SME Guide to Cyber Security - Focus on the Baltics, Germany, Poland and the Czech Republic

A part of the ISALIP Seeding Materials

Co-funded by the European Union

Co-funded by
the European Union

This document was produced as part of the Erasmus+ project.

"Information Security Awareness, Literacy and Privacy – ISALIP"

Project Partners:

Betriebswirtschaftliches Forschungszentrum für Fragen der mittelständischen Wirtschaft e. V. an der Universität Bayreuth
(Business Research Center for Small and Medium-Sized Enterprises e. V. at the University of Bayreuth),
Germany
https://www.bfm-bayreuth.de

eCampus-Lausitz e. V.,
Germany
https://www.ecampus-lausitz.de

MYKOLO ROMERIO UNIVERSITETAS,
Lithuania
https://www.mruni.eu

This document was produced as part of the ERASMUS+ project "Information Security Awareness, Literacy and Privacy – ISALIP", Project ID: 2021-2-DE02-KA210-ADU-000051308

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

1 Introduction

This output document was developed in the ERASMUS+ project ISALIP ("Information Security Awareness, Literacy and Privacy") as part of the ISALIP Seeding Materials and is intended to give a practical tool for SME in the field of information security.

In the initial activity of the project focused on international supply chains against the background of information security. Data interchange in international supply chains is highly vulnerable, and incidents reduce the availability of goods, resources and commodities. Relating to this fact it is important to understand that next to digital challenges also regulative challenges exist, which hinder SMEs to act cross-country.

Cyber security regulations within the European Union (EU) can present both challenges and opportunities for businesses looking to enter EU markets. While these regulations are designed to enhance cyber security and protect data, they can also introduce complexity and compliance requirements that businesses must navigate. Also, Small- and Medium-sized Enterprises (SMEs) face a unique set of cyber security challenges due to their limited resources, expertise, and budget constraints.

With the aim of providing practical support for SMEs in this 1st ISALIP Seeding Material, the key challenges for SMEs in the area of cyber security were identified. These were supplemented by the challenges of a potential market entry in another EU country and operating securely within an international supply chain in the context of a complex European regulatory environment.

In order to counter these challenges, the advantages of European domestic market action in the context of cyber security are then highlighted and a guide for SMEs is presented.

To make it easier for SMEs to put this advice into practice, the basic EU regulations, frameworks and players in the individual countries are presented in the following. The originally planned screening of country-specific regulations has been shortened and supplemented by an outlook on the upcoming European harmonizations NIS2 and CRA.

Nevertheless, the document contains a detailed analysis of all the key players in the Baltic States (Lithuania, Latvia, Estonia) and the European Region Spree-Neisse-Bober (Germany, Poland and Czech Republic). An overview with links to the most important sources of information in the individual countries seemed to the project team to have the most practical value.

As a result, this document should give an overview over facets in low-level information security frameworks and living realities.

The analysis focused in particular on the partner countries Germany and Lithuania. As a result of the analysis of regulatory barriers entering the market of the other EU country it has to be stated that even though the ISO 27001 standard provides an international basis for an information security framework, and this also applies to Europe, the national interpretations of the European requirements are not congruent.

The analysis revealed a strong link between the Lithuanian regulations and ISO 27001, but in Germany a lot of specific regulations could be found. A special focus was on the "IT-Grundschutz" which is the standard for the German public institutions and recommended for every other organization (also firms and SME). The Lithuanian and German regulations are structured differently and, in some cases, elaborated differently. The analysis in this way showed an important need for SME from both countries: In order to overcome the knowledge gap about the information security regulations of another country, a comparison of both regulations brings great added value, but also has to contend with the language barrier. To overcome this challenge, the project team translated the "Mapping table mapping ISO/IEC 27001 and ISO/IEC 27002 to IT baseline protection" (Bundesamt für Sicherheit in der Informationstechnik (BSI), 4th edition 2021) and thus created a result with a high practical added value for Lithuanian SME (see ISALIP Seeding Materials).

2 Table of Contents

3 Challenges for Small and Medium-sized Enterprises in a European Environment

3.1 Key Cyber Security Challenges of SME

Small and medium-sized enterprises (SMEs) face a number of unique cyber security challenges due to their limited resources, expertise and budget. These challenges can make them attractive targets for cyberattacks.

Key cyber security challenges:

Limited Resources and Budgets:

- SMEs often have limited financial resources to invest in cyber security measures, making it challenging to implement comprehensive security solutions. They often face a resource allocation dilemma allocating limited resources between business growth and cyber security, which can lead to trade-offs in security investments.

Lack of In-House Expertise:

- Many SMEs do not have dedicated cyber security professionals on staff, which can affect their ability to effectively manage and respond to security threats.

Inadequate Security Awareness:

- Employees in SMEs may not be adequately trained in cyber security best practices, making them more susceptible to social engineering attacks and phishing scams.

Outdated Software and Hardware:

- SMEs may rely on older software and hardware that is no longer supported or updated, leaving them vulnerable to known vulnerabilities.

Third-Party Risks:

- Working with multiple third-party vendors can pose security risks if these partners do not have robust cybersecurity practices.

Data Protection and Privacy Compliance:

- Compliance with data protection regulations such as the GDPR can be challenging for SMEs, especially if they lack the necessary resources.

Limited Incident Response Capability:

- SMEs may struggle to develop and maintain an effective incident response plan, making it difficult to mitigate the impact of a cyberattack or data breach.

Supply Chain & Third-Party Vulnerabilities:

- SMEs may not have visibility into the cyber security practices of their suppliers and may inadvertently introduce vulnerabilities into their own systems through supply chain connections. They also have a lack of resources to thoroughly assess the security of third-party vendors or software solutions they use, potentially exposing them to supply chain attacks.

Ransomware Threats:

- Ransomware attacks can be particularly devastating for SMEs, as they may not have robust backup and recovery systems in place.

Mobile and Remote Work Security:

- With the rise of remote work, securing mobile devices and remote access to company resources becomes a challenge.

Cybersecurity Awareness and Training:

- Employees are often targeted by phishing emails and social engineering attacks, which can lead to data breaches or financial losses. Training employees on cyber security best practices may be overlooked due to time and resource constraints, leaving the organization vulnerable to human error.

3.2 SME Challenges and Opportunities in the European Cyber Security Regulation Environment

Cyber security regulations within the European Union pose major challenges for SMEs looking to enter EU markets. While these regulations are designed to enhance cyber security and protect data, they can also introduce complexity and compliance requirements that businesses must navigate.

Challenges:

Complex Regulatory Landscape:

- The EU consists of multiple member states, each with its own cyber security regulations and data protection laws. This complexity can be challenging for businesses to understand and comply with, especially if they plan to operate in multiple EU countries.

Compliance Costs:

- Meeting the requirements of various EU cyber security regulations and data protection laws can be costly in terms of both time and resources. This can pose a barrier to entry for smaller businesses with limited budgets.

Data Localization Requirements:

- Some EU member states may have data localization requirements that mandate the storage and processing of data within their borders. This can impact the flexibility and scalability of businesses' operations.

Varying Penalties:

- Different EU member states may impose varying penalties for non-compliance with cyber security regulations, which can make it challenging for businesses to assess the potential risks and consequences.

Constant Regulatory Changes:

- EU cyber security regulations are subject to updates and revisions. Businesses must stay informed about changes to ensure ongoing compliance.

3.3 SME Challenges in International Supply Chains

The establishment of international supply chains within the European Union (EU) entails additional requirements that go beyond the “simple” case of entering another European market. European and country-specific regulations can have implications for supply chain management, data handling, and overall security.

Challenges:

Data Transfer and Localization:

- EU cyber security and data protection regulations can impose restrictions on the transfer of data outside the EU. Supply chain partners may need to implement appropriate safeguards to ensure data compliance, and data localization requirements in some member states may complicate data storage and processing.

