Betriebswirtschaftliches Forschungszentrum für Fragen der mittelständischen Wirtschaft e.V.

TeBeISi

Desk Research Germany

Document Details:	
Reference	**TeBeISi**
IO / Activity	IO1 – Desk research
Author(s)	<Eimecke, J.; Rath, S.; Sporer, F.>
Character	Country Report Germany
Date	15.01.2019

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

This document was produced within the scope of the ERASMUS+ Project “Teilzertifizierung im Berufsfeld Informationssicherheit – TeBeiSi”, Project ID: 2018-1-EN02-KA202-005218

.

Funded by the
Erasmus+ Programme
of the European Union

Table of Content

1. Aim of the Report 3
2. National Rules & Regulations Concerning Information Security and Data Protection in SME & Nonprofit Organisations 5
3. Vocational and Continuing Education and Training in this area 8
3.1. Overview of Existing Training Offers in the Field of Information Security 12
3.2. Overview of Existing Training regarding Data Protection 15
4. Overview of jobs offered in the field of Information Security and Data Protection 16
4.1. Overview of job offers in the field of Information Security 17
4.2. Overview of job offers in the field of Data Protection 21
5. Existing Methods for Assessing and Certification of Vocational Skills aquired outside formal Education 25
6. Executive Summary and Resume 28
Reference list 32

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. Aim of the Report

The IT sector is characterized by short innovation and product cycles among developers and manufacturers. The half-life of central elements of technical knowledge can be regarded as "short" here. Studies show that approx. 50% of the product- and performance-specific knowledge required by a technical employee in three years is not yet available today. This imposes high and dynamically changing requirements on IT employees and their qualifications. Learning and recognition of informal aspects (keyword "learning on the job") is becoming "the crucial factor in the IT sector".

The report focuses on the validation of learning outcomes from non-formal and informal learning in the field of Information Security and Data Protection and the job profiles of "Information Security" and "Data Protection" are addressed. In the participating countries, formal vocational qualifications exist for these purposes. Since in the entire occupational field, i.e. the labour market segment, many lateral entrants are active without degrees and work in a thoroughly solid manner in practice, the aim is to examine in a comparison of countries of the partners how non-formally and informally acquired learning outcomes can be determined diagnostically and validated on the basis of the examination regulations for formal degrees.

Against this background the aim of this report is to provide an overview of the offers from Vocational training providers and the demands and needs of the labor markets in the field of Data Protection and Information Security and the related methods for validating informal learning in the partner countries.

In this regard, an overview of national rules and regulations concerning Information Security and Data Protection relevant for organisations in the profit and non-profit sector will be given. Next qualification offers covering this topic will be identified and their suitability will be estimated. Furthermore, the current demand of the labor market in terms of available job offers and the acquired competences will be described. Against this background a possible profile for Information Security Officers and Data Protection Officers will be drafted in two different competence levels (experienced staff & expert level).

Definition of Terms

As the terms Information Security and Data Protection are frequently slightly different used it will be clarified for this report here.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. (Wikipedia 2019b)

Data Protection, also known as data privacy or information privacy, is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them.

Privacy concerns exist wherever personally identifiable information or other sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Legal framework within the EU is the General Data Protection Regulation (EU 2016/697) (Wikipedia 2019a).

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

As Wikipedia is not a scientific source for disseminations, further definitions of Information Security and Data Protection will be useful.

Information Security:

Preservation of confidentiality, integrity and availability of information.

Confidentiality Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity Property of accuracy and completeness

Availability Property of being accessible and usable upon demand by an authorized entity

(Brookson et al. 2015, p.16)

Definition Industrie- und Handelskammer

IHK stands for « Industrie- und Handelskammer » and in Germany are existing 79 of them. The insitutions are based in the economy of each region and contribute together with their member firms to the economic growth (IHK 2019). Partially the IHK is financed from the german federal government.

To avoid misunderstandings the « Industrie und Handelskammer » is not – as often done - translated with « Chamber of commers ».

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2. National Rules & Regulations Concerning Information Security and Data Protection in SME & Nonprofit Organisations

2.1 Corporate Governance

In the past years several legal regulations were passed, from which direct action and liability obligations of the executive board or more specifically the management of a company to questions about information security can be deducted. Those regulations apply both for stock companies as well as limited liability companies.

Principles of the Corporate Governance were codified in the German Corporate Governance Code. Next to essential legal regulations about corporate management and publicity the code provides information about recommendation to the direcitng and monitoring of publicly traded companies.

In this context it is pointet to the law of control and transparency in business units ("Gesetz zur Kontrolle und Transparenz im Unternehmensbereich", **KonTraG**), which became effective in May 1998. The **KonTraG** is a so-called articel law and complements or changes laws like the commercial code ("Handelsgesetzbuch", HGB) and the Stock Corporation Act ("Aktiengesetz"). In particular, the demand for an early risk detection system for corporations – that means for stock corporations and limited liability companies – was not included in the previous regulations and had to be set up by the companies themselves. As part of the European measure **EuroSox** in 2006, minimum requirements for risk management were described and the duties of auditors were defined. In Germany the Accounting Modernisation Act ("Bilanzierungsmodernisierungsgesetz", **BilMoG)** came into force in 2012, which requires corporations, for example, to present their internal control systems in annual financial statements.

The managing directors of a limited liability company (in German GmbH) are required by the **GmbH-regulations** to exercise "the diligence of a prudent businessman" (§ 43 Para. 1 GmbHG). Issues of consumer protection are dealt with in various laws. The use of information technology, the use of the internet or the use of telecommunications services are regulated very precisely. Relevant laws include, for example, the law on the use of teleservices ("Gesetz zur Nutzung von Telediensten"), the Telecommunications Act ("Telekommunikationsgesetz"), the State Treaty on Media Services ("Mediendienste-Staatsvertrag"), copyright law ("Urheberrecht") as well as various directives at EU level. The handling of personal data is regulated in the data protection laws of the federal and state governments ("Datenschutzgesetzen des Bundes und der Länder"), the law on data protection for teleservices, the Telecommunications Data Protection Ordinance ("Telekommunikations-Datenschutzverordnung") and in some cases in the laws already listed (Bundesamt für Sicherheit in der Informationstechnik 2012, p. 17f.).

In the HGB, due diligence is imposed in Section 347. Generally speaking, "diligence" is measured differently from industry to industry. However, the same standard applies everywhere: a businessman (definition of a businessman according to section 1 HGB) is obliged to inform himself about the corresponding rules of his commercial business. It can therefore be deduced that a businessman must constantly inform himself independently about current norms and laws and must be liable for the damage incurred in the event of non-compliance. Nevertheless, this is not explicitly codified, but is regarded as a general standard on which entrepreneurial action is based.

It is therefore of existential importance for companies to understand IT security as part of their entrepreneurial duty of care. Knowledge of the aforementioned legal content and the significance of the underlying standards of due diligence are therefore essential for the correct handling of data protection and information security.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.2 Information Security

The law to increase the security of information technology systems ("Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme", IT Security Act (IT-SiG)), which came into force in July 2015, is an article law which amends and supplements the law of the Federal Office for Information Security ("Bundesamtes für Sicherheit in der Informationstechnik", BSI), the Energy Industry Act ("Energiewirtschaftsgesetz"), the Telemedia Act ("Telemediengesetz") and the Telecommunications Act ("Telekommunikationsgesetz"). The IT-SiG represents a revised version of the federal act to strengthen security in information technology of the federal government of 2009 and is intended to meet the needs of the changing risk situation through the progressing digitalisation of state, economy and society. At the same time, the "IT Security Catalogue pursuant to Section 11 (1a) EnWG" was adopted, which establishes IT security requirements specifically for operators of electricity and gas grids. A further security catalogue ("IT security catalogue pursuant to Section § 11 paragraph 1b EnWG") was published in December 2018, in which the security requirements for operators of energy systems are defined.

The law was extended in May 2016 by the KRITIS regulation, the first part of the BSI ordinance. The June 2017 amendment stipulated that the energy, water, transport and traffic, health, finance and insurance sectors are to be classified as Critical Infrastructures (KRITIS) and are therefore obliged to equip their IT systems with state-of-the-art technology and have their information security checked every two years. Since May 2018, the Basic Data Protection Regulation ("Datenschutzgrundverordnung", DSGVO) issued by the European Commission has provided these standards for other companies with sensitive data (Bundesnetzagentur 2019).

