D2.3 – 2nd Resilience preparedness/business continuity plans in the industrial ecosystem

Project number: 101074552

Silicon Euro cluster

Serving the electronics value chain for maintaining sovereignty in microelectronics, components and systems for a greener, more digital and resilient future Europe.

Call	SMP-COSME-2021-CLUSTER		
Topic	SMP-COSME-2021-CLUSTER-01		
Type of action:	SMP-GFS	**Service**	EISMEA/I/02
Start date of project:	1 September 2022	**Duration:**	30 months

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

Funded by the European Union

Related WP	WP2
WP leader	MESAP
Responsible author (s)	Alessia Menduni, Fabrizio Fallarini, Francesca Pisino (MESAP)
Contributor(s)	Alessia Menduni, Fabrizio Fallarini, Francesca Pisino, Laure de Tassini
Planned delivery month	M12
Actual delivery month	M20
Document Dissemination Level[1]	PU
Document Nature[2]	RE

Synopsis:	Analysis of the second resilience preparedness/business continuity plans in the industrial ecosystem, based on the companies and clusters' feedback
List of keywords:	Business Continuity, Business Impact Analysis, Critical Processes, Clusters, Electronics, European Union, Resilience, SMEs, Survey, Testing & Exercising

[1] PU: Public, SEN: Sensitive, limited under the conditions of the Grand Agreement
[2] RE: Report, DEC: Websites, patent filings, videos

DOCUMENT HISTORY

Version	Status[3]	Date	Comments	Author
01	Draft/under review	17/11/2023	1st draft: survey architecture according to the main objectives of the D2.3 deliverable Survey set up: approved by consortium and promoted through their channels	Alessia Menduni MESAP Fabrizio Fallarini MESAP
02	Draft/under review	01/02/2024	2nd draft: theoretical approach/philosophy of the deliverable	Alessia Menduni MESAP
03	Draft/under review	29/02/2024	3rd draft: finalization of the theoretical approach/philosophy and first isographic collection	Alessia Menduni MESAP
04	Draft/under review	15/03/2024	4th draft: 1st analysis of the raw data and sitographic analysis	Francesca Pisino MESAP Fabrizio Fallarini MESAP
05	Draft/under review	08/04/2024	5th draft: 1st analysis of the survey data and finetuning of sitographic analysis according to the survey	Francesca Pisino MESAP Fabrizio Fallarini MESAP
06	Draft/under review	29/04/2024	6th draft: final check	Fabrizio Fallarini MESAP Francesca Pisino MESAP Laure de Tassigny Minalogic
07	Issued	30/04/2024	Final version	Laure de Tassigny Minalogic
08	Issued	06/11/2024	Final version V2: integrated the PO's comments	Fabrizio Fallarini MESAP Alessia Menduni MESAP

[3] Draft: This version is under development by one or several partners; Under Review: This version has been sent for review; Issued: This version of the document has been submitted to EC

Table of Contents

List of abbreviations

SEA	Silicon Europe Alliance
SME	Small and Medium Enterprise
EU	European Union
WP	Work Package
ICT	Information and Communication Technologies
IoT	Internet of Things
AI	Artificial Intelligence
RPBCP	Resilience Preparedness/ Business Continuity Plan
BIA	Business Impact Analysis
SWOT	Strengths, Weaknesses, Opportunities, Threats
PESTEL	Political, Economic, Social, Technological, Environmental, Legal
AR/VR	Augmented and virtual reality
VUCA	Volatility, Uncertainty, Complexity, Ambiguity
BCP	Business Continuity Planning
FSTP	Financial Support of Third Parties
M	Month
D	Deliverable
R&D	Research & Development
BCM	Business Continuity Management
CEO	Chief Executive Manager
CTO	Chief Technology Manager
QA	Quality Assurance
DRP	Disaster Recovery
NDAs	Non-Disclosure Agreement
IP	Intellectual Property
CAD	Computer Aided Design
ECCP	European Cluster Collaboration Platform
EEN	European Enterprise Network
ERDF	European Regional Development Fund
EIP	European Innovation Partnership

Table of figures

1. INTRODUCTION

This deliverable is part of WP2 that aims at creating the best conditions for the Silicon Eurocluster partners as well as the EU electronics value chains to implement digital technologies and greener solutions, stay resilient and well-connected to face possible emergencies or economic crises.

It is realized in the framework of *O1. Network for resilience to improve the resilience of the EU industrial ecosystems by developing value chains interlinkages in the EU Single Market*.

The main action of this objective is to design and build new collaboration models between companies and provide some hints to European cluster organizations and other key actors facilitating value chain interlinkages along and across different industrial ecosystems.

According to the Euroclusters purposes, the aim of the document is to consider the elements that emerged in the deliverables *D.2.1 | Desk Research/ Analysis and D2.2 | SWOT + 1st Resilience preparedness/business continuity plans in the industrial ecosystem/s* to help SMEs with common resilience, green or digital transformation challenges to enable them to identify and implement the most competitive solutions. Indeed, this deliverable is aimed to offer an agile and preliminary overview of main methods that could be implemented by companies to understand, organize, manage, and safeguard their business. Moreover, it explores and analyses 3 application sectors, for which it will offer 3 resilience preparedness/business continuity plans.

Finally, the deliverable includes a brief Pan EU Clusters resilience analysis to identify clusters' gaps, promoting cross-clusters learning.

The final statement of the *D2.2 | SWOT + 1st Resilience preparedness/business continuity plans in the industrial ecosystem/s* included a small section describing the next steps, in which we included a provision of the main topics envisaged in the D2.3. In particular:

- SWOT of the EU Electronics Industry: general SWOT of the electronic industry in EU countries, analysis of the gaps between the countries, analysis on how EU members could enhance their competitive advantage against Asia and America
- Insights coming from the Silicon Eurocluster partners ecosystem: SWOT analysis coming from the community platform and from companies who will receive the funds, additional information on risk management communing from Instant poll
- How clusters can manage this complexity: analysis of clusters' main gaps and synergies

However, after careful discussion within the consortium, we decided not to primarily emphasise the SWOT approach. The SWOT tool remains fundamental as a starting point, but it cannot stand alone effectively. It is a limited tool if used without similar complements (e.g. VUCA, PESTEL,…) that we have explored in the deliverable. In particular, SWOT analysis alone cannot sufficiently determine whether companies are really prepared to handle potential crises or offer viable solutions to deal with them. For this reason, the RPBCP incorporates several interrelated tools that help companies, especially SMEs, to deal pragmatically with risks and provides recommendations for resilience activities to be implemented.

2. RECAP OF PREVIOUS ANALYSIS

The European electronics industry stands as one of the largest and most established markets worldwide, boasting a market size of €400 billion and a steady annual growth rate of 4%. It encompasses a diverse array of products and services, including semiconductors, electronic components, electronic equipment, and consumer electronics. Notably, the industry distinguishes itself through its robust innovation capabilities and steadfast commitment to sustainability and environmental preservation.

Within Europe, numerous entities contribute to this industry landscape, ranging from major global enterprises such as Siemens, Philips, Ericsson, STMicroelectronics, and NXP Semiconductors to dynamic startups. However, European firms confront significant challenges, as the competition from Asian counterparts capable of producing electronic components at lower costs, thereby exerting pressure on European manufacturers to slash prices. Furthermore, a notable obstacle is the scarcity of skilled labor, particularly in fields such as software engineering, data analysis, and artificial intelligence.

With the aim of helping companies (mainly SMEs) tackle these obstacles, we developed the project' SWOT + 1st RPBCP: it provides an overview of the primary literature and methodologies enabling companies to comprehend, organize, manage, and safeguard their operations.

Initially, the document elucidates the concept of SWOT analysis, delving into crafting effective SWOT analyses and explaining their key advantages, such as versatility, affordability, and ease of implementation.

Furthermore, it suggests augmenting SWOT analyses with complementary frameworks:

- Porter's Five Forces model, which delineates five competitive forces shaping industries, aiding companies in discerning strengths and weaknesses and formulating corporate strategies.
- The PESTEL framework, cataloging external factors for companies to consider when formulating business continuity plans.
- The VUCA model scrutinizes volatile, uncertain, complex, and ambiguous situations to quantify risks and vulnerabilities and devise mitigation strategies.

These methodologies and frameworks underscore the "ontological complexity" inherent in businesses, highlighting the emergence of intricate networks comprising elements, data, technologies, personnel, and products, thereby engendering a dynamic and uncertain environment.

The subsequent section of the document concentrates on risk management, an essential practice enabling proactive mitigation of vulnerabilities to forestall significant damages. It delineates strategies for identifying, evaluating, tracking, and enhancing the risk mitigation process, including classifications and quantifications of risks, as well as the implementation of suitable strategies.

Lastly, the document explores Business Continuity Planning (BCP), a subset of risk management crucial for aiding organizations in recovery following disruptions, encompassing scenarios ranging from cyberattacks to natural disasters.

The analysis has been instrumental in animating regional workshops (*D2.5 Organization of Regional Workshops*), fostering a microelectronics ecosystem as an interactive hub for reflection and action. These workshops integrate regional sectoral expertise, engage pertinent stakeholders, and disseminate cohesive information to local communities to raise awareness on resilience and sustainability topics. The presentation slides incorporated instant polls to foster audience interaction, stimulating discussions and idea-sharing on resilience and sustainability themes throughout the events.

3. COMPANY SURVEY

3.1 Companies survey ratio

The survey endeavors to examine the value chains of the electronics and semiconductor industries with the objective of gaining deeper insights into the opportunities and challenges confronting companies.

MESAP formulated a preliminary set of inquiries and methodology, disseminating them among the consortium via an Excel file on the shared platform. Each partner had the opportunity to provide feedback and comments. Subsequently, all comments were compiled, and adjustments were made to the survey accordingly.

In order to ensure a greater impact and to collect more information from different stakeholders and other WPs inputs, the delivery has been postponed from M12 to M20.

It includes:

- Companies who applied to the open call
- Companies awarded by Silicon Eurocluster open call for demonstration projects
- Companies participating in the regional workshops (*Task 2.2 Inform our electronics communities and the application industries*)
- Companies reached through communication actions made by the consortium partners including the WP5 activities (WP5 Dissemination & Communication and Sustainability).

Moreover, the initial approach was to analyze the following topics, based on survey data analysis:

- The selection of the 3 most popular industrial sectors
- The selection of 3 companies having 3 different "*Resilience readiness level*" (i.e. "weak" "medium" "strong")
- The selection of 3 companies having the lowest "*Resilience readiness level"* in specific questions

According to the proposal, the first option was adopted, in order to have an in-depth analysis covering a wide range of companies belonging to the electronics sector. Therefore, in chapter 4 we focus on the development of 3 different RPBCP (Resilience Preparedness/ Business Continuity Plan) of the 3 most represented sectors in the survey.