Data Breach Reporting:

- GDPR requires the reporting of data breaches within 72 hours. This can be challenging for international supply chains, as timely reporting across borders can be complex. There may be variations in how these incidents are reported or handled at the national level

Third-Party Risk Management:

- Supply chains often involve multiple third-party vendors and partners. Ensuring that all partners adhere to cyber security and data protection standards can be a challenge.

Compliance Costs:

- Complying with EU cyber security and data protection regulations can be costly, especially for small and medium-sized enterprises (SMEs) with limited resources.

Supply Chain Resilience:

- Ensuring the cyber security and resilience of the supply chain against cyber threats is crucial. Weak links in the supply chain can expose the entire operation to risk.

Regulatory Variations:

- While there is a common framework in the EU, there can still be variations in cyber security and data protection regulations among member states. Businesses need to be aware of these differences and ensure compliance with local laws. For example, each EU member state has its own national Data Protection Authority responsible for enforcing data protection regulations. While GDPR provides a common framework, national DPAs may have specific interpretations or guidance that can vary.

Sector-Specific Regulations:

- Certain industries, such as finance or healthcare, may have sector-specific cybersecurity and data protection regulations that add additional requirements on top of GDPR.

Cybersecurity Certification:

- While the EU Cybersecurity Act provides an EU-wide framework for certification of ICT products and services, countries may have their own certification bodies or requirements.

Language Requirements:

- Some countries may have language-specific requirements for data protection documentation, such as privacy notices or consent forms, which need to be available in the official language(s) of the country. Legal documents, including contracts and agreements related to cyber security, may need to be available in the official language(s) of the country.

3.4 SME Guide – Overcome the challenges and seize the opportunities

To address the Key Cyber Security Challenges of SME, SMEs should consider:

Implementation of a risk-based approach to cyber security:

- Implementation of a risk-based approach to cyber security, focusing on the most critical assets and threats.

Use external support:

- It is recommended - due to a lack of resources – to use external support through managed security service providers (MSSPs) or collaborating with industry groups and government agencies that offer cyber security guidance and resources tailored to SME.

Although the EU regulatory environment in cyber security is a challenge for SME, it also offers opportunities:

Uniform Data Protection Standards:

- The EU's General Data Protection Regulation (GDPR) provides a unified set of data protection standards across member states. Businesses that comply with GDPR can benefit from a consistent framework for handling personal data throughout the EU. This standardization can simplify data handling and compliance for international supply chain operations within the EU.

Cyber security Standards:

- While there may be variations in specific cyber security regulations among EU member states, the EU is working to harmonize cyber security standards and practices across the bloc. This can provide a level of consistency and predictability for businesses. Complying with these regulations can help businesses build trust with customers and partners.

Market Access:

- Compliance with EU cyber security regulations is often a prerequisite for accessing EU markets. By meeting these requirements, businesses can access a market of over 400 million consumers.

Quality Infrastructure:

- The EU generally has well-developed infrastructure, including transportation, logistics, and communication networks, which can facilitate international supply chain operations.

Competitive Advantage:

- Businesses that prioritize cyber security and data protection can gain a competitive advantage by demonstrating their commitment to security and privacy, which can be a selling point for customers and partners.

International Alignment:

- Compliance with EU regulations can align a business with global best practices in cyber security and data protection, which can be beneficial when conducting business internationally.

To successfully navigate the challenges posed by different cyber security regulations within the EU and to successfully establish international supply chains within the EU SME should consider the following:

Seize the opportunities:

- While EU cyber security regulations may introduce complexity, compliance is often a necessary step to access the European market and can be a competitive advantage in an increasingly data-driven and security-conscious business environment.

Access specific regulations:

- Conduct a thorough assessment of the specific cyber security and data protection regulations that apply to their industry and operations in each EU member state they plan to enter.

Expand your risk management to include the horizon of the supply chain:

- Conduct a thorough risk assessment to identify cyber security and data protection risks within the supply chain.

Develop cyber security and compliance strategy:

- Develop a robust compliance strategy that accounts for both the GDPR and any additional country-specific regulations. A robust cyber security strategy aligns with EU regulations and includes contractual agreements with supply chain partners.

Invest in cyber security:

- Invest in cyber security measures, such as encryption, access controls, and incident response plans, to protect sensitive data and operations.

Use external support on local and European level:

- Consider seeking legal counsel or consulting with cyber security experts to ensure full compliance. Think about the language barrier and use local experts.

Stay informed:

- Stay informed about changes in EU cybersecurity regulations and adapt supply chain practices accordingly.

Consider cyber security as a key part of your business model:

- Prioritize cyber security and data protection as a fundamental aspect of business operations to build trust with customers and partners.

Overall, while there are challenges associated with navigating EU cyber security regulations, careful planning and investment in cyber security measures can help businesses establish and maintain secure and compliant international supply chains within the EU.

To make it easier for SMEs to put this advice into practice, the basic EU regulations, frameworks and players in the individual countries are presented below.

4 European regulations in cyber security and data protection

In EUR-Lex, the official database of EU legal documents, we have about 74 matches for searching “Cyber Security” only in 2022. Furthermore, cyber security is a requirement that is reflected in the majority of European regulatory projects – from overarching policies over economic and market aspects to education and much more.

In order to describe the European regulatory landscape in a meaningful way, it would first be necessary to digress into various terms, for example to differentiate between the meaning of “regulations”, “directives”, “decisions”, “delegated” and “implemented acts”, or “recommendations” and “options” or the “councils conclusions” and “resolutions”.

In the end, the regulatory environment is highly complex and cannot be fully described within the scope of this document (the ISALIP project). The focus is therefore on a brief introduction and presentation of relevant information providers.

For instance, in 2004, the EU established the European Network and Information Security Agency (ENISA; now Agency for Cyber security) and in 2013 the first EU Cyber security Strategy, “An Open, Safe and Secure Cyberspace” was published. In 2016, EU Member States and the European Parliament adopted the EU’s first horizontal cyber security legislation, the first Network and Information Security (NIS) Directive.

Here are some notable examples of EU cyber security and data protection regulations:

General Data Protection Regulation (GDPR):

- GDPR is one of the most significant and well-known regulations in the EU. It governs the processing of personal data and imposes strict requirements on organizations that handle such data. Compliance with GDPR is essential for businesses that collect or process personal data of EU citizens.

Network and Information Security Directive (NIS Directive):

- The NIS Directive aims to enhance the overall cyber security posture of critical infrastructure operators and digital service providers in the EU. It mandates reporting of certain cyber security incidents and requires entities to implement cyber security measures.

ePrivacy Regulation (ePR):

- The ePrivacy Regulation, once finalized and enacted, will govern the privacy and confidentiality of electronic communications, including electronic marketing and the use of cookies. It will complement GDPR and impact online businesses and advertisers.

Payment Services Directive 2 (PSD2):

- While primarily focused on the financial sector, PSD2 introduces strong authentication requirements for online payments, enhancing security for digital financial transactions.

Cyber Security Act:

- The Cyber Security Act establishes an EU framework for certification of information and communication technology (ICT) products, services, and processes. It aims to improve the cyber security of products and services used in critical sectors.

Directive on Security of Network and Information Systems (SNIS Directive):

- This directive complements the NIS Directive and establishes security requirements for operators of essential services in sectors such as energy, transport, banking, and healthcare.

eIDAS Regulation:

- The eIDAS Regulation facilitates the use of electronic identification (eID) and electronic trust services across borders within the EU. It has implications for the security and authentication of electronic transactions.

EU Cybersecurity Certification Framework:

- Under this framework, the EU has developed specific certification schemes for ICT products, services, and processes. Compliance with these schemes may be required for certain products and services.

Schrems II Ruling:

- While not a regulation, the Schrems II ruling by the European Court of Justice has implications for international data transfers. It clarified the requirements for ensuring that data transfers outside the EU provide an equivalent level of data protection as within the EU.

