CO-SECUR BOOKLET

D3.1 Societal Development Plan: Guidelines for advancing Social Innovation in Urban Security



Funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them. Grant Agreement no. 101121325

Document details

Deliverable D.3.2
"D3.1 Societal Development Plan: Guidelines for advancing Social Innovation in Urban Security"

Legal disclaimer
- Call: HORIZON-CL3-2022-SSRI-01 (Strengthened Security Research and Innovation 2022)
- Topic: HORIZON-CL3-2022-SSRI-01-04
- Type of Action: HORIZON-RIA

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

Authors
Noemí Garcia, Rebeca Lucas, Maite Ferrando, Meike Hecker, Anna Rau, Francisco Rodenas, Estrella Durá, Jordi Garcés, Maria Mekri, M., Carina Dantas, Harm op den Akker, Paola Bello, Andrea Marinho, Natalia Machado, Lucia Cristea, Denisa Andrei, Marga Marin, Beata Dec, Aleksandra Kamińska, Michal Woch, Konstantinos Nikolaidis-Konstas, Andrius Jaržemskis, Ieva Girdvainienė, Emilija Venskūnaitė, Dorina Stamou, Alper Tanriverdi. (2026).

How to cite this deliverable
Garcia, N, Lucas, R, Ferrando, M., Hecker, M., Rau, A., Rodenas, F., Durá, E., Garcés, J., Mekri, M., Dantas, C., op den Akker, H., Bello, P., Machado, N., Marinho, A., Cristea, L., Andrei, L., Marin, M., Dec, B., Kamińska, A., Woch, M., Nikolaidis-Konstas, D., Jaržemskis, A., Girdvainienė, I., Venskūnaitė E., Stamou D., Tanriverdi, A. (2026). Societal Development Plan: Guidelines for advancing Social Innovation in Urban Security. Available in CO-SECUR website at: https://cosecur.eu/resources/

Project consortium
The CO-SECUR consortium, led by Kveloce, brings together 10 multidisciplinary partners with expertise in participatory research, public engagement, and mixed methods. The selection of partners from 9 European countries - Spain, BelgiRum, Finland, Germany, Portugal, Romania, Poland, Greece, and Lithuania reflects the project's goal to address the complex diversity of laws, security measures, politics, and social realities of different European regions.

Kveloce - SENIOR EUROPA SOCIEDAD LIMITADA | UVEG - UNIVERSITAT DE VALENCIA | SG SAFERGLOBE RY | DEFUS: DEUTSCH-EUROPAISCHES FORUM FUR URBANE SICHERHEIT e.V | SHINE 2EUROPE LDA | EIP - EUROPEAN INTEGRATED PROJECT | EVALU sp. Zo.o. | TERO MONOPROSOPI IKE | SMART CONTINENT LT UAB | DIGITALEUROPE AISBL

Copyright © 2026 by CO-SECUR.
This deliverable is licensed under the Creative Commons Attribution 4.0 International licence (CC BY 4.0).

Table of Contents

Executive Summary 08

1. Introduction 09

1.1 Background

1.2 The CO-SECUR Project and the Societal Development Plan

1.3 Key definitions

Mechanisms of action

Safety

Security

Social Innovation in Security (SIS)

Stakeholders (in Social Innovation in Security)

Responsible Research and Innovation (RRI)