To conclude, there are several benefits for companies engaging in the survey, including:

- Being informed on strategic topics and tools to be more resilient and competitive
- Receiving in advance strategic information on services and funding opportunities, such as the Silicon Eurocluster open call for green financial support
- Orienting the EU policy of semiconductors by using Silicon Eurocluster as a "sounding board" for their interests and needs

3.2 Companies survey structure

The survey is designed to maintain anonymity and is structured into 9 sections, divided into 2 parts. The first part (sections 1-8) is dedicated to comprehensively understanding the current resilience and

risk management approaches of EU companies. The second part (section 9) delves into the potential development of New-to-firm products and services within the electronics ecosystem, focusing on activities, included in *D4.3 New-to-firm products or services in the industrial ecosystem/s* (initially scheduled for M17 but postponed to M20). The survey can be accessed here.

Each section offers a concise overview of the topics covered to assist users in navigating the survey. Both open-ended and multiple-choice questions are included, with a predominance of the latter to streamline the questionnaire completion process and facilitate the analysis of consistent data.

Additionally, participants are encouraged to explore the *D2.2 SWOT+1st resilience preparedness/business continuity plans in the industrial ecosystem/s* available on the Silicon Europe website to enhance their understanding of these topics. The report can be accessed here.

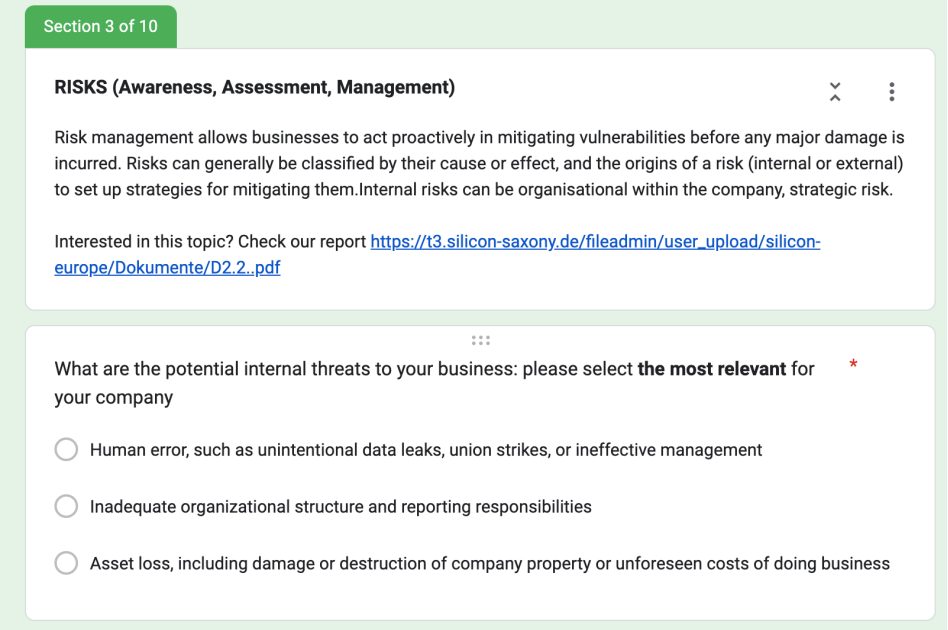

Table 1 Screenshot from the survey

3.3 Results Analysis

As of March 31st, a total of 47 companies participated in the survey. The collected data was then analyzed using an Excel file. Below, we delve deeper into the data to offer valuable insights.

3.3.1 Section 1 – Contact

The first section contains a brief description of the survey structure and objectives, followed by the indication of the deadline (i.e. 31st March 2024) and the request for an email contact.

3.3.2 Section 2 - Companies Information

The second section contains questions aimed at gathering information on the main characteristics of the sample of companies (such as name, website, contact, etc.).

QUESTION 2.1: Please fill with the country of your company (in case of large company/ transnational, please include an EU plant)

Half of the European states are represented in the questionnaire. Most companies come from Bulgaria (9), followed by Germany (7), Italy (6) and Austria (6).

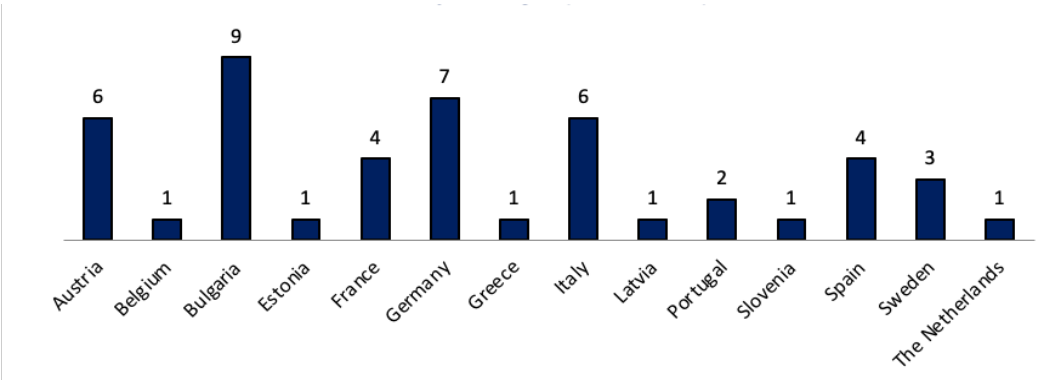

Table 2 Country of origin

QUESTION 2.2: Please fill with your company size (in terms of employees)

While the majority, comprising 85% of the sample, consists of Micro/Small Enterprises, Medium Enterprises represent 13% and Large Companies make up 2% of the sample.

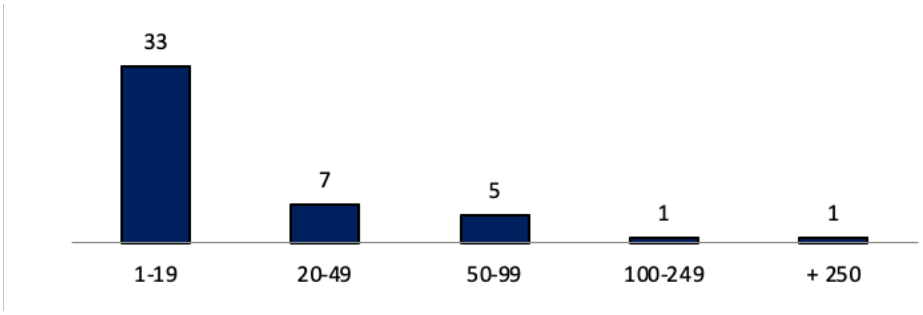

Table 3 Companies' employee number

QUESTION 2.3: What is the sector(s) of your organization?

Companies which participated in the survey are from 16 different business segments. The three most represented segments are Electronics and Microelectronics Energy/ Environment (23%), ICT (22%) and Machine tools, plant engineering/ robotics & automation. These sectors will undergo further analysis in the subsequent chapter to develop a tailored Resilience preparedness/business continuity Plan (RPBCP).

The total is 108 since most companies are active in more than one sector of business.

Sectors	Count	%
Agrifood	4	4%
ICT	**24**	**22%**
Aerospace & defense	4	4%
Construction (building, domotics, lighting...)	4	4%
Automotive, mobility & transport	8	7%
Biomedical, Health & Wellness	2	2%
Machine tools, plant engineering/robotics & automation	**10**	**9%**
Energy & Environment	7	6%
Electronics and Microelectronics Energy/environment	**25**	**23%**
Chemicals	1	1%
Operating machines/ logistics /intralogistics	3	3%
Print	2	2%
Nanotechnologies	5	5%
Rail	1	1%
Optoelectronics & Photonics	6	6%
Maritime & Naval	2	2%
Total	**108**	**1**

Table 4 Business Sectors

QUESTION 2.4: Who are your main customers?

Main customers served include Large Companies (35%), Mid-Caps (31%) and MSMEs (19%). The total is 98 since most companies serve more than one segment of customers.

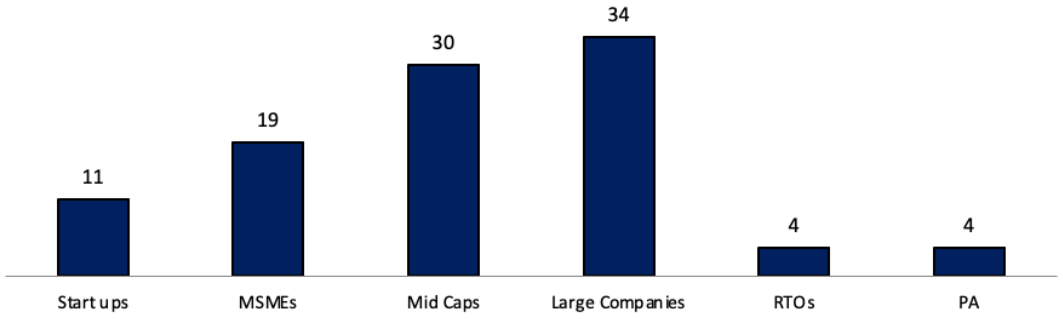

Table 5 Customer Segments

3.3.3 Section 3 - Risk Assessment

Risk management allows businesses to act proactively in mitigating vulnerabilities before any major damage is incurred. To set up risk mitigation strategies, risks can generally be classified by their cause or effect, and by origins (internal or external). This section aims to identify what are the main risks perceived by companies and how do they assess them.

QUESTION 3.1: What are the potential internal threats to your business?

The findings demonstrate a nearly even distribution among the three primary categories of threats. Among the sampled companies, larger enterprises (with 50 employees or more) cite inadequate organizational structure and reporting responsibilities, along with asset loss, as their main threats. Conversely, human error is predominantly perceived as a risk by small enterprises.

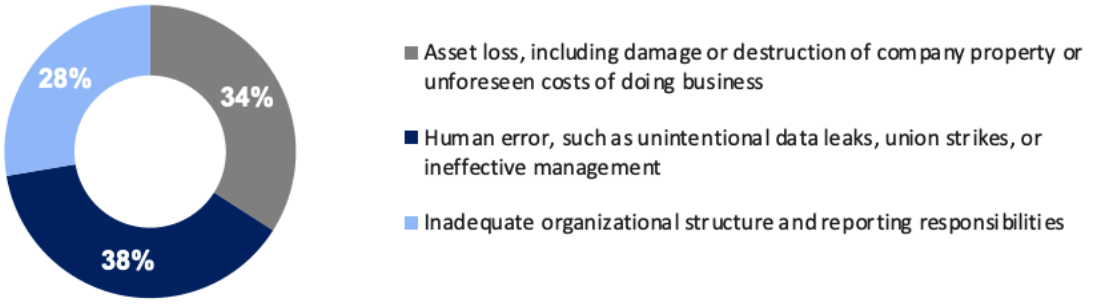

Table 6 Internal threats for companies

QUESTION 3.2: Have you identified and documented internally potential risks specific to the semiconductor industry (e.g. supply chain disruptions, technological obsolescence)?
Just 47% of the sample have pinpointed and recorded potential risks unique to the semiconductor industry. The primary risks identified include supply chain disruptions, such as difficulties in sourcing specific components, rising costs, and the emergence of new technologies. These risks are primarily documented through periodic reports.

QUESTION 3.3: How do you assess the likelihood and potential impact of semiconductor supply shortages or disruptions?
Nearly half (47%) of the companies undertake assessments to gauge the potential impact of semiconductor supply shortages. Among these companies, the majority perceive this risk as medium to high, indicating a significant level of concern regarding its potential consequences. Conversely, a small portion assesses the risk as small, suggesting a more optimistic outlook. On the other hand, the remaining half of the companies currently do not conduct assessments to evaluate the potential impact of semiconductor supply shortages. This indicates a gap in risk management practices among these companies, as they may not be fully aware of or prepared for the potential ramifications of such shortages on their operations.

