Project number: 101158811
Project name: North Macedonia Safer Internet Centre
Project acronym: MkSafeNet
Granting authority: European Health and Digital Executive Agency

Sustainability plan

WP2/ Milestone MS2

Deliverable No	Deliverable Name	Work package No	Legal Beneficiary	Type	Dissemination Level	Due Date (month)
MS2		WP2	IMPETUS	R — Document, report	PU - Public	18

PREPARED BY: IMPETUS, FINKI, CKM, UKLO, MAGMA, C3I, Megjashi
MKSafeNet / Project implemented by the Ministry of Digital Transformation (MDT) and project partners, Consortium
.

Table of Contents

Summary

The North Macedonia Safer Internet Centre (MKSafeNet) functions as the **national Safer Internet Centre**, established through a **Government Decision** and anchored within a **multi-institutional coordination framework**. The Centre operates under the strategic leadership of a **National Coordinator**, who is the **State Secretary of the Ministry of Digital Transformation**, ensuring direct alignment with national digital policies, child protection priorities, and EU digital governance frameworks. It has 11 institutional members as well as a position of Secretary, performing administrative -technical affairs.

The mission of MKSafeNet is to provide a **coherent national response** to online risks affecting children and young people, through prevention, awareness-raising, education, helpline support, inter-institutional coordination, and evidence-based policy engagement. Its long-term vision is to function as a **permanent national public-interest mechanism**, embedded within the institutional system of the Republic of North Macedonia and fully interoperable with the European Safer Internet Centers ecosystem.

In this context, the Sustainability Plan represents a **strategic necessity**, rather than a project add-on. While Digital Europe funding enables the establishment and initial operationalization of MKSafeNet, international and EU experience demonstrates that **long-term digital safety services require institutional continuity, predictable resources, and stable governance arrangements** beyond project cycles. Without a structured sustainability framework, critical functions—such as the national helpline, reporting mechanisms, and educational outreach—face significant risks of fragmentation or discontinuation after external funding ends.

Drawing on EU best practices from established Safer Internet Centres and comparable donor-funded platforms, the Sustainability Plan adopts a **systemic approach** to sustainability. It addresses institutional anchoring, governance, human resources, technical infrastructure, financial diversification, and risk management as interconnected pillars. Particular emphasis is placed on the role of **multi-institutional ownership**, ensuring that responsibility for safer internet policies and services is shared across relevant public authorities, rather than concentrated within a single institution or project structure.

Recognizing the rapidly evolving nature of the digital environment, the Sustainability Plan is conceived as a **living and adaptive document**. It establishes an expectation of **annual review and update**, coordinated by the National Coordinator, to reflect changes in policy priorities, technological developments, stakeholder partnerships, funding opportunities, and emerging online risks. This iterative process ensures that MKSafeNet remains relevant, resilient, and responsive over time.
Through this framework, the Sustainability Plan provides a **clear pathway for institutional continuity**, safeguards public investment, and supports the long-term integration of MKSafeNet into national digital governance and child protection systems, fully aligned with EU standards and values.

1. Operational context of SIC

1.1 Governance Structure and Institutional Sustainability of the SIC

The North Macedonia Safer Internet Centre (MKSafeNet) operates as the officially designated national Safer Internet Centre, established by a Government Decision and embedded within a formal multi-institutional coordination framework. This governance model reflects the cross-cutting nature of child online safety, which spans digital policy, education, social protection, law enforcement, and fundamental rights.

MKSafeNet is governed at the strategic level by a **National Coordinator**, a role assigned to the **State Secretary of the Ministry of Digital Transformation (MDT)**. This arrangement ensures high-level political and administrative leadership, direct alignment with national digital transformation priorities, and coherence with EU digital governance and child protection frameworks. Positioning the National Coordinator at State Secretary level enables effective inter-ministerial coordination, policy alignment, and institutional authority, while safeguarding

MKSafeNet's role as a public-interest mechanism rather than a project-based initiative.
The Centre is supported by a **multi-institutional governing body composed of 11 institutional members**, representing key public authorities and stakeholders with statutory or operational responsibilities related to child protection, digital policy, education, regulation, and online safety. This structure ensures shared ownership, collective accountability, and coordinated decision-making across institutions, reducing dependency on any single organization and strengthening long-term institutional sustainability.
The multi-institutional body provides strategic direction, validates annual priorities, supports inter-institutional cooperation, and ensures that MKSafeNet's activities remain aligned with national legislation, international commitments, and EU standards.

1.2 Secretary Role as a Pillar of Operational Continuity and Institutional Memory

In addition to strategic leadership and institutional membership, MKSafeNet includes a **secretary position responsible for administrative and technical affairs**, supporting the day-to-day functioning of the Centre. This role is critical for ensuring continuity between strategic decisions and operational implementation, including coordination of meetings, documentation, follow-up on decisions, record-keeping, and liaison with institutional members and partners.

As part of the long-term sustainability strategy, it is proposed that the **Secretary position be institutionalized as a permanent role within the Ministry of Digital Transformation**. Employing the Secretary directly within MDT would:

- **Ensure institutional memory**, preserving knowledge of decisions, procedures, partnerships, and historical context beyond project cycles or staff turnover;

- **Strengthen administrative continuity**, providing stable support to the National Coordinator and the multi-institutional body;
- **Reduce reliance on project-funded positions**, mitigating risks associated with funding gaps after external financing ends;
- **Enhance accountability and transparency**, through consistent documentation and follow-up of governance processes;
- **Support long-term integration of MKSafeNet into the state administration**, reinforcing its status as a permanent national mechanism.

1.3 Contribution to Long-Term Sustainability

This governance model—combining high-level strategic leadership, multi-institutional ownership, and a permanent administrative anchor within MDT—provides a robust foundation for the long-term sustainability of MKSafeNet. By institutionalizing both decision-making and operational coordination within government structures, the Centre can maintain continuity, legitimacy, and effectiveness beyond individual projects, while remaining adaptable to evolving digital risks and policy priorities.

In this way, MKSafeNet is positioned not only as a service provider, but as a durable governance mechanism embedded in the national digital ecosystem and fully aligned with European Safer Internet principles.

2. Helpline Infrastructure

Creating a sustainable helpline will be the most challenging technical task. It requires maintaining multiple different channels for communication. We had several options for development.

1. Create a self-hosted solution for telephony real-time chat communication and further develop modules that will integrate with the various chat platforms that are used. For this approach we explored several options for telephone conversations, based on the well-known Asterisk PBX and standalone like the call-center software ViciDIAL. We concluded that ViciDIAL is not suited for our use-case, so focused on the Asterisk based solutions. We have explored several Asterisk solutions as well as hosting a bare-metal Asterisk instance. Our explored self-hosted solutions included FreePBX and Issabel. The main problem with this approach is the required maintenance for the base system as well as developing modules for integration with popular chat-based services.
2. Use a well-known cloud-based solution. We explored several platforms for hosting the helpline: 3cx, Bitrix24, Nextiva and several others. All of them are paid options, but 3cx has a very approachable free tier that integrates:
    - Telephony, with up to 6 parallel communication lines
    - SMS,
    - Web-chat with up to 10 parallel connections

- WhatsApp communication
- Facebook integration
- Clients for: Windows, Web, iOS, Andorid
- Video conferencing
- Call queues, recordings, reports, etc.

All of these features are available out-of-the-box in its unlimited free plan.
Although the unlimited free plan for3cx was initially deemed as appropriate, the plan was unfeasible. 3Cx does not provide service in North Macedonia and thus this option was abandoned in favor of self-hosted FreePBX based solution for call center functionality, an integrated self-hosted web-based solution for real-time text communication, with possibilities for integration with Facebook Messenger, Instagram and WhatsApp. In addition. The chat-based subsystem is AI ready and can be integrated with custom AI solutions.

As for maintenance, we have made a special effort that all the solutions will require minimal maintenance, so that should not be added to the bill in any significant way.

2.1 Review of Existing Technology, Platforms, and Infrastructure

One organization ("Megjashi") currently operates a combination of **secure telephone lines, online communication channels, informational websites, and email support**, enabling confidential and real-time assistance to children, young people, families, and professionals. These systems form the operational backbone of the helpline within the Safer Internet Centre (SIC) framework. However, as MKSafeNet evolves into a national-scale service, the existing technological setup requires systematic review to assess its **capacity, scalability, integration potential, and compliance with advanced data protection standards**.

Megjashi currently operates secure telephone lines, online chat platforms, supportive and informative websites, and email support that enables confidential, real-time communication. These systems must be evaluated to ensure they can handle increased demand, integrate smoothly with the wider SIC platform, and maintain the highest standards of data privacy and user confidentiality.

From Megjashi's perspective, the current technological setup supporting the helpline within the Safer Internet Centre is foundational but faces significant limitations that impact on its overall effectiveness. The primary communication channel remains a traditional phone system, which serves as the main gateway for children, young people, families, and professionals seeking support. While this approach ensures direct, personal contact, the existing phone infrastructure restricts the helpline to handling only one call at a time. This creates bottlenecks during periods of high demand, causing other callers to wait, which may discourage vulnerable users in urgent need from reaching out promptly.

Each incoming call to the helpline is documented in Microsoft Word, using a standardized form based on the CHI (Child Helpline International) template, translated into Macedonian. The Operators fill in structured information by marking predefined categories and typing responses to open-ended questions. This method ensures consistency in data entry and allows staff to quickly reference call details. Microsoft Excel is used to log basic statistical information—such as the phone number and name of the caller, age, gender, type of issue, and call frequency. This statistical record functions as both a quick-reference database and a resource for generating analytical insights, identifying repeated callers, and producing summary statistics. Monthly reports are compiled using Word templates that include tables and summaries of call types, frequency, and trends, while Canva is used to design more polished, visually engaging semi-annual and annual reports. All documents—both call records and reports—are stored on a shared server on Microsoft Teams, organized by month for systematic retrieval. While this setup is manageable and cost-effective for a small team with limited resources, it is largely manual, fragmented, and non-scalable. As the role of helpline grows or as data demands increase, this infrastructure may hinder real-time responsiveness, data analysis, security, and collaboration.

In addition to the phone system, Megjashi leverages social media platforms as supplementary communication channels. These platforms offer more flexible access, including through mobile devices, and support real-time interactions such as messaging. The current webchat feature on the AloBushavko web page, which is based on older technology, does not function reliably and often experiences technical issues. However, the webchat system integrated into the helpline's website, intended to broaden accessibility and convenience, is currently unreliable. It frequently fails to receive inquiries properly, diminishing its role as an effective tool for engagement and support. This limits its effectiveness as a communication channel and may discourage users from reaching out via the website. Integrating a fully functional, modernized webchat into the new cloud-based contact center platform is a key priority to improve accessibility and user experience across all digital channels. This gap highlights the need for more robust, user-friendly digital communication solutions tailored to the diverse ways children and youth prefer to connect.

Case management and data handling at the helpline currently rely on manual processes. Without a dedicated Customer Relationship Management (CRM) system or specialized case management software, the team records all relevant personal data and case information in Excel spreadsheets. While this approach allows the organization to collect necessary information and filter cases for appropriate follow-up, it presents challenges related to data security, consistency, and efficient information retrieval. Only a small number of authorized helpline staff members have access to these records, both digitally and on paper, and have signed confidentiality agreements to protect sensitive information. Despite these efforts, the absence of advanced data protection tools, encryption, or secure access protocols raises concerns about the long-term security and privacy of the data handled.

The technological platforms currently in use offer limited cross-device accessibility. Social media channels provide some mobile access, facilitating communication on the go, but most

other documentation and case files are accessible only through desktop environments. There is no support for live video interactions or integrated chat services within the current system. Moreover, the helpline does not employ any automated or AI-assisted tools for initial triage, case prioritization, or routing of inquiries, which limits the capacity to manage incoming contacts efficiently and delays response times in critical situations.
Regarding system resilience, Megjashi adheres to the national Law on Personal Data Protection, aligned with the GDPR, and has established a baseline legal framework for data handling and privacy safeguards. However, to strengthen the operational capacity of the helpline and ensure continuity in service delivery, further technical enhancements are needed.

These include the development of structured procedures for data backup, disaster recovery, and continuity planning to mitigate the risks of data loss or service disruption in case of technical failures or cyber incidents. Although privacy is taken seriously, the current system faces limitations in handling multiple simultaneous calls, relies on manual data processing for reporting, and lacks automated mechanisms for incident response and data protection audits. These gaps highlight the need for a modernized, integrated system that not only ensures compliance but also enables secure, efficient, and uninterrupted support for children and young people.

Recognizing these challenges, Megjashi through the MkSafeNet project, is actively working on the development of a new, unified platform designed to significantly enhance communication channels, case management, and data security. This forthcoming platform aims to provide multi-channel accessibility—including phone, chat, and social media integration—with real-time interaction capabilities, better data protection mechanisms, and automated workflow features to improve efficiency. Detailed information on this planned upgrade will be provided separately, reflecting the organization's commitment to evolving the helpline's technological foundation to better serve children, families, and professionals within the Safer Internet Centre framework.

2.2 Need for New Solutions

Currently, Megjashi's helpline relies on a basic technological setupThe existing technological tools are accessible and familiar, reducing the need for training and ensuring a low-cost implementation. Microsoft Word and Excel are versatile and widely used, which suits the current needs of the organization. However, as call volumes increase and the scope of operations expands, these tools may become insufficient. Word documents, for instance, are not ideal for structured data analysis, and Excel sheets, while useful, are limited when it comes to real-time data sharing, tracking complex trends, or ensuring secure and scalable caller information storage.

This opens up a need for more integrated, dedicated solutions such as case management software tailored to helplines, CRM platforms, or database systems with forms for input and dashboards for reporting.

The helpline operates via traditional phone system and social media channels for communication. While these tools are available and functional to some extent, they do not fully align with the communication preferences of the helpline's primary users. Most young people prefer text-based communication methods such as chatting rather than phone calls, but the existing webchat system is unreliable and often fails to receive messages, limiting accessibility for this key group. Furthermore, the phone service is funded directly by Megjashi and is not toll-free, which could potentially discourage some users from reaching out due to cost concerns.

The limitations of these existing technologies become apparent in daily operations. The single-line phone system can only handle one incoming call at a time, leading to caller wait times and missed opportunities for immediate support. There is also a lack of an integrated case management system, with staff manually entering data into spreadsheets, which is inefficient and poses challenges for secure data handling and timely reporting. Moreover, the absence of automated routing, multi-channel integration, and mobile accessibility restricts the helpline's ability to respond flexibly and promptly across diverse user needs.
These gaps underscore a clear and urgent need for modernized technological solutions that can better support the helpline's mission. A new platform should prioritize multi-channel communication, including reliable chat functions, to meet the preferred contact methods of children and young people. It should also offer secure data management, mobile-friendly access, and automated features to enhance workflow efficiency. Addressing these needs will not only improve service quality but also ensure more inclusive, timely, and confidential support for vulnerable users. Despite budgetary and organizational constraints, the development and implementation of such solutions are critical for the helpline's growth and effectiveness.

