Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence, Civil Protection and Sport DDPS

National Cyber Security Centre NCSC
Analysis and Prevention

10 June 2025

Measurability and testability of IT security

1. Introduction

"Measure what is measurable, and make measurable what is not so" is a quote attributed to the Italian polymath, mathematician and physicist Galileo Galilei.[1] IT security specialists face similar challenges today. The management of companies and organisations demands information about the status of their own IT security or that of their suppliers. Similar issues are the subject of public debate. It is often expected that the IT security of products, services and organisations be tested before they are deployed or used, or before working together with service providers.

To date, numerous attempts have been made to measure IT security. Having the measurement results or the achievement of a defined "IT target security" confirmed (especially in the form of certificates) is common today and is often required in connection with the fulfilment of compliance requirements or the awarding of contracts. IT security certification services have now developed into a lucrative business model.

Nevertheless, the question remains as to how IT security can be sustainably improved and whether its measurement, testing and even certification are necessary prerequisites. There may be more than one answer to this question, and there are no "magic bullets" for improving IT security. Nevertheless, the National Cyber Security Centre (NCSC) is convinced that there is a need for complementary or alternative approaches to today's widely used methods for measuring and testing IT security.

Before discussing this topic in four theses, the current situation and the underlying problem will first be analysed in more detail [1].[2]

2. Definition of the problem

To be able to measure meaningfully, it is first necessary to define what exactly is meant by the "variable" to be measured. This is a trivial statement, but suitable definitions of "security" as a variable to be measured in general and "IT security' in particular are not easy to find.

[1] There is no historical evidence that Galileo actually said this, however. Nevertheless, the quote is considered emblematic of Galileo's attitude, which continues to characterise (scientific) research to this day.

[2] The presentation in the next section is a summary derived from [1], where additional useful explanations and details can be found.

Once this difficulty has been highlighted, two approaches to measuring IT security will be presented, both of which, however, have considerable disadvantages.

a. Definition of security

It is difficult to define "security" because it can vary depending on the context and area of application. However, the essence of all definitions is that there are no serious dangers, threats or risks in a particular situation. A stakeholder who is sufficiently well prepared for all possible eventualities and can always react appropriately is considered secure. However, what constitutes "serious' dangers, threats and risks, being "sufficiently well" prepared and "appropriate" reactions depends not only on the situation, but also on the observer. This means that the concept of security is subjective and depends in part on the observer's perception and willingness to accept some level of risk, meaning that there is no precise definition that is the same for everyone. However, if you have a concept such as "security+, which is subjective and cannot be defined precisely and consistently for everyone, measurement or testing – according to the maxim "if you can't define it, you can't measure it" [2] – is not possible or only possible with restrictions. The difficulty arises in particular from the fact that although a metric or test criteria would be required that are clear and unambiguous, these cannot be found due to the imprecise definition.

b. Measurability – verifying and falsifying approaches

Often, one may at least try to find properties and features that are characteristic of the term and, to a certain extent, can be measured, tested or verified. In such a *verifying approach*, a simpler definition must be constructed for the term so that verification is feasible [1]. One obvious possibility is to replace IT security with one or more other properties or characteristics that can be measured and thus verified. Think of the classic "CIA" triad, for example, in which IT security is replaced by the three properties of confidentiality, integrity and availability. An IT system is described as secure if it protects the confidentiality, integrity and availability of the stored, processed and transmitted data. Breaking down a complex, difficult-to-manage system property such as IT security into sub-aspects is intended to increase its measurability and testability, which is nevertheless only possible to a limited extent due to its inherent complexity.[3]

A further attempt to define and measure IT security is the development of the Common Criteria for Information Technology Security Evaluation (referred to simply as "common criteria" and abbreviated as CC). The CC have been used since the turn of the millennium to evaluate the security of IT products and their components and to certify them for the international market on this basis [3]. Here too, attempts are made to define security via verifiable properties and characteristics, such as functionality classes and trustworthiness (in terms of correctness of implementation and depth of testing). However, the CC have not yet established themselves in the field of evaluation and certification, and the number of certified IT products is still comparatively small. In addition, certifiable products and components tend to be designed for individual functions and in this sense are not particularly complex (e.g. smartcards and smartcard readers or sensors). As soon as a product reaches a certain level