These regulations aim to enhance data protection, privacy, and cyber security within the EU. While they provide a strong framework for safeguarding digital assets and individuals' rights, they also present compliance challenges, particularly for businesses with international operations or supply chains. Organizations doing business in the EU or with EU citizens should carefully assess their obligations under these regulations and take appropriate measures to ensure compliance.

4.1 Upcoming Harmonization in European Regulations

The European harmonization projects NIS2 and CIS promote competition and strengthens the EU internal market as a whole. Companies can now offer their products and services more easily in different Member States, leading to greater choice for consumers and businesses while increasing innovation within the EU.

Due to the forthcoming NIS2 and CRA regulations, it seems no longer necessary to consider the national particularities in the European regions, as these will be reformed in the medium term by NIS2 and CRA and adapted to a largely uniform level.

4.1.1 NIS2 - Network and Information Systems Directive

The NIS2 (Network and Information Systems) Directive represents a significant step towards a unified and improved information security landscape in the European Union. This regulation, which replaces the original NIS Directive from 2016, aims to strengthen cyber security in the member states while creating harmonized legislation that affects the entire European single market.

The NIS2 directive leads to a positive standardization of national legislation on information security. Before NIS2, many EU countries had different regulations and standards, which led to a patchwork of regulations. Germany, in particular, should be mentioned with its BSI IT baseline protection („IT-Grundschutz“), which is compatible with ISO 27001 but is an example of a special national approach. This fragmentation presented companies with considerable challenges, especially if they wanted to operate in several EU countries. With the introduction of NIS2, a uniform framework is being created that prescribes minimum cyber security requirements in all member states.

This harmonization of regulations now makes it easier for companies to implement their safety measures in different countries without having to take local peculiarities into account each time. This reduces the administrative burden and costs associated with complying with different national regulations. At the same time, a higher level of safety is guaranteed as all member states are aligned to the same standards.

4.1.2 CRA – EU Cyber Resilience Act

In connection with the EU Cyber Resilience Act, EU-wide information security standards for products are being defined for the first time. This means that all products that are to be imported into the EU internal market must comply with certain cyber security standards. Cyber security thus becomes an integral part of the declaration of conformity required for market access.

This step is revolutionary as it ensures that all products sold in the EU have a high level of cyber security. This not only protects consumers, but also boosts confidence in the Digital Single Market. Companies must now ensure that their products comply with the new security requirements, leading to an overall increase in the level of security across the single market.

4.2 Frameworks

The task of information security management is to systematically secure an information-processing network. The selection and implementation of security standards is one of the tasks of security management. International standards exist for evaluating and certifying the security of computer systems; the most common standard in the EU (and internationally) is ISO27001. In the respective areas, various "best practice" methods have been developed, such as ITIL, COBIT, ISO or Basel II.

Ultimately, cyber security frameworks are essential for organizations to develop a structured approach to managing cybersecurity risk and compliance.

In Poland, the Czech Republic, Latvia, Lithuania, Estonia and Germany, organizations often refer to well-known international cyber security frameworks and standards like:

1. NIST Cybersecurity Framework:

- NIST Cybersecurity Framework is a set of guidelines for mitigating organizational cybersecurity risks published by the US National Institute of Standards and Technology based on existing standards, guidelines and practices.
- The principles of the NIST framework are applied in the countries under consideration, and the principles are adapted in local cyber security standards and regulations. In particular organizations with international business relationships use appropriate references. In Poland, we can speak of an even closer bond - the NIST Cybersecurity Framework is often cited as a reference for best practices in the field of cyber security.

2. ISO 27001 (Information Security Management System - ISMS):

- ISO 27001 is a widely adopted international standard for information security management. Organizations in these countries often use it to establish, implement, maintain, and continually improve their information security management systems.
- ISO 27001 is commonly implemented in both the public and private sectors.

3. GDPR (General Data Protection Regulation):

- GDPR is a European Union regulation that governs data protection and privacy. While not a cyber security framework per se, it sets strict requirements for the protection of personal data, and organizations in these countries must adhere to GDPR when handling data.

- Compliance with GDPR often involves cyber security measures and practices.

4. CIS Controls (Critical Security Controls):

The CIS Critical Security Controls (CIS Controls) are a prioritized list of protective measures to ward off the most common cyberattacks on IT systems.

- Depending on the size and resources of the company, these individual measures are divided into three priority groups:
    - IG1: Measures for micro-enterprises
    - IG2: Measures for SMEs and
    - IG3: Measures for large companies with their own IT security team.

5. Local/National Cybersecurity Frameworks:

- In addition to international frameworks, some countries may have their own national or sector-specific cybersecurity frameworks or guidelines. For example:
    - In Poland, the Polish Information Security Management System (Polski System Zarządzania Bezpieczeństwem Informacji - PSZBI) is used.
    - In Germany, the Federal Office for Information Security (BSI) publishes guidance and recommendations for information security.

Organizations in the countries typically select a cyber security framework or standard that aligns with their specific needs, industry, and regulatory requirements. Additionally, they may leverage the guidance provided by national or sector-specific authorities. It's important to note that the choice of a cyber security framework or standard should be based on a comprehensive risk assessment, organizational goals, and the specific regulatory environment in which the organization operates. Additionally, the cyber security landscape is dynamic, so organizations should regularly update their practices to address emerging threats and vulnerabilities.

The analysis revealed a strong link between the Lithuanian regulations and ISO 27001, but in Germany a lot of specific regulations could be found. A special focus was on the "IT-Grundschutz" which is the standard for the German public institutions and recommended for every other organization (also firms and SME). The Lithuanian and German regulations are structured differently and, in some cases, elaborated differently. The analysis in this way showed an important need for SME from both countries: In order to overcome the knowledge gap about the information security regulations of another country, a comparison of both regulations brings great added value, but also has to contend with the language barrier. To overcome this challenge, the project team translated the "Mapping table mapping ISO/IEC 27001 and ISO/IEC 27002 to IT baseline protection" (Bundesamt für Sicherheit in der Informationstechnik (BSI), 4th edition 2021) and thus created a result with a high practical added value for Lithuanian SME (see ISALIP Seeding Materials).

5 Institutions: Aid to overcome the challenges

5.1 Complex Cyber Security Architecture

Cyber security architecture can be divided into four layers. The top level is the international level, with a still manageable complexity. It is made up of actors from the UN and other international actors, such as the OSZE or Interpol. Below this is the European level with e.g. the European Network and Information Security Agency (ENISA). The European level is already characterized by a high degree of complexity, numerous working groups and sector-specific institutions expand the main European institutions, such as the European Commission or the European Council. NATO and its organs can be placed between the two upper levels (or on both) due to their strong European influence. An overview can be found in the following graphic (Figure 1), which corresponds to a partial section of a graphic on the German cybersecurity architecture of the “Stiftung Neue Verantwortung e.V.“ from 2022 (see also the following graphics).