Based on the federal government's digital agenda from 2014, the law is intended to contribute to improving the security and protection of IT systems and services. Particularly with regard to critical infrastructures, threats or supply bottlenecks would have far-reaching consequences for the state, the economy and society in Germany. The KRITIS Ordinance (BSI-KritisV) clarifies which facilities, installations or parts thereof are specifically covered by the requirements of the IT-SiG. Further goals of the law are an improved IT security of enterprises, administration, institutions as well as a larger protection of Federal citizens for the use of the Internet. The main adressees are operators of critical infrastructures, web service providers, telecommunications companies and the BSI (Bundesamt für Sicherheit in der Informationstechnik 2016, S. 5).

In June 2017, the directive on high network and information security (NIS Directive) was issued by the European Commission in order to create a uniform legal framework to strengthen IT security for KRITIS operators and providers of digital services. In terms of content, the IT-SiG covers the obligations of critical infrastructures, which was extended in May 2018 to include the law enacted to implement the NIS Directive (Bundesamt für Sicherheit in der Informationstechnik 2019b).

In practice, standards have been developed by the BSI to ensure that companies meet information security requirements. The BSI standards define requirements for an information security management system (BSI Standard 200-1), which is intended to ensure that personal data is processed in compliance with the law. Standard 200-1 conforms to the international standard ISO 27001 (Bundesnetzagentur 2015).

With the changing legal situation and the associated classification of energy plants as critical infrastructures, there are new requirements for the IT security of the affected companies, which have until the end of February 2019 to name their contact person for IT security to the Federal Network Agency and subsequently have to provide proof by 31 March 2021 that the requirements of the security catalogue have been implemented. Knowledge of the new requirements is therefore of vital importance both for the companies and for the employees responsible for information security. An information security management system (ISMS) for SMEs is not (yet) legally binding. In practice, however, it is necessary to comply with standards in the supply chain when doing business with listed companies, as this is required in the supply contracts.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.3 Data Protection

The Basic Data Protection Ordinance (DSGVO), which came into force in May 2018, replaces the Federal Data Protection Act ("Bundesdatenschutzgesetz", BDSG-alt) in Germany, which had been in force until then. The implementation of the opening clauses contained in the DSGVO was regulated in Germany by the EU Data Protection Adaptation and Implementation Act (BDSG-new), which became effective at the same time and thus supplements the DSGVO with the leeway given to the federal states. In addition, the BDSG-new also regulates areas that remain unaffected by the DSGVO (Datenschutz.org 2018).

The new BDSG is divided into four sections: The first part contains general provisions, the second part deals with the specification and amendment of the DSGVO, part 3 implements the EU Data Protection Directive for Police and Justice (EU 2016/680) (and therefore does not apply to private companies) and part 4 regulates areas that are neither covered by the DSGVO nor by Directive 2016/680 (Datenschutz.org 2018).

The complementary character of the BDSG-new can be seen in various places. Article 38, together with the DSGVO, regulates, among other things, when a data protection officer must be appointed (This is the case if the processing by a private position involves extensive or systematic observation of persons, if the core activity of the position is the processing of personal data, if at least ten persons are permanently engaged in the automated processing of personal data and (irrespective of the number of persons entrusted) if data are processed for the purpose of transmission of market and opinion research) (Landesbeauftragte für Datenschutz und Informationssicherheit Nordrhein-Westfalen 2019). Another point is the employment data protection (DSGVO Art. 88), which explicitly provides for national regulations. This was implemented by § 26 BDSG-neu. Finally, the BDGS provides for punitive measures in the event of data protection violations (§ 42), which go beyond the envisaged fines of the DSGVO (Art. 83). These are only a few examples of the interaction between the Federal Data Protection Act and the Basic Data Protection Ordinance. In principle, when applying the DSGVO, attention must be paid to statements in the BDSG (Datenschutz.org 2018).

Security officers are required to have precise knowledge of data protection law following the amendment in 2018. All in all, the laws introduced in recent years place high demands on the correct handling of information and data security, which makes continuous further training of security officers in legal issues indispensable. This poses particular challenges for small and medium-sized enterprises (SMEs), as the resources required for this, such as their own IT or legal advice, are not sufficient for this type of conversion processes.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3. Vocational and Continuing Education and Training in this area

The levels of the European Qualifications Framework (EQF) were implemented in Germany through the introduction of the German Qualifications Framework (DQR) (the National Qualifications Framework (NQR) in Germany). The eight levels of the DQR correspond to the stages of the EQF, taking into account the German dual education system (vocational and school education). The levels of the DQR are structured differently from those of the EQF: instead of the three competence fields of the EQF to describe a learning outcome ("knowledge", "skills" and "responsibility and autonomy"), the four fields "knowledge", "skill", "social affairs" and "autonomy" were used to adequately characterise the learning outcomes sought in the German education system (DIHK 2016). The qualifications available in Germany are classified in the DQR according to Figure 1:

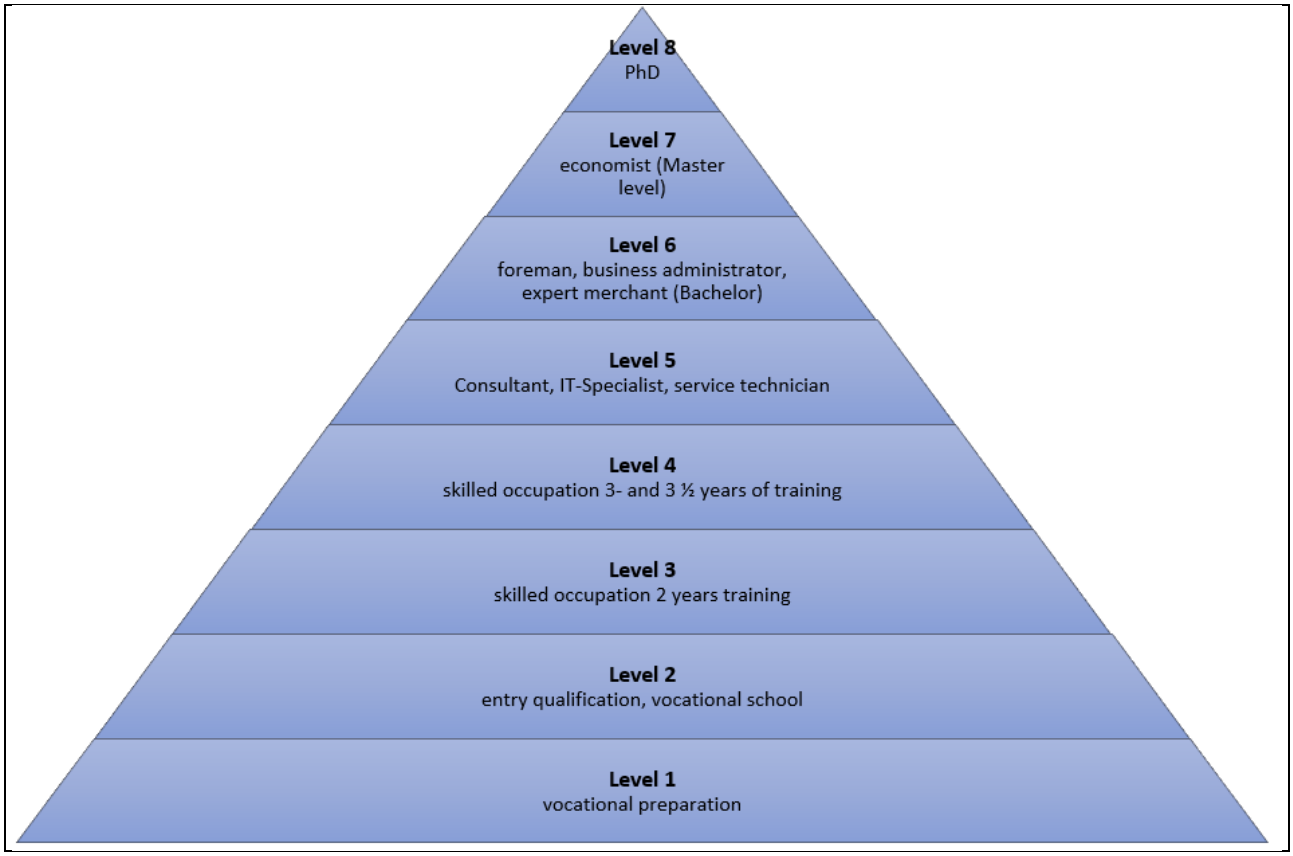

Figure 1: DQR educational levels (IHK)
Source: Own presentation based on DIHK (2016)

Against this background, training courses up to DQR level 4 represent vocational training whose qualifications are not acquired at a university but at a vocational school and are usually linked to in-company training. These degrees are awarded by the IHK. Levels 4 and 5 include the following qualifications:

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Level	Qualification
4	• Dual vocational training (3 and 3 ½ years training) • Vocational school (assistent jobs) • Vocational school (fully qualified vocational training – BBiG/HwO))
5	• IT-Specialist (certified) • Service technician (audited)

Figure 2: Professional qualifications level 4 and 5
Source: Own presentation based on DQR (2014, p. 2)

At this level, three and three and a half year trainings and certification as an IT specialist are of particular interest (see Figure 2). Not unmentioned at this point are the possibilities of education at colleges and universities. There are various Master's programmes in the fields of information security and data protection. The profile area of cyber security at Darmstadt Technical University, which offers the Master of Science (M.Sc.) in IT security, deserves special mention here. Table 1 provides a brief overview of study programmes in the field of IT and data security.