[3] The procedure described is a fundamental concept in computer science and is known as *divide-and-conquer*. The aim is to *divide* a problem into sub-problems, which are solved individually (*conquered*) and then combined to form the overall solution. In the case of IT security, this approach fails because it cannot be reduced to the properties of confidentiality, integrity and availability. Rather, IT security encompasses other aspects such as reliability, anonymity, efficiency or user-friendliness, which are not only impossible to consider or analyse in isolation, but also sometimes conflict with each other, such as authenticity and reliability on the one hand and anonymity on the other (e.g. in the case of e-voting).

of complexity, evaluation and certification is hardly possible and would, in principle, have to be repeated for each new release, at least in some simplified form.

Verifying approaches are also used in the area of organisational security and IT-related business processes: if an organisation wants to present itself as secure and acting in accordance with best practices in the area of IT security, the establishment, implementation, maintenance and continuous improvement of a documented information security management system (ISMS) in accordance with ISO/IEC 27001 [4] is an option. To achieve greater visibility, such an ISMS can even be certified. Security is reduced to the existence of an ISMS with corresponding security control measures, i.e. it is assumed that an organisation is acting securely if it can rely on such an ISMS. Whether the individual security control measures are also suitable for meeting the organisation's security requirements remains unanswered or at the discretion of the auditor. It is therefore not clear a priori to what extent this assumption is justified and to what extent security correlates with the existence of an ISMS in accordance with ISO/IEC 27001. Due to these uncertainties, attempts to derive security metrics from ISMS implementation are often difficult or inadequate.

In addition to the verifying approaches just described, there are also *falsifying approaches*. A falsifying approach does not attempt to define IT security using verifiable properties and features. Instead, an attempt is made to show that an IT system under discussion and to be tested can be compromised in a certain way. This rather proves insecurity and thus disproves security. Such a falsifying approach is therefore basically designed for a test, where the test consists of the fact that the IT system cannot be compromised. At best, a metric could be derived from the difficulty of compromise, but such a metric would also be arbitrary to some extent.

In IT security, the system to be tested must therefore be compromised as part of a falsifying approach. To do this, suitable attack vectors must be found and put together in such a way that successfully compromises the system. This is a heuristic and creative activity that largely depends on the expert knowledge and skills of the tester. Instead of a predefined list of properties and characteristics that can be checked individually, such a list is created in an ad hoc manner (i.e. during the test). Although this has the advantage that a test is not predictable, the result depends on the tester and is to a certain extent arbitrary. While not ideal, this is the best possible solution in many areas. A correspondingly large number of offers for such security tests are available on the market. Think of ethical hackers, penetration testers, bug bounty hunters and red teams. They all offer audits and tests that can differ greatly in terms of methodology, effort and intensity.

The above explanations have shown that security is a concept that not only cannot be precisely defined and tested accordingly, but strictly speaking can only be falsified. Moreover, even a lack of falsification still does not allow any absolute statement to be made about security. Even an IT system that is proven not to be insecure is not necessarily secure, for example if the (measurement) result is attributable to the experts' lack of skills or resources.

To summarise, verifying approaches deliver the desired results in terms of objectivity and traceability, and in this sense are also the declared aim of scientific endeavours (also in the field of IT security). However, such approaches (as described for CC certificates) are only possible for small and simple products or components for which a comprehensive and meaningful set of verifiable properties and characteristics can be defined. Above a certain size and complexity, this is no longer possible, so that falsifying security tests are required.[4]

Certification will be discussed in more detail below.

c. Certification

Various certifications now exist, primarily in the area of verifying approaches, which all require a measurement or test of IT security and serve as proof of the quality assurance of standards. They are offered both for product standards (CC certificates) and for standards in the area of services and organisations (ISO/IEC 27001 certificates).