QUESTION 3.4: Are you monitoring geopolitical and economic factors that could impact the semiconductor market?
Again, only about half (49%) of the companies actively monitor geopolitical and economic factors that could potentially influence the semiconductor market. Among these companies, the majority rely on news outlets and media sources to stay abreast of current developments and trends. Additionally, some companies are affiliated with business associations that facilitate the exchange of pertinent data, enabling them to remain informed about relevant geopolitical and economic events. Others take a more direct approach by monitoring their partners and suppliers for any indications of shifts or disruptions in the semiconductor market. This diversity in monitoring methods highlights the importance placed on staying informed about external factors that could impact the semiconductor industry, ensuring companies can adapt their strategies and operations accordingly.

3.3.4 Section 4 - Business Impact Analysis

A business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. A BIA is an essential component of an organization's business continuity plan,

QUESTION 4.1: Which processes and functions are most critical for the organization's survival and continued operation?

Companies have identified a diverse range of functions and processes as critical to their operations. Among these, Research and Development (R&D), Sales & Marketing, and Finance have emerged as the most crucial areas for handling various business-related aspects.

Critical Processes and functions	Count	%
Finance to handle business-related aspects such as funding, accounting, budgets, and financial oversight	**17**	**13%**
HR/Personnel/Recruitment	13	10%
Information technology to develop & operate applications, systems, hardware, and software	14	11%
Operations management : how to utilizing resources from staff, materials, equipment, and technology	15	12%
Production & Quality	12	9%
Research & Development	**24**	**19%**
Sales & Marketing (Product packaging design, Event and media planning, Email marketing, Influencer marketing, digital marketing...)	**21**	**16%**
Supply chains management: Buying/Purchasing, Distribution /Logistics	12	9%
Total	**128**	**1**

Table 7 Critical processes and functions

QUESTION 4.2: Have you determined the maximum acceptable downtime for each critical function? Which is the maximum?

The majority of the companies flagged a maximum acceptable downtime value of less than 2 weeks. This means that in the event of a disruption or downtime in their operations, these companies aim to resume normal business activities within a timeframe of 2 weeks or less. Having a maximum acceptable downtime value helps companies set clear expectations and objectives for their continuity and recovery plans. By identifying and setting this threshold companies can prioritize resources and efforts towards implementing robust resilience measures and strategies to achieve timely recovery and maintain business continuity.

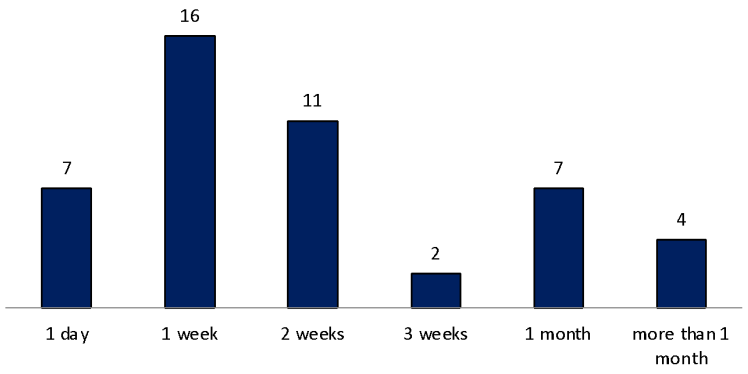

Table 8 Maximum acceptable downtime

QUESTION 4.3: What preventive measures are implemented to minimize the likelihood of disruptions? (i.e. pandemics, natural disasters, transportation failures and delays, product problems, price fluctuations, cyberattacks, redundant systems ...)

Preventive measures deployed to reduce the probability of disruption encompass consistent supplier monitoring, cybersecurity protocols, advance ordering, workforce redundancy and safety stock, and fostering employee personal development

QUESTION 4.4: Have you diversified your suppliers or partners to minimize dependency on a single source?

The adoption of a diversification strategy is widespread among companies aiming to decrease their reliance on a sole supplier or partner. Nearly three-quarters of the companies surveyed utilize such a strategy. By diversifying, companies can decrease dependency on individual suppliers or partners, lower risks, bolster resilience, seize new opportunities, and uphold regulatory compliance.

QUESTION 4.5: Have you considered implementing business continuity management standards or frameworks (e.g. ISO 22301)?

Th finding that only 7 companies from the sample implement business continuity management standards or frameworks can be attributed to various factors:

- Awareness and Understanding: many companies may lack awareness or understanding of BCM standards, leading to low prioritization
- Resource Constraints: Limited resources, including finances and expertise, may hinder companies from allocating sufficient resources to BCM implementation
- Perceived risk tolerance: some companies may believe that they can manage disruptions effectively without formal BCM frameworks, leading to lower prioritization
- Complexity and compliance burden: BCM standards can be complex and burdensome to comply with, deterring adoption due to administrative burden and compliance costs

QUESTION4 4.6: Have you identified critical suppliers and assessed their geographic locations and potential vulnerabilities?

While the findings regarding supplier diversification showed positive outcomes, it's noteworthy that only 40% of the companies surveyed possess a clear understanding of which suppliers are critical to their operations. Interestingly, many companies recognize suppliers from China and the US as being among the most critical to their business.

3.3.5 Section 5 - Business Continuity Plan

While risk management focuses on mitigating problems from the outside, business continuity plans outline what a company should do in case it faces the worst possible outcome and if it is prepared for any scenario that may come its way. BCP is a detailed strategy and set of systems for ensuring an organization's ability to prevent a rapid recovery from a significant disruption to its operations.

QUESTION 5.1: Do you have communication protocols/ business continuity plan for informing employees, customers, and stakeholders during a crisis?

Only 38% of companies have a defined communication protocol or a business continuity plan to inform shareholders during a crisis. Among those companies some have specific communications to be sent to employees in different crisis situations, others have regular training and unified communication protocols for both employees and clients.

QUESTION 5.2: Have you identified key personnel responsible for executing the plan during a crisis?

Although less than 40% of companies have a defined communication protocol to inform stakeholders, almost 50% of them have identified key people to execute the plan during a potential crisis.

Key personnel identified by companies include mainly CEOs, CTOs, Project Managers, or other members of the management team.

QUESTION 5.3: Are decision-making processes decentralized to empower teams to respond quickly to changes?

Only 43% of companies decentralize decision making processes in order to empower teams. Within the sample, companies which appointed the CEO or the management team as responsible to execute plan during a crisis, tend not to decentralize decision making processes to employees.

3.3.6 Section 6 - Testing and Exercising

T&E ensures the plan will work if needed, educating employees on their roles and responsibilities in these scenarios and conducting trials of various elements of the plan. For example, stress-tests help companies assess major changes in one or two specific variables whose effects would be major and immediate, although the exact timing is not forecastable.

QUESTION 6.1: How frequently do you conduct tests or simulations of your business resilience plan?

The majority of the companies have never conducted tests or simulations of their business resilience plan. However, tests and simulations are crucial, since they allow organizations to gauge the effectiveness of their response strategies and procedures. By simulating different scenarios, companies can assess whether their plans adequately mitigate risks and whether their response teams are prepared to execute them effectively.

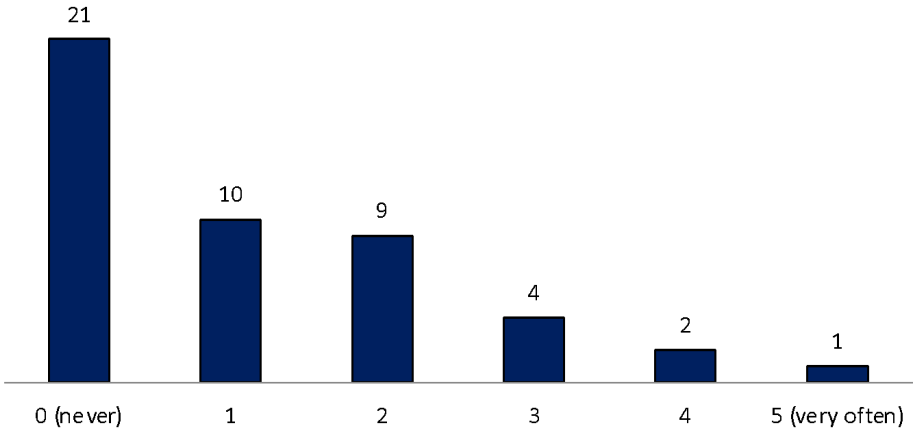

Table 9 Frequency of tests on business resilience plan

QUESTION 6.2: What lessons have you learned from previous tests or real-life incidents, and how have you incorporated them into your plan?

The lessons learned by companies from previous tests or real-life incidents are varied:

- Dependency on Asian Suppliers: Companies acknowledge the unavoidable dependency on Asian suppliers and prioritize monitoring and evaluating them based on risk.
- Quality Assurance Testing: QA testing is recognized as essential for improving product quality and resilience in production processes.
- Alternate Sourcing: The most crucial learning is to ensure alternate sourcing of both components and manufacturing services to mitigate supply chain disruptions.
- Decentralized Communication and Remote Work: Incorporating decentralized communication and remote work capabilities into BCPs to maintain operations during disruptions.

- Supplier Monitoring and Evaluation: Continuously monitoring and evaluating suppliers and supply chain risks is vital for resilience.
- Financial and Material Stockpiling: Building financial and material stocks to mitigate shortages and disruptions in the supply chain.
- Personnel Training and Delegation: Ensuring personnel are trained and having designated deputies for key roles to maintain operations during personnel absences.
- Documentation and Process Improvement: Investing in process documentation, personnel training, and documenting changes in organizational structure to enhance resilience.
- Minimize Supply Chain and Diversify Client Base: Minimizing supply chain complexity and diversifying client profiles to reduce dependency and spread risks.
- Prevention and Information Sharing: Prioritizing prevention measures and information sharing within the organization to enhance preparedness.
- Survivability Filters: Implementing filters such as team strength, financial stability, and technological readiness to assess survivability during crises.
- Suspicious Communication Protocol: Adopting a cautious approach to suspicious communication, even if it appears to originate from colleagues, to prevent security breaches.
- Warehouse Expansion: Increasing component warehouses to mitigate the impact of supply chain disruptions.
- Business Continuity Draft: Recognizing the necessity of developing a business continuity plan draft for the survival of the company during crises

By incorporating these lessons into their BCPs, companies aim to enhance their resilience and ability to withstand disruptions in the future.

QUESTION 6.3: Have you provided training to employees regarding their roles and responsibilities during a disruption?

Only 28% of companies provide regular training to employees regarding their roles and responsibilities during a crisis. However, regular training plays a crucial role in enhancing employee preparedness, clarity of roles, coordination, communication, confidence, and resilience during a crisis. It is an essential component of effective crisis management and should be prioritized by organizations seeking to strengthen their resilience and response capabilities.

QUESTION 6.4: Are there regular refresher training sessions to keep employees prepared and informed?

