EUROPEAN CYBER SECURITY ORGANISATION

European Cyber Security Certification

Assessment Options

WG1 I Standardisation, certification, labelling and supply chain management

September 2019

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg1_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

Copyright Notice

EXECUTIVE SUMMARY

This document discusses the best practices for the assessment of products, systems and services. It defines both self-assessment and accredited self-assessment as two ways to structure an in-house process that improves the overall security of the developed products, systems and services. It explains how organisations that are building their cybersecurity capabilities as a key part of their business often resort to a process-based approach to cybersecurity, where self-assessment, vulnerability monitoring and post-compromise management are essential ingredients to cope with highly dynamic cybersecurity needs. Examples of the best practices are provided for both self-assessment and third-party assessments, where the departments responsible for assessment are separate from the development departments.

Two choices are important to make when assessing the required cybersecurity properties of a system or service: 1) which cybersecurity standards will apply, and 2) which party will assess that the requirements are actually met. Which cybersecurity standards are relevant is market dependent as it is currently not realistic to demand nation-state level security strength, e.g. for consumer devices, a risk-based approach to identify the right trade-off is usually followed. The level of independence of the assessor may influence the confidence in the assessment, but it has no bearing on the security requirements themselves.

This document discusses the different options for assessment and presents an analysis of how organisations can benefit from the right mix of assessments. For instance, organisations can link the assessment with the risk management, or they can even use it to help build in-house cybersecurity capabilities and benefit from economy-of-scale, or avoid double processes in regulated industries. Organisations can also tightly integrate the assessment in the full lifecycle management with modern DevOps methodologies. Additional relevant considerations for organisations in the context of an assessment are linked to other market-related factors such as simplifying the protection of the Intellectual Property, supporting a robust decentralised digital economy, and promoting low cost and fast time to market. Organisations also need to consider technological aspects such as avoiding supplier lock-in and strengthening security by assessments performed by multiple parties, providing impartial assessments that provide a high level of trust, strengthening company procedures to resists market pressure to shortcut security assessments, increasing confidence and transparency to customers, consumers and authorities, providing international recognition of developed items, enabling repeatable assessments, and providing for a large choice of international standards that can be tailored to the specific domains. *A combination of assessment methods could also be used when high levels of assurances are needed.* Market surveillance techniques that do not rely on developer-supplied information are the only way to address the issue that fraudulent organisations may provide false evidence to evaluations. Naturally, in-house assessment options are only fully available to organisations that have built the required capabilities.

In the second part of the document, possible adaptations of assessments to fit potential business constraints are also discussed. Different types of assessments, *initial*, *renewal*, *partial* and *full*, are presented and how they can allow an adjustment of the effort (time and cost) in a balanced way as required by a competitive market is discussed. The flexibility in the most suitable type of assessment also has validity for the technical scope of the assessment itself. Third-party assessment can be based on many different international standards which enables organisations

to find the perfect fit between the market constraints, and the relevant standards and requirements. In cybersecurity, the wide range of standards identified in the ECSO State Of The Art (SOTA) document [1] show the need to have a sector-specific approach.

The document concludes by stating that harmonising cybersecurity requirements for all assessment types is a main objective for the Digital Single Market and recommends that ENISA includes this in its objectives.

TABLE OF CONTENTS

1 INTRODUCTION

Increasingly, organisations and companies have decided that cybersecurity is a key part of their business model, and they are continually investing in building their cybersecurity capabilities. A famous example of such a decision is the announcement of Maersk at the World Economic Forum: in reaction to the not-Petya attack, they unveiled a new strategy to build a leading capability in cybersecurity, as a key differentiator for their company [2]. These cybersecurity capabilities involve assessment, like *Red-teaming* or *in-house penetration testing facilities*.

Cybersecurity is a combination of education, policies and procedures, physical security and technology. Feedback from the industry is that developments in cybersecurity are evolving at a dazzling speed. To deal with this dynamic environment, it is felt that a process-based approach to cybersecurity is essential and the most stable. For example, Microsoft established the secure software development lifecycle process as a response to the increased security needs of their products. This evolved to standards like NIST SP 800-160 [3].

This can be illustrated using a typical example of the complexities of digitisation of an industry, products and services are being connected through digital infrastructures. This can be healthcare, or any other industry that is in transformation towards the Digital Single Market. Typically, a system consists of online services, digital infrastructure, and end-point devices that are not always in a managed environment but can be located anywhere in society. Most components, like servers, integrated circuits (ICs), routers, operating systems, and the like, are commercial-of-the-shelf components that are integrated in the overall system and similarly the services are often constructed using commercial sub-services and commercial software components. It is a known fact that any of these components can be compromised at any time. Whether it is a database that has been breached, or an operating system bug that is leading to a global exploit like WANNACRY, or a software supplier that issues an update with a malicious payload like not-Petya, or a flaw in the WiFi WPA2 protocol, or a hardware component that contains a fundamental flaw like Meltdown/Spectre.

The results are the same: the entire system is composed of elements that may be compromised at an unpredictable moment. Such zero-day attacks cannot be predicted and before their existence is known it is impossible to verify and test against them. Therefore, processes to deal with vulnerability monitoring and post-compromise management become essential ingredients for the cybersecurity of these systems.

For known attacks, it is possible and, in many cases, desirable to test that developed products, systems and services are not vulnerable to them. Penetration testing and vulnerability analysis techniques are important processes that contribute to the overall security of the system.

This document aims to describe the different options for assessment highlighting how they can improve the level of cybersecurity, and confidence regarding the level of cybersecurity of products, systems and services. Assessment procedures are established to address both societal and business concerns, as illustrated in Figure 1. This document further describes the best practices in assessment of products, systems and services.

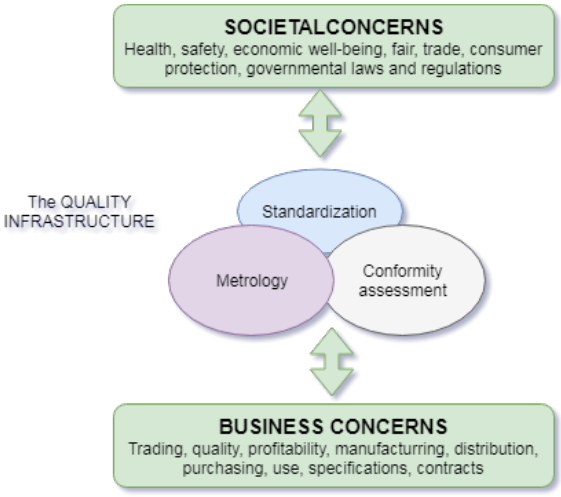

Figure 1 - Conformity Assessment toolbox (ISO credits)

The remainder of the document is organised as follows. This chapter introduces basic concepts pertaining to the assessment and the perimeter of this document. Chapter 2 discusses the benefits and disadvantages of the various assessment methods with the intent to guide the reader in the selection of the most suitable type of assessment. Chapter 3 focuses on the criteria and considerations for the assessment. Chapter 4 describes the most common best practices for an assessment. Chapter 5 lists the standards that can be optionally used in assessment. Chapter 6 discusses the relation and exchangeability of self-assessment with third-party or national certification and self-declaration. Chapter 7 concludes the document and gives final recommendations.

1.1 Background information

The Objective of the European Cyber Security Organisation (ECSO) Working Group 1 (WG1) “Certification, Standardisation, Labelling & Supply Chain Management” is to establish trusted supply chains and reduce the (technical and business) impact of cybersecurity attacks to improve resilience for the increasingly digitalisation of the society and industrial sectors. Thus, assessing the security claims of products, systems, services and organisations is essential.

This document merges the results of the work carried out in the “WS1.x.3 Self-Assessment” and “WS1.x.2 Third-Party Assessment” ECSO work streams, and only lightly touches the aspects linked to National Assessment.

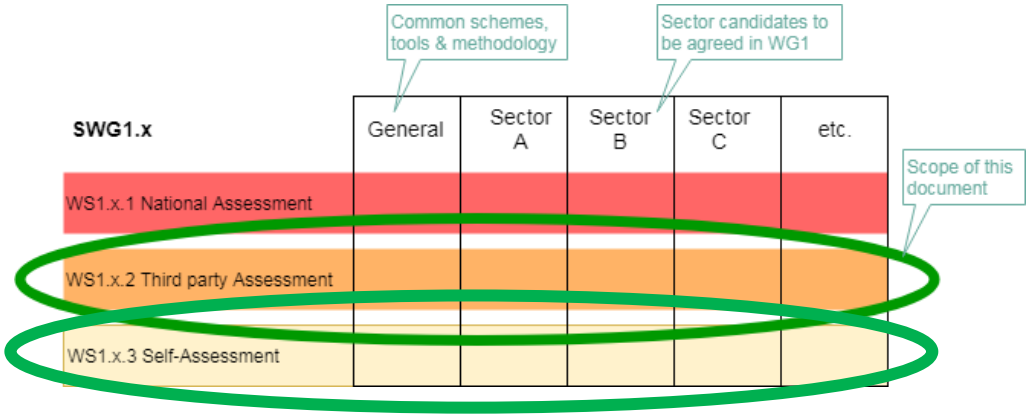

Figure 2 - Scope of the working group

The document addresses only the general aspects and specific cybersecurity requirements for individual sectors are outside its scope.

1.1.1 Link with the Cybersecurity Act

The Cybersecurity Act (Regulation 2019/881) [4], amongst others, defined key points like:

- Article 51: Security objectives (data confidentiality, data integrity, data/services right management, data/services access/logs, incident response, patch management).
- Article 52: Assurance levels (basic: limited degree of confidence, substantial: certificate with a substantial decrease of the risk, high: certificate to prevent cybersecurity incidents).
- Article 54: Certification schemes defining evaluation criteria depending on security objectives.

The notes accompanying the Cybersecurity Act refer to assessment repeatedly. In summary, ICT processes, products and services comply with requirements to protect the **availability, authenticity, integrity and confidentiality** of systems throughout their **life cycle**. However, conformity assessment and certification cannot guarantee per se that certified ICT products and services are cyber secure. Certified conformity assessment is rather a **procedure to attest** that ICT products and services have been tested, that should be carried out by an independent **third party**. A European cybersecurity certification scheme could specify **assurance levels** for European cybersecurity **certificates** and EU **statements of conformity** issued under that scheme. Each certificate could refer to one of the assurance levels: basic, substantial or high. The assurance levels provide a corresponding **degree of efforts for the evaluation.** The choice, by the users, of the appropriate level of certification and associated security requirements should be based on a **risk analysis** of the intended use.

1.2 Types of assessments

It is important to distinguish the assessment of the security of a product, system or services from the declaration made regarding the security of a product, system or service. The assessment aims to deliver the *evidence* that the item conforms to the security *requirements*. The declaration, i.e.,

statement or attestation, provides the decision that the fulfilment of the security requirements has been demonstrated.