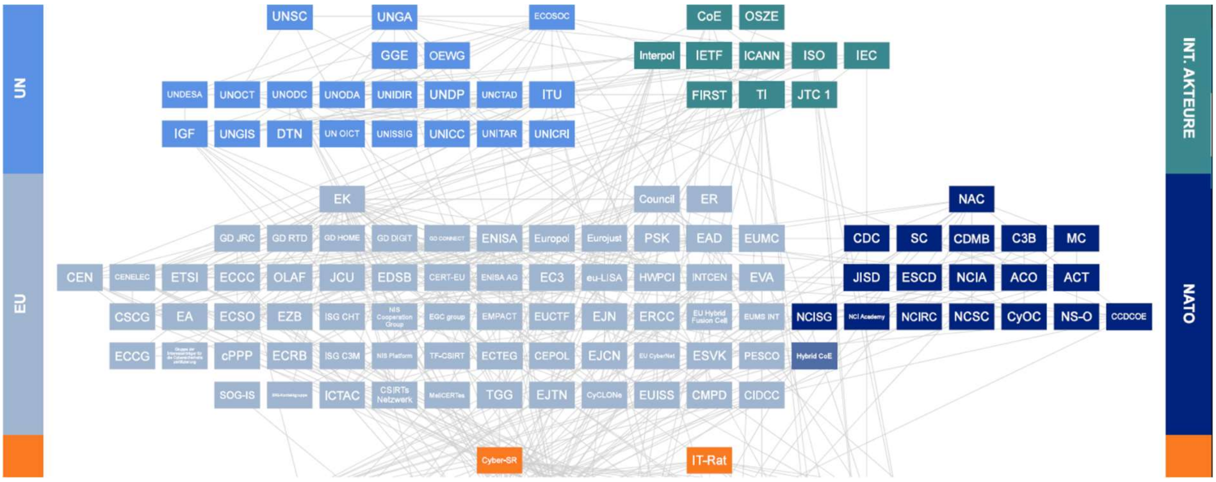

Figure 1: Cyber Security Architecture on International and EU-Level (Herpig, Rupp 2022; Stiftung Neue Verantwortung)

At the national levels, cyber security architecture is comparable in many areas, but there are also significant differences. For example, differences can already be found in the classification of cyber security under the sovereignty of the Ministry of the Interior (as in Germany) or the Ministry of Defense (as in the Baltic States). There are quite comparable institutions in all countries that reflect the official interests of e.g. the police or secret service or serve the certification or provision of official information. As an example, the cyber security architecture of the Federal Republic of Germany is shown below (Figure 2).

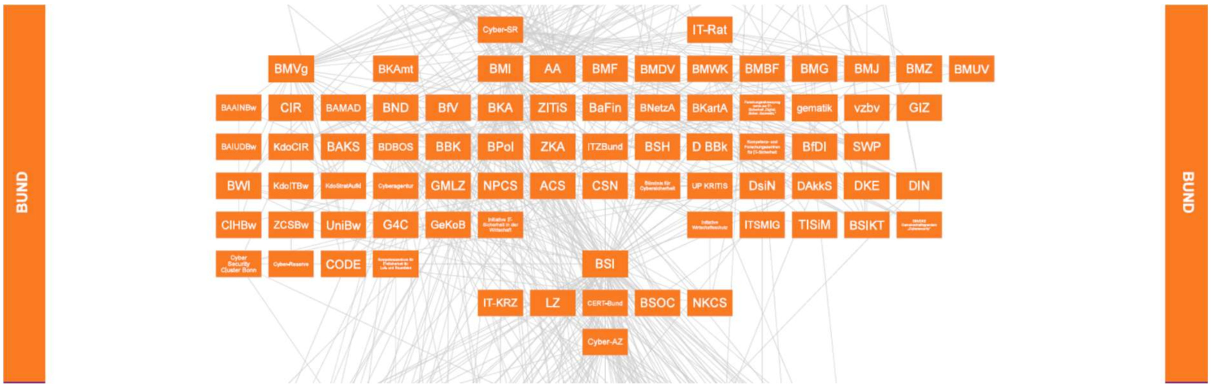

Figure 2: Cyber Security Architecture on national level by the Example of Germany (Herpig, Rupp 2022; Stiftung Neue Verantwortung)

For the Baltic countries and Poland as well as the Czech Republic, comparable structures can be found here, albeit somewhat less complex. In Germany, the strong federalism is another driver of complexity. For each federal state, there are numerous institutions that serve as public contacts in various situations, such as data protection or incident reporting. In addition to the typical state offices for crime or the protection of the constitution, there is also the state commissioner for data protection and numerous other institutions (Figure 3).

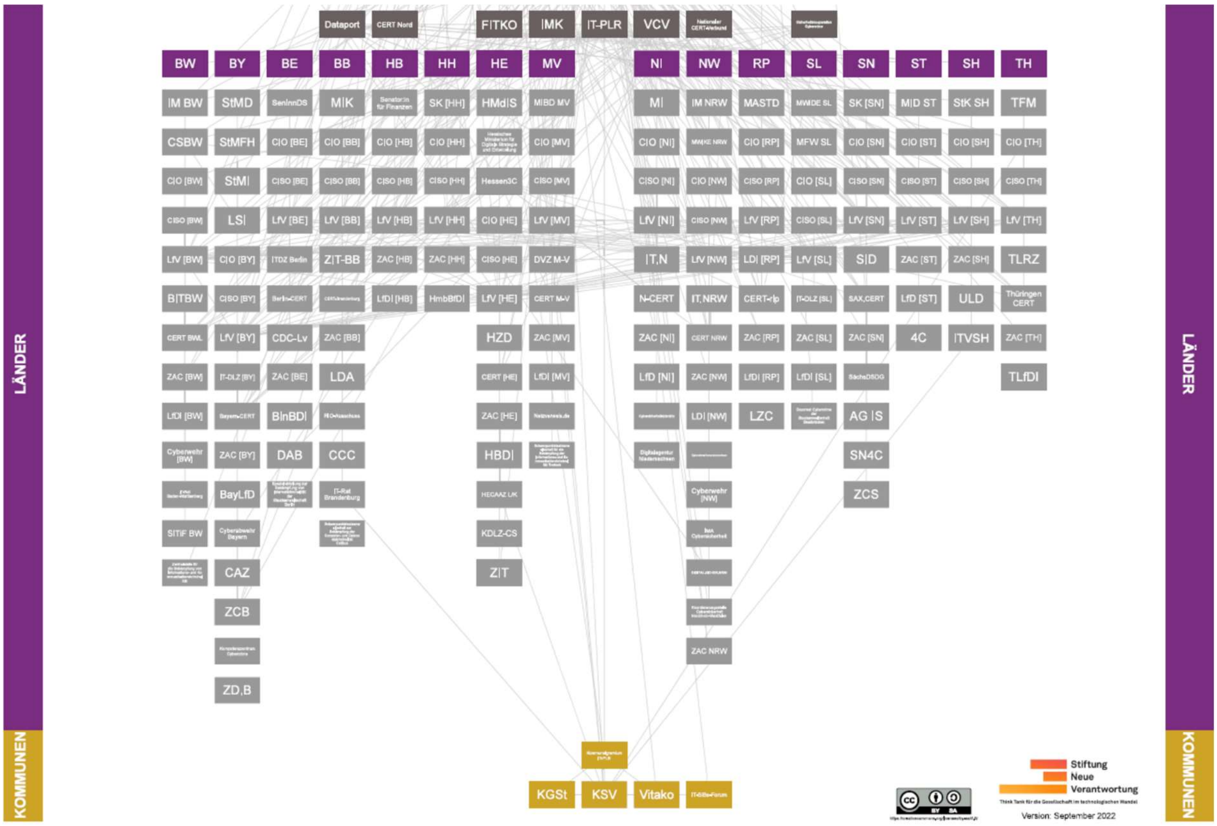

Figure 3: Cyber Security Architecture on at federal state and municipal level by the Example of Germany (Herpig, Rupp 2022; Stiftung Neue Verantwortung)

However, for SMEs that want to provide a service for a municipal provider the key players at the municipal level are relevant too. These include, for example, municipal administrations and municipal IT service providers. A detailed description of the cyber security architecture at the state and municipal level can be found in the following figure.

Overall, a high level of complexity can be observed in an entangled construct of cybersecurity actors within the EU, state, state and municipality. The institutions work together with a high degree of dependence and networking on one level and across levels. From these explanations it is easy to see that we can hardly give an overview of all relevant institutions in the following. We hope to have made a practical selection for SMEs – without being able to make a promise of completeness or topicality in the highly dynamic environment of cyber security.

5.2 Institutions at European and national level

Overall, while cyber security standards can present challenges for SMEs entering a new market, proactive planning, risk assessment, and a commitment to cyber security can help SMEs meet these challenges and ensure a more secure and successful market entry.

