Osservatorio
ACCREDIA

1 | 2022

Cybersecurity and data protection: the role of accredited certification

Executive Summary

In collaboration with:

CYBERSECURITY
NATIONAL LAB

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

Osservatorio Accredia

Chief editor
Gianluca Di Giulio

Editorial coordination
Alessandro Nisi
Francesca Nizzero

Graphics
ZERO ONE

This document is the Executive Summary of the study created by the joint "Cybersecurity and Certification" laboratory set up by Accredia and the Cybersecurity National Lab of the National Interuniversity Consortium for Information Technology (CINI).

For Accredia: working group coordinated by the Corporate and External Relations - Studies and Statistics area, consisting of Riccardo Bianconi, Amerigo Cancellieri, Gianluca Di Giulio, Lorenza Guglielmi, Alessandro Nisi, Guglielmo Tozzi, Pietro Vitaliano, Alessandra Zacchetti.

For the Cybersecurity National Lab: working group directed by Alessandro Armando and consisting of Francesco Buccafurri, Fabio De Rosa, Giorgio Giacinto, Paolo Prinetto, Leonardo Querzoni, Luca Verderame.

ACCREDIA
The Italian Accreditation Body

Via Guglielmo Saliceto, 7/9
00161 Roma

Tel. +39 06 844099.1
Fax. +39 06 8841199

info@accredia.it
www.accredia.it

Cybersecurity and data protection: the role of accredited certification

Cybersecurity has taken on a leading role in the agenda of governments, institutions and companies, becoming one of the priorities of the countries of the European Union. With the development of the digital society and the prevalence of ICT services, the issue of cybersecurity now performs a strategic role; it is a problem that needs to be tackled seriously, in order to ensure the correct protection of data, applications and systems, by all types of organisations, both public and private, but also by individual citizens. The importance of the issue is further increased by the fact that today many critical infrastructures on a national scale are managed through IT systems which can become the object of attacks whose effects can compromise the provision of public utility services.

The analyses contained in the study by the Accredia Osservatorio "Cybersecurity and data protection: the role of accredited certification" provide useful elements in support of the principle according to which the assessment of conformity with technical standards, strengthened by accreditation, represent enabling factors for cybersecurity, playing a decisive part in the current digital transformation process of society.

The normative context

In Europe, the Network and Information Security Directive (EU Directive 2016/1148) known as NIS[1] (Network and Information Security) was the first piece of legislation on cybersecurity at EU level, with the aim of improving IT security and information throughout the Union. A series of security obligations were imposed on the member countries, to achieve a high common level of network and information system security.

In particular, the Directive required Member States to adopt a national strategy, establishing additional security and notification obligations for operators of essential services and digital service providers. With the same Directive, the Member States were obliged to designate competent national authorities, single contact points and Computer Security Incident Response Teams (CSIRT) with tasks related to cybersecurity.

[1] Today, the proposal for a new EU NIS2 Directive is part of a package of measures by the European Commission aimed at further improving the resilience and incident response capabilities of public and private entities, competent authorities and the Union as a whole, in the field cybersecurity and critical infrastructure protection.
The draft of the new Directive includes a new strategy for cybersecurity, aiming to strengthen the strategic autonomy of the Union in order to improve its resilience (especially of critical operators of essential services) and the collective response to cyber incidents.

More recently, the EU Regulation 2019/881, the so-called Cybersecurity Act, constitutes a fundamental part of the new EU strategy for cyber security, aiming to strengthen the Union's resilience to cyber attacks and to create a single cyber security market in terms of ICT products, services and processes. The intention is to increase consumer confidence in digital technologies.

A first key point of the Regulation concerns the strengthening of the role of the European Union Agency for Cybersecurity (ENISA)[2]. In particular, a permanent mandate is guaranteed to ENISA, which contains technical consultancy tasks, as well as support for the operative management of IT incidents on the part of Member States.