Table 1: Exemplary Master's programmes in Germany (DQR 8)
Source: Own presentation

Study programme	Short description	Link
M. Sc. Applied IT-Security	• Part-time correspondence course • Covers IT security and new technologies • Addresses (economic) computer scientists, physicists and mathematicians, engineers	https://www.master-and-more.de/nc/mastersuche/detailansicht/profil/studiengang/applied-it-security-99000026288/
M.Eng. IT Security and forensic science	• Part-time correspondence course • Train experts for IT security in companies and public institutes • Detect cyber attacks in time and plan and implement appropriate security measures	https://www.master-and-more.de/nc/mastersuche/detailansicht/profil/studiengang/it-sicherheit-und-forensik-99000048600/
MBA Compliance and data protection	• Part-time • Training as management and technical specialist in the areas of compliance and data protection, fraud and risk management, controlling and corporate ethics, corruption prevention	https://www.master-and-more.de/nc/mastersuche/detailansicht/profil/studiengang/compliance-und-datenschutz-99000052184/
M.Sc. Security Management	• Part-time • Business and technical IT-relevant security topics • Individual profiling with elective subjects possible (e.g. bank security, cyberwar and cybersecurity, information security or IT forensics)	https://www.master-and-more.de/nc/mastersuche/detailansicht/profil/studiengang/security-management-9900004957/
M. Sc. Digitale forensic science	• Part-time • Information and telecommunications technology • Legal science	https://www.master-and-more.de/nc/mastersuche/detailansicht/profil/studiengang/digitale-forensik-9900005296/

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Within the framework of vocational training, the IHK offers seminars, trainings and apprenticeships in several areas. Seminars take place on data protection in the personnel area and data protection officers in the company, the "White Hacker" is offered as a training. Apprenticeships with state-approved DQR level 4 are possible to become an information technology clerk, an IT system clerk and an IT system electronics technician (IHK 2018b, 2018c).

Building on this, further training to operative (DQR level 6) and strategic (DQR level 7) professionals is possible (see Figure 3): a specialist qualification (DQR level 5) in one of 14 possible fields of work, relevant for this is the IT security coordinator, allows admission to the examination of an operative as well as a continuing strategic professional. In the field of continuing vocational training, the specialist qualification forms the link between the vocational training and the level of the operative professionals regulated in the continuing vocational training. Figure 3 illustrates the continuing training structure of the IHK.

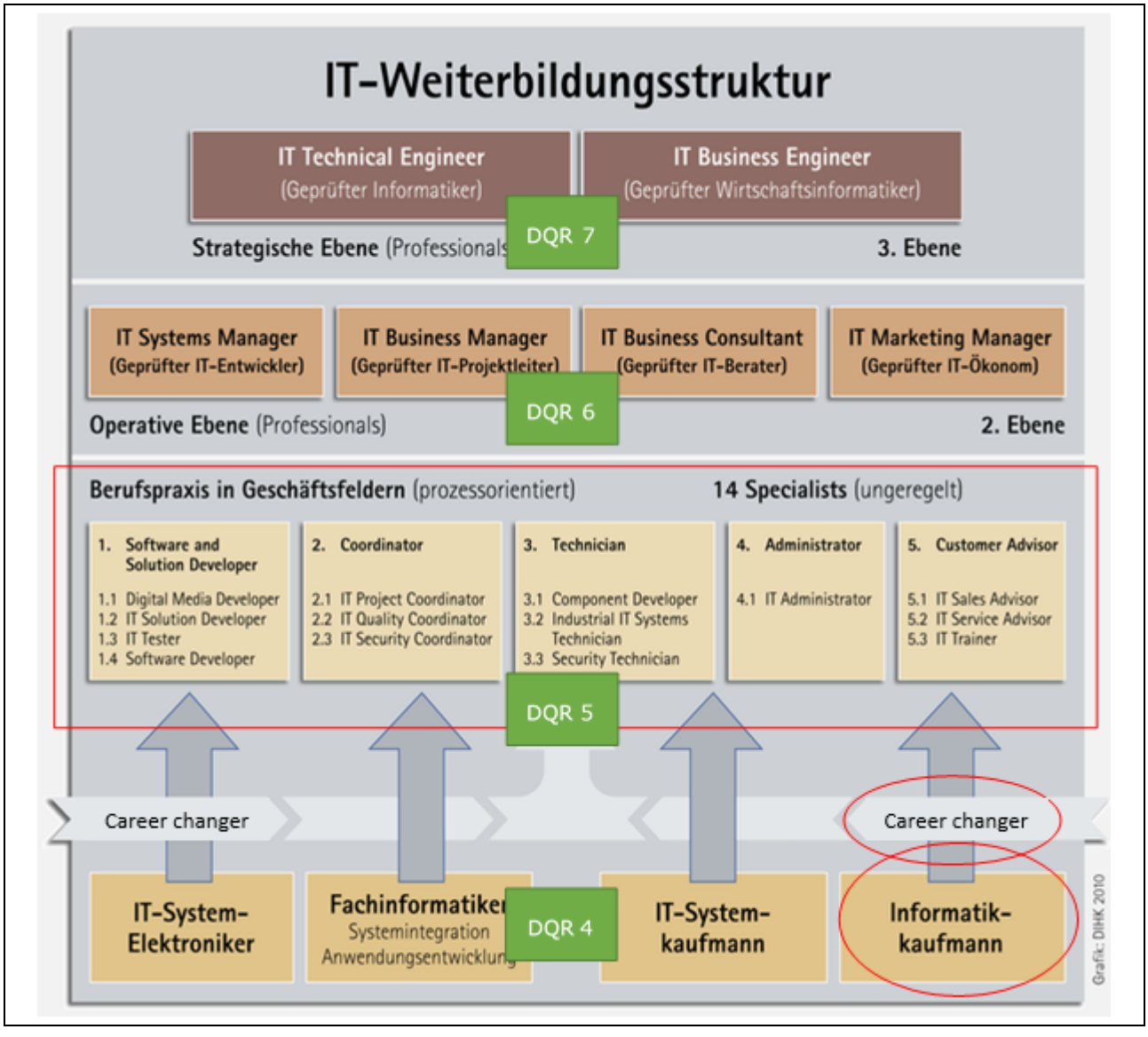

Figure 3: Continuing training structure of the IHK
Source: Own presentation based on IHK (2018d)

A completed vocational training to participate in a further training to become an IT specialist is, however, not absolutely necessary, as can be seen from the figure above.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Admission requirements exist above all in the area of continuing education under public law, e.g. for the state-recognised examination for IT professionals. For the certificate area of continuing education, such as that of an IT specialist, there are usually no requirements. Nevertheless, admission requirements determine the qualification for entering a certain level of continuing education. The qualification to become an IT specialist also requires a certain entry level. In connection with the certification of individuals, it was stipulated that a continuous training participant must either

- a vocational qualification in an IT profession or
- other professional qualifications and at least one year's relevant professional experience in the IT field, or
- must have at least four years' relevant professional experience.

Those who, by presenting certificates or by other means, can demonstrate that they have achieved the qualification justifying admission to certification are also admitted. In order to ensure the entry level of their qualification offers for IT specialists, the IHKs comply with these admission requirements.

In order to improve the competence-related self-assessment of people who want to validate non-formal competences, so-called Development Centres (DC) are used. They represent a special form or further development of the Assessment Centre (SC). These are procedures in which the participants go through different diagnostic modules (e.g. interviews, role plays, psychological test procedures, etc.) for two to three days and receive detailed feedback on their results (Klebl und Nerdinger 2010). The IHK offers three to four-day DC for business founders (IHK 2018a).