1.4 Objectives of the document

1.5 Scope and target audience

1.6 Structure of the document

1.7 Methodological approach

1.8 The stakeholder ecosystem in Social Innovation in Security

2. Challenges and enabling conditions for the adoption of Social Innovation in Security 21

2.1 Challenges for the adoption of Social Innovation in Security

2.1.1 Institutional challenge

2.1.2 Social and governance challenges

2.1.3 Capacity and knowledge gaps

2.1.4 Emerging risks and threats

2.2 Opportunities and enabling factors for the adoption of Social Innovation in Security

3. Strategic guidelines for supporting Social Innovation in Security 26

3.1 Participatory governance

Guideline 1. Institutionalise citizen participation

Guideline 2. Ensure inclusive and representative engagement

Guideline 3. Integrate mediation and trust-building mechanisms

3.2 Cross-sector Collaboration

Guideline 4. Establish formal coordination frameworks

Guideline 5. Create permanent coordination structures

Guideline 6. Strengthen multi-actor ecosystems

3.3 Communication and Awareness

Guideline 7. Develop proactive communication strategies

Guideline 8. Ensure inclusive and accessible communication

Guideline 9. Counter misinformation and harmful narratives

3.4 Environmental and Urban Design

Guideline 10. Integrate security into urban planning

Guideline 11. Adopt user-centred and inclusive design

3.5 Technological Integration

Guideline 12. Use technology as an enabling tool

Guideline 13. Ensure ethical and transparent use of technology

Guideline 14. Promote interoperable and data-driven systems

4. Roadmap for implementing Social Innovation in Urban Security 45

4.1 Analysis and diagnosis phase

Milestone 1: Analysing the local context

Milestone 2: Building partnerships and a shared vision for SIS

Milestone 3: Co-designing the SIS solution

4.2 Implementation phase

Milestone 4: Implementing SIS Actions

4.3 Evaluation and Transfer phases

Milestone 5: Monitoring and Evaluating

Milestone 6: Replicability, scalability and sustainability

5. Conclusions 64

6. References 66

Annexes 68

Annex I. Methodological approach

Annex II. Stakeholder roles across the guidelines and the roadmap

Principles for engaging stakeholders

Annex III. List of contributors

List of Tables

Table 1 19

Stakeholder groups in Social Innovation in Security

Table 2 25

Summary of key challenges and enabling conditions for SIS adoption

Table 3 27

Summary of strategic guidelines for Social Innovation in Security

Table 4 70

D3.1 Societal Development Plan Methodology

Table 5 72

Indicative roles of stakeholder groups in the six milestones of the roadmap

Table 6 73

Indicative lead and support roles by strategic guideline

List of abbreviations

This glossary provides a list of key terms that are used thereinafter and their definitions for the purposes of this document. It is not meant to provide an exhaustive list of all the terms related to the subject of this study.

Term	Definition
AI	Artificial Intelligence
CAME	**C**orrect, **A**dapt, **M**aintain, **E**xploit
CPTED	Crime Prevention Through Environmental Design
CSO	Civil Society Organization
IoT	Internet of Things
PE	Participatory Event / Participatory Events
NGOs	Non-Governmental Organisations
SDP	Societal Development Plan
SIS	Social Innovation in Security
RRI	Responsible Research and Innovation
SWOT	**S**trengths, **W**eaknesses, **O**pportunities and **T**hreats

Executive Summary

Urban security in Europe is shaped by more than crime and enforcement. Crowded public spaces, large events, nightlife, public transport, gender-based violence, inequalities and declining trust in institutions all influence how safe people are and how safe they feel. Approaches based only on surveillance, enforcement or technology are sometimes necessary, but they are rarely enough to address these social and governance dimensions.

Social Innovation in Security (SIS) offers a complementary approach. It places citizens and communities at the centre of security innovation, working alongside public authorities, law enforcement, civil society, researchers, private and media sectors to understand local problems and co-create solutions that are effective, legitimate and sustainable.

This Societal Development Plan, developed within the CO-SECUR project, translates the project's evidence into practical guidance for policymakers and practitioners. It draws on a literature review, a mapping of SIS initiatives across Europe, selected case studies and SWOT and CAME analyses carried out with stakeholders in nine countries (more information on the methodology can be found in Annex I). The document is organised around three elements:

- **Challenges and enabling conditions**. Fragmented governance, short-term funding, limited trust and capacity gaps are the main barriers to SIS adoption. European policy support, growing local innovation capacity and the exchange of good practices are the main enablers.