The different options to claim that a product, system or services complies with a standard are the following:

- Self-Declaration without any assessment;
- Self-Declaration based upon a self-assessment or a voluntary third-party assessment;
- Accredited certificate based upon a third-party assessment (in-house or external);
- Certificate issued by a National Authority based upon a third-party assessment (external).

The decision on the type of option is under the responsibility of the manufacturer who should choose it after having conducted a risk analysis to measure the liability.

In accordance with the definitions given in the Blue Guide [5], this chapter discusses the different types of assessment. We distinguish four types of conformity assessments:

Type of conformity assessment
Self-assessment
Third-party assessment (in-house or external)
National third-party assessment

It is important to notice that the conformity assessments are always under the responsibility of the manufacturer.

Self-assessment means that the manufacturer or service provider performs an in-house assessment of the security. This may be done through penetration testing, evaluation of conformity to certain standards, vulnerability analysis or other. It is not mandatory to ensure independence between the design/production team and the assessment team, but it is seen as important that the department responsible for the assessment is not the same department responsible for the development.

- Unaccredited self-assessment occurs when the manufacturer or the service provider uses processes and organisational structures for assessment that have not been inspected and accredited by a third party for the particular self-assessment activities under consideration.

Third-party assessment means that an independent party, not under the control of the developing organisation or service provider, performs an assessment of the security. The same techniques as defined for self-assessment can be used to carry forward the assessment. The third party is ideally an accredited body, that is declared technically competent. These requirements may come from e.g. ISO/IEC 17025 [6] and other standards. Third-party assessment is a global activity which can be based on reviews / audits / tests / etc. (as required in ISO/IEC 17065 §7.4.3 [7]). Third-party assessment could be ensured by three kinds of entities:

- **(Accredited) In-house body**. Manufacturer or services provider leads assessment of its own products. It requires a certain level of independence (defined in ISO/IEC 17025 [6]) between design teams and testing entities. Processes and organisational structures of the body for the particular assessment activities are periodically inspected and are accredited by the National Accreditation Body (NAB) or an authorised third party. The certificates issued by the in-house body is equivalent to the certificates issued by an external third party (mutual recognition) with the same level of confidence.
- **(Accredited) external body.** An independent party, not under the control of the manufacturer or the service provider, performs the assessment of the *target*. The processes and the organisational structures of the body are periodically inspected and are accredited by the National Accreditation Body. These requirements may come from e.g. ISO/IEC 17065 [8] and other standards. Third-party assessment is used in schemes based on ISO/IEC 15408 (Common Criteria) [9] and many other schemes.
- **National body** is the specific case where the third-party assessor is a National entity. Such assessments are mostly used when national security is at stake, for instance around military or nuclear projects.

In terms of third-party assessment, it is possible to refer to the Conformity Assessment Body (CAB), i.e., the body that performs the conformity assessment activities including calibration, testing, certification and inspection.

Declaration (self-attestation – [765/2008/EC] [10]**)** means that the manufacturer or service provider makes a public statement about the security provided, sometimes referring to one or more standards that is being adhered to. The manufacturer or services provider (first party) uses processes and organisational structures to declare the conformity of the owned *target of the evaluation (product, system or service)*. It can be based on the previously available conformity assessments or any other kind of verification (test, document review, etc.).

Self-declaration is for instance assumed by the CE marking conformity framework. The self-declaration activities are technically led by the manufacturer but can also be sub-contracted.

Apart from the product, system, or service, also the developing and managing organisation may be the target of an assessment or declaration. Larger systems and services typically consist of a set of items, and each one of them may have its own assessment strategy and possibly individual declarations. For example, the security-by-design work processes of an organisation might have undergone an assessment by an external body, whereas the items developed under these processes might undergo an assessment by a (third-party accredited) in-house body.

2 ASSESSMENT TYPE SELECTION

For each one of the different types of assessment, e.g. conformity assessment or ethical hacking, there are potential benefits and disadvantages. One important factor to consider is the industry sector and the best practices in use. This chapter discusses these benefits and disadvantages from an independent point of view to give the reader the relevant instruments and knowledge to decide on the most suitable type of assessment. ENISA also captures some of these considerations in its survey report [11].

For several decades, third-party assessment has been the standard for certifying *targets* in many fields. For instance, when safety is at stake, like in some critical domains, such as railway, dangerous equipment machinery, medical devices and consumer products, the voluntary or regulated approach for the field relies often on third-party assessment. Moving from safety, where a risk-based strategy is usually adopted, to cybersecurity, it is likely that a similar approach can be used to identify and assess the risk associated and thus the most suitable type assessment.

There are both advantages and limitations to the various kinds of assessment as a mean to improve the cybersecurity of products, systems and services. This chapter will delve into the details to understand the stakes of each kind.

2.1 Mix of assessment types

In many cases, organisations apply a mix of self-assessments and assessments by multiple (types of) third parties. Third parties could help organisation understanding the evolving threats, building the essential cybersecurity knowledge, and keeping internal security processes up to speed. By structuring additional third-party assessments as black-box penetration tests, where no specific information is transferred from the manufacturer / service provider to the assessment body, thus reproducing a setting similar to an external attacker, the risks associated to leak sensitive information, such as company know-how and Intellectual Property (IP) is minimised when the external body is used.

In a situation of mix of self- and third-party assessment, third-party assessments could also target the organisations rather than the items that are developed, or an accredited in-house body can be used. Also, in these cases, no sensitive information and know-how need to be transferred outside the organisation.

2.2 Risk management

Cybersecurity is one of the driving risk factors in connected products. The financial legislations like SOX (Sarbanes-Oxley Act[1]) might require that organisations establish the controls to manage all types of financial risks, and, as such, cybersecurity risk management for connected products and services must be established within the organisation.

By having an in-house assessment, the parties can tailor their security assessment to the risk. Products, services and organisations differ in their risk profiles, which is best understood by the party whom it concerns.

Risk assessments and classifications can also be performed by an external third-party assessment body. Depending on the domain of an assessment, there are relevant international standards which provide information of risk classification. For instance, IEC 62443 [12] provides a four-level approach towards security assessment, based on an initial risk classification. The security assessment can continue from that point by investigating the applicable security requirements and controls.

In conclusion, for an organisation it could be smoother and more efficient to perform the risk management process (including risk assessment and selection of relevant controls) in-house, as long as the organisation has sufficient experience in correctly and completely executing such a task. Higher financial risks can also require higher levels of cybersecurity assurance, and, in this case, the risk classification and selection of relevant security controls and requirements to be further tested can also be provided by third parties.

2.3 Strategic in-house cybersecurity capabilities versus economy of scale

More and more organisations and companies identify cybersecurity as a strategic differentiator for their business, motivating their continuous investment in building their own cybersecurity capabilities. A famous example of such a decision is the announcement made by Maersk at the World Economic Forum: in reaction to the not-Petya attack, they unveiled a new strategy to build a leading capability in cybersecurity, as a key differentiator for their company [2].

This trend also aligns with the fact that security is seen ultimately being the responsibility of the manufacturer, either for a product or service. The adoption of security-by-design principles, the development of internal skills in cybersecurity, and the effort for products/services conformity assessment underline the need for organisations to master cybersecurity and make the skills/know-how in the field an asset and market differentiator.

[1] ENISA. Threat and Risk Management. U.S. Sarbanes-Oxley Act of 2002 available at https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/corporate-governance/sarbanes-oxley-act [Last Access: 21 May 2019]

Performing a high-quality assessment requires skills, tools, time and budget. These elements could be challenging or hard to plan for small organisations where the critical mass is not reached. The volume of activities managed by third-party bodies (ensured by various customers) could provide an economy-of-scale that eases resources management, efficiency (also in terms of costs) and faster time-to-market.

2.4 Avoiding double processes in regulated industries

In regulated industries like healthcare, there are already many standards for managing risks, like safety, and associated work processes that must be adhered to. Safety could depend on the way cybersecurity aspects are managed. If addressed separately, overlapping requirements could be handled in potentially separated third-party workflows. This could slow down developments, operations and may raise cost.

Organisations in regulated industries should work to streamline these internal processes to avoid double work and effectively organize both development and operations. This would require the organisations to have the capability of correctly and completely comply to the relevant standards which address cybersecurity. For such a validation, an external third party could be used to certify the processes followed by the organisation to address cybersecurity issues.

An example of how tailor-made assessments adapted on customer constraints can be structured in processes is given in Section 6.1.

2.5 Tight integration in development processes and lifecycle management

In this era of addressing the needs of a fast-changing digital market, many connected products and services are never “finished”, but instead they are continuously evolving their functionality. This concept lies at the basis of models like continuous deployment and DevOps. Vendors update their products and services in reaction to the ongoing dialogue with customers and consumers, changes in regulations and directives, culture and market. Large services that consist of many sub-services with independent release schedules may have a new update released every day (or more). Figure 3 visualizes how development methodologies have evolved to keep up with the fast-changing business landscape.

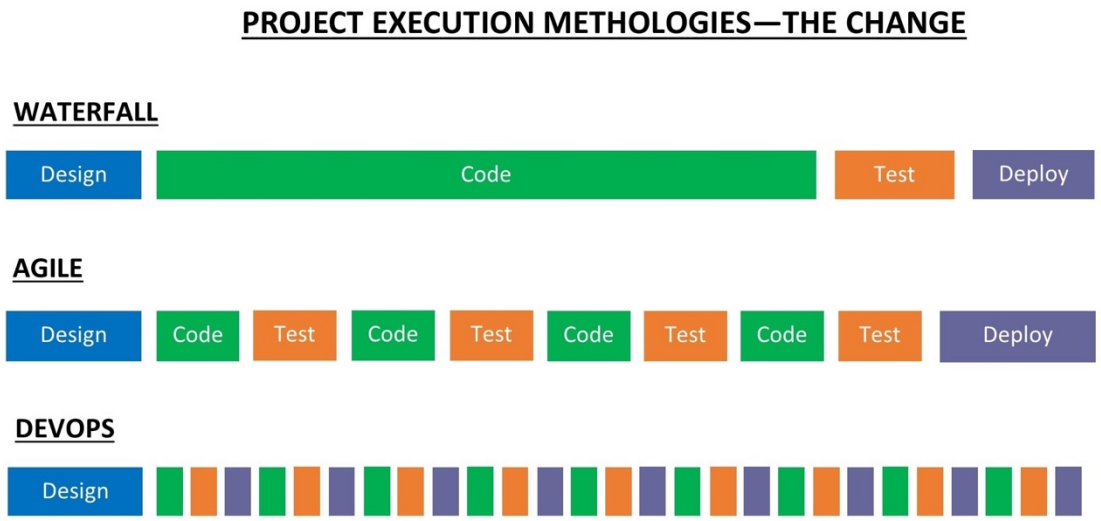

Figure 3 – Development methodologies

To guarantee cybersecurity in such continuously evolving systems, manufacturers and service providers found that the security assessment needs to be tightly integrated in the internal evolution processes. This has led to development of industry best practice in effective assurance methodologies, including the Software Assurance Forum for Excellence in Code (SAFECode)[2], and the Open Web Application Security Project (OWASP)[3]. To increase trust, an external body could be used to certify and periodically review the processes used by the organisation for addressing cybersecurity.