However, the use of DCs in the area of IT security is not known.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.1. Overview of Existing Training Offers in the Field of Information Security

In order to gain an overview of the training opportunities available in the field of information security, a combined search with the following keywords was carried out: "IT Security", "Information Security" and "Continuing Education". The IHK offers apprenticeships and seminars at DQR level 4 and above. The admission requirements vary depending on the programme; in some cases, only interest and a school certificate are required, but in others work experience in the respective field is also required (cf. Fig. 3). The mentioned examples do not necessarily focus on the topics of information security and data protection, but at least temporarily deal with these topics within the framework of training. Table 2 provides an overview.

Table 2: Apprenticeships of the IHK
Source: Own presentation based on IHK Bayreuth (2018)

Name of Training Course	Main Content / Objective	Target Groups (basic /intermediate / proficiant user)	Skills acquired (professional, social and transversal)	Kind of Testimonial
Apprenticeship Information Technology Management Assistant (DQR 4)	Procurement and administration of information and telecommunication systems, determination of user requirements, planning and creation of application solutions, consulting and training of users, ensuring economic efficiency and customer- and user-oriented organization of projects.	basic user, access at any age (<18 with medical certificate), predominantly first-year trainees with university entrance qualification; if qualification is obtained from abroad, an equivalence certificate can be obtained	• Interest in commercial-organizational activities, in social-consulting activities, in theoretical-abstract activities • Performance and operational readiness. Care, independence, flexibility, willingness to learn, communication skills, friendly and winning character, customer and service orientation, negotiation skills, assertiveness. • Abstract-logical, computational and linguistic thinking, technical understanding, etc.	Information Technology Management Assistant diploma
Apprenticeship IT system electronics	Planning and installation as well as configuration and commissioning of customer-specific IT systems, system	Basic user, High School deploma, secondary school diploma and general	• Interest in practical and concrete activities, in organizational and auditing activities, in theoretical and abstract activities	IT system electronics technician diploma

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

technician (DQR 4)	maintenance, fault analysis, troubleshooting; consulting and training of customers	school diploma, few without any school diploma	• Performance and operational readiness. Care, independent working method, flexibility, willingness to learn, customer and service orientation. • Abstract-logical, computational and linguistic thinking, technical understanding, etc.	
Training White Hacker	Contact person for IT security management issues, development and implementation of suitable attack and protection measures in the company, consulting in the design of IT security, support in the implementation and maintenance of associated business and development processes.	Developers, programmers, IT managers, administrators, project managers, management consultants, employees in the field of IT security	work experience	White Hacker certificate

Trainings and courses that last only a few days or weeks are offered by various service providers. These are not controlled or standardised by official chambers such as the IHK and therefore do not offer generally valid certification for graduates of these courses. The only prerequisites for taking an examination with these service providers are participation in the course and payment of the fees. Table 3 shows some of these service providers and their course offerings. However, special offers tailored to the needs of SMEs are not offered at the current state of research. The list shown is based on information provided by the BSI (Bundesamt für Sicherheit in der Informationstechnik 2018b) and represents only examples of training offerings. The complete list can be found at: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/SchulunganderenAnbieter/schulungandereranbieter_node.html
.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table 3: Offerings by service providers in the area of information security
Source: Own presentation

Service provider	**Course name**
Bitkom	Certificate training for the introduction of an information security management system (ISMS)
Bechtle	Basic IT protection with I-DOIT VIVA Training
Bristol Group	Certification as Information Security Officer ITSIBE / CISO
TÜV	Basic IT protection expert
Akademie der DGI Deutsche Gesellschaft für Informations-sicherheit AG	• Training as IT Security Officer (ITSiBe)/ Information Security Officer (ISO) according to ISO/IEC 27001 and BSI basic IT protection • Training as BSI basic IT protection expert according to BSI basic IT protection Compendium and BSI Standards • Training as Business Continuity Manager according to ISO 22301 and BSI IT-Grundschutz • Training as qualified IT risk manager according to ISO 31000 and ONR 49003

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.2. Overview of Existing Training regarding Data Protection

As well as for information security, there are also service providers for certifications in the area of data protection. These are equally not examined by a chamber like the IHK regarding the course contents. The admission requirements for an examination are the same as for the service providers in Table 3, payment of the course fee and completion of the course. Table 4 shows some service providers for certification in the area of data protection, but these are only examples of offers. However, as in Chapter 3.1, special offers tailored to the needs of SMEs are not offered. The table shown is also based on BSI information (Bundesamt für Sicherheit in der Informationstechnik 2018b). The complete list can be found at: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/SchulungandererAnbieter/schulungandereranbieter_node.html .

Table 4: Offerings of service providers in the area of data protection
Source: Own presentation

TÜV	Data protection officer according to DSGVO and BDSG-new
TÜV Nord	Data Protection – Cloud Computing
TÜV Nord	Data Protection in Marketing and advertising measures
GDD e.V.	Data Protection Officer
VDI	Implementing the GDPR
IHK	Training: Date protection in the personnel area
IHK	Training: Data protection officer in the company

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. Overview of jobs offered in the field of Information Security and Data Protection

According to BITCOM, there were 55,000 vacancies for IT specialists at the end of 2017, an increase of 20% compared to the previous year in Germany. This increase is most noticeable in the area of IT security experts: there is a particularly strong imbalance between the jobs offered and the number of applicants. For example, there were about four advertised positions for one security engineer, the same ratio prevailed for IT consultants with IT security expertise. In the case of IT administrators, there were still 3 advertised positions for every applicant. The most difficult field to fill in IT security in German companies is network security, followed by mobile applications and risk management (Berg 2017).

However, the growth in demand is strongly industry-specific: in the Internet of Things (IoT) segment, the demand for IT security experts increased by 370% compared to 2016. In cloud computing, demand increased by 138%, followed by application security (33%), mobile applications (29.9%) and compliance (22.4%) (Berg 2017).

Overall, the demand for IT security experts across all industries increased from 12% of all companies in 2015 to 20% in 2017. 28% of all companies are looking for software developers for security (compared to 17% in 2015) (Berg 2017).

The increased demand for security experts is also reflected in the average salaries, which at €75,000 are higher for employees without personnel responsibility than for project managers or SAP consultants (Mesmer 2018).

An evaluation of job offers in the IT security sector has shown that around 60% of job offers are directed at IT security, data protection and data security specialists. Furthermore, approx. 30% of the job offers were directed at IT consultants and approx. 6% at software developers specialising in IT security. The task most frequently described was "developing, implementing and monitoring concepts, guidelines and strategies" (68.7%). More than half of the ads examined required work experience. With regard to concrete specialist knowledge, experience in system or network administration was required in 26.2% of the advertisements and knowledge of the ISO/IEC 27000 series of standards was explicitly required in around a quarter of all advertisements.

With regard to the required certification, a degree in computer science (70%) or business informatics (31.9%) was required by a large margin. However, candidates with IT or computer science training also had good chances (26.8%). A completely new development can be seen in the required qualification of a law degree with 16.3% (Blindert 2018).

With these facts in mind, most positions are advertised in the areas of Consultant Information Security, Data Protection Officer, Programmer, IT-Consutant, Advisory and Compliance as well as Legal Affairs.

In order to address the security concerns of companies, the job of Chief Security Information Officer (CISO) has existed for some time now. He is responsible for information security in the company (Whitten 2008, S. 15). A combined search with the keywords "CISO" and "job" in common job portals and the subsequent screaning of the job offers revealed that the companies expect a completed degree or a comparable education with several years of professional experience, various certificates such as ISO 27001 or CISM as well as expert knowledge in information security management. An input at the job portal "Indeed" of the search term "CISO" delivered 64 hits, while an input of the term "data security" yielded approx. 12,000 hits and "information security" approx. 1,200 hits.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4.1. Overview of job offers in the field of Information Security

If you look for job offers in the field of information security on the websites of small and medium-sized enterprises (SMEs), large enterprises and non-governmental organisations (NGOs), you will come across many job postings. This illustrates the high relevance of data and information security for companies as well as the need for suitable specialists. The following table (Table 5) provides a brief overview of these job postings.