- **Strategic guidelines**. Fourteen guidelines, grouped under five mechanisms of action (participatory governance, cross-sector collaboration, communication and awareness, environmental and urban design, and technological integration), set out where and how to act. Case studies illustrate their application in real contexts.

- **Implementation roadmap**. Six milestones guide local actors from analysing the local context to building partnerships, co-designing and implementing actions, monitoring and evaluating results, and ensuring replicability, scalability and sustainability. The roadmap is iterative and adaptable to different governance structures and levels of capacity.

The Plan is grounded in Responsible Research and Innovation (RRI) principles, ensuring that security solutions respect fundamental rights, privacy, inclusion and transparency.

The central message is that SIS should be considered an integral component of security policy rather than an optional complement. Its success depends on political commitment, coordination between institutions, adequate resources, capacity-building and continuous learning. The Plan is intended as a practical entry point for local and regional authorities, policymakers, law enforcement, civil society, planners and researchers who wish to strengthen more inclusive, participatory and responsible approaches to urban security.

01
Introduction

CO-SECUR

Funded by
the European Union



1.1 Background

Urban security in Europe is increasingly shaped by complex and interconnected challenges. Changes in patterns of urbanisation, social fragmentation, inequalities, evolving security threats, misinformation, and declining trust in institutions can all influence both actual security conditions and how security is perceived by citizens. These challenges are particularly relevant in public spaces and other environments where different population groups, institutions and activities interact, including neighbourhoods, public transport systems, nightlife areas and large events.

Addressing these challenges requires approaches that can recognise the complexity of local contexts and respond to both objective security risks and citizens' experiences and perceptions. Traditional approaches based primarily on top-down decision-making, enforcement or technological solutions may be necessary in specific circumstances, but they are not always sufficient to address the social and governance dimensions of security. In particular, they may not adequately address issues such as institutional trust, social cohesion, inclusion, perceived safety or the different ways in which security challenges are experienced by diverse population groups.

In this context, Social Innovation in Security (SIS) provides a complementary approach that places societal needs, participation and collaboration at the centre of security innovation. Within CO-SECUR, SIS refers to practices and processes involving social, economic, technological, governance and/or policy innovation that aim to improve people's security, including security perception and behaviour. SIS approaches are characterised by the active involvement of citizens and other stakeholders in identifying challenges and co-creating solutions, as well as by their potential for adaptation, transfer and scaling across different contexts.

Responsible Research and Innovation (RRI) provides an important complementary dimension to this approach. Security-related innovations can have significant implications for privacy, equality, fundamental rights and public trust. Integrating RRI principles therefore helps ensure that security solutions are not only effective, but also ethically grounded, transparent, inclusive and responsive to societal needs. In practice, this means considering societal and ethical implications throughout the innovation process rather than addressing them only after a solution has been developed.

The adoption of SIS, however, cannot be based on a single model or intervention. Security challenges, institutional arrangements, available resources, community characteristics and levels of trust vary considerably between cities and regions. A solution that is effective in one context may therefore require significant adaptation before it can be transferred elsewhere. This makes context-sensitive diagnosis, stakeholder engagement, collaborative design, continuous learning and institutional capacity essential conditions for successful SIS implementation.

1.2 The CO-SECUR Project and the Societal Development Plan

The present report has been developed in the framework of the CO-SECUR Project, a Horizon Europe research and innovation project aimed at supporting the adoption of Social Innovation in Security (SIS) in urban contexts.

It brings together a multidisciplinary team of public authorities, research organisations, and innovation actors to promote more inclusive, participatory, and responsible approaches to security.

The project involves partners from Spain, Belgium, Portugal, Greece, Poland, Lithuania, Finland, Romania, and Germany, reflecting a diversity of institutional and socio-economic contexts and enabling the transfer of practices across Europe.