In the European Union (EU), there are several institutions, organizations, and agencies that can help enterprises, including Small and Medium-sized Enterprises (SMEs), address the challenges related to cyber security compliance and standards. These entities offer guidance, support, resources, and expertise to assist businesses. Notable institutions and organizations are:

European Union Agency for Cybersecurity (ENISA):

- ENISA is the EU's agency dedicated to promoting and enhancing cybersecurity across Europe. They provide various resources, including guidelines, best practices, and reports, to help organizations improve their cyber security resilience.
  https://www.enisa.europa.eu/

European Cyber Security Organisation (ECSO):

- ECSO is a public-private partnership that aims to support the development of a competitive European cyber security industry. They offer networking opportunities, access to funding, and collaboration with industry experts.
- https://www.ecs-org.eu/

European Commission: Digital Europe Program:

- The Digital Europe Program, part of the European Commission, provides funding opportunities for projects related to digital technologies, including cybersecurity. SMEs can access funding to enhance their cybersecurity capabilities.
  https://digital-strategy.ec.europa.eu/en/policies/digital-europe-programme

European DIGITAL SME Alliance:

- The DIGITAL SME is the largest network of ICT small and medium enterprises (SMEs) in Europe, representing more than 45,000 digital SMEs across the EU. DIGITAL SME works with both legislators and companies to ensure that European legislation is suitable for the market and that resources are available to help SMEs protect themselves. https://www.digitalsme.eu/cybersecurity-privacy/

National Cyber Security Institutions and Organizations:

Many EU member states have their own national cyber security agencies or authorities that offer resources and guidance on cyber security standards and compliance (e.g., in Germany the BSI). In EU member states local and regional chambers of commerce offer support and resources for businesses, including guidance on cybersecurity compliance. Industry associations provide industry-specific guidance and resources on cybersecurity standards and compliance in various industries, such as banking and manufacturing. On a regional and local level business support centers offer workshops, training programs, and consultancy services to help SMEs improve their cyber security practices. Academic institutions and research centers in the EU often conduct research, offer training programs related to cyber security or collaborate with businesses to address cyber security challenges.

When seeking support from these institutions, it is important to assess the specific needs and challenges of your business to find the most appropriate resources and support.

In Poland, the Czech Republic, Latvia, Lithuania, Estonia, and Germany, there are various institutions and organizations that can help businesses, including Small and Medium-sized Enterprises (SMEs), with cyber security-related challenges, standards, and compliance. The cyber security ecosystem in each country involves a range of stakeholders and market participants, including government agencies, businesses, research institutions, and non-governmental organizations.

A selection of relevant stakeholders and actors per country is shown in the following structure:

Government Agencies

The structure of the authorities and public contact points responsible for cyber security and the associated responsibilities is sometimes very complex in the individual countries (especially in the federal system in Germany). A selection is provided here to serve as initial points of contact - also for foreign companies.

Industry Associations and Clusters

Industry associations and clusters play an important role in representing specific interests and answering detailed questions, e.g. for specific industry solutions.

Companies with similar interests network here and comprehensive information is often provided with a high depth of information.

Businesses and Enterprises:

There are large enterprises which dedicated cyber security teams and invest heavily in securing their digital assets. They often work with cyber security vendors, consultants, and service providers.

Cyber security Vendors and Solution Providers:

Numerous cyber security companies, both domestic and international, operate in the countries. They offer a wide range of products and services, including antivirus software, firewall solutions, threat intelligence, and incident response services.

Research and Academic Institution:

Universities and research institutions are actively engaged in cyber security research and development. They collaborate with government agencies and businesses on cyber security projects and provide a talent pipeline for the industry. A small selection of particularly relevant research institutions is presented here.

Certification and Testing Bodies:

"Trust is good - but a certificate is better" In today's markets for products and services, secure solutions are more in demand than ever - certifications are the most effective approach.

Please note that the following lists of relevant stakeholders are not exhaustive. The cybersecurity landscape is generally characterized by a high level of dynamism. In the countries considered, there are numerous large and small organizations that contribute to the growth and development of the sector.

5.3 Germany

5.3.1 Government Agencies:

Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI):

- BSI is the federal authority responsible for information security in Germany. It plays a central role in developing cyber security standards, providing guidance, and coordinating cyber security efforts at the national level. It is also the publisher of the German “IT-Grundschutz” standard and offers advice for SME. All information are available in English and Plain Englisch.
  https://www.bsi.bund.de

Federal Criminal Police Office (Bundeskriminalamt - BKA):

- BKA investigates cybercrime and collaborates with other law enforcement agencies in combating cyber threats.
  https://www.bka.de

Cyber Defense Center (**Cyber-Abwehrzentrum - cA-Z):**

- The Cyber Defense Center is a facility operated jointly by the BSI and the BKA. It is used for the early detection, analysis and defense against cyber-attacks on critical infrastructures and state institutions. The center promotes close cooperation between authorities, companies and other stakeholders in order to respond quickly and effectively to cyber threats.
  https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html

Federal Intelligence Service (Bundesnachrichtendienst - BND):

- BND plays a role in cyber security by monitoring and analyzing cyber threats.

Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz - BfV):

- BfV is responsible for protecting critical infrastructure and preventing espionage.
  https://www.verfassungsschutz.de/EN/topics/cyber-defence/cyber-defence_node.html

Federal Data Protection Commissioner (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit - BfDI):

- BfDI oversees data protection and privacy issues, including those related to cyber security.
  https://www.bfdi.bund.de/EN

German Chambers of Commerce (Deutsche Industrie- und Handelskammertag - DIHK):

- The DIHK may provide information and support related to cyber security and data protection for businesses in Germany.
  https://www.dihk.de/en

5.3.2 Industry Associations and Clusters:

Bitkom:

- Bitkom is a leading German association for the digital economy. It represents companies in the information technology, telecommunications, and digital industries and advocates for cyber security policies.
  https://www.bitkom.org/

Cyber Security Hubs:

- Various regions in Germany, such as Berlin, Munich, and North Rhine-Westphalia, have established cyber security clusters and hubs that bring together companies, researchers, and startups to foster innovation and collaboration.
- **Cyber Cluster Berlin-Brandenburg:** This is one of the cybersecurity hubs in Germany, fostering collaboration among companies and research institutions. https://www.digital-bb.de/innovationsfelder/it-sicherheit

TeleTrusT - IT Security Association Germany:

- TeleTrusT is a network of companies and organizations working on information security. https://www.teletrust.de/en/

Bavarian IT Security Cluster:

- Located in Bavaria, this cluster brings together companies and experts in the field of cybersecurity. https://www.it-sicherheitscluster.de/english/

5.3.3 Businesses and Enterprises:

Allianz Global Corporate & Specialty SE:

- Allianz offers cyber security insurance and risk management services.

Deutsche Telekom AG:

- Deutsche Telekom provides cyber security services for businesses and government agencies.

SAP SE:

- SAP, headquartered in Walldorf, is a global leader in enterprise software, including cyber security solutions.

Siemens AG:

- Siemens offers industrial cyber security solutions to protect critical infrastructure.

T-Systems International GmbH:

- T-Systems is a subsidiary of Deutsche Telekom and provides managed security services.

5.3.4 Cyber security Vendors and Solution Providers:

Check Point Software Technologies GmbH:

- Check Point offers network security and threat prevention solutions.

FireEye Germany GmbH:

- FireEye specializes in advanced threat intelligence and cybersecurity solutions.

Kaspersky Lab:

- Kaspersky is a well-known cybersecurity company that offers a range of security solutions.

McAfee Germany GmbH:

- McAfee is a global cybersecurity company with a presence in Germany, offering security software and services.

Sophos GmbH:

- Sophos provides cybersecurity products and services, including antivirus and endpoint security.