A second point of attention contained in the Cybersecurity Act concerns the introduction of an overall framework of rules governing the European IT security certification schemes without defining, per se, directly operative certification schemes; on the contrary, a basic framework is created on which to establish European schemes for certification. There are three possible levels of certification of reliability regarding cybersecurity: basic, substantial and high level. The level of reliability is in line with the risk regarding with the intended use of the ICT product, service or process, in terms of the likelihood and impact of an incident.

For ICT products, services and processes with a high risk level, certification can only be issued by the National Cybersecurity Authority, or, in the following cases, by a conformity assessment body:

a) subject to approval by the national cybersecurity certification authority for each individual European cybersecurity certificate issued by a conformity assessment body; or

b) on the basis of a general delegation of the task of issuing such European cybersecurity certificates to a conformity assessment body by the national cybersecurity certification authority.

In Italy, the national cybersecurity structural approach is defined in Legislative Decree 82/2021, which establishes the national cyber security system and the National Cybersecurity Agency (ACN). Among other things, the ACN has the function of National Cybersecurity Certification Authority (NCCA) and therefore of all functions relating to cyber security certification, including those concerning the Security Perimeter National Cybernetics (PSNC)[3].

[2] *The European Union Agency for Cybersecurity (ENISA) is a center of expertise in the field of cybersecurity established, in its current configuration, with EU Regulation 2019/881 (EU Cybersecurity Act). The European Agency's mission is to help the EU and its member countries be better equipped and prepared to prevent, detect and respond to information security problems. It contributes to the EU's IT security policy, to improve the trustworthiness of ICT products, services and processes with cybersecurity certification programmes.*

[3] *The national legislation (DL 105/2019) on the National Cybernetics Security Perimeter (PSNC) seeks to implement in Italy all the requirements of the current European regulations on cybersecurity, in particular by the NIS Directive and by the Cybersecurity Act. Several subsequent regulatory measures have been introduced regarding the PSNC, in particular:*

- *with DPCM 131/2020 (DPCM I) the methods and procedural criteria for identifying the public and private parties included in the PSNC were defined;*
- *with DPCM 81/2021 (DPCM II) which specifies the modalities and content of communications of incidents by the parties belonging to the PSNC and lists a series of safety measures that the subject of the PSNC must adopt and the relative adoption timelines for ICT assets relating to it, recorded in special lists;*
- *with DPCM of June 15, 2021 (DPCM III) the types of ICT goods and services are defined which must be submitted to verification and inspection procedures in accordance with Presidential Decree 54/2021.*

Subsequently, with Legislative Decree 123/2022, the national legal system is adapted to the provisions contained in title III "Cybersecurity Certification Framework" of EU Regulation 2019/881.

In particular, the role of the ACN as national cybersecurity certification authority is confirmed for the conduct of market surveillance activities and the issuance of certain types of European cybersecurity certificates.

The ACN will therefore supervise the correct application of the rules established by the European cybersecurity certification systems by suppliers and manufacturers of ICT products, issuers of EU declarations of conformity, and holders of European certificates, and conformity assessment bodies.

The ACN, together with these activities and on the basis of a specific agreement, will actively support Accredia in monitoring and supervising the activities of the conformity assessment bodies accredited by it.

The ACN is directly responsible for issuing certifications with a high level of reliability and, in carrying out this task, makes use of the IT Security Certification Body. It may also be issued by a conformity assessment body acting on the basis of a general delegation from the ACN, or following approval by the ACN for each certificate issued.

Certifications with a basic or substantial level of reliability may also be issued by accredited conformity assessment bodies according to Regulation EC 765/2008. In this case, the ACN will participate with its representatives in the decisions regarding the accreditation of the conformity assessment bodies.

Accredia, in carrying out its tasks in accordance with Regulation EU 2019/881, will communicate to the ACN and to the single liaison office designated for Italy (Ministry of Economic Development) any update regarding the accredited conformity assessment bodies (new accreditations, withdrawals, suspensions and reductions of the accreditation certificate).

The Agency will also update and make public two lists of experts and testing laboratories authorized by it to operate in support of its surveillance and issuance of certificate activities. The experts and testing laboratories included in the list of authorized entities shall not carry out assessment activities for the issuance of certificates with a substantial or basic level of reliability at a national level, nor may they be accredited as conformity assessment bodies for the issuance of these certificates.

