Cyber Security Certifications

What to expect from certifications in the EU Cybersecurity Act and how to assess the security of ICT systems in the meantime?

Part 1

Christian Damsgaard Jensen

DTU Compute

Master of Cyber Security Whitepaper 2020

Introduction

With the growing reliance on Information and Communication Technologies (ICT), most aspects of society are becoming increasingly vulnerable to accidental or intentional disruption to ICT services. A branch of the Military Intelligence Services (Da. “Center for Cybersikkerhed”) has been tasked with the protection of Government agencies and critical infrastructure, but cyber security has also moved up on the agenda in many Danish companies and among many ordinary citizens.

In particular, the substantial financial and reputational losses, suffered by large Danish companies as results of successful cyber-attacks in recent years, e.g. the Not-Petya attack that hit Maersk in 2017 and the ransomware attack against Demant in 2019, demonstrates the need for robust cyber-defences. This is not only a Danish phenomenon, the Online Trust Alliance estimates a global financial impact across all types of cyber-incidents in excess of $45 billion in 2018 [1].

The rising awareness about the need for cyber security among business leaders and government officials must be translated into action, which requires the ability to specify, design, build, deploy and maintain secure ICT systems.

Most ICT systems are constructed as systems of systems, where that the overall security of the system effectively aggregates the security mechanisms and policies of all the components that make up the system. Each of these software components, services or computing and network infrastructures may be outsourced to separate software developers or service/infrastructure providers, which means that **system owners need the ability to understand the security properties of the individual components and services**.

The aggregation and integration of ICT components with different provenance into a single secure ICT system, is made significantly easier by standards that define desired security properties and certifications to attest that products and/or services meet the objectives defined by the security standards.

Introduction

The adoption of the EU Cybersecurity Act [2] in 2017 reformed the EU Cybersecurity Agency (ENISA) and created a framework for cyber security certification across the EU. This gives suppliers of ICT software and services a common framework for describing and certifying the security properties of their products, but more importantly, it provides customers the ability to specify their demands for security and to avoid software and services with inadequate security.

Although the Cybersecurity Act came into effect on 27 June 2019, the security standards and common certification framework have not yet emerged, so customers of security software and services still have to rely on their own assessments and the promises of the security software and service provider (often supported by a contract and/or a service level agreement).

Introduction

As there are currently few security certified products and services available on the consumer market, i.e. products not primarily developed for the defence sector, the second part of this whitepaper will examine ways for customers to assess the cybersecurity of products and services.

In addition to the summary of intensions described in the Cybersecurity Act, we examine some of the existing cybersecurity standards and certifications to provide the context for a discussion of the likely impact of an EU wide cybersecurity certification of IT products and services.

As there are currently few security certified products and services available on the consumer market, i.e. products not primarily developed for the defence sector, the second part of this whitepaper will examine ways for customers to assess the cybersecurity of products and services.

Cyber Security Certifications

Cyber Security Certifications

Certifications generally have two complementary purposes: 1) To specify the asserted functionality of the product or service and 2) To validate that the product or service meets the stated goals. Together this allows customers to compare the functionality offered by different products and services and to rank potential product and services according to the validated functionalities that they offer.

> *Security has only recently emerged as a competitive parameter in commercial (civilian) systems, so existing computer and network security certification schemes have predominantly focused on the defence sector or areas of critical infrastructure, i.e. high priced systems with high demands for security.*

This means that certification procedures typically require significant efforts from all parties, which makes them inappropriate for both common off the shelf (COTS) software and systems and consumer products, such as the many Internet of Things (IoT) products on the market.

Moreover, recognition of existing certifications is either national, which means that providers of products or services must certify their products in all countries where they do business, or industry specific, which means that providers of products or services must certify their products within every industry where they do business.

Cyber Security Certifications

The European Union has therefore identified the need for common cybersecurity certifications to help consumers identify products with adequate cybersecurity, and ensure that providers of products or services only need to obtain certification once, thus **establishing a single market for cybersecure products and services within the EU**.

The common cyber security certification framework has been included in the Cyber Security act and will be outlined in the following.

Cyber Security Certifications

Certifications in the EU Cybersecurity Act

The Cybersecurity Act defines an overall framework for implementing an EU wide certification framework for cyber security, but it does not specify which technology standards or specific assessment procedures to follow. These standards and assessment procedures will be prepared by the EU Cybersecurity Agency ENISA in consultation with relevant standardisation organisations, in particular EU organisations.