5.3.5 Research and Academic Institutions:

Fraunhofer Institute for Secure Information Technology (SIT):

- Fraunhofer SIT conducts applied research in IT security.

Ruhr-University Bochum:

- Ruhr-Universität Bochum has a strong focus on IT security research and hosts the Horst Görtz Institute for IT Security.

Technical University of Darmstadt:

- TU Darmstadt is known for its research in cybersecurity and hosts the Center for Advanced Security Research Darmstadt (CASED).

University of Passau:

- The University of Passau has a cybersecurity research group and offers programs in cybersecurity.

University of Stuttgart:

- The University of Stuttgart conducts research in cybersecurity and hosts the Stuttgart Research Center for Cyber Risk.

5.3.6 Certification and Testing Bodies:

Bundesdruckerei GmbH:

- Bundesdruckerei offers cyber security services, including certification and security consulting.

DEKRA Certification GmbH:

- DEKRA provides testing and certification services, including cyber security certification.

EuroPriSe GmbH:

- EuroPriSe specializes in privacy and data protection certifications, which may include cyber security aspects.

TÜV Rheinland:

- TÜV Rheinland is a well-known certification body that offers testing and certification services for cyber security products.

VDE Testing and Certification Institute:

- VDE is involved in testing and certifying electrical and electronic products, including cyber security -related certifications.

5.4 Poland

5.4.1 Government Agencies:

Cert Polska:

- Cert Polska is Poland's national computer emergency response team (CERT) responsible for monitoring and responding to cyber security threats.
  https://cert.pl/en/

Polish National Police - Central Office for Combating Cybercrime (Policja - Centralne Biuro Zwalczania Cyberprzestępczości):

- The Polish National Police include a Cybercrime Unit dedicated to investigating cybercrimes.
  https://cbzc.policja.gov.pl/

Office of Electronic Communications (UKE - Urząd Komunikacji Elektronicznej):

- UKE regulates and supervises the electronic communications market in Poland, including aspects of cyber security.
  https://www.uke.gov.pl/en/

Polish Financial Supervision Authority (KNF - Komisja Nadzoru Finansowego):

- KNF oversees the financial sector in Poland and plays a role in ensuring financial cyber security.
  https://www.knf.gov.pl/en/

Polish National Cyber security Center (Narodowe Centrum Cyberbezpieczeństwa - NCC):

- NCC is responsible for coordinating and enhancing cyber security efforts in Poland.
  https://www.gov.pl/web/cyber-nccpl

5.4.2 Industry Associations and Clusters:

PIIT - Polish Chamber of IT and Telecommunications (Polska Izba Informatyki i Telekomunikacji):

- PIIT represents the IT and telecommunications industry in Poland and advocates for cyber security policies.
  https://piit.org.pl/projekty

Cybersec Hub:

- Cybersec Hub is a Polish organization fostering collaboration and innovation in the field of cyber security.
  https://cybersechub.eu/home/

KSWIB - Polish Cyber security Cluster (Klaster Cyberbezpieczeństwa i Szczególnych Wyrobów Informatycznych i Bezpieczeństwa):

- KSWIB is a cluster focused on cyber security and specialized IT products.
  https://cybermadeinpoland.pl/droga-do-nis2/

Polish Association for Secure Communications (Polskie Stowarzyszenie Komunikacji Bezpiecznej):

- This association focuses on secure communications and cyber security.
  https://www.ptks.pl/en/

5.4.3 Businesses and Enterprises:

Asseco Poland:

- Asseco Poland is an IT company that provides a wide range of IT security and cyber security services.

Kaspersky Lab Poland:

- Kaspersky Lab operates in Poland, offering cyber security solutions for businesses and consumers.

Orange Polska:

- Orange Polska is a telecommunications provider that offers cyber security services for businesses.

PGE Group (Polska Grupa Energetyczna):

- PGE Group focuses on securing critical infrastructure and the energy sector.

PKO Bank Polski:

- As one of the largest banks in Poland, PKO Bank Polski invests in cyber security to protect financial assets.

5.4.4 Cyber security Vendors and Solution Providers:

Agnitio Consulting Group:

- Agnitio offers cyber security consulting and advisory services in Poland.

Check Point Software Technologies Poland:

- Check Point provides network security and threat prevention solutions.

ESET Poland:

- ESET is a well-known cyber security company that offers antivirus and endpoint security solutions.

F-Secure Poland:

- F-Secure is a global cyber security company with a presence in Poland, offering security products and services.

NASK - Research and Academic Computer Network (Naukowa i Akademicka Sieć Komputerowa):

- NASK provides cyber security services, including DNS security and network monitoring.

5.4.5 Research and Academic Institutions:

AGH University of Science and Technology (Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie):

- AGH University is known for its research in information security.

CERT-PL Research Team:

- This research team is associated with Cert Polska and focuses on cyber security research and threat analysis.

Military University of Technology (Wojskowa Akademia Techniczna):

- The Military University of Technology conducts research and education in the field of cyber security.

University of Warsaw (Uniwersytet Warszawski):

- The University of Warsaw has a cyber security research group and offers academic programs in the field.

Wrocław University of Science and Technology (Politechnika Wrocławska):

- The university is involved in cyber security research and education.

5.4.6 Certification and Testing Bodies:

Apator ITGW:

- Cyberspace Security: Apator ITGW specializes in cyber security, including testing and evaluation of security solutions.

DEKRA Polska:

- DEKRA provides cyber security testing and certification services, including assessments of products and systems.

Luxoft Poland:

- Luxoft offers cyber security testing and evaluation services, including penetration testing.

SecuRing Polska:

- SecuRing provides cyber security consulting and testing services, including compliance assessments.

TÜV Rheinland Polska:

- TÜV Rheinland offers cyber security testing and certification services in Poland.

5.5 Czech Republic

5.5.1 Government Agencies:

Czech National Cyber and Information Security Agency (Národní agentura pro komunikační a informační technologie - NÚKIB):

- NÚKIB is the national cyber security agency responsible for coordinating and enhancing cyber security efforts in the Czech Republic.
https://nukib.gov.cz/en/cyber-security/

Czech Police - Cybercrime Unit (Policie České republiky - Útvar pro odhalování organizovaného zločinu a kriminality kybernetické):

- The Cybercrime Unit investigates cybercrimes and collaborates with other law enforcement agencies.
https://www.policie.cz/clanek/Police-of-the-Czech-Republic.aspx

Office for Personal Data Protection (Úřad pro ochranu osobních údajů):

- This office oversees data protection and privacy issues, including those related to cyber security.
https://uoou.gov.cz/en

Czech Telecommunication Office (Český telekomunikační úřad):

- The CTU regulates the telecommunications market in the Czech Republic, including aspects of cyber security.
https://ctu.gov.cz/en

Ministry of Defense (Ministerstvo obrany České republiky):

- The Ministry of Defense plays a role in securing critical infrastructure and protecting national security interests in cyberspace.
https://www.army.cz/en/armed-forces/organisational-structure/cyb/cyber-forces-command-218593/

5.5.2 Industry Associations and Clusters:

Czech Association for Cyber security (Asociace pro kybernetickou bezpečnost):

- This association focuses on promoting cyber security awareness and best practices in the Czech Republic.
https://www.kybersoutez.cz/ks_soutez.html

ICT Unie:

- ICT Unie is an industry association representing information and communication technology companies in the Czech Republic, including those involved in cyber security.
https://ictu.cz/en/about-ictu/workgroups

CyberCentral CZ:

- CyberCentral CZ is a platform for networking and collaboration among cyber security professionals and organizations.
https://cybercentral.eu/

5.5.3 Businesses and Enterprises:

Avast Software:

- Avast is a cyber security company headquartered in Prague, known for its antivirus and cyber security products.

CEZ Group:

- CEZ is a prominent energy company in the Czech Republic that focuses on securing critical infrastructure.

Kaspersky Lab Czech Republic:

- Kaspersky Lab operates in the Czech Republic, offering cyber security solutions for businesses and consumers.