2.6 Protect sensitive know-how and intellectual property

One of the largest threats to European organisations is the risk of theft of their sensitive know-how and intellectual property. Cybersecurity impacts almost all components in the system, any software or hardware that can process or be influenced by external information is subject to cybersecurity. Therefore, the assessor may require significant know-how of the product or service under consideration or potentially significant access to valuable intellectual property to carry a thorough cybersecurity assessment. By keeping the assessment within the organisation, it could become easier to protect the sensitive know-how and prevent losing control over intellectual property.

In order to perform any assessment, the third-party evaluator may need access to sensitive information related to the device/project/company. Thus, confidentiality is a major issue which is basically addressed in the accreditation process of the third party. Both ISO/IEC 17065 [8] and ISO/IEC 17025 [6], which may be used for Conformity Assessment Body (CAB) accreditation in

[2] https://safecode.org/

[3] https://www.owasp.org/

cybersecurity, include specific confidentiality requirements. The CAB has to indicate those requirements within their certification agreement and shall ensure that appropriate confidentiality measures are taken into consideration. In specific cases, additional provisions can be adopted between counterparts. For instance, Non-Disclosure Agreements (NDAs) or specific clearances are commonly used. These kinds of arrangements give a higher level of confidence regarding confidentiality.

2.7 Concentration could contribute to a fragile economy with large-scale cyber risks

From an EU perspective, let us consider the scenario where all products and services are evaluated by a select number of third-party certifiers. In this case, if one of those third-party actors is compromised, then the intellectual property, as well as the vulnerabilities, of a significant part of the EU industry could be directly exposed. This has many similarities with software monocultures where security vulnerabilities have (too) great impact due to the lack of diversity. This centralisation of (cybersecurity) know-how is undesirable as it creates a fragile economy with large-scale cyber risks.

It is noted that when it comes to the market of passports and payment scheme certification, there is already centralisation. How this centralisation would translate to the entire industry in Europe and what precautions/requirements should be enforced on certifiers, and are sufficient to scale this up, are some of the remaining open questions.

2.8 Cost and time to market perspective

For a thorough cybersecurity assessment, a considerable amount of know-how needs to be transferred. Large products may have millions of lines of code, all integrated in a complex system architecture, that an assessor needs to understand before a thorough cybersecurity assessment can be made. Transferring such know-how within the same organisation may be easier than to an external third party.

After the release of the product, new vulnerabilities can still emerge, since cybersecurity is a dynamic, fast moving field, with intelligent and malicious opponents. Zero-day attacks like WANNACRY or vulnerabilities like Meltdown may still occur. Therefore, it is essential that organisations build and maintain cybersecurity capabilities to continuously learn about – and are able to react fast to – zero-day attacks and newly discovered vulnerabilities. With these capabilities in place an assessment carried out by in-house bodies could also be organised cost-effectively.

Cost and time to market are two of the challenges identified by the industry in the Challenges of the Industry (COTI) [13] document regarding the currently existing third-party certification schemes. These aspects need to be addressed in a very careful way, as they will be key for the market adoption of a specific certification scheme. In response to that, several initiatives are already flourishing with the idea of keeping a “light” approach towards assessment. This would involve a smaller burden on the organisation or manufacturer regarding the amount and format of the provided evidence. An example is the strict format of evidence in a Common Criteria [9] evaluation.

To respond to the needs of addressing the time to market issue, there are initiatives like the French CSPN [14] or the Dutch Baseline Security Product Assessment (BSPA) certification programs; the latter has fixed time-frames of 25 man-days over a period of 8 weeks for the execution of testing. This ensures a small and predictable certification process. The downside is that more simplified the approach is, lower could be the level of assurance, which can be however acceptable for relatively lower risk products or services.

The Cybersecurity Act deals with the protection of people and companies, third-party assessments and certification schemes have to be agile enough to manage with the cost and time challenges.

2.9 Avoiding supplier lock-in

For a well-functioning market, it is essential that an organisation does not depend on a single supplier for resilient reasons, being able to freely switch between suppliers or preferably having a second one. This implies that a market for third-party assessment will have to take care of the following.

- Having multiple suppliers of assessment services might imply that a company spreads its sensitive know-how and intellectual property to multiple external parties, thus, increasing the risk mentioned above of IP theft.
- Switching suppliers is costly, as the knowledge necessary for a thorough assessment needs to be transferred again, taking time and money. This is especially relevant for large, complex and continuously evolving systems.

However, changing of assessors is always a good practice to have a different point of view of the assessment.

Traditionally, whenever the risk of supplier lock-in occurs, organisations react by integrating such functions into a single company. Nevertheless, the third-party certification domain is based on a competitive and open market as it adheres to a set of harmonised standards. This stimulates the commercial competition of the different Conformity Assessment Bodies (CABs) while guaranteeing harmonised scope (ensured by accredited process).

Because of the international recognition, an international or European CAB can be called for an assessment even if not present in the concerned area. Furthermore, and specifically for cybersecurity, a large part of the assessment can be performed remotely.

2.10 Schemes that rely on developer-supplied (false) evidence can be misled

Self-assessment does not provide any protection against malicious developers that on purpose weaken the cybersecurity of their systems. Actions by a malicious insider would also likely not be detected by an accredited in-house assessment body or external assessment: in large systems, cleverly disguised backdoors, e.g. as *innocent* bugs, are usually undetectable even by full-scale assessments, and are certainly deniable. If a party is malicious and knowingly adds security

weaknesses to a product, it can present false evidence that omits the weaknesses to evaluators, so (self-)assessment schemes that depend on developer-supplied evidence will be misled.

This is an issue that cannot be controlled during an external third-party assessment, especially in an approach which is optimised for time to market. In such a situation, the evaluators would rely as much as possible on the evidence and partial testing results provided by the target organisation or manufacturer, to avoid duplication of work.

Finding structural solutions to deal with innocently disguised backdoors is one of the hardest issues, for which it is difficult to define proper market surveillance mechanisms.

Recommendation: When results of an assessment are no more granted (found vulnerabilities or false evidences), CABs should notify publicly the disposal of the certificate (may be centralised at the European level) and so all certificates could be available on a centralised platform.

Recommendation: Market surveillance could be added in the next version of the Cybersecurity Act – as already present in the Blue Guide with the RAPEX or Rapid Alert System possibilities [5].

2.11 Impartiality / Independence

An independent third-party Conformity Assessment Body (in-house or external) cannot be involved in the design, manufacturing, supply, repair or maintenance of the type of items being assessed to ensure that there is no conflict of interest in the result of the testing, inspection or certification activities. This is the opposite to a pure self-declaration made by the developing party. This requirement is important to minimise the risk that a developing party, under pressure to take a shortcut to churn out a product to meet a certain market window or simply to save money, might possibly bypass the assessment or minimise the security evaluation below acceptability.

The accreditation of the assessment can strengthen the company procedures to resist such pressures and lower the probability for this scenario. A third party could check if the procedures are and were properly followed. The competence and the impartiality of CABs is ensured by recognition or accreditation. Thus, the accreditation creates credibility and trust while at the same time it provides the same level of competence of accredited Conformity Assessment Bodies (CABs) internationally.

2.12 Confidence in certified products / systems / services

Consumers and authorities can enjoy a higher level of confidence when they know that the *targets* have been tested, inspected and certified.

In the field of voluntary certification, there are numerous cases of *targets* entering the market bearing the third-party mark of the certification body. Consumers know that they can trust the assessment of the product and the resultant mark can therefore help consumers identifying safe products. This trust is supported by the transparent way in which a product's conformity is assessed; there are clear requirements that a product has to fulfil.

Confidence is reinforced when the target has been checked both by the manufacturer and a third party, as complementary points of view could be highlighted.

2.13 International recognition

Through mutual recognition and international agreements between accreditation bodies, accredited certificates based on recognised standards are internationally recognised. This recognition ensures that a *target* certified with an accredited certificate will be recognised as such internationally.

Multilateral agreements (MLA) already exist at EA (European Accreditation), IAF (International Accreditation Forum) and ILAC (International Laboratory Accreditation Cooperation) levels and can be easily extended to cybersecurity certification.

Additionally, recognition can be ensured by the scheme owner. Typically, recognition agreements initiated at this level are more focused on technical issues (comparing to accreditation which is focused on ethic and processes). It is important to note that agreements have various ranges. For instance, SOG-IS MRA [15] agreement which is relevant for Common Criteria involves 17 European and EFTA national bodies (in July 2017), member bodies of the IEC Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)[4] represent more than 50 countries and the ISASecure agreement concerns less than 5 states. In order to have a dynamic technical exchange between experts over the globe, some organisations (e.g. IECEE) lead technical working groups sharing their knowledge. These technical working groups promote a close collaboration between technical assessors in order to get a common understanding and uniform practices.

Recommendation: In the cybersecurity domain, information evolves rapidly (discovery of vulnerabilities, new attacks, evolution of standards, etc.), and it seems essential to establish experts' networks able to share information quickly and efficiently, such as the IECEE working groups.

2.14 Transparency (by publication)

The results of certification and technical information associated with the process are in the public domain. The information is generally available online from websites managed by Conformity Assessment Bodies and/or scheme owner organisation. This can help all stakeholders (citizens, public organisations, users, insurance companies) in understanding the results of an assessment and selecting *targets* based on the level on certification.

Recommendation: certificates shall be published on centralised website to share this added value (while guaranteeing confidentiality of the report). Preferably, this database should be managed by

[4] https://www.iecee.org/

a dedicated European organisation (but could be managed at the national level or by the CAB itself).

The information to share is contained in the conformity certificate which generally identifies the following data:

- Reference used for assessment (as detailed as possible: sub part / version)
- Identification of the *target* (commercial name)
- Entity or Name of the manufacturer
- Description of the technical scope of assessment (as detailed as possible)
- Version of the software/hardware assessed
- Validity of the certificate
- Logo of the accreditation body or logo of the scheme owner (for international recognition)
- Identification of the assessment report (held by the assessment body)
- Assessment hypothesis (potential exclusion)
- Reference to document containing operating constraints (installation / operations / maintenance provisions)
- Technical description of the *target* and additional information.