The fact that only 23% of companies provide regular refresher training sessions underscores a missed opportunity in maintaining employee preparedness and awareness. These sessions serve as valuable opportunities to reinforce crisis response protocols, update employees on evolving best practices, and ensure that everyone remains informed and ready to act effectively during emergencies. Without regular refresher training, there's a risk of knowledge degradation over time and employees may not be adequately equipped to handle unexpected situations, potentially compromising the organization's ability to manage crises efficiently.

3.3.7 Section 7 - Technological Resilience

T&R prepares organizations to overcome challenges when their technology stack is compromised, reducing the frequency of catastrophic events and enabling them to recover faster in the case of an event (it is also defined as DRP disaster recovery plan).

QUESTION 7.1: How do you stay updated on technological advancements in the semiconductor industry?

Companies stay updated on technological advancements through various means. Some of them include:

- Regular visits to online media platforms, reading specialized press publications and magazines
- Engagement with scientific literature, exploring research papers
- Interaction with R&D institutes and participation in events (online seminars, clusters' events)
- Utilization of marketing analysis and customer inputs
- Engagement with suppliers

QUESTION 7.2: Do you have strategies in place to pivot or adapt your product offerings based on market trends?

Roughly 50% of companies have defined strategies to adapt their product offering according to market trends. Some of them actively engage in R&D projects to align with current trends and customer needs. Others regularly adapt their roadmap based on market feedback, emphasizing modular product designs, flexible services and continuous monitoring.

QUESTION 7.3: Do you conduct regular testing and validation of your products to ensure their performance and reliability?

The majority of companies, specifically 81%, engage in regular testing and validation procedures for their products. This process involves systematically assessing the performance and reliability of their products through various testing methodologies. These tests may include functional testing, stress testing, durability testing, and quality assurance checks to ensure that the products meet predetermined standards and specifications. By conducting regular testing and validation, companies can identify and address any potential issues or defects early in the product development lifecycle, thereby enhancing the overall quality, reliability, and customer satisfaction of their products. This proactive approach helps companies maintain a competitive edge in the market and build trust with their customers by delivering high-quality and reliable products.

QUESTION 7.4: How do you safeguard your intellectual property (IP) and proprietary technologies?

Only 62% of companies within the sample safeguard their intellectual property and proprietary technologies. Various means are used, including:

- Innovation: developing solutions that are difficult to copy and constantly progressing
- Legal protection: obtaining patents, design protection, trademark protection and entering into non-disclosure agreements (NDAs) to safeguard inventions and designs
- Business logic: Utilizing business logic to protect proprietary processes and methodologies
- Restricted access: controlling access to sensitive information within the organization
- Cybersecurity measures: incorporating cybersecurity measures to protect digital assets, encrypting data to prevent unauthorized access

QUESTION 7.5: Have you established legal protections and agreements to prevent unauthorized use of your IP?

Approximately 60% of the companies surveyed have taken proactive measures to safeguard their intellectual property (IP) through legal means. This includes establishing legal protections such as patents, trademarks, and design protections to secure their inventions, designs, and processes. Additionally, these companies have entered into agreements, such as non-disclosure agreements (NDAs), with employees, customers, and suppliers to prevent unauthorized use or disclosure of their proprietary information. By implementing these legal safeguards, these companies aim to protect their valuable IP assets and maintain their competitive advantage in the market.

QUESTION 7.6: Are you prepared to respond to IP infringement disputes or legal challenges?

55% of the companies surveyed have measures in place to respond to intellectual property (IP) infringement disputes or legal challenges, while the remaining 45% do not have such preparations. Being prepared to respond to IP infringement disputes or legal challenges involves having a strategy and resources in place to address allegations of IP infringement or unauthorized use of proprietary technology, designs, or trademarks. This may include having legal representation, documentation of IP rights, and processes for monitoring and enforcing IP protection. Companies that are prepared for such challenges are better equipped to defend their intellectual property rights, mitigate potential damages, and safeguard their competitive advantage in the marketplace. On the other hand, companies that lack preparation may face greater risks of financial losses, reputational damage, and legal liabilities in the event of IP infringement disputes or legal challenges. Therefore, being prepared to respond to IP infringement disputes or legal challenges is essential for protecting and defending valuable intellectual property assets.

QUESTION 7.7: Do you have a communication plan to address stakeholders during an electronics/ semiconductors-related crisis (e.g. supply chain disruption, product recall)?

Out of the entire sample of companies surveyed, only nine have developed a specific communication plan to address stakeholders during a crisis related to the electronics or semiconductor industry. A communication plan outlines the strategies, channels, and messaging a company will use to communicate with various stakeholders, including employees, customers, investors, regulators, and the public, during a crisis.

For companies without a communication plan, the lack of preparedness poses significant risks. During a crisis, effective communication is crucial for managing the situation, mitigating potential damage to the company's reputation, and maintaining stakeholders' trust and confidence. Without a structured plan in place, companies may struggle to provide timely and accurate information, leading to confusion, speculation, and loss of credibility.

QUESTION 7.8: How do you manage and protect your company's reputation in the face of challenges?

Companies employ various strategies to manage and protect their reputation in the face of challenges:

- Continuous cooperation and open communication with clients: maintaining ongoing collaboration with clients foster trust and strengthens the company reputation
- Team cohesion: keeping the team united ensures a cohesive approach to addressing challenges and upholding the company's image
- Risk management and planning: Implementing robust risk management strategies and contingency plans helps mitigate potential threats to the company's reputation

- Effective support during problems: Providing timely and effective support when issues arise demonstrates commitment to customer satisfaction and protects the company's reputation
- Legal advice: Seeking legal advice, when necessary, ensures compliance with regulations and protects the company's reputation from legal risks
- Proactive public relations: Engaging in proactive public relations efforts helps shape public perception and protect the company's reputation

QUESTION 7.9: Please tick the profiles that from your point of view are the most sought after by European industry since January 2022 (in terms of number of hires)

The profiles most sought after by European industry, from companies' perspective, include:

- Software Engineers: Software engineers are essential for developing and maintaining software applications and systems across various industries. With the increasing digitization of business processes and the growing importance of software-driven solutions, the demand for skilled software engineers is on the rise. These professionals possess expertise in programming languages, software development methodologies, and system architecture design. They work on diverse projects, ranging from developing enterprise software applications to designing embedded systems for IoT (Internet of Things) devices. Software engineers play a critical role in driving technological innovation and digital transformation initiatives within European industries.
- Design Engineers: Design engineers are in high demand across European industries due to their critical role in product development and innovation. These professionals are responsible for conceptualizing, designing, and prototyping new products or systems. They possess a deep understanding of engineering principles, CAD software, and manufacturing processes. Design engineers collaborate closely with cross-functional teams to translate customer requirements into viable product designs that meet quality standards and market demands. Their expertise is essential for driving product innovation and maintaining competitiveness in dynamic markets.
- Data Scientists: With the increasing importance of data-driven decision-making, data scientists are highly sought after by European industries. These professionals possess the expertise to analyze large volumes of data, derive meaningful insights, and develop predictive models. Their skills in data mining, machine learning, and statistical analysis are invaluable for businesses looking to gain a competitive edge through data-driven strategies. Data scientists play a crucial role in various sectors, including finance, healthcare, manufacturing, and technology.

Profiles that are the most sought after by European industry since January 2022 (in terms of number of hires)	Count	%
Analog design engineer	3	2%
Application engineer	5	4%
Data scientist	**15**	**12%**
Design engineer: i.e. Electrical design engineer, electrical project engineer, electrical product engineer, product developn	**20**	**16%**
Digital design engineer	5	4%
Expert in cybersecurity	8	6%
Maintenance technician: Electrical technician, breakdown technician	3	2%
Marketing engineer	4	3%
Operator / Inspector: Machine operator, inspector, repair operator, general laborer	4	3%
Process engineer: Manufacturing (support) engineer	4	3%
Process technician: Manufacturing (support) technician	5	4%
Robotic engineer: Electrical automation engineer, controls and robotic engineer, control system engineer, PLC programmer engin	7	6%
Software engineer	**29**	**23%**
System design engineer (complex ASIC, SoC, SiP, SoP)	5	4%
Test engineer: Product test engineer, test engineer, Design For Test (DFT) engineer, associate test engineer, senior test enginee	7	6%
Test technician: Electrical test technician, environmental and life-time test technician, troubleshooter technician, quality technician	1	1%
Total	**125**	**1**

Table 10 Most sought profiles in EU

QUESTION 7.10: Do you review and update your business continuity plan periodically?

Results are positive because a majority, specifically 62% of the companies surveyed, regularly review and update their business plans.

Periodically reviewing and updating the business plan is crucial for ensuring that the company remains agile, responsive, and aligned with its strategic objectives and market conditions. By regularly assessing the business plan, companies can identify emerging opportunities, anticipate challenges, and adjust their strategies accordingly. This iterative process enables organizations to adapt to changes in the competitive landscape, customer preferences, technology advancements, and regulatory requirements.

Companies that review and update their business plans periodically demonstrate a commitment to continuous improvement and strategic foresight. They are better positioned to capitalize on market trends, innovate products and services, optimize resource allocation, and mitigate risks effectively. Ultimately, this proactive approach enhances the company's resilience, competitiveness, and long-term sustainability in a dynamic business environment.

QUESTION 7.11: Is there a mechanism in place to gather feedback from employees and stakeholders for plan improvement? (test, questionnaire, simulation, teambuilding, …)

While a majority of companies, specifically 62%, regularly review and update their business plans, a smaller percentage, only 43%, incorporate feedback from employees and stakeholders during this process.

Incorporating feedback from employees and stakeholders is essential for creating a comprehensive and effective business plan. Employees, being closely involved in day-to-day operations, often possess valuable insights into the company's strengths, weaknesses, opportunities, and threats. Likewise, stakeholders such as customers, suppliers, investors, and community members can provide valuable perspectives on market trends, customer needs, industry regulations, and societal expectations.

By involving employees and stakeholders in the business planning process, companies can gain a more holistic understanding of their business environment and make more informed strategic decisions. This collaborative approach fosters a sense of ownership, engagement, and alignment among stakeholders, leading to greater buy-in and support for the company's goals and initiatives.

Companies that fail to incorporate feedback from employees and stakeholders may overlook important insights and perspectives, leading to potential blind spots, missed opportunities, and disconnects between the business plan and stakeholder expectations. This could result in suboptimal decision-making, reduced employee morale, stakeholder dissatisfaction, and ultimately, hindered business performance and growth.

Therefore, while regular review and updating of the business plan are important, it's equally crucial for companies to actively seek and incorporate feedback from employees and stakeholders to ensure the plan remains relevant, realistic, and responsive to the evolving needs and dynamics of the business environment.

3.3.8 Section 8 - Green Topics

QUESTION 8.1: What actions is your company undertaking to be more resource efficient?

The current trend among companies involves implementing targeted measures to enhance resource efficiency, with various initiatives being undertaken to achieve this goal. Some of the most prevalent initiatives include:

- Product Designs for Maintenance, Repair, or Reuse (17%): Many companies are focusing on designing products that are easier to maintain, repair, or reuse. By incorporating features such

as modular components, standardized parts, and simplified assembly processes, companies aim to prolong the lifespan of their products and reduce the need for frequent replacements. This approach not only enhances resource efficiency but also contributes to reducing waste and promoting sustainability.