2.3 Identify potential technical challenges and opportunities for innovation

Transitioning to more advanced systems introduces several technical challenges. First, data migration from Word and Excel to a structured database could be labor-intensive and require data cleansing. Second, user adoption may be hindered by resistance to change or lack of training in new tools. Third, setting up custom software solutions may require specialized IT support, which can strain limited resources.
Within the MkSafeNet project, T3.5, T3.5.4 a central technical focus is the development of a modern, cloud-based unified contact center platform designed to integrate multiple communication channels such as phone, SMS, webchat, and social media platforms including Facebook Messenger, WhatsApp, Twitter, and Instagram. This platform aims to increase accessibility for children and youth, allowing them to contact trained counselors through the channels they naturally use, while enabling counselors to respond within a single, streamlined system. However, this ambitious vision comes with several technical challenges and sustainability risks—both immediate and long-term.
One of the most pressing challenges is incomplete multichannel integration. The new platform, custom-designed by the FINKI team in collaboration with the IT specialist and the team from Megjashi, is tailored specifically for efficient and secure case management. Every step of the

process is automated to reduce manual work and improve consistency, from case registration to documentation and reporting. Cases are recorded and tracked using Word templates based on the CHI system we previously used, ensuring that all information is structured, accurate, and standardized. This not only streamlines the workflow but also guarantees that all data is properly documented for future reference. The platform includes a dedicated analytics section that provides comprehensive statistical insights. Here, staff can access real-time overviews of all cases, analyze trends, and generate reports that support decision-making and program evaluation. The statistical information is fully integrated with the case data, offering a complete picture without requiring additional data entry.

In addition, the platform features a section for creating official correspondence to institutions. These documents can be generated directly from the platform, incorporating all relevant information from the case and analytics sections, ensuring accuracy, consistency, and efficiency in communications.
With mobile-friendly access, secure data management, and automation throughout, the platform not only improves workflow efficiency but also ensures confidentiality, inclusivity, and timely support for vulnerable users. By integrating all aspects of case management, analytics, and institutional reporting in one system, it provides a comprehensive, reliable, and user-friendly tool for staff to manage cases effectively.

We are in the final phase of replacing the outdated webchat with a modern communication application, developed with the support of our IT specialist and fully incorporated into the new platform. The new solution utilizes Asterisk and FreePBX , a industry standard, secure and modern SIP-based communication infrastructure as well as Sipnetic clients that support instant messaging with text and voice chat, encrypted communication, presence information, and multimedia capabilities such as voice and video calls**.** By integrating these features directly into the AloBushavko webpage, we will provide users with a more reliable and versatile communication channel that is resilient, secure, and aligned with current standards, ensuring seamless engagement for those who prefer online text-based interaction while reducing technical strain on our resources. This new application will require regular maintenance, updates, hosting oversight, and technical support to ensure ongoing performance, security, and compatibility with evolving standards and user needs. Investing in this level of operational support is essential to guarantee continuity of service accessibility, particularly for users who prefer online text communication, and to uphold the quality and reliability expected by both users and stakeholders.

The data protection and privacy compliance is of critical importance in relation to the platform for case management. The platform uses modern 2-factor authentication and is hosted on the FINKI (Faculty of Computer Science and Engineering - Skopje) internal data and cloud center, which ensures a short-term, low-cost solution. As the platform starts to handle sensitive personal data—particularly in high-risk cases involving online abuse, grooming, or CSAM—there is a pressing need for a dedicated, secure, and GDPR-compliant hosting environment. Hosting would eventually be transferred to a commertial server provider within the EU or a jurisdiction that fully meets European data protection standards, ensuring encrypted data

storage, regular backups, and access control protocols. This migration would also entail new technical and financial resources.

In addition to infrastructure, the system will require periodic upgrades, maintenance, and scaling to remain secure, functional, and relevant. Over time, as the number of users, complexity of cases, and legal obligations increase, the platform must evolve—requiring dedicated technical personnel such as a system administrator, application developer and quality assurance engineer. This personnel is essential to maintain integrations, ensure security patches, optimize system performance, and provide rapid troubleshooting. Without these human resources, even a well-designed system can quickly become obsolete or vulnerable.
The platform is also not yet ready for advanced functionalities, such as AI-powered case triaging, case summary, natural language processing (NLP), or smart analytics dashboards. While such technologies could improve efficiency and help identify urgent or high-risk cases more quickly, the organization is far from being AI-ready—both technically and organizationally. Implementation of these tools would require additional infrastructure, specialized expertise, and ethical safeguards. If not addressed, this could result in a widening innovation gap between MkSafeNet and more technologically advanced helpline systems across Europe.

Regarding interoperability, the platform must be designed for seamless integration with key national institutions, including the Safety Internet Center for escalation of cyber violence cases, as well as the Ministry of Social Policy, law enforcement agencies, and social work centers for other cases managed by the helpline. Achieving this will require the implementation of open APIs, a modular system architecture, and clearly defined data-sharing protocols that fully comply with GDPR and other relevant data protection regulations. Without these technical and procedural foundations, the helpline's capacity to efficiently escalate cases, refer children to appropriate institutional services, and facilitate effective cross-sector collaboration will be significantly limited.

Furthermore, there is a growing demand to engage youth where they already spend time online. While the MkSafeNet communication strategy foresees outreach via social media and gamified tools, actual implementation will depend on technical readiness and integration with the core platform. Innovations such as TikTok awareness campaigns, AI chat companions, or mobile self-help tools can be highly impactful—but only if they are secure, moderated, and connected to real-time human support.

Lastly, long-term success will depend not only on software and servers, but also on a stable team of trained IT personnel capable of maintaining and expanding the system. This includes technical roles for ongoing system management, data protection oversight, user training, and digital security. As these roles are not yet institutionalized or guaranteed post-project, they must be anticipated in future planning and budgeting.
In summary, while the platform represents a major innovation, it comes with multiple technical challenges—from limited integration and potential cost escalation, to temporary hosting and lack of in-house IT staff. Without dedicated resources for system upgrades, , interoperability,

operational staff (coordinator, operators, communication and financial manager) and technical staffing, the platform's long-term functionality, safety, and impact could be at risk. Strategic planning and institutional commitment will be crucial for sustaining this system beyond the scope of the project.

2.4 Evaluate Risks Associated with Technology and Infrastructure

The transition to a new cloud-based contact center platform under the MkSafeNet project represents a significant improvement in capacity and operational flexibility. However, several technological and infrastructure-related risks must be considered. The **current infrastructure cannot handle a substantial increase in user demand**, but the implementation of the new platform will support multiple concurrent users on the 116 111-helpline number and provide a centralized view across channels for better triage and prioritization.

The newly established platform is self-hosted and built using the enterprise-grade PBX solution Asterisk. The platform is fully configurable and enables multiple concurrent voice lines for communication. Additionally, the newly created website has integrated real-time communication subsystem that enables centralized platform that provides real-time web-chat functionality as well as video and social chat integration (Facebook messenger, Instagram, WhatsApp business etc.). The communication subsystem is AI ready and can be integrated with the popular general AI solutions or used with specialized and custom developed solution.
Furthermore, as long as the communication on the AloBushavko website is not utilizing third parties (e.g. Facebook, Instagram, WhatsApp), all of the communication is kept locally on the servers of Megjashi.

Each path implies resource implications and potential downtime risks. From a cybersecurity standpoint, sensitive case data is currently accessible only to trained operators, the helpline coordinator, the programme manager, the consultant and the director of Megjashi— with user authentication and tiered access being built into the platform. Bitdefender is installed to monitor and alert against intrusion attempts. However, during the transition phase, the reliance on tools such as Excel for case tracking still poses risks for data exposure and GDPR compliance, despite careful internal handling.
An incident response plan is necessary and should include protocols for isolating compromised systems, notifying internal and external stakeholders, conducting forensic review, reporting to the national data protection authority, and performing a post-incident evaluation.
Looking ahead, **future risks** include:

- **Unforeseen costs** if the platform transitions to a paid model or if premium integrations become necessary.
- **Dependence on external vendors or institutions** (only applicable if the server is hosted on FINKI), such as FINKI, which could affect autonomy or sustainability.
- **Inability to scale** if digital demand grows faster than infrastructure or staff capacity.
- **Lack of in-house technical staff** for platform maintenance, system upgrades, or responding to emergencies.

- **GDPR enforcement tightening** — which could require additional security audits, documentation, or user consent mechanisms that are not yet in place.

To ensure resilience, long-term planning should include a dedicated operational staff and IT team, a scalable hosting and server strategy, a sustainable budget for platform upgrades, web hosting, and maintenance, as well as clear arrangements for management and responsibility of the digital infrastructure — ensuring that children and young people can continue accessing support services reliably and without interruption.

2.5 Technical and Infrastructure Risks

1. **Single Point of Failure** – If the platform or server goes down (due to hosting failure, cyberattack, or misconfiguration), there may be no immediate fallback option or backup line.
2. **Lack of Redundancy** – No mirrored systems or secondary servers to maintain service during maintenance or outages. This must be addressed in the yearly plans as the infrastructure runs on several standard and relatively inexpensive cloud-based virtual machines and self-hosted VPN and PBX infrastructure.
3. **Unstable Internet Connectivity** – If the internet connection at the hosting location or helpline office is unstable, real-time support can be disrupted.
4. **Software Obsolescence** – We have made maximum effort to self-host most of the solutions either using well-established and long-term developed open-source solutions (e.g. Asterisk and FreePBX), or custom made software that relies on well-established technological stack that provides clear upgrade and maintenance path.

Financial and Sustainability Risks

1. **Dependency on Free Software Tools** – The free software tools used are open-source and well-established, with large communities. Current reliance on a free platform (C3X) poses a long-term risk if the provider switches to a paid model or reduces free feature availability.
2. **Hidden Costs** – Unexpected expenses such as licensing, storage overage, cybersecurity tools, GDPR compliance tools, or future staff training.
3. **Funding Gaps** – After the MkSafeNet project ends, there may be no earmarked budget to cover hosting, required updates, technical support, or new feature development.

Data Protection and Cybersecurity Risks

1. **Data Breaches** – Sensitive case data (e.g., on minors, abuse, self-harm) is a high-value target; lacking robust intrusion detection, encryption, or monitoring may leave it vulnerable.
2. **Access Control Mismanagement** – Without role-based permissions and activity logging, unauthorized access or accidental exposure of case data is possible.
3. **Weak Authentication** – If passwords are not managed securely (no 2FA, weak policies), there's a risk of unauthorized system access.

Operational and Human Risks

1. **Lack of Technical Support Team** – If no in-house staff can troubleshoot or update the system, reliance on external help can delay response and cost more.
2. **Loss of Knowledge** – If the current tech setup is managed by one or two people, and they leave, documentation and know-how may be lost.
3. **Inadequate User Training** – Operators may make errors (e.g., logging into wrong accounts, sending case notes to the wrong channel) if the system is too complex or poorly explained.

Scalability and Service Quality Risks

1. **Unsalable System Architecture** – If the platform can't handle increased call/text volume, it will degrade service quality or crash.
2. **Channel Overload** – Managing messages across many social platforms without smart routing or AI triage could overwhelm human operators.
3. **Fragmented Case History** – Without proper case management tools, tracking ongoing or repeated contacts becomes difficult, leading to inconsistent care.

External Dependency and Legal Risks

1. **Dependence on Platform Providers** – Changes in Meta or WhatsApp policies could cut off integration or impose new requirements (e.g. verified business accounts).
2. **Lack of Legal Agreements** – Hosting at FINKI or using third-party tools without formal MoUs or service-level agreements (SLAs) carries legal and operational risks.
3. **Noncompliance with Child Protection Regulations** – If digital record-keeping does not meet child protection protocols or retention timelines, accountability could be questioned.

Strategic and Long-Term Risks

1. **No Exit Strategy** – If the platform or system proves unfit or unsustainable, there may be no plan or budget for migration.
2. **Reputation Damage** – A publicized data breach or service interruption could damage trust among users and stakeholders.
3. **Inflexibility to Evolve** – Inability to integrate future innovations (AI chat, TikTok outreach, smart triage bots) could make the helpline outdated for youth.

3. Human Resources

The current helpline team is composed of a coordinator and four full-time operators, three psychologists and one operator with law background, all employed under the MkSafeNet project with contracts valid until February 2026. These professionals are supported by approximately 12 volunteers who help maintain 24/7 availability, ensuring continuous service alongside the full-time staff. Additionally, an IT specialist, also funded through the MkSafeNet project, collaborates closely with FINKI University on the development, implementation, and maintenance of the new cloud-based contact center platform. During the MkSafeNet project we secured a psychologist-supervisor, which conducted supervision session with the operators on the helpline.

Despite this solid core, several significant human resource challenges and risks must be acknowledged:

- **Post-project Staffing Sustainability:** The reliance on project-based funding creates uncertainty about the continuation of key personnel beyond early 2026. Once the MkSafeNet project concludes, the contracts for all full-time operators, the coordinator, the supervisor, and the IT specialists will expire unless new funding sources are secured. Without these positions funded, the helpline risks losing vital operational and technical capacity, threatening continuity and service quality. To further strengthen the Safer Internet Centre and the helpline, future Digital Europe calls can be strategically utilized.
- **Scalability and Demand Growth:** Currently, the team size is calibrated for existing call and messaging volumes. However, if demand doubles or triples — a realistic scenario given rising digital risks and awareness — the current workforce will be insufficient to meet needs. This would require hiring (additional) operators and support staff. Recruitment, onboarding, and training are resource-intensive processes that require careful financial and logistical planning, particularly given limited organizational budgets.
- **Training and Capacity Building:** Continuous professional development is crucial in the helpline context due to the complexity and emotional demands of cases handled. There is a need to expand training opportunities focused on digital safety, including recognizing digital threats, distinguishing between various forms of cyber violence, and enhancing the overall capacity of professionals working with children and youth in the digital environment. The organization presently relies on external training opportunities, such as those offered by Child Helpline International (CHI), to build staff skills. Participation in these programs is currently enabled through project funding and associated memberships. Within the MkSafeNet project, one training for strengthening the skills on response to digital violence was conducted, anyhow without ongoing funding, access to high-quality training may be restricted, impacting staff preparedness and service quality.

Emotional Support and Burnout Prevention: Helpline operators face high emotional stress, dealing with sensitive and often traumatic cases. To address this, the helpline has conducted **regular supervision sessions as part of project activities**, with support from the **MKSafenet project**, allowing operators to discuss cases and receive psychological guidance from dedicated supervisors. This structure has been critical to operator wellbeing and retention. However, once the project concludes, continued provision of these supervision sessions will require dedicated funding and additional resources to maintain the support framework. Without sustained financial and operational support, there is a risk that this essential component of staff wellbeing may be compromised as the team expands or demand increases.