All the above information is typically published. A sample of a certificate is available in the annex of this document. All this information allows the end-user to have a clear perimeter of the *target* assessed. This could also be applicable to the National Assessment approach.

2.15 Assessment based on a large choice of international standards

Assessments are based on standards and one of the most important criteria is the choice of the most appropriate and relevant standard. There are many standards existing in various domains, so the selection has to be carefully undertaken such that it is fit for purpose to the *target*. The conformity assessment bodies have to adapt their assessment to the relevant standard.

The “one size fits all” approach will not be able to meet cybersecurity expectations of the stakeholders and particularly the end user.

Through testing, inspecting and certification, third parties provide assurance that the *target* meets the legal requirements and minimises any threat or harm to society and the environment.

This assurance is derived from international standards, published by regulatory authorities, standardisation bodies or technical specifications from professional associations, and are thus widely recognised and accepted in a large panel of market sectors.

It can be noted that the range of various internationally recognised standards can also be applied directly by the organisation, manufacturer or service providers in the self-assessment of their targets. For an increase in trust, an external third party can certify the assessment processes, to ensure that the standards are followed in a correct and complete way.

2.16 Repeatable assessment

When an accredited party performs an assessment, the assessment follows a programme (scheme) ensuring the following properties:

1. It provides the same results through different assessments of the (unchanged) *target.*
2. It provides the same results even if it is performed by a different CAB.

In case of highly complex assessments or in those cases where 100% coverage cannot be achieved, e.g. millions of lines of code, these criteria are often hardly feasible for high levels of security assessments. Another case to consider are the management of zero-days vulnerabilities as a zero-day vulnerability discovered during an assessment by a first CAB might not be detected by a second CAB.

Repeatability of an assessment can be ensured by requiring that the assessment is based on "proof of compliance" with the requirements. In other modes of assessment, like *ethical hacking*, it is dependent on the time / skills of the team.

2.17 Assessment methodology levelled to other domains

A CAB must adapt its methods depending on its domains of activity, taking into account the requirements in the different domains to develop an adequate, efficient and realistic assessment method.

This is achieved by involving all key stakeholders of the domains under consideration, such as manufacturers, end users, national or supranational authoritative bodies, independent experts of the domain, accreditation bodies, testing laboratories, etc.

3 CRITERIA AND CONSIDERATIONS

A number of criteria should be considered to complement the analysis of a cybersecurity assessment. These criteria originate mainly from the internal discussions in ECSO WG1, and the collection of challenges identified in the Challenges of the Industry COTI document [13] and discussed for the definition of the ECSO Meta-Scheme Approach [16].

- Harmonising cybersecurity requirements across Europe and preferably internationally is one of the main objectives. The aim is to prevent different, incompatible, cybersecurity requirements in different countries to avoid costly duplication of development efforts. Such a harmonisation objective also needs to apply to requirements that different countries place on (self-) assessed items. Harmonisation between standards used in self-assessment and third-party certification would allow switching between the two assessment methods with little effort, e.g. third-party certification used on major releases.

- Harmonised requirements should be SMART: Specific, Measurable, Actionable, Realistic and Timely. Not all standards referenced in the State of the Art Syllabus document [1] are defined and written considering this principle in mind.
- The requirements to assess should be as concise as possible, or it may lead to a loss of overview that might generate additional security risks. An example is the comparison between approaches from OWASP / MS SDL focusing on practical requirements and ISO more prone to less concise and wordy requirements.
- Harmonised standards should be open and accessible based on Fair, Reasonable, And Non-Discriminatory (FRAND) principles. Openness contributes to adoption.
- Standards that are used to harmonise requirements on cybersecurity, e.g. defining required evidence and test criteria, should lead to real improved security. Hence, a realistic path from each standardised criterion to a cybersecurity improvement needs to be defined. The effect of formalised cybersecurity standards should also be judged through the eyes of the hacker / malicious actor.

  It is worth considering that cyber sabotage can be assessment aware, thus, the assessment scheme should not become an indication of non-assessed areas where vulnerabilities may be found. This is the reason why evaluation labs (company internal and external) should be encouraged to develop new attacks, and to use new attack tools and new methods. Standards should accommodate this. For example, part of a standard could be a free-format penetration test.
- Self-assessment and attestation should not undermine security. For instance, the latest version of a software library including patches might not have gone through full assessment yet, but it is most certainly more secure than a fully assessed older version with a published vulnerability in it.
- The time for the evaluation and certification should not have a significant impact on security. In case of (external) third-party assessment, the evaluation (and certification) processes could take longer, having a potential impact on security, especially in those cases of organisations or manufacturers that frequently deploy security related updates. Special attention must be given to the definition of an efficient assessment process, such that security relevant updates can be done in an efficient way. A possible approach could be a detailed process-focused certification, which smooth subsequent assessments of the deployed updates.
- Requirements should be technology neutral to avoid providing implicitly particular solution directions.
- Requirements should be jurisdiction aware and tolerant, providing mechanisms to reconcile differences especially in world-wide systems.
- The maturity of an organisation, expressed in its track record, needs to be considered when examining the results of the assessment declarations. The maturity of an organisation could be measured by metrics such as size, age and public reputation, however, they have not always been a guarantee that (avoidable) breaches do not occur. This issue can be assessed by means of accreditation. By obtaining an official accreditation from the National Accreditation Body, an organisation can demonstrate that it has the maturity necessary for conducting the relevant security assessment. Accreditation can apply to both internal and external assessment bodies.
- To foster innovation formal standards must evolve at same speed as the digital society.

- Even without a malicious attacker that is trying to compromise a system, failures or bugs may cause vulnerabilities. Traditionally, an unintentional failure is the subject of failure mode analysis and safety regulation. However, there may be issues where a failure has no effect on the safety, but it may allow a subsequent attacker granting easier access. The definitions of security, safety and failures should be consistent and compatible.
- To achieve meaningful security ratings, the identification of relevant attacks and related security objectives should be done per application domain.
- A full assessment should address all aspects of a system (in combination): the technical parts that compose the system, the interconnections with other systems, and the people managing and using it. The complexity stands in harmonising the assessment of processes and people, e.g. identifying available standards that are suitable for DevOps / continuous delivery.
- Heavy documentation and penetration testing forms can be a bottleneck for accredited self-assessment, as well as for external assessment bodies. Lightweight schemes for *delta* assessment, that avoid too heavy overhead, and lean re-assessment should be defined. Such schemes could be very beneficial to organisations which deploy frequent security updates (e.g. Cloud Service Providers), as well as for products which rely on updates as a means to continuously address new vulnerabilities (e.g. consumer Internet of Things or automotive products).
- It is desirable to have easy to understand “levelled” security standards, i.e., where the level says something meaningfully about the provided corresponding security to end users. In most cases, the language and proper understanding of the cybersecurity strength and appropriate scopes are missing, implying the goal of the standard to be elusive. A known best-practice example of a “levelled” security standard is IEC 62443 [12]. However, even for this standard, doubts have been raised whether the security levels are fully defined. There are strong doubts whether the measures in IEC 62443 are sufficient to fend off state organisations at the highest level, especially as no rationale is provided on how the measures meet their *target*. One can argue that a product is either fit-for-purpose for its specific category (e.g. car, fridge), or it is not, leading to a single level of security requirements, e.g. for consumer devices.
- For items targeting the consumer market, the consumer perspective and the respect of their fundamental rights are relevant. A consideration is to have consumer organisation representation in standardisation setting meetings. Moreover, the profile of potential customers / consumers need to be taken into account when defining the cyber usage of an item.
- In large systems that consists of smaller systems, i.e., *systems of systems*, lean re-assessment should be considered when sub systems reach end-of-life and needs to be replaced as they cannot receive security patches any longer. Only if lean re-assessment of the large system is not possible, then full reassessment should be considered.
- For components with many different intended uses, the main challenge is to identify what schemes exist that provide a meaningful security statement that can be used for the different use-cases. This is even more important when the achieved cybersecurity strength depends significantly on the use-case.
- For highly adaptive / evolving systems, efficient and effective assessment of incremental adaptations is desirable, which may need attention in the applicable schemes and standards.

- It must be ensured that the same security standards apply to small and large players in the same way, with equivalent effect.
- Legislations should not introduce new risks to the European industry. For example, weak mandatory security controls or high fines might potentially harm the innovation in industry rather than educating and raising the security baseline in the industry.
- The long-term impact of the work of the ECSO framework (putting new assessment requirements on products) should be evaluated, because the impact of new requirements on products, systems and services is still uncertain. Requirements may improve but also degrade cybersecurity, may hurt or help competitiveness of the European industrial sector, etc.

4 ASSESSMENT OPTIONS

This section describes the best practices in assessment. It is expected that for the different industry segments, these best-practices might diverge to address the specific needs of the sectors and comply with sector regulations and directives. Often, the business sector of an organisation drives the architecture of the product or service that is being created and maintained. Processes are needed to support each of the components in this architecture, and a matching organisational structure is typically put in place to run these processes. In a nutshell, the Business determines the Architecture, which requires the Processes, implemented by a suitable Organisational structure (BAPO). Therefore, it is to be expected that in different industries, there are different organisational structures and best practices when it comes to cybersecurity.

4.1 Self-assessment

The self-assessment option is suitable for organisations that have sufficient scale to perform cybersecurity assessments in-house and have the capability. Figure 4 shows a possible structure. Items (be it products, services, or as it is more common, product-service combinations) are developed by a development department, usually in collaboration with a set of component suppliers and sub-service providers. Cybersecurity is a development criterion. The developers typically work according to a set of controls defined in one or more standards, and the developed item is designed to meet a set of requirements defined in one or more standards.

Once the item has reached a certain maturity status, it is passed on to a department that is responsible for assessing whether the product is secure. This internal assessment department works according to a set of guidelines that are usually defined in one or more standards. The internal department can be accredited or not. An accredited in-house department is, in the context of this document, an internal department that has been assessed by an external body (accreditation or certification body), certifying that the carried assessment processes are complete and correct. Such an accredited in-house body is considered in this document as part of the third-party category of assessments (see Section 1.2). An unaccredited internal department is regarded as self-assessment.

The assessment department can perform black-box tests, i.e., it does not get access to the design documents of the Item, or white-box assessments, i.e., it may have access to the design documents and ask questions to the developers to deepen and speed up the assessment.