The ACN may also, in the absence of a European certification scheme, introduce national certification schemes for ICT products, ICT services or ICT processes, after consultation with interested parties. In order to avoid fragmentation of the internal market for certification schemes, Member States will have to inform the Commission and the European Cybersecurity Certification Group (ECCG) of any intention to develop new national cybersecurity certification schemes.

Remaining on the topic of cybersecurity certification, the National Cybersecurity Strategy 2022-2026 issued in May 2022 by the ACN promotes the development of a homogeneous and coherent framework of European cybersecurity standards. The Strategy identifies three fundamental objectives to be pursued: protection, response and development. In particular, within the context of objective 1 of the Strategy (protection of national strategic assets) it is considered essential to strengthen the capacities of the National Evaluation and Certification Centre of the NCA and, in the areas of competence, of the Evaluation Centres of the Ministries of the Interior and of Defence, as well as integration with a network of accredited testing laboratories.

The Strategy reinforces the need to define an up-to-date and coherent national legal framework on cybersecurity. In this context, the following are relevant:

- support for the development of certification schemes and European and international standards on cybersecurity;

- promotion of the use of European certification schemes in the field of cybersecurity, by specialized Italian companies, in order to achieve a competitive advantage on the market.

Accredited activities for cybersecurity

The concrete risk of compromising IT systems and technological safeguards, which is accompanied by the possible breach of personal data, is constantly growing. In 2021, cyberattacks around the world increased by 10% compared to the previous year[4]. New ways of attacking demonstrate that cybercriminals are increasingly sophisticated and able to network with organized crime.

In the light of this, it is important to set up an action of preparation for attacks as well as detection, containment and response capabilities. Systemic action must lead to an improvement of the overall security set-up, and this necessarily requires an intervention that involves the diverse sectors of society and the productive world.

Technical standards, together with national and European legislation, play a central role. In particular, compliance with technical standards and regulations means the ability to define and plan cybersecurity strategies. It also means the ability to monitor the actions hinged on the strategy adopted and it means the ability to be able to demonstrate, through objective references, the maturity of such strategies with respect to third parties. This last aspect is based on two pillars, closely inter-connected: the assessment of conformity with technical standards, and accreditation; the latter, in particular, ensures the existence of impartiality, competence and independence profiles of the bodies that perform conformity assessment services.

Accredited services (certifications, inspections and assessments undertaken by accredited bodies and laboratories) offer assurances on the quality and safety of the products and services purchased. The benefit provided is significant in a variety of areas, but becomes crucial in a sensitive area such as cybersecurity. They offer guarantees on compliance with fundamental security requirements, such as the protection of privacy and of essential services from the cyber threat.

Since 2002, Accredia has been operating in the fields of both information and cybersecurity.

The involvement of the Accreditation Body in cybersecurity is wide-ranging and concerns many technical skills amongst which the main ones are:

- Information Security Management Systems and cybersecurity (ISMS);

- the competences of professionals operating in the ambit of information security and cybersecurity, including the Data Protection Officer (DPO) and the GDPR Auditor, as well as ISMS assessors;

[4] *https://clusit.it/rapporto-clusit/*

- product, process and service certifications, such as, for example, those relating to the SPID (Public Digital Identity System) and the eIDAS and GDPR EU regulations;

- inspection activities conducted at various levels, such as inspections of plants and facilities;

- Testing Laboratories, with reference to the Vulnerability Assessment and Penetration Testing processes.

Also in the domain of privacy and personal data protection, accredited services contribute to the effective achievement of the objectives defined by the European Regulation 2016/679, known as the General Data Protection Regulation (GDPR), the reference normative framework in this area. The Regulation covers the right to the protection of personal data, while at the same time sanctioning the principle of free movement of data within the European Union.

The Regulation provides for the establishment of "data protection certification mechanisms as well as data protection seals and marks for the purpose of demonstrating compliance with this Regulation for the processing operations carried out by the data controllers and data processors", without prejudicing responsibilities or overriding the duties and powers of the control authorities towards them. The Regulation provides that the certifications must be issued by accredited bodies according to Regulation EC 765/2008 or by the competent control authority. In Italy, the guarantor for the protection of personal data decided to entrust Accredia with the accreditation of the certification schemes, which must be approved by the guarantor for the protection of personal data.