CO-SECUR focuses on key areas where social innovation can enhance security, including mass events and large gatherings, nightlife and urban coexistence, public transport safety, prevention of gender-based violence, and community safety in neighbourhoods. Across these domains, the project explores how governance, citizen engagement, mediation, communication, urban design, and technology can be combined to improve both security outcomes and its perception.

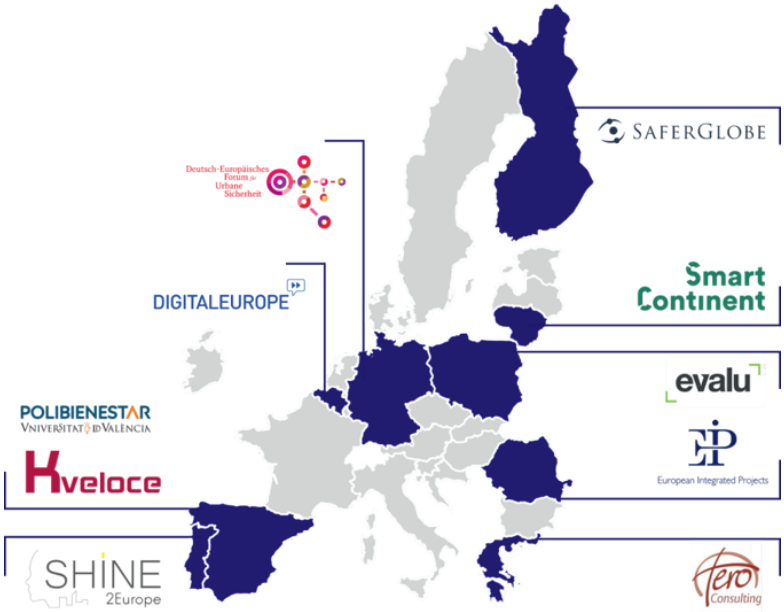

Figure 1. **CO-SECUR international partnership**

The Societal Development Plan (SDP) is one of the project's key outputs. It brings together the knowledge, evidence and practical experience developed throughout CO-SECUR and translates these into a structured framework to support the adoption and implementation of SIS approaches.

The SDP is designed to bridge the gap between understanding the challenges faced by local communities and translating this understanding into practical action. It brings together three complementary elements:

- **Challenges and enabling conditions**, which describe the contextual factors that may constrain or facilitate the adoption of SIS;
- **Strategic Guidelines**, which translate these insights into principles and areas for action; and
- **An implementation roadmap**, which provides practical guidance on how and when these principles can be put into practice.

The framework is complemented by **tools and methods** that can support implementation and by **case studies** that illustrate how SIS approaches have been applied in different contexts. These elements are intended to support learning and adaptation rather than prescribe a single way of implementing SIS.

1.3 Key definitions

Mechanisms of action

Evidence-based mechanisms of action refer to identifiable causal processes within an intervention that explain how and why that intervention produces its desired effects on a given population or context. According to Peters et al. (2020), these mechanisms allow for the construction of logical models that articulate the components of an intervention with its expected outcomes, facilitating its evaluation, adaptation, and transfer. Drawing from the CO-SECUR literature review, the following five mechanisms of action were identified in Social Innovation for Security (SIS):

- **Participatory Governance**: deliberative processes and co-creation (e.g. participatory budgeting, community mediation).
- **Technological Integration**: IoT, AI and digital twins to improve situational awareness.
- **Communication and Awareness**: prevention campaigns and safety training.
- **Environmental and Urban Design**: inclusive redesign of public spaces applying Crime Prevention Through Environmental Design (CPTED).
- **Cross-Sector Collaboration**: partnerships between the public, private and civil society sectors (e.g. Urban Labs).

Safety

Safety focuses on protection against accidental or unintentional risks, such as natural disasters, workplace accidents, structural failures or health problems. This term refers to conditions of well-being and prevention of harm in everyday situations, so its focus usually includes regulatory measures, emergency protocols and safety standards in infrastructure and products.

Security

Security has been defined as 'the condition of being protected from or not exposed to danger; […] a feeling of safety or freedom from or absence of danger'. It is a basic right for citizens that must be protected. Security is the cornerstone of a stable and prosperous society. Good internal security means that the population can enjoy the rights and freedoms guaranteed by the legal system without fear or insecurity caused by crime, disorder, accidents and national or international phenomena.

Social Innovation in Security (SIS)

Social Innovation in Security (SIS) refers to the practices and processes that involve social, economic, technological, governance and/or policy innovations based on human needs with the aim of improving people's security (including security perception and behaviour). These solutions must be innovative, transferable, and scalable, and must be co-created through participatory processes and from a multidisciplinary perspective.

For example, instead of responding to safety concerns in a public park solely by increasing surveillance or police presence, a SIS approach would involve local residents, youth groups, municipal authorities, urban planners and community organisations in jointly identifying the causes of insecurity and co-designing a combination of solutions. These might include redesigning public spaces, improving lighting, organising community activities and introducing appropriate technological tools where needed.

As such, it emphasises:

- Active citizen engagement in identifying problems and co-designing solutions
- Collaboration across public authorities, civil society, and private actors
- Attention to vulnerable groups and diverse perceptions of safety
- The integration of social, spatial, and technological dimensions

By supporting these elements, SIS contributes to more legitimate, effective, and sustainable security outcomes, particularly in complex urban environments.

Stakeholders (in Social Innovation in Security)

Stakeholders are the individuals, groups and organisations that influence, implement, are affected by, or contribute to security-related challenges and solutions. In Social Innovation in Security (SIS), stakeholders typically include citizens, public authorities, law enforcement agencies, civil society organisations, community groups, researchers, private sector actors and media. A defining characteristic of SIS is the active involvement of citizens as partners in identifying challenges and co-designing solutions, supported by collaboration across sectors and governance levels to achieve more legitimate, effective and sustainable security outcomes. Detailed information on stakeholders and their role in SIS can be found in Annex II.

Responsible Research and Innovation (RRI)

Responsible Research and Innovation (RRI) provides a framework to ensure that research and innovation processes are aligned with societal values, needs, and expectations. In the context of security, RRI is essential to address ethical concerns, protect fundamental rights, and ensure public trust.

The application of RRI to SIS involves several key dimensions:

- **Inclusiveness and engagement**: involving citizens and stakeholders throughout the innovation process.
- **Ethics and fundamental rights**: ensuring that solutions respect privacy, non-discrimination, and human dignity.
- **Transparency and openness**: making processes and decisions understandable and accessible, including open data practices where appropriate and shared learning environments.
- **Responsiveness and adaptability**: adjusting interventions based on feedback and evolving contexts.
-

Integrating RRI principles into SIS ensures that security innovations are not only effective, but also socially acceptable and democratically grounded.

1.4 Objectives of the document

The main objective of the Societal Development Plan (SDP) is to provide practical and strategic guidance to support the adoption of Social Innovation and Responsible Research and Innovation principles in the field of urban security.

More specifically, the SDP aims to:

- translate research findings and project outcomes into actionable guidance for policymakers and practitioners;
- identify key mechanisms that can enable effective Social Innovation in Security;
- provide strategic guidelines to support the design, implementation and longer-term development of SIS initiatives;
- offer a practical roadmap for local authorities and stakeholders to put these approaches into practice;
- provide examples, tools and methods that can support implementation and learning; and
- facilitate the adaptation, transfer and scaling of relevant SIS approaches across different contexts.

The SDP is therefore intended not only to present the findings of CO-SECUR, but also to provide a practical entry point for actors wishing to explore or strengthen SIS approaches in their own context.

1.5 Scope and target audience

This document is primarily addressed to:

- Local and regional authorities responsible for urban security
- Policymakers at national and European levels
- Law enforcement agencies and security practitioners
- Civil society organisations and community groups
- Urban planners, researchers, and innovation actors

The guidelines and roadmap presented in this document are designed to be adaptable to different territorial contexts, governance structures, and levels of institutional capacity. While the focus is on urban environments, many of the principles and approaches are also relevant to peri-urban and rural settings.

1.6 Structure of the document

Following the logic of the SDP framework presented above, the remainder of the document moves from understanding the context to translating insights into strategic guidance and practical implementation.

Section 2 – Challenges and Enabling Conditions for the Adoption of SIS presents the main challenges and enabling conditions identified through the CO-SECUR analysis and stakeholder engagement activities. It provides the contextual basis for the Strategic Guidelines.

Section 3 – Strategic Guidelines for Supporting Social Innovation in Security presents the 14 Strategic Guidelines, organised around the five mechanisms of action identified within CO-SECUR: participatory governance, cross-sector collaboration, communication and awareness, environmental and urban design, and technological integration.

Section 4 – Roadmap for Implementing Social Innovation in Security translates the Strategic Guidelines into six implementation milestones, covering the journey from understanding the local context to building partnerships, co-designing and implementing SIS actions, monitoring and evaluation, and ultimately replication, scaling and sustainability.

Section 5 – Conclusions summarise the main insights of the SDP and highlights the conditions required for the effective and sustainable adoption of SIS.

The **Annexes** present the methodological approach, stakeholder roles and the list of contributors of this document.

Together, these sections provide a pathway from **understanding the local context, through strategic action, to learning and longer-term sustainability**.

The figure below illustrates how these elements are connected and how they can support practitioners in moving from understanding local challenges to implementing, evaluating and sustaining Social Innovation in Security initiatives.