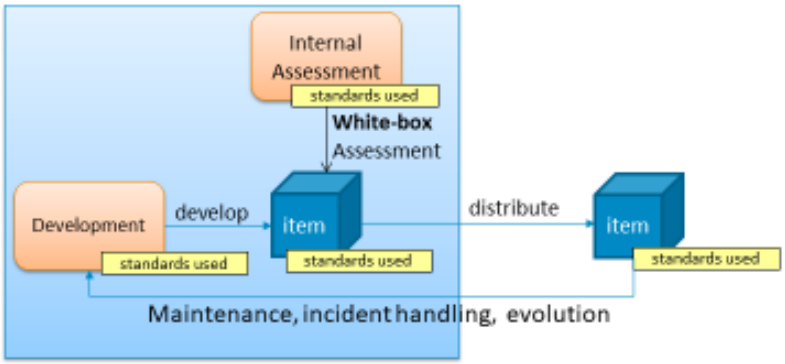

Figure 4 – Unaccredited Assessment

Once the item is released and distributed outside the organisation, the next steps are security maintenance and security incidents handling, for example when one of the components or sub-services used has been compromised. Finally, the item may evolve over time as new versions are released. These ongoing processes can be structured according to certain standards as well.

Ability to compare assessment results

For a fair comparison of suppliers, the internal assessment should be based on public and harmonised standards, to provide transparency in the security aspects that have been evaluated. For possible standards see Section 5.

To avoid the risk that *conforming* to standard requirements could actually lower the security provided by the system or service, it may be possible to include aspects where the standard does not apply, indicating why this is beneficial for security. For example, if requirements were not written down in a strictly technology-neutral way, new security developments may lead to the adoption of better technological solutions that may not strictly satisfy the (old) requirements.

4.2 Third-party assessment options

Many schemes for third-party assessments (on cybersecurity but not limited to) exist depending on the technical domains. The following sections depict some examples of certification schemes to give an overview of the different approaches.

4.2.1 Accredited in-house assessment body

Figure 5 shows a model of assessment by an accredited in-house assessment body. In safety, it is quite common that the development processes are assessed by external third parties, and this may well be applicable and extendable to cybersecurity development and assessment as well. The next step can be to fully accredit these departments. This step authorizes the department (organisation) to also formally issue declarations for its individual products and services that have been assessed against the applicable requirements.

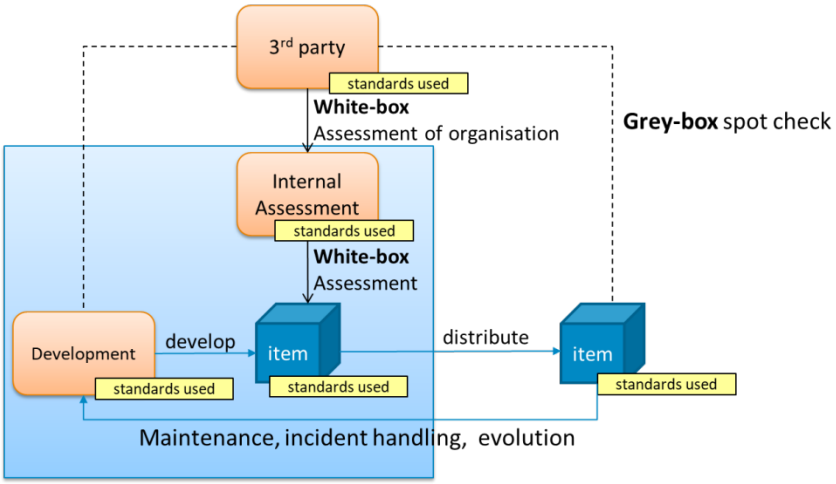

Figure 5 – Accredited Assessment

On top of the basic self-assessment, an accredited in-house assessment adds a third-party assessment of the organisation and of how the organisation structures its cybersecurity processes. As such, it does not directly change the cybersecurity strength of developed items, nor it directly changes how the cybersecurity of a developed item is assessed. However, it does raise the confidence that the assessment processes are performed in full accordance with the standards that are intended to be used.

If the standards that are used for the assessment evolve over time, e.g. to reflect the increasing complexity of cybersecurity, such assessments (and potentially corrective actions) can be seen as a way to keep up to date with the latest developments. Third-party assessments of the organisation then help raising the cybersecurity capabilities that an organisation tries to build.

As a further option, accredited in-house assessment may also be supported by the market surveillance of the items that have been distributed, for instance, to verify in a grey-box mode that the proclaimed security properties are in place.

Note: In the context of this document, the term “accredited in-house body” refers to an internal body which is assessed by an independent external third party, with the goal of confirming its competence and impartiality. It is worth noting that, based on the definitions from the Blue Guide [5], an accredited in-house body can only be accredited by a National Accreditation Body. In other words, an accreditation could result only after an assessment performed by the National Accreditation Body. *As an example, a National Accreditation Body can issue a ISO/IEC 17025* [6] *accreditation to the in-house body, accrediting it for performing testing in line with a relevant scope (ex. Common Criteria* [9]*).* Assessments of the in-house body performed by other external third parties (different from a National Accreditation Body) would not result in an accreditation, but in a certification or licensing. *Such an example can be a third-party lab certifying an in-house body for maintaining a development process in line with IEC 62443* [12]. After discussions within the ECSO WG1, it was concluded that a strict situation in which the in-house body can only be assessed by the National Accreditation Body would induce difficulties and possible limitations. Therefore, an approach in which the assessment can be performed by either a National Accreditation Body, or a different (accredited and recognised) third party, would be desirable. For simplicity, in this document both of these options are covered under the same term of “accredited in-house body”.

4.2.2 External assessment body

An alternative to the accredited in-house assessment body is that the security assessment is performed by an external body. This body is in turn accredited by a relevant accreditation body, for performing assessment services with respect to a specific standard (for example ISO/IEC 17025 [6] accreditation with the scope of IEC 62443 [12] assessments). In addition to that, the external body can also be licensed to operate under a certain evaluation scheme. An example of that is the Common Criteria evaluation process, where the accredited labs are also licensed by the national Common Criteria body, in order to be allowed to perform subsequent Common Criteria evaluations.

The external body can still rely a lot on the evaluation evidence provided by the developer. This can also include test results collected by the developer following its own testing. The role of the external body will be to assess the completeness and correctness of the provided evidence, as well as to perform additional validation testing on the relevant scope.

The assessment performed by an external assessment body raises the confidence in the provided evaluation results, as the external body is fully independent from the evaluated organisation or product. At the same time, confidence is obtained that the evaluation was carried out completely and correctly following the relevant evaluation criteria (as an example, the Common Criteria methodology).

One of the concerns in these types of assessments is regarding the efficiency of the process, especially in dealing with updates in the evaluated and certified scope. In case such updates are frequent (for example updates resulting from an organisation that follows a DevOps methodology), constantly involving an external body to re-assess each new version will very likely result in a cumbersome process, affecting the actual security or time to market.

4.3 Specific schemes for specific domains

Figure 6 shows three specific schemes (or programmes).

The “Blue Guide” [5] scheme is related to products sold on the European Common Market. It is covered by related EU directives and the regulation related to product liability (Decision 768/2008 [17]) and to accreditation and market surveillance (Regulation 765/2008 [10]). The Blue Guide introduces conformity assessment performed by an external (or accredited in-house) third party. It defines how assessments on specific standards can be used to demonstrate a *presumption of conformity* – those standards called harmonised standards, are generally technical or domain dependent, e.g. machinery, lift.

The next scheme in Figure 6 represents the process used in the nuclear domain. Some characteristics inherent to this domain should be noted. Firstly, the term “*certification*” is not commonly used, “*qualification*” is preferred. Secondly, the nuclear operator has a central role and refers directly to national safety authorities which deliver the operational licenses. Therefore, the operator is responsible for the safety aspects of critical devices and activities led by contractors/suppliers on the plant. Third-party bodies are not directly involved in this scheme.

The last scheme represented in Figure 6 is relative to the railway sector. This is the most complex one, due to the presence of numerous stakeholders. Qualified & Accredited bodies have an important role; they deliver certificates which are required to the operator by the authorities prior to be granted with a license to operate.

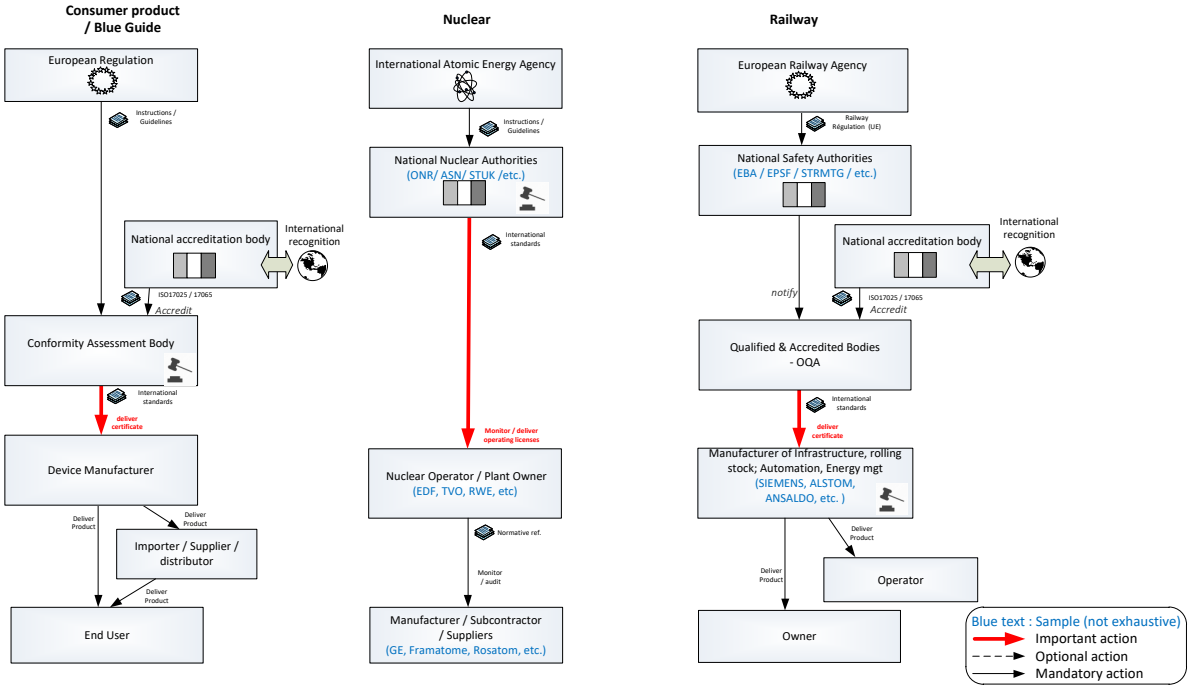

Figure 6 – Several approaches of certification schemes

4.4 Existing schemes for cybersecurity domain

Figure 7 depicts some examples of certification schemes used in the cybersecurity domain.