The Data Protection Officer (DPO)[5] was introduced to support public organizations, with the aim of informing and providing consultancy to the data controller[6] or data processor[7], as well as to the employees who carry out the processing regarding the obligations deriving from the GDPR. This is a professional person with highly specialized knowledge of data protection legislation and practices, and the ability to perform the tasks assigned to her/him by the law. The world of technical standardization has regulated this professional person by means of the voluntary standard UNI 11697 and the Reference Practice UNI/PdR 66:2019. The importance of the activities performed by the DPO, the need to have assurances regarding the effectiveness of actions and the importance of the qualification of competences with respect to the market has – despite the fact that it is a voluntary scheme – prompted 15 certification bodies to obtain accreditation in accordance with ISO/IEC 17024 and 687 professionals to certify their skills.

[5] *In Italy, a voluntary technical standard has been drawn up which establishes the requirements relating to the professionals who will operate in the field of personal data processing and protection. It should be remembered that, despite not having formally recognized these certifications, the guarantor for the protection of personal data took part in the development of UNI 11697:2017, participating in the work table for the drafting of the standard. Certification to UNI 11697:2017, obtained from an accredited body according to ISO/IEC 17024, is considered a presumption of competence of the members of the audit team when they certify in the area of privacy.*

[6] *It is the natural or legal person, public authority, service or other body which, individually or together with others, determines the purposes and means of processing personal data.*

[7] *Defined as the natural or legal person, public authority, service or other body that processes personal data on behalf of the data controller.*

Table 1 below shows the main accredited conformity assessment schemes in the cybersecurity field for which the related accreditation certificates have already been issued.

Table 1. Cybersecurity - accredited conformity assessment schemes - updated 13/10/2022

Accreditation standard	Certification standard	Description	Number of accreditations	Number of Certifications
ISO/IEC 17021-1	ISO/IEC 20001-1	Management systems for IT services	9 certification bodies	327 certified companies
ISO/IEC 17021-1	UNI ISO 27001	Information security management systems	20 certification bodies	3.474 certified companies
ISO/IEC 17021-1	UNI EN ISO 22301	Business continuity management systems	9 certification bodies	222 certified companies
ISO/IEC 17025		Vulnerability Assessment	5 testing laboratories	
ISO/IEC 17024	UNI 11697:2017 UNI PdR 66:2019 ECF PRIVACY	Data protection officers	15 certified bodies	687 certified persons
ISO/IEC 17024	UNI 11506 Standards UNI 11621-x (Multipart)	ICT Professionals (WEB, Security, Operations)	7 certification bodies	250 certified persons
ISO/IEC 17020	National Cyber Security Framework – CSF 2.0 February 2019	Inspection type A/C	2 inspection bodies	
ISO/IEC 17065	ISDP©10003:2015	Certification of processes for the protection of individuals with regard to the processing of personal data – Reg. EU 679/2016	2 certification bodies	16 certified companies
ISO/IEC 17065	UNI/PdR 43	Guideline for personal data management within ICT according to Regulation (EU) 679/2016 (GDPR)	2 certification bodies	12 certified companies
ISO/IEC 17065	Series IEC 61508 Series IEC 61511 IEC 62061 Series ISO 26262	Safety Instrumented Functions	3 certification bodies 1 inspection body	
ISO/IEC 17065	Series IEC 62443	OT (Operational Technology) System Safety	2 certification bodies	
ISO/IEC 17065 ETSI 319 403	eIDAS Regulation ETSI 319 401 series standards Standards dedicated to TSP (Trust Services Providers) services	Conformity to the eIDAS and TSP services Regulation	7 certification bodies	
ISO/IEC 17065	Technical Specification AgID [checklist]	SPID services	4 certification bodies	

The study of the benefits deriving from the use of accredited services.