Cyber security certification will mostly be voluntary and the EU certifications may exist alongside existing or emerging certifications within particular industries, such as the Payment Card Industry Data Security Standard (PCI DSS) [3]. Industry and private standardisation organisations are also welcome to submit their standards for consideration as the basis for an EU certification scheme, which may provide a way to jump-start the certification process.

The Cybersecurity Act recognises that **there is not one-size-fits-all in cyber security,** so different certification schemes will be defined for different types of product and possibly even different application scenarios, e.g. different certifications may be introduced for IoT devices controlling private homes and industrial processes.

The cyber security certification should help end-users make informed decisions about which products or services to rely on, so the description of the security functions provided by the product or service must be adapted to the expected technical level of the intended end user. In addition to different certification schemes for different product types, each scheme may include more than one level of compliance. This allows different versions of the IoT device mentioned above to be certified for “personal use” or “industrial grade” within the same certification scheme.

Cyber Security Certifications

Certifications in the EU Cybersecurity Act (contd.)

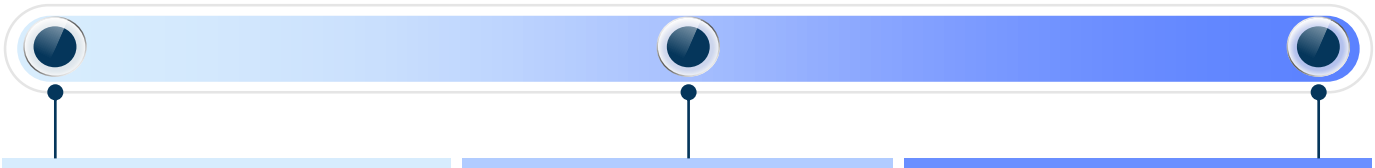
The certification framework, defined in the Cybersecurity Act, explicitly mentions three 0assurance levels: “basic”, “substantial” and “high” (cf. Sidebar 1). These levels reflect the estimated strength of the security functions and the confidence in the assessment. The assurance levels also reflects the level of risk that the product or service may comfortably be exposed to, i.e. a product with security assurance “high” should be selected for systems of high value and with a high probability of attack, while a system with assurance level “basic” may be used for less sensitive systems.

The amount of material considered and the rigour of the assessment process increases with the assurance levels. The minimum requirements for assessment at the three levels defined by the Cybersecurity Act are defined in Sidebar 1.

Certification schemes should consider current software and hardware development methods. In particular, the impact of frequent software and/or firmware updates on individual European cybersecurity certificates. The certification schemes should specify the conditions under which an update may require recertification or that the scope of a European cybersecurity certificate be reduced. This suggests that products or services must be recertifies, if an update is likely to have an adverse effect on the compliance of the cybersecurity certificate.

Sidebar 1 Requirements for assessment levels

Cybersecurity Assurance Levels



Basic	Substantial	High
The minimum requirement for a “basic” assurance level assessment includes at least a review of technical documentation.	In addition to the requirements for a “basic” assurance level assessment, a “substantial” assessment must include a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the product or service correctly implements the necessary security functionalities.	In addition to the requirements for a “substantial” assurance level assessment, a “high” assurance level assessment must include testing to demonstrate that the product or service correctly implement the necessary security functionalities at the state of the art and an assessment of their resistance to skilled attackers, using penetration testing.

Cyber Security Certifications

Certifications in the EU Cybersecurity Act (contd.)

For aficionados of security evaluation criteria, such as the Orange Book [4] or the Common Criteria [5], it is interesting to note that the Cybersecurity Act, does not require formal modelling and validation of the product or service for certification at the higher assurance levels. This gives a very strong indication that **the new certifications are intended to be achievable with significantly less effort than the previous (defence sector) certification schemes.**

In addition to the increased focus on simple code review and testing, **the Cybersecurity Act introduces the possibility of conformity self-assessment,** where the manufacturer or service provider issues a so called EU statement of conformity, which states that the fulfilment of the requirements set out in the scheme has been demonstrated.

The internal documentation for this demonstration must be made available to the national cybersecurity certification authority and a copy sent to ENISA. An EU Statement of Conformity based on self-assessment can only certify products and services at the “basic” level, all other certificates must be issued by the national cybersecurity certification authority or by a conformity assessment body that is accredited by a national accreditation body as defined in Regulation (EC) No 765/2008 [6].