- Energy Saving Efforts (16%): Another common initiative is implementing energy-saving measures to reduce energy consumption and minimize environmental impact. Companies are adopting various strategies such as upgrading energy-efficient equipment, optimizing production processes, and implementing smart energy management systems. By reducing energy usage, companies not only lower their operational costs but also mitigate their carbon footprint and contribute to environmental conservation efforts.
- Waste Minimization Endeavours (16%): Many companies are prioritizing waste minimization initiatives to reduce the generation of waste and promote recycling and reuse practices. This includes implementing waste reduction strategies throughout the production process, such as optimizing material usage, implementing recycling programs, and adopting circular economy principles. By minimizing waste generation, companies can reduce disposal costs, conserve resources, and mitigate environmental pollution.

These initiatives reflect a growing recognition among companies of the importance of resource efficiency in achieving sustainable business practices. By adopting targeted measures such as product design improvements, energy-saving efforts, and waste minimization endeavours, companies can enhance their operational efficiency, reduce their environmental footprint, and contribute to the transition towards a more sustainable economy.

QUESTION 8.2: What type of support does your company rely on in its efforts to be more resource efficient?

Nearly 40% of companies depend on supplementary public funding initiatives, such as grants, guarantees, or loans, to enhance resource efficiency. Additionally, a portion of these companies seek guidance from business associations and clusters (14%), while others consider private funding sources like banks, investment firms, or venture capital (11%). However, alternative forms of non-financial advice (from consulting/audit companies, public authorities, or supply chain partners) appear to be less commonly utilized, as well as private funding from personal networks like friends and relatives.

QUESTION 8.3: Which one of the following would help your company the most to be resource efficient?

To improve resource efficiency almost ⅓ of the companies would mainly need:

- Grant or subsidies (29%): access to such funding can offset the initial cost associated with implementing efficiency measures and incentivize companies to adopt sustainable strategies
- Demonstration of new technologies or processes to improve resource efficiency (15%): these demonstrations provide valuable insights into the feasibility, effectiveness, and potential benefits of adopting new solutions, helping companies make informed decisions about their investments in resource efficiency
- Advice on funding possibilities and financial planning for resource efficiency investments (12%): expert advice can help companies navigate complex funding landscapes, identify suitable financing options, and develop robust financial plans to support their efficiency initiatives effectively

Overall, addressing these needs can empower companies to overcome barriers and accelerate their journey towards achieving greater resource efficiency and sustainability.

QUESTION 8.4: Does your company offer green products or services?

The fact that nearly 70% of European companies are currently offering or planning to offer green products and services within the next two years reflects a significant focus on sustainability matters. This trend demonstrates a growing awareness of environmental responsibility and a proactive response to consumer demand for eco-friendly options. By embracing sustainability initiatives, companies not only contribute to environmental protection but also seize market opportunities, enhance competitiveness, and strengthen their corporate social responsibility profiles.

QUESTION 8.5: Does your company encounter any of the following difficulties when trying to set up resource efficiency actions?

The primary challenges faced by companies when implementing resource efficiency actions often revolve around economic and administrative barriers. Economically, companies struggle with the high costs associated with environmental initiatives, which can include investments in green technologies, process upgrades, and sustainable practices. On the administrative side, complexities arise from navigating intricate legal and administrative procedures and obtaining environmental labeling and certification. These hurdles can pose significant barriers to companies seeking to improve resource efficiency, requiring careful planning, resource allocation, and expertise to overcome.

4. FOCUS ON BUSINESS RESILIENCE AND RECOVERY PLAN IMPLEMENTATION

The three most represented business segments in the survey are Electronics and Microelectronics Energy/ Environment, ICT and Machine tools, plant engineering/ robotics & automation.

Within this chapter, our goal is to describe the specific characteristics of Resilience/ Preparedness Business Continuity Plan (RPBCP) for these sectors and to provide some useful tools/ frameworks in support.

4.1 Electronics and Microelectronics Energy/ Environment

4.1.1 Sector Overview

The Electronics and Microelectronics sector involves producing and distributing electronic components and devices at micro and nanoscales, crucial for industries like telecommunications, consumer electronics, and healthcare. It's known for its innovation in integrated circuits, semiconductor devices, and sensors, and it is driven by technological advancements, global competition, and a focus on miniaturization and connectivity.

4.1.2 How to implement a RPBCP

To build an efficient RPBCP in the electronics and microelectronics sector, several useful frameworks can be applied to assess risks, identify vulnerabilities, and develop strategies for resilience. Here are some of them:

- **SWOT Analysis**: it helps identify internal strengths and weaknesses of the organization, as well as external opportunities and threats in the market environment. In the electronics and microelectronics sector, this analysis can highlight strengths in technological innovation, weaknesses in supply chain dependencies, opportunities in emerging markets, and threats from rapid technological changes or supply chain disruptions.
- **PESTEL Analysis**: it evaluates external factors that could impact the business environment in the electronics and microelectronics sector. This includes factors that could impact the business environment in the sector, such as regulatory changes, economic trends, technological advancements, environmental regulations, and legal requirements.
- **Risk Assessment and Management**: conduct comprehensive risk assessments to identify and prioritize risks specific to the electronics and microelectronics sector, such as supply chain disruptions, cybersecurity threats, technological failures, or regulatory changes. Use risk management strategies to mitigate, transfer, or accept identified risks.
- **Supply Chain Risk Management**: evaluate supply chain vulnerabilities and dependencies within the electronics and microelectronics sector, considering factors such as sourcing of raw materials, transportation logistics, and supplier reliability. Develop strategies to diversify suppliers, establish alternative sourcing options, and strengthen relationships with key suppliers to mitigate supply chain disruptions.
- **Technological Risk Assessment:** identify and mitigate technological risks specific to the electronics and microelectronics sector, such as rapid technological obsolescence, intellectual property theft, cybersecurity threats and product quality issues. Implement measures to

protect sensitive data, intellectual property, and critical infrastructure from cyberattacks and technological disruptions.

- **Regulatory Compliance Frameworks**: ensure compliance with industry-specific regulations and standards governing the electronics and microelectronics sectors, such as the ISO standards for quality management and environmental management systems. Develop processes and procedures to meet regulatory requirements and enhance resilience to regulatory changes.
- **Crisis Management Plan**: develop a crisis management plan that outlines protocols, roles, and responsibilities for responding to emergencies or crises in the electronics and microelectronics sector. This plan should include communication strategies, escalation procedures, and recovery measures to ensure business continuity, with a focus on restoring manufacturing operations and customer deliveries.

By utilizing these frameworks, organizations in the electronics and microelectronics sector can develop an efficient Resilience Preparedness/Business Continuity Plan to mitigate risks, enhance resilience, and sustain business continuity in the face of disruptions and uncertainties.

4.1.3 Useful tools to support the implementation of RPBCP

Here are some online tools specifically tailored for resilience planning in the electronics and microelectronics energy/environment sector:

- **Resilinc:** Resilinc offers a comprehensive platform for supply chain resilience and risk management, which can be tailored for the electronics and microelectronics energy/environment sector. Their solution provides real-time monitoring, risk assessment, and visualization tools to help organizations identify vulnerabilities and develop strategies to mitigate disruptions. Link
- **Riskmethods:** Riskmethods provides supply chain risk management software designed for various industries, including electronics and microelectronics energy/environment. Their platform enables organizations to identify, assess, and mitigate risks across the supply chain, with features such as supplier risk assessment, monitoring, and incident response planning. Link
- **Resilience360 by DHL**: Resilience360, offered by DHL, is a cloud-based platform that helps organizations monitor, assess, and mitigate risks in their supply chains, including those in the electronics and microelectronics energy/environment sector. It offers tools for supply chain visibility, risk assessment, and contingency planning. Link
- **Elementum:** Elementum provides a supply chain orchestration platform with capabilities for risk management and resilience planning, suitable for the electronics and microelectronics energy/environment sector. Their platform helps organizations proactively identify and respond to supply chain disruptions, ensuring continuity of operations. Link
- **Avetta**: Avetta offers a supplier risk management platform that helps organizations in various sectors, including electronics and microelectronics energy/environment, assess and manage supplier risk. Their platform includes tools for supplier prequalification, compliance management, and risk assessment, enabling organizations to build resilient supply chains. Link
- **Oracle Supply Chain Management Cloud**: Oracle's suite of cloud-based supply chain management solutions includes resilience planning capabilities suitable for the electronics and microelectronics energy/environment sector. Their platform helps organizations optimize supply chain operations, mitigate risks, and respond effectively to disruptions. Link

These tools can assist organizations in the electronics and microelectronics energy/environment sector in proactively identifying and mitigating risks in their supply chains, ensuring resilience and continuity of operations even in the face of disruptions.

4.2 ICT

4.2.1 Sector Overview

The ICT (Information and Communication Technology) sector encompasses technologies involved in storing, retrieving, transmitting, and manipulating data. It includes hardware, software, networks, and services, playing a central role in modern communication, computing, and information systems. Key components include computers, software applications, telecommunications infrastructure, and internet services. The sector drives innovation across industries, facilitating connectivity, automation, and digital transformation. Rapid advancements in ICT continually shape and redefine how businesses and individuals interact, communicate, and access information.

4.2.2 How to implement a RPBCP

By utilizing the following frameworks organizations within the ICT sector can develop an effective Resilience Preparedness/Business Continuity Plan to mitigate risks, enhance resilience, and sustain business continuity in the face of disruptions and uncertainties specific to the ICT industry.

- **SWOT Analysis**: in the ICT sector, this analysis can highlight strengths in technological innovation, weaknesses in cybersecurity infrastructure, opportunities in emerging markets, and threats from rapid technological changes.
- **PESTEL Analysis**: in addition to factors like regulatory changes and economic trends, the ICT sector may face unique technological challenges such as rapid advancements, emerging cybersecurity threats, and evolving consumer preferences.
- **Risk Assessment and Management**: conduct comprehensive risk assessments to identify and prioritize risks specific to the ICT sector, such as cybersecurity threats, technological failures, regulatory changes, or natural disasters. Given the nature of the ICT sector, there may be a greater emphasis on cybersecurity risks and vulnerabilities in data infrastructure and networks.
- **VUCA Framework**: The VUCA framework helps organizations understand and navigate the volatile and uncertain business environment. In the ICT sector, organizations may face rapid technological changes, evolving consumer demands, and geopolitical uncertainties, necessitating a proactive approach to adaptability and resilience.
- **Scenario Planning**: Develop multiple plausible scenarios of potential disruptions, such as cyberattacks, system failures, or supply chain disruptions. Given the interconnected nature of ICT systems, scenario planning in the ICT sector may focus on understanding cascading effects and dependencies across networks and infrastructure.
- **Cybersecurity Frameworks**: Implement cybersecurity frameworks such as NIST Cybersecurity Framework or ISO/IEC 27001 to identify, protect, detect, respond to, and recover from cybersecurity threats in the ICT sector. Enhance cybersecurity measures to protect sensitive data, intellectual property, and critical infrastructure, recognizing the central role of cybersecurity in ICT resilience.
- **Crisis Management Plan**: Develop a crisis management plan that outlines protocols, roles, and responsibilities for responding to emergencies or crises in the ICT sector. This plan should

include communication strategies, escalation procedures, and recovery measures to ensure business continuity, with a focus on restoring digital services and data integrity.