- **Technical and IT Staffing:** The involvement of a dedicated IT specialist funded through the MkSafeNet project is a considerable advantage, ensuring technical stability and ongoing platform development. Nevertheless, the future of this role beyond the project is uncertain. Without a permanent technical resource, maintenance and

troubleshooting of the platform could face delays, risking service disruptions. External consultancy might be needed, potentially increasing costs.

- **Volunteer Management:** Volunteers play an essential role in extending coverage and providing flexible staffing. However, managing and training volunteers effectively requires dedicated coordination and resources to maintain quality and reliability.

Overall, the human resource landscape presents a complex mix of strengths and vulnerabilities. The helpline's capacity to sustain and grow its workforce post-project will depend on strategic planning, securing diversified funding streams, and balancing operational demands with staff wellbeing. Currently, it is uncertain whether the existing operators will continue, and the helpline may have to rely primarily on volunteers, with no dedicated operators in place. Proactive investment in training, recruitment, and supervision infrastructure will be vital to uphold the quality and responsiveness of helpline services amid evolving digital challenges.

4. Operational Costs

The helpline's operational costs are currently funded primarily through the MkSafeNet project, which supports personnel, platform development, and IT infrastructure. However, a detailed understanding of current and future operational expenses is critical to ensuring the sustainability and scalability of services beyond the project timeline.

- **Personnel Costs:** The largest portion of operational costs stems from salaries for key personnel, including the coordinator, full-time operators, communication manager, financial manager, supervisor and IT specialists. These roles are essential for ensuring the day-to-day functioning of the helpline, maintaining technical infrastructure, managing cases, overseeing outreach and public visibility, ensuring transparent financial operations, and securing continuous service availability. Volunteer coordination also requires administrative effort, which translates into indirect operational costs.

Platform and Software Licensing: The new cloud-based contact center platform has been custom-built by the FINKI team together with the IT specialist from Megjashi, designed specifically for automated case management, analytics, and institutional reporting. All core functionalities, including case documentation using Word templates based on the CHI system, automated workflows, and a section for official correspondence (*pretstavka/dopis*), are fully integrated. The platform also incorporates Asterisk and FreePBX for secure and reliable voice/telephone communication, while the website communication subsystem provides for real-time chat and video communication. While the platform currently operates without paid software licensing for its core modules, ongoing maintenance, hosting, and technical support will require dedicated resources as part of the sustainability plan. Future upgrades, integrations, or additional features may also incur costs, which should be anticipated and budgeted for. By consolidating case management, analytics, and communication into a single system, the platform provides a scalable, sustainable, and efficient solution for long-term operational needs.

All of the solutions use either an open-source license or are custom made for this project, so the licensing costs are non-exstant.

- **Hosting and Infrastructure:** The platform is planned to be hosted both onFINKI University's cloud servers and within Megjashi's own infrastructure, depending on technical requirements and financial feasibility. While hosting at FINKI may initially reduce infrastructure costs, provide amplebandwidth and storage capacity, the maintenance will require skilled IT personnel . Hosting within Megjashi would require dedicated investment in server capacity, maintenance, and IT support. Self-hosting part of the infrastructure, in our case the telephone lines, requires redundant hardware that should be additionaly acquired as soon as possible.In any case, future growth in usage could lead to increased demands and costs. Additionally, hosting and regularly publishing content on the organization's official website will entail further operational expenses, particularly for secure management, timely updates, and ensuring accessibility and data protection compliance.
- **Infrastructure and Physical Security**: In addition to digital safety, there is a pressing need to improve the physical infrastructure of the office to ensure secure access to the premises and better protection of equipment and staff. This includes upgrading locks and access control systems, setting up surveillance where needed, and ensuring that the office layout supports safe and efficient working conditions. Recently, **A1 donated equipment and resources** to support the implementation of EU harmonized number 116 111, helping enhance both security and operational functionality. Strengthening the physical space is essential for safeguarding sensitive data, maintaining the integrity of technical equipment, and ensuring a safe environment for employees and visitors. These measures are particularly important given the nature of work involving vulnerable populations and confidential case data.
- **Training and Development:** Participation in external training and capacity-building initiatives, such as those offered by Child Helpline International and other partners, incurs costs including membership fees, travel, accommodation, and course fees. Currently covered by the project, these costs need to be considered for future budgeting to maintain staff competence and wellbeing.
- **Cybersecurity and Data Protection:** Operational costs must also cover cybersecurity tools and protocols to protect sensitive case data. The current use of Bitdefender antivirus software provides baseline protection, but more advanced monitoring, intrusion detection, data encryption, and compliance activities (e.g., GDPR adherence) may require further investment in specialized tools and personnel.
- **General Administrative Expenses:** Utilities, office supplies, communication costs (phone, internet), and other overheads contribute to the ongoing expenses of running the helpline. These are often underestimated but are vital for uninterrupted service delivery.
- **Contingency and Incident Response:** Resources must be allocated to develop and maintain an incident response plan, including potential costs related to security incidents, data breaches, or technical failures. Planning contingencies ensures faster recovery and minimizes operational disruption.

Summary: Once this project concludes, the helpline will rely solely on volunteers , as there will be no paid coordinator, operators, IT support or dedicated supervision. Essential

operational needs—such as platform maintenance, software licensing, and infrastructure—will remain, but sustaining them without dedicated funding will be challenging. This situation underscores the urgent need to explore diversified funding sources, strategic partnerships, and cost-effective measures to ensure the helpline can continue providing critical support to those who need it.

5. Overview of Cost and Resource Planning

1. Human Resources – roles

Role	Description	Current Status	Future Needs & Risks	Estimated Cost / Notes	Contribution / Source
Coordinator	Manages daily operations, coordination with partners, reporting	Employed until Feb 2026 (MkSafeNet)	Renewal needed; burnout risk if scope increases	Salaries covered until Feb 2026; post-project funding uncertain	MkSafeNet project
Full-time Operators	Respond to children in distress, manage cases, provide psychological support	4 full-time staff hired	Contract renewal and expansion if call volume increases	Salaries covered until Feb 2026; ongoing funding depends on approval of the next project phase	MkSafeNet project
Communicatio n Manager	Leads visibility, media relations, public campaigns	Employed via project	Risk of gap in outreach if not retained	Currently funded; long-term sustainability uncertain	MkSafeNet project
Financial Manager	Oversees budget tracking, financial reporting	Employed via project	Needed for compliance and multi-donor reporting	Essential for future grant management	MkSafeNet project
IT Specialist	Ensures system stability,	Contracted through project	Need full-time role to support	Critical for future system resilience,	MkSafeNet project

	upgrades, troubleshooting		platform, security, backups	depends on approval of the next project phase	
Volunteers	10+ trained, rotate for 24/7 coverage	Active but limited availability	Ongoing recruitment, training, and supervision required	Training covered via Megjashi	Megjashi

2. Platform & Technology

Component	**Current Status**	**Future Needs & Risks**	**Estimated Cost / Notes**	**Contribution / Source**
Self-hosted VOIP call center	Functional	Needs hardware redundancy and depends on dedicated phone line	Free & Open Source, Sustainability risk	Under discussion — possible options include Megjashi or FINKI All of the equipment is contributed by A1 and FINKI
Microsoft 365 Environment	Under consideration for integration	Licensing costs if full migration needed	Secure, scalable option for document and team management	TBD
Webchat (AloBushavko site)	Legacy system	Requires full upgrade and integration	May require custom development	Megjashi contribution
Server Hosting	Not yet implemented: planned on FINKI or Megjashi servers	GDPR compliance concerns	Long-term hosting, bandwidth and storage cost may increase	FINKI/Megjashi in-kind
Website Publishing	Currently hosted on external CMS	May need dedicated subdomain or security upgrades	Cost for SSL, dev, and admin time	Megjashi contribution

Platform Maintenance & Upgrades	No funds allocated post-project	Need for regular updates, feature expansion (Meta, TikTok, Viber etc.)	Needs to be budgeted annually	Unknown yet

3. Infrastructure & Security

Category	**Current Status**	**Future Needs & Risks**	**Estimated Cost / Notes**	**Contribution / Source**
Physical Office Infrastructure	Adequate for current use	Upgrades needed for secure access, equipment storage, and emergency exits	Investment in access control, fire-proof cabinets, etc.	Megjashi facility
Cybersecurity Measures	Antivirus (Bitdefender), limited firewalling	Need full incident response plan, better encryption, network monitoring	Either in-house or via external consultants	TBD
Data Backup & Storage	Manual Excel logs, no automated backup	Risk of loss during outages or attacks	GDPR-compliant cloud or local backup solutions needed	TBD
Disaster Recovery	No documented procedure	Need continuity planning (calls, server crash)	Policy + backup infrastructure	TBD

4. Capacity Building

Focus Area	**Current Status**	**Future Needs & Risks**	**Estimated Cost / Notes**	**Contribution / Source**
Operator Training	Basic training in digital violence, helpline protocols	Need expanded modules on AI, cyberthreat detection, digital safety, GDPR	Yearly refreshers required	CHI supported, project supported

Volunteer Training	Inconsistent cycle, training depends on staff time	Structured, recurring training program needed	Training should be sustainable and adaptable to volunteer needs	CHI / Megjashi
Communication / Media	Limited to project period	Need training in crisis communication, campaigns	Could be integrated with annual budget	TBD
Physical Security Awareness	No training module	Training for staff on safe access, emergency response	Optional add-on	TBD

5. Operational Risks & Funding Outlook

Area	**Risk Description**	**Strategic Need**	**Current Mitigation**	**Sustainability Plan**
Scalability	Platform and team may not match rising demand	Scalable cloud hosting, flexible staff pool	Currently limited	Include in new grant applications
Legal Compliance	Partial alignment with GDPR, full national law compliant	Need annual GDPR implementation review	Basic procedures in place	Partner with DPO or legal consultant
Funding Gap Post-2026	Project ends in Feb 2026	Multisource funding strategy required	N/A	Develop donor diversification strategy by late 2025

Key Takeaways:

- Personnel and IT represent the most critical sustainability pillars; Volunteer training and capacity building require structured, recurring programs.
- Infrastructure (physical and digital) needs urgent strengthening.
- Stronger planning is needed for hosting, security, backups, and legal compliance.
- Clear cost estimates and budgeting strategy must be developed before 2026 to secure continuity.
- Partnerships and stakeholder collaboration are vital for long-term success.
- Risk management (including vendor dependency and data security) should be prioritized.

This project has technical constraints that it should be sustainable after the eventual project end-date. For that we need to estimate the costs that are currently and will be incurred in the

future. From a technical perspective, there are several services that need to be available in the present and future.

6. Initial (Establishment) Costs

Estimation on the initial and ongoing costs associated with establishing and maintaining the SIC. Based on the full operational, technical, HR and infrastructure context you provided, below is a **realistic and defensible estimation** of the **initial (establishment) one-time costs for Year 1** of establishing MKSafeNet as a national Safer Internet Centre.

The estimates are conservative and aligned with:

- 4–5 core staff onboarding
- Self-hosted Asterisk / FreePBX infrastructure
- Dedicated hosting migration
- Basic physical office reinforcement
- Compliance and GDPR setup
- Public institutional launch

For this Sustainability plan we need to make estimation of costs and **North Macedonia–specific cost estimate table** using available **local market data** on salaries and economic norms (e.g., average wages, typical IT salary ranges, and general local costs).

- Below is a **realistic estimate for Year 1 establishment costs** tailored to the North Macedonian context, based on typical salary ranges, general office needs, and service-related expenses:

Category	Description	Estimated Cost (EUR)
Personnel Recruitment & Setup	Hiring + onboarding + initial training for coordinator, 3–4 operators, supervisor, IT specialist. Salary assumptions: operators ~MKD 40,000–80,000/month; IT specialist ~MKD 36,000–80,000/month; other roles relative to average	**70,000**
Office Setup	Rent deposit, furniture, secure equipment storage, minimal physical upgrades	**18,000**
Helpline & Hotline Setup	PBX/Asterisk equipment, redundant hardware, VoIP phones, SIP trunk, initial cybersecurity tools	**30,000**
Website & Platform Development	Platform integration, secure chat solution, analytics dashboards, mobile optimization, compliance testing	**25,000**

Category	Description	Estimated Cost (EUR)
Branding & Launch Campaign	Institutional launch, PR/visibility, informational materials	**15,000**
Legal & Compliance Setup and Training	Data protection advisory, GDPR documentation, MoUs	**8,000**
Contingency (10%)	Contingency buffer for unexpected costs	**11,400**
Total Year 1 Establishment Cost Estimate:		**≈ 167,400 EUR**

7. How to save money

7.1 Explore potential revenue streams

Potential revenue streams can include: EU grants, government funding, private sector partnerships, international organizations and NGOs and other possible sources (e.g., government funding, private sector partnerships).

1) European Union Funding

Since North Macedonia is a candidate country for EU accession, it is eligible for various pre-accession and thematic funding instruments.

Connecting Europe Facility (CEF) Digital

The digital part of the Connecting Europe Facility (CEF Digital) will support and catalyse both public and private investments in digital connectivity infrastructures between 2021 and 2027.

-**Relevance**: Directly supports Safer Internet Centres across Europe.

-**Use**: Infrastructure, awareness-raising campaigns, helplines, and hotlines.

-**Application**: Through calls by the European Health and Digital Executive Agency (HaDEA).

B. Instrument for Pre-Accession Assistance (IPA III)

This instrument refers to the third phase of the Instrument for Pre-accession Assistance, a EU funding mechanism for countries aspiring to join the EU, covering the period from 2021 to 2027.

-Relevance: Supports institutional reform, including digital transformation and child protection.

-**Use**: Capacity building, training, policy development, and technical infrastructure.

-**Potential**: Partnering with local ministries for joint applications.

C. Horizon Europe & Digital Europe Programme (DIGITAL)

The Horizon Europe and the Digital Europe Programme (DIGITAL) are two distinct but complementary EU funding programs focused on different aspects of digital transformation. In essence, Horizon Europe supports the creation of new digital technologies, while DIGITAL focuses on ensuring these technologies are widely used and integrated into various sectors.

-**Relevance**: Funds digital literacy, cybersecurity, and innovation.

-**Use**: Collaborative R&D, training, and cross-border initiatives with existing SICs.

2) Government Funding

This type of potential revenue streams may involve several ministries such as: Ministry of Digital Transformation, Ministry of Education and Science, Ministry of Interior, Ministry of Social Policy, Demographics and youth.

A. Ministry of Digital Transformation (MDT)

Could fund digital infrastructure and education initiatives related to internet safety.