Seznam.cz:

- Seznam.cz, a major Czech internet company, offers cyber security services, including email security.

T-Mobile Czech Republic (T-Mobile Česká republika):

- T-Mobile offers cyber security services and solutions for businesses.

5.5.4 Cyber security Vendors and Solution Providers:

Check Point Software Technologies Czech Republic:

- Check Point provides network security and threat prevention solutions.

ESET Czech Republic:

- ESET is a globally recognized cyber security company with a presence in the Czech Republic, offering antivirus and endpoint security solutions.

Fortinet Czech Republic:

- Fortinet specializes in cyber security solutions, including network security and firewall technology.

McAfee Czech Republic:

- McAfee is a global cyber security company with a presence in the Czech Republic, offering security software and services.

Trend Micro Czech Republic:

- Trend Micro offers a range of cyber security solutions, including endpoint security and threat intelligence.

5.5.5 Research and Academic Institutions:

Czech Academy of Sciences (Akademie věd České republiky):

- The Czech Academy of Sciences conducts research in various fields, including cyber security.

Czech Institute of Informatics, Robotics, and Cybernetics (Český institut informatiky, robotiky a kybernetiky):

- This institute focuses on research in informatics, robotics, and cybernetics, including cyber security.

Czech Technical University in Prague (České vysoké učení technické v Praze):

- CTU in Prague conducts research and education in the field of cyber security.

Masaryk University (Masarykova univerzita):

- Masaryk University in Brno is involved in cyber security research and education.

Brno University of Technology (Vysoké učení technické v Brně):

- Brno University of Technology is known for its cyber security research and education.

5.5.6 Certification and Testing Bodies:

Avast Virus Lab (Avast Virová laboratoř):

- Avast operates a virus lab in the Czech Republic involved in testing and analyzing cyber security threats.

CERT-UKB (University of West Bohemia - Univerzita západních Čech v Plzni):

- CERT-UKB is a Computer Emergency Response Team affiliated with the University of West Bohemia.

DEKRA Czech Republic:

- DEKRA provides cyber security testing and certification services, including assessments of products and systems.

SK CERT (National Research Network for Communication, Information and Informatics - Národní výzkumná síť pro komunikaci, informace a informatiku):

- SK CERT provides cyber security services, including incident response and testing.

TÜV SÜD Czech Republic:

- TÜV SÜD offers cyber security testing and certification services in the Czech Republic.

5.6 Latvia

5.6.1 Government Agencies:

Latvian National Computer Security Incident Response Team (CERT.LV):

- CERT.LV is Latvia's national computer security incident response team responsible for monitoring and responding to cyber security threats. https://cert.lv/en/

State Police of Latvia (Latvijas Valsts policija):

- The State Police of Latvia includes a dedicated cybercrime unit that investigates cybercrimes and collaborates with international law enforcement agencies. https://www.vp.gov.lv/en/

Data State Inspectorate (Datu valsts inspekcija):

- The Data State Inspectorate oversees data protection and privacy issues in Latvia, including aspects of cyber security. https://www.dvi.gov.lv/en

Latvian Ministry of Defense (Aizsardzības ministrija):

- The Ministry of Defense plays a role in securing critical infrastructure and protecting national security interests in cyberspace. https://www.mod.gov.lv/en/cybersecurity

Latvian Regulatory Authority for Electronic Communications and Postal Services (Elektronisko sakaru regulēšanas iestāde):

- The Regulatory Authority regulates electronic communications in Latvia, including aspects of cyber security. https://www.sprk.gov.lv/en/content/electronic-communications

Latvian National Computer Security Incident Response Team (CERT.LV):

- CERT.LV is Latvia's national computer security incident response team. They provide cyber security resources and support to organizations in Latvia. https://www.cert.lv/en/

5.6.2 Industry Associations and Clusters:

Latvian Information and Communication Technology Association (LIKTA - Latvijas Informācijas un komunikācijas tehnoloģiju asociācija):

- LIKTA represents the ICT industry in Latvia and promotes cyber security awareness and best practices. https://likta.lv/digitalo-prasmju-projekts/

Latvian Chamber of Commerce and Industry (Latvijas Tirdzniecības un rūpniecības kameras):

- The Chamber may offer information and support related to cyber security for businesses in Latvia.
  https://ltrk.lv/en

5.6.3 Businesses and Enterprises:

Baltic Computer Academy (Baltijas Datoru Akadēmija):

- This academy offers training and certification programs in cyber security and IT.

Cybernetica Latvia:

- Cybernetica is an IT company that provides a range of IT security and cyber security services.

Latvenergo:

- Latvenergo is the state-owned electricity company in Latvia, focused on securing critical infrastructure.

Swedbank Latvia:

- Swedbank is a major financial institution in Latvia that invests in cyber security to protect financial assets.

Telia Latvia (Telia Latvija):

- Telia offers cyber security services for businesses, including network security and threat detection.

5.6.4 Cyber security Vendors and Solution Providers:

Biosoft Latvia:

- Biosoft offers cyber security solutions and services, including cyber security training and consulting.

Check Point Software Technologies Latvia:

- Check Point provides network security and threat prevention solutions.

ESET Latvia:

- ESET is a well-known cyber security company that offers antivirus and endpoint security solutions.

Fortinet Latvia:

- Fortinet specializes in cyber security solutions, including network security and firewall technology.

Trend Micro Latvia:

- Trend Micro offers a range of cyber security solutions, including endpoint security and threat intelligence.

5.6.5 Research and Academic Institutions:

BA School of Business and Finance (Banku Augstskola):

- BA School offers cyber security programs and collaborates on research projects related to cyber security.

CERT.LV Research Team:

- The research team associated with CERT.LV focuses on cyber security research and threat analysis.

Latvian Academy of Sciences (Latvijas Zinātņu akadēmija):

- The Latvian Academy of Sciences conducts research in various fields, including cyber security.

Riga Technical University (Rīgas Tehniskā Universitāte):

- RTU is known for its research in IT security and offers academic programs in the field.

University of Latvia (Latvijas Universitāte):

- The University of Latvia conducts research and education in the field of cyber security.

5.6.6 Certification and Testing Bodies:

CERT.LV Testing and Evaluation Team:

- CERT.LV offers cyber security testing and evaluation services for products and solutions.

DEKRA Latvia:

- DEKRA provides cyber security testing and certification services, including assessments of products and systems.

Latvian Standard (Latvijas Standarts):

- Latvian Standard is involved in standards development, including cyber security standards.

TechNet IT School (TechNet IT Skola):

- TechNet IT School offers training and certification programs in cyber security

TÜV SÜD Latvia:

- TÜV SÜD offers cyber security testing and certification services in Latvia.

5.7 Lithuania

5.7.1 Government Agencies:

National Cyber Security Centre of Lithuania (Nacionalinis Kibernetinės Saugos Centras - NKSC):

- NKSC is responsible for monitoring and responding to cyber security threats in Lithuania.
  https://www.nksc.lt/

Lithuanian Criminal Police Bureau (Lietuvos Policijos Kriminalinės Policijos Biuras):

- The Criminal Police Bureau includes a dedicated Cybercrime Investigation Unit focused on investigating cybercrimes.
  https://lkpb.policija.lrv.lt/en/

State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija):

- The State Data Protection Inspectorate oversees data protection and privacy issues, including aspects of cyber security compliance.
  https://vdai.lrv.lt/en/

Lithuanian Ministry of National Defence (Nacionalinė gynybos ministerija):

- The Ministry of National Defence plays a role in securing critical infrastructure and protecting national security interests in cyberspace.
  https://kam.lt/en/cyber-security/

Lithuanian Communications Regulatory Authority (Ryšių reguliavimo tarnyba):

- The Communications Regulatory Authority regulates electronic communications in Lithuania, including aspects of cyber security.
  https://www.rrt.lt/en/

5.7.2 Industry Associations and Clusters:

BCCS (Blockchain, Cyber Security and Compliance Solutions) Cluster

- BCCS is a Digital Innovation Hub that supports businesses in the Fintech and Web3 industries.
  https://bccs.tech/services/cybersecurity/

Vilnius Tech Park:

- Vilnius Tech Park is a technology and startup hub that includes cyber security - focused companies and startups.
  https://techzity.com/vilnius-tech-park/

Lithuanian Innovation Center (Lietuvos inovacijų centras):

- The center supports innovation and research, including projects related to cyber security.
  https://www.lic.lt/en/

Lithuanian Chamber of Commerce, Industry, and Crafts (Lietuvos pramonininkų konfederacija):

- The Chamber may offer information and support related to cyber security for businesses in Lithuania.
  https://lpk.lt/en

5.7.3 Businesses and Enterprises:

NFQ Technologies:

- NFQ Technologies is an IT company in Lithuania that offers cyber security solutions and services.

