
   d. Protecția infrastructurii
   e. Altă categorie *(vă rog specificați)*

5. Certificatele de securitate cibernetică utilizate în cadrul organizației pe care o reprezentați sunt standard?
   a. Da, toate
   b. Da, unele
   c. Nu
   d. Nu știu

6. Care este nivelul de standardizare al certificatelor de securitate cibernetică utilizate în cadrul organizației pe care o reprezentați? *(răspuns multiplu)* (pentru cine selectează a,b la DQ5)
   a. Național
   b. Internațional, vă rog menționați în ce țări/regiune

7. Care sunt provocările pe care le aveți în procesul de certificare? *(răspuns multiplu)*
   a. Lipsa unei scheme de certificare în domeniul securității cibernetice, recunoscută în UE
   b. Durata
   c. Costul
   d. Birocrație
   e. Lipsa de reglementări legislative clare, la nivel național, cu privire la schemele de certificare în domeniul securității cibernetice specifice pentru un anumit produs/serviciu/proces TIC (vă rog specificați produsul/procesul/serviciul)
   f. Altele *(vă rog specificați)*

8. Care estimați că este nivelul de asigurare la care se află certificatele dvs. de securitate cibernetică pe scala de măsurare a securității cibernetice? *(răspuns multiplu)*
   a. De bază *(sunt îndeplinite cerințele de securitate corespunzătoare, la un nivel care urmărește minimizarea riscurilor de bază cunoscute de incidente și atacuri cibernetice)*
   b. Substanțial *(sunt îndeplinite cerințele de securitate corespunzătoare, la un nivel care urmărește minimizarea riscurilor pentru securitatea cibernetică cunoscute și a riscurilor de incidente și atacuri cibernetice desfășurate de actori cu competențe și resurse limitate)*
   c. Ridicat *(sunt îndeplinite cerințele de securitate corespunzătoare, la un nivel care urmărește minimizarea riscului de atacuri cibernetice de ultimă generație desfășurate de actori cu competențe și resurse substanțiale)*

9. Cum apreciați scala de măsurare a securității cibernetice?
   a. În mare măsură bine definită
   b. Bine definită
   c. În mică măsură bine definită

10. Ce îmbunătățiri considerați că s-ar putea aduce scalei de măsurare a securității cibernetice? *(răspuns multiplu)* (pentru cine selectează b,c la DQ9)
    a. Dezvoltarea părții calitative
    b. Dezvoltarea părții cantitative

c. Introducerea unor elemente obiective
d. Altele *(vă rog specificați)*

E. Organisme de evaluare a conformității în domeniul securității cibernetice
Organismele de evaluare a conformității sunt organizații acreditate care efectuează activități de evaluare a conformității, inclusiv etalonare, testare, certificare și inspecție, conform Regulamentului (CE) nr.765/2008.

1. Considerați benefică creșterea numărului de organizații care să activeze ca organism de evaluare a conformității în domeniul securității cibernetice?
   a. Da
   b. Nu
   c. Nu știu

2. Considerați organizația pe care o reprezentați ca fiind potrivită pentru rolul de organism de evaluare a conformității în domeniul securității cibernetice ?
   a. Da
   b. Nu
   c. Nu știu

F. Laboratoare de certificare în domeniul securității cibernetice
Laboratoarele de certificare sunt organizații acreditate care permit organismului de evaluare a conformității să efectueze încercările și testele de laborator necesare certificării la un nivel de înaltă siguranță.

1. Considerați benefică creșterea numărului de laboratoare care să desfășoare activități de certificare în domeniul securității cibernetice?
   a. Da
   b. Nu
   c. Nu știu

2. Considerați organizația pe care o reprezentați ca fiind potrivită pentru rolul de laborator de certificare în domeniul securității cibernetice?
   a. Da
   b. Nu
   c. Nu știu

G. Date de contact
1. Ați fi interesat/ă să fiți contact/ă de către un reprezentant pentru a răspunde la câteva întrebări suplimentare?
   a. Da
   b. Nu

2. Vă rog să completați următoarele informații pentru a putea fi contactat/ă:
   Nume și prenume, Funcție
   Adresă e-mail, Număr telefon