However, none of these certifications have gained widespread acceptance to date. Where such certificates are used, there are usually also corresponding regulatory requirements, all of which are aimed at influencing the trustworthy behaviour of an organisation and thus either supporting customers or ensuring the availability of certain goods or services relevant to the functioning of a country. In addition to the difficulty of finding simplifying definitions with properties and features characteristic of IT security, the main problems with these approaches are that certifications are complex and expensive, and that the market for certificates itself shows signs of a "lemon market" [5].[5] Accordingly, there is a risk that the quality of certificates will erode under constant price pressure. The only tools available to counteract – and ideally prevent – such erosion are state accreditation of authorised certification bodies and regulation of their liability. If a certificate can be issued without the simultaneous assumption of liability claims, then it appears difficult to maintain a high quality and informative value of the certificates. In addition, the market for certificates is organised internationally, so that the control options of individual states are limited by default.

In summary, the benefits of certificates are limited. In the case of IT products, certificates are often limited to a few functionalities and would in principle have to be retested and reissued for each release, which means that the cost and benefit are disproportionate. Experience with the European Union's Cyber Resilience Act (CRA) will show whether this impression will again be confirmed.[6] Certificates for more complex test objects whose security cannot be defined precisely and therefore cannot be meaningfully measured or tested (e.g. in the context of ISO/IEC 27001 certificates) certify (at best) that certain processes, procedures, measures and documentation are complied with or are in place at the time of the test.[7] Whether and to what extent these fit the company and contribute to its security is not clear a priori.

---

[4] According to the Austrian-British philosopher Karl R. Popper (1902–1994), this applies in general to scientific theories (as an example of a complex system). Scientific theories can never be definitively proven (verified), but they can be refuted (falsified). Popper emphasised that a theory is only considered scientific if it is falsifiable, i.e. if it is formulated in such a way that a counterexample can be found in principle to disprove it.

[5] In an essay by the Nobel Prize-winning economist George A. Akerlof (2001), a "lemon" is defined as a "Monday car" or a bad used car. The market for used cars is characterised by an asymmetry of knowledge. While the seller knows the true condition of the car, this is difficult for the buyer to assess. Akerlof has shown that prices erode in such markets, i.e. low sales proceeds are achieved for both lemons and good quality used cars.

[6] As part of the CRA, the conformity of a product with the cybersecurity requirements is confirmed by awarding the CE marking (Conformité Européenne) in the sense of a "certificate". For low-risk products, a self-declaration by the manufacturer is sufficient. However, for products with a high risk potential – such as those used in critical infrastructures – testing by an authorised, independent and notified body is mandatory in order to obtain the CE marking.

[7] In the discussion below (thesis 4), we will go into more detail about the fact that, in the absence of alternatives, criteria such as maturity are often used for certification, which have less to do with the IT security itself than with the methodical correctness of the implementation.

3. Alternative approaches

As mentioned, defining IT security, measuring it, testing it and the certifications based on it are difficult challenges. The respective approaches have often only become established in niches, and certificates are used (more) widely only if provided for by regulations. To the best of our knowledge, there have been no studies on their benefits to date. Nevertheless, states are (generally) focusing on increasingly complex regulations. The aforementioned Cyber Resilience Act (CRA) of the EU in the area of product safety [6] and the Directive for a high level of cybersecurity across the Union (NIS 2 Directive) [7] are two examples that affect all states of the European Union.

The following section examines alternative approaches that (i) increase the measurability and testability of IT security and (ii) incorporate aspects of IT security along the supply chain (suppliers, subcontractors and providers). The approaches are formulated in the form of four theses.

a. Thesis 1: Reducing complexity

A widely used standard for improving cybersecurity in companies and organisations is the Cybersecurity Framework (CSF) published by the U.S. National Institute of Standards and Technology (NIST) [8]. The Minimum ICT Standard developed by the federal government [9] and declared binding for the electricity sector as of 1 July 2024, for example, is based on the NIST CSF [10]. The CSF 1.1 from 2018, which underlies the minimum standard, was based on five core functions (Identify, Protect, Detect, Respond and Recover) with 23 categories and a total of 108 subcategories or measures (known as "controls"). With the publication of the NIST CSF 2.0 in February 2024, a sixth core function "Govern" was added. The core functions have since been divided into 22 categories and a total of 106 subcategories (measures). The ISO/IEC 27001 standard is also widely used [4]. In its current 2022 version, it contains 93 controls, divided into four main categories (Organisational Controls, People Controls, Physical Controls, Technological Controls). Compared to ISO 27001:2013, which still listed 114 controls spread across 14 categories, this reduction represents a simplification that is welcome in principle. Nevertheless, it should be noted that the number of measures is high for both common standards.