It is the national cybersecurity certification authority in each member state, which is responsible for the supervisory tasks in that country; this includes monitoring and enforcing compliance to the certification schemes by accredited conformity assessment bodies and self-assessment by product manufacturers and service providers.

For the manufacturers and service providers, the new cybersecurity certification schemes significantly reduces the effort required to obtain a cybersecurity certification.

The recognition of cybersecurity certificates throughout the EU, means that products or services only have to be certified once and the manufacturer or service provider decides where to submit the application for certification, e.g. either in their home country or in their main export market.

Moreover, the introduction of self-assessment makes it possible for companies with good cybersecurity processes to obtain a “basic” assurance level certification with very low overhead.

Cyber Security Certifications

Certifications in the EU Cybersecurity Act (contd.)

For the consumers and the end-users, the availability of cybersecurity certified products in the marketplace, makes it easier to protect themselves by choosing certified products and thereby demonstrate demand for cybersecure products. This will increase the value of cybersecurity as a differentiator in the market and hopefully lead to an increased cybersecurity in all products.

The fact that all conformity assessment bodies, including self-assessments, is ultimately monitored by the national certification authority, means higher consumer confidence in the cybersecurity certifications, so a total collapse of confidence in the certifications, as we saw with the numerous security and trust shields that adorned many webpages at the turn of the century, is unlikely to repeat itself.

Other Cyber Security Standards and Certification Schemes

As mentioned above, **certification requires measurable objectives that can be methodically assessed and attested** by the certification authority. This means that there are security standards associated with most certification schemes.

On the other hand, there are many standards that do not have specific certification schemes associated with them; the most common of these are known as “Best Practices;” these are often industry specific. We provide a brief overview of such standards and best practices in the following, before examining some of the standards that have certifications associated with them.

Cyber Security Certifications

Other Cyber Security Standards and Certification Schemes (contd.)

Regulations, Standards and Best Practices

Cybersecurity has received increasing regulatory attention from the EU over the past couple of years and one of the milestone regulations is the Directive on Security of Network and Information Systems (a.k.a. the NIS Directive) [7]. The directive focuses on digital service providers (DSPs) and operators of essential services* (OESs) with the aim of improving the overall level of cybersecurity in the EU. With the introduction of the NIS Directive, both DSPs and OES are required to report major security incidents to Computer Security Incident Response Teams (CSIRT). This ensures a comprehensive knowledgebase that renders the CSIRTs more effective, but if industry agrees to a broader sharing of these incident reports, this may also allow individual companies to learn from the mistakes of others, to the benefit of all.

Another central piece of EU legislation that has helped push cybersecurity high on the agenda is the General Data Protection Regulation (GDPR) [8], which has been covered extensively elsewhere. It is included here, because it states that development of new IT systems must follow the principles of privacy-by-design, *privacy-by-default and security-by-design*. These principles are not explicitly defined in the regulation, but the need to follow best practices in security and privacy is clear, and the potential fines for non-compliance are significant.

The EU regulation has been mentioned first, because it has direct effect on all Danish organisations, but **the US has in many ways lead the development of standards and security technologies.** In particular, the National Institute of Standards and Technology (NIST) publishes many security relevant standards in the Federal Information Processing (FIPS) series [9], but many of the most relevant security standards are published in the Special Publications 800 Series [10]. Especially SP 800-39, SP 800-37 Rev. 2 and SP 800-30 Rev. 1 that deal with risk management, SP 800-61 Rev. 2 that covers incident handling, SP 800-137A (Draft) on continuous monitoring of information security, and SP 800-160 (vol. 1 + 2) on engineering of cybersecure systems provide information valuable to a larger audience.

A number of private organisations and institutions also provide recommendations and best practises for cybersecurity. Some of the best-known standards are COBIT, published by the Information Systems Audit and Control Association (ISACA), and ITIL, published by AXELOS**. Both of these standards provide broad recommendations on IT systems management and governance, but they also contain valuable resources related to cybersecurity. Another non-profit organisation that should be mentioned here is the International Information System Security Certification Consortium, or $(ISC)^2$, which specializes in training and certifications for cybersecurity professionals – most notably the Certified Information Systems Security Professional (CISSP), which is widely recognized by the cybersecurity industry. Together with the standards and best practises mentioned above, these certifications by non-government organisations illustrate **the three targets of certification in cybersecurity: *products* (systems or services), *processes* and *people*.**

**Operators of essential services include any organizations whose operations would be greatly affected in the case of a security breach if they engage in critical societal or economic activities;*

***AXELOS is a joint venture between Capita and the UK Cabinet Office.*

Cyber Security Certifications

Other Cyber Security Standards and Certification Schemes (contd.)