B. Ministry of Education and Science

Possible funding for educational campaigns and school-based programs.

C. Ministry of Interior / Ministry of Social Policy, Demographics and Youth

Involved in child protection and cybercrime prevention; can support helplines or policy efforts.

3) Private Sector Partnerships

These partnerships can include several big companies in North Macedonia such as:

A. Telecom Operators (A1 Macedonia, Makedonski Telekom)

-Incentives: Corporate Social Responsibility (CSR), brand alignment with child safety, digital responsibility.

-Support options: In-kind donations, co-branded awareness campaigns, or direct funding.

B. Tech Companies (Google, Meta, Microsoft)

They may offer: grants for local initiatives, toolkits or technical support, sponsorships of events or awareness campaigns.

C. Banks & Insurance Companies

They may offer: community support for development and education via Corporate Social Responsibility (CSR) budgets.

4) International Organizations & NGOs

-UNICEF North Macedonia: Strong focus on child rights and digital safety.

-OSCE Mission to Skopje: Works on rule of law and media freedom, could support capacity building.

-Council of Europe: Grants and technical support through Cybercrime and Children's Rights programs.

5) Other Possible Sources

A. Crowdfunding & Donations - -Campaigns targeting diaspora or local businesses for seed funding.

B. Academic Grants

-Universities can collaborate on research and receive funding for internet safety projects via Erasmus+ or other academic funds.

C. Public-Private Consortiums

-Create a multi-stakeholder body to pool resources (telecoms, NGOs, government) under a shared goal.

6) Discuss strategies for financial sustainability beyond donor funding:

Some strategies for financial sustainability beyond donor funding may include: public-private partnerships, social enterprises, subscription-based services, government co-funding, integration into national digital and educational infrastructure, events and campaign monetization, digital tools and product development etc.

1. Public-Private Partnerships

Telecoms, tech companies, banks, and media have a vested interest in a safe digital environment. They may use some of the following strategies:

-CSR-Based Sponsorships: Collaborate with companies like A1, Makedonski Telekom, or Microsoft to co-fund awareness campaigns, provide equipment, or sponsor school programs.

-Service-based collaboration: Offer co-branded safety initiatives (e.g., child-safe internet packages) in exchange for long-term partnership support.

-Digital Education Packages: Develop digital literacy content that companies can include in employee training or community outreach.

2. Social Enterprise Model

This model may achieve self-generated income in order to reduce dependency and to fosters innovation. Social enterprises may use the following strategies:

-Paid Training Services: Offer certified training for teachers, parents, and youth workers on digital safety and online behavior.

-Consulting Services: Provide expert advisory on child protection online to schools, local governments, and NGOs.

-Educational Materials: Sell or license high-quality, culturally adapted educational content to schools and media outlets.

3. Subscription-Based Services

Recurring revenue can support operational costs and growth. Subscription-based services may use the following strategies:

-School Subscriptions: Create a tiered subscription model offering schools access to exclusive toolkits, workshops, and helpline access.

-Corporate Memberships: Offer an annual membership to companies interested in digital safety certification, staff training, or joint awareness campaigns.

4. Government Co-Financing

Embedding the SIC into national digital policy ensures long-term relevance and funding. It may include:

-Annual Budget Line: Advocate for the SIC to be formally recognized and funded as part of digital transformation or child protection strategies.

-Performance-Based Agreements: Position the SIC as a service provider for achieving national objectives in cybersecurity, education, and child welfare.

5. Integration into National Digital and Educational Infrastructure

Embedding the center's services within national systems builds long-term relevance and recurring financing. It may include:

-Formal Partnerships with Ministries: Develop memorandums of understanding with the Ministry of Education to integrate SIC programs into school curricula.

-Curriculum Licensing: Offer co-developed internet safety curriculum to education institutions under a paid license or subscription.

6. Events and Campaign Monetization

Events raise awareness and can generate revenue. The following strategies can be used here:

-Sponsorships for Safer Internet Day and National Campaigns: Secure annual sponsorships from businesses to fund events in exchange for visibility.

-Branded Workshops or Conferences: Charge attendance fees for professional training days or national forums on digital safety.

7. Digital Tools and Product Development

Products provide recurring value and potential licensing revenue. Here, the following strategies may be used:

-Mobile Application or Online Platform: Create a parental control or awareness application with a freemium model.

-Data & Research Services: Offer insights or trend analysis reports on digital behavior for media, academia, or private sector.

-Evaluate potential revenue streams and financial benefits.

When it comes to evaluation of potential revenue streams and financial benefits, the following table can be taken into consideration.

Table: Evaluation of Potential Revenue Streams & Financial Benefits

Revenue Stream	**Description**	**Financial Potential**	**Scalability**	**Alignment with Mission**	**Risks / Considerations**
1. Government Co-Financing	Annual budget support from relevant ministries (Education, Digitalization, Interior).	Medium to High (depending on political will and policy integration).	Moderate (can grow with service delivery results).	Very high – aligns with national digital safety and education goals.	Vulnerable to political changes and budget reallocations.
2. EU Grants (e.g., CEF, IPA III, Erasmus+)	Programmatic funding from EU institutions for SIC setup, operations, and collaboration.	High (initial capital, program coverage, capacity-building).	High (with proper proposal writing & partnerships).	Very high – designed for exactly such centers.	Competitive, complex applications, periodic cycles.
3. Private Sector Partnerships (CSR)	Corporate sponsorships (telecoms, banks, tech firms) for campaigns, training, equipment.	Medium	Medium	High – especially on shared responsibility for internet safety.	Dependent on continued corporate interest; may seek branding leverage.
4. Fee-Based Training and Consulting	Offering paid workshops to educators, professionals,	Low to Moderate	High (once expertise and	High – delivers mission while	Market may be limited; initial demand-

	parents, or youth organizations.		brand are established).	generating revenue.	building required.
5. Licensing Educational Content / Tools	Selling or licensing training materials, safety curriculum, or apps to schools and NGOs.	Moderate	High (scales nationally and regionally).	High – promotes safe online behavior education.	Requires strong IP development and protection.
6. Membership / Subscription Models	Paid access to toolkits, events, or premium services for schools, companies, or NGOs.	Low to Moderate	Medium	Medium – if benefits are clearly tied to internet safety.	Needs a strong value proposition to attract and retain members.
7. Sponsorship of National Campaigns	Partnering with brands for Safer Internet Day or awareness drives.	Low to Moderate	Low to Medium	High – supports awareness-raising mission.	Event-specific; dependent on annual planning and visibility.
8. Paid Research and Reports	Producing commissioned studies on child online behavior, digital risks, etc.	Low	Low to Moderate	Medium – promotes knowledge, can build expertise.	Market is niche; requires research capacity.
9. Freemium Digital Tools / App	Basic free online safety tools with paid premium features for schools or families.	Moderate (if scaled successfully)	High	High – directly supports safer internet usage.	Development costs, ongoing maintenance, and adoption rates.

10. Crowdfunding & Donations	Community or diaspora-based fundraising for specific causes or tools.	Low	Low	Medium – if tied to specific impact-driven goals.	Not reliable for core funding; useful only for small projects.

7.2. Most Important Cost-Saving Sustainability Ideas

DO NOT create a new legal entity

The Feasibility Study clearly indicates that long-term sustainability and cost-efficiency of the Safer Internet Centre (SIC) can be achieved through four key strategic choices. First, instead of establishing a new legal entity, the SIC should be embedded within the Ministry of Digital Transformation (MDT) and gradually transitioned from a project unit into a Secretariat structure, thereby avoiding duplication of administrative, HR, legal, and infrastructure costs

The feasibility study clearly states that establishing a new agency or authority is **not realistic** in the remaining period and suggests:

Transition from project unit → Secretariat under State Secretary → Institutionalization within MDT. Instead, embedding within **Ministry of Digital Transformation (MDT)**:

- Removes separate rent
- Removes separate administrative staff
- Removes need for new legal framework
- Uses existing ministry infrastructure
- Uses existing procurement systems
- Uses existing legal department
- Uses existing HR department

Estimated annual savings: → **30,000–50,000 EUR per year**

Use the Consortia Model to Reduce HR Costs

Second, the consortia-led hybrid governance model should be maintained, allowing NGOs, academia, and private sector partners to deliver specific services (such as awareness campaigns, research, youth engagement, or hotline functions) through Memoranda of Understanding, rather than creating parallel in-house structures, which significantly reduces staffing and operational expenses.

Instead of hiring:

- Full-time Awareness team
- Full-time Youth Panel staff
- Full-time Hotline staff

You can:

Function	Cost-Saving Alternative
Awareness campaigns	Universities + BDE + NGO partners
Youth Panel	Youth NGOs + volunteer model
Hotline	MoU with NGO instead of creating new unit
Research	Academic partners (FINKI, UKIM, UKLO)

Result: You pay only for:

- Coordination
- Minimum technical staff
- Core helpline operators

Instead of full institutional replication.

Estimated annual savings:
→ **40,000–70,000 EUR**

Phased Implementation = Controlled Budget Growth

Third, a phased implementation approach—moving from initial operational setup to structured governance and eventual institutionalization—ensures controlled budget growth and prevents premature expansion beyond available resources

Instead of launching everything at once (helpline + hotline + awareness + youth + AI tools), you:

Phase	Core Focus	Operational Scope	Cost-Control Effect
Phase 1 – Initial Operational Setup	Establish functional minimum service	• Basic helpline• Basic awareness activities• No expensive AI tools• No large staff expansion	Prevents early over-spending and avoids unnecessary technological and HR scaling before service demand is validated
Phase 2 – Secretariat Model	Governance consolidation under MDT	• Transition to Secretariat structure• Minimal HR expansion (coordination-focused)• Strengthened SOPs and structured oversight	Avoids premature infrastructure expansion while improving coordination efficiency
Phase 3 – Institutionalization	Long-term structural embedding	• Formalized governance model• Full institutional integration• Expansion only once stable funding exists	Prevents hiring too early and ensures infrastructure growth aligns with secured and predictable funding

Do NOT Over-Engineer Technology in Early Years

Finally, technological development should follow a gradual and scalable model, prioritizing open-source solutions and essential functionality in early stages, while postponing advanced features such as AI integration until stable funding and technical capacity are secured

Together, these four elements form a realistic and financially sustainable pathway for establishing and maintaining the SIC in North Macedonia without creating unnecessary structural or financial burdens.

USE the teachers Network for Informatics as baseline

Leverage the existing Teachers' Network for Informatics as a foundational operational layer for the SIC. This network represents a strategically valuable resource that can function as a structured outsourcing mechanism, given that its members are already employed and remunerated by the Ministry of Education. Through formal cooperation arrangements, the network can contribute to the delivery of educational activities, co-design of digital safety curricula and materials, strategic advisory input, dissemination of awareness campaigns, and support in research data collection and analysis. Utilizing this pre-existing, institutionally anchored capacity reduces additional staffing costs, avoids duplication of effort, and strengthens cross-ministerial ownership while maintaining financial efficiency and operational scalability.

Cooperate with the Bureau for Educational Development to introduce obligatory training for teachers.

7.3 Revised Sustainable Cost Model (If Applying These Ideas)

If you apply the feasibility logic correctly, instead of **~200,000 EUR annually, SIC** can realistically operate at:

💰 130,000–150,000 EUR annually by:

- Embedding in MDT
- Using consortia partners for service delivery
- Avoiding new legal structure
- Phasing technological upgrades
- Delaying AI features
- Using MoUs for hotline
- Keeping youth panel voluntary

7.4 Strong Sense of Stakeholder Ownership and Participation – IMPACT

For the purpose of the Sustainability Plan, **the impact sustainability is defined as the stakeholder ownership and participation in the current and future activities of the center (involvement) and the opportunities for reinforcing and replicating its impact through partnerships and collaborations. Impact sustainability is a social and systemic function — not just about surviving but thriving through ecosystem integration.**

Focused on engagement, co-creation, and responsiveness, this subsection shows how SIC fosters long-term relevance and legitimacy by meaningfully involving its stakeholders.

9.1 **Structured Stakeholder Mapping - Identification of Key Actors**: Mapping of relevant private sector entities (e.g. ISPs, social media platforms, mobile operators, cybersecurity firms), as well as public institutions, educators, parents' associations, youth groups, and NGOs.

Segmentation: Categorizing stakeholders by sector, expertise, geographical relevance, and level of influence in internet governance and child online protection.

9.2. Engagement Mechanisms - To ensure relevance and responsiveness, SIC needs to implement structured processes to engage with the private sector and other key stakeholders:

- **Advisory Committees**: Regular input from a multi-sector advisory group, including representatives from ICT companies, education, government, and youth organizations.
- **Industry Roundtables**: Hosting annual roundtables with tech platforms, ISPs, and cybersecurity firms to align priorities and address emerging challenges.
- **Feedback Mechanisms**: Utilizing online surveys, consultation sessions, and public forums to gather input from users, including children, parents, and educators.
- **Co-Creation Models**: Involving stakeholders to participate in the design and evaluation of educational materials, campaigns, and reporting tools.
- **Formalized Partnerships**: Establishing Memoranda of Understanding (MoUs) with private sector actors to support in-kind contributions, joint campaigns, and data sharing agreements.

9.3 Feedback Integration & Response Process

- **Feedback logging and analysis:** All inputs are recorded, analyzed thematically, and forwarded to relevant teams to influence program development
- **Response timeline:** SIC acknowledges input within two weeks and provides a substantive response within one month
- **Annual Feedback Report:** A public summary of stakeholder contributions, how they were addressed, and the resulting actions or changes
- **Adaptive program design:** Using stakeholder feedback to update and refine strategies and services

Reinforcing Impact Through Partnerships and Collaborations - Focused on scalability, leverage of resources, and policy influence.

Types of Partnerships

Public sector: Education, law enforcement, regulatory bodies

Private sector: ISPs, tech platforms, telecommunications companies

Academia, Universities, Research centers other types of higher education institutions

NGOs, and international networks: child rights organizations, regional and EU-level safety coalitions, other NGOs

Partnership Benefits and Functions

Shared expertise: Specialized knowledge and innovation from academic institutions, NGOs, government agencies, and tech companies

Expanded outreach: Wider geographic and demographic scope for SIC's campaigns and services

Joint project development: Collaborating to secure national and international funding

Policy alignment: Coordinated stakeholder approach to influence national and EU-level policy

Formalization and Longevity

Memoranda of Understanding (MoUs): Agreements with partners for in-kind contributions, data sharing, and joint campaigns

Joint KPIs or outcomes: Co-defined metrics to track partnership impact

Sustainability clauses: Embedding long-term collaboration goals in partnership agreements

SIC embraces the Quadruple Helix model, which integrates academia, government, industry, and civil society as co-creators in shaping the safer internet ecosystem. This model ensures diversity of perspectives, fosters systemic innovation, and helps embed safer internet practices in policy, education, and technological development.