Table 5: Job offerings in the area of information security
Source. Own presentation

Job offer / enterprise	General description	Skills required (professional, social and transversal)	Link
IT advisor Information Security Analysis Volkswagen AG	• Processing of information security requests regarding compliance with the Volkswagen IT security settings within the framework of the ITSP programs • Tracking and monitoring of the implementation of measures to request and track exemptions • Execution of plausibility checks of URL filter requests • Ensuring knowledge transfer including maintenance of the IRIS knowledge database	• Processing of information security requests regarding compliance with the Volkswagen IT security settings within the framework of the ITSP programs • Tracking and monitoring of the implementation of measures to request and track exemptions • Execution of plausibility checks of URL filter requests • Ensuring knowledge transfer including maintenance of the IRIS knowledge database	https://jobs.volkswagen-groupservices.com/sap/bc/bsp/sap/zgs_hcmx_ui_ext/desktop.html?wt_mc=sea.text-ad.vw%20karriere.brand.div&gclid=Cj0KCQiAvebhBRD5ARIsAIQUmnng2DVsNms9gVJf3e2OW8FIvO8QxwZL7GpSP6kzNkOy1i2HINjABWsaAvv_EALw_wcB#/SEARCH/SIMPLE/
Senior Security Management Consultant F-Secure (KMU)	• Delivering and managing security and risk management tasks • customer support • Identify new trends and developments in information security services	• Expertise in information security management • Experience with ISO 27001 implementation • Risk assessment, risk modelling and threat modelling • -T forensics	https://emp.jobylon.com/jobs/32848-f-secure-senior-security-management-consultant-senior-manager-level/

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

		• Certification of risk, security and data protection desirable	
Senior Consultant Information Security (f/m) PERM4 (KMU)	• Optimization of information security services and products • Management of customer projects • Contact for customers with questions about information security • Participation in sales	• Degree in information technology or natural science • Several years of professional experience in information security, preferably in the banking environment • Independent, structured and solution-oriented way of working • Fluent in German for negotiations	https://de.indeed.com/viewjob?jk=85a5e84a413107d8&tk=1d10pq20a91sh800&from=serp&alid=3&advn=5851112616713407&sjdu=4_2iX105lbnBMz5tAvt_34Bever85Oq0g0Hk4cPJLvyCr5X8SeL3D689nEULUVv_-FJNsFCyHmMrexyPARNeiWhKwJwY-gRqP5u6mkUQr7k
Employee (f/m/d) for information security and technical data protection Regio iT (KMU)	• responsible for the implementation of existing information security measures and document these accordingly. • contribute to the further development of our security processes and the resulting tasks. • Carry out penetration tests and support the implementation of internal audits. • Interdisciplinary cooperation with colleagues from our entire organization • advise and support our customers in topics of their area of responsibility	• completed apprenticeship in information technology or security or several years' professional experience in this field • Knowledge of national and international standards, methods and procedures of information security and technical data protection • Open to new requirements, willingness to further training • Team player (f/m/d), communicative and goal-oriented working • dedicated, resilient and flexible • good English skills	https://de.indeed.com/viewjob?jk=902660bf085903e4&tk=1d10pskgb91sh800&from=serp&alid=3&advn=3907019553144236&sjdu=pkrpf4JGU-IUZM4Z9MCPybFhL62ylFQxCVJrcJShWvhK1jiR77-ENB4nqmd6wxg0T5vOSlvgFvE3GDEEYyzrCA
Senior Consultant (m/f/d) Data Security and	• Advising national and international companies on the requirements of the EU data protection basic regulation	• Successfully completed university studies in law, economics, business informatics, industrial engineering, computer science, mathematics or comparable subjects	https://jobs.deloitte.de/job/mehrere-Standorte-Senior-Consultant-Data-Protection/335387501/

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Information Security Deloitte	• Implement data protection requirements in policies, standards and processes • Development, analysis and optimization of data protection management systems • Collaboration in cross-functional teams	• At least 3 years' relevant professional experience as a data protection officer or consultant • Sound knowledge of data protection requirements (basic EU data protection regulation) • Basic knowledge in the area of information security management as well as the relevant standards, e.g. ISO 27001 • High IT and process affinity • Good MS-Office knowledge, especially Excel and Powerpoint; • Confident appearance, initiative, mobility and ability to work in a team • Excellent presentation and communication skills in German and English • Data protection certification desirable	
IT Security / Cloud Architect Amnesty International	• Independent conceptual further development of the IT system landscape • Extension and development of IT security measures • Planning and implementation of the developed concepts • IT project management and quality assurance • Control and coordination of the supporting external service providers • Optimization of the IT value added depth	• Preferably completed studies or training with professional experience in the IT field • Technical Know-How • Knowledge of IT service processes and standards • Reliability, ability to work in a team, resilience	https://amnesty.jobbase.io/job/4njf1tui

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Consultant (m/w/d) IT-Security (IAM, PKI, SIEM) 7 Principles	• Consulting and assiting in the conception, commissioning and operation of IT security components and applications • Idetification and evaluation of current customer requirements, development of concepts and solutions taking into account regulatory requirements, standards and best practices • Participation in projects for the introduction of ISMS	• Completed study of (business) computer science or comparable qualification • Professional experience in the conception and administration of IT security components and applications • In-depth knowledge of IT and network technology • Relevant certifications (CISSP, ITIL, Cobit, etc.) • Knowledge of relevant norms and standards for information security and IT service management (e.g. DIN ISO/IEC 27001/2, Cobit, BSI IT-Grundschutz, ITIL) • German and English spoken and written skills • Analytical and communicative skills • Willingness to travel within Germany, no readiness to move necessary	https://www.7p-group.com/job/consultant_it_security/#job

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4.2. Overview of job offers in the field of Data Protection

Just as in chapter 4.1, in this chapter the websites of companies and NGOs were searched for job offers, only this time not in the area of information security, but in the area of data protection. Table 6 gives an overview of these jobs.

Table 6: Job offerings in the area of data protection
Source: Own presentation

Job offer / enterprise	General description	Skills required (professional, social and transversal)	
Specialist in Data Security Porsche AG	• Counselling the departments on data protection requirements in national and international business environment, in particular on data protection conformity of products • Execution of risk analyses in the data protection environment and preparation of corresponding reports and action plans • Review and control of business and product development processes, information systems, guidelines and contracts for compliance with national and international data protection requirements, as well as corresponding consulting • Creating of data protection relevant forms, guidelines and agreements, also in cooperation with the responsible specialist departments	• Successfully completed law studies with a degree of distinction or comparable qualification • Long-time professional experience (usually 5 years) in a comparable environment • Very good knowledge of IT and data protection law • Fluent in English and willingness to travel • Strong analytical skills and an independent, structured and goal-oriented way of working • Strong team, communication and assertiveness skills	https://jobs.porsche.com/index.php?ac=jobad&id=16528

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	• Conception, planning and implementation of training and awareness-raising measures		
Data Security Officer PERM4 (KMU)	• Support of municipal customers with regard to data protection issues • Participation in the development of a data protection management system • Preparation of data protection concepts • Ensuring compliance with EU-DSGVO requirements • Review of orders and contracts • Organisation and implementation of training courses • Close cooperation with the supervisory authority	• Completed studies in business informatics or a comparable education with IT-related background • Professional experience in the fields of data protection and information security • Knowledge of administrative processes in the municipal sector • Service and process-oriented working methods • Business fluent in German	https://de.indeed.com/viewjob?jk=7569c383ace91868&tk=1d10pi8nb91sh800&from=serp&alid=3&advn=5851112616713407&sjdu=4_2iX105lbnBMz5tAvt_3-W_EXcx3io1MLdLaV8vjb79Aail7DRMbkHNCYaBxIGcpvuAm-omvnXPWFnxgk16ww
Consultant (m/f/d) Data Security and IT Security (nationwide operation) DATEV	• Analysis, evaluation and optimization of business processes with regard to data protection and IT security • Working with managing directors and partners of our customers as a trustworthy advisor • Presentations and sales activities in direct customer contact • active development of methods and services in the field of data protection and IT security • Customer support during the implementation of measures • Independent planning and control of the work in compliance with the objectives	• Knowledge of business processes, in the area of data protection law and its application as well as IT know-how • Experience as data protection officer • high consulting competence and conceptual skills • special feeling for customer needs, ideally acquired in a renowned consulting company • Enjoying teamwork and Germany-wide assignments	https://www.datev.de/bms/cgi-bin/appl/selfservice.pl?action=jobdetail;job_pub_nr=D37756E7-01F1-4F53-B293-8461D4AE4B2D;p=homepage
Employees (m/f/d) Data	• support and advise the management and employees on data protection and compliance issues	• successfully completed studies in the field of economics with a focus on data protection or comparable qualifications and at least two years of	https://de.indeed.com/viewjob?jk=7c79a7e708b38cbf&tk=1d10q30gn91sh800&from=serp&alid=3&advn=245953091847357&s