Is it possible to provide a concrete indication of the benefits brought by the use of accredited services for cybersecurity?
To answer this question, two complementary methodologies have been adopted: a first, based on the analysis of selected case studies that led to the definition of a series of qualitative indications related to the benefits deriving from obtaining and maintaining accredited certification to the standard UNI CEI EN ISO/IEC 27001. The second methodology was based on analysis of the vulnerabilities of web services reported by a large sample of organizations, with the correlation of the results of this analysis with respect to possession (or not) of accredited certification to UNI CEI EN ISO/IEC 27001. This second method of analysis made it possible to obtain indicators of a quantitative nature regarding the level of risk exposure of the certified companies. An activity of this type is able to provide very clear indications about the security set-up of the organization, since web services are the ones most targeted by attackers to ensure an entry point within the organization's perimeter. The analysis of the case studies started from the identification of the companies to be interviewed. The selection was based on specific factors that took into account the size, nature, reference market and age of the certification. Based on these factors, a list of Italian companies with UNI CEI EN ISO/IEC 27001 certification was considered, from which the following case studies were selected:

- *Gruppo BCC Iccrea* - It is the largest Italian cooperative banking group, the only national banking group with entirely Italian capital and the fourth largest banking group in Italy by assets. The BCC Iccrea Group consists (data as of 06/30/2022) of 120 Cooperative Credit Banks present in over 1700 Italian municipalities with almost 2500 branches, and of other banking, financial and instrumental companies controlled by the parent company, BCC Banca Iccrea, which provides services in the fields of finance, corporate credit, securities administration and payment systems. The Group has more than 3 million customers, approximately 845,000 shareholders and over 22000 employees.

- *Poste Italiane* - The group, with its 160-year history, constitutes the largest service distribution network in Italy, active in the sectors of logistics, mail and parcel delivery, financial and insurance services, payment systems and telephony.

- *Atac* - The mobility company of the Municipal Authority of Rome is the first urban mobility operator in Italy and one of the largest local public transport management companies in Europe. Today Atac has a staff of more than 10 thousand, with extremely diversified roles and professions.

- *Notartel* - The company of the Consiglio Nazionale del Notariato and of the Cassa Nazionale that has been offering IT services to Italian notaries for over twenty years. For several years it has managed the issue of Digital Signatures and smart cards and the Certified Electronic Mail service of Italian notaries, as well as being the data archive body for the National Council of Notaries.

The analysis of the case studies made it possible to trace some general elements related to ISMS certification. A first important point is that the reasons underlying the decision to certify an ISMS will hardly represent the only return on the investments made over time.

[8] *Dati al 30 giugno 2022.*

All the experiences gathered with the case studies have made it possible to understand how certified organizations are only able to fully understand how much the path followed has profoundly changed their organization over time, with a tangible improvement in many contexts, not necessarily limited to better cyber risk management.

A second aspect is the fact that the certification of an ISMS is a facilitating element for compliance with the numerous regulations which, in various sectors, impose requirements related to cybersecurity.

The risk-based approach represents, on the one hand, one of the most important added values acquired with the adoption of this type of ISMS, but also one of the critical points in the adaptation phase and subsequently in the improvement and maintenance of the certification. The activities necessary in this sense are many, requiring commitment and frequently involving a radical change in the way of thinking of an organization. The cost of all this, also in terms of human resources, can be significant and not necessarily within the reach of smaller organizations or those who have to operate in highly competitive markets.

Once these obstacles have been overcome, an ISMS can contribute positively to the life of the organization by means of the harmonization of the monitoring and improvement processes, of performance evaluation and independent auditing that enable the organization to manage incidents and future adjustments in a reasoned and coherent way.

The standards for security management and the related certification processes represent a real driver for the cultural growth of the organizations that adopt them. The culture of safety and everything that comes with it take years to develop. This type of investment has a long-term return, which guarantees lasting benefits, which become an integral part of the organization.