The scheme depicted on the left side of Figure 7 is typically used for Common Criteria assessment. National cybersecurity agencies deliver the certification based upon an assessment performed by licensed companies (licenses are delivered by the national agency). For this scheme, international recognition is ensured at two levels:

- By the National Accreditation Body (NAB),
- By specific agreement (SOG-IS [15]) signed by several national agencies over the world. This ensures an efficient sharing of technical information (e.g. protection profiles, certification policies).

The other schemes shown in Figure 7 are related to an assessment based on private programmes. The certification and assessment teams compose the Conformity Assessment Body (CAB). The CAB assesses *targets* in regards of standards following internal assessment programmes. For this kind of scheme, the accreditation by their national body is not necessarily mandatory but provides additional recognition and brings added value to the certificate. As in the Common Criteria scheme, international recognition operates at two levels.

Note: In some cases, CAB are organised in two separate entities (companies). Tests and/or assessments (technical activities) are ensured by dedicate laboratories (CBTL – Certification Body Testing Laboratories) which report to another organisation (NCB - National Certification Bodies) in charge of issuance of certificates. This is typically the organisation implemented by IECEE[4].

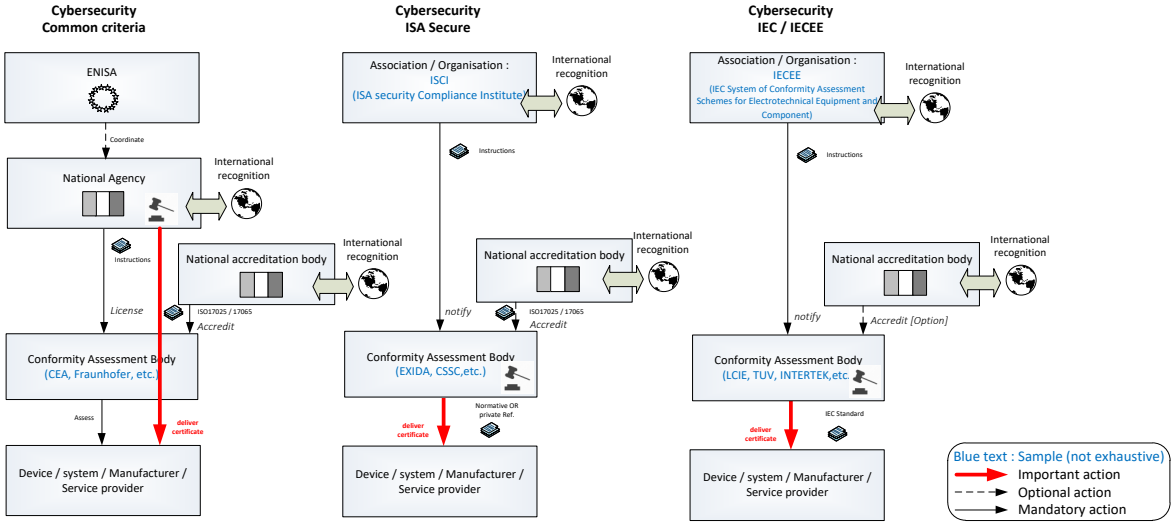

Figure 7 – Samples of certification schemes for cybersecurity domain

4.5 Cybersecurity overview

Here below, a chart resuming all stakes to be taken into account for an assessment in cybersecurity.

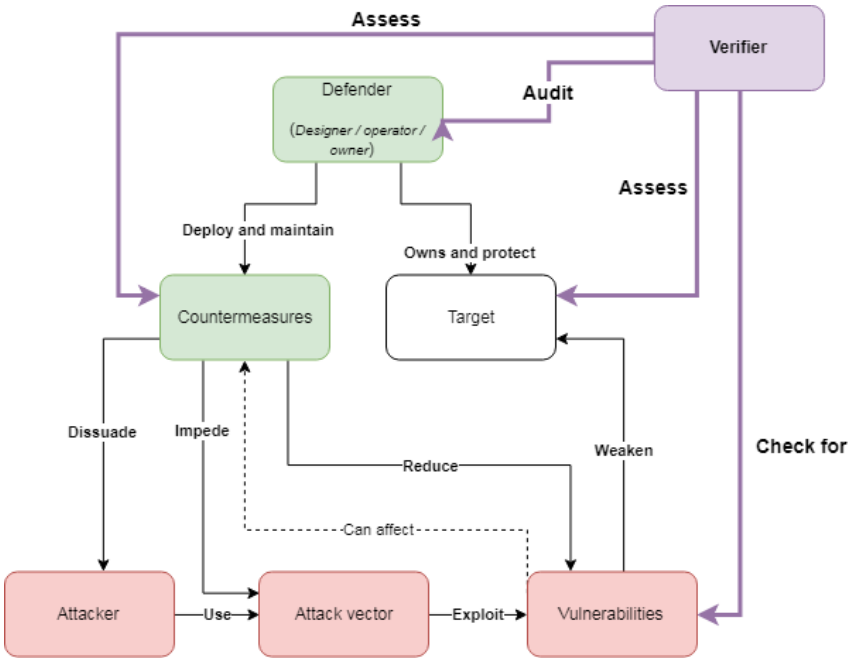

Figure 8 – Overview of typical assessment

5 STANDARDS TO USE IN ASSESSMENT

As seen earlier and as identified in the ECSO State of the Art Syllabus [1], there exists a plethora of standards addressing different kinds of requirements. To give the opportunity for the end-user to use components with a certain level of confidence in cybersecurity, a selection of relevant standards could be linked to different classes of *targets*. Depending on the class of *targets* and the intended use, a smaller set of standards could be more appropriate to use.

This selection could be done by National/European bodies or by expert groups and would be an entry point for the assessments and so the Conformity Assessment Bodies (CABs).

At the moment, there are no harmonised requirements on self-assessment in the EU, but there are a number of standards available that can be used by organisations to structure their self-assessment or to assess their products or services against. For example, ISO/IEC 17025 [6] gives general requirements for the competence of testing and calibration laboratories, these can also apply to cybersecurity assessments. Another example is OWASP, which provides a generic framework/guide for use with application testing [18]. More sector specific is for example IEC 62304 [19] that gives requirements on medical device lifecycles.

Assessment against a selected set of security requirements.

- OWASP Guides (Developer, Testing, Code Review) https://www.owasp.org/
- Common Weakness Enumeration (CWE) http://cwe.mitre.org/
- Common Attack Pattern Enumeration and Classification (CAPEC) https://capec.mitre.org/

Assessment against selected (recognised) security standards.

- ISO/IEC 15408 (Information technology - Evaluation criteria for IT security) [9]
- ISO/IEC 27002 (Code of practice for information security controls) [20]
- ISO/IEC 27017 (Code of practice for information security controls for cloud services) [21]
- IEC 62443-3-3 (System security requirements and security levels) [12]
- NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations) [22]
- Sector specific (e.g. ISO/IEC 62304 for medical devices) [19]

Self-Assessment against the (ENISA proposed) security certification framework.

- ENISA can help harmonise standards that should be used in self-assessment, and (see next section) provide clear rules on the relation between self-assessment and third-party or national assessments, and what the conditions are for exchanging one assessment type with the other.

5.1 Standards and Regulations

The following standards and regulations define the whole framework on the conformity assessment (developed later).

- Part “General normative context” (ISO/IEC 17000 [23], ISO/IEC 17025 [6] and ISO/IEC 17065 [8])
- Part “Legal Context” (EC regulation) (768/2008 [17] (marketing of products) and 765/2008 [10] (accreditation and market surveillance relating of products)).

5.2 Accreditation mechanisms

The recognition of an assessment depends on the maturity and quality of the process (resources and procedures) to perform an assessment. This framework is handled by accreditation which defines a clear way to operate. Hereunder the stakes of accreditation are summarised.

The methodology is structured and is based on a unique vocabulary defining different roles and objectives (defined in ISO/IEC 17011 [24]):

- Conformity Assessment (CA): Demonstration that specified requirements relating to a *target* are fulfilled.
- Conformity Assessment Body (CAB): Body that performs CA services (e.g. Bureau Veritas, SGS, TUV, UL).
- Conformity Assessment System Rules: Procedures and management for carrying out CA (e.g. IEC62443 [12], ISO27001 [25], IEC 15408 [9], Harmonised standards).
- Conformity Assessment Scheme (or Programme): CA system related to specified objects of CA, to which the same specified requirements, specific rules and procedures apply.
- Accreditation body (AB): National body that gives accreditation to CAB (e.g. COFRAC, DAKKS).

CABs are regularly audited by accreditation bodies to ensure they comply with process and programmes. The methodologies used to perform those evaluations are defined and based on standards allowing different schemes, the schemes are based on different techniques of assessment: testing, inspection, review, audit, qualification:

- ISO/IEC 17000 Conformity assessment — Vocabulary and general principles [23].
- ISO/IEC 17020 Conformity assessment — Requirements for the operation of various types of bodies performing inspection [26].
- ISO/IEC 17021 Conformity assessment — Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements [27].
- ISO/IEC 17024 Conformity assessment - General requirements for bodies operating certification of persons [28].
- ISO/IEC 17025 Conformity assessment — General requirements for the competence of testing and calibration laboratories [29].
- ISO/IEC 17065 Conformity assessment — Requirements for bodies certifying products, processes and services [7].
- ISO/IEC 17067 Conformity assessment -- Fundamentals of product certification and guidelines for product certification schemes [30].

6 RELATION / EXCHANGEABILITY BETWEEN THIRD-PARTY / NATIONAL CERTIFICATION / SELF-DECLARATION / SELF-ASSESSMENT

Assessments are typically part of a larger scheme or development lifecycle. Within a scheme conformity assessment and its relation to other assessment types and accreditation that make up the scheme are defined. Similarly, a conformity assessment may be replaced or coexist with other assessment types. The scheme may be complemented by governmental oversight, market surveillance, etc.

As introduced above, self-assessment, third-party certification and national certification can in many cases be based on the same cybersecurity standards. Therefore, when assessing the required cybersecurity properties of a systems or services, two choices need to be made:

1. Which cybersecurity standards will apply, and
2. Which party will assess that the requirements are actually met, and how it can be ensured that this party will do a proper assessment.

The value of the assessment is determined by the degree the cybersecurity standards, that are assessed, adequately represent the actual cybersecurity requirements, that need to be satisfied. The selection of the right cybersecurity standard depends mostly on the market. Different cybersecurity standards pose more-or-less strong cybersecurity requirements on the assessed items. As it is currently not realistic to demand nation-state level security strength from consumer devices, a risk-based trade-off is needed to determine the cybersecurity requirements imposed on the item. A risk-based approach could be instrumented through the specification of (security) baseline profiles for particular categories, e.g. collections of use cases or market segments.

Accredited in-house assessment bodies are enabled by external third-party accreditation. The vendor assesses the product or service and the external third party accredits the vendor organisation and its development and assessment processes.