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

protection and compliance Meyer Quick Service Logistics GmbH & Co. KG (KMU)	• This also includes the design and implementation of internal training courses and the further development of compliance management. • Review data privacy notifications, assist with directory creation and capture and evaluation of data privacy issues • Advice on legal issues in connection with compliance matters and, if necessary, the revision of contracts of all kinds • Travel activity due to the support of national and international locations • report directly to management	professional experience in the compliance area and/or in areas relevant to it • Ideally, further training with regard to the EU-DSGVO as well as experience in legal issues, especially in the area of data protection. • quick comprehension as well as a structured, reliable, result-oriented and precise way of working • High level of consulting and social competence also in an international environment, ability to work in a team, confident appearance and persuasiveness • Good knowledge of MS Office and very good written and spoken English skills	jdu=kotibzAfyPb4-t2PCLyuzQq_gWyyjRk4roJTTjRocCvVqPgO0eN5xO4vODJX63o5vDa7FWtwRu3eQWkzfDjBGtEHbPNS8WrbGmVedW49gNeb9cVpeRvA9RalyKIeBQFZ
(Senior) Consultant (m/w/d) Data Governance / Data Security Business Intelligence 7 Principles	• Supporting customers in the design and implementation of solutions in the field of Business Intelligence & Big Data • Preparation of data protection concepts, data protection documentation and advice to customers on data protection issues • Development of solutions in cooperation with the data protection officer taking customer requirements into account • Taking over the function of external data protection officer for customers and carrying out data protection analyses, procedures and applications • Interface between IT and specialist departments and data protection officer	• Completed studies or comparable apprenticeship • secure knowledge of data protection and data security • familiar with the application of the current EU data protection basic regulation • sound knowledge of Business Intelligence and/or Big Data • Knowledge of handling an ETL tool or BI frontend • Development of creative solutions in the project team • Willingness to familiarise oneself with new topics at short notice • Promote projects with commitment	https://www.7p-group.com/job/senior-consulant-data-governance-datenschutz-business-intelligence/#job

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	• Carrying out audits in the area of data protection to monitor the legal requirements in accordance with the Basic Data Protection Ordinance	• Analytical and goal-oriented work • very good knowledge of German and good knowledge of written and spoken English • willingness to travel	

The job descriptions do not show any differences in the demands placed on employees between large companies and SMEs.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5. Existing Methods for Assessing and Certification of Vocational Skills aquired outside formal Education

Due to its complexity, a data protection officer is legally obliged to undergo training. Pursuant to art. 39 paragraph 2 DS-GVO, the company employing the data protection officer has the duty to support him in the performance of his tasks and, in particular, to provide him with the resources required to perform his duties and maintain his expertise. Therefore, it must also facilitate appropriate qualification. The „Society for data protection and data security e.V.“ (Gesellschaft für Datenschutz und Datensicherheit e.V.) has been offering training concepts for the training and further education of data protection and security officers in companies for 30 years (GDD 2018).

The BSI offers several certification methods for information security. The ISO 27001 is a certificate for companies that is issued only after an external audit and certifies that the company has basic IT protection (Bundesamt für Sicherheit in der Informationstechnik 2018c). It is not a certification for a person regarding their competences, but is intended exclusively for companies.

The entire certification procedure of the BSI for persons is shown in Figure 4 and takes about three years. After a positive examination of the application, the applicant is evaluated. The competence assessment is carried out by an external service provider. If the applicant passes this evaluation phase, his competences are monitored and maintained for three years. After completion of the certification phase, the applicant submits a new application and receives a certificate if the evaluation is positive. The certification is limited to a period of three years (Bundesamt für Sicherheit in der Informationstechnik 2017, 2018a).

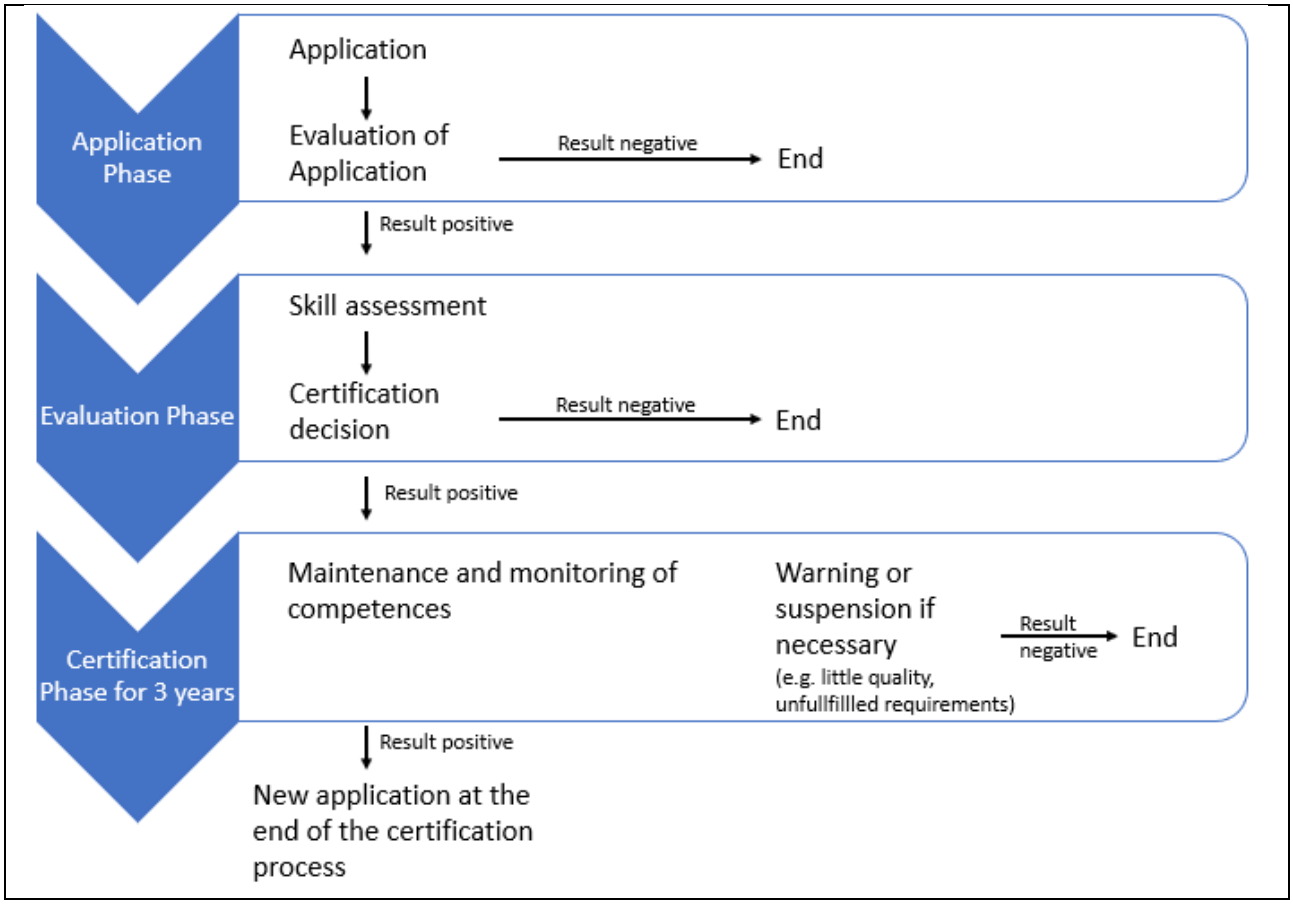

Figure 4: Certification procedure oft he BSI
Surce: Own presentation based on Bundesamt für Sicherheit in der Informatinstechnik 2017, p. 6

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Certification is possible as a: Audit team leaders, De-Mail auditor, Smart Meter Gateway administrator auditor, "Secure E-Mail Transport" auditor, RESISCAN auditor for BSI-TR 03138, Secure CA Operation auditor, IS auditor, penetration tester, CC evaluator & Common Criteria training, TR auditor, BOS interoperability tester/ZPL employee.

Other providers such as the Academy of the DGI (German Society of information security AG - Deutsche Gesellschaft für Informationssicherheit AG), EDV-Fortress or TÜV offer training courses on basic IT protection, which, however, are not checked for content or quality by the BSI, as already mentioned in Chapter 3 (Bundesamt für Sicherheit in der Informationstechnik 2019a; BayLDA 2016). A complete overview is provided in Table 7 (see Annex).

Valikom offers a validation procedure in cooperation with the IHK and the Chamber of Trade (Handwerkskammer - HWK) (https://www.validierungsverfahren.de/startseite/). The target group here are people who:

- are at least 25 years old
- regardless of their current employment status
- have acquired professional skills at home or abroad
- but cannot prove this by means of a degree
- can prove relevant professional experience.