The second methodology for analysing the potential benefits deriving from the use of accredited services is based on a technical study on two groups of Italian private and public organisations: one with security certification to UNI CEI EN ISO/IEC 27001 and one with UNI EN ISO 9001:2015 quality certification. In particular, through a non-invasive Vulnerability Assessment campaign of the web services publicly divulged by the organizations themselves, it was possible to evaluate:

- the positioning of the software used for these services with respect to the known serious vulnerabilities included in national and international databases (e.g. the CVE database);

- correct use of the HTTPS protocol;

- the update and security levels of the Content Management Systems (CMS).

For the purposes of the analysis, all public and private organizations with registered offices in Italy, present in the Accredia database and active at the extraction date (March 2022) were considered. These organizations were then divided into two different categories[9], consisting of:

1. organizations with UNI CEI EN ISO/IEC 27001 security certification;
2. organizations with UNI EN ISO 9001:2015 quality certification.

[9] *Organizations holding both certifications were excluded to avoid overlap between the two categories.*

100 organizations were extracted, 50 from the first group and 50 from the second, using the "non-probabilistic convenience sampling" technique, taking into account the company size and the sector of activity to which they belong.

In general, organizations certified to UNI CEI EN ISO/IEC 27001 are less susceptible to serious security vulnerabilities. The analysis of the vulnerabilities identified using the OSINT[10] sources made it possible to identify 1207 CVE vulnerabilities on the 100 web services being analysed, of which 683 (57%) in the sample of organizations certified to UNI EN ISO 9001:2015 and 524 (43%) in the sample certified to UNI CEI EN ISO/IEC 27001.

The analysis of activities on the use of the HTTPS protocol has highlighted how UNI CEI EN ISO/IEC 27001 certified organizations have a high degree of security in the use of the protocol; 50% of the sample analysed obtained ratings of A and A+ (the highest degree of safety). 42% instead reached grade B, fully passing the sufficiency threshold.

As far as organizations certified to UNI EN ISO 9001:2015 are concerned, however, only 37% manage to reach the maximum degree of security configuration (A, A+), while 50% of the services had a B security level.

Finally, the analysis activities on the website services of the sample made it possible to identify the presence of various Content Management System (CMS) technologies. In 62.7% of the websites analysed, the use of a CMS belonging to 8 different technologies was found.

The activities of analysis continued for determining, for each CMS, the version number, with the objective of assessing the update level of the CMS, which is often subject to high-impact security vulnerabilities. 24% of organizations certified to UNI CEI EN ISO/IEC 27001 have an updated version of their CMS, whilst for UNI EN ISO 9001:2015 certified organizations the figure stands at 18%.

The quantitative analysis activities - while not representing an exhaustive assessment of the security status of an organization - have confirmed a better security set-up of the organizations with accredited certification to UNI CEI EN ISO/IEC 27001.

Future perspectives on the contribution of accredited services for cybersecurity

Accredited cybersecurity services play a central role in building relationships of "trust" between producers and consumers of digital products and services. This role is destined to grow in the light of national and EU initiatives aimed at strengthening the defences and resilience of digital services and, more generally, of the essential functions of the State such as, for example, the National Cybersecurity Strategy, published by the ACN, and the Cybersecurity Act.

The National Cybersecurity Strategy exists in continuity with the normative requirements implementing the NIS and related Directives, which led to the creation of the "National Cyber Security Perimeter". Organizations operating within this perimeter will need to have certain categories of their assets assessed by the ACN National Assessment and Certification Center and will need to follow the security requirements provided by the ACN.

[10] *Open Source INTelligence (OSINT) techniques are aimed at exploiting all publicly available and traceable information, as described in the WSTG-INFO "Information Gathering" control set.*