Monitoring and Evaluating Impact Sustainability

SIC tracks the effectiveness of its engagement and partnerships:

Stakeholder engagement KPIs: Participation rate, retention, activity levels

Campaign reach and policy uptake: Metrics for public impact and policy influence

Replication indicators: Number of replicated tools, initiatives, or campaigns by partners

Inclusion metrics: Engagement of underrepresented groups, especially youth from minority communities

Public reporting and reviews: Annual reports, data insights, and structured evaluations

Knowledge sharing: Integration of new evidence and best practices through national and EU networks

.Stakeholder's Input

Regarding the process for collecting input from the private sector and other relevant stakeholders, SIC recognizes that multi-stakeholder engagement is essential for developing effective, relevant, and responsive internet safety policies and services. The process for collecting input is designed to be structured, inclusive, transparent, and continuous. It includes the following components:

Engagement Platforms and Mechanisms

Multi-Stakeholder Advisory Committee: A permanent committee including representatives from the private sector, academia, child protection agencies, youth representatives, and civil society organizations. This body meets quarterly to:

- Provide strategic advice on SIC priorities
- Review emerging risks and mitigation strategies
- Validate annual plans and policy recommendations

Sector-Specific Working Groups: These are thematic sub-groups (e.g., content moderation, reporting and takedown mechanisms, AI and children's safety) that meet as needed to provide specialized feedback.

Annual Industry Roundtables: A formal convening of digital industry leaders and SIC stakeholders to:

- Review the impact of SIC programs on industry practices
- Identify co-creation opportunities for tools, awareness campaigns, and reporting mechanisms
- Share innovations and discuss regulatory trends

Public Consultations and Surveys: These include:

- Online surveys targeting industry professionals, educators, and parents
- Anonymous feedback tools for youth to share concerns or suggest improvements
- National public consultation periods when revising policies or introducing major programs

Digital Collaboration Hub: A secure, interactive online platform where stakeholders can:

- Submit ideas or proposals
- Comment on policy drafts
- Access real-time updates and discussion threads
- Download stakeholder briefings and share input asynchronously

Youth Participation Channels

Youth Advisory Board: Comprising young people from diverse backgrounds, the board:

- Reviews educational materials and campaign messaging
- Advises on online trends, youth behaviors, and platform usage
- Participates in consultations with tech companies to ensure youth perspectives are represented

Youth-Led Consultations: Facilitated peer-to-peer sessions where youth gather feedback from their peers and present findings to SIC and stakeholders.

Feedback Integration and Response

Feedback Log and Analysis: All inputs are recorded, thematically analyzed, and shared with relevant teams to inform program design, campaign development, and policy positions.

Response Timeline: SIC commits to acknowledging stakeholder input within two weeks and providing a substantive response or update within one month.

Annual Feedback Report: A public summary of stakeholder contributions, how they were addressed, and resulting actions or changes to SIC operations or policies.

This process ensures that the voices of industry, civil society, children, and the public are consistently integrated into the planning, delivery, and evaluation of SIC services—helping build trust, accountability, and relevance in all aspects of safer internet governance.

8. ANNEX 1- Roadmap to Risk Identification, Management and Mitigation

A. Technical Risks (Technology-related risks

Technology Risk refers to technological failure that leads to the inability to use the environment properly and timely provide services. It is closely linked to operational risk. The process may be exposed to potential breakdowns from a number of sources, e.g., hacking, power failure, system faults, etc., and any breakdown in this chain leads to an inability to complete the operation. If technology failure is persistent and severe, the regulator may step in and impose penalties or revoke the license; users may simply abandon the service, since they lost trust or it can leave opportunities for fraudsters to take advantage of system inadequacies to conduct unauthorized access to sensitive personal data and information.

While determining service levels provided by technology, the focus should be put on the quality and availability of the technology. It is therefore important to have clear and agreed-upon fault diagnosis, resolution, and escalation processes in place. Another potential risk is measurement of the end-user experience. When entering into partner agreements, it is essential to determine in advance technology KPIs and ensure that these can be measured in full. Also, a potential exit strategy should be taken into consideration.

Based on the MKSafeNet's technical architecture and infrastructure, following technical risks are detected:

Software Vulnerabilities and Failure: Inherent in any technical system is the potential for software issues. There are many potential causes of software vulnerabilities and failure, such as bugs, changes to seemingly unrelated systems both in-house and in partner systems, and poor update and maintenance procedures. If systems are not adequately maintained and available so that users and other connected parties, it may result in a significant reputational damage for SIC. It is not realistic to imagine that any system can provide full availability, nor it can be expected from newly deployed applications to contain zero-day availability, but service outages can be minimized by employing rigorous good practices or regular time patching. Identification of potential software failures begins with the identification of all systems involved in each type of activity. There are several different systems and types of software that may be involved in an SIC implementation, and once identified, a risk analysis can be conducted to understand the potential vulnerabilities of the SIC' system(s) and the interactions with other systems. As far as possible, SIC should also understand the pressure points in their partners' systems to ensure that partners (other involved stakeholders – helplines, hotlines, etc.) can fully provide the required service levels. At each layer, SIC should have a consistent plan for training, testing, and maintenance of the software, with proactive measures to prevent and detect any potential issues that could affect services. In addition, SIC must ensure that they have a clear service level agreement with their service providers and technology vendors that details not only response and resolution times for issues but also confirms the roles and responsibilities of each party. Typically, for business-critical systems, the SIC provider should specify system availability and other KPIs to ensure quality of service and then work to enforce these standards with all parties involved in the channel. When

determining service levels provided by the technology, most technical departments focus on the quality and availability of the technology for which they are responsible. As the SIC scope of services grows, it is important that there are regular meetings between technical and commercial teams to ensure that there is sufficient capacity planning to cope with growth and to support any marketing campaigns that could cause a demand spike.

Hardware Failure: Hardware failure is the inability to transact due to the failure of physical devices, as well as back-office servers and networking components. The biggest risk lies with the servers that host the SIC applications. Providers need to ensure that they have a solid business continuity plan in place. This should include backup servers that can easily be utilized in a case of failure, ideally through a 'mirrored' service that ensures that the live servers are replicated in real time, so that in the case of failure, the backup will be immediately available. Power outages can be an issue in many emerging markets, so reserved power supplies are needed. These may be generators in large establishments like the provider's offices, or other relevant devices as simple as solar chargers. In addition, there is a need for disaster recovery systems that can be brought online at short notice in case of a catastrophic failure of the main servers, such as fire, flood, or a terrorist attack. Many countries have regulations dictating the minimum distance between the main site and that of the disaster recovery system, and the maximum duration of the switchover before the service is again available. Unavoidable "wear and tear" necessitates regular maintenance and updating of hardware. Many companies now operate systems in the cloud and assume that this ensures a constantly maintained and updated, distributed system in which capacity increases and disaster recovery is guaranteed. These assumptions need to be clarified in the hosting contract and regularly reconfirmed. However, using the cloud presents other potential risks. Cloud-based services rely on high-quality internet links, and the provider should use a minimum of two independent internet services in the country with sufficient capacity and availability on different internet routing. Another risk of cloud service is security; cloud-based servers make the SIC provider dependent on the cloud provider to ensure that suitable security measures are in place, and the SIC provider may need to perform an audit of the hosting sites and protocols to confirm that this is indeed the case. Devices are not typically covered by service-level agreements, but rather through manufacturer's warranties. When selecting devices, there should be legal agreements concerning device maintenance, repair and replacement, including liabilities, timings, and costs as well as expected normal failure rates for the devices. It is important to note that hardware failure may be caused by failure of the device itself or failure of its connection to the back-end software. It is important that the provider is able to quickly diagnose the root cause of hardware failure in order to know the type of solution to apply to maintain service.

Usage of legacy system that is dated or supported system: The reliability and security of the technical infrastructure are critical to the SIC's operation; thus, in case of usage of the legacy system it should be able to support modern security tools or patch updates, making them prime targets for exploitation.

Network Connectivity Failure: Hardware failure also includes connectivity issues, which continue to be a major challenge in developing markets, particularly in rural areas. Intermittent coverage, insufficient availability, and network downtime inhibit transactions and can result in

a loss of business. Connectivity starts with the internal networks of the provider and extends to the communication infrastructure that connects to third parties involved in the channel offering and to the client. If networks are down, the user will not be able to use SIC's services. If this is a persistent issue, it will lead to reputational risk as it affects the user's experience when there are long time periods for networks to come back online. Since voice and SMS channels are relatively more stable and have wider availability than data networks, it is recommendable to choose to use those channels instead of data. It is recommended that SIC can provide devices with dual SIMs so that it can be easy to switch between them when one operator is down.

Operation Activities Delays: These delays may be caused by technology having insufficient capacity to deal with demand, causing queues in the system. If there are multiple interconnected systems, a breakdown at any point in the chain could cause the service to be delayed or not provided at all. This can include delays in the receipt of a confirmation SMS to the user's device. These queues can also have more significant consequences, such as the system failing to process activities or leaving them hanging indefinitely. Additionally, regarding platform reliability and downtime, interruptions in reporting platforms, helpline systems, or websites can further disrupt services for victims of online abuse.

System Downtime or Failure: Interruptions in security information and event management (SIEM), firewalls, or detection tools can create blind spots in the center's monitoring capabilities, increasing risk exposure.

Loss of Data: Data protection should be included in the providers' business continuity plans to ensure that the use of data is not lost or compromised through theft, loss, neglect, or insecure practices. User data should be stored off-site with backups.

Cyber Attacks: Cyber-attacks are security threats to the user integrity, as well as potential attacks of corporate espionage to gain access to internal processes and technological strategies through hacking or malware. Cybersecurity threats like advanced Persistent Threats (APTs), Distributed Denial of Service (DDoS) attacks, and ransomware campaigns specifically target SICs, especially when operating helplines and/or hotline (s) to disable critical infrastructure or steal sensitive data. In this line, vulnerabilities connected to cyber-attacks connected to SIC should be evaluated and appropriate security measures should be implemented. A variety of factors are driving exposure to cybersecurity threats. The interplay between advances in technology, changes in business models, and changes in how organizations and their users use technology creates vulnerabilities in information technology systems. For example, web-based activities can create opportunities for attackers to disrupt or gain access to users' information. The landscape of threat actors includes cybercriminals whose objective may be to steal sensitive data and information for commercial gain, nation states that may acquire information to advance national objectives, and hacktivists whose objectives may be to disrupt and embarrass an entity. Attackers and the tools available are increasingly sophisticated. Insiders, too, can pose significant threats. Cyber-attacks are often carried out in four stages: infiltration, where the attacker gains first access; propagation, where the attacker expands access through back doors or password mining; aggregation, where the attacker collects records and data; and exfiltration, when the data is exported. Most defense is focused on the infiltration stage, but since attackers are often the most skilled ones, successful defense should be included at all

stages. To manage the risk of cyberattacks, SIC can work with auditors to develop threat models where breach points are mapped and mitigation strategies developed.

Other external events risks: SIC also faces challenges from events beyond its control that can compromise operations or safety such as natural disasters or environmental hazards (floods, fires, or other disasters) that can physically damage servers or data centers, disrupting operations and compromising stored data.

Failure to Keep Up with Digital Trends: As online threats evolve rapidly, failure to keep staff and systems updated poses a serious risk to relevance and effectiveness.

MkSafeNet should build its capacities, keeping the following points in mind:

A sound governance framework with strong leadership is essential. Tone from the top engagement on technical issues is critical to the success of technical and cybersecurity programs.

Proactive risk assessment provides a basis for making informed decisions about mitigating potential threats to SIC's operations and strategic goals. Due to rapid technological evolution and faced increasement threats from cyber-attacks, data breaches, and technology obsolescence, the risk assessment should be focused on: technology risk assessment, IT risk assessment and Information security risk assessment. It is an ongoing process that should be integrated into the broader internal risk management strategy and performed at least once a year.

Technology risk assessment focuses broadly on the risks associated with using, managing, operating, and adopting technology within an organization. It covers many risks like cyber threats, system failures, data problems, and following compliance with technology standards. The goal is to identify and mitigate risks that could impact technology's ability to support business objectives effectively.

IT risk assessment is a subset of technology risk assessment, primarily concentrating on the information technology infrastructure of SIC. It involves evaluating risks related to IT systems, networks, and data management processes. The assessment aims to ensure the reliability, availability, and security of IT resources, addressing risks from both technical and operational perspectives.

Information security risk assessment delves into risks specifically related to data confidentiality, integrity, and availability. It identifies vulnerabilities and threats to an SIC's information assets, including risks of unauthorized access, data breaches, and loss of sensitive information. This assessment develops strategies to protect data against cyber threats and ensure compliance with applicable data protection laws and regulations.

Technical controls, a central component in an SIC's cybersecurity program, are highly contingent on individual situations.

SIC should develop, implement, and test incident response plans. Key elements of such plans include containment and mitigation, eradication and recovery, investigation, notification, and customer communication.

If SIC uses vendors for its services, the vendor or open-source platform has access to confidential and/or sensitive information or access to the organization's system. In this line, cybersecurity risk exposures that arise from these relationships by exercising strong due diligence across the lifecycle of vendor/open-source relationships should be provided.

Well-trained staff represent an important defense against cyberattacks and other technical aspects. Even well-intentioned staff can become inadvertent vectors for successful cyberattacks, for example, through the unintentional downloading of malware. Effective training, as well as implementation of technical measures, helps reduce the likelihood that such attacks will be successful.

SIC should consider taking advantage of intelligence-sharing opportunities to protect itself from cyber threats. There are significant opportunities to engage in collaborative self-defense through such sharing with other relevant institutions and regulators.

SIC can protect by using cloud services that are likely more secure than proprietary hosting or purchase cyber-attack insurance to protect against losses from financial and data loss, or legal expenses.

Based on the model defined in point 3 of this Sustainability plan, following insights should be pointed out:

Call center: Investment in redundant hardware and skilled IT personnel. .

Wordpress: A strong, cost-effective platform if security is tightly managed. However, it is also one of the most exploited platforms if plugins are outdated or poorly configured. Regular updates, access control, and web application firewall (WAF) implementation are strongly recommended.

Case Management (Microsoft .NET): Requires a dedicated hosting environment. Automating software updates should be considered, and penetration tests should be conducted annually or biannually.

Telecom Line Call center: Using a Macedonian telecom provider is sensible for local compliance. In this line, data routing and call logs should be provided to remain confidential and compliant with national privacy regulations.