The validation process is divided into the following steps:

1. The applicant must report to a contact person (at HK or IHK).
2. An advisory interview follows with this contact person, discussing the validation process and the choice of the appropriate reference occupation. The reference occupation corresponds to a professional qualification.
3. The relevant skills of the applicant are described and a curriculum vitae is drawn up which reflects the skills (everyday working life, training and further education, everyday life if relevant). These competences are entered in a self-assessment form.
4. The applicant's competences are compared with those required for the reference occupation.
5. The application documents for the validation are submitted to the chamber, which evaluates in which activities of the reference occupation an external evaluation will take place.
6. The external evaluation is carried out by experts of the respective reference occupation and tests the applicant's abilities in practice. This includes work samples, a technical discussion or trial work in a company.
7. The expert submits the results of the external evaluation to the chamber.
8. Depending on the result of the external evaluation, the chamber shall issue a validation certificate confirming full or partial equivalence with the reference occupation.

Another validation of professional competences is offered through the website https://www.myskills.de/. In cooperation with the Employment Agency, applicants carry out a computer-based test on the basis of which a certificate is issued. The test is so far only for eight occupational groups available, which limits it very much. Valikom on the other hand is by far more detailed and contains a practice test, which makes it more valuable for applicants and enterprises.

The DQR working group (the coordination group responsible for the development of the DQR set up by the Federal Ministry of Education and Research and the Conference of the Ministers of Education and Cultural Affairs of Germany) has not yet published its own validation methods for non-formally and informally acquired competences, which is why allocations to existing DQR levels are not yet possible.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Other important issues regarding the topic of the report

For SMEs in particular, a certification of skills is relevant when dealing with large corporations in B2B transactions. These corporations increasingly require standard certifications to ensure that all information security and privacy requirements are met. Accordingly, SMEs in particular need employees with special knowledge because they have to take care of maintaining IT security themselves. The legal regulations for SMEs are less complex than e.g. for sock corporations, but they must avoid high training costs due to a lack of resources.

Having said this, the classification at DQR level 4, which people can gain after several years of professional experience, is only of limited use. If the respective persons have already worked in their profession for several years, a classification on a higher level would be desirable.

The research showed that for jobs in the field of information security or data protection, a successfully completed university degree is usually a prerequisite. It is therefore necessary to adapt the learning content of an IT continuing education course to that of the Master's programme. However, it is questionable whether studying is always necessary for the qualifications sought or whether a qualification at DQR level 6 or 7 would also be sufficient.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6. Executive Summary and Resume

The corporate landscape in Germany is confronted with a large demand for IT security specialists at present and a further increase in demand in the near future. Due to the legal situation, information and data security in companies is of considerable importance and skilled workers are urgently needed. The main demand is for experts at operational and strategic level, usually in conjunction with a (presumed) university degree. These experts should not only have technical know-how, but also be familiar with the legal framework.

The requirements for IT security experts are therefore high. In addition to knowledge of the DSGVO (or BDSG-new) regulation, IT security experts need to know about the industry-specific legal situation of information security, especially if their company is active in the field of critical infrastructures.

The increasing demand for IT security experts on the part of companies is thus associated with a high requirement profile, which makes it more difficult to fill a new position than in hardly any other industry. Further education and training of employees therefore represent an important opportunity for companies to close this competence gap. On the employees' side, the possibility of validating their informal knowledge is gaining importance as they can communicate their skills more credibly.

The certification of knowledge and competences in the areas of information security and data protection is carried out by a large number of providers, but the learning content and the examination certificate are not standardised. That means there is a lack of clarity to the significance of a certificate outside the company for which it was acquired. However, it is possible to participate in a further training of the IHK to become an IT specialist by proving work experience, whereby a degree with DQR level 5 is obtained and participation in further certifications (DQR 6 and 7) is made possible. With regard to the validation of non-formally acquired competences, the IHK equates four years of work experience with a formally acquired qualification at EQR level 4, which gives professionals with informally acquired skills a good chance of entering the IHK's validated IT training programme.

In addition, the increased use of development centers offers an opportunity to determine the level of knowledge more precisely and, if necessary, to support the further training of IT specialists through targeted measures. The BSI also offers a certification procedure, which takes about 3 years. The competencies of the applicant are monitored during this time and if these competencies are maintained and expanded, a certificate is issued after the 3-year period. Other validation possibilities for informal competences are offered, but are only partially checked by public authorities and therefore are only to a limited extent helpful for applicants.

In conclusion, it can be deduced from the current situation that most training pathways take place at DQR levels 5-7 and validation of DQR level 4 usually only includes admission requirements such as relevant work experience. There is therefore a gap for the validation of informally acquired competences at higher levels. In Germany, although there are possibilities for validating informal competences, it is questionable to what extent these are recognised as certifications by companies. There is a lack of an official recognition of informal competences, through which the skills of the applicants are presented in a manner acceptable to companies, so that suitable candidates can be selected for the respective job. In particular, the validation of very specific knowledge required for information security and data protection is still scarce.

Specific offers for SMEs regarding informally acquired competences cannot be found according to the current state of research.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Annex:

Table 7: List of trainings and apprenticeships
Source: Own presentation

Anbieter	Titel	Link
IHK	Apprenticeship as information technology officer (DQR 4)	https://berufenet.arbeitsagentur.de/berufenet/faces/index;BERUFENETJSESSIONID=i4UuIJkFWa4sOgLJLuRPFK2-UICFQleQCGV6XaNUnoy0s8cTGEJb!1571221991?path=null/suchergebnisse/kurzbeschreibung&dkz=7795
IHK	Apprenticeship IT-System-electronics technician (DQR 4)	https://berufenet.arbeitsagentur.de/berufenet/faces/index?path=null/suchergebnisse/kurzbeschreibung&dkz=2927&_afrLoop=1195389263869631&_afrWindowMode=0&_afrWindowId=null&_adf.ctrl-state=zqxrrojrv_74
IHK	Training White Hacker	https://www.bayreuth.ihk.de/upload_ihk_alless01/IHK_Bildungskatalog_2018_2_439350.pdf; S. 37
IHK	Training: Date protection in the personnel area	https://www.bayreuth.ihk.de/upload_ihk_alless01/IHK_Bildungskatalog_2018_2_439350.pdf; S. 105
IHK	Training: Data protection officer in the company	https://www.bayreuth.ihk.de/upload_ihk_alless01/IHK_Bildungskatalog_2018_2_439350.pdf; S. 125
See below: BSI, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/SchulungandererAnbieter/schulungandereranbieter_node.html		
Bitkom	Certificate Course for the Introduction of an Information Security Management System (ISMS)	https://www.bitkom-akademie.de/sites/default/files/BA%20-%20ISMS%20&%20BSI-Grundschutz-Standards%20-

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

		%20Ausbildung%20zum%20Information%20Security%20Officer.pdf
Bechtle	Basic IT Protection with I-DOIT VIVA Training	https://training.bechtle.com/kurse/EDU700014_IT-Grundschutz+mit+I-DOIT+VIVA
Bristol Group	Certification as Information Security Officer ITSIBE / CISO	https://www.bristol.de/workshops/zertifizierung-zum-informations-sicherheitsbeauftragten-itsibe-ciso-01-04/
TÜV	Basic IT Protection expert	https://www.tuev-nord.de/de/weiterbildung/seminare/it-grundschutz-experte-tuev-a/
TÜV Nord	Data protection officer according to DSGVO and BDSG-new	https://www.tuev-nord.de/de/weiterbildung/seminare/datenschutzbeauftragter-tuev-a/
TÜV Nord	Data Protection – Cloud Computing	https://akademie.tuv.com/page/cloud-computing?wt_ga=43769757340_264437767905&wt_kw=b_43769757340_cloud%20schulung&gclid=EAIaIQobChMIpMnBssbe3wIVRaWaCh32GgT9EAAYASAAEgLbSvD_BwE
TÜV Nord	Data Protection in Marketing and advertising measures	https://www.tuev-sued.de/akademie-de/seminare-management/datenschutz/1117018#
GDD e.V.	Data Protection Officer	https://www.gdd.de/seminare/basis-schulungen
Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG	Training as IT Security Officer (ITSiBe)/ Information Security Officer (ISO) according to ISO/IEC 27001 and BSI basic IT protection	

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	Training as BSI basic IT protection expert according to BSI basic IT protection Compendium and BSI Standards Training as Business Continuity Manager according to ISO 22301 and BSI IT-Grundschutz Training as qualified IT risk manager according to ISO 31000 and ONR 49003	

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

BayLDA (2016): EU-Datenschutz-Grundverordnung (DS-GVO), S. 1–2. Online verfügbar unter https://www.lda.bayern.de/media/baylda_ds-gvo_2_certification.pdf, zuletzt geprüft am 04.01.2019.

