isecureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

ERASMUS+ cooperation partnership
Digital education tools for
SECURITY RISK MANAGEMENT

RECOMMENDATIONS
for higher education institutions teaching security

▶ FOCUS ON SECURITY RISK MANAGEMENT

INTRODUCTION

Consequently, it is evident that there is a pressing need not only for high-quality training for young security specialists but also for training that will enable them to better prepare for crises and potentially mitigate numerous threats before they escalate into full-blown crises.

This need prompted the formation of a consortium consisting of seven partner organizations from six countries. The primary objective of this consortium is to develop diverse digital teaching and learning materials focused on security risk management, including those recommendations for higher education institutions and training centres and organisations preparing security specialists.

ABOUT THE PROJECT

Partners from Latvia, Lithuania, Finland, the Netherlands, Norway and Spain joined their knowledge and expertise and developed an ERASMUS+ cooperation partnership project which aims to develop various teaching materials on security risk management.

This project aims to establish a sustainable security specialists' network, which can cooperate on a long term basis. During the project partners developed recommendations for Universities that are preparing security specialists in Europe. Also, the partnership developed comprehensive and up-to-date digital teaching materials and tools, gathered on one web platform which contains the most updated information on security risk management aspects available for all security experts, students and academics.

Find more materials on the project website: https://security.turiba.lv/

Project partners:

ABOUT THIS PUBLICATION

These recommendations contain information on how to enhance security study programmes and incorporate the topic of security risk management into study and training programmes. This document includes recommendations regarding focus, topics, methods, and further educational suggestions. We hope that these recommendations will contribute to the improvement of study programmes and methods related to security education and security risk management in European countries, fostering a common approach in the preparation of young specialists.

The target audience for this material includes academic and management staff of higher education institutions, representatives from training centres offering education on security. This material can also be interesting for everyone who has a keen interest in security risk management, as well as professionals working within the field of security.

LIST OF AUTHORS

TURIBA UNIVERSITY:
Kristīne Neimane, Head of the Project department, lecturer at Turiba University, Latvia
Uģis Začs, lecturer at Turiba University, Latvia
Kārlis Apalups, lecturer at Turiba University, Latvia
Ivita Kīsnica, lecturer at Turiba University, Latvia
NORD University:
Natalia Andreassen, Professor, Nord University Business School, Center for Crisis Management and Collaboration, Norway
Rune Elvegård, Senior Advisor, Nord University Business School, Center for Crisis Management and Collaboration, Norway
Daniel Kibsgaard, Advisor, Nord University Business School, Center for Crisis Management and Collaboration, Norway
Ensieh Roud, Associate Professor, Nord University Business School, Center for Crisis Management and Collaboration, Norway
STICHTING AVANS:
Bert Bambach, Senior lecturer, Avans University of Applied Sciences, Netherlands
Beyke Goffin, Senior lecturer, Avans University of Applied Sciences, Netherlands
Jack Bergman, Senior lecturer, Avans University of Applied Sciences, Netherlands
FUNDACIÓ UNIVERSITAT AUTÒNOMA DE BARCELONA:
Xavier Dorado, Research Technician, Fundació Universitat Autònoma de Barcelona, Prevenció i Seguretat Integral, Spain
Elisabet Garcia, Research Technician, Fundació Universitat Autònoma de Barcelona, Prevenció i Seguretat Integral, Spain
LAUREA UNIVERSITY OF APPLIED SCIENCES:
Anja Aatsinki, Senior Lecturer, Laurea University of Applied Sciences, Finland
Hanna Iisakkila Rojas, Senior Lecturer, Laurea University of Applied Sciences, Finland
KAZIMIERAS SIMONAVICIUS UNIVERSITY:
Raimundas Kalesnykas, Professor at the Institute of Law and Technology, Kazimieras Simonavicius University, Lithuania

1. THE ROLE AND PROFILE OF A SECURITY SPECIALIST

1.1. What are the roles and profile of a security specialist nowadays?

The role and profile of a security specialist can vary depending on the specific industry, organization, and the nature of the security threats they are addressing. However, in a broad sense, security specialists today are responsible for protecting an organization's digital and physical assets from a wide range of threats, including cyberattacks, physical intrusions, and other security risks.

In international environment there are various types of security specialist roles, and some of them are:

- ➢ **Physical Security Specialist**: Securing an organization's physical premises, assets, and staff. This may involve the use of surveillance systems, access control, alarm systems, security personnel management, and emergency response planning. Skills: Knowledge of physical security system design and technology, emergency management, and safety protocols.
- ➢ **Security Operations Center (SOC) Analyst**: Monitoring and analyzing security events in real-time, investigating alerts, and responding to incidents. SOC analysts play a critical role in identifying and mitigating cyber threats. Skills: Proficiency in security information and event management (SIEM) tools, incident response procedures, and the ability to work under pressure.
- ➢ **Compliance and Risk Manager**: Ensuring an organization complies with industry regulations and standards. Identifying and managing security risks, developing risk mitigation strategies, and maintaining compliance documentation. Skills: Deep knowledge of relevant regulations (e.g., GDPR, HIPAA), risk assessment methodologies, and audit processes.
- ➢ **Director of Security**: This specialist is responsible for overseeing all security operations within an organization. They develop security policies and procedures, manage security budgets, and coordinate with other departments to ensure that security measures are integrated into all aspects of the organization.
- ➢ **Security Manager:** This specialist is responsible for managing the security team and ensuring that all security protocols are followed. They also coordinate with other departments to ensure that security measures are integrated into all aspects of the organization.
- ➢ **Security Consultant:** Providing advisory services to clients or within an organization to assess, plan, and implement security solutions. This role often involves working on various security projects. This specialist reviews current security measures and practices and recommends new alarm systems or other security measures and strategies. Skills: Strong problem-solving skills, the ability to assess an organization's unique security needs, and the ability to recommend and implement security measures accordingly.
- ➢ **Security Architect:** Design and build security systems, including firewalls, intrusion detection systems, and other security measures and infrastructure. This role involves creating secure network and software architectures, and working closely with development and IT teams. Skills: In-depth knowledge of security principles, encryption, and secure design principles.
- ➢ **Cybersecurity Specialist**: Protect an organization's computer systems, networks, and data from cyber threats. This involves identifying vulnerabilities, implementing security measures, monitoring for breaches, and responding to incidents. This specialist maintains the security of an organization's database, ensuring that it's free

from cyber threats and unusual activities. They upgrade hardware and software applications, configure networks to improve optimization, address any unauthorized access on the database, troubleshoot system discrepancies conduct security audits on the system, and improve automated processes. <u>Skills</u>: Knowledge of cybersecurity technologies, risk management, and understanding of various attack vectors. Proficiency in tools and techniques for intrusion detection, malware analysis, and threat mitigation.

- **Information Security Analyst**: Assess an organization's information security posture, develop security policies and procedures, and ensure compliance with relevant regulations and standards. <u>Skills:</u> Understanding of security frameworks and standards, risk assessment, and the ability to evaluate security controls and technologies.
- **Application Security Specialist**: This specialist installs, configures, and maintains security software designed to prevent outside attacks on the company's internal networks.
- **Personnel Security (PERSEC) Specialist**: This specialist ensures that employees and contractors in a facility obtain a proper security clearance. They conduct background checks for applicants who apply for government jobs that require a security clearance.
- **Incident Responder:** Respond to security incidents, contain and mitigate the damage, and help with recovery efforts. This role requires quick thinking and adaptability. <u>Skills:</u> Strong problem-solving skills, knowledge of digital forensics, and incident response procedures.
- **Security Awareness and Training Specialist:** Educate employees and stakeholders on security best practices, raise security awareness, and develop training programs. <u>Skills</u>: Strong communication skills, knowledge of adult learning principles, and an understanding of the human element in security.

The roles and profiles of security specialists are evolving rapidly as technology advances and new threats emerge. Security specialists need to stay up-to-date with the latest security trends, technologies, and best practices to effectively protect their organizations from a constantly changing threat landscape.

Although the profile of a security specialist can be quite diverse, several skills emerge as common to all of these profiles, and without which the profession of a security specialist is unimaginable today.

Three skills — knowledge of security principles, risk management, and communication — are not only essential for security specialists but also act as the cornerstone for their success in safeguarding organizations against evolving security challenges.

As this project partnership has explored and provided information in the following sections - security programs offered in partner countries, they are sufficiently focused to allow young security specialists to thoroughly acquire basic knowledge of security principles. At the same time, the partnership's research indicates that communication skills, one of the so-called soft skills, are often mentioned as skills that young security specialists need to improve. As the third mentioned skill, there is risk management - that is, knowledge and the ability to apply risk management principles, an understanding of the framework and process of risk management. Conducting a self-assessment of the 6-country partnership, it was found that both graduates and lecturers rate risk management skills of students' as average. That's why this project primarily focuses on risk management skills. While this document will

examine the focus and skills of a security specialist in a broader context, the main emphasis will be on security risk management skills.

Role of a security specialist

Each security specialist is a professional responsible for ensuring the safety and security of individuals, organizations, or assets. They play a crucial role in identifying, mitigating, and responding to various security risks and threats. Here is an overview of the role and profile of a security specialist:

- **Risk Assessment**: Security specialists assess potential security risks and vulnerabilities by conducting security audits and risk assessments. They identify weaknesses in physical security, information security, and operational security.
- **Security Planning:** They develop comprehensive security plans and strategies to protect assets, people, and information. This includes designing security protocols and systems.
- **Information Security**: They work on safeguarding digital assets and sensitive information by establishing and maintaining cybersecurity protocols, including firewalls, encryption, and intrusion detection systems.
- **Emergency Response:** In the event of security breaches or emergencies, security specialists lead responses to mitigate damage and restore safety. This includes coordinating with first responders and law enforcement.
- **Security Training:** They provide security awareness and training programs for employees or clients, ensuring that security policies and procedures are understood and followed.
- **Security Compliance**: Ensure compliance with relevant laws, regulations, and industry standards related to security, privacy, and data protection.
- **Investigations:** Conduct investigations into security incidents, breaches, or suspicious activities to identify the cause and responsible parties.

The profile of a security specialist can vary depending on the specific position and organization they work for. However, some of the common skills, education, and experience required for a security specialist are:

- **Education:** A security specialist typically possesses a bachelor's degree in a relevant field, such as cybersecurity, information security, criminology, computer science, or a related discipline. Many security specialists pursue advanced degrees or professional certifications to enhance their knowledge and skills.
- **Experience:** Security specialists may have several years of experience in related roles, such as security analysts, network administrators, or IT support. Experience is often required for mid-level and senior security positions.
- **Certifications**: Many security specialists pursue industry-specific certifications, such as Certified Information Systems Security Professional (CISSP), Certified Protection Professional (CPP), or Certified Security Professional (CSP), depending on their country and area of expertise.
- **Communication Skills**: Effective written and verbal communication skills are essential for reporting and presenting security findings and strategies to stakeholders. Effective communication and interpersonal skills are crucial, as security specialists frequently collaborate with various stakeholders and need to educate and train others on security best practices.

7

- **Problem-Solving Skills:** The ability to analyze complex security issues, identify vulnerabilities, and develop solutions is crucial for security specialists.
- **Technical Proficiency:** Depending on the specific role, security specialists may need expertise in physical security systems, cybersecurity tools, or investigative techniques.
- **Attention to Detail:** A strong eye for detail is necessary to identify security risks and vulnerabilities.
- **Ethical and Legal Understanding:** must adhere to high ethical standards, as they often handle sensitive information and have access to secure environments. A security specialist should have a clear understanding of ethical considerations and the legal aspects of security, including laws related to data protection, privacy, and cybersecurity. Ethical Conduct: Security specialists.
- **Physical Fitness:** For roles that involve physical security, such as security guards, being in good physical shape may be necessary.
- **Adaptability:** The security landscape is ever-evolving, so the ability to stay updated on emerging threats, technologies, and best practices is essential for a security specialist.

As key competencies for security specialists can be named risk management, threat assessment, security planning and policy development, incident response, security technology expertise, compliance and legal knowledge, communication and education, attention to detail, adaptability.

In summary, a security specialist's role is to protect an organization from various security threats by assessing risks, implementing security measures, responding to incidents, and ensuring compliance with regulations. Their profile should reflect a strong educational background, relevant certifications, experience, technical skills, and a commitment to staying informed about the latest security developments.

1.2. Security specialist standards in Europe and partner countries

At the moment, there are no uniform standards in Europe that would determine the profile of a security specialist and what a security specialist should necessarily observe. Considering the wide profile of security specialists, the specifics of their fields of activity, it is impossible to develop a single standard for all. Currently, there are various separate security standards, such as general risk management, cyber security, fire safety, etc. standards, but there are no standards that include the standard of physical security specialists. There are also no uniform standards that a security specialist should know and learn.

Consequently, each country has developed its own standards, putting emphasis on the various aspects that are most important in their opinion. In addition, the profiles of the universities where security specialists are trained are also different.

Here, we offer you a brief overview of the standards and regulations related to the profession of security specialists in each project partner country.

LATVIA

In **Latvia** there are security specialist professional standard. This standard target such specific groups are fire safety specialists, corporate (organisational) security specialists, OSH specialists, information security specialists.

Professional standards are made by NGOs and accepted by a special commission under Cabinet of Ministers. They are made with the intention of being able to accredit and certify education programmes that would provide the increased safety standards and quality.

Focus in this standards are on risk analysis, creation of organisation security concept, business management, training of staff, project management, understanding of security equipment, understanding of criminal law, labour protection law and data protection law.

The standards include a reference to the knowledge and competency to perform or coordinate risk management activities, but no reference to specific risk management standards.

Although standards include a broad variety of skills and competencies, there is room for improvement and change. There should be a greater emphasis on interdisciplinary skills from other fields. For example, physical security specialists should possess an understanding of information security, and vice versa, as security domains are converging.

Link to Standards:

https://registri.visc.gov.lv/profizglitiba/dokumenti/standarti/2017/PS-192.pdf (Security specialist)

https://registri.visc.gov.lv/profizglitiba/dokumenti/standarti/2017/PS-235.pdf (Fire safety and civil protection technician)

https://registri.visc.gov.lv/profizglitiba/dokumenti/standarti/20170614_Profesiju_standarti_5.pdf (Head of security service)

https://registri.visc.gov.lv/profizglitiba/dokumenti/standarti/ps0278.pdf (Fire safety and civil protection engineer)

https://registri.visc.gov.lv/profizglitiba/dokumenti/standarti/2017/PS-179.pdf (OSH specialist)

https://registri.visc.gov.lv/profizglitiba/dokumenti/standarti/2017/PS-207.pdf (OSH senior specialist)

https://registri.visc.gov.lv/profizglitiba/dokumenti/standarti/2017/PS-168.pdf (Information security manager)

LITHUANIA

In **Lithuani**a there are 2 types of standards: Professional Standard for the Sector of Service administration, Service of Institutions and Security Activities (hereinafter – Professional Service Standard) which was approved in 2019, and Vocational Training Standards for police officers, for border guards, and for firefighters-rescuers (2007).

The Professional Service Standard includes 9 qualifications, among which 3 categories of security professionals are distinguished: security guard, security manager and security systems specialist. The Professional Service Standard defines the following qualification levels which are in line with the levels of the European Qualifications Framework (EQF): (1) Security Guard/Level 3 (skill groups: protection of objects, natural persons, mass events; use of special measures and physical coercion; firearm control, etc.; (2) Security Manager/Level 4 (skill groups: organization of protection of objects, mass events and natural persons; carrying out crime prevention functions; performing investigations of administrative offences, etc.; (3) Safety Systems Specialist/Level 6 (skill groups: providing security services and solutions; participating in the development and implementation of the organization-level security strategy; selection of risk management models and tools; ensuring control of risk management processes, security system management, etc).

The Professional Service Standard does not comply with the provisions of the Personal and Property Security Law of the Republic of Lithuania, which is focused on the security services market and that provision should be changed. Professionals working in the private security sector would meet the same professional standards as in the public security sector.

The Professional standard for the sector of service administration, service of institutions and security activities **can be found here**:
https://www.e-tar.lt/portal/lt/legalAct/eddbf5f09f0111e9878fc525390407ce
https://www.kpmpc.lt/kpmpc/kvalifikaciju-formavimas/standartai-2/profesinio-rengimo-standartai/

THE NETHERLANDS

The Netherlands have security specialist professional standards on professions covered by the Private Security Services Act. It should be noted that universities do not, and cannot, offer the training in this field, including the specialist qualification. The target group of those standards are security guards, stewards, security services personnel who are: planning, installing, repairing, or altering structural protection & electronic monitoring, and who perform the planning of other security arrangements. They could also be managers of private security services.
Security guards and stewards have their own training and license requirements. Security services personnel have a licence requirement, but no specific education requirement (may be locksmiths, electricians, etc.). Managers of private security services must have completed a specialist qualification of security officers. The standards above refer to education at the secondary vocational level.

At the bachelor, post-bachelor and master level security education focuses primarily on Security Fundamentals; Business Operations; Risk Management and Response Management. Enrolment in the various levels of education will be allowed to anyone at senior secondary vocational, Bachelor, University level if they have appropriate entry level qualifications. Post Bachelor education and courses, training and workshops can be only enrolled in if one has the right pre-education and experience in the working field of security.

FINLAND

Finland has security specialist professional standards on professions covered by the Private Security Services Act. It should be noted that universities do not, and cannot, offer the training mentioned, including the specialist qualification. The target group of those standards are:
- Security guards.
- Stewards.
- Private security services personnel planning, installing, repairing, or altering structural protection & electronic monitoring, and the planning of other security arrangements.
- Managers of private security services.

Security guards and stewards have their own training and license requirements. Security services personnel have a licence requirement, but no specific education requirement (may be for example trained as locksmiths, electricians, etc.). Managers of private security services must have a specialist qualification of security officers completed.

Standard focus is on private security legislation, then depending on position things like security technology, tactics, reporting, etc.
In specialist qualification of security officers, basic knowledge of risk management is part of the curriculum. Others mentioned are strictly vocational and do not need to have knowledge of security risk assessment and management.

SPAIN

Spain has security specialist professional standards which target technicians in occupational risk prevention, security directors and private investigators. Depending on the cases, the competent body to approve the rules regulating the competences, requirements and access to the aforementioned careers is the Government or the Congress, by means of regulatory norms such as Royal Decree 39/1997, of 17 January, approving the Prevention Services Regulations (occupational risk technicians), or rules with the status of law, such as Law 5/2014, of 4 April, on Private Security (private directors or detectives).

In order to carry out the functions of technician in occupational risk prevention it is necessary to have an official university degree, and to possess minimum training accredited by a university with the content specified in the programme. The duration is no less than six hundred hours and an hourly distribution appropriate to each training project. There are three specialities: occupational safety; industrial hygiene; occupational medicine and ergonomics and applied psychosociology.

For security managers and directors, by obtaining either an official university degree in the field of security that accredits the acquisition of the competences that are determined, or by the title of the security management course, recognised by the Ministry of the Interior. As of now, and unlike higher technicians in occupational health, it is not strictly necessary to be in possession of a bachelor's degree.

For private detectives, by obtaining either a university degree in the field of private investigation that accredits the acquisition of the competences that are determined, or the qualification of the private investigation course, recognised by the Ministry of the Interior. As of now, and unlike higher technicians in occupational health, it is not strictly necessary to be in possession of a bachelor's degree.

Some regulations need to be updated according to the security processes affected by the rise of new information technologies, artificial intelligence, process automation, big data analysis, access control through biometric technology, drones, and other aspects that have changed the world of security.

Training and requirements must be adapted to this new reality in terms of legislation and regulations, both in the field of occupational risk prevention and in the field of private security. On another note, is should be pointed out that, over the last years, there have been public discussions as to whether or not the private directors and detectives should be in possession of a bachelor's degree, which could be a reality in the near future.

Links to the Standards:

https://www.boe.es/buscar/act.php?id=BOE-A-1997-1853

https://www.boe.es/buscar/act.php?id=BOE-A-2014-3649

All education in **Norway** follows the Norwegian qualifications framework for lifelong learning (NQF), in line with the European Qualifications Framework (EQF). There are no other central standards that govern the education and responsibilities for all security specialists. In general, different security sectors have their own frameworks and standards, adapted to the challenges the specialist will face in his/her work.

There are, however, some fields of work that require state mandated training – some examples follow: The Norwegian police academy is a three year bachelor's degree, whereas security guards undertake a 163 hour long course – both including on the job training. Firefighters must apply for a job at their local fire department and serve as aspirants through a standardised on the job-training program. Standards for the education of ambulance workers and paramedics are regulated by law, and the learning objectives are based on national guidelines.

In the realm of cyber security and other specialised fields, the education and training is primarily market driven. Most standards imposed on industries and businesses are guidelines and frameworks by national authorities and directorates, such as The Norwegian National Security Authority (NSM) or The Norwegian Directorate for Civil Protection (DSB).

In general, all national safety and security work is built on central principles, based on national law. A central aspect of Norwegian security and preparedness work is that of collaboration – there is a shared understanding that no one actor is able to handle difficult situations alone.

In 2018, Standard Norge published the official Norwegian version of ISO 31000 – Risk management guidelines. The standard is relevant for all organisations, and is quickly gaining purchase in a number of Norwegian corporations. Several private actors offer courses and certifications in the operationalization of the standard. In addition, DSB actively uses the standard in their work on official guidelines.

Links:

Norwegian National Security Authority, English landing site: https://nsm.no/home/

Instructions for departmental work on societal security (Norwegian principles for societal security and preparedness work): https://lovdata.no/dokument/INS/forskrift/2017-09-01-1349/KAPITTEL_3#KAPITTEL_3

ISO 31000 Norwegian standard for risk management:
https://standard.no/fagomrader/risikostyring/iso-31000-risikostyring--retningslinjer/

There are over 4000 higher education institutions in Europe and at least several hundred universities across Europe that offer security-related study programs at both the bachelor's and master's levels.

The focuses and aims of security-related study programs in European universities can vary depending on the specific programme and the university offering it. However, generally, these programs aim to provide students with a comprehensive understanding of security-related issues, strategies, and challenges, and they often focus on various aspects of security, including international security, cybersecurity, homeland security, and more.

In order to present an overview of various security study programs, the ERASMUS+ SECUREU project conducted an analysis of the programs offered by six partner institutions of higher education within the field of security. It is evident that this overview may not encompass a comprehensive understanding of security programs throughout the entirety of Europe. Nevertheless, it does afford the opportunity to compare the objectives, tasks, acquired skills, and competencies imparted by these programs across diverse European universities, encompassing Northern Europe, the Baltic States, as well as institutions situated in Central and Southern Europe. Through the scrutiny of the programs proffered by the partner institutions, commonalities as well as distinctions emerge. These findings offer an intriguing perspective on the breadth of security studies in disparate European nations and furnish insights into the integration and pedagogical approach concerning security risk management within these programs.

All 6 partner Universities offer security study programs which aim to equip students with the knowledge, skills, and attitudes necessary for careers in various aspects of security, safety, and crisis management. They also emphasize the development of professionals who can adapt to changing global and socio-economic environments.

Turiba University (Latvia) offers a Bachelor's program in Organization Security. The program aims to equip students with the necessary knowledge and skills to excel in the field of security. It focuses on fostering a deep understanding of personnel control, communication, risk assessment, crisis management, and first aid. Graduates are prepared to take on roles as heads of security services, ensuring compliance with safety regulations and effectively managing organizational security. The program places significant emphasis on practical aspects, including risk analysis and security management.

Name of the programme: Organization Security

Level: Bachelor

Duration: 4 years

ECTS: 240

Aim: To promote the formation of students' attitudes, necessary knowledge, and skills related to organizational security and prepare them for professional roles in security services.

Turiba University, Latvia

Name of the programme: Law and Economic Security	
Level: Bachelor	
Duration: 3.5 years	
ECTS: 210	
Aim: To form graduates' legal thinking, awareness and perception, to provide them with special knowledge about the principles, regularities and peculiarities of the interaction of law and economic security, to develop security business in Lithuania.	

Kazimieras Simonavicius University, Lithuania

Kazimieras Simonavičius University (Lithuania) offers a Bachelor's program in Law and Economic Security. This program aims to develop students' legal thinking and awareness, with a specific focus on the principles and intricacies of the interaction between law and economic security. Graduates are equipped with skills in business risk analysis and planning, problem-solving, legal analysis, and conflict resolution. The program covers a range of knowledge areas, including public and private law, international law, economic, risk management and information security. Graduates are prepared to engage in legal research, demonstrate ethical responsibility, and adapt to changing environment.

FUABformació
Escola de Prevenció i Seguretat Integral

Name of the programme: Prevention and Integral Safety and Security	
Level: Bachelor	
Duration: 4 years	
ECTS: 240	
Aim: To prepare students for careers in prevention and security, covering 3 large sectors such as public, private, and health and safety.	

Fundació universitat autònoma de Barcelona, Spain

Fundació Universitat Autònoma de Barcelona (Spain) offers a bachelor's degree in Prevention and Integral Safety and Security. This program aims to prepare students for careers in various sectors, including public, private, health, and safety. It offers specializations in labour security, private security management, and more. Students develop skills in labour security, hygiene, ergonomics, industrial security, and risk analysis. They gain knowledge in cybersecurity, risk prevention, and compliance with security regulations. The program focuses on competences such as ethical responsibility, adaptability, critical thinking, and effective communication.

LAU REA
AMMATTIKORKEAKOULU
University of Applied Sciences

Name of the programme: Safety, Security and Risk Management	
Level: Bachelor	
Duration: 3.5 years	
ECTS: 210	
Aim: To ensure high level of integrity and critical understanding of risk management, enabling to apply this knowledge effectively in both private and public sectors. To develop a business-oriented mindset and provide the skills needed to lead safety and security functions.	

Laurea university of applied sciences, Finland

Laurea University of Applied Sciences (Finland) offers a Bachelor's program in Safety, Security, and Risk Management. This program focuses on providing students with a strong foundation in risk management, safety, and security. Graduates are prepared to work in various roles, emphasizing a business mindset. The program covers skills in risk management, business continuity, safety and security management, organizational compliance, and sustainability. Competences developed include independent study skills, research, development, and effective communication.

avans university of applied sciences	**Name of the programme:** Integrated Safety and Security
	Level: Bachelor
	Duration: 4 years
	ECTS: 160
AVANS University of Applied Sciences The Netherlands	**Aim:** To develop students' risk management skills, focusing on safety and security in various sectors.

AVANS University of Applied Sciences (The Netherlands) offers a Bachelor's program in Integrated Safety & Security. This program aims to enhance students' risk management skills to proficiency levels. It covers subjects like security management, incident investigation, and safety/security behaviour. Graduates acquire skills in risk management, incident investigation, technology integration, and security staffing. They gain knowledge in security fundamentals, business operations, and risk management. The program emphasizes competences such as analyzing research-based knowledge, acquiring competence development knowledge, and generating innovative solutions.

NORD University	**Name of the programme:** Preparedness and emergency management
	Level: Master
	Duration: 3 years
	ECTS: 90
NORD University, Norway	**Aim:** To provide management-oriented education for personnel responsible for emergency management and crisis response. The programme targets leaders, managers and other staff holding safety and preparedness responsibilities in both public, private and voluntary organizations.

NORD University (Norway) offers a Master's program in Preparedness and Emergency Management. Geared toward leaders and professionals responsible for emergency management, the program facilitates knowledge and experience exchange. Students develop skills in analyzing preparedness strategies, conducting independent research, and utilizing IT-based management tools. The program covers knowledge areas such as preparedness systems, crisis management theories, organizational learning, and strategic communication. Competences include analyzing research-based knowledge, competence development, and creative problem-solving.

All these programs provide diverse skills and knowledge in security, risk management, and emergency preparedness, catering to various career paths within the security and safety field.

Skills

Common skills focused across programmes:

Risk assessment and management: All programs emphasize risk assessment and management to varying degrees. Students are trained to identify, evaluate, and manage risks related to safety, security, and emergency situations.

Communication skills: Effective communication is a key skill across programs. Students learn to communicate with colleagues, clients, and other stakeholders during crisis situations and in normal

operations. Students must be capable of communicating information, ideas, problems and solutions to both specialised and non-specialised audiences.

Ethical responsibility: Ethical considerations are integrated into the programs. Students are taught to act with ethical responsibility, respecting fundamental rights, and adhering to legal and ethical standards.

Critical thinking: Critical thinking is fostered, allowing students to analyze situations, assess risks, and make informed decisions. It is essential for students to be able to evaluate the technical, social and legal impact of new scientific discoveries and new technological developments. This skill is crucial in emergency management and risk assessment.

Analytical skills: Analytical skills are honed to evaluate data, research problems, and make data-driven decisions in the context of security, safety, and risk management.

Common competencies reflect the multifaceted nature of security and risk management programs, which aim to equip students with a diverse set of skills and knowledge to address complex challenges in the field of security and risk management effectively. These competences include legal, economic, technological, and leadership aspects, as well as the ability to adapt to changing environments and effectively manage risks.

Not all universities offer courses explicitly named "Security risk assessment and management," they do provide education in related areas, including risk assessment, security planning, crisis management, and compliance requirements. Students in these programs are likely to gain a strong foundation in security and risk management practices, which can be applied to various professional contexts.

Some of the partner universities offer dedicated courses on security risk assessment and management, while others have a broader focus on emergency management and related topics. The specific methods used and the amount of coverage may vary between programs.

In the self-assessment process of the security study programs, we engaged both lecturers and recent graduates, including last year's students and alumni. We collected **feedback** from them regarding the strengths and weaknesses of the study programs, as well as their insights into their knowledge and skills in security risk management. In total, there were **16 lecturers** and **36 students/alumni** who participated in the feedback surveys across these six universities.

Based on the feedback provided by lecturers and alumni from the six universities, we can identify common strong sides and areas for improvement.

Common strong sides:

Theoretical knowledge: Across several universities, lecturers highlight that students have a strong theoretical knowledge of security and risk management concepts. This theoretical foundation seems to be a key strength.

Broad knowledge: Many universities emphasize that their programs provide students with broad knowledge of different topics within the security field. This is valuable for students' overall understanding of the subject.

Analytical skills: Students are praised for their ability to assess risks in organizations and analyze information to identify regularities. These analytical skills are considered strong.

Practical insights: In some universities, lecturers appreciate that professionals from the security industry contribute to the program, offering practical insights and real-world experience.

Interdisciplinary skills: Multiple universities mention the importance of interdisciplinary skills, which help students understand security in a holistic way and apply knowledge across various domains.

Teamwork and collaboration: Students are recognized for their ability to work in teams and engage with real-world clients or situations, improving their collaboration skills.

Common areas for improvement:

Presentation and communication skills: Weaknesses in presentation and public speaking skills are noted by several universities. Effective communication skills, which are crucial for leadership roles, are an area for improvement.

Digital literacy: Some universities suggest that students need to enhance their digital literacy skills, which are increasingly important in the field of security, especially in areas like cybersecurity.

Stress management skills: Stress management skills are highlighted as an area that could be improved. This is particularly relevant in high-pressure security and risk management roles.

Specific technological knowledge: Students express a need for more intensive coverage of new technologies, including radio, communication systems, transmission, and digital signals.

Personnel and human resource management: Alumni suggest a more in-depth focus on personnel management and human resource management, which are crucial aspects of security organizations.

Cybersecurity and data protection: Several alumni recommend adding courses in cybersecurity and data protection to the program, reflecting the increasing importance of these areas.

Security systems and technologies: The inclusion of courses related to security systems and technologies is suggested to keep students updated on the latest security tools and solutions.

International security law: Some universities propose adding courses on international security law to provide students with a more comprehensive understanding of global security issues.
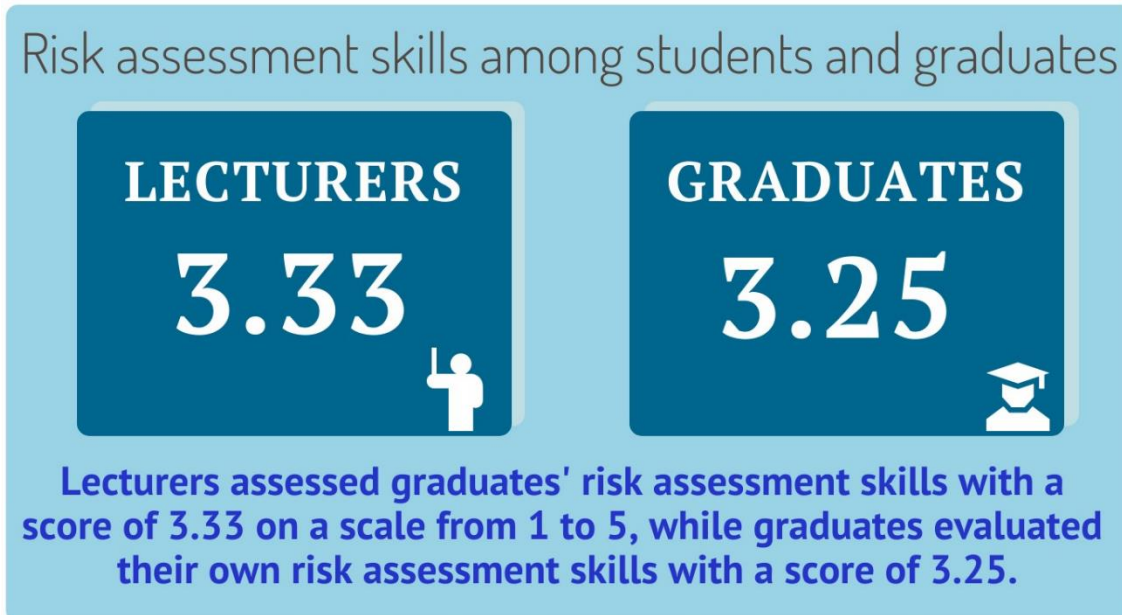
Practical application: Alumni suggest that the program should include more practical, hands-on experiences related to implementing security measures and responding to real-world security challenges.

Environmental safety: In some cases, alumni express the need for more content related to environmental safety and sustainability, reflecting the growing focus on these aspects in the security field.

We also asked feedback from lecturers regarding the evaluation of **risk assessment skills** among students and alumni. The average assessment score was 3.33. It is evident that lecturers perceive the risk assessment skills of students and alumni as average, indicating that there is room for improvement.

In addition, students and alumni self-assessed their risk assessment skills with an average score of 3.25. This suggests that students and alumni themselves recognize the potential for

improvement in their risk assessment and management abilities. Consequently, it underscores the need for the inclusion of risk management courses and the expansion of programs that encompass the development of topics and practical skills pertaining to risk management within higher education curricula.

Risk assessment skills among students and graduates

LECTURERS
3.33

GRADUATES
3.25

Lecturers assessed graduates' risk assessment skills with a score of 3.33 on a scale from 1 to 5, while graduates evaluated their own risk assessment skills with a score of 3.25.

In conclusion, the feedback from both lecturers and alumni across six universities highlights several common strengths and areas for improvement in security and risk management programs. Strong theoretical foundations, broad knowledge, analytical skills, and interdisciplinary approaches are consistent strengths, underlining the academic rigor of these programs. However, there is a shared need for improvements in communication and digital literacy skills, stress management, and practical application. The future of security studies appears to be evolving towards greater emphasis on emerging technologies, including cybersecurity, environmental considerations, and international perspectives, reflecting the ever-changing landscape of security challenges. To remain relevant and prepare students effectively for careers in security, universities should consider incorporating these aspects into their curricula while fostering practical experiences and strong industry collaborations.

3. SKILLS AND KNOWLEDGE OF A SECURITY SPECIALIST

3.1. Skills identified by experts in round table discussions across six countries

The main aim of organising 6 round table discussions in Latvia, Lithuania, Finland, Spain, the Netherlands and Norway was to gather security and risk management specialists and to ask their opinion about questions like what should be taught to young security specialists, what skills are missing, what the future perspectives and perceived risks are for the security field and for the security specialist profession in general.

7 events were organised in summer and autumn 2022:
8th June 2022, Riga, **Latvia,** Turiba University
17th June 2022, **Finland**, Laurea University
1st July and 29th August, 2022, Bodo, **Norway**, Nord University
13th September 2022, Barcelona, **Spain,** School of Prevention and Integral Safety and Security
22nd September 2022, Vilnius, **Lithuania**, Kazimieras Simonavičius University
23rd September 2022, Den Bosch, **the Netherlands**, Avans University of applied science

The participants were security specialists from various institutions and companies as well as academics and lecturers from partner Universities. Among the participants there were representatives from many Retail and Service industry enterprises, Police, a Joint Emergency Services Call Centre, Social Insurance Institutions, Regional Health Authorities, Air Forces. In total 48 experts took part in those events and contributed to the content of this report.

It appears that countries worldwide are grappling with similar challenges, and the perspectives of the experts regarding the essential skills of security specialists, as well as the future of the security field itself, exhibit remarkable similarity.

Experts from various countries have emphasized several common skill sets that hold significant importance for aspiring security specialists. These include soft skills, strategic thinking, and strategic management, as well as enhanced overall management skills and leadership abilities. Furthermore, there is a pressing need for the development of capabilities related to information security, cybersecurity, and technological and digital literacy.

Experts from all countries highlighted several similarities and skills' groups which are important for young security specialists, no matter which country they come from:

Strategy	Strategic thinking, strategic management, understanding organisation's strategy, ability to balance business risks and security risks, holistic view.
Management	Better management skills, organisational skills, leadership skills.
Soft skills	Importance of soft skills – communication (including interaction and dealing with different generations, knowledge about generation studies, active listening, argumentation) critical thinking, media literacy.
IT, cyber-security	Ability to manage information security, cyber-security, technological and digital literacy.

Practice	More practice in the study process. More problem based education.
Basics	At the same time it is vital not to neglect or exclude very basic information about security in the study process.

Experts also deliberated on and proposed the qualities that make a security professional an effective member of a security team. In response to this question, experts from all six countries shared similar opinions. They frequently underscored the importance of various soft skills, management abilities, and strategic thinking skills. Here is a summary of the insights from each country.

LATVIA
Ability to orientate in different situations, different security systems and issues in the broadest sense. Ability to communicate and collaborate; substantiate and argue their own point of view.

LITHUANIA
Constantly learning, improving qualifications and seeking new knowledge.
Being motivated and willing to work in the chosen security profession, being able to creatively apply acquired knowledge in daily activities.
Dutifulness and responsibility in carrying out assigned security tasks (security projects) and bringing them to final results.
Ability to communicate with the organization, i.e. a security professional cannot retreat to his assigned function field and think about security narrowly; the security product created should be used in the full scope of the organization's activities and operations.
Understanding the organization's business model and helping achieve the organization's goals through the protection of the organization's resources (human, material, digital, etc.).

SPAIN
Soft skills related to proximity, to the extent that this is the model that requires most implementation.
Organizational intelligence in the field of proximity. Analysis of citizens' needs from the proximity model. Analysis of insecurity from proximity.
Working the predictive policing model. Interpreting citizens' needs.

FINLAND
Enthusiasm about the mission of the organization; committed to the strategy and goals of the organization, understanding that they are supporting it; interested in development, to do better, courage to change things.
Wide experience, also beyond the required core; project working skills; a service attitude - understanding that security is a supporting function; social skills, cooperation skills, deep knowledge in one's own area – and recognising when you don't know something.

THE NETHERLANDS
Ability to reinforce positive security behaviour. Investigative skills and asking thorough follow up questions. Awareness of threats related to using technical elements such as cameras, apps, software. Better than average understanding about primary processes, especially in IT and IT security.
Entrepreneurial spirit, analysing & conceptual thinking capabilities, knowledge about applying LEAN.

NORWAY

Collaboration and team working, communication abilities and justifying their action with valid arguments; problem-solving, ability to approach a problem systematically, analytical capacities to look critical on things and to ask questions, team management and people management skills, to learn fast and be realistic, open to learning from failures, to connect educational content, general concepts to practical use.

Additionally, the experts analysed the most significant weaknesses and «shortcomings» in security professionals today. Here, you'll find a visualization of the primary findings:
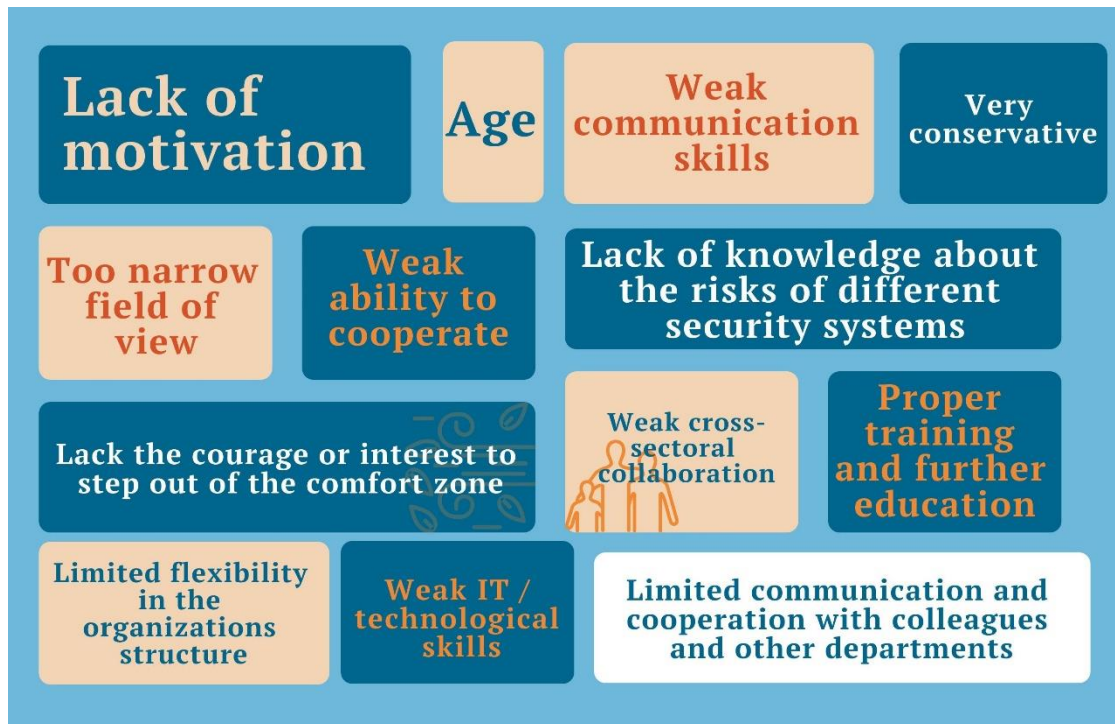
The experts also discussed the future of the security field. The future for the security field is information technologies, artificial intelligence and business analytics, cross-sectoral skills, building links between business and security, cyber security, data security, and technology literacy.

Specialists will need to be able to work with a wide variety of stakeholders. Security staff will need to get out of the "bubble" and avoid doing security for security's sake. They will be required to understand interdependencies of various functions within the organization and outside the organization.

Business continuity is more and more dependent on IT. More and more processes are automated, resumption time is slowly decreasing. However, everything is interdependent and therefore there is increased vulnerability, particularly after Covid-19.

In the future, physical security will become less significant as a permanent function of the organization, the digitalization of the organization's business processes will cause a greater need for cyber security specialists and analytics of security information. Security professionals with data analytics and cross-sectoral knowledge and skills, who are able to apply the processed data in the decision-making process using artificial intelligence tools will be in demand on the security business

market. In the security business, the executors of security functions perform more of a "firewall" function when security officers extinguish security incidents that have already occurred. However, in the future, the area of integrated security risk and compliance management will become dominant in the security market, i.e. specialists with a broad spectrum of knowledge and skills regarding applying security requirements, who are able to identify, assess and manage security risk, to set and take actions addressing the identified risk, etc.

The labour market will demand specialists who have knowledge of risk and compliance management in order to ensure sustainable and high-quality provision of security services to the organization. The ability to understand the opportunities of integrating different security systems, their impact on the organization's activities and benefits, and the ability to work with various data that are relevant to the organization (analyse, compare, draw conclusions and provide solutions on how to effectively manage risks with acceptable costs to the organization). In the future, various Security Competence Centres (HUBs) will be in high demand as security service providers, as it will become very expensive for organizations to have and retain security specialists with narrow professional expertise.

Within business continuity management there is a big move towards new platforms, networks and applications, for example, salary payments. Many different types of software or apps are involved, proxy systems, credentials checking, third parties, banks etc. These can be inside or outside the organisation. This 'landscape of applications' needs housekeeping in order to prevent large impact in case of, let's say, a ransomware attack, to avoid a domino effect.

There is too much IT involved in the future and we already need to be so broadly developed in what we know: BCM, physical security, security culture etc. Sometimes even combined with safety management. Moreover, information security differs from IT security, and differs from Cyber security.

Full report can be found **HERE**

3.2. Skills identified by the CONRIS network for security and safety specialists

The CONRIS Network, which stands for Cooperation Network for Risk, Safety & Security Studies, is a collaborative network focused on research and studies related to risk, safety, and security.

CONRIS is a network of universities with accredited degree programs in risk, safety & security management. CONRIS aims at increasing safety and security in Europe through collaboration in education and research.

The network brings together researchers, experts, and professionals from various disciplines and organizations to share knowledge, exchange ideas, and collaborate on projects related to risk assessment, safety management, and security practices. There are 18 members in this networks from Finland, Belgium, Norway, the Netherlands, Spain, Germany, Poland, Austria, Croatia, United Kingdom, Portugal, Bulgaria, and Italy.

The SECUREU partnership organized an international discussion with the CONRIS network members. These discussions were held 2nd of July 2022 during a hybrid CONRIS meeting. Two round tables

were organized in 's-Hertogenbosch (the Netherlands) and one - online, with the online participants. The three group discussions focused on the skills and qualities required for young security professionals, the qualities of good security team members, and the knowledge, skillset, and awareness needed in the security business in the next 3 to 7 years

The discussions highlighted various **skills and qualities that are lacking in young security professionals**. It is noteworthy that many of these pertain to metaskills and qualities that should be improved, besides providing them with deeper expertise in the field. Addressing these gaps can help enhance the overall effectiveness of young security professionals in their roles.

Experts identified following skills:

- Lack of tolerance for **different cultures** and an inability to **actively listen** to others with diverse backgrounds and priorities;
- Limited understanding of **security terminology** and differing perspectives on what security means to different individuals;
- Insufficient **critical thinking** skills;
- Need for the **ability to question actions** and consider the intelligence of one's decisions;
- Lack of **knowledge in risk management** and related specialized subjects;
- Inconsistent **ethical sensibilities;**
- Awareness of importance of **questioning assumptions**, **considering uncertainties**, and understanding that not everything goes according to plan;
- Personal **leadership skills**, which may not be initially recognized by new students but become apparent later on;
- **Mental and physical resilience;**
- Bridging **the gap between theoretical learning and practical application** to understand the significance of acquired knowledge;
- Incorporating **practical learning experiences** into teaching, focusing on aspects that cannot be easily self-taught
- Familiarity with relevant **cybersecurity technologies** and terminologies.

CONRIS network experts also discussed what qualities a security professional has that make him/her a good member of a security team. Experts concluded that all qualities may be divided into three groups: analytical, creativity and ethical. These qualities collectively contribute to the effectiveness and success of a security team.

☞ **Clear communication** using appropriate disciplinary and professional language;

☞ Consideration of different personalities within a team and **effective team management;**

☞ **Awareness of potential differences** between security teams and other types of teams, including time constraints;
Strong **analytical skills** to critically assess situations, ask relevant questions, and consider grey areas;

☞ **Fast learning** and a realistic approach, being open to **learning from failures;**

☞ **Valuing cooperation and networking** for effective security management;

☞ Ability to **communicate the economic background** of security, understanding the costs involved, and the advantage of collaborative approaches to security issues;

☞ Connecting educational content and general concepts to practical use, emphasizing the **application of theory**. Security managers should have the ability to translate general knowledge into specific security domains, such as cyber security, using a specialized professional language;

☞ Demonstration of integrity and confidence in **decision-making;**

☞ **Critical thinking** in decision-making while operating within time constraints;

☞ Skills to **integrate artificial intelligence** (AI) into security practices, given the increasing reliance on computer support, data, and analytics. Developing analytical abilities to integrate multiple measures and information, including big data;

☞ **Creativity skills,** including self-reflection, fostering teamwork, and collaboration. Utilizing software programs creatively, as computers based on AI can generate any picture, but it is the team of professionals who must imagine and develop ideas;

☞ **Personal skills** related to security management roles, including **coordination** and implementing team measures effectively;

☞ **Ethical qualities** that prevent common failures in security management, such as misuse of power and arrogance. Prioritization and consideration of internal and external motivations.

Experts discussed **what knowledge, skillset, awareness is needed in the security business** taking into account a **3 years' experience** perspective. Here is a data visualisation:
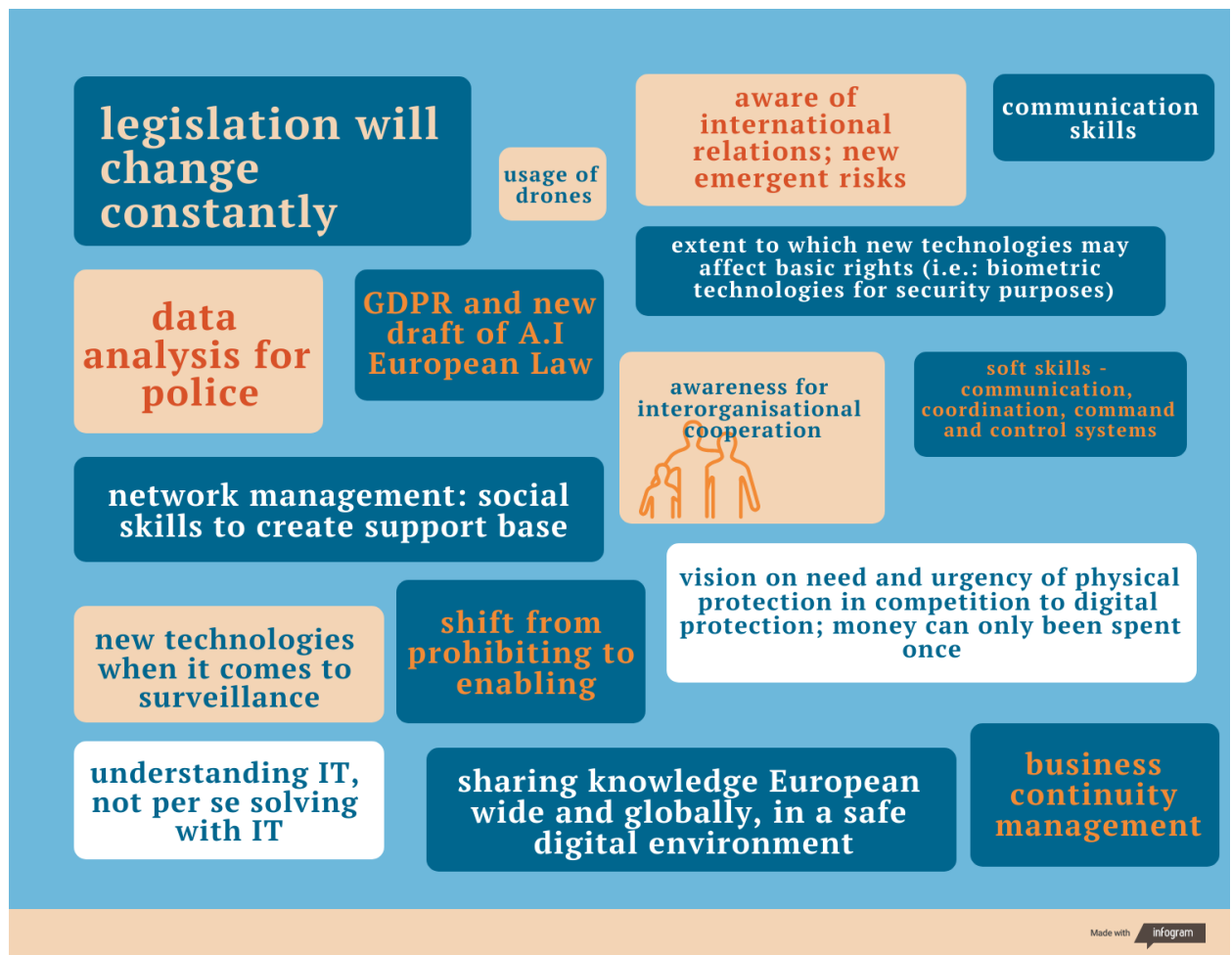
Knowledge, skillset, awareness needed in security business – **5 to 7 years' perspective:**
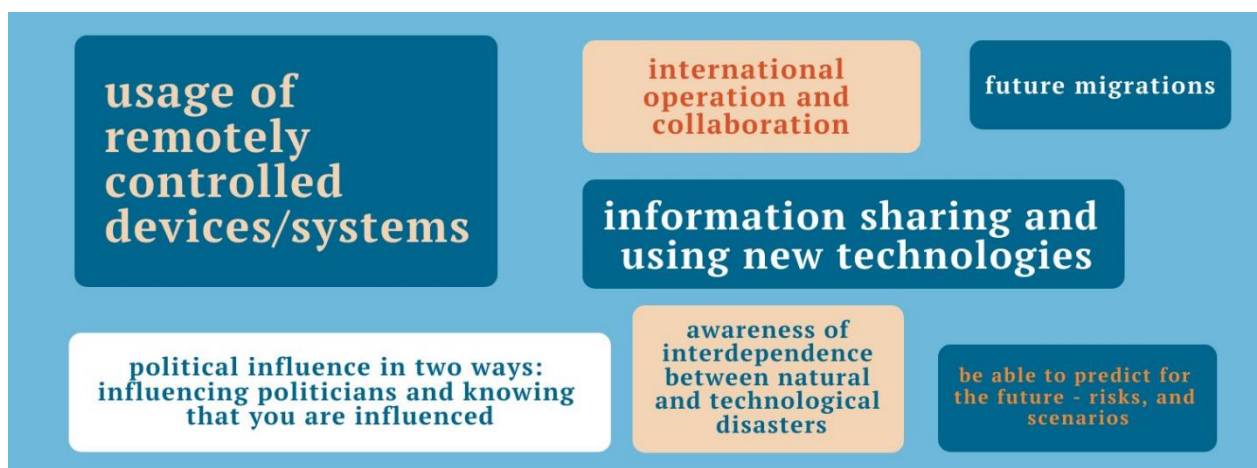
4. INTERNATIONAL STANDARDS (ISO, COSO, ERM)

4.1. Introduction to ISO, COSO, ERM

ISO

ISO is a global standard for trusted goods and services. Standards define what great looks like, setting consistent benchmarks for businesses and consumers alike — ensuring reliability, building trust, and simplifying choices. International standards ensure that the products and services you use daily are safe, reliable, and of high quality. They also guide businesses in adopting sustainable and ethical practices, helping to create a future where your purchases not only perform excellently but also safeguard our planet. In essence, standards seamlessly blend quality with conscience, enhancing your everyday experiences and choices.

ISO 31000:2018 is a Risk management standard. This document is for use by people who create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance. Organizations of all types and sizes face external and internal factors and influences that make it uncertain whether they will achieve their objectives.

Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions. Managing risk is part of governance and leadership, and is fundamental to how the organization is managed at all levels. It contributes to the improvement of management systems. Managing risk is part of all activities associated with an organization and includes interaction with stakeholders. Managing risk considers the external and internal context of the organization, including human behaviour and cultural factors.

When evaluating the risks of organizations and companies, we can look at them by dividing them into segments, such as:

Enterprise risk management
Management, Risk and Liability
Operational risk management
Project, program and portfolio risk management
Political risk management
Reputation risk management
Supply chain risk management
Business continuity risk management
Risk management of owners, investors and lenders (stakeholders)
Ethical risk management
Cyber risk management
Financial risk management

And, of course, **security risk management**, which is important and is part of all the segments mentioned above. Managing risk is based on the principles, framework and process outlined in this ISO Standard 31000:2018 document, as illustrated in the figure below. These components might already exist in full or in part within the organization, however, they might need to be adapted or improved so that managing risk is efficient, effective and consistent.

Principles (clause 4)

Framework (clause 5)

Process (clause 6)
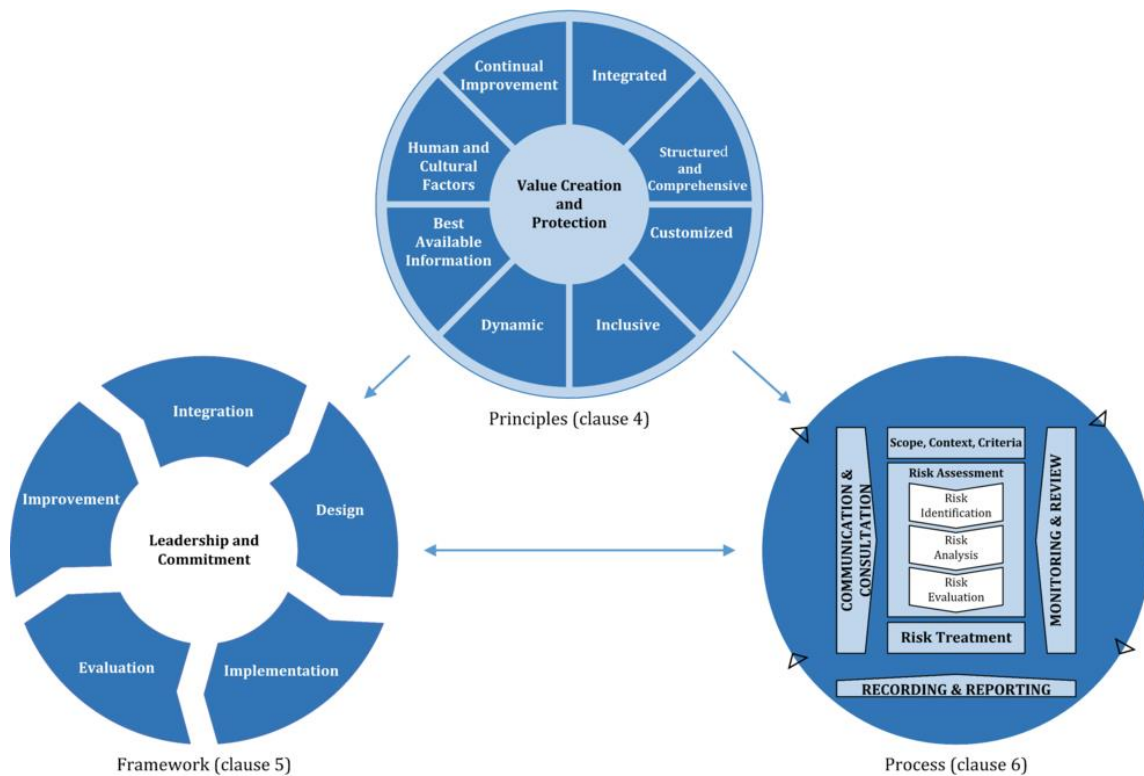
COSO-ERM

Following all kinds of accounting scandals and fraud cases in large organizations, the need arose around the turn of the century to issue a guideline to support management in improving the internal control system for internal control. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed the Enterprise Risk Management Framework (COSO-ERM 2017) for this purpose. The COSO-ERM 2017 is a framework containing a systematic arrangement of organizational objectives, control components and activities to help companies and other organizations assess and improve internal control systems. The starting point of the model is that the company deals responsibly with risks that are inextricably linked to achieving the corporate objectives. To achieve this, the risks must be identified and appropriate measures taken, in line with the risk attitude of management. This makes the COSO-ERM 2017 a risk management system that focuses on the interaction between risk, performance, strategy and value.

The COSO-ERM 2017 is not a function or department within an organization, it is 'the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving , and realizing value' (Enterprise Risk Management Integrating with Strategy and Performance, 2017, p. 3). It goes further than an inventory of the possible risks by management. The COSO-ERM 2017 is broader than a risk inventory and consists of active management of risk management by management, which is visible within all organizational layers.

An appropriate information system is in line with the processes that need to be monitored and is in principle not a stand-alone system within an organization. It is connected to other internal and external systems and therefore the connection with the other systems is a point of attention. But of course the system must above all generate reliable information and this requires

organizational measures. To achieve that we can use the Three Lines model, which is part of the COSO-ERM.

The risk management process is of great importance for the security expert because it determines their position and the work to be carried out. Management will want to be continuously informed about the actual state of affairs within the organization and any deviations observed compared to the set goals. To this end, the security expert must have an information system that is appropriate for the activities and the risks identified. The lack of an appropriate information system prevents the security expert from taking necessary actions if necessary.

4.2. Why is it important to teach and use those standards in security risk management education?

The models are important because they create a common framework for security officers and other stakeholders to address and discuss risk management issues and to take actionable measures. Precisely because of the differing interests within organizations and between organizations, it is important that specialists do not merely speak their own language, which makes communication difficult. By paying attention to this during the training, security officers are trained to speak that universal language and to be able to weigh the different interests against each other in a balanced way.

It is also important to teach these standards so that security professionals have tools and proven systems on the basis of which the organization can build an internal security system and work with security risks to avoid major crises with severe consequences.

4.3. How to link security specialists with Administrative Organization, reference to standards

Risk management is based on information processing, where the information is created on the basis of data from the processes that take place within an organization. For this reason, a security officer must understand the administrative organization, the way in which processes are designed and managed. This can be done on the basis of own observations, but must also be based on overviews that show the processes within the entire organization. These overviews are suitable for identifying risks within the processes and for agreeing with other stakeholders within the organization who are responsible for managing those risks. Based on the tasks, authorities and responsibilities for the processes, it can be determined whether and to what extent the security officer is responsible for processes and the associated risks or whether other line or staff officers are primarily responsible. This prevents the security officer from being addressed as responsible for a process, while that responsibility is placed elsewhere.

5. RECOMMENDATIONS FOR DEVELOPMENT OF STUDY AND TRAINING PROGRAMMES FOR SECURITY SPECIALISTS

5.1. Body of knowledge and skills

The Security professional needs a strong knowledge base and mastery of competencies to be able to carry out their work. On the one hand, in order to be able to carry out the various tasks and to establish cooperation with relevant parties, there is a need for Security professionals who can delve into certain security themes and therefore develop into specialists. This means that the modules must at minimum provide a good introduction to the disciplines. Many Security professionals are not specialists in a field, but must be able to unlock the knowledge of specialists.

Regarding the breadth of the Body of Knowledge and Body of Skills for the work field of the Security professional, roughly the following classification can be made:

Tools for the Security professional; concepts, policy, governance, culture, collaboration, communication, design, research.

Partners for the Security professional; citizens, administrative levels, administrative bodies, justice and police, armed forces, private security and security management, private executive management.

Work areas of the security professional; crime, information security, terrorism, disasters/crises, industry, transportation, retail, events, water.

This classification is based on the results of the survey for the Standards for Security Specialists / Profession including National professional and education profiles and Roundtable discussions per participating university in the SECUREU project.

In practice, due to the diverse Body of Knowledge and Skills, security management can be classified in many different ways. Universities sometimes choose to focus on a specific subject or theme within the context of the Security work field and select the relevant Body of Knowledge and Skills. Each university does this in its own way.

BODY OF KNOWLEDGE	
SECURITY BASICS	• Trends and developments in the field of security • Security in an international perspective (e.g. sustainability, Sustainable Development Goals) • Security concepts (e.g. social security, physical security, security, security, environmental security, information security, objective and subjective security, security perception, security chain, resilience)
SECURITY, MANAGEMENT AND ORGANIZATION	• Systems thinking • Quality management • Organizational Science • Change Management • Security management • Project Management • Crisis management • Information security management • Risk management • Cyber security management • Business continuity
SECURITY AND GOVERNANCE	• Policy science • Public administration • Political science
SECURITY, ECONOMY AND OPERATIONS	• Administrative organization • Cost-benefit analysis • Social cost-benefit analysis
SECURITY AND JUSTICE	• Criminal law • Environmental law • Occupational safety law • Private law • Municipal law • Privacy law
SECURITY AND BEHAVIOUR	• Criminology • Ethics • Sociology • Security culture • Psychology
SECURITY AND COMMUNICATION	• Crisis communication • Risk communication • Intercultural communication
SECURITY AND RESEARCH	• Incident investigation • Risk analysis • Qualitative and quantitative research methods

BODY OF SKILLS	
ANALYTICAL AND INVESTIGATIVE SKILLS	The Security professional has research skills and thinks critically, can systematically search for the answer to the central question in every phase of the action cycle, and can provide insight into this method and accountability. The Security professional has the ability to analyse complex problems and to distinguish between main and secondary issues. He can structure information and, if necessary, restructure it and see connections, substantiate conclusions and oversee consequences. In addition, the Security professional is able to analyse and interpret data from management information systems in terms of risks. The Security professional can make an assessment of whether information is correct.
DECISIVENESS	The Security professional has the ability to arrive at realistic, substantiated and useful conclusions about possible alternatives, based on available information. The Security professional can take a well-considered position and make decisions after consultation. Not only in clear but also in more diffuse situations, where not all factors are fully known or transparent. The Security professional must be able to balance between providing sufficient protection on the one hand and accepting acceptable risks on the other. He must be able to make trade-offs when taking security measures that affect privacy.
COMMUNICATION	The Security professional has the ability to convey information about risks, ideas and solutions in a targeted and clear manner to an audience consisting of specialists and/or non-specialists. He can adequately deal with various communicative situations and communication partners. He can use various means effectively in information and communication, and make effective use of the possibilities offered by ICT. The Security professional is aware of their style of communication in different roles, for example the role of advisor or director. They can build a relationship of trust with a client and other parties involved, and support the thinking at a strategic level: the question behind the question. The Security professional can respond to resistance and uncertainties, and turn them into commitment. They dare to confront if necessary and know how to maintain the relationship of trust.
INNOVATIVE CAPACITY	When solving problems, the Security professional has a curious and inquisitive point of view and is able to approach security issues from different angles and thereby break established thinking patterns. They are able to translate methods and instruments developed elsewhere into the specific practical situation of the client. The Security professional has a broad view of the world, is open to innovations and sees coherence between their own work and other disciplines.

LEADERSHIP	Self-regulation is a first form of leadership: the Security professional is able to respond to changes in the context in which they work, and to further professionalize themselves to remain employable. In addition, the Security professional shows leadership in dealing with other professionals. In this way, they can lead dialogues and discussions about the security policy to be implemented and about the long-term perspective on the security of the organization. They know how to create involvement within the organization around security policy. The Security professional has the qualities to lead teams and groups in a results-oriented way, taking into account both the task-oriented and the people-oriented aspects. They are team-oriented, create support and contribute to team bonding and the 'we-feeling'.
ORGANIZATIONAL AND SITUATIONAL AWARENESS	The Security professional identifies relevant developments in the environment of the organization, can anticipate them and is able to translate these into policy. They use this knowledge to advice for the benefit of the organization and/or their own field of expertise. The security expert can estimate, understand and knows how to act on the relationships and effects of the political and administrative force field inside and outside the organization.
REFLECTIVE ABILITY	The Security professional is self-critical and able to oversee their role with regard to the social interest. The Security professional can look back in a structured way and reflect on their own professional actions and draw lessons from them. The Security professional appreciates the social consequences of security problems and solutions. They can find a reasoned balance between different values such as freedom and equality or innovation and continuity.
FOCUS ON RESULTS	The Security professional is able to set concrete goals and determine priorities. They can weigh how much time is involved in the work and what activities and resources are needed to achieve those goals.
COOPERATE	The Security professional has the willingness and ability to work together with others on security in a multidisciplinary and multicultural environment, to support those involved in achieving the common objectives. The Security professional can balance between different interests, transfer the right information, place trust in other parties and encourage them to share their knowledge and skills. The Security professional is able to establish, build and maintain contacts with other professionals and agencies, and to share information and expertise with the aim of working in a safe(r) environment.

Body of Knowledge and Skills for Security Specialists

KNOWLEDGE

SECURITY BASICS

- Trends and developments in the field of security
- Security in an international perspective (e.g. sustainability, Sustainable Development Goals)
- Security concepts (e.g. social security, physical security, environmental security, information security, objective and subjective security, security perception, security chain, resilience)

SECURITY AND GOVERNANCE

- Policy science
- Public administration
- Political science

SECURITY AND JUSTICE

- Criminal law
- Occupational safety law
- Privacy law
- Environmental law
- Municipal law
- Private law

SECURITY AND COMMUNICATION

- Crisis communication
- Risk communication
- Intercultural communication

SECURITY, MANAGEMENT AND ORGANIZATION

- Systems thinking
- Organizational Science
- Security management
- Information management
- Risk management
- Business continuity
- Quality management
- Change Management
- Project Management
- Crisis management
- Cyber security management

SECURITY, ECONOMY AND OPERATIONS

- Administrative organization
- Cost-benefit analysis
- Social cost-benefit analysis

SECURITY AND BEHAVIOUR

- Criminology
- Sociology
- Psychology
- Ethics
- Security culture

SECURITY AND RESEARCH

- Incident investigation
- Risk analysis
- Qualitative and quantitative research methods

More on:
http://security.turiba.lv

34

Body of Knowledge and Skills for Security Specialists

SKILLS

ANALYTICAL AND INVESTIGATIVE SKILLS

- Critical thinking
- Analysing complex problems
- Structuring information
- Data analysis and interpretation
- Assessing information

COMMUNICATION

- Communicating information to different audiences
- Managing various communication situations
- Effective use of ICT
- Using communication techniques
- Resolving conflicts
- Building trust with clients/employees

LEADERSHIP

- Self-regulation and ability to respond to contextual changes
- Excellent interpersonal skills Leading discussions and dialogues, fostering involvement
- Team management
- Setting and achieving team goals
- Providing support, creating trust, and fostering a sense of unity

FOCUS ON RESULTS

- Setting goals and priorities
- Assessing and planning resources
- Planning and structuring

DECISIVENESS

- Making conclusions
- Evaluating alternatives
- Listening to others and making decisions after consultation
- Balancing security and business risks

INNOVATIVE CAPACITY

- Curiosity, desire to learn
- Development and adaptation of new methods and tools
- Openness, broad perspective, interdisciplinarity
- Open to innovations

ORGANIZATIONAL AND SITUATIONAL AWARENESS

- Analyzing situations
- Planning, formulating, and implementing policies

REFLECTIVE ABILITY

- Self-criticism
- Structured analysis of past experiences
- Analyzing the social consequences of security problems
- Value analysis

COOPERATE

- Cooperating with others
- Working in a multidisciplinary and multicultural environment
- Transferring information
- Balancing different interests
- Sharing information, knowledge, and experience

http://security.turiba.lv

5.2. Methods and approaches, tools, best practices

Pedagogical approaches

Pedagogical approaches for the training of security professionals start from various social constructivist viewpoints. One such perspective is cognitive constructivism. According to this framework, cognitive and physical activity lies at the core of effective learning, and teaching should be grounded in students' prior understanding. By employing active learning methods, students construct knowledge, assimilate new information, and broaden their perspectives. Physical engagement and sensory experiences stimulate critical thinking. In essence, engaging students in thought-provoking activities fosters meaningful learning.

Additionally, the social constructivist view emphasizes the value of discussions and collaborative learning. For security professionals, creating an environment in which students can interact with peers, educators, and subject matter experts is crucial. These interactions allow for diverse interpretations of given scenarios based on varying experiences and interests.

For decades, problem-based learning approaches have championed experiential learning and experience-based education. This method centres around students actively engaging in facilitated problem-solving. Instead of the traditional approach where a teacher deals out facts and concepts to a passive classroom, students struggle with real-world problems that lack a single straightforward solution. Collaborating in groups, students identify the knowledge and skills necessary to handle these challenges. Teachers have the role of a facilitator, guiding students toward discovery and deeper understanding.

Exercises as Effective Tools for Experiential Learning

Discussion-based exercises serve as a particularly effective learning method. They contribute to enhancing security risk management capabilities. By creating conversational spaces, team members can reflect on their collective experiences and discuss potential response actions. To optimize the learning outcomes of such exercises, it is essential to provide a safe and realistic environment that mirrors the complexity of real-world situations during training.

Exercises play a crucial role in experiential learning for teams. To maximize their impact, several considerations come into play:

1. Preparation for Educators:

- **Realistic Scenarios:** A well-designed exercise should mirror real-world situations, allowing participants to immerse themselves in experiences closely similar to actual events. Realism is key to providing learners with valuable insights.

- **Pre-Exercise Materials**: Teachers must meticulously prepare pre-exercise materials. These include risk management plans and detailed information about exercise delivery and structure.

- **Investigating Realism**: Educators should assess the realism of the exercise. This involves ensuring that the tasks presented do align with the scenarios in the professional practice, as well as considering how practitioners would be affected in real-life situations.

- **Regular Exercise Integration:** Planning for regular exercises within a course or semester ensures consistent learning opportunities.

- o **Leveraging Digital Tools:** Various tools may be used for facilitating collaborative learning allowing students to discuss their experiences with peers, gaining diverse perspectives. Some digital tools may support reflective processes, allowing students to engage in knowledge acquisition and self-assessment.

2. **Student Commitment and Engagement:**

- o **Concrete Experiences:** Students should actively engage in the exercise, seeking concrete experiences within their teams. Hands-on participation fosters deeper understanding.

- o **Reflection and Conversation**: Encouraging reflection and open dialogue about exercise experiences allows learners to process and learn from their actions.

- o **Critical Thinking:** Students should analyze their team's work critically, exploring alternative approaches and solutions.

- o **Benefits for Experienced Practitioners:** Even experienced professionals can enhance their skills through well- structured exercises.

In summary, exercises, when thoughtfully designed and integrated, contribute significantly to the development of security professionals' competencies. By combining realism, active participation, and digital resources, educators can create impactful learning experiences.

Best practice example

As an illustrative example, the Centre for Crisis Management and Collaboration at Nord University (Norway) employs various exercise types, each serving distinct learning objectives, levels of realism, and designs. Here are the key exercise categories:

1. **Discussion-Based Exercises:**
   - o **Format**: Participants collaboratively explore solutions, share insights, and refine their understanding of risk management roles and procedures.
   - o **Focus**: These exercises engage participants in facilitated discussions, simulating how they would tackle challenges presented in exercise scenarios.
   - o **Learning outcome**: Familiarize participants with security risks analyses and emergency plans, roles, and responsibilities.
2. **Functional or Command-Post Exercises:**
   - o **Format**: Participants operate in a simulated command-post environment, responding to unfolding events and coordinating resources.
   - o **Focus**: These exercises emphasize testing situational awareness, coordination, command, and control within a potential security unit.
   - o **Learning outcome**: Enhanced decision-making skills and effective communication during high-risk situations.

3. **Full-Scale Exercises:**
   - o **Format**: Participants face realistic scenarios that mirror actual emergency situations.

- o **Focus**: These comprehensive exercises evaluate all major functions specified for security risk professionals.
- o **Learning outcome**: Validate the effectiveness of emergency response procedures, resource allocation, and inter-agency collaboration.

Strategically employing various exercise types, security risk management professionals enhance their capabilities and contribute to effective emergency preparedness.

Practical exercises help to train skills and knowledge in security risk management field. Continuity in exercises involves regular, ongoing practice over time. Developing a long-term plan for exercising different aspects of risk management and improving the skills of security professionals proves highly advantageous.

5.3. Recommendations for further education

Further education after a Bachelor's degree in Security Risk Management can take many forms. Lifelong learning is almost a required aspect of a security professional's life, as the security landscape and especially technology evolve rapidly. New threats are discovered constantly, as societies benefit from the opportunities offered by digitalization, free trade and movement, social media, generative technologies, et cetera.

Focussing on education, specifically a more formal lifelong learning, there are a few types that could be mentioned:

- Formal higher education degrees above Bachelor, i.e. a Master's degree or a Doctorate. Universities and universities of applied sciences, such as those participating in the SECUREU project, offer these degrees. The duration of a Master's degree is usually approximately half the duration of a Bachelor's degree.
- Informal higher education, such as open university courses offered by higher education institutions. Many universities or universities of applied sciences can offer singular courses. Someone with a bachelor's degree may choose to attend new bachelor studies that they have not yet attended as part of their degree, to update and upgrade their competence. One could also take study units comparable to master's degree studies in preparation for entry to a formal Master's degree programme.
- Formal or structured certifications, which are popular especially within IT security and cybersecurity. Examples include CISSP, CISA or CISM. EFQM and various HSE-certifications are other possibilities. Though most of them are achieved by simply taking an exam or task, several organizations offer targeted training in order to complete one of these certifications.

Keeping up to date on various opportunities for further education can be accomplished by following the social media pages and news pages of education institutions and training providers.

6. HOW TO INCORPORATE SECURITY RISK MANAGEMENT TEACHING IN CURRENT STUDY PROGRAMMES

The SECUREU project is aimed at developing comprehensive and up-to-date digital teaching materials and tools, gathered on one web platform which contains the most updated information on security risk management aspects available for all security experts, students, and academics.

All the results produced by this project can be adapted to the various levels of higher education taught at universities, i.e., undergraduate, and graduate level degrees and courses.

LEVELS OF STUDY PROGRAMMES

All materials and results can be used and implemented at both undergraduate and graduate levels. There is, however, content that may suit introduction level subjects best, more linked to undergraduate studies (first courses), while other content is intended for advanced level courses, more related to late undergraduate modules or master-level study programmes.

USE OF PRODUCTS

**SKILLS' REPORTS AND BODY OF SKILLS AND KNOWLEDGE**
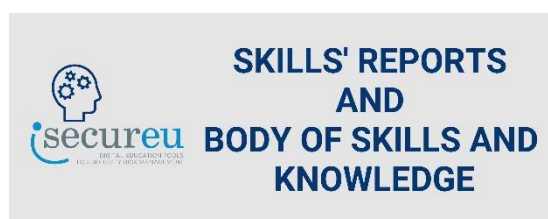
As part of the project, we studied and analysed what skills a security specialist needs, and what skills will be in demand in the future. On the website you will find several reports that provide insight into the knowledge and skills needed by security specialists. When you design and develop security programmes, training courses or study modules or courses on security, please explore them and incorporate the skills and knowledge mentioned in these reports into your teaching process.

You will find a summary of the skills and knowledge needed by security specialists, as well as perspectives on the future of the security field in the 1) **Round table report**, in which experts from 6 EU countries participated, and 2) the **CONRIS network report**.

Additionally, chapter 5.1 Body of knowledge and skills will provide a structured insight into the necessary skills and knowledge for security risk professionals.

VOCABULARY GLOSSARY AND QUIZLET
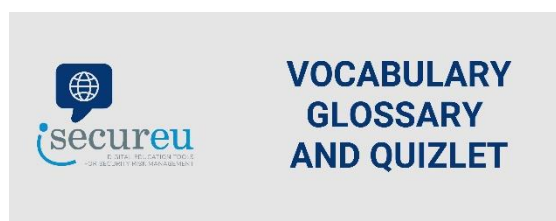
On the project website's "Security Vocabulary" section, you can access a glossary containing definitions for key terms, a vocabulary list of over 100 words, and engaging interactive games on Quizlet. These materials are available in English, Latvian, Lithuanian, Spanish, Norwegian, Finnish, Ukrainian and Dutch.

While most of the definitions are suitable for introductory-level studies, some are integral to the entire study process, extending up to master's level studies, as they are interconnected with complex processes and competencies.

Teachers can seamlessly integrate these materials into their lessons, either by linking them when working with digital content or incorporating them as footnotes in traditional student handbooks. The Quizlet games offer a dynamic tool for interactive language teaching in professional terminology classes or for self-training purposes.

Videos can be used in all courses and at all levels, but depending on their content, they can be divided into introduction level videos, more linked to first level courses at undergraduate level, or more advanced video content, more appropriate for pre-graduate courses or master-level courses. The lecturer can refer to the videos during the lessons, while explaining a topic; or use the videos to show examples of good practice; or ask the students to watch the videos as homework and later discuss the videos in the classroom, analysing the application of ISO 31000 and best practices.

Best practices include a comprehensive compilation of various subtopics related to security risk management. This material includes articles highlighting best practices, practical case examples, and expert advice. In the *Methodological guidelines on how to implement the results in security stud*y programmes the lecturer can check if the content is thought more appropriate for beginners or for advanced level students.

The lecturer can use Best practice cases with their audience to analyse each case, provide examples, or ask the students to read this material at home to later discuss it with the audience or, for example, prepare conclusions about the application of ISO31000 standards in risk management in the context of a specific case.

Practical tasks offer the opportunity to enhance skills in security risk management through different exercises. These exercises can be completed either individually or in groups. The lecturer's practical tasks can be used in group work in workshops or these tasks can be assigned individually or to groups as homework or tests.

The SECUREU project has chosen to work with the structure of ISO 31000. This norm provides a standard for risk management which is internationally supported and whose structure: Risk Management Framework – Leadership and Commitment; Risk Management Principles – Value creation and protection and Risk Management Process – Scope, Context, Criteria, Risk Assessment (Risk Identification, Risk Analysis, Risk Evaluation), Risk Treatment, Recording & Reporting, Communication & Consultation, Monitoring & Review provides a shared base for understanding the various ways of managing security risks in Europe. Although this approach has never been tested in the field of security studies and practices, it has now been applied as the starting point for the modules to be developed in the field of security risk management for young security specialists, in order to make them better prepared for a crisis.

Lecturers will thus have the opportunity to utilize and share informational materials about the ISO 31000 standard and its application in security risk management with students.

7. CONCLUSIONS AND FURTHER RECOMMENDATIONS

PROFILE OF SECURITY SPECIALISTS

The profile of a security professional is multifaceted. At the moment, there are no uniform standards in Europe that would determine the profile of a security specialist and what a security specialist should necessarily be capable of. Considering the wide profile of security specialists, the specifics of their fields of activity, it is impossible to develop a single standard for all. Each country has a different approach and different practices to develop standards for security professionals.

Thus, we believe that it is not possible to develop uniform standards for Security Specialists on a European scale. Instead, the focus should be on the skills and competencies of Security Specialists. Although the specializations of security professionals can be very diverse, the skills that any professional in this industry would need can be clearly outlined. Within the framework of these recommendations and in general in the context of the SECUREU project, we have extensively studied and analysed the skills that would be necessary for Security Specialists. Detailed information can be found in section No 3 of these recommendations and on the project website https://security.turiba.lv

STRENGTHS AND WEAKNESSES OF PARTNERS' STUDY PROGRAMMES

In assessing security study programmes across six European universities, common strengths and areas for improvement have surfaced. The programmes, designed to provide students with a broad understanding of security-related issues, show theoretical knowledge, analytical skills, and interdisciplinary approaches. Notably, practical insights from industry professionals and students' collaborative teamwork are acknowledged. However, there's a recognized need for improvements in communication and digital literacy skills, stress management, and practical application. The evaluation of risk assessment skills, both by lecturers and self-assessment by students and alumni, indicates an average proficiency, emphasizing a scope for enhancement.

To enhance programme effectiveness, there is consensus among lecturers and alumni about the importance of reinforcing communication skills, embracing digital literacy, and integrating practical experience Stress management skills, specific technological knowledge, and a deeper focus on personnel and human resource management are identified as crucial areas for improvement. Incorporating courses on cybersecurity, data protection, security systems, and international security law is recommended to align programmes with emerging trends. Additionally, fostering practical, hands-on experience and addressing environmental safety and sustainability concerns would further enrich the educational experience. In conclusion, continuous adaptation and refinement, addressing both strengths and areas for improvement, will ensure that security education remains relevant, equipping students with the competencies they need in order to navigate the evolving challenges of the security landscape effectively.

SKILLS OF YOUNG SECURITY SPECIALISTS

The series of round table discussions conducted across Latvia, Lithuania, Finland, Spain, the Netherlands, and Norway brought together a diverse group of security and risk management specialists. Their collective insights shed light on the commonalities and challenges faced by security professionals worldwide.

The collaborative round table discussions underscored the universal importance of soft skills, strategic thinking, and enhanced management abilities for young security specialists. Experts across countries emphasized the critical need for practical experience, problem-based education, and a balance between fundamental principles and advanced knowledge. Furthermore, addressing identified weaknesses, including communication and stress management skills, emerged as essential for refining the capabilities of future security professionals. To enhance the educational approach, tailored strategies focusing on metaskills and holistic security understanding are recommended.

**DIVERSE AND COMPLEX BODY OF KNOWLEDGE AND SKILLS**

The diverse and complex nature of the security profession, as outlined in the Body of Knowledge and Skills (chapter 5.1), highlights the need for a comprehensive educational approach. Security professionals must possess a broad understanding of various disciplines, including tools, partners, work areas, and specific skills. To enhance the effectiveness of security professionals, educational programmes should focus on providing a well-rounded foundation covering analytical, communication, leadership, and technical skills. This approach ensures that security professionals are not only capable of collaborating with specialists but also equipped to address a wide range of security challenges in different contexts.

Institutions offering security risk management education should adopt an integrated curriculum design that spans across the diverse domains of the security field. This would involve incorporating essential components from each category of the Body of Knowledge and Skills. Such a holistic curriculum should emphasize interdisciplinary learning, encouraging students to explore connections between various aspects of security. Additionally, hands-on experience, case studies, and practical exercises should be integrated to reinforce theoretical knowledge and develop practical skills.

Additionally, the Body of Skills highlights the importance of soft skills such as communication, decisiveness, innovative capacity, leadership, and collaboration. These skills are crucial for security professionals to effectively navigate complex situations, engage with diverse stakeholders, and lead teams.

APPROACHES FOR KNOWLEDGE AND SKILLS ACQUISITION
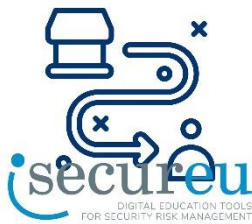
When it comes to preparing security professionals, emphasizing social constructivism as a pedagogical approach is essential. This means prioritizing collaborative learning, where young professionals actively engage with peers and educators. Additionally, problem-based learning fosters creativity, reflection, and a deeper understanding of real-world situations.

We recommend incorporating exercises as effective tools for active learning. A well-designed exercise mirrors real-world scenarios and requires careful planning by educators. It encourages student engagement and utilizes digital tools to facilitate collaborative learning and reflection. In Chapter 5.2 you will find best practice illustrative examples from the Centre for Crisis Management and Collaboration – NORDLAB. These examples cover discussion-based, functional, and full-scale exercises, providing valuable insights for security professionals.

Remember, a holistic training approach that combines theory, practice, and collaboration will empower security professionals to excel in their roles and contribute effectively to real-world security challenges.

LIFELONG LEARNING FOR SECURITY PROFESSIONALS

Lifelong learning is essential for security professionals due to the rapidly evolving security landscape and technology. Further education after a Bachelor's degree in Security Risk Management can take many forms, including formal higher education degrees such as Master's and Doctorate programs offered by universities and applied sciences institutions, informal higher education like open university courses to update and upgrade skills, and structured certifications like CISSP, CISA, and CISM in IT security and cybersecurity. Staying informed about educational opportunities can be achieved by following the social media pages and news updates of relevant institutions and training providers.

FUTURE OS SECURITY SPECIALISTS

Experts collectively envision a future security landscape shaped by information technologies, artificial intelligence, and business analytics. The emphasis on cross-sectoral skills, a deeper connection between business and security, and heightened cybersecurity awareness highlights key trends. The demand for specialists with comprehensive knowledge of risk and compliance management signals a shift towards integrated security risk and compliance management. To prepare for this future, educational institutions should incorporate interdisciplinary aspects, continuously update curricula, and foster adaptability among security professionals.

INTERNATIONAL APPROACH

Today, the field of security has become global, security risk management cannot be imagined within the borders of one country. Therefore, it is essential for a Security Specialist to acquire skills and knowledge related to global thinking, a global approach. Our research and the collaboration by the partners in this project have shown how important international cooperation is both in the learning process and in the development of the security field in general.

We emphasize and recommend the inclusion of various training courses in security study programmes, which allow future security specialists to understand global aspects - global and cross-border social, political and economic processes, the importance of cooperation in business and economy, the impact on logistics, business, cultural and cooperation issues, as well as sustainability issues.

It is equally important to include teaching methods that promote international cooperation in the teaching process - international summer schools, intensive courses, international conferences, student work competitions, joint lectures between different universities. Such activities give young security professionals the opportunity to get to know other cultures, to better understand different mentalities and to learn to communicate and cooperate with representatives of different countries.

INTEGRATION OF ISO 31000 STANDARD IN SECURITY RISK MANAGEMENT

The SECUREU project has chosen to work with the structure of ISO 31000. This norm provides a standard for risk management which is internationally supported and whose structure and Risk Management Process provide a shared base for understanding the different ways of managing security risks in Europe. Although this approach has never been tested in the field of security studies and practices before this project, it has now been applied as the starting point for the modules to be developed in the field of security risk management for young security specialists, in order to make them better prepared for crises.

ISO 31000 is a generic risk management standard that can be applied to various domains, including security risk management. When it comes to security risk management, ISO 31000 provides a foundation and guidance for organizations to identify, assess, and manage security risks in a systematic and structured manner.

By incorporating the principles and guidance of ISO 31000 into their security risk management processes, organizations can establish a structured, systematic, and proactive approach to identifying, assessing, and managing security risks effectively. It helps organizations to better protect their assets, operations, and stakeholders from security threats and vulnerabilities.

Therefore, it is reasonable to give security students the opportunity to become familiar with the ISO 31000 standard in risk management in detail during the study process, to understand the process, values, and practical application in order to be able to apply it in the management of security risks in their professional activities.

Security managers are expected to recognize and assess risks so that they can give sound advice on taking to take measures that reduce the risks. This is only possible if they work on the basis

of facts and for this it is necessary that they have correct, complete and timely information. The delivery information is the responsibility of line management (the 'first line role') because they are primarily responsible for the management of the business processes. In that process, security managers are responsible for advising on the content of the information that can be controlled (the 'second line role'), so that they can properly fulfil their advisory role.