Both NIST CSF and ISO 27001 provide for flexible and risk-based implementation of the measures. However, if certain controls are not implemented, this must be justified. It is often argued that there is a low residual risk. The problem of risk assessments is discussed in more detail below. At this point, it should already be noted that probability-based (i.e. quantitative) risk assessments are fundamentally difficult and not optimal for assessing whether certain measures should be implemented [11]. A risk-based omission of measures is also not suitable when it comes to creating transparency, given that comparable companies – despite complying with the same standard – can arrive at different risk assessments and thus different catalogues of measures.

To overcome these disadvantages, a fundamental reduction in complexity can be proposed. Instead of numerous individual measures, each of which is evaluated and implemented or rejected pursuant to a probability-based risk analysis, the NCSC relies on an extended basic protection approach. This approach defines the smallest possible number of binding basic requirements that must be implemented. Additional technical and organisational measures (TOMs) should only be implemented if there is an increased need for IT protection. In contrast to the approaches postulated in [12,13], a probability-based risk analysis is not used.[8]

Fewer, but general measures that are to be implemented (regardless of risk considerations) reduce complexity and increase transparency, as it is clear at all times what must be implemented as a minimum. This approach is based in part on the findings of the Government CERT (GovCERT.ch) from numerous analysed IT security incidents, which could often have been prevented by simple measures such as the introduction of two-factor authentication. Additional TOMs can be selected and implemented on the basis of threat modelling (see below). This allows the purpose of each measure to be explained and transparently understood.

b. Thesis 2: Measures based on facts

People are used to analysing facts and drawing conclusions from them. Developing and evaluating fictitious scenarios and events, on the other hand, is much more difficult. In particular, estimating the probability of occurrence and the extent of damage of a particular event is extremely difficult – if not impossible – in such cases. This is not only because people tend to subconsciously incorporate ideological prejudices and personal experience when evaluating fictitious scenarios, but also because statistical analyses require a large enough sample size of comparable events, which is often lacking.[9] The results of probability-based risk analyses are therefore often arbitrary, have little informative value [2,11,14] and are therefore suitable for deriving meaningful IT security measures only to a limited extent. Because IT security specialists often know intuitively which measures make sense, the NCSC has found that they often help themselves by calculating risks "backwards" and applying them appropriately (in any tools that may be at their disposal) so that the measures they want to implement (based on their wealth of experience) are the ones that result. However, this reconstruction of the risks from the measures reduces the idea of risk analysis to absurdity.

The NCSC therefore recommends that measures should not be selected based on fictitious events and scenarios. They should either apply universally – as in the basic protection approach mentioned above – or be derived on the basis of facts if there is an increased need for protection. The necessary bases for determining the protection requirements, such as business processes, process objectives with maximum permissible deviations and the hardware and software components involved, can be determined objectively, can be verified by third parties and do not require any arbitrary assumptions. If an increased need for protection is identified, threat modelling according to STRIDE [15] or STRIDE-LM is suitable for the structured derivation of measures.[10] The six threat categories of this method are

[8] As explained below, the increased need for protection is not determined by a probability-based risk analysis, but by assessing the impact of defined IT security threats on business and production processes (see section 4.a on information security management systems (ISMSs)).

[9] With zero-day exploits and other previously unknown attack vectors, for example, no other option exists.

[10] STRIDE is a security risk model that was originally developed by Loren Kohnfelder and Praerit Garg for threat modelling at Microsoft and is now used worldwide. The name is an acronym made up of the first letters of the original six categories of security threats that are differentiated within STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. As part of STRIDE-LM, the LM "Lateral Movement" category (i.e. the ability to compromise other systems in a network) has been added to the model in the context of the CSF and with regard to current threats in networks.

universal (footnote 10). The same applies to the typical associated countermeasures.[11,12]

Scenarios characterised by major uncertainties are not necessary.