Berg, Achim (2017): Der Arbeitsmarkt für IT-Fachkräfte. Hg. v. bitkom. Berlin. Online verfügbar unter https://www.bitkom.org/sites/default/files/pdf/Presse/Anhaenge-an-PIs/2017/11-November/Bitkom-Charts-IT-Fachkraefte-07-11-2017-final.pdf, zuletzt geprüft am 04.01.2019.

Blindert, Ute (2018): Heiß begehrt: IT-Security-Experten. DEKRA Arbeitsmarktreport 2018. Hg. v. karriereletter. Online verfügbar unter https://www.karriereletter.de/heiss-begehrt-it-security-experten-dekra-arbeitsmarkt-report-2018/, zuletzt aktualisiert am 17.07.2018, zuletzt geprüft am 04.01.2019.

Brookson, Charles; Cadzow, Scott; Eckmaier, Ralph; Eschweiler, Jörg; Gerber, Berthold; Guarino, Alessandro et al. (2015): Definition of cybersecurity. Gaps and overlaps in standardisation. Heraklion: ENISA.

Bundesamt für Sicherheit in der Informationstechnik (2012): Leitfaden Informationssicherheit. IT Grundschutz kompakt (BSI-Bro12/311), S. 1–91. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile&v=3, zuletzt geprüft am 04.01.2019.

Bundesamt für Sicherheit in der Informationstechnik (2016): Das IT-Sicherheitsgesetz. Kritische Infrastrukturen schützen. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Bonn (19). Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=7, zuletzt geprüft am 13.01.2019.

Bundesamt für Sicherheit in der Informationstechnik (2017): Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen, S. 1–14. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/VB-Personen.pdf?__blob=publicationFile&v=4, zuletzt geprüft am 04.01.2019.

Bundesamt für Sicherheit in der Informationstechnik (2018a): BSI - Kompetenzfeststellung und Zertifizierung von Personen. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Personenzertifizierung/personen_node.html, zuletzt geprüft am 04.01.2019.

Bundesamt für Sicherheit in der Informationstechnik (2018b): BSI - Schulungen anderer Anbieter. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/SchulungandererAnbieter/schulungandereranbieter_node.html, zuletzt geprüft am 12.01.2019.

Bundesamt für Sicherheit in der Informationstechnik (2018c): ISO 27001 Zertifizierung auf Basis von IT-Grundschutz. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html, zuletzt geprüft am 04.01.2019.

Bundesamt für Sicherheit in der Informationstechnik (2019a): BSI - Schulungen anderer Anbieter. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/SchulungandererAnbieter/schulungandereranbieter_node.html, zuletzt geprüft am 04.01.2019.

Bundesamt für Sicherheit in der Informationstechnik (2019b): Gesetz zur Umsetzung der NIS-Richtlinie. Mehr Aufgaben und Befugnisse für das BSI. Hg. v. Bundesamt für Sicherheit in der

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html, zuletzt geprüft am 13.01.2019.

Bundesnetzagentur (2015): IT-Sicherheitskatalog gemäß §11 Absatz 1a Energiewirtschaftsgesetz, S. 1–16. Online verfügbar unter https://www.dekra-certification.de/media/10-pdf-downloads/it-sicherheitskatalog-08-2015.pdf, zuletzt geprüft am 04.01.2019.

Bundesnetzagentur (2019): IT-Sicherheit im Energiesektor. Hg. v. Bundesnetzagentur. Online verfügbar unter https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheit.html, zuletzt geprüft am 04.01.2019.

Datenschutz.org (2018): BDSG-neu: Neues Bundesdatenschutzgesetz | Datenschutz 2019. Hg. v. Datenschutz.org. Online verfügbar unter https://www.datenschutz.org/bdsg-neu/, zuletzt aktualisiert am 04.01.2019, zuletzt geprüft am 04.01.2019.

DIHK (2016): Deutscher Qualifikationsrahmen (DQR). IHK-Fortbildungsabschlüsse auf Hochschul-Niveau. Hg. v. DIHK. Online verfügbar unter http://ihk-bic.de/ihk-praxisstudium/deutscher-qualifikationsrahmen-dqr/, zuletzt geprüft am 12.01.2019.

DQR (2014): Liste der zugeordneten Qualifikationen. Hg. v. DQR. Online verfügbar unter https://www.dqr.de/media/content/Liste_der_zugeordneten_Qualifikationen_31_03_2014_bf.pdf, zuletzt geprüft am 12.01.2019.

GDD (2018): Schulungen bei der GDD — GDD e.V. Das Ausbildungskonzept der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. Online verfügbar unter https://www.gdd.de/seminare, zuletzt geprüft am 04.01.2019.

IHK (2018a): 03_LK BAR | IHK-Projektgesellschaft mbH. Lotsendienst für Existenzgründer Landkreis Barnim. Hg. v. IHK. Ostbrandenburg. Online verfügbar unter https://www.ihk-projekt.de/unsere-projekte/national/02-lotsendienst-ff-los-um-und-bar/03-lk-bar/?L=0,https://www.ihk-bildungszentrum-cottbus.de/details.jsp?ver_id=2330, zuletzt geprüft am 04.01.2019.

IHK (2018b): IHK Bayreuth-Bildungskatalog 2018.2. Die Weiterbildung für Oberfranken (2), S. 1–156. Online verfügbar unter https://www.bayreuth.ihk.de/upload_ihk_alless01/IHK_Bildungskatalog_2018_2_439350.pdf, zuletzt geprüft am 04.01.2019.

IHK (2018c): Sachliche und zeitliche Gliederung der Berufsausbildung. Anlage zum Berufsausbildungsvertrag, S. 1–17, zuletzt geprüft am 04.01.2019.

IHK (2018d): Überblick - Weiterbildungs-Informations-System (WIS). Hg. v. IHK. Online verfügbar unter https://wis.ihk.de/informationen/spezialthemen/it-weiterbildung/ueberblick.html, zuletzt geprüft am 12.01.2019.

IHK (2019): Das IHK-Netzwerk - IHK. Hg. v. IHK. Online verfügbar unter https://www.ihk.de/wir-uber-uns, zuletzt geprüft am 12.01.2019.

IHK Bayreuth (2018): IHK Bayreuth-Bildungskatalog 2018.2. Die Weiterbildung für Oberfranken, S. 1–156. Online verfügbar unter https://www.bayreuth.ihk.de/upload_ihk_alless01/IHK_Bildungskatalog_2018_2_439350.pdf, zuletzt geprüft am 12.01.2019.

Klebl, Ulfried; Nerdinger, Friedemann W. (2010): Kompetenzentwicklung durch Development-Center. In: *Zeitschrift für Arbeits- und Organisationspsychologie A&O* 54 (2), S. 57–67. DOI: 10.1026/0932-4089/a000012.

Landesbeauftragte für Datenschutz und Informationssicherheit Nordrhein-Westfalen (2019): Wann müssen Datenschutzbeauftragte bestellt werden? Hg. v. Landesbeauftragte für

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Datenschutz und Informationssicherheit Nordrhein-Westfalen. Online verfügbar unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Betriebliche_Datenschutzbeauftragte/Inhalt/FAQ/Bestellung_DSB.php, zuletzt geprüft am 12.01.2019.

Mesmer, Alexandra (2018): Softwareentwicker, Security-Experten und Berater besonders begehrt. Hg. v. Computerwoche. Online verfügbar unter https://www.computerwoche.de/a/softwareentwickler-security-experten-und-berater-sind-besonders-begehrt,3545136, zuletzt aktualisiert am 11.06.2018, zuletzt geprüft am 04.01.2019.

Whitten, Dwayne (2008): The Chief Information Security Officer. An Analysis of the Skills Required for Success. In: *Journal of Computer Information Systems* 48 (3), S. 15–19. DOI: 10.1080/08874417.2008.11646017.

Wikipedia (2019a): Information privacy. Hg. v. Wikipedia. Online verfügbar unter https://en.wikipedia.org/w/index.php?oldid=873938916, zuletzt aktualisiert am 31.12.2018, zuletzt geprüft am 04.01.2019.

Wikipedia (2019b): Information security. Hg. v. Wikipedia. Online verfügbar unter https://en.wikipedia.org/w/index.php?oldid=876029889, zuletzt aktualisiert am 02.01.2019, zuletzt geprüft am 04.01.2019.

Funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.