Security Standards with Certifications

Organisations that follow cybersecurity standards and best practices in recruitment and product development to build cybersecure products or services, may want a way to demonstrate their commitment to cybersecurity to their customer. Several of the existing cybersecurity standards therefore have certification schemes associated with them.

All government (state) institutions in Denmark must follow the ISO/IEC 27001 standard [11], which is part of the general ISO 27000 family of standards in cybersecurity. The ISO 27001 standard follows a risk-based approach to security and emphasises the role of management in the specification and enforcement of security policies. The focus of the standard is therefore on all the processes that organisations implement to evaluate and mitigate risks associated with the use of information and communication technologies. **The ISO 27000 family covers a broad range of topics and systems, but the core focus is on the administrative processes and controls** that must be in place to ensure cybersecure IT systems. ISO 27000 covers the general issues in most IT systems, but does not address many of the security issues that arise in cyber physical systems

To address the security demands of Industrial Automation and Control Systems (IACS), the International Electrotechnical Commission (IEC) has developed the IEC 62443 family of security standards for these types of systems. According to IEC 62443-1-1 [12], an Industrial Automation and Control System (IACS) is a “collection of processes, personnel, hardware, and software that can affect or influence the safe, secure and reliable operation of an industrial process.” The IEC 62443 standard includes a certification program created by the International Security Compliance Institute (ISCI) in 2007. This program allows accredited institutions to certify Commercial Off-the-shelf (COTS) automation, control systems, and IOT devices, according to the standard. **The need for certification is well known to the electronics industry**, where new products need CE certification or approval from DEMKO, so it is perhaps only natural that this industry is among the first to implement a cybersecurity certification scheme for electric products.

The financial sector relies on the trust of the consumers, so online security is crucial to their operation, e.g. product manufacturers often claim that their product is “as secure as your online bank”. Part of the security of online banking is defined in the Payment Card Industry Data Security Standard (PCI DSS) [3]. The PCI DSS standard is mandated by the credit card brands but administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually or quarterly either by an external Qualified Security Assessor (QSA) or by a firm specific Internal Security Assessor (ISA), or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes. While the PCI DSS mention specific technologies, e.g. installation and maintenance of a firewall, most of the standards and the validation of compliance focus on proper implementation of the required processes.

Cyber Security Certifications

Other Cyber Security Standards and Certification Schemes (contd.)

Security Standards with Certifications (contd.)

The final certification scheme that we will cover here is the only scheme developed specifically for secure IT products and systems. The Common Criteria [5] were developed for the defence industry and combines the best parts of many national evaluation schemes, such as the US Trusted Computing Systems Evaluation Criteria (TCSEC) defined in the Orange Book [4] mentioned above. The Common Criteria introduces the notion of Protection Profiles (PP), which define the security goals that the evaluated system, a.k.a. the Target of Evaluation (ToE), must meet. The Common Criteria distinguishes between the security objectives defined in the PP and the Evaluation Assurance Level (EAL) that indicates the confidence in the result of the evaluation (similar to the assurance levels defined in the Cybersecurity Act). Certification at the higher assurance levels requires the system to be specified according to a formal model, which is then verified as part of the evaluation. The CC certification process requires a lot of effort, especially at the higher EAL, so it is primarily used in the defence industry where the high security demands and the price of individual products al.

Seals, Shields and Marks

The turn of this century saw a proliferation of seals and shields related to web-security and online trust. Many of these were provided by private companies for a fee, but **many web-users lost confidence in these shields after a few of the companies failed to properly check the web-sites that carried their shields and many of these shields** no longer exist today.

The remaining shields are either issued by the web-sites certificate authority, which also provides the web-site's TLS certificate, or from a security service provider (e.g. one of the well-known antivirus companies, such as McAfee or Norton). In both cases, the seal provider guarantees the validation of the identity of the organisation that receives the certificate, but it may also include indications of system security, e.g. running end-point protection software or periodically passing security scans.

There are also a few shields that focus on the good business behaviour of the company operating the website. In Denmark, the best-known shield of this type is "e-Mærket", which is operated by the consumer organization "Forbrugerrådet Tænk" together with all relevant industry organisations.