If IT security concept measures are based on facts that can also be verified by third parties (see also thesis 4) instead of random or fictitious scenarios, this represents a benefit not only for IT security, but also for transparency with regard to the necessity of certain measures, which at the same time increases testability or makes it possible in the first place.

c. Thesis 3: Combining verifying and falsifying approaches

Two approaches to determining the IT security of an organisation or company are described above. One approach was called verifying, the other falsifying. In the first case, the "presence of security" is confirmed by verifying whether a defined procedure (e.g. vulnerability management) has been implemented correctly. In the second case, the "absence of insecurity" is confirmed, for example when ethical hackers do not succeed in compromising IT security. Both approaches have advantages but also disadvantages, where the latter can ideally be compensated for by a combination of both approaches.

If the IT security of a company or organisation is viewed using both approaches, the perspective changes. The verifying approach focuses on the individual (technical and organisational) measures and their implementation. In the falsifying approach (ethical hacking, penetration tests, etc.), an attack on IT security is carried out or simulated. The attack can be successfully defended against if the combined measures can withstand or fend off the attack. The focus is therefore also on examining the interplay and interactions between the TOMs to prevent attacks.[13]

By combining both testing approaches (verifying and falsifying), the IT security of an organisation can be assessed more comprehensively than is possible by using just one approach in isolation. This is because the strengths of one approach are evident where the other has gaps in knowledge ('blind spots').

The proposal presented here does not envisage testing every process or every hardware and software component using both approaches. Rather, it is about using the available resources in a targeted and strategic manner to strengthen the cybersecurity of the company or organisation in the best possible way. Depending on the use case, one approach may be more suitable than the other. However, when protecting central business and production processes in particular, it may make sense to use both approaches in parallel in order to achieve more comprehensive protection.

d. Thesis 4: Creating IT security through trust and transparency

In this thesis, the question of the benefits of certificates and their significance for IT security is again examined. There are (essentially) three reasons for companies and organisations to have the implementation of a security standard certified: firstly, because it is required by law.

---

[11] Examples include authentication as a measure against the threat of spoofing, or encryption as a measure against the threat of data leakage (information disclosure). These measures are generally applicable and can be customised flexibly and coherently to different systems.

[12] Compared to the direct derivation of measures without a threat model, such as the CIA triad, which only defines IT protection goals such as confidentiality, integrity and availability, STRIDE offers a clear, systematic and traceable framework for identifying threats and deriving suitable measures. This makes it possible to tailor security measures to specifically analysed threats – a decisive advantage over less structured approaches such as the CIA triad.

[13] Following the Greek polymath Aristotle, one could say: the whole (tested, for example, in ethical hacking) is something *other* than the sum of its parts (tested by verifying the individual measures). The knowledge gained differs and complements each other accordingly.

Secondly, because the company expects to gain a market advantage (i.e. its customers prefer certified providers). The third reason, namely the (external) review and possible optimisation of their own IT security and resilience, presumably often only plays a subordinate role. This is surprising, as the third point should be the actual core motivation for certification from the perspective of the company or organisation. The first two points lead to the conclusion that both authorities and customers expect certified companies and organisations to be more comprehensively and better protected against IT security failures and disruptions than those without certificates. However, this expectation is often unrealistic.

IT security – especially when the system to be tested is highly complex – can neither be precisely defined nor objectively measured. Nevertheless, it is precisely these impossible "measurements" that are supposed to form the basis for certifications. In the absence of practicable alternatives, the maturity of a system – such as a security procedure – is often used for certification. However, this metric primarily shows how methodically complete a solution has been implemented, but not its actual security effectiveness.[14] Maturity models only allow limited conclusions to be drawn about actual IT security.

Another problem is the lack of transparency of the certification process, which takes place exclusively between the company or organisation to be audited and the certification body. This means that authorities and customers have no way of knowing whether and how their important concerns are being taken into account – they neither know the underlying risk considerations nor can they influence the implementation of IT security measures.

Authorities and customers should internalise that certificates only have limited significance for IT security and that certification is no guarantee that a company or organisation ensures the expected high IT security standard. This raises the fundamental question of what can be expected of companies or organisations with regard to their IT security and how these expectations can be tested.