In principle, accredited in-house assessments are exchangeable with assessments by external bodies, they may use the same requirements and standards. For organisations incapable of accredited in-house assessment, external third-party assessments would be an alternative or for instance bringing resources from consulting services in the firm.

Furthermore, the level of independence of the assessor of the developer is seen as a measure of trustworthiness. If there is insufficient trust in the self-assessment capabilities of a developer, accredited in-house assessment may increase the confidence that the assessment is carried out properly. If the accreditation of an in-house department is still considered insufficiently trustworthy, an external accredited third party may be tasked to do the assessment. This can be done either as a third-party declaration based on documents / materials supplied by the developer, or it can be

structured as a fully self-contained third-party assessment and certification. Finally, there may be situations in which nothing less than a national body is trusted to perform the assessments.

In particular for complex systems, different assessment types according to different cybersecurity standards may co-exist, e.g. when next to a global assessment of the overall product or service, individual components are assessed. Especially when third parties are highly specialised in a particular assessment, it may be beneficial to mix self-assessment of more generic standards with third-party assessments of highly specialised standards.

To a large extent oversight determines the effectiveness of a scheme, in particular for self-assessment. While, market surveillance should provide insight in the trends of assessment effectiveness and organisational behaviour. Governments and legislators may use this to enforce or update policies and legislations. It must be ensured that any result of self- or third-party assessment actually pertains to the items delivered to the market. Beside certification schemes, this may also affect (harmonised) standards that provide the cybersecurity requirements which are assessed. The latter also involves a relationship with industry and stakeholders through standardisation.

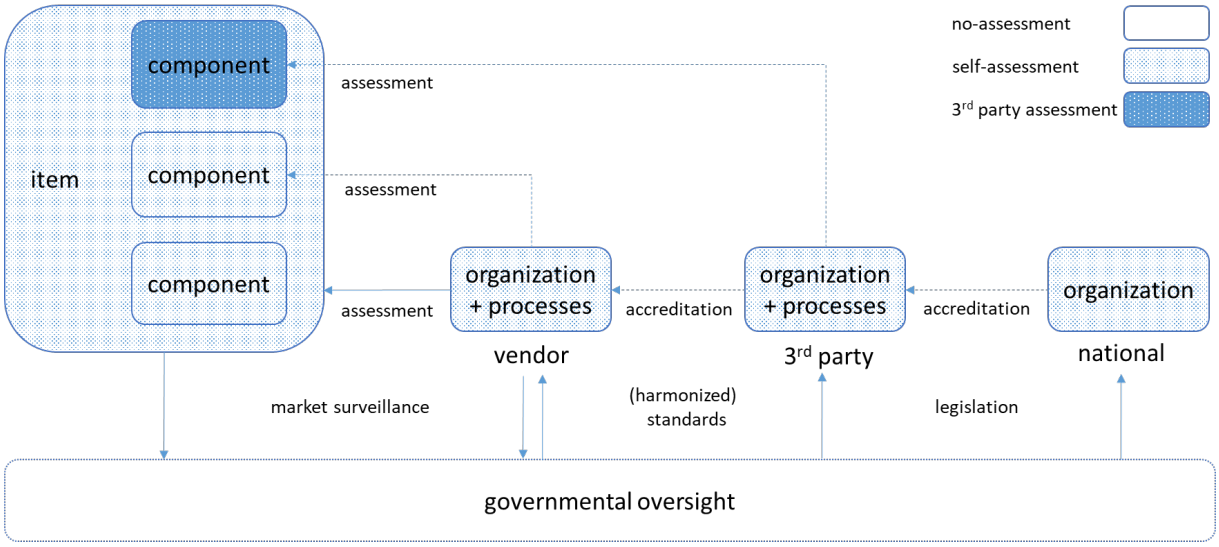

Figure 9 – Relation / exchangeability with third-party / national certification / self-declaration

Figure 9 captures in a single view the concepts above discussed. On the left it is depicted the *item* subject to the assessment. On the right there are the organisations involved in the assessment process, respectively the *vendor*, the *third party* and the *national body*. The organisations can be involved by either performing the *assessment* of the (*component of an) item*, or the *accreditation* of another *organisation* and its *processes* for its role in the assessment process. Self-assessment / self-declaration is captured in the second block from the left of Figure 9 by the vendor performing the assessment of the item or component. The figure also illustrates the option when the third-party certification body assesses a component or item directly, either in co-existence with self-assessment or as an alternative. The accreditation of a third party by a national body is optional. All organisations are subject to the legislation that defines their role, which may also mandate certain standards, by appropriate governmental or legislative bodies. These bodies also monitor how items and organisations perform in the market and society.

6.1 Tailor made assessment

An assessment has to follow a defined process, but it is adapted on customer constraints with a degree of flexibility.

6.1.1 Assessment by layer

The system of certification aims to take benefits from other certified items in order to minimise the amount of work that needs to be repeated. Typically, this recognition is the key to perform an efficient assessment. For example, even if the assessment is on cybersecurity, credits from a quality management certification can be used in the cybersecurity demonstration. Indeed, some cybersecurity requirements are related to corporate processes, and, in a certain way, credits from quality certification provide some evidences which can be reused, thus reducing the effort required during the cybersecurity evaluation.

Moreover, in the regulatory context (e.g. medical devices, toys, construction products), cybersecurity will be a goal as important, i.e., mandatory, as safety because some cybersecurity measures are common with safety measures, hence, it makes sense to use safety certification for particular items.

6.1.2 Partial assessment

In the software development domain, several types of development models exist: V cycle, Waterfall, agile, spiral, etc. As the assessment scheme is independent of the development model, it is possible to adapt the assessment steps to any product development cycle. As illustrated below partial assessment could be a good alternative sticking as close to the development cycle. Figure 10 illustrates this process.

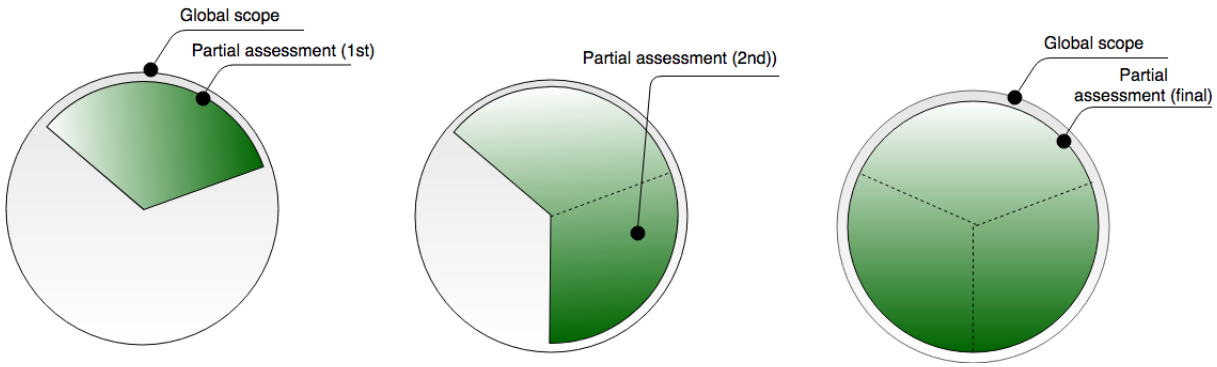

Figure 10 – An example of process of partial assessment close to the development cycle

6.1.3 Initial and renewal assessment

Another typical use case is the assessment with two levels of verification. For the first version of the *target*, all the requirements of the standard are checked. For the updated versions, the assessment is performed considering the differences from the last assessed version (technical

controls) and up to date process of development (organisational controls including some specific verification on the continuous monitoring of the *target*). In this case, the assessment is lighter while still ensuring the same level of confidence. This use case requires a classification of *target* changes (minor, major, critical...), which would have an impact of a necessary renewal assessment or not. This process is illustrated below:

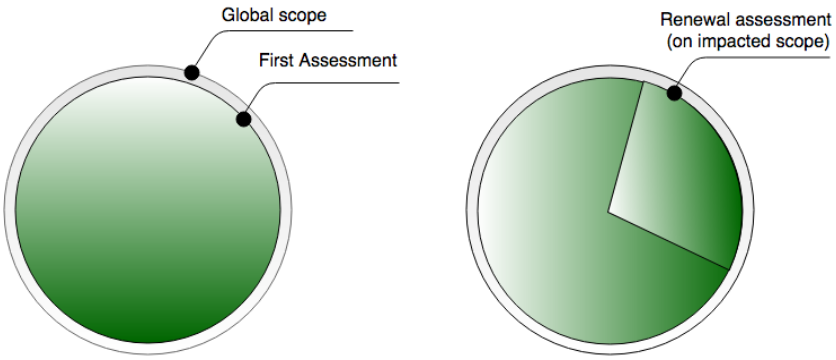

Figure 11 – Initial and renewal assessment

With the same reasoning, such processes use Initial / renewal assessment in order maintain the validity of certificates (e.g. ISO27001 / ISO9001). This is typically used for global companies with multiple locations where the full assessment is practiced at the top management processes (head office) and renewal ones are cyclically executed for satellite sites. Following illustration shows this process.

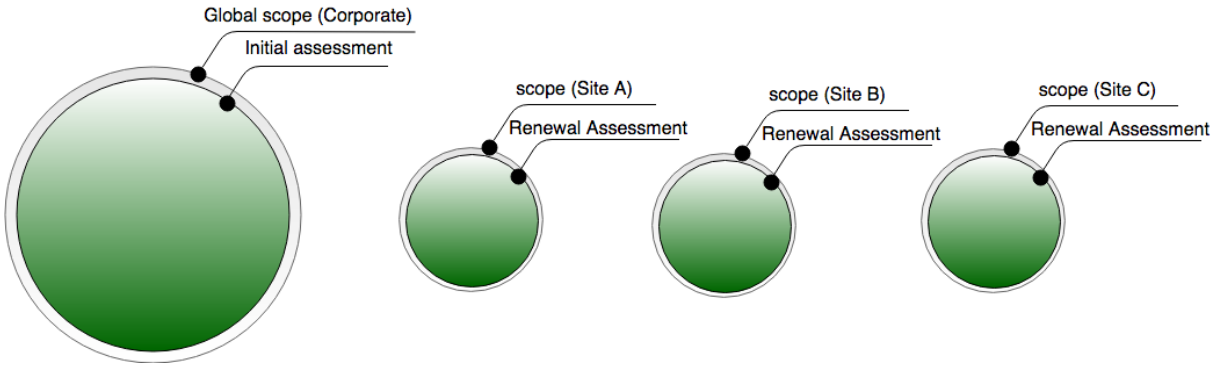

Figure 12 – Initial and renewal assessment: the example of global companies with mutiple sites

6.2 Principles of Conformity Assessment

The evaluation measures presented in the following section can be adapted depending on the assurance level of the targets.