Summary and Discussion

Summary and Discussion

In this whitepaper, we have examined the three types of certifications, i.e. certification of products, processes and people, where most of the surveyed certifications target the two first types. Product certification generally requires time and significant efforts, but **the Cybersecurity Act aims to reduce the certification time and costs,** which should increase the number of affordable certified cybersecure products on the market. Process certification also requires significant efforts, but the target of evaluation is typically the entire organization, which helps amortize the costs.

The certification of people typically require significant efforts from individuals, who follow courses and pass exams, but the financial costs and organizational investments for the certification of an individual are typically negligible (although the accumulated costs of certifying all employees may be prohibitive.)

> In the B2B scenarios, certification helps accelerate trust in new business partners [...]

Understanding these types of certification includes understanding the intended audience of the certification and the estimated importance attributed to the certification by that audience. The intended audience may either be a regulatory body (e.g. government), other organisations (e.g. B2B) or end-users (e.g. B2C). If the need for certification arises with a regulatory body, this becomes part of the license to operate, so certification must be achieve regardless of costs, the PCI DSS is an example of regulatory certification that is required for any business that wishes to handle payment cards; in this scenario, the type of certification is defined by the regulatory requirements.

Summary and Discussion

In the B2B scenarios, certification helps accelerate trust in new business partners, because the certification demonstrates that their security meets the requirements defined in the certification; this goes for both product and process certification, whereas certification of people is cumbersome to demonstrate on demand. Finally, **in the B2C scenario, the main focus should be on product certification**, where process certification mostly plays a role in the absence of such certification and people certification play little to no role here. That being said, **investing in people certification helps build cybersecurity competences in the organisation** and thereby provides the necessary foundation for the two other types of certification.

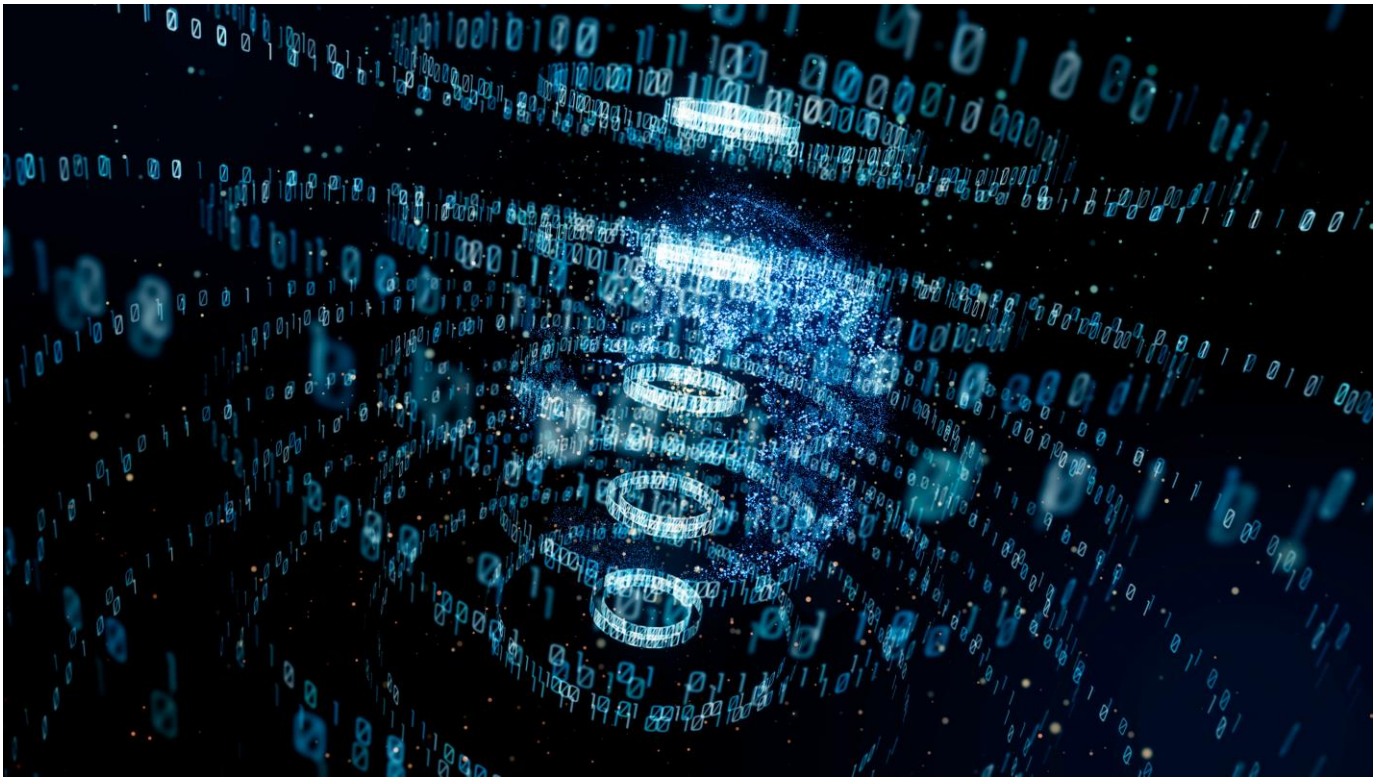
We have seen that product certifications have historically been expensive, and time consuming to obtain and maintain, but the certifications introduced through the EU Cybersecurity Act aims to reduce the time and money invested in cybersecurity certifications. This will hopefully make cybersecurity an attractive differentiator in the marketplace, and thereby ensure consumers a good choice of cybersecure products.