A realistic expectation is that a company or organisation is aware of its responsibility for the functioning of a country (this applies in particular to operators of critical infrastructures, see below) and for the economic prosperity of its customers, and that it "promises" to implement its IT security in accordance with the state of the art, which may also include the implementation of suitable standards. Authorities and customers should demand verifiable transparency instead of certificates in order to be able to check compliance with this commitment in a meaningful way. The concept of "security through trust and transparency" represents a promising alternative to conventional certifications that is worth examining – despite the obvious challenges involved in scaling.[15]

As indicated, scalability is the greatest challenge in implementing the concept of "security through trust and transparency". One possible solution could be the idea motivating RFC 9116 [16]: in April 2022, the Internet Engineering Task Force (IETF) published this document, which has since become established among many website operators. RFC 9116

---

[14] Certifications often confirm a certain level of maturity. This always refers to a specific system – such as a specific information security management system (ISMS) or a business continuity management system (BCMS) – and reflects how *methodically complete* the organisation has implemented it. A high level of maturity therefore does not automatically mean a high level of IT security – especially in the case of complex systems. This is especially true if the system in question is unsuitable for the specific requirements of the organisation or is based on incorrect assumptions – such as inaccurate risk assessments. The significance of the maturity level therefore depends to a large extent on how accurately the system has been selected and how well it has been implemented.

[15] The fact that certificates are used at all despite their shortcomings can be explained in part by their scalability and practicability. However, companies must recognise that they share responsibility for any damage they suffer as a result of their suppliers' lack of IT security. A reductionist attitude that is limited to demanding certificates is risky or even negligent.

defines the format and use of the "security.txt" file, which organisations can use to disclose their vulnerability disclosure processes. This file is stored on the web server and offers an effective way of bringing security researchers and administrators into contact with each other. This makes it easier to report vulnerabilities, which can help to improve the security of a website.

Based on the concept of "security.txt", it is proposed to introduce a file named "cybersecurity-transparency.txt". The purpose of this file is to transparently document the IT security measures and mechanisms implemented by an organisation or company and to disclose them to third parties, such as authorities or customers. The documentation is carried out for each business or production process and product, with information including the following: process objectives, IT protection objectives, implemented IT security baseline requirements, responsibilities, contact information and the date of the last update.

Because the disclosure of detailed technical measures, configurations or known vulnerabilities could provide potential attackers with targeted information, transparency should take place at a higher level. It is therefore advisable to limit the information to principles, processes and responsibilities and to avoid operational details that could allow conclusions to be drawn about specific attack vectors. References to these disclosure limits must also be noted in "cybersecurity-transparency.txt".

Whether and to what extent a company or organisation creates and publishes the "cybersecurity-transparency.txt" file should be left to its own discretion. It would be a possibility, for example, to make the file available to potential customers in a targeted and exclusive manner as part of the quotation process or to publish it for a general audience on the company’s website. In either case, the company or organisation creates a trusting basis for cooperation and demonstrates an open and responsible approach to the topic of IT security towards customers and partners. The presentation of the "cybersecurity-transparency.txt" file could in future serve as a modern alternative to conventional certificates, in which – unlike certificates – every business partner has the opportunity to check the supplier's IT security with regard to their priorities themselves, or to use the document as a starting point for further discussions (see also the section "Cybersecurity in the supply chain" below).

4. Applications of the theses

The following section uses examples to show how the theses can be put into practice. The examples are taken from current projects that have been planned, developed and in some cases already implemented in the field of preventive cybersecurity at the NCSC.

a. Information security management systems (ISMSs)

Information security management systems (ISMSs) are a particularly relevant area for the testability and measurability of IT security. An ISMS can be defined as follows:

An ISMS is a system made up of procedures and rules that can be implemented within an organisation or company to ensure information security – that is, to define concrete information security objectives, and to plan, manage, and ensure their achievement.

The NCSC is currently developing a method that will form the basis for establishing an ISMS in accordance with the above definition. The method will take into account the reduction of complexity (thesis 1) as well as the factual basis of the measures (thesis 2). It will rely on universally applicable basic requirements consisting of around 20 measures that will need to be implemented in every case. Additional (technical and organisational) measures will be developed in a targeted manner if there is an increased need for protection. Parameters such as business processes, process objectives, their maximum permissible deviations and the hardware and software components involved in the business processes will be used for this purpose. These factors will be objectively ascertainable and can be verified by third parties if necessary. The measures will be derived from a threat analysis in accordance with STRIDE or STRIDE-LM. The six threat categories will be just as universally valid as the corresponding countermeasures (see footnote 11). Risk scenarios with a high degree of uncertainty and the assessment of their probability of occurrence will be excluded.

b. Cybersecurity in the supply chain

A concrete example of how IT security can be strengthened through trust and transparency (thesis 4) is the NCSC approach to dealing with IT security in the supply chain. In 2024, a pilot project was launched in cooperation with the private sector. The aim is to sensitise companies and organisations to not only pay attention to the quality of products and services when selecting suppliers, but also to include aspects of IT security from the outset and to coordinate these with the suppliers.