6.2.1 Evaluation of measures

At each level of assurance (basic, substantial and high, as defined in the Cybersecurity Act [4]), the depth of the assessment has to be proportional to the assurance level.

When highest levels of assurance are requested, ethical hacking provides increased assurance that vulnerabilities are covered. This concept is illustrated below in Figure 13

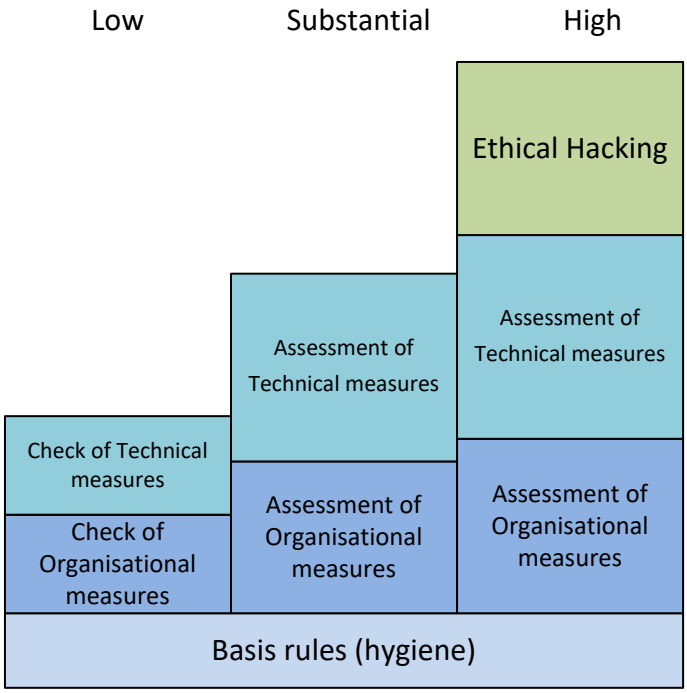

Figure 13 – Example of gradual assessment approach

The following information have to be considered:

- The ranking for the different levels are given as an example – it has to be adjusted.
- The evaluation measures are cumulative through the different assurance levels (Substantial includes measures from the Low level – High includes Substantial measures)

7 CONCLUSIONS & RECOMMENDATIONS

Organisations that are building their cybersecurity capabilities as a key part of their business often resort to a process-based approach to cybersecurity. As an example, security-assessment processes for products and services contribute to their overall security. When the manufacturer or the service provider uses processes and organisational structures for assessment that have not been inspected and accredited by a third party for the particular self-assessment activities, this is called unaccredited self-assessment. If these processes themselves are carried out with a certain level of independence between design teams and an (accredited) in-house body or external body, this is called third-party assessment. Since it is impossible to test against all attacks, the processes to deal with the monitoring of vulnerabilities and post-compromise management are equally essential ingredients for cybersecurity.

When assessing the required cybersecurity properties of a system or service, two choices need to be made: 1) which cybersecurity standards will apply, and 2) which party will assess that the requirements are actually met. Which cybersecurity standards are relevant is market dependent. Depending on the level of assurance, basic rules, such as assessment of organisational measures, conformity assessment of technical measures and ethical hacking techniques, can all contribute to the overall assessment. As it is currently not realistic to demand nation-state level security strength from e.g. consumer devices, a risk-based trade-off is needed in what cybersecurity requirements are adhered to. The level of independence of the assessor may influence confidence in the assessment but has no bearing on the security requirements.

Improving security through the right mix of assessments can provide many benefits: it can link with risk-management, help build in-house cybersecurity capabilities and benefit from economy-of-scale, avoid double processes in regulated industries, allow tight integration in the full lifecycle management and modern DevOps methodologies, simplify protection of Intellectual Property, support a robust decentralised digital economy, promote low cost and fast time to market, avoid supplier lock-in and strengthen security by assessments performed by multiple parties, provide impartial assessments that provide a high level of trust, strengthen company procedures to resists market pressure to shortcut security assessments, increase confidence and transparency to customers, consumers and authorities, and provide international recognition of developed items. It can also enable repeatable assessments or provide for a large choice of international standards that can be tailored to specific domains, while a combination of assessment methods can be used when high levels of assurances are needed. Market surveillance techniques that do not rely on developer-supplied information are the only way to address the issue that fraudulent organisations may provide false evidence to evaluations. Naturally, in-house assessment options are only fully available to organisations that have built the required capabilities.

It is possible to adapt the assessment steps to any product development cycle and any organisational structure. Partial assessment can be a good alternative if full assessment is not feasible. For example, as many systems and organisations are structured in a layered fashion, assessment can be performed by layer. Over time, renewal assessments can be made (cost) effective by focusing on the differences from the previous assessment, or by assessing different security aspects.

Harmonising cybersecurity requirements is a main objective for all assessment types, as it allows for a single digital market of all products and services. At this time, there are no harmonised

requirements on self-assessment in the EU, but there are a number of standards available that can be used by organisations to assess their products or services against. We recommend that ENISA also helps harmonise the standards used for both self-assessment and the various types of third-party assessment and defines the conditions for exchanging one assessment method with another.

APPENDIX: EXAMPLE OF A CERTIFICATE

Conformity assessment body (CAB) logo

TYPE CERTIFICATE BY ASSESSMENT OF THE PRODUCT DESIGN

Issued to

[Customer's legal name and address]

Certifies that the design of the product mentioned below has been assessed and fulfills the relevant requirements of the following standard:

[International standard used for the assesment]

[Product information: Commercial name]

Is compliant with the cybersecurity level [SL-XY0]*,
according to the description and the configuration defined in the Appendix

*Technical information regarding the assesment

This certificate only applies to the design of the product (as referred above) and to the corresponding technical file.

Assessment report: [Reference number]

The Appendix is an integral part of this certificate.

Certificate No: [.....]
Emission date: [dd/mm/yyyy]
End of validity: [dd/mm/yyyy]

[Signature of the cybersecurity certification authority representative]

Accredited body logo

Name of the certification organisation
Address of the certification organisation

This certificate consists of 2 pages (1 out of 2)

The product versions of the hardware components used for the assessment:

Component type	Component	Product Reference	Hardware Version	Software Version
[Series]	[Specifications]	[Ref. No]	[v X.Y]	[v X.Y]

Context of use and recommendations are stated in the security manual [document reference number]**.**

These elements must be considered for each implementation of the product by the final user.

The certified security function(s) of the product:

		Assessment Scope		Final Results	
	FR ID O	FR Description	Applicability	Security Level Capability	Security Level Achieved
Foundational Requirements	FR 1 (AC)	Identification & authentication control	Yes	SLC 1	SLA 1
	FR 2 (UC)	Use control	No	SLC 2	SLA 2
	FR 3 [...]	[...]	[Yes/No]	SLC [...]	SLA [...]
	FR 4 [...]	[...]	[Yes/No]	SLC [...]	SLA [...]
	FR 5 [...]	[...]	[Yes/No]	SLC [...]	SLA[...]

Remark: [additional information used for precision]

[Legal Disclaimer]

[Terms of Use]

This certificate consists of 2 pages (2 out of 2)

Name of the certification organisation

Address of the certification organisation

REFERENCES

[1] European Cyber Security Organisation (ECSO) WG1, *State-of-the-Art Syllabus: Overview of existing Cybersecurity standards and certification schemes,* Brussels, 2017.

[2] "The Untold Story of NotPetya, the Most Devastating Cyber attack in History," [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. [Accessed 13 May 2019].

[3] NIST, "SP 800-160 Systems Security Engineering," 2018.

[4] European Parliament, Council of the European Union, *Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).*

[5] European Commission, "Commission Notice: The 'Blue Guide' on the implementation of EU products rules 2016 (2016/C 272/01)," 2016.

[6] ISO/IEC 17025, "General requirements for the competence of testing and calibration laboratories," 2017.

[7] ISO/IEC 17065, "Conformity assessment -- Requirements for bodies certifying products, processes and services," 2012 (reviewed and confirmed in 2018).

[8] ISO/IEC 17065, "Conformity assessment — Requirements for bodies certifying products, processes and services," 2012.

[9] ISO/IEC 15408, "Information technology -- Security techniques -- Evaluation criteria for IT security," 2009.

[10] European Parliament, Council of the European Union, "Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93," 9 July 2008.

[11] ENISA, "Considerations on ICT security certification in EU - Survey Report," September 2017.

[12] IEC 62443, "Security for industrial automation and control systems".

[13] European Cyber Security Organisation (ECSO) WG1, *Challenges of the Industry. Internal document,* Brussels, 2017.

[14] ANSSI, "Certification de Securite de Premier Niveau (CSPN)," 2008. [Online]. Available: https://www.ssi.gouv.fr/administration/produits-certifies/cspn/les-centres-devaluation/. [Accessed December 2017].

[15] Security, Senior Officials Group Information Systems, “SOGIS,” [Online]. Available: http://www.sogis.org/.

[16] European Cyber Security Organisation (ECSO) WG1, “European Cyber Security Certification: A Meta-Scheme Approach v1.0,” 2017.

[17] European Parliament, Council of the European Union, “Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC,” 9 July 2008.

[18] Open Web Application Security Project (OWASP), “OWASP Testing Guide v4,” available at https://www.owasp.org/images/1/19/OTGv4.pdf, 2015.

[19] IEC 62304, “Medical device software – Software life cycle processes,” 2006.

[20] ISO/IEC 27002, “Information technology -- Security techniques -- Code of practice for information security controls,” 2013.

[21] ISO/IEC 27017, “Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services,” 2015.

[22] NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” 2013.

[23] ISO/IEC 17000, “Conformity assessment -- Vocabulary and general principles,” 2004.

[24] ISO/IEC 17011, “Conformity assessment -- Requirements for accreditation bodies accrediting conformity assessment bodies,” 2017.

[25] ISO/IEC 27001, “Information technology -- Security techniques -- Information security management systems -- Requirements,” 2013.

[26] ISO/IEC 17020, “Conformity assessment -- Requirements for the operation of various types of bodies performing inspection,” 2012 (reviewed and confirmed in 2017).

[27] ISO/IEC 17021-1, “Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements,” 2015.

[28] ISO/IEC 17024, “Conformity assessment -- General requirements for bodies operating certification of persons,” 2012 (reviewed and confirmed in 2018).

[29] ISO/IEC 17025, “General requirements for the competence of testing and calibration laboratories,” 2017.

[30] ISO/IEC 17067, “Conformity assessment -- Fundamentals of product certification and guidelines for product certification schemes,” 2013.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

10, RUE MONTOYER - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE: WWW.ECS-ORG.EU - TWITTER: ECSO_EU