4.2.3 Useful tools to support the implementation of RPBCP

Here are some online tools specifically tailored for resilience planning in the ICT (Information and Communication Technology) sector:

- **Resilience360 by DHL[4]:** Link
- **Riskmethods[4]**: Link
- **Everbridge**: Everbridge offers a Critical Event Management platform that helps organizations in the ICT sector manage and respond to critical events and disruptions. It provides real-time threat intelligence, communication tools, and incident response capabilities to ensure business resilience. Link
- **Sungard AS**: Sungard AS provides a suite of IT resilience solutions tailored for the ICT sector. Their offerings include disaster recovery as a service (DRaaS), business continuity planning, and managed IT services to help organizations ensure the availability and resilience of their IT infrastructure. Link
- **IBM Resilience**: IBM offers a range of resilience solutions for the ICT sector, including business continuity planning, disaster recovery, and cyber resilience. Their platform provides capabilities for risk assessment, incident response, and recovery to help organizations maintain continuity of operations. Link
- **MetricStream**: MetricStream offers a Governance, Risk, and Compliance (GRC) platform with modules for business continuity management and risk assessment, suitable for the ICT sector. Their solution helps organizations streamline resilience planning, compliance, and incident response processes. Link
- **BMC Helix ITSM**: BMC Helix IT Service Management (ITSM) provides IT service management capabilities that include incident management, change management, and service continuity planning, specifically designed for the ICT sector. It helps organizations manage and respond to IT disruptions effectively. Link

4.3 Machine tools, plant engineering/ robotics & automation

4.3.1 Sector Overview

The Machine Tools, Plant Engineering/Robotics & Automation sector involves the design, manufacturing, and implementation of machinery and systems for industrial automation and manufacturing processes. It encompasses a wide range of equipment, including machine tools, robotic systems, and automation solutions. This sector plays a vital role in increasing productivity, precision, and efficiency in manufacturing operations across various industries, such as automotive, aerospace, and electronics. Key focuses include developing advanced robotics, automation technologies, and intelligent manufacturing systems to streamline production processes and meet evolving industry demands.

[4] These tools can be used across both Electronics and ICT sectors

4.3.2 How to implement a RPBCP

Here are some useful tools and frameworks for developing a Resilience Preparedness/Business Continuity Plan (BCP) in the Machine Tools, Plant Engineering/Robotics & Automation sector:

- **SWOT Analysis**: in the Machine Tools, Plant Engineering/Robotics & Automation sector, this analysis can highlight strengths in technological expertise, weaknesses in supply chain dependencies, opportunities in emerging markets, and threats from technological disruptions.
- **PESTEL Analysis**: in addition to factors like regulatory changes and economic trends, this sector may face unique challenges such as technological advancements, changing environmental regulations, and global economic shifts impacting demand.
- **Risk Assessment and Management**: conduct comprehensive risk assessments to identify and prioritize risks specific to the Machine Tools, Plant Engineering/Robotics & Automation sector, such as supply chain disruptions, equipment failures, cybersecurity threats, or regulatory compliance issues. Implement risk management strategies to mitigate, transfer, or accept identified risks.
- **VUCA Framework**: in this sector, organizations may face volatility in demand, uncertainty in technological advancements, complexity in supply chain logistics, and ambiguity in regulatory requirements, necessitating an adaptive and resilient approach.
- **Scenario Planning**: given the sector's reliance on advanced machinery and automation, scenario planning may focus on understanding the impact of technological failures or disruptions in supply chains on production processes and customer deliveries.
- **Supply Chain Risk Management**: evaluate supply chain vulnerabilities and dependencies within the sector, considering factors such as sourcing of raw materials, transportation logistics, and supplier reliability. Develop strategies to diversify suppliers, establish alternative sourcing options, and strengthen relationships with key suppliers to mitigate supply chain disruptions.
- **Crisis Management Plan**: Develop a crisis management plan that outlines protocols, roles, and responsibilities for responding to emergencies or crises in the Machine Tools, Plant Engineering/Robotics & Automation sector. This plan should include communication strategies, escalation procedures, and recovery measures to ensure business continuity, with a focus on restoring manufacturing operations and customer deliveries.

By utilizing these tools and frameworks tailored to the Machine Tools, Plant Engineering/Robotics & Automation sector, organizations can develop an effective Resilience Preparedness/Business Continuity Plan to mitigate risks, enhance resilience, and sustain business continuity in the face of disruptions and uncertainties specific to this industry.

4.3.3 Useful tools to support the implementation of RPBCP

Here are some online tools specifically tailored for resilience planning in the machine tools, plant engineering, and robotics automation sector:

- **ROB-EX Scheduler**: ROB-EX Scheduler is a production planning and scheduling software designed for manufacturing companies, including those in the machine tools and robotics automation sector. It helps organizations optimize production processes, allocate resources efficiently, and respond effectively to disruptions. Link
- **FactoryLogix MES**: FactoryLogix Manufacturing Execution System (MES) is a comprehensive software solution for managing production operations, quality, and traceability in the

manufacturing industry. It offers features such as real-time monitoring, workflow automation, and predictive analytics, helping organizations enhance resilience and agility in their operations. Link

- **Visual Components**: Visual Components provides 3D simulation and visualization software for designing and optimizing manufacturing processes, including those in the robotics automation sector. It enables organizations to create digital twins of their production environments, simulate various scenarios, and identify opportunities for improvement to enhance resilience. Link
- **Siemens Tecnomatix**: Siemens Tecnomatix is a digital manufacturing software suite that offers solutions for process planning, simulation, and optimization in the plant engineering and robotics automation sector. It helps organizations streamline production workflows, reduce cycle times, and improve overall resilience in manufacturing operations. Link
- **Rockwell Automation FactoryTalk ProductionCentre**: Rockwell Automation FactoryTalk ProductionCentre, a manufacturing operations management (MOM) software suite that helps organizations in the machine tools and robotics automation sector optimize production processes, monitor performance in real-time, and respond quickly to disruptions. Link
- **ABB RobotStudio**: ABB RobotStudio is a simulation and programming software for robot systems. It allows organizations in the robotics automation sector to design, simulate, and optimize robot applications, ensuring resilience through virtual testing and validation of automation processes before implementation. Link
- **Hexagon Production Software**: Hexagon offers a range of production software solutions, including CAM (Computer-Aided Manufacturing) and MES (Manufacturing Execution System) software, designed to optimize manufacturing processes and enhance resilience in the machine tools and plant engineering sector. Link

These tools can assist organizations in the machine tools, plant engineering, and robotics automation sector in proactively identifying and mitigating risks, ensuring resilience, and maintaining continuity of operations in the face of disruptions.

5. CLUSTER RESILIENCE SURVEY

5.1 Cluster survey ratio and structure

The analysis provided operates on a European scale, encompassing clusters not solely dedicated to electronics but also those with significant representation from this sector. This approach was chosen to broaden the scope of our study, incorporating a diverse array of European clusters to facilitate comprehensive data processing and analysis.

The primary objective of the survey is to identify and address deficiencies within clusters, promoting knowledge sharing across clusters to bolster support for European SMEs in fortifying their resilience. Top of Form

European clusters stand to gain several benefits by participating in this survey, including:

- Access to strategic insights and tools to bolster resilience and competitiveness.
- Early access to strategic information regarding services and funding opportunities, such as the open call for green financial support
- Influence EU semiconductor policy by leveraging the Silicon Eurocluster as a platform to voice interests and needs.
- Foster synergies and share best practices to enhance effectiveness within their ecosystem.

The survey was designed to maintain anonymity and was concise, comprising fewer than ten questions. The survey can be accessed here.

5.2 Cluster survey results

QUESTION 1: How would you rate the cluster's overall level of resilience in the face of disruptions (from 1 to 5)?

To assess their resilience, clusters should monitor various metrics including employee engagement, turnover rates, customer satisfaction, loyalty metrics, and innovation indices. By analyzing these metrics, clusters can identify areas of strength as well as gaps that need attention, thereby enhancing their resilience. On average, clusters demonstrated a level of resilience around 3.5 on a scale from 1 to 5 when facing disruptions. This indicates a moderate level of resilience, suggesting that while clusters possess some strengths, there is still room for improvement to better navigate and withstand disruptive challenges. By tracking these metrics and striving for continuous improvement, clusters can enhance their overall resilience and adaptability in the face of uncertainties.

Cluster's overall level of resilience in the face of disruptions	Count	%
1	0	0%
2	3	10%
3	12	40%
4	13	43%
5	2	7%
Total	**30**	**1**

Table 11 Clusters' overall resilience level (scale 1-5)

QUESTION 2: Does your cluster organize activities for your team? (training, team building, special meetings, workshops...)?

Almost all clusters organize training, team building and other special activities for their teams at least once per year. The majority of them organize them periodically.

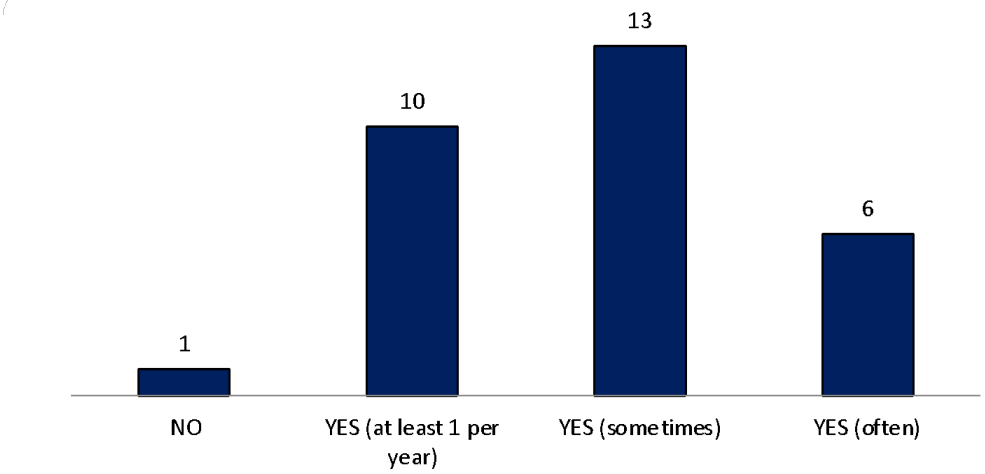

Table 12 Frequency of organization of team activities

QUESTION 3: If you reply YES to the question above, what are the main topics addressed by these activities? Please refer to the activities realized by your cluster

Team activities organized by clusters cover a range of important topics to support their members. The main areas addressed by these activities include:

- **Funding Opportunities (24%)**: to provide information and guidance on accessing funding sources, such as grants, loans, or investment opportunities
- **Soft Skills (22%)**: to enhance employees' interpersonal, communication, leadership, and teamwork skills. These skills are crucial for fostering effective collaboration, problem-solving, and decision-making within organizations
- **Technological Megatrends (22%)**: to keep personnel informed about emerging technological trends and innovations that have the potential to disrupt industries or create new business opportunities
- **Business Methodologies (17%)**: to provide employees with tools, frameworks, and best practices for improving their operational efficiency, strategic planning, marketing, and other business functions. This enables them to optimize their processes and achieve sustainable growth to incentive employees to adopt eco-friendly practices, reduce their environmental footprint, and capitalize on opportunities in the green economy.