The NCSC recommends systematically integrating IT security requirements into the supplier selection and testing process. For this purpose, a control loop with seven steps was developed, ranging from the identification and evaluation of the supply chain to the supplier audit and the contractual definition of measures. Specific key questions for suppliers, recommended measures and information on contractual safeguards are listed in the relevant NCSC resources [17].

In contrast to simply obtaining certificates, which offers little insight into the actual IT security situation of suppliers, this approach enables the requirements and expectations to be specifically tailored to the individual needs of the partners. Although this procedure is more time-consuming than obtaining a certificate, it is an essential task for any responsible company and should not be delegated (footnote 15).

Providing a "cybersecurity-transparency.txt" file could offer a low-threshold and efficient entry point into the dialogue with suppliers. Ideally, this exchange will lead to a strengthened relationship of trust and cooperation that can sustainably improve cybersecurity along the entire supply chain.

c. Cybersecurity and critical infrastructure protection

Ensuring IT security in certain companies is also of central importance from a governmental perspective – especially for operators of critical infrastructures. Since their ability to function depends to a large extent on IT security, the state even has a constitutional mandate to help protect them. In this context, states often take on a regulatory role and oblige the market participants concerned to comply with certain standards. This makes particular sense where different interests (of the state and companies) exist.[16]

However, this does not take into account the fact that many companies have a considerable interest in protecting themselves against IT security incidents – not least because such incidents also jeopardise their own business interests. In some cases, companies lack the necessary expertise rather than the will to implement appropriate protective measures. In such situations, the transfer of knowledge and practical assistance – in the sense of "helping

[16] Different interests arise, for example, when companies are obliged to prepare for certain events in the interests of the state – for example, to protect the economy and the population – but the effort required to do so significantly exceeds the potential benefit of continued service or goods production in the event of an incident. One example is the maintenance of telecommunications services in the event of a prolonged power outage.

people to help themselves' and in consideration of theses 1, 2 and 4 – can be a sensible and effective alternative or supplement to pure regulation.

As part of the implementation of the National Cyber Strategy (NCS), the NCSC offers a wide range of support. The technology considerations of the NCSC address current and relevant topics, including cloud computing [18], quantum computing and post-quantum cryptography [19], as well as challenges of today's internet architecture in connection with network-based attacks and possible solutions such as SCION [20].

NCSC publications are written from a neutral perspective, often in consultation with experts from the private sector and academia. These publications support companies in making well-founded and fact-based decisions in the field of IT security.

Another way to promote transparency (thesis 4) is to use the NCSC Cyber Security Hub (CSH) as a central platform for the exchange of information between authorities and operators of critical infrastructures. The CSH already enables a structured exchange on cyberthreats, incidents and best practices and thus supports operational cybersecurity. In future, the CSH is to be used increasingly for preventative purposes, for example by providing tools with which operators of critical infrastructures can assess the status of their IT security themselves or compare it (anonymised) with other companies in their sector ('benchmarking'). Such self-assessments provide companies with valuable information for the further development of their cybersecurity and at the same time enable the state to gain aggregated insights into the level of security in the sector in order to develop targeted improvement measures together with the industry as needed.

This approach requires transparency and mutual trust: an open dialogue that promotes the continuous improvement of cybersecurity can take place only if the exchange is voluntary and confidential.[17]

5. Conclusion

Based on the above, IT security generally cannot be measured or tested in any meaningful way – and when this is possible, it is usually only in (trivial) individual cases. Certificates can be misleading and often suggest properties that do not hold up under closer scrutiny. IT security cannot be assessed at a surface level. To properly evaluate a system's IT security, you have to look deep into its core and examine it closely. In practice, this means that for organisations and companies, the starting point has to be the business and production processes that depend on a functioning IT infrastructure. For products and services too, the key is always to focus on the actual use case. Security technologies are never an end in themselves – they exist to support a business or production process, or a use case, and they need to protect the overall socio-technical system.