NRD Cyber Security:

- NRD Cyber Security provides a range of IT security and cyber security services.

Swedbank Lithuania (Swedbank Lietuva):

- Swedbank is a financial institution in Lithuania that invests in cyber security to protect financial assets.

Telco Security Lithuania:

- Telco Security offers cyber security services for businesses in Lithuania, including network security and threat detection.

Telia Lithuania (Telia Lietuva):

- Telia offers cyber security services for businesses, including network security and threat intelligence.

5.7.4 Cyber security Vendors and Solution Providers:

Check Point Software Technologies Lithuania:

- Check Point provides network security and threat prevention solutions.

ESET Lithuania:

- ESET is a well-known cyber security company that offers antivirus and endpoint security solutions.

SentinelOne Lithuania:

- SentinelOne provides next-generation endpoint protection and security solutions.

Telia Lithuania Cyber Security:

- Telia Lithuania offers a variety of cyber security services, including managed security services.

5.7.5 Research and Academic Institutions:

Cyber Centre of Excellence (Cyber Kooperacijos Centras):

- The center focuses on cyber security research, development, and training.

Kaunas University of Technology (Kauno technologijos universitetas):

- KTU is known for its research in information security and offers academic programs in the field.

Lithuanian University of Educational Sciences (Lietuvos edukologijos universitetas):

- The university offers programs and events related to cyber security and IT.

Mykolas Romeris University (Mykolo Romerio universitetas):

- MRU is involved in research and education related to cyber security and cyber law.

Vilnius University (Vilniaus universitetas):

- Vilnius University conducts research and education in the field of cyber security.

5.7.6 Certification and Testing Bodies:

CERT-LT (Lithuanian Computer Emergency Response Team):

- CERT-LT offers cyber security incident response and testing services.

CyberNorth:

- CyberNorth provides cyber security consulting, training, and testing services in Lithuania

DEKRA Lithuania:

- DEKRA provides cyber security testing and certification services, including assessments of products and systems.

Lithuanian Standards Board (Lietuvos standartizacijos departamentas):

- The Lithuanian Standards Board is involved in standards development, including cyber security standards.

TÜV SÜD Lithuania:

- TÜV SÜD offers cyber security testing and certification services in Lithuania.

5.8 Estonia

5.8.1 Government Agencies:

Estonian Information System Authority (RIA - Riigi Infosüsteemi Amet):

- RIA is responsible for cyber security and e-government initiatives in Estonia, including the management of the Estonian Cyber Security Strategy. https://www.itvaatlik.ee/

Estonian Police and Border Guard Board (Politsei- ja Piirivalveamet):

- The Estonian Police and Border Guard Board include a dedicated Cybercrime Bureau focused on investigating cybercrimes. https://www.politsei.ee/en/

Data Protection Inspectorate (Andmekaitse Inspektsioon):

- The Data Protection Inspectorate oversees data protection and privacy issues, including aspects of cyber security compliance. https://www.aki.ee/en

Estonian Ministry of Defence (Kaitseministeerium):

- The Ministry of Defence plays a role in securing critical infrastructure and national security interests in cyberspace. https://kaitseministeerium.ee/en/Open-Cyber-Range

CERT-EE (Estonian Computer Emergency Response Team - CERT-Estonia):

- CERT-EE is responsible for monitoring and responding to cyber security incidents in Estonia. https://www.ria.ee/en/cyber-security/ncsc-ee/cyber-security-centre-ncsc-ee

5.8.2 Industry Associations and Clusters:

Estonian ICT Cluster (Eesti IKT Klaster):

- The Estonian ICT Cluster promotes collaboration and innovation in the ICT sector, including cyber security. https://itl.ee/en/cyber-support/

e-Governance Academy (e-Governance Akadeemia):

- The e-Governance Academy in Estonia focuses on promoting e-governance, digital society, and cyber security best practices. https://ega.ee/services/#cybersecurity

Estonian Cyber Security Cluster (Eesti Küberkaitse Klaster):

- The Estonian Cyber Security Cluster fosters collaboration among cyber security professionals and organizations in Estonia. https://defence.ee/cluster-and-members/

Estonian Chamber of Commerce and Industry (Eesti Kaubandus-Tööstuskoda):

- The Chamber may offer information and support related to cyber security for businesses in Estonia. https://www.koda.ee/en/

5.8.3 Businesses and Enterprises:

Cybernetica:

- Cybernetica is an Estonian technology company that provides secure e-government and cyber security solutions.

Guardtime:

- Guardtime is an Estonian company specializing in blockchain-based cyber security solutions.

Nortal:

- Nortal is an IT company in Estonia that provides a range of IT security and cyber security services.

Swedbank Estonia (Swedbank Eesti):

- Swedbank is a financial institution in Estonia that invests in cyber security to protect financial assets.

Telia Estonia (Telia Eesti):

- Telia offers cyber security services for businesses in Estonia, including network security and threat detection.

5.8.4 Cyber security Vendors and Solution Providers:

Certified Security Solutions (CSS):

- CSS offers cyber security solutions, including public key infrastructure (PKI) and digital identity management.

Cybernetica:

- Cybernetica is involved in developing secure e-government solutions, including digital identity and data protection.

ESET Estonia:

- ESET is a well-known cyber security company that offers antivirus and endpoint security solutions.

RangeForce:

- RangeForce is an Estonian cyber security training and skills development platform.

SentinelOne Estonia:

- SentinelOne provides next-generation endpoint protection and security solutions.

5.8.5 Research and Academic Institutions:

Cybernetica Research:

- Cybernetica is actively engaged in research and development in the field of cyber security.

e-Governance Academy (e-Governance Akadeemia):

- The academy is involved in research and training related to e-governance and cyber security.

Estonian Information Technology College (Eesti Infotehnoloogia Kolledž):

- The college offers programs and events related to cyber security and IT.

Tallinn University of Technology (Tallinna Tehnikaülikool):

- TTÜ is known for its research in information security and offers academic programs in the field.

University of Tartu (Tartu Ülikool):

- The University of Tartu conducts research and education in the field of cyber security.

5.8.6 Certification and Testing Bodies:

BHC Laboratory (BHC Laborid):

- BHC Laboratory provides cyber security and information security testing and assessment services.

Cybernetica Testing and Evaluation Team:

- Cybernetica offers cyber security testing and evaluation services, including secure e-government solutions.

eGA-CERT (E-Governance Academy Computer Emergency Response Team):

- eGA-CERT offers cyber security incident response and testing services.

Guardtime Estonia:

- Guardtime provides blockchain-based cyber security solutions and services.

TÜV SÜD Estonia:

- TÜV SÜD offers cyber security testing and certification services in Estonia.

We thank the co-authors from:

BF/M-Bayreuth

eCampus-Lausitz

Mykolas Romeris University

Information Security Awareness, Literacy and Privacy - ISALIP

Co-funded by the European Union

Co-funded by
the European Union

ISALIP