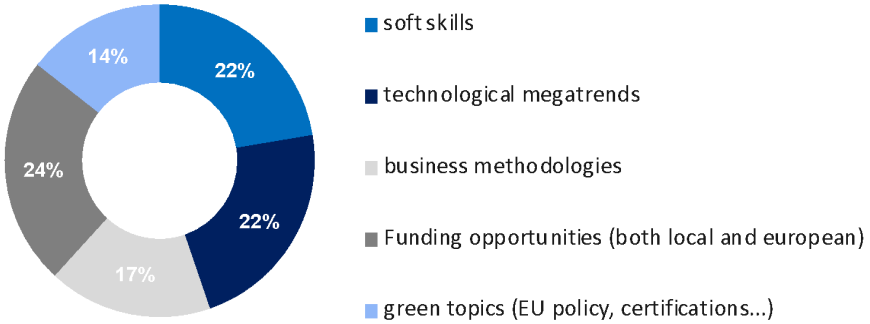

Table 13 Main topics addressed by team activities

QUESTION 4: How does your cluster secure funding and financial sustainability for its initiatives?

Almost all clusters secure funding and financial sustainability through a balanced mix of Regional Funds, EU Funds and Members' fees.

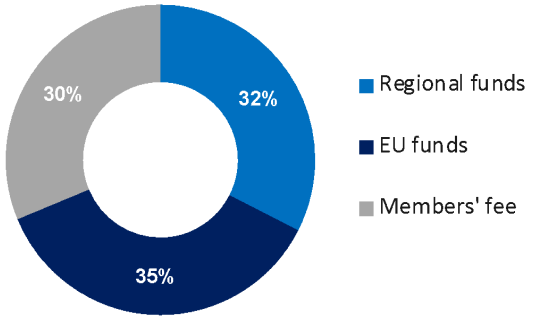

Table 14 How clusters secure funding and financial sustainability

QUESTION 5: How does your cluster communicate and share information with its stakeholders during crisis (e.g. covid19, conflicts, shortage) and related measures (e.g. private and public measures, initiatives, technologies)?

Clusters employ a diverse mix of communication channels to engage with their stakeholders effectively. The primary communication means utilized by clusters include websites, newsletters, social, emails, webinars and events. By employing this mix of communication channels, clusters can effectively engage with their stakeholders, build relationships, foster collaboration, and drive collective action towards common goals. These means of communication enable clusters to disseminate information, facilitate knowledge-sharing, and create a sense of community among stakeholders within the cluster ecosystem.

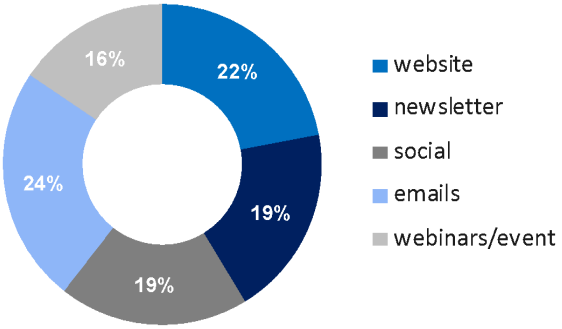

Table 15 How clusters communicate and share info with shareholders

QUESTION 6: Does the cluster have a formalized resilience and recovery plan?

It's notable that none of the clusters that participated in the study have a formalized resilience and recovery plan in place.

If there is no such plan, clusters may face challenges in effectively mitigating risks, minimizing the impact of disruptions, and swiftly recovering operations. Formalized plans provide a roadmap for coordinated responses, helping to ensure continuity of essential services, protect assets and resources, and maintain stakeholder confidence during times of adversity

QUESTION 7: Please provide any suggestions, or recommendations for enhancing the clusters' resilience

To enhance their own resilience, clusters provided the following suggestions:

- Focus on Soft Skills and Methodology: improve soft skills and establish a shared methodology for addressing problems and meeting companies' needs through team-building activities
- Increase collaboration within the Ecosystem: collaborate with other entities/ clusters within the ecosystem to ensure the resilience of the cluster and prevent/ respond to upcoming challenges collectively
- Staff training and empowerment: provide staff with valuable tools and training to empower them and enhance their capabilities
- Secure members' loyalty: build and maintain members' loyalty through valuable services and contribute to regional policy to strengthen the cluster's position
- Diversify financing sources: explore diverse sources of financing to ensure sustainable funding for cluster activities
- Share best practices: share best practices and knowledge among clusters to learn from each other
- Prioritize cybersecurity: address cybersecurity concerns to protect cluster operations and members' data

5.3 Useful tools to increase Clusters' Resilience

Here are some useful links for European clusters looking to improve their resilience:

- **European Cluster Collaboration Platform**: ECCP provides a wealth of resources, tools, and opportunities for European clusters to collaborate, share best practices, and enhance their resilience. They offer matchmaking events, webinars, and access to funding opportunities. ECCP website
- **European Commission's Cluster Policy**: The European Commission has a dedicated section on its website outlining cluster policy initiatives, funding programs, and support mechanisms aimed at strengthening clusters across Europe. European Commission's Cluster Policy
- **Horizon Europe**: The EU's flagship research and innovation program, Horizon Europe, offers various funding opportunities for clusters to engage in collaborative projects, innovation activities, and capacity building aimed at enhancing resilience. Horizon Europe website
- **European Cluster Observatory**: This platform provides insights, analyses, and data on clusters across Europe, helping cluster organizations to understand market trends, identify opportunities, and develop strategies for resilience. European Cluster Observatory
- **European Enterprise Network**: EEN offers support services to help businesses and clusters access international markets, find partners, and navigate EU regulations. They provide valuable resources and networking opportunities for clusters aiming to strengthen their resilience. EEN website
- **European Regional Development Fund** (ERDF): ERDF supports regional development initiatives, including those aimed at strengthening industrial clusters and fostering innovation. Clusters can explore funding opportunities through their regional ERDF programs. ERDF website
- **European Innovation Partnership** (EIP) on Smart Cities and Communities: Clusters focusing on smart city solutions can benefit from the resources and collaboration opportunities offered by

the EIP on Smart Cities and Communities, which aims to accelerate the transition to sustainable and resilient urban development. EIP website

These resources should provide a good starting point for European clusters seeking to enhance their resilience and competitiveness.

Digital Sources

- European Commission Staff Working Document: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024SC0077
- The 2024 Annual Single Market and Competitiveness Report: https://single-market-economy.ec.europa.eu/publications/2024-annual-single-market-and-competitiveness-report_en
- Accenture Research Reports: https://www.accenture.com/it-it
- L'Europa alla guerra dei chips: https://www.ispionline.it/it/pubblicazione/leuropa-alla-guerra-dei-chips-36760
- The European Chips Act: https://www.european-chips-act.com/European_Chips_Act_Links.html
- The EU Cybersecurity Act: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- Risk Engineering – Electronics & Semiconductors: https://www.tuvsud.com/en-us/services/risk-management/semiconductor
- How to Manage Supply Chain Risks in Electronics Manufacturing 2024: https://www.icdrex.com/manage-supply-chain-risks-electronics-manufacturing-guide/
- SEMI issues recommendations for European Commission to bolster Europe's Chip Ecosystem Resilience: https://www.semi.org/en/news-media-press-releases/semi-press-releases/semi-issues-recommendations-for-european-commission-to-bolster-europe%27s-chip-ecosystem-resilience-and-competitiveness
- The Resilience of the Semiconductor Supply Chain: https://www.dhl.com/global-en/home/insights-and-innovation/thought-leadership/white-papers/semicon-supply-chain-resilience.html
- Why a resilient semiconductor supply chain is imperative: https://www.kearney.com/industry/technology/article/-/insights/why-a-resilient-semiconductor-supply-chain-is-imperative-and-how-to-create-one
- Continuità operativa e ICT: https://www.cybersecurity360.it/soluzioni-aziendali/continuita-operativa-e-ict-non-solo-disaster-recovery-soluzioni-per-prevenire-gli-incidenti/
- Automation built for resiliency: https://www.plantengineering.com/articles/automation-built-for-resiliency/
- Study on the Electronics Ecosystem (European Commission): https://www.ipcei-me.eu/wp-content/uploads/2020/11/Study-on-the-Electronic-Ecosystem_Decision_Feb2020.pdf
- Promoting Safety and Resilience in the ICT industry: https://www.linkedin.com/pulse/promoting-safety-resilience-ict-industry-enhancing-business-beharry/
- The future of Machine Tools Industry: Automation & Robotics Revolutionizing the Sector: https://www.mtwmag.com/future-of-machine-tools-industry/
- A resilient EU robotics policy: https://www.linkedin.com/pulse/resilient-eu-robotics-policy-maro%C5%A1-%C5%A1ef%C4%8Dovi%C4%8D/

- Business Continuity in manufacturing: https://invenioit.com/continuity/business-continuity-manufacturing/
- A technology Survival Guide for resilience: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-technology-survival-guide-for-resilience
- Business Interruption and Resilience for Technology: https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/business-interruption-and-resilience-for-technology-companies.pdf
- European cluster collaboration platform: https://clustercollaboration.eu/in-focus/resilience
- European observatory for clusters and industrial change: https://single-market-economy.ec.europa.eu/industry/strategy/cluster-policy/observatory_en

Annex – Company Survey Results

Question 2.1 Country of your company (in case of large company/transnational, please include a EU plant)

Country of Origin	Count	%
Austria	6	13%
Belgium	1	2%
Bulgaria	9	19%
Estonia	1	2%
France	4	9%
Germany	7	15%
Greece	1	2%
Italy	6	13%
Latvia	1	2%
Portugal	2	4%
Slovenia	1	2%
Spain	4	9%
Sweden	3	6%
The Netherlands	1	2%
Totale	**47**	**1**

Question 2.2 Company size (employees)

Companies' size	Count	%
1-19	33	70%
20-49	7	15%
50-99	5	11%
100-249	1	2%
+ 250	1	2%
Totale	**47**	**1**

Question 2.3 What is the sector(s) of your organisation?

Customers served	Count	%
Start ups	11	11%
MSMEs	19	19%
Mid Caps	30	31%
Large Companies	34	35%
RTOs	4	4%
PA	4	4%
Totale	**98**	**1**

Question 2.4 Who are your main customers?

Sectors	Count	%
Agrifood	4	4%
ICT	**24**	**22%**
Aerospace & defense	4	4%
Construction (building, domotics, lighting...)	4	4%
Automotive, mobility & transport	8	7%
Biomedical, Health & Wellness	2	2%
Machine tools, plant engineering/robotics & automation	**10**	**9%**
Energy & Environment	7	6%
Electronics and Microelectronics Energy/environment	**25**	**23%**
Chemicals	1	1%
Operating machines/ logistics /intralogistics	3	3%
Print	2	2%
Nanotechnologies	5	5%
Rail	1	1%
Optoelectronics & Photonics	6	6%
Maritime & Naval	2	2%
Total	**108**	**1**

Question 3.1 What are the potential internal threats to your business: please select the most relevant for your company

Potential Threats Identified	Count	%
Asset loss, including damage or destruction of company property or unforeseen costs of doing business	16	34%
Human error, such as unintentional data leaks, union strikes, or ineffective management	18	38%
Inadequate organizational structure and reporting responsibilities	13	28%
Total	**47**	**1**

Question 3.2 Have you identified and documented internally potential risks specific to the semiconductor industry (e.g., supply chain disruptions, technological obsolescence)?