If IT security is to be made measurable and testable in this context, alternative approaches (to certification) need to be considered. This paper outlines a few examples: reducing complexity (thesis 1), measures based on facts (thesis 2), combining verifying and falsifying approaches (thesis 3) and creating security through trust and transparency (thesis 4). Of course, other theses can also be developed and combined with those already proposed to help establish a meaningful and practical way of measuring and testing IT security.

---

[17] In this area, numerous other opportunities for cooperation based on mutual trust and transparency are conceivable. Such models can prove to be more sustainable and efficient in terms of improving cybersecurity than approaches that rely on strict guidelines, mistrust and controls.

Abbreviations

BCMS	Business continuity management system
CC	Common Criteria
CE	Conformité Européenne
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, Availability
CRA	Cyber Resilience Act of the European Union
CSH	Cyber Security Hub (NCSC information system)
EU	European Union
GovCERT.ch	Government CERT (part of NCSC)
IETF	Internet Engineering Task Force
ISMS	Information security management system
ISO / IEC	International Organization for Standardization / International Electrotechnical Commission
NCS	National Cyber Strategy
NCSC	National Cyber Security Centre
NIS 2	Measures for a high common level of cybersecurity across the European Union
NIST CSF	NIST Cybersecurity Framework
NIST	National Institute of Standards and Technology
RFC	Request for comments
SaaS	Software as a Service
SCION	Scalability, Control and Isolation on Next-Generation Networks
STRIDE-LM	Acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege, Lateral Movement
TOM	Technical and organisational measure

References

[1] A. Grünert, J. B. Michael, R. Oppliger and R. Rytz, "On the Measurability and Testability of IT Security" in IEEE Computer, vol. 58, no. 3, pp. 120-126, March 2025

[2] Rolf Oppliger and Andreas Grünert, "How to Measure Cybersecurity and Why Heuristics Matter" in IEEE Computer, vol. 57, no. 2, pp 111-115, February 2024

[3] ISO/IEC 15408-1, Information security, cybersecurity and privacy protection – Evaluation criteria for IT security, Part 1: Introduction and general model, 2022

[4] ISO/IEC 27001, Information security, cybersecurity and privacy protection – Information security management systems – Requirements, 2022

[5] George A. Akerlof, The Market for Lemons: Quality Uncertainty and the Market Mechanism, The Quarterly Journal of Economics, Vol. 84, No. 3, August 1970, pp. 488-500

[6] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[8] National Institute of Standards and Technology (NIST), 2024. NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: National Institute of Standards and Technology

[9] Federal Office for National Economic Supply FONES, Minimum standard for improving ICT resilience, May 2023

[10] Article 5a of the Electricity Supply Ordinance (ESO) of 14 March 2008 (Status as of 1 January 2025), SR 734.71

[11] Andreas Grünert, James Bret Michael, Rolf Oppliger and Ruedi Rytz, Why Probabilities Cannot Be Used in Cyber Risk Management, IEEE Computer, Vol. 57, No. 10, October 2024, pp. 86-89

[12] ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks

[13] NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, September 2012

[14] Rolf Oppliger and Andreas Grünert, How to Manage Cyber Risks: Lessons Learnt from Medical Science, IEEE Computer, Vol. 56, No. 1, January 2023, pp. 117-119

[15] Loren Kohnfelder and Praerit Garg, "The threats to our products", 1 April 1999

[16] Internet Engineering Task Force (IETF). (2022). *RFC 9116: A file format to aid in security vulnerability disclosure*. Retrieved from https://www.rfc-editor.org/rfc/rfc9116.pdf

[17] National Cyber Security Centre NCSC, Cybersecurity in the supply chain, 2024, https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/lieferkette.html

[18] National Cyber Security Centre NCSC, Technology brief: Cloud computing and cybersecurity, 2025

[19] National Cyber Security Centre NCSC, Technology brief: Quantum computers and post-quantum cryptography, 2024

[20] National Cyber Security Centre NCSC, Technology considerations: SCION, 2025