In addition to the certification efforts initiated through the Cybersecurity Act, **the Danish Industry Foundation (Da. "Industriens Fond") has funded a project to develop and promote a cybersecurity seal for Danish products and service providers**. This seal may co-exist with similar seals created with basis in the Cybersecurity Act, but it is likely that the national seal over time will align itself with the requirements of the EU wide certification scheme, so that seals obtained in Denmark will be recognized in all EU countries. **The national efforts are important, because it allows Danish companies a head start** and Danish consumers a choice of cybersecure products before the EU certification seals are finally approved.

Summary and Discussion

Easy and affordable product certification is, however, not yet available, so customers need other ways to determine whether potential providers of products and services will be able to provide these with an adequate level of cybersecurity. For individual consumers, this is a daunting task, but for those who purchase IT product and services in companies with identified IT security needs, there are a few metrics, beyond simple functionality, that may help decide which products to buy or external services to rely on.

In the second part of this whitepaper, we will examine the problem of assessing the security of software products and services without having access to the system design specification and/or the source code, i.e. what externally observable properties reveal information about the security of software or services.



References

1. Online Trust Alliance, “2018 Cyber Incident & Breach Trends Report,” Internet Society, https://www.internetsociety.org/breach2019/ , 2019.
2. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019,” *Official Journal of the European Union, 2019.*
3. PCI Security Standards Council, “Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures , Version 3.2.1,” Payment Card Industry Security Standards Council, May 2018.
4. US Department of Defense, “Trusted Computer System Evaluation Criteria,” US Department of Defense, August 1983.
5. Common Criteria Recognition Arrangement, “Common Criteria for Information Technology Security Evaluation, Version 3.1 (Revision 5),” Common Criteria Recognition Arrangement, April 2017.
6. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008,” Official Journal of the European Union, 2008.
7. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016,” Official Journal of the European Union, 2016.
8. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016,” Official Journal of the European Union, 2016.
9. Computer Security Resource Center, “Publication Search: FIPS,” National Institute of Standards and Technology, January 2020. [Online]. Available: https://csrc.nist.gov/publications/fips . [Accessed January 2020].
10. Computer Security Resource Center, “Publication Search : SP 800,” national Instityte of Standards and Technology, January 2020. [Online]. Available: https://csrc.nist.gov/publications/sp800 . [Accessed January 2020].
11. ISO/IEC JTC 1 - SC 27, “ISO/IEC 27001 - Information technology - Security Techniques - Information security management systems — Requirements,” Internatoinal Standards Organisation, 2013.
12. International Electrotechnical Commission, “Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models,” International Electrotechnical Commission, 2009.

DTU Compute Master in Cyber Security Whitepapers

This whitepaper is part of a series of whitepapers intended for security professionals working in Danish companies, with special interest in the topics covered in the whitepaper, or security professionals who may simply wish to broaden their horizon.

Topics of these whitepapers may cover all aspects of cyber security, from user awareness and insider threats to advanced technologies and emerging security paradigms, but the main focus of this series will be on the practical application of theoretical and technological advances in cyber security.

The Master in Cyber Security whitepaper series is published by:

Department of Applied Mathematics and Computer Science
Technical University of Denmark
Building 324
Richard Petersens Plads
DK-2800 Kgs. Lyngby
Denmark