Category	Technical Characteristics (As Provided)	Alignment with Strategic Priorities	Observations / Recommendations
1. Governance & Leadership	Technical description to be explicitly addressed	Detailed governance structure should be provided	A governance framework overseeing platform maintenance, security policy enforcement (f**ormal cybersecurity and IT governance policies** including vendor management, risk assessment timelines, and leadership roles needs to be provided and implemented), vendor selection, and periodic reviews should be introduced. Ensure leadership involvement in tech decision-making.
2. Risk Assessments (Technology, IT, InfoSec)	Platforms chosen for low maintenance, cost-effective; limited mention of cybersecurity risks	Risk assessments are not mentioned	Formal annual **Technology**, **IT**, and **Information Security** risk assessments (e.g., vulnerability scanning, compliance reviews, threat modeling) for Wordpress, Call Center, .NET case management, and all integrated services.
3. Technical Controls & Incident Response	3CX offers out-of-the-box controls (call logs, reports). Minimal maintenance noted, but response plans or backup strategies are not mentioned	Incident response plans and technical control strategies are missing.	**Disaster recovery and Incident response plans** (containment, investigation, recovery) for each platform should be developed and tested, and technical controls (e.g., access restrictions, encryption, monitoring) should be further defined. Response protocols for cyberattacks or data breaches should be also included. **Routine security audits and updates**, especially for Wordpress plugins and cloud service

			configurations, should be implemented.
4. Third-Party and Open-Source Risk Management	Uses Wordpress (open-source), FreePBX, Asterisk,, and Microsoft .NET hosting. The evaluation of self-hosted vs. cloud solutions is provided	**All third-party platform dependencies**, ensuring backup options and alternatives are identified, documented and evaluated.	Maintain a **vendor and platform risk register**. Changes in third-party platforms (e.g., API updates, feature deprecation) should be regularly monitored. Long-term sustainability and API change risks are considered. Ensure agreements include data protection clauses.
5. Staff Training and Awareness	Internal technical or cybersecurity training should be provided	**Staff training programs** for general cybersecurity hygiene and platform-specific maintenance should be regularly provided	**Staff cybersecurity training** to prevent unintentional threats (e.g., phishing, malware) should be introduced. Technical administrators should receive training on Wordpress hardening, 3CX configurations, and .NET patch management.
6. Intelligence Sharing & Collaboration	Intelligence Sharing & Collaboration should be provided	**Collaboration for these issues is crucial**	**MKSafeNet should be part of national cybersecurity networks** or threat-sharing communities (e.g., MKD-CERT, regional digital CSO networks, etc).
7. Protective Tools (Cloud, Insurance)	Hosting via third-party providers . The use of Wordpress aligns with low-cost distribution	**These tools should lower the total risk of used infrastructure**	**Cyber insurance** options for potential data breaches or system outages should be explored. **Backups on secure cloud infrastructure should be provided**. Wordpress security plugins, SSL, and regular patching should be provided.

			Ensure cloud platforms have built-in compliance (e.g., GDPR readiness).

Summary:

The effective operation of the SIC would depend on up-to-date and reliable technology that allows for smooth functioning in terms of online reporting tools, as well as learning platforms. The main technical risks are connected to how reliable, secure and adaptable these systems are. The early detection and response to various challenges will help prevent disruptions in the provision of services and keep the Centre effective. In the line, the following technical risks are:

Technology infrastructure and maintenance – The digital infrastructure of the Centre (ex. reporting system, helpline databases, websites) can potentially become obsolete or unreliable if there is no adequate maintenance. Considerable technical malfunctions can lead to the inability to provide services or assistance to users.

Mitigation: Resources should be planned and set aside for maintenance of the system, including updates and enhancements. The Centre will regularly examine all systems to make sure they work properly and can cope with new users over time. Partnerships with IT providers, and use of modular technologies, which are widely supported, will further reduce the risk of outdated technology and operation interruption.

Cybersecurity threats – The center is unique because it is the only capability in the country to provide digital safety services of this kind and therefore it is necessary to implement mechanisms for dealing with cyberattacks or unauthorized access attempts. In that context, data breaches or extended breakdown because of ransomware, for example, would cause distrust among users and will affect the regular operation of the center.

Mitigation: Adequate cybersecurity protocols and data protection measures should be implemented. These will specify regular system checks in relation to security issues, testing for weaknesses, using updated firewalls and encryption to protect sensitive data, and stipulate clear incident response plans. Cybersecurity training will be provided to the Centre's staff, and a technical team will be appointed to constantly watch for risks. These measures will serve to limit the damage of any attack and ensure quick recovery of services.

Mitigation measures:

Technical Implementation of Strong Cybersecurity Protocols:

Usage of encrypted communications (SSL/TLS), multi-factor authentication and usage of strong passwords, and regular vulnerability assessments.

Partnership or outsourcing with cybersecurity firms for regular penetration testing.

Investment in Reliable IT Infrastructure:

Usage cloud-based, scalable platforms with 99.9% uptime.

Having redundant systems in place to ensure continuity during failures.

Regular software and systems updated (operating systems, and security tools to patch vulnerabilities).

Leverage advanced security tools: Utilize firewalls, intrusion detection systems, and endpoint protection software to enhance security.

Encryption of sensitive data: Use encryption to protect data in transit and at rest.

Network segmentation: Isolate critical systems to limit the impact of breaches.

Keeping pace with Technology:

Establishment of innovation and research unit within the SIC to monitor digital safety trends (e.g., AI-generated abuse, deepfakes) and how it can be used as evidence for criminal proceedings.

Train staff continuously (at least once annually) on the latest online threats and mitigation strategies.

By detecting and facing technical challenges, the Centre will provide a safe service to its users. However, technology alone is not enough; sustained operation also depends on financial stability. The next set of risks is related to budget and financial management.

B. Operational Risks and Mitigation

Operational risk is inherent in every business. It refers to risks associated with services, business practices, damage to physical assets, as well as the execution, delivery, and process management of the service. In practice, this refers to the diverse range of activities needed to administer the operational activities. For the most part, operational risks are internal to the organization and can therefore be carefully managed.

In terms of MkSafeNet, the critical area of operation is the day-to-day services provided to support users. This can include functions connected with operational activities, such as:

Customer service operations: aiding external users of the service (customers and others) and escalating issues that they cannot resolve

Back-office operations: such as troubleshooting issues, and testing any changes to the service (usually minor operational updates)

Finance operations: providing business reports

Technical operations: providing the hosting environment and support for the technology.

Operational (Business) Processes: The key to efficient operations that minimize risk is to have high-quality, efficient, and effective operational processes. Operational processes should always add value to customers and mitigate risks. While many institutions blame technology or governance as the cause of fraud, many cases of major internal SIC fraud can be traced back to inadequate (or non-existent) operational processes that allowed fraudsters to abuse the service. Every operational process that is performed regularly should be documented, describing what needs to be done, how to do it, and who is responsible for doing it. Operational processes should also cater for exceptions, specifying the manner of conduct if something goes wrong at any point in the process and thus the standard path cannot be followed.

These processes need to be reviewed and updated regularly to ensure that they are still relevant. This is particularly important in the early part of the service lifecycle. It is recommended that draft operational processes created before launch are reviewed and finalized in a previously defined time framework after launch, when the operations team has experience with real-life operations. Thereafter, they should ideally be reviewed annually. If new functionality is introduced, new operational processes will be required to manage the new activities. Suitable technology can be used to prevent the occurrence of different risk events, but ultimately, particularly as the technology for many SIC is not yet fully mature, the best protection from operational risk is well constructed operational processes that are properly followed and updated, and which are regularly reviewed during internal audits to ensure compliance.

Internal Control: Internal control procedures are used to protect against fraud, disruptions, and reputational risk by ensuring adherence to operational processes. The internal control department conducts operational audits on the SIC and its employees to ensure that correct procedures are complying with applicable regulations and operational standards. The internal control department tests the effectiveness of these procedures and standards and revises policies and procedures based on continuous feedback and a learning loop.

Internal Audit: Internal audits provide assurance and checking of processes and controls. The internal audit department is responsible for ensuring that financial reporting is accurate and reflective of the real state of financial affairs of the SIC; those business/operational risks are assessed and mitigated; and that controls are effective. Based on risk-based methodology approach, internal audits may conduct more frequent audits of the entity, high-risk functions and processes, as well as operational spot audits of employees, recording of activities, and to detect fraud and other misdemeanors.

Segregation of Duties: Segregation of duties is a procedural methodology that ensures there are adequate checks and balances in place to protect against conflicts of interest and control

breakdowns. An example of segregation of duties is the accounting principle (sometimes known as "maker, checker and approver") whereby the person carrying out a service or process is separated from the one reviewing the activity and the one approving the activity, to minimize errors and opportunities for fraud and mismanagement of funds. IT systems can be set up so that there is role-based access depending on the requirements for each job function. An example of role-based access is to enforce segregation of duties so that an operator can only access those functions required to perform their job.

External Reporting: International organizations, being part of a network, donors, and shareholders, may require additional reporting to monitor performance, minimize the risk of their investments, and ensure early detection of problems, either operational or financial. Reporting is conducted on a defined time framework, challenges, and lessons learned.

External (Financial) Audit: Most institutions, especially regulated or public institutions, are required to have external audits conducted at least once per year. An external audit is mostly focused on the financial reporting of the institution and ensuring accurate posting of transactions as well as adequate depreciation and valuation of the institution's assets. It may also include further checks on controls, particularly for high-risk activities and processes.

Damage to Physical Assets: Damage to physical assets can result from normal wear and tear, natural disasters, acts of terrorism, or vandalism. It is important that potential damage to physical assets is included as part of business continuity plans and disaster recovery plans. Potential mitigation strategies can include property insurance, backup systems, and off-site data storage.

Execution, Delivery, and Process Management: Operational risk derived from operator error in execution, delivery, and process management includes risks such as data entry errors, accounting errors, lack of mandatory reporting and negligent loss of client data information. It is closely linked to technology. In some regions, regulators are now implementing new guidelines to reduce this risk and protect customer funds. Mitigation of operator error risk can include "segregation of duties" between the person recording or reviewing it and the person approving it; role-based access to systems; agent and staff training; monitoring; or specific agents or staff who make errors frequently. Data analytics, dashboards, and algorithms can be powerful tools in mitigating operator errors if they are followed up by resolution, training, or policy enhancement that reduces the risk of continued errors.

Based on the abovementioned, operational risks can be grouped in following categories:

People-related risks connected to human factors are often the weakest link in cybersecurity and can pose significant threats to SIC:

Insufficient or inadequate Employee Training: Without regular, role-specific training for handling the sensitive cases or merging online threats and/or cybersecurity protocols, staff may inadvertently expose systems to risks through poor practices, such as weak password use or mishandling sensitive information.

Employee Misconduct or Insider Threats: Disgruntled or compromised employees could deliberately leak confidential data, disable security systems, or assist cybercriminals. Insider threats are particularly dangerous because they can bypass perimeter defenses.

Staff Burnout and Turnover: High emotional load in helpline and hotline teams can lead to stress, burnout, and attrition.

Lack of Expertise or Role Misalignment: Cybersecurity requires highly specialized skills. Inadequately trained analysts or improperly assigned roles can lead to gaps in threat detection, slow incident response, and poor risk assessments.

Process-related risks connected to flawed or outdated processes can hinder a SIC's ability to respond to threats effectively:

Ineffective Reporting Mechanisms: Poor user experience or lack of trust in reporting tools can reduce the number of incidents reported.

Inefficient Incident Response Workflows: If protocols for handling alerts, breaches, or suspicious activity are unclear or too slow, attackers may exploit this delay to cause greater damage.

Poor Monitoring and Auditing: Inadequate logging, analysis, or oversight can allow security incidents to go unnoticed, hindering both real-time defense and post-event investigation.

Failure to Update Standard Operating Procedures (SOPs): Cyber threats evolve rapidly. SOPs that are not regularly reviewed and updated may leave the center vulnerable to new forms of attack or compliance failures.

Partnership Failures: Breakdowns in coordination with law enforcement, schools, ISPs, or NGOs can reduce the center's reach and impact.

Systems-related risks (technical risks already explained in detail in point A)

Financial Risks and Mitigation

Financial sustainability is crucial for the Safer Internet Centre to continue its mission beyond the MkSafeNet project duration. The development of the SIC through MkSafeNet is currently supported by EU grants and partner contributions, but long-term success requires stable and diversified funding. Key financial risks and their mitigation strategies are outlined below. A clear focus is placed on preventing funding gaps and ensuring efficient resources usage:

Funding uncertainty after project end – The Centre currently depends on EU grants and partners' contribution, however, there needs to be commitment for continued financial support to ensure the sustainability of the SIC after the MkSafeNet project concludes. To be more precise, the uncertainty of public funding has been identified as a serious threat to the sustainability of Safer Internet Centre.

Mitigation: A long-term financial sustainability plan should be developed and implemented before the EU funding stops. The consortium is actively engaging with national authorities to

encourage institutional support (e.g. government budget inclusion for the SIC) and exploring partnerships with the private sector (corporate social responsibility programs, tech industry sponsorships) to diversify income. In this line, a reserve fund should be established to cover 6-12 months of essential operations. The Centre will engage in fundraising and advocacy efforts to increase core funding and seek additional grants or EU programs (EU grants e.g., from the Digital Europe Programme), and report its results transparently, to ensure stakeholders' trust and support. By broadening the funding base, MkSafeNet can reduce dependence on a single source and ensure continuity of services.

Exceeding the budget or cost underestimation – If the Centre's spending (salaries for the employees, service-based income for consultancy, technology upgrades, outreach activities, etc.) exceeds plans or if actual costs are higher than predicted, it could face financial difficulties. Overspending might result in interruption of services.

Mitigation: It is important to introduce strict financial management and oversight. The management team will ensure that financial planning supports the SIC's operational continuity, conducting quarterly reviews to check the financial plan realization. Resources will be planned in case of unexpected costs. If overspending risks are identified, via for ex. Implemented financial dashboards to track spending against forecast budgets, the Centre will respond swiftly by prioritizing essential functions and reallocating resources where possible, ensuring uninterrupted delivery of its core services. This approach will help the Centre stay within budget and still reach its goals.

Even with a sufficient budget in place, the Centre's success depends greatly on uninterrupted and effective operation and strong management. The following operational and organizational risks point out potential internal challenges that could influence the Centre's performance, along with measures to manage them.

Operational and Organizational Risks and mitigation

The MkSafeNet project is currently coordinated by a multi-stakeholder group—including government, academia, NGOs, and industry partners—to lay the groundwork for a future national Safer Internet Centre (SIC). While the collaborative system brings diversity in terms of expertise, it also involves risks of operations—such as coordination issues, overlapping roles, or uneven participation. Such likely risks, if left unchecked, may impact the stability and performance of the SIC upon operation. Anticipating and dealing with them at the project level will make it easier to make a transition to stable and sustainable future Centre operational mode, regardless of the eventual institutional form. The main operational risks and mitigation measures include:

Staff changes and skill gaps – The Centre relies on experienced employees, such as counselors, trainers, and technical experts to fulfill its operational goals. There is a risk that some of the key personnel could leave (due to burnout or better job offers) or that the team may not be large enough to keep up with growing needs. Losing key personnel or not having enough employees could result in interruption of services, as well as loss of valuable investment in staff development and institutional memory.