This service will be implemented through an accreditation process that will fall under the provisions of EC Regulation 765/2008, through the operative collaboration between ACN, Accredia and the laboratories accredited by Accredia.
In addition to product certifications, the ISMS area of certifications is of particular importance, as well as the provision of trust-based ICT services. Without this systemic component, product certifications alone risk not having the desired effect.
The 20 certification bodies accredited by Accredia for information security management systems (UNI CEI EN ISO/IEC 27001) undertake the monitoring (initial certification, surveillance and renewals) of around 3500 companies which, together with the 5 laboratories and Trust Service Providers in the SPID and eIDAS fields, amount to around 4300 parties. The creation of the know-how among professionals performing accreditation activities to ensure the conformity assessment services provided by these entities is not a short or simple process. It is sufficient to consider that professionals in possession of professional certification for information security audits do not exceed forty in the whole country. The enlargement of the security perimeter, which will probably be introduced with the so-called NIS2 Directive, and which would bring the number of organizations under ACN monitoring to several thousand, will be difficult to manage in the short term. Therefore a dialogue and close collaboration between ACN and Accredia is not only desirable, but necessary; and this is the direction in which the two bodies are proactively moving, with the signing of the agreement which regulates the methods of use by the ACN, of the conformity assessment services conducted by Accredia and through the application of Legislative Decree 123/2022.
Although the context is particularly favourable for a wider use of accredited cybersecurity services, it should be noted that current certification schemes do not always meet the needs of important market sectors.
The development of certification schemes capable of offering an adequate level of security in operative contexts characterized by a low level of risk, without incurring particularly onerous timelines and costs, known as “lightweight” certification schemes, would make it possible to expand the range of potential users significantly, with a notable collective benefit.
To fully seize the opportunities offered by the growing attention to accredited cybersecurity services, it is essential that certification schemes can evolve in the directions required by the market. In particular:

- the DevOps model which combines the development and operations phases of the software, ensuring that the new functions introduced during the development phase are implemented very quickly. In fact, this model opens up interesting scenarios for the certification of software products. In particular, the possibility of including automatic security checks in the various phases of the life cycle of the application would allow for the automatic generation of the documentation necessary for the certification not only of the initial version of the product, but of all the versions that will subsequently be issued. “Lightweight” cybersecurity certification schemes would be made more efficient, both in terms of time and costs.

- created for military purposes, the Cyber-Ranges are IT platforms which, thanks to virtualization technologies, support the simulation of cyber attacks in highly realistic ICT scenarios.

> The Cyber-Ranges support the execution of sophisticated and large-scale attacks by offering an unprecedented opportunity for the creation of new generation certification schemes, aimed at assessing the skills of personnel, cybersecurity products and business processes.

Finally, a further element of analysis of the potential future involvement of accredited cybersecurity services concerns the certification of professional competences. This issue is already central to European and national legislation. The attention arises from the need for qualified personnel on specialized and constantly evolving skills. In fact, despite the fact that in the range of professional ICT certifications, those envisaged by the UNI 11506 standard and by the so-called "multipart" standards of the UNI 11621 series are already available on the market today, there remains a lack of skills in the matter of cybersecurity. In this context, actions have been taken not only to increase the workforce available, but also to increase the quality of candidates and equip them with the skills most in demand in the sector. Examples are the CyberChallenge.it, OlyCyber.it and CyberTrials programs promoted in Italy by the Cybersecurity National Lab (CINI).

At the regulatory level, the European Cybersecurity Skills Framework (ECSF) aims to create a common understanding of the roles, competences, skills and knowledge used by and for individuals, employers and training providers across all EU Member States, in order to address the shortage of cybersecurity skills. Furthermore, it is the intention of the legislator that this will contribute to further facilitate the recognition of cybersecurity skills and to support the design of cybersecurity training programs for the development of skills and career opportunities. Similar goals have also been included in the renewed Digital Education Action Plan (2021-2027)[11].

In Italy, the National Cybersecurity Strategy promotes cyber security culture. The goal is to promote widespread knowledge of the risks associated with the use of digital tools and disseminate specific competences in the field of cybersecurity. In particular, in order to ensure the effectiveness of training activities, the development of a national system of certification of learning and the acquisition of specific professional skills is necessary: technical skills at high school, university and professional level. The ACN will have to maintain a list of training courses, approved by the Agency itself, at the end of which the relative attestation or certificate will be issued.

[11] *https://education.ec.europa.eu/focus-topics/digital-education/digital-education-action-plan*

OA Osservatorio ACCREDIA

Via Guglielmo Saliceto, 7/9
00161 Roma

Tel. +39 06 844099.1
Fax. +39 06 8841199

info@accredia.it
www.accredia.it

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO