CYBER RISK AUDIT MATRIX

ENCRYPT 4.0

Co-funded by the
Erasmus+ Programme
of the European Union

ENCRYPT4.0 Project (2020-1-RO01-KA202-079983) has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Contents

1. INTRODUCTION

Manufacturing productivity, quality and costs can potentially benefit from dramatic improvements by the increasing connectivity of Industry 4.0, the use of digital computation and off-site data storage. However, there are associated risks for manufacturing SMEs such as the potentiality of competitors and adversaries to access their data. Cyberattacks are increasingly more and more common and are usually implemented to extract or steal confidential and/or proprietary data, manipulate captured data to cause unwanted effects and destroy capital assets (Margot Hutchins & Stefanie Robinson, 2015). Cyberattacks can be defined as "an attack, via cyberspace, targeting an enterprise's use of cyberspace to disrupt, disable, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information" (National Institute for Standards and Technology, 2012, p. B3). The World Economic Forum (2017) prioritize two solutions to address innovation-driven cyber-risks: i) Cyber-risk measurement and ii) Cybersecurity assessment. In 2019, data fraud or theft and cyberattacks were identified by the World Economic Forum as the fourth and fifth most likely risks to occur (World Economic Forum, 2020), in 2020 it has identified cyber-related issues, such as cyberattacks and data fraud or theft, within the list of top 10 long-term risks.

The Manufacturing Industry needs tools to incorporate cyber risks into their existing risk management processes. In this context, the ENCRYPT 4.0 addresses this identified need, focusing on Cybersecurity assessment, by developing the Cyber Risk Audit Matrix (CRAM). The CRAM is a comprehensive tool aimed at supporting managers of manufacturing SMEs to perform a comprehensive analysis of their processes taking into account the use of innovative Industry 4.0-based technological solutions, identifying cyber risks and supporting them into designing and setting effective controls at place. The CRAM will be developed considering expertise from national, EU and worldwide standards (Annex A) as well as feedback from experts in cybersecurity from six European countries – Austria, Portugal, Romania, Bulgary, Cyprus and Spain.

- This document comprises a) the CRAM value proposition, b) CRAM methodology, c) the description of the Cyber Risk Audit Matrix categories, c) the steps to conduct Cybersecurity audits d) bibliographic references.

ENCRYPT 4.0 focus on Cybersecurity assessment, by developing the Cyber Risk Audit Matrix

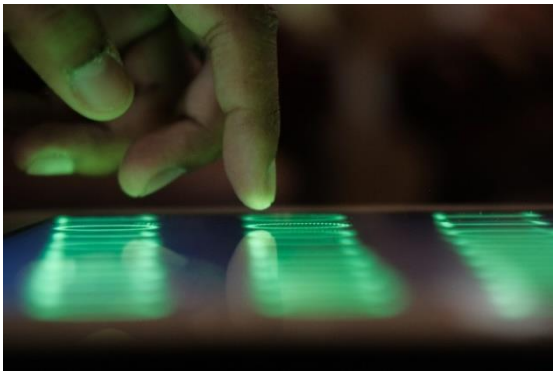
2. CRAM VALUE PROPOSITION

The **Cyber Risk Audit Matrix** (**CRAM**) will enable smart factories to perform a systematic overview of their cyber risk landscape and create an accurate profile of the cyber threats risk. The Encrypt 4.0 CRAM, will

enable smart factories to perform a consistent real-time data analyses and evaluate its cyber risks, based on a specific and extensive matrix.

The Cyber Risk Audit Matrix will be an analytic tool that will support the manufacturing companies to identify, analyse, prioritise risks and establish protective measures promptly. In recent years, one of the most pressing problems of the digital world is cybersecurity and data privacy protection. In 2019 the World Economic Forum (WEF) ranked cyberattacks among the top five global risks.

In 2020, with the COVID-19 pandemic, the higher dependency on connectivity and digital infrastructure due to the global lockdown increased the opportunities for cyber intrusion and attacks. At the same time, to maximise damage and financial gain, cybercriminals are shifting their targets from individuals and small businesses to major corporations, governments and critical infrastructure, which play a crucial role in responding to the outbreak (INTERPOL G. S., 2020). “Cyberattacks pose more danger to democracies and economies than guns and tanks” (Juncker, 2017).



Cybersecurity Ventures, the world's leading researcher in the global cyber economy, predicted that “global damages related to cybercrime in 2021 will reach six trillion dollars, which will be more than all-natural disasters in a year” (Cybersecurity Ventures, 2020). The 2019 Official Annual Cybercrime Report stated that “at the end of 2016, a business fell victim to a ransomware attack every 40 seconds” (Cybersecurity Ventures, 2019) and the predictions are this figure will rise to every 11 seconds by 2021.

Cyberattacks on critical infrastructure, rated the fifth top risk in 2020 by WEF expert network have become the new normal across sectors such as energy, healthcare and transportation. However, manufacturing is suffering from increasing cyberattacks as the 2020 Data Breach Investigations Report showed, detailing 922 incidents, 381 with confirmed data disclosure, in the US alone (Verizon, 2020). The organized cybercrime’ organizations are joining forces and their likelihood of detection and prosecution is estimated to be as low as 0.05% in the United States, “cybercrime-as-a-service is a growing business model, as the increasing sophistication of tools on the Darknet makes malicious services more affordable and easily accessible for anyone” (World Economic Forum, 2020).

SMEs’ defence ability is typically weaker compared to larger enterprises and figures suggest that only 14% of the affected SMEs can recover on their own. Furthermore, the National Cyber Security Alliance states that 60% of SMEs which undergo a cyber-attack lose their business within 6 months and “manufacturers are much more prone to threats to their security because of connectivity in IT and OT (Operational Technologies) systems through Industry 4.0 digitalization” (Verizon, 2017).

Most of the manufacturing companies in their attempt to keep a competitive edge adapting to Industry 4.0 practices, make sporadic efforts investing in control systems and external advisers, but they lack an integrated approach to cyber risk management. Their efforts fail to effectively tackle the quickly evolving cyber threats because most manufacturing systems were traditionally developed to focus on safety and high performance, rather than security. Moreover, when it comes to security, manufacturers were historically concerned mainly in securing their OT environment, often neglecting IT security, "the emergence of Industry 4.0 introduces new technologies into traditional OT environments and thus people familiar with OT that work in such environments need to adapt" (EU Agency for Cybersecurity, 2019). Employees often use potentially conflicting information to describe or evaluate some aspects of cyber risk.

The Cyber Risk Audit Matrix (CRAM) will outline key-risks indicators which will be easily applied to real-time data. The CRAM will enable employees not only to make a long-term cybersecurity strategy but also to quickly perform daily reporting. This will show the actual risk levels for the processes at any given moment, of crucial importance in the manufacturing environment since keeping the production ongoing is a critical and the shortest destitution of certain process may have an irreparable impact and cause huge financial loss. Security risks in manufacturing are getting more and more complex and evolving, making it of huge importance to equip manufacturing SMEs with the adequate analytic tool to outline the precautions to be taken into account on a day-to-day basis in the manufacturing setting. As opposed to failures in mechanical processes which can be categorised as static, cybersecurity failures are dynamic since they incorporate closely with human interactions.

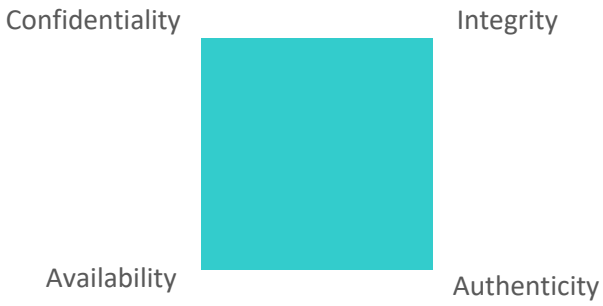
The **CRAM main objective** is to provide **manufacturing leaders** with an insight into the **potential cybersecurity risks in their systems** and support them to **adopt an effective strategy to mitigate risks**. Since only limited research in the field of cybersecurity risk assessment in manufacturing systems is available, the Encrypt 4.0 CRAM will represent an innovate tool aimed to be incorporated into the risk management policy of the manufacturing companies.

The Cyber Risk Audit Matrix will outline key-risks indicators which will be easily applied to real-time data

The CRAM main objective is to provide manufacturing leaders with an insight into the potential cybersecurity risks in their systems and support them to adopt an effective strategy to mitigate risks.

3. THE CYBER RISK AUDIT MATRIX METHODOLOGY

The CRAM was designed considering the **CIAA** quartet of **confidentiality**, **integrity**, **availability** and **authenticity**. Two main aspects will be measured: **Risk likelihood** and **Risk impact**, tailored to **respond** to the specific needs of the manufacturing SMEs with the potential to be easily shaped and adapted in the individual organizational culture of a given company.



The CRAM was designed considering the CIAA quartet

The CRAM also includes: i) risk number, ii) risk category, iii) risk source, iv) risk description, v) potential costs associated with the consequences of the risk, vi) organization department that might be affected, vii) mitigation/actions previously implemented, viii) risk impact, ix) risk likelihood, x) overall risk level, xi) triggers, xii) mitigation/actions to be implemented, xiii) potential costs of mitigation, xiv) deadline, xv) person responsible for the risk management, xvi) supervisor responsible for monitoring and xvii) effectiveness evaluation.

Below, the description of the main concepts that comprise the Cyber Risk Audit Matrix:

Availability: Ensuring timely and reliable access of information.

Authenticity: Ensuring the data property of being genuine and original, able to be verified and confidence in the validity of a transmission, a message, or message originator. (Encrypt 4.0 project, 2020).

Cybersecurity assessment: Enhanced cybersecurity guidance and assessment mechanisms, including common principles for cybersecurity assessments, a point-based scoring mechanism and practical steps for improvement, that allow companies to evaluate and improve their cybersecurity readiness (World Economic Forum , 2017).

Confidentiality: Preserving (controlled) restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Impact: The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of *low*, *moderate*, or *high*.

Integrity: Protection against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.

Likelihood: A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

Descriptions inspired on the Guide for Conducting Risk Assessments (National Institute of Standards and Technology, 2012).

4. CYBER RISK AUDIT MATRIX (CRAM)

Encrypt 4.0 CRAM represents a comprehensive tool aimed at supporting managers of manufacturing SMEs to perform a comprehensive analysis of their processes taking into account the use of innovative Industry 4.0-based technological solutions and identify cyber risks and support them into designing and setting effective controls at place.

4.1 CYBER RISKS AUDIT MATRIX CATEGORIES

These categories were derived from a conducted research and analysis of over 20 standards (Annex A) in the field of information security and data protection as well as on conducted 12 in-depth interviews conducted with cybersecurity experts from Austria, Portugal, Romania, Bulgaria, Cyprus and Spain.

Table 1. Categories of the Cyber Risks Audit Matrix

Risk Category	Risk Category Description
Human resources	Identification of the risks that are related with the human resources of the company. The risks that are related with the roles and responsibilities of company's personnel, decision making, management of identities, control of accesses, awareness raising…
Intellectual Property	Identification of the risks that are related with the Intellectual Property of the company. Intellectual Property includes Industrial Property, Copyright and Related Rights and confers the right to exclusive use of the respective technical, commercial and industrial information. Industrial Property aims to protect inventions, patents, brands and projects covered by exclusive use, production and marketing rights.
Industrial Control systems (ICS) Security	ICS security involves safekeeping and securing industrial control systems as well as the necessary software and hardware that are used by the system.
Products	Identification of the risks that are related with the products. The occurrence of this type of risk may jeopardize the products produced by the organization.
Cybersecurity Legal Risks	Identification of the risks that are related with legal and regulatory responsibilities. The occurrence of this type of risk may jeopardize legal and / or regulatory responsibilities of the organization.
Supply-chain attacks	Identification of vulnerabilities in the supply chain. The organization must define, evaluate and manage risk management processes of the supply and logistics chain. Identification of the links to vendors with poor security postures.
Technology, ICT and operational safety	Identification of the risks that are related with Technology, ICT and company operations. To tackle the hazards resulting from functional insufficiencies of the intended functionality, operational disturbances or by reasonably foreseeable misuse/errors by the collaborators related with technology, ICT and operations.
Customers	The occurrence of a certain risk may jeopardize the service provided to the organization's customers or compromise customers' data.
Physical cybersecurity	Physical cybersecurity is the protection of cyber physical systems, internet of things devices, the protection of people, property, and physical assets from actions and events that could cause damage or loss.

5. CYBERSECURITY AUDITS

5.1 WHAT IS A CYBERSECURITY AUDIT?

The fourth industrial revolution or Industry 4.0 has brought a number or new technologies connecting the physical and the digital worlds of business processes in integrated smart systems. This brings many opportunities for improving processes and overall performance, but also many new responsibilities and threats. The higher level of connectivity between all systems through Internet of things, cloud computing and many other technologies, apart from many benefits, possess new challenges to companies related to the security of the information, Big data, etc. which is processed by these integrated systems. This is why companies and especially SMEs need tools to support them in the process of checking and analysing their weaknesses when it comes to the security of the Industry 4.0 technologies that they have in place. An effective tool to implement this check it the conduction of cybersecurity audit.

A cybersecurity audit represents an evaluation of performance against specifications, standards, controls, or guidelines.

A cybersecurity audit represents an evaluation of performance against specifications, standards, controls, or guidelines (CyLumena, 2020). Cybersecurity audits are typically done against a checklist of controls (controls library) that are defined based on certain standards for cybersecurity (national, international, internal for the company) and/or company procedures and/or policies. The aim of a cybersecurity audit is to help organisations assess whether they have proper security mechanisms set in place by identifying security gaps or validating the procedures and policies applied. Cybersecurity audits help businesses verify what is on their network, what needs to be protected, and what gaps there are in their existing protections so they can make improvements (Dosal, 2020).

CYBERSECURITY AUDITS VS. CYBERSECURITY ASSESSMENT

Cybersecurity audits differ from cybersecurity assessments. While the cybersecurity audit is concerned whether there are certain controls set in place, the cybersecurity assessment aims to evaluate the effectiveness of these controls (Aldorisio, 2020). Assessments may include some degree of an audit but not always. Cybersecurity audits, depending on the aim, could also be applied when an organization wants to evaluate their compliance with certain law or standards, in this case usually the audit is conducted by a third external party having the necessary competence. The cybersecurity assessments, on the other hand, could be carried out internally by people within the organization who have good knowledge of the cybersecurity infrastructure.

EXTERNAL VS. INTERNAL CYBERSECURITY AUDITS

External audits are carried out by professionals, especially when the aim of the audit is to provide ground for certification under certain cybersecurity standards and compliance assessment against official standards, laws, etc. Internal cybersecurity audits (first party audits) could be conduct by internal expert who is well aware of the company processes and cybersecurity architecture. According to GDPR (GDPR.EU N.d.), each company is legally required to have a nominated Data Protection Officer who to be aware of the data management – what information comes in and out of the company, in what processes it's used and how it is managed. Therefore, a natural choice for conducting an internal cybersecurity audit could be the nominated Data Protection Officer or a company team depending on the scope of the audit. In the next sections of this document we will present a combined approach towards carrying out an internal cybersecurity audit and assessment based on several before mentioned categories that need to be taken into account in the auditing process.

5.2 HOW TO CONDUCT AN INTERNAL CYBERSECURITY AUDIT?

The aim of this section is to provide easy to follow guidance for conduction of self-cybersecurity audit (internal cybersecurity audit) which could serve as an effective tool to evaluate the cyber and data security within your organization and/or as preparation for external (third-party) cybersecurity audits.

STEP 1: Define your organisation security priorities and the scope of the audit

At this stage the person or the team appointed to conduct the audit have to identify what will be the scope of the auditing process. A good starting point is to list all of the company's cyber assets, such could be cyber assets associated with critical assets such as: control systems; Data acquisition systems; Networking equipment; Hardware platforms for virtual machines or storage; Secondary or supporting systems such as virus scanners, HVAC systems, and uninterruptible power supplies (UPS) (n.d., Versify Solutions);

Next, you need to evaluate which are the critical cyber assets (CCA). According to the Critical Infrastructure Protection (CIP) standard, version 4 by the North American Electric Reliability Corporation (NERC) a CCA is "any device that uses a routable protocol to communicate outside the electronic security perimeter (ESP), uses a routable protocol within a control centre, or is dial-up accessible."(2011, Flick & Morehouse).

In more simple words, assets can vary from computer equipment to various systems and sensitive customer and company information, internal documentation, and communication systems.

Once the critical cyber assets have been identified, you will have to identify where the critical security parameters lie and thus segment what will be included in the audit scope (2019, LeCount). Security parameters and assets will greatly vary from company to company, therefore this initial step and the correct definition of the audit scope are of crucial importance for the effectiveness of the auditing process. Once the audit scope is defined, you can proceed to the next step – identification of potential threats.

STEP 2: Identify the potential risks & threats

Based on in-depth interviews with 12 experts in the field of cybersecurity, the ENCRYPT 4.0 consortium has identified nine possible risk categories and has compiled a list of potential threats that each of these categories may pose to critical cyber assets. ENCRYPT model involves the following nine risk categories to be taken into account: (1) Human resources ; (2) Intellectual property; (3) Industrial control systems (ICS) security; (4) Products; (5) Cybersecurity legal risks; (6) Supply-chain attacks; (7) Technology, ICT and operational safety; (8) Customers; (9) Cybersecurity physical. Have in mind that depending on your organisation's business activities, business model and sector of operations not all categories might apply to you or you may decide you have no critical cyber assets connected to these categories. To evaluate this check Annex 1 and choose the applicable categories to your organization and the threats you deem relevant depending on the identified crucial cyber assets within your company.

STEP 3: Prioritize the risks

At this crucial step you need to check the list of potential threats you deem applicable to your company and according to a set of criteria to decide which risks are highly probable and with potentially more serious adverse impact. For this reason, the ENCRYPT 4.0 consortium has elaborated a risk assessment methodology which takes into account the following components:

- Potential costs associated with the consequences of the risk;
- Organisation's department(s) that might be affected;
- Potential impact;
- Likelihood – when assessing the likelihood, take into account industry trends, previous security breaches;
- Risk level.

You can directly use the ENCRYPT 4.0 Cybersecurity Risk Assessment Matrix (CRAM) tool developed to easily prioritize the potential risks.

STEP 4: Audit current security measures in place

Having identified the applicable risk categories and threats to your organization, the next step is to evaluate if your critical cyber assets and infrastructure are vulnerable to any of these threats. For this purpose, you need to assess the security protocols/procedures/measures set in place with regards identifying potential security gaps which need addressing. In table 2, you will find some guiding questions and tips on how to evaluate whether the security measures in place are adequate, however it also depends on the threats you deem applicable in each category.

Table 2. Tips on how to identify security measures in place

No.	Category	Tips on how to audit security measures in place
1	**Human resources**	Check distribution of roles and responsibilities connected to data management and security; cybersecurity; system control, etc. Talk with appointed responsible employees within these domains – ask them how would they react in certain situations, what security protocols would they implement, thus you will be able to evaluate if the staff is aware and prepared in the case of realisation of certain cybersecurity risks; if they need training or not. Analyse accidents and security breaches due to employees' mistakes and how they were handled. Think is there is something more that could be done to further minimize the occurrence of this threat in the future.
2	**Intellectual property**	Check distribution of roles and responsibilities connected to intellectual property management as well as commercial secrets, etc. Interview the responsible employees, review relevant documentation regarding assets protection such as patents, trademarks copyrights. How this documentation is kept and managed, who has access to it? Were there incidents in the past connected to information breaches, missing information in this domain? How they were handled, is the security protocol updated?
3	**Industrial control systems (ICS) security**	Who has remote and/or physical access to the ICS? How is the remote access to ICS administered? Are there any security controls such as strong authentication, access control, and encryption to protect against unauthorized access to and exploitation of these systems? What are physical access control measures? Do you use ICS protocol-aware firewalls to enforce access controls on ICS network traffic? Do you have an Intrusion prevention system set in place?
4	**Products**	Depending on the products' production process, you need to identify in which processes sensitive information is being handled and in what way it's being managed and administered. Are there any commercial secrets related to the products production, etc. How is the company ensuring that this information is safely managed? What is the protocol – roles and responsibilities, procedures, etc.?

		Is there any control of physical and remote access to computers and networks; production systems, etc.? How are those secured and controlled?
5	**Cybersecurity legal risks**	Is there any control of physical and remote access to company computers and networks? How are those secured and controlled? How is legal data being managed and administered? Is the server secured? Who has access to this information? Were there any security breaches in the past? How were they handled? Is there a way to improve the security protocols based on recent trends/events/technology developments?
6	**Supply-chain attacks**	Who has access to supply management systems? Is there Privileged Access Management? Who has access to sensitive data? How is this access secured? Do you have Honeytokens implemented? What is the level of controls on access by service vendors? How many vendors have access to software? Is the vendor network monitored for vulnerabilities?
7	**Technology, ICT and operational safety**	Do you have strict mobile security and data safeguard policies? Are all software applications and operating systems up to date? Are there access controls in place for critical cybersecurity assets? Do you monitor activity of user accounts, logging and access to your network? Check if firewalls are properly configured, ensure you have end-to-end encryption for sensitive data. Do you have mechanisms set in place to recognize and avoid attacks such as phishing and pharming?
8	**Customers**	Who has access to important customer data? Do you have back-up of important business data and information?
9	**Physical cybersecurity**	How is maintenance of equipment and critical cybersecurity assets managed? Who has physical access to equipment and critical cybersecurity assets? How is access secured?

STEP 5: Set/ update the security protocols based on the audit

Upon completion of STEP 4, you need to have your list of identified threats applicable to your organization, to be aware of what you are already doing and what is maybe missing and identify adequate information security controls to neutralize or eradicate the risk of threat (2020, LeCount).

Information security controls are measures taken to reduce information security risks such as information systems breaches, data theft, and unauthorized changes to digital information or systems (Garcia, 2019). The main aim of security controls is to protect the availability, confidentiality, and integrity of data and networks within a company. As mentioned, security controls are typically implemented after an information or cybersecurity risk assessment and represent a desired outcome of cybersecurity assessments and audits with regards addressing identified actual or potential security gaps.

In table 3, in line with the ENCRYPT 4.0 cybersecurity risk assessment model based on interviews with cybersecurity experts from 6 EU countries, we have identified two types of controls – preventive and corrective in each of the nine risk categories. Based on the audit conducted in STEP 4 you are already aware of the cybersecurity procedures in place within your organization. In table 3, you can find some suggestions preventive and corrective controls for each of the categories that you may miss in your organization.

Table 3. Cybersecurity preventive and corrective controls

Risk Category	Preventive Measures	Corrective measures
Human resources	Establish a training and awareness program Clearly identify the management of identities, authentication, and control of accesses The company shall have a policy that includes: ● List of authorized software. ● Authorized software repository and license registry. ● Disciplinary sanctions associated with non-compliance with these regulations. Rotate the passwords on a quarterly basis ("strong password policy") Develop disaster recovery solutions and business continuity plans	User permissions control Implement the Intrusion Detection System (IDS) to detect no-authorized access to a pc or a network Change all passwords after a possible data breach Lock accounts suspected of unauthorized access Set up two-factor authentication when possible which will provide a two-factor authentication

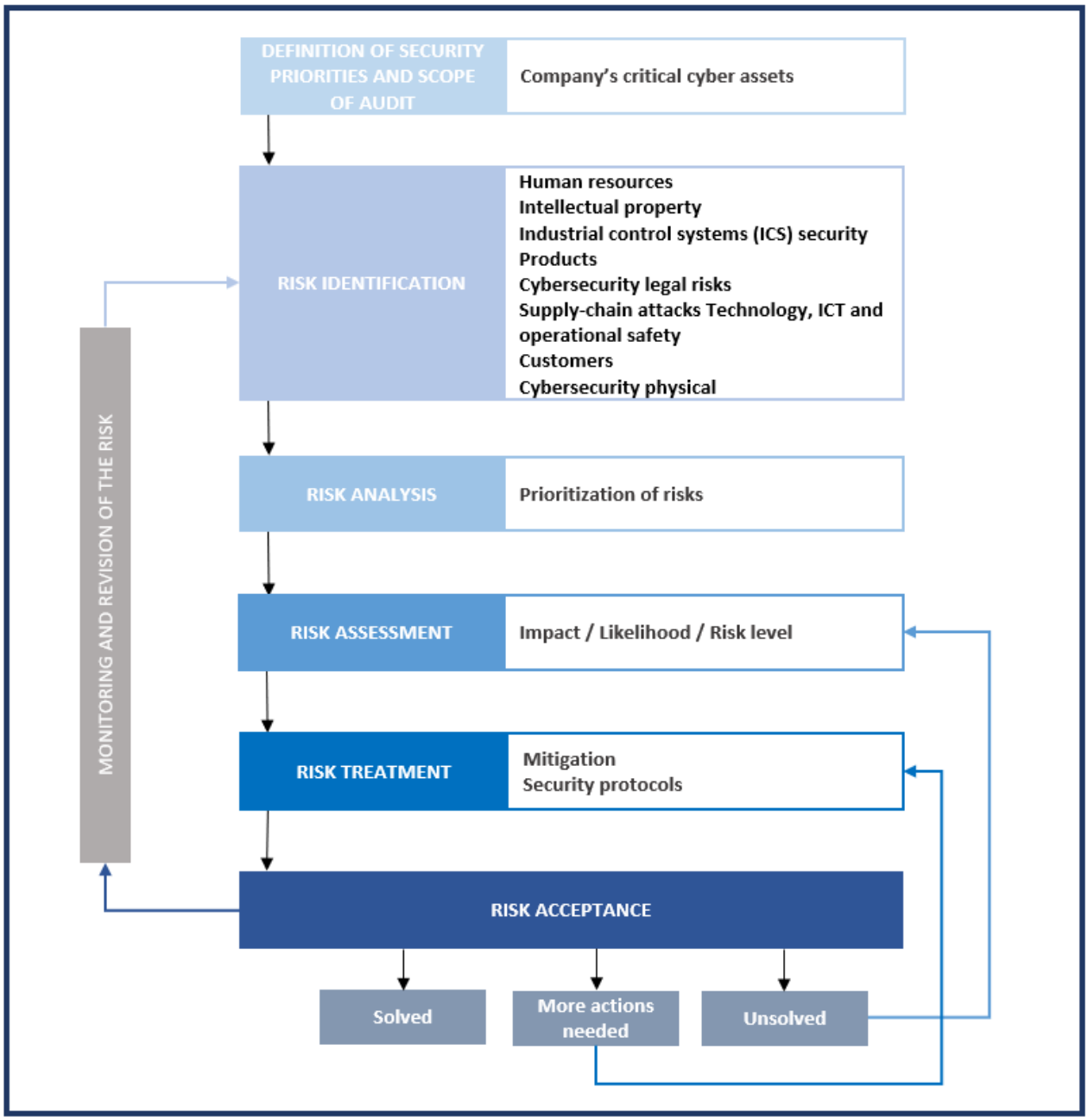
Risk Category	Preventive Measures	Corrective measures
Intellectual Property	Proper policies and responsibilities on managing intellectual property All applicable assets should be protected by registered patents, copyrights and trademarks. Relevant assets should be monitored and protected by insurances. Developing measures, policies and responsibilities on managing reputation	Regular assessment and updating policies and responsibilities If registered patent is missing a provisional patent, trademark and copyrights must be obtained Regular assessment and updating policies and responsibilities
Industrial Control systems (ICS) Security	Developing measures, policies, responsibilities and rapid response in case of incidence	Regular assessment and updating policies and responsibilities.
Products	Workflow processes assessment Standardization and evolution Control physical access to computers and network components	Implement a layered approach for every risk or at least for those that are with high potential in the specific case in order to have at least a few layers protection no matter when it comes to technologies, employees, processes, customers, etc.
Cybersecurity Legal Risks	Keep Only What You Need. Inventory the type and quantity of information in your files and on your computers Safeguard Data Destroy Before Disposal Update Procedures Educate/Train Employees Control Computer Usage. Secure All Computers.	Identify affected parties Notify affected persons Seek legal counsel
Supply-chain attacks	Implement Honeytokens Secure Privileged Access Management Identify all potential insider threads Identify and protect vulnerable resources Minimize access to sensitive data	Check the licenses in all supply chain of the SMEs Look for the data of contact of your preventive and corrective maintenance of SMEs machinery in all the supply chain at regional/local level

Risk Category	Preventive Measures	Corrective measures
	Send regular third-party risk assessments Monitor vendor network for vulnerabilities Identify all vendor data leaks	
Technology, ICT and operational safety	Download and install software updates for your operating systems and applications as they become available Operating systems and firmware updated Install firewall between the internet and the LAN Identify critical assets Security awareness, Backup and recovery, Vulnerability and patch management, Apply access controls, Use content and whitelist filtering, Properly configure endpoints, Establish incident response processes, Use threat-intelligence solutions and systems. Properly configured firewalls, strict mobile security policies, end to end encryption, audit logging and authorising devices to access the network are some of the practices that reduce the threats from the use of mobile devices on a corporate network. Assess software in respect to cyber security principles. Ensure that operating systems and all software applications are up to date, Ensure that sensitive data is encrypted, Use data protection software,	Check all the OS and firmware deadlines, that you have in your SMEs, and supervise all is updated To install firewall between the Internet and the LAN. Remove software illegal or not allowed in the software repository Standard installations to all computer equipment To configure VPN if it is necessary to connect from outside. Identification and correction of the issue. Auditing and updating the security policies and rules.

Risk Category	Preventive Measures	Corrective measures
	Regularly monitor the activity of user accounts, Manage privacy settings for mobile applications, Enforce strict device controls for removable media, Establish mechanisms to recognize and avoid attacks like phishing and pharming. Operation based on security policies and rules.	
Customers	Make backup copies of important business data and information	Set up two-factor authentication when possible which will provide a two-factor authentication Lock accounts suspected of unauthorized access Block IP addresses of suspected threat actors based upon detected activities
Physical cybersecurity	To implement a safety Plan in case of fires, floods, thefts, losses… Switch off any tools or equipment that aren't in use To have a backup uninterruptible power supply or to get second emergency energy source Regularly check all devices Do back-ups Have preferably all data hosted in the cloud	On the premises, be up to date on building safety and have anti-fire measures in place. To have a backup battery for your computer or get a second emergency energy source. To do a "security copy" Make a Safety switch Replace or fix damaged or failed devices

GRAPHICAL OVERVIEW OF THE PROCESS WITH THE CRAM

Here is represented the graphical overview of the audit process by using the Encrypt 4.0 CRAM as a tool outlining the corresponding measures to be taken by the responsible person in manufacturing SMEs to perform a comprehensive analysis of their processes by identifying the cyber risks and supporting them into designing and setting effective controls at place according the progressing nature of the cyber-attack.



The Encrypt 4.0 CRAM is a systematic, continuous process. It is a cyclical process that once it has identified, analyzed, assessed, evaluated, addressed, and accepted the risks, it must carry out a risk monitoring and review process. In case the problem persists, you will need to apply further complementary actions to solve the problem, and for this, you will need to go back to the previous step of risk treatment. And if the problem remains unresolved, you will need to re-evaluate the risk.

6. PROJECT AND PARTNERS

ENCRYPT 4.0

Joint Cyber Workforce Development Initiative to Enable The European Industry to Overcome the Shortage of Cybersecurity Professionals

The ENCRYPT4.0 Project (2020-1-RO01-KA202-079983) aims to enable manufacturing SMEs management to adopt a proactive approach towards cybersecurity by supporting them in the process of analyzing, identifying and tackling the cyber risks and threats applicable to their organization. By promoting interactive project-based learning with regards to boosting cyber-security skills and competences of SMEs' employees or/and cybersecurity professionals.

"George Emil Palade" University of Medicine, Pharmacy, Sciences and Technology of Târgu Mureș - Romania

Project coordinator

European Center for Quality Ltd., Consulting company - Bulgary

Instituto de Soldadura e Qualidade, Technological institution - Portugal

Avantalia, technology-based SME - Spain

FH Joanneum, University of Applied Sciencies - Austria

PCX Management, Computers & Information Systems Ltd. - Cyprus

BIBLIOGRAPHIC REFERENCES

Aldorisio, J., 2020. Best Practices for Cybersecurity Auditing [a Step-by-Step Checklist]. Security Scorecard. Retrieved from https://securityscorecard.com/blog/best-practices-for-a-cybersecurity-audit

Cybersecurity Ventures. (2019). *Cybersecurity Ventures Official Annual Cybercrime Report.* Retrieved from https://cybersecurityventures.com/annual-cybercrime-report-2019/

Cybersecurity Ventures. (2020). *Cybersecurity Ventures Official Annual Cybercrime Report.* Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

EU Agency for Cybersecurity. (2019). *Industry 4.0 Cybersecurity: Challenges & recommendations.*

European Union Agency for Cybersecurity. (2015). *Information security and privacy standards for SMEs - Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.* ENISA. doi: 10.2824/829076

Juncker, C. P.-C. (2017). Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

Margot Hutchins, R. B., & Stefanie Robinson, J. S. (2015). Framework for Identifying Cybersecurity Risks in. *U.S. Department of Energy*, 17.

National Institute for Standards and Technology. (2012). *Guide for Conducting Risk Assessments.* Gaithersburg: Special Publication 800-30.

Verizon. (2017). *Verizon Data Breach Investigations Report.* Retrieved from https://www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/

Verizon. (2020). *Manufacturing*. Retrieved from Verizon: https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/manufacturing-data-breaches/

World Economic Forum . (2017). *Innovation-Driven Ciber-risk to Costumer Data in Financial Services.* Cologny/Geneva.

World Economic Forum. (2020). *The Global Risks Report.*

World Economic Forum. (2020). *Wild Wide Web - Consequences of Digital Fragmentation*. Retrieved from World Economic Forum: https://reports.weforum.org/global-risks-report-2020/wild-wide-web/

ANNEX A - COLLECTION OF EXISTING STANDARDS FOR CYBERSECURITY RISKS

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Information Security (Cross-Industry)	ISO/IEC 27001:2018 Information security management systems – Requirements
	ISO/IEC 27002:2018 Code of practice for information security controls
	ISO/IEC 27003:2017 Information security management systems guidance
	ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
	International Organisation for Standardisation and International Electrotechnical Commission
	ISO/IEC 27014:2013 Governance of information security
	ISO/IEC TR 27016:2014 Information security management - Organisational economics
	ISO/IEC 27032:2012 Guidelines for information security
	ISO/IEC 27033-1:2015 Network security - Part 1: Overview and concepts
	ISO/IEC 27033-2:2012 Network security - Part 2: Guidelines for the design and implementation of network security
	ISO/IEC 27033-3:2010 Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
	ISO/IEC 27033-4:2014 Network security - Part 4: Securing communications between networks using security gateways
	ISO/IEC 27033-5:2013 Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
	ISO/IEC 27033-6:2016 Network security - Part 6: Securing wireless IP network access
	ISO/IEC 27034-1:2011 Application security - Part 1: Overview and concepts
	ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection systems (IDPS)
	ISO/IEC 27040:2015 Storage security
	CSA Cloud Controls Matrix
	BSI PAS 555:2013 Cybersecurity risk. Governance and management. Specification
	PCI Data Security Standard
	ISF The Standard of Good Practice for Information Security
	UK Gov. Security policy framework
	UK Gov. Cyber essentials scheme
	ETSI GS ISI 001 Part 1: A full set of operational indicators for organisations to use to benchmark their security posture
	ETSI TR 103 305 Critical Security Controls for Effective Cyber Defence
	BSI 100-1 Information Security Management Systems (ISMS)
	BSI 100-2: IT- Grundschutz Methodology
	BSI 200-1 Information Security Management Systems (ISMS)
	BSI 200-2: IT- Grundschutz Methodology
	ISO/IEC 15408-1:2009 Evaluation criteria for IT security - Part 1: Introduction and general model

	ISO/IEC 15408-2:2008 Evaluation criteria for IT security - Part 2: Security functional components
	ISO/IEC 15408-3:2008 Evaluation criteria for IT security - Part 3: Security assurance components
	ISO/IEC 19790:2012 Security requirements for cryptographic modules
	ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems
	ISO/IEC 27007:2017 Guidelines for information security management systems auditing
	ISO/IEC 27014:2020 Governance of information security
	ISO/IEC 27017:2015: Code of practice for information security controls based on ISO/IEC 27002 for cloud services
	ISO/IEC 29147:2018: Vulnerability disclosure
	ISO/IEC 30111:2019: Vulnerability handling processes
	OENORM A 7700-3:201910 Web Applications - Part 3: Security requirements
	ISO/IEC 27701:2019 Security techniques- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines
	ISO/IEC TS 27100:2020 Information technology -Cybersecurity- Overview and concepts

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Risk Management	ISO/TR 31004:2013 Risk management - Guidance for the implementation of ISO 31000
	ISO/IEC 27005:2016 Information security risk management
	ISO/IEC 31000 Risk management - Risk assessment techniques
	IEC 31010:2009 Risk management - Risk assessment techniques
	BSI BIP 0076 Information security risk management. Handbook for ISO/IEC 27001
	BSI 100-3: Risk Analysis based on IT-Grundschutz
	BSI 200-3: Risk Analysis based on IT-Grundschutz
	ISO/IEC 27005:2018 Information security risk management
	ISO/IEC 27102:2019 Information security management — Guidelines for cyber-insurance

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Business Continuity Management	ISO 22301:2012 Business continuity management systems – Requirements
	ISO 22313:2012 Business continuity management systems – Guidance
	ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity
	100-4: Business Continuity Management
	OENORM A 7700-4:201910 Web Applications - Part 4: Requirements for secure operations

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Data Protection and Privacy	ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
	ISO/IEC 29100:2011 Privacy framework
	ISO/IEC 29101:2013 Privacy architecture framework
	BSI BS 10012:2009 Data protection. Specification for a personal information management system
	CEN CWA 16113:2010 Personal Data Protection Good Practices
	OEVE/OENORM 17529:2020: Data protection and privacy by design and by default
	OENORM A 7700-2:201912 Web Applications - Part 2: Data protection requirements
	ISO/IEC 27018:2019: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
	ISO/IEC 29134:2017: Guidelines for privacy impact assessment
	ÖNORM EN 419231:2019 11 01: Protection profile for trustworthy systems supporting time stamping
	ÖNORM EN 419241-1:2019 03 15: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements
	ÖNORM EN 419241-2:2019 06 01: Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Incident Management	ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management
	ISO/IEC 27036-2:2014 Information security for supplier relationships - Part 2: Requirements
	ISO/IEC 27036-3:2013 Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security
	ISO/IEC 27035-1:2016 Information security incident management — Part 1: Principles of incident management
	ISO/IEC 27035-1:2016 Information security incident management — Part 2: Guidelines to plan and prepare for incident response

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Third-Party Management	ISO/IEC 27036-1:2014 Information security for supplier relationships - Part 1: Overview and concepts
	ISO/IEC 27035:2011 Information security incident management
	ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Industrial security	OVE EN IEC 62443-4-1:2018 11 01: Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements
	OVE EN IEC 62443-4-2:2020 01 01: Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components
	OVE IEC TS 62351-100-1:2020 06 01