Mitigation: The focus should be development and strategies for keeping personnel. The employees will receive training, chances to grow professionally, and a supportive workplace to help them stay motivated. The salaries should also be competitive, and clear career paths should be provided to prevent losing personnel. To protect important knowledge, key processes should be documented in manuals and guides to ensure quick adaptation and instruction of new personnel. For critical roles, there should be a succession plan in place. Finally, its workload exceeds the current employee capacity; the Centre can engage volunteers or ask for partner organizations' support to temporarily fill capacity gaps.

Consortium coordination and governance – Given that several partners are involved, there is the risk of miscommunication, delayed decision-making, or inconsistency in consortium partners' priorities. Deficiencies in coordination can lead to wasted work or omitted tasks, undermining the Centre's output. In addition, a major partner can withdraw support, compromising the ability of the consortium to deliver.

Mitigation: Open governance framework and communication processes should be created from the beginning. One representative from each of the partners forms a steering committee, which makes strategic decisions, and day-to-day work is managed by individual working groups or coordinators. Day-to-day activity coordination and solving of issues is done through regular consortium meetings and joint planning sessions. Every partner has a clearly defined role and tasks in written agreements (e.g. Memoranda of Understanding), which binds them. If one partner is unable to perform its role, the governance plan has a backup plan, such as redistributing work among other partner members or finding a new partner to ensure continuity in the development and future operation of the SIC.

Stakeholder engagement and uptake –The viability of the Centre also relies on sustained demand for its services and support from the community. There is a risk that the SIC's efforts are not sufficiently recognized, and engagement is lacking by the target groups (children, parents, schools) or stakeholders (policymakers, law enforcement). Low public awareness or confidence can contribute to low usage of the helpline or poor response in awareness campaigns, decreasing the Centre's impact.

Mitigation: Put in place an effective communications strategy and stakeholder engagement plan. The Centre will undertake ongoing outreach – for instance, operating live social media campaigns, school outreach initiatives, and public webinars to make people aware of online safety and the SIC's services. School, youth organization, and media partnerships will provide an opportunity for maximum audience reach. Feedback loops are put in place (surveys, youth and parent focus groups) to find out what the community needs and believes, so that the SIC can shape its services accordingly. By showing responsiveness and value in what it does, the Centre will establish trust with users and key stakeholders and encourage greater use and support. Close collaboration with national authorities and the EU Safer Internet network will also make the Centre's activities widely acknowledged and supported at policy level, further enhancing stakeholder trust.

Enhancing Staff Capacity and Wellbeing - The quality and resilience of helpline and hotline services rely heavily on the wellbeing and preparedness of frontline staff. Given the

emotionally demanding nature of their work, there is a risk of burnout and secondary trauma, which can compromise service delivery and staff retention.

Mitigation: The Centre will strengthen internal support systems by providing access to mental health services, professional supervision, and regular debriefing sessions. Flexible work schedules, adequate rest periods, and peer support mechanisms will also be implemented to promote staff well-being and long-term engagement.

Improving Reporting Mechanisms: Accessible and trustworthy reporting channels are critical for empowering victims and facilitating timely intervention. However, complex interfaces, language barriers, or concerns about anonymity can discourage reporting and reduce the effectiveness of SIC services.

Mitigation: To address this, the Centre will develop user-friendly digital reporting tools with built-in anonymity and multilingual support. These tools will be designed with input from victims and key stakeholders to ensure they are accessible, intuitive, and aligned with user needs. Regular feedback will be collected to refine these systems and build greater trust in the reporting process.

Investing in Ongoing Training: Staff must be equipped with up-to-date skills to respond effectively to the evolving landscape of online abuse. Without regular training, there is a risk that staff may be unprepared to handle complex or emerging digital threats.

Mitigation: The Centre will deliver continuous, scenario-based training to ensure staff can navigate sensitive and multifaceted abuse cases. Cross-training will also be provided in relevant areas such as child protection, cybersecurity, legal frameworks, and digital rights to promote a well-rounded skill set and foster interdepartmental collaboration.

Strengthening Strategic Partnerships: Effective responses to online safety challenges require close coordination across sectors. Weak institutional linkages or lack of formal cooperation can hinder case resolution and limit the Centre's impact.

Mitigation: The Centre will formalize partnerships through Memorandums of Understanding (MoUs) with key stakeholders including law enforcement, education ministries, telecom regulators, and child protection NGOs. Collaborative activities—such as joint workshops, simulation drills, and regular protocol alignment meetings—will be conducted to ensure clear coordination, shared responsibilities, and consistent approaches across all involved actors.

Apart from the internal risks listed above, events in the overall external environment can also profoundly affect the long-term sustainability of the Centre. The following section considers uncertainties like regulatory change and technology development that are beyond the immediate control of the consortium but need to be integrated into planning for sustainability.

C. External Uncertainties: Regulatory and Technological Shifts

The online environment and policy context are fluid. Developments in regulation, legislation, or new technology may create uncertainties that impact how the Safer Internet Centre

functions. Such external events, while outside the control of the project, require anticipation and reaction as a crucial aspect of risk management. There are two significant external uncertainties:

Regulatory and policy changes – New laws or a change in government policy (national or at EU level) may affect the Centre's mandate or mode of operation. For instance, stricter data protection legislation or new digital safety legislation can necessitate more stringent compliance procedures, increased levels of security, or extended services. On the other hand, changes in regulation could also provide new opportunities (e.g., government-mandated activities to protect children online, which the Centre might undertake).

Mitigation: Follow closely with policy changes. The consortium is to appoint a policy liaison (legal counsel or policy advisor (s) to track associated regulatory initiatives and ensure compliance and advocate for supportive regulations – from European directives (e.g., the Digital Services Act) to national legislation in child online protection or cybersecurity. The Centre will work actively at stakeholder consultation as well as keep in touch with authorities to predict forthcoming changes. Internally, the Centre will remain flexible in its procedures to integrate new legal requirements as they emerge (e.g., more stringent data management, ePrivacy regulations, GDPR updates, legality of specific content takedown actions and reporting procedures). These modifications are incorporated by the team without delay. Compliance audits should be conducted in order to ensure that ongoing compatibility with legal and ethical standards is maintained.

Technological shifts in online behavior – Unexpected changes in user behavior and technologies have the ability to change the character of risks on the internet. An example can be seen in the emergence of new social media platforms, greater use of end-to-end encryption, or innovations in technologies such as artificial intelligence, which might rebalance how youngsters and children are interacting on the internet and what type of danger is dominating. Such trends might render some of the Centre's tools or approaches less effective over time, unless regularly reviewed and adapted.

Mitigation: Adaptive, proactive programme design approach can be adopted. The Centre will remain alert to new young people's online trends and new threats (AI-Driven Content e.g. AI-generated deepfakes, fake nudes, interactive virtual reality environments and other AI harassment tools) through research and its links with the wider Safer Internet community. The Centre will benefit from experience-sharing and best practices exchanged through the European Safer Internet network (emergence of new platforms like decentralized social media, anonymous apps, or virtual reality platforms increases complexity of monitoring). The Centre will also be ready to try out new equipment or projects in response to emerging trends in technology – i.e., creating new learning materials for a new trendy app, or using advanced content analysis packages if necessary. Vigilance and flexibility will be used to maintain the SIC as current and relevant in the event of technological change.

A. Key Legal Risk Areas

Legal risk is one of the most critical and complex areas for a Safe Internet Centre. The sensitivity of its mission demands high standards of compliance, accountability, and ongoing

vigilance. By embedding legal risk mitigation into MkSafeNet everyday operations, training, partnerships, and governance structures, both its users and institutional integrity can be protected.

1. **Potential Legal Risks for an Institutionally Established National Coordinating Body with an Inclusive Structure**

If MkSafeNet is organized as a national coordinating body within the Government institutionally established to include representatives from government institutions, the business community, NGOs, and other stakeholders, several legal risks that should be properly and timely mitigated:

Legal Status and Mandate

The legal basis for the national coordinating body should be clearly defined (e.g. by law, government decision, or regulation), to obtain certainty about its mandate, competencies, and authority.

Its nature (advisory, executive, or coordinating) should be clearly defined in order not to overlap or impose conflicts with other institutions or bodies.

The roles and responsibilities, as well as necessary resources to be clearly defined

Compliance with Legal Procedures

If the National Coordination Body's operations influence public policy or decision-making, established legal procedures for public consultations, publication, and participation should be further developed especially on timely harmonization of interconnected activities in relevant and connected laws where different institutions have a mandate.

Operations should be in accordance with administrative law (such as the Administrative Procedure Law) in order not to render decisions or make outputs legally invalid.

Transparency in member selection of the body (since they come from different parts) or decision-making processes must be provided for future legal challenges and/or reputational damage to avoid. Open and non-discriminatory access to participation should be garanteed.

Accountability and Responsibility

Accountability for all stakeholders as members of this body should be defined (whether public officials, private sector representatives, or NGOs), in order for legal uncertainty in cases of misconduct or negligence to be properly addressed.

Oversight or auditing mechanisms should be provided in order to detect liability in cases of fund mismanagement or failure to meet objectives.

Data Protection and Privacy

In case of operations processing activities connected with personal data—particularly from vulnerable groups—it must comply with the Law on Personal Data Protection (aligned with GDPR), for fines and legal action to be avoided.

Financial Liability and Misuse of Funds

If public or donor funds are managed by the National Coordination Body, it must implement transparent procurement, spending, and auditing procedures. Mismanagement may lead to financial penalties, criminal charges, or administrative sanctions.

Mitigation measures:

Clear legal acts or mandate establishing the National coordination body (e.g. government decision, law, or formal memorandum) should be defined.

Roles and responsibilities (coordination, monitoring, advisory) should be precisely defined.

Code of ethics and a conflict-of-interest registry for members shoudl be implemented.

Transparent procedures for decision-making, consultations, and public reporting should be established.

Compliance with **data protection, financial accountability**, and inclusive participation standards.

2. Data Protection and Privacy Compliance

Taking into consideration that MKSafeNet will handle personally identifiable information (PII), including reports of online abuse involving children or vulnerable individuals, mishandling this data can lead to legal liability, fines, or loss of user trust.

The following regulations is directly applicable for the Centre:

Data Protection Regulation;

National child protection or safeguarding legislation;

ePrivacy Directive and related telecom privacy laws.

Mitigation measures:

Appointment of a Data Protection Officer (DPO).

Maintenance of updated Data Protection Impact Assessments (DPIAs) for all digital tools and platforms that will be used.

For MKSafeNet operations secure data storage, end-to-end encryption, and minimal data retention periods.

2. Content Moderation and Legal Liability

In case, MKSafeNet provides hotline service, reporting platforms may be legally responsible for how quickly and appropriately they respond to reports of illegal or harmful content (e.g., child sexual abuse material - CSAM). In this regard, failure to report to the authorities could result in criminal or civil liability or other legal exposure if not compliant with the reporting procedures because it can lead to corruption or distortion of the investigation.

Mitigation measures:

The roles, responsibilities and duties need to be detailed prescribed in the Memorandum of Understanding (MoU) with law enforcement institutions. And other relevant institutions.

In this line, the operational activities should be following national and EU frameworks (e.g., INHOPE standards, EU Code of Conduct on illegal hate speech, etc.).

An action plan for providing automated content filters and escalation protocols to ensure timely handling.

Provide training on national reporting obligations to all staff and volunteers for MKSafeNet needs.

Set clear, documented workflows for case referral to police, child protection services, social service centers, etc.

Maintain audit trails showing compliance with reporting timelines and procedures.

3. Cross-Border Data Sharing

MKSafeNet often collaborates with international partners, networks, or organizations (like Europol, Interpol, INHOPE, etc.), requiring data transfer across borders.

Legal Challenge: Transferring data outside the EU requires compliance with international data protection transfer in accordance with the national data protection regulations.

Mitigation measures:

MKSafeNet should provide procedures for harmonization and usage of Standard Contractual Clauses (SCCs) or ensure international partners with adequate data protection (as defined by the European Commission). In this line, storing or processing sensitive data in countries with weak privacy laws should be avoided, and approval from the relevant Agency for data protection should be provided.

Transfer impact assessments for major cross-border collaborations should be maintained.

4. Intellectual Property and Platform Use

The maintenance of the MKSafeNet's website and campaigns can result in misuse of third-party content (logos, images, educational materials, etc.) and further result in intellectual property claims.

Mitigation measures:

Ensure all necessary licenses are in place for all third-party materials.

Provide internal procedures for usage of open-source or royalty-free content when possible.

Train communications teams on digital rights and content attribution.

5. Evolving Legal Uncertainties

In addition to current laws, MKSafeNet has to be prepared for future legislative changes and legal gray areas under EU and national regulation. In this line, even though there is no direct

implementation of EU legislation into national law, this can affect national regulation due to the process of harmonization.

Digital Services Act (DSA) and Online Safety Bills

This Act increases obligations on platforms to remove harmful content and protect minors. MKSafeNet can play a role in advising or monitoring compliance.

Mitigation measures: DSA enforcement updates should be followed, and MKSafeNet should become a trusted flagger organization to fast-track content takedown requests.

AI Regulation

Taking into consideration the increasing use of AI in abuse detection (e.g., grooming detection, image classification etc.), the upcoming EU AI Act may impose risk-classification and accountability standards.

Mitigation measures: If using AI, classify tools as per risk categories and conduct AI impact assessments.

Freedom of Expression vs. Harmful Content

Legal Balance: SICs may face criticism or legal disputes when advocating for content removal. There is often a fine legal line between removing harmful content and infringing on free speech rights.

Mitigation measures: Develop transparent content moderation policies and partner with legal advisors to review flagged cases.

To manage these legal risks proactively, the SIC should implement a structured approach:

Legal Compliance Framework

Maintain a Legal Compliance Regulatory Matrix that maps each MKSafeNet operation (helpline, hotline if applicable, awareness campaigns, etc.) to relevant national and EU laws.

Conduct quarterly compliance reviews and update internal policies and procedures accordingly.

Documentation and Record-Keeping

Logs of legal decisions, referrals, and data handling incidents should be treated as confidential.

Document staff on consent to legal policies and provide annual legal training.

Legal Partnerships should provide establishment of relationships with:

Data protection authorities and centers for social work for guidance on handling sensitive cases;

Law enforcement agencies through written collaboration agreements;

Pro bono legal support networks (e.g., child protection lawyers).

Risk Register and Legal Contingency Plans

Include legal risks in the general Risk Register with assigned legal owners.

Develop contingency plans for scenarios such as data breach investigations, lawsuit defense preparation and regulatory audit or inspection.

Mitigation measures:

In the line the following set of documents can be further used:

1. Legal Risk Checklist should be created for legal vulnerabilities to be identified, such as:

Data processing without lawful basis

Missing data protection impact assessments (DPIAs)

Unclear consent mechanisms

Incomplete cookie policies

Contracts with third-party data processors lacking required clauses

Lack of user-facing privacy policies

Untrained staff on data handling obligations

2. Legal Compliance Matrix Template that will be structured in the following manner:

Legal requirement

Source law or regulation

Responsible person/team

Current compliance status

Risk level if not complied with

Required action

Legal audits

Preparing for inspections or certifications

Board reporting.

3. Legal Awareness Training Pack (for Staff)

Materials to help train your staff:

Slide deck with key legal concepts (data privacy, consent, safeguarding)

Case studies relevant to hotlines and helplines.

Societal and Cultural Trends

Rising Digital Nationalism or Misinformation could reduce public trust and trust in MkSafeNet.

Mitigation measures: Proactively engage in public awareness campaigns to position the SIC as a trusted authority in digital safety.

As a result of the wide range of the abovementioned risks that have been identified, ranging from internal financial and technical problems to outside regulatory changes, have to further be managed by a structured, ongoing process. Therefore, a comprehensive risk management system should be established to support the Centre during and after the MkSafeNet project.

Risk Management Framework

A structured risk management framework has been developed to support the ongoing operation and resilience of the MkSafeNet. The framework promotes responsibility and improvement over time as situations change, in accordance with the best practices of the European Commission for project governance. The main elements of the framework are:

Risk Register as a living/central document: The consortium maintains a live/central risk register (digital spreadsheet or risk management software) listing all of the identified risks. Each risk is defined, assigned to a category (technical, financial, operational, legal, etc.), has an estimate of likelihood and impact, and the planned mitigation. The register is an evolving document and is updated when new risks are identified or the circumstances change. All partners assist in the identification and listing of risks in their domains in order to ensure all domains are covered. The structure should incorporate at least following elements:

Risk description

Type (technical, financial, operational)

Probability (High/Medium/Low)

Impact (High/Medium/Low)

Mitigation actions

Owner responsible

Review date and status and update

Assignment of ownership and accountability: Each risk that has been discovered must have an owner (a partner organization, institution or team leader), responsible for implementing the mitigation and reporting back on progress. By allocating owners unambiguously, the MkSafeNet is ensuring that each materially significant risk does have an owner held responsible for its management. It is the responsibility of the Project coordinator to oversee the

process and make sure that the resources and authority required to finish mitigations are assigned to the risk owners.

Risk Management Framework for documenting and managing risks as part of the sustainability planning process

In the process of supporting the long-term operation of the Safer Internet Centre (SIC), which is being established through the MkSafeNet project, it is necessary that risks are expediently identified and managed in a proactive and effective manner. This section deals with and lists the potential risks to the Centre's sustainability in terms of technical, financial, and operational aspects, and elaborates on strategies to overcome them. It also provides an analysis of external factors, such as the changes in legislation, as well as technological advancements, which may be relevant to the Centre's sustainability. Finally, a structured framework is provided for documenting and managing risks, harmonizing with the best practices for EU-funded digital safety initiatives.

A comprehensive risk management and mitigation plan for a Safe Internet Centre (SIC) should focus on educating users, raising awareness, and implementing technical safeguards.

1. Risk Assessment and Identification:

1.1. Regularly identification, assessment and mitigation measures regarding potential risks:

This includes understanding the threat landscape, potential vulnerabilities in systems and processes, and the impact of various cyber threats.

Introduction to Risk Assessment for a Safe Internet Centre (SIC)

A wide spectrum of risks including operational disruptions, cyber-attacks, legal non-compliance, financial mismanagement, and technical vulnerabilities. In order for appropriate risk assessment to be conducted, a robust Risk Assessment Methodology should be prescribed in order for the SIC to:

Identify the inherent risk and categorize risks

Evaluate the likelihood and impact

Integrate already established control mechanisms

Calculate residual risk

Implement appropriate Action plan with mitigations measures, responsible persons/units and timeframe for their implementation in timely and quality manner

Continuously monitor emerging threats

Continuously monitor the implementation of the system;

Improve the established system.

2. Risk Assessment Methodology Overview

A comprehensive risk assessment methodology suitable for a Safe Internet Centre should have the following elements:

Step 1: Risk Identification

Regularly assess and identify potential risks by:

a) Understanding the Threat Landscape

Conduct internal and external assessments to map out threats (e.g., DDoS, phishing, insider threats).

Use sources like CERTs, ENISA (EU Cyber Security Organization) reports, ISACs (Information Sharing and Analysis Center), and partner agencies.

b) Identifying Vulnerabilities in Systems and Processes

Audit IT infrastructure, network configurations, access controls, and software lifecycle.

Review organizational policies, staff awareness, and third-party vendor practices.

c) Stakeholder Input

Engage technical teams, legal advisors, finance officers, helpline operators, and hotline personnel to identify domain-specific risks.

d) Risk Categories

Identify risks under the following domains:

Category	Examples
Operational	Service outages, staff turnover, inadequate response protocols.
Financial	Budget shortfalls, misuse of funds, and funding volatility.
Legal/Compliance	GDPR violations, regulatory fines, and liability for user data.
Cyber	Malware, ransomware, DDoS, credential theft.
Technical	Outdated systems, interoperability issues, third-party failures.
Reputational	Public criticism, media exposure, and stakeholder mistrust.

Step 2: Risk Analysis

For each identified risk, the following should be further assessed:

Likelihood (How probable is it for a risk to happen?)

Impact (What would the consequences be?)

A qualitative or quantitative scoring system shall be used:

Risk Score Matrix

Likelihood: Rare (1) → Almost Certain (5)

Impact: Negligible (1) → Catastrophic (5)

The risk is calculated as a sum between likelihood and impact

Risk = Likelihood × Impact

(for example: DDoS attack (Likelihood = 4, Impact = 5) → Risk Score = 20 (High)

Step 3: Risk Evaluation & Prioritization

Rank risks based on score.

Determine risk appetite and tolerance.

Group risks: High, Medium, Low priority.

(Risk Register as template is provided as Annex to this document)

Step 4: Risk Mitigation and Control Planning

Risk Treatment Plan should be developed in the next stage:

Avoid – not continuing further with the activity.

Mitigate – reduce likelihood or impact.

Transfer – outsource or insure.

Accept – acknowledge and monitor.

Examples:

Cyber: Deploy firewalls, IDS/IPS, EDR systems, backup strategy.

Operational: Cross-train staff, maintain response SOPs.

Legal: Regular audits, legal consultations, GDPR training.

Financial: Multi-level budget reviews, contingency funding.

Technical: System patching, redundant infrastructure.

Step 5: Monitoring and Review

a) Continuous Monitoring

Usage SIEM tools, monitoring dashboards, and log analysis.

Review incident reports, near misses, and threat intelligence.

b) Periodic Risk Review

Conduct quarterly risk reviews and annual audits.

Update risk assessments to reflect new systems, threats, or regulations.

c) Reporting

Use dashboards or risk registers for stakeholders.

Escalate high-risk items to board-level governance.

Step 6: Consider Emerging Trends

Proactivity will be provided by:

Trend Monitoring: Subscribe to cybersecurity feeds, government alerts, academic journals, and NGO watchlists.

Scenario Planning: Model hypothetical threats (e.g., AI-generated abuse content).

Training & Awareness: Regular staff upskilling in phishing, new tech, and policy changes.

Technology Scanning: Evaluate the AI impact, quantum computing, 5G, etc., on your threat surface.

Emerging trends: New technologies and online safety issues to proactively address and include potential risks should be continuously considered and assessed.

2. Education and Awareness:

Provide ongoing security awareness training:

Train users in identifying phishing, using strong passwords, maintaining good cyber hygiene, and reporting suspicious activities.

Raise awareness of online safety and potential risks:

Educate users about harmful content, contact and conduct online, and encourage them to seek help when needed.

3. Empowerment of the users:

Provide them with the knowledge and skills to navigate the online world safely and responsibly.

4. Incident Response:

Develop a detailed incident response plan: Outline steps for detecting, containing, and recovering security incidents.

Establish clear reporting procedures: Ensure users and employees know how to report security incidents and that they are taken seriously.

Regularly test and update the incident response plan: Practice and refine the plan to ensure its effectiveness.

5. Mitigation measures:

Appointment of Risk Management Lead within the SIC or assign a rotating risk officer role.

Quarterly risk reviews in management meetings should be included

Escalating identified risks should be tracked and flagged, as well as notified to the top.

6. Regular review and monitoring: The risk register is regularly reviewed (e.g., quarterly reviews and at every major project milestone) as well as ad-hoc if a significant event takes place. Upon review, the consortium assesses each risk's status, whether reduction measures have been effective, and re-prioritizes. High-risk or growing risks are brought to immediate attention to the project steering committee for action. This ongoing monitoring keeps problems from deteriorating or being neglected; it brings risk awareness into everyday management.

7. **Documentation and reporting:** Risk status changes and risk management actions are recorded in meeting notes of project meetings and are covered in regular progress reports to the consortium and to the funding agency. The transparency in reporting ensures that all parties (including the European Commission project officers and national authorities) are aware of how the risks are being mitigated. This also provides an audit trail of risk decisions and accommodations made over time, which is useful for accountability as well as learning in the post-project time.

8. Continuous improvement: The risk management strategy will be developed during the course of the project. Lessons from any accidents or near-misses are cycled back into the system – e.g., if a mitigation works, then the framework is refreshed in response. By embedding a culture of risk awareness and learning within the team, the Centre can remain adaptable to emerging challenges over time. This adaptive management triggers resilience: not only does the Centre respond to immediate threats, but it also becomes increasingly prepared for emerging uncertainties.

Via risk identification, pre-emptive mitigation, and systematic monitoring, MkSafeNet is laying the cornerstone for the enduring sustainability of the Safer Internet Centre. This comprehensive Risk Management and Mitigation plan allows the Safer Internet Centre to overcome difficulties – whether technical setbacks, funding problems, operational problems, or external changes – and continue to ensure a secure online environment for children and young people in North Macedonia for years to come.

Risk assessment methodology with other supporting documentation is provided as Annexx to this Sustainability Plan.

Impact sustainability – Consortia involvement (CKM , MDT)

Identify partnerships benefits, institutional sustainability, networking and resources development

Define the process for collecting input from the private sector and other relevant stakeholders.

The Safer Internet Centre's sustainability plan is grounded in collaborative action, institutional resilience, and inclusive engagement. By fostering strategic partnerships, investing in capacity, and maintaining a strong feedback loop with the public and private sector and other stakeholders, SIC is well-positioned to deliver long-term impact and lead national efforts in digital safety and wellbeing.

SIC's sustainability should be built on the following core strategies:

Capacity Building: Investing in staff development, digital literacy training, and knowledge management to retain institutional expertise.

Integrated Governance: Embedding digital safety objectives into the strategic and operational frameworks of participating institutions.

Financial Resilience: Diversifying funding streams—including government grants, EU funding mechanisms, private sponsorships, and public campaigns—to ensure financial stability.

Compliance and Alignment: Ensuring ongoing alignment with national child protection policies, EU regulations, and global digital safety frameworks.

9. ANNEX 2- Roadmap to perform Cost-benefit analysis for project's financial viability

In theory and practice, cost-benefit analysis is most often used to assess the advantages and disadvantages of projects, that is, to assess their economic efficiency. In other words, cost-benefit analysis involves clearly identifying and quantifying all potential costs and benefits associated with a project. This analysis covers direct and indirect social effects, as well as other broader external effects such as: the project's contribution for increased employment, the effects on the growth of the population's well-being, energy efficiency, ecology, internet safety and similar issues. This allows decisions makers to see what difference the project would make to the community.

This Annex serves as a check point on how to determine and estimate a 5-year spending plan for SIC operational functioning. From a technical point of view, the main problems that arise when using cost-benefit analysis for a new project are:

1) Determination of the project costs such as: project implementation costs and operational costs, and

2) Determination of the project benefits that can be: tangible benefits (direct and measurable), intangible benefits (indirect and immeasurable).

Cost-benefit elements for project analysis	
Costs	**Benefits**
Project implementation costs -project platform development, -integration with other systems, -capital equipment costs **Operational costs** -personnel costs (salaries for key personnel), -platform and software licensing, -costs regarding future upgrades, integrations, or customizations of the platform, -hosting and infrastructure, -infrastructure and physical security,	**Tangible benefits (direct and measurable)** -energy savings, -time savings, -decreased staff number **Intangible benefits (indirect and immeasurable)** -more satisfies users (improved accessibility and user experience), -better data security, consistency and efficient information retrieval, -dedicated Customer Relationship Management (CRM) system, -better cross-device accessibility, -advanced data protection tools, encryption and secure access,

-training and development, -cybersecurity and data protection, -general administrative expenses (utilities, office supplies, communication costs (phone, internet), and other overheads), -contingency and incident response, -hidden costs (unexpected expenses such as licensing, storage overage, cybersecurity tools, GDPR compliance tools, or future staff training), -unforeseen costs (if the platform transitions to a paid model or if premium integrations become necessary).	-development of structured procedures for data backup, disaster recovery, and continuity planning to mitigate the risks of data loss or service disruption in case of technical failures or cyber incidents.

Having in mind that intangible benefits (unlike costs) are difficult to quantify, a specific cost analysis of the project is given in the table below.

1. Project Overview

Objective: To establish and operate a Safer Internet Centre, to promote digital safety, to operate a national helpline, to provide awareness campaigns, educational programs, and combat online risks to children and youth.

Time Horizon: 5 years, **Currency:** EUR (€)

2. Table: Estimated Costs

Cost Category	**Annual Cost (EUR)**	**5-Year Cost (EUR)**	**Notes**
Personnel	€90,000	€450,000	~4–5 full-time staff including project manager, helpline operators, trainers
Office & Operations	€20,000	€100,000	Rent, utilities, internet, admin

Helpline Infrastructure	€15,000	€75,000	Technology, call systems, software, hosting
Awareness Campaigns & Materials	€30,000	€150,000	Online/offline campaigns, printing, school visits
Training & Workshops	€20,000	€100,000	Annual training programs for teachers, parents, youth
IT Development (website, tools, app)	€25,000	€25,000	One-time investment (maintenance included in ops)
Monitoring & Evaluation	€5,000	€25,000	Surveys, impact reports
Contingency (10%)	€20,500	€102,500	For unexpected costs
Total	**€225,500**	**€1,027,500**	Over 5 years

MKSafeNet

Project implemented by the Ministry of Digital Transformation (MDT) in collaboration with project partners and the Consortium.