Identification and documentation of potential risks in the semiconductor industry	Count	%
No	25	53%
Yes	22	47%
Total	**47**	**1**

Question 3.3 How do you assess the likelihood and potential impact of semiconductor supply shortages or disruptions? If you don't do it, please write "currently we don't assess it"

Assessment of the impact of semiconductor supply shortages/ disruptions on the business	Count	%
No	25	53%
Yes	22	47%
Total	**47**	**1**

Question 3.4 Are you monitoring geopolitical and economic factors that could impact the semiconductor market? If YES please briefly explain how; if NOT please write a X

Monitoring of geopolitical and economic factors (that could impact the semiconductor industry)	Count	%
No	24	51%
Yes	23	49%
Total	**47**	**1**

Question 4.1 Which processes and functions are most critical for the organization's survival and continued operation?

Critical Processes and functions	Count	%
Finance to handle business-related aspects such as funding, accounting, budgets, and financial oversight	**17**	**13%**
HR/Personnel/Recruitment	13	10%
Information technology to develop & operate applications, systems, hardware, and software	14	11%
Operations management : how to utilizing resources from staff, materials, equipment, and technology	15	12%
Production & Quality	12	9%
Research & Development	**24**	**19%**
Sales & Marketing (Product packaging design, Event and media planning, Email marketing, Influencer marketing, digital marketing...)	**21**	**16%**
Supply chains management: Buying/Purchasing, Distribution /Logistics	12	9%
Total	**128**	**1**

Question 4.2 Have you determined the maximum acceptable downtime for each critical function? Which is the maximum?

Maximum acceptable downtime for critical functions	Count	%
1 day	7	15%
1 week	16	34%
2 weeks	11	23%
3 weeks	2	4%
1 month	7	15%
more than 1 month	4	9%
Total	**47**	**1**

Question 4.4 Have you diversified your suppliers or partners to minimize dependency on a single source?

Diversification of partners and suppliers	Count	%
Yes	34	72%
No	13	28%
Total	**47**	**1**

Question 4.5 Have you considered implementing business continuity management standards or frameworks (e.g., ISO 22301)?

Implementation of Business Continuity management stardards/ fra	Count	%
Yes	7	15%
No	40	85%
Total	**47**	**1**

Question 4.6 Have you identified critical suppliers and assessed their geographic locations and potential vulnerabilities?

Identification of critical suppliers	Count	%
Yes	19	40%
No	28	60%
Total	**47**	**1**

Question 5.1 Do you have communication protocols/business continuity plan for informing employees, customers, and stakeholders during a crisis?

Communication protocols/ business continuity plan for informing stakeholders during a crisis	Count	%
Yes	18	38%
No	29	62%
Total	**47**	**1**

Question 5.2 Have you identified key personnel responsible for executing the plan during a crisis?

Identification of key personnel to execute the plan during a crisis	Count	%
Yes	23	49%
No	24	51%
Total	**47**	**1**

Question 5.3 Are decision-making processes decentralized to empower teams to respond quickly to changes?

Decision making processes decentralization (to empower teams)	Count	%
Yes	20	43%
No	27	57%
Total	**47**	**1**

Question 6.1 How frequently do you conduct tests or simulations of your business resilience plan? (0= never, 5=very often)

How frequently test/ simulations of business resilience plan are conducted	Count	%
0 (never)	21	45%
1	10	21%
2	9	19%
3	4	9%
4	2	4%
5 (very often)	1	2%
Total	**47**	**1**

Question 6.3 Have you provided training to employees regarding their roles and responsibilities during a disruption?

Training sessions for employees	Count	%
Yes	13	28%
No	34	72%
Total	**47**	**1**

Question 6.4 Are there regular refresher training sessions to keep employees prepared and informed?

Refreshment training sessions for employees	Count	%
Yes	11	23%
No	36	77%
Total	**47**	**1**

Question 7.3 Do you conduct regular testing and validation of your products to ensure their performance and reliability?

Regular testing and validation of products	Count	%
Yes	38	81%
No	9	19%
Total	**47**	**1**

Question 7.5 Have you established legal protections and agreements to prevent unauthorized use of your IP?

Legal protections and agreements	Count	%
Yes	29	62%
No	18	38%
Total	**47**	**1**

Question 7.6 Are you prepared to respond to IP infringement disputes or legal challenges?

Preparation to respond to IP infringement disputes or legal challenges	Count	%
Yes	26	55%
No	21	45%
Total	**47**	**1**

Question 7.7 Do you have a communication plan to address stakeholders during a electronics / semiconductors -related crisis (e.g., supply chain disruption, product recall)?

Communication plan to address stakeholders during a electronics / semiconductors -related crisis	Count	%
Yes	9	19%
No	38	81%
Total	**47**	**1**

Question 7.9 Please tick the profiles that from your point of view are the most sought after by European industry since January 2022 (in terms of number of hires).

Profiles that are the most sought after by European industry since January 2022 (in terms of numb	Count	%
Analog design engineer	3	2%
Application engineer	5	4%
Data scientist	**15**	**12%**
Design engineer: i.e. Electrical design engineer, electrical project engineer, electrical produc	**20**	**16%**
Digital design engineer	5	4%
Expert in cybersecurity	8	6%
Maintenance technician: Electrical technician, breakdown technician	3	2%
Marketing engineer	4	3%
Operator / Inspector: Machine operator, inspector, repair operator, general laborer	4	3%
Process engineer: Manufacturing (support) engineer	4	3%
Process technician: Manufacturing (support) technician	5	4%
Robotic engineer: Electrical automation engineer, controls and robotic engineer, control system en	7	6%
Software engineer	**29**	**23%**
System design engineer (complex ASIC, SoC, SiP, SoP)	5	4%
Test engineer: Product test engineer, test engineer, Design For Test (DFT) engineer, associate tes	7	6%
Test technician: Electrical test technician, environmental and life-time test technician, troubleshoote	1	1%
Total	**125**	**1**

Question 7.10 Do you review and update your business continuity plan periodically?

Periodic review and update of business continuity plan	Count	%
Yes	29	62%
No	18	38%
Total	**47**	**1**

Question 7.11 Is there a mechanism in place to gather feedback from employees and stakeholders for plan improvement? (test, questionnaire, simulation, teambuilding…)

Mechanism to gather feedback from employees and stakeholders for plan improvement	Count	%
Yes	20	43%
No	27	57%
Total	**47**	**1**

Question 8.1 What actions is your company undertaking to be more resource efficient?

Actions undertaken to improve resource efficiency	Count	%
Adopting/purchasing new technological solutions to reduce emissions	8	7%
Designing products that are easier to maintain, repair or reuse	20	17%
Developing new technological solutions to reduce emissions	18	15%
Minimising waste	19	16%
None	2	2%
Recycling, by reusing material or waste within the company	9	8%
Saving energy	19	16%
Saving materials	5	4%
Saving water	2	2%
Selling your residues and waste to another company	1	1%
Switching to greener suppliers of materials	8	7%
Using predominantly renewable energy (e.g. including own production through solar panels)	6	5%
Total	**117**	**100%**

Question 8.2 Which type of support does your company rely on in its efforts to be more resource efficient?

Type of support to rely on to be more resource efficient	Count	%
Advice or other non-financial assistance from business associations and clusters	12	14%
Advice or other non-financial assistance from private consulting and audit companies	6	7%
Advice or other non-financial assistance from public administration	7	8%
Advice or other non-financial assistance from supply chain partners	4	5%
Don't know /No answer	9	11%
Private funding from a bank, an investment company or venture capital fund	8	10%
Private funding from friends and relatives	5	6%
Public funding such as grants, guarantees or loans	32	39%
Total	**83**	**100%**

Question 8.3 Which of the following would help your company the most to be more resource efficient?

Helpful ways to be more resource efficient	Count	%
A tool to self-assess how resource efficient your company is with respect to other companies	10	10%
Advice on funding possibilities and financial planning for resource efficiency investments	12	12%
Better cooperation between companies across sectors so that new processes to reuse waste and by	8	8%
Clearer rules on the use of secondary raw materials	2	2%
Consultancy on how to improve resource efficiency in your company	9	9%
Database with case studies that show the benefits of resource efficiency for companies	9	9%
Demonstration of new technologies or processes to improve resource efficiency	15	15%
Grants or subsidies	28	29%
None/Don't know/No answer	4	4%
Total	**97**	**100%**

Question 8.4 Does your company offer green products or services?

Offer of green products/ services	Count	%
Don't know/No answer	12	26%
No and you are not planning to do so	3	6%
Yes (please specify)	18	38%
No, but you are planning to do so in the next 2 years	14	30%
Total	**47**	**100%**

Question 8.5 Does your company encounter any of the following difficulties when trying to set up resource efficiency actions?

Difficulties encountered when trying to set up resource efficiency actions	Count	%
Complexity associated with environmental labelling and certification	12	14%
Complexity of administrative or legal procedures	15	18%
Cost of environmental actions	19	23%
Difficulty to adapt environmental legislation to your company	3	4%
Lack of demand for resource efficient products or services	3	4%
Lack of specific environmental expertise	8	10%
Lack of supply of required materials, parts, products or services	7	8%
None/ Don't know/No answer	11	13%
Technical requirements of the legislation not being up to date	5	6%
Total	**83**	**1**

Annex – Cluster Survey Results

Question 1 How would you rate the cluster's overall level of resilience in the face of disruptions?

Cluster's overall level of resilience in the face of disruptions	Count	%
1	0	0%
2	3	10%
3	12	40%
4	13	43%
5	2	7%
Total	**30**	**1**

Question 2 Does your cluster organize activities for your team?

Cluster's organization of team activities (training, team building,	Count	%
NO	1	3%
YES (at least 1 per year)	10	33%
YES (sometimes)	13	43%
YES (often)	6	20%
Total	**30**	**1**

Question 3 What are the main topics addressed in these activities?

Main topic addressed by these activities include	Count	%
soft skills	17	22%
technological megatrends	17	22%
business methodologies	13	17%
Funding opportunities (both local and european)	18	24%
green topics (EU policy, certifications...)	11	14%
Total	**76**	**1**

Question 4 How your cluster secure funding and financial sustainability for its initiatives?

Secure funding and financial sustainability for its initiatives	Count	%
Regional funds	26	32%
EU funds	29	35%
Members' fee	25	30%
Training courses	1	1%
Laboratories	1	1%
Total	**82**	**1**

Question 5 How your cluster communicate and share information with its stakeholders during crisis (e.g. covid19, conflicts, shortage,..) and related measures as private and public measures, initiatives, technologies...?

Communicate with stakeholders during crisis and related mea	Count	%
website	24	22%
newsletter	21	19%
social	21	19%
emails	26	24%
webinars/event	17	16%
Total	**109**	**1**