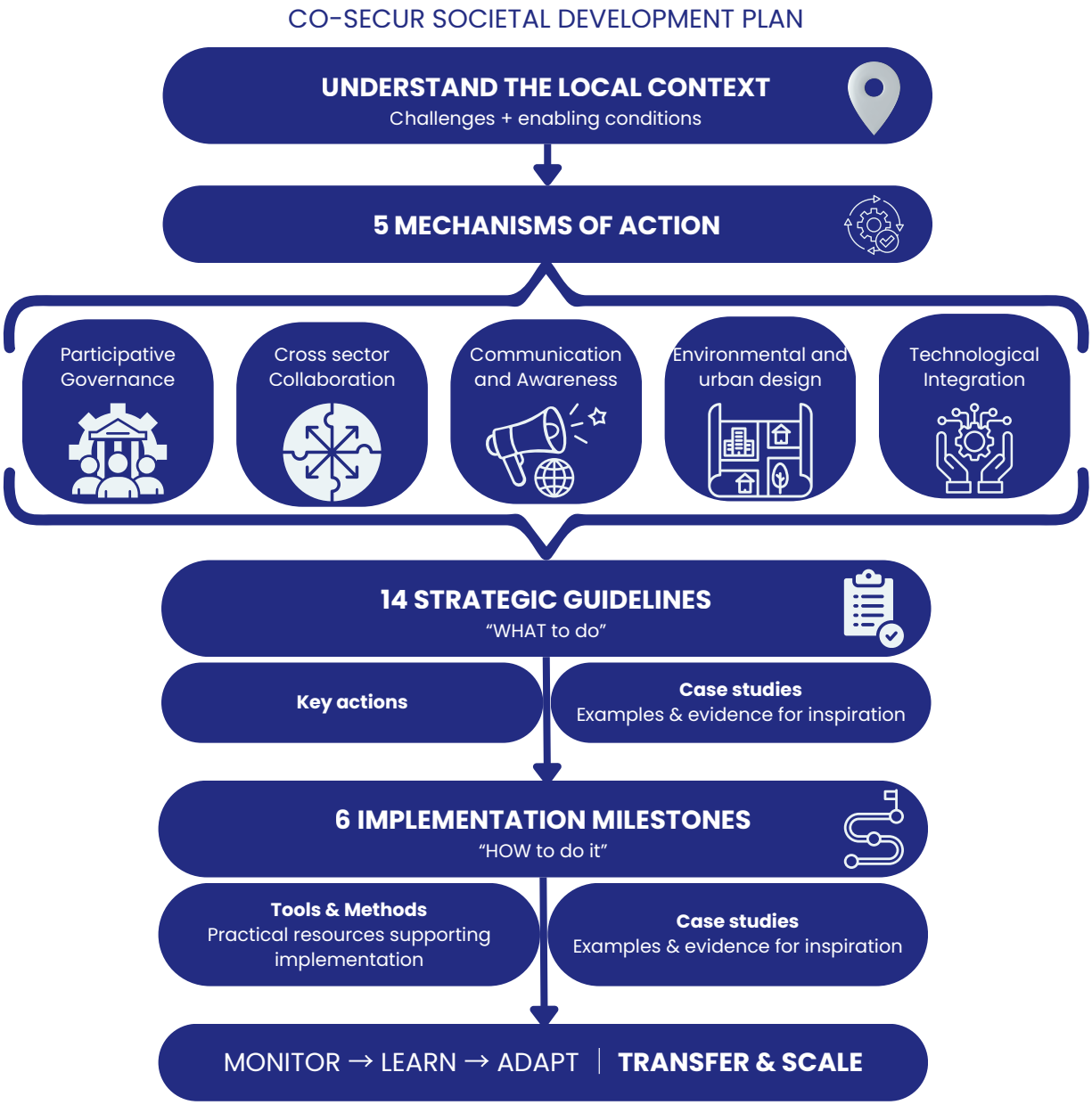

Figure 2. **CO-SECUR Societal Development Plan – Framework**

1.7 Methodological approach

This report has been developed through an iterative process combining evidence review, qualitative interviews, practical experience from Social Innovation in Security (SIS) initiatives across Europe, and consultation with researchers and practitioners.

The development process included four complementary stages:

- **Review of evidence**, drawing on academic literature, policy documents and previous CO-SECUR research.
- **Analysis of SIS case studies**, identifying common practices, implementation factors and recurring challenges.
- **Co-creation and expert consultation**, involving project partners and external stakeholders to validate findings and identify practical recommendations.
- **Development of the Societal Development Plan**, translating evidence into actionable guidance for policymakers and practitioners.

More details on the methodology followed can be found in Annex I.

This document is complemented by a suite of tools specifically targeted to different stakeholders: policy makers, civil society, private sector, researchers and media sector, available on the COSECUR project website: https://cosecur.eu/resources/.

1.8 The stakeholder ecosystem in Social Innovation in Security

Social Innovation in Security (SIS) depends on the participation of many different actors. No single institution holds all the knowledge, legitimacy, resources and competences needed to address urban security challenges, particularly those related to perceptions of safety, trust and social cohesion.

The groups presented here are functional categories rather than a fixed list of organisations. Their composition varies between cities and regions, one organisation may play different roles at different stages of an initiative, and some groups, such as citizens or informal community groups, may not be formally organised. Identifying who is who in each local context is the purpose of the stakeholder mapping proposed in Milestone 1. A detailed map of the institutional landscape is provided in Annex II.

The next table describes the ten stakeholder groups used in this document, the role they typically play in SIS, what they can contribute and the main considerations when engaging them.

Table 1. **Stakeholder groups in Social Innovation in Security**

Stakeholder group	Role in SIS	What they contribute	Engagement considerations
1. Local and regional authorities *Municipalities, regional governments, city councils, local security boards and municipal departments in charge of security, public space or social policy.*	Natural convener and, in most cases, lead of SIS initiatives; hold competences over public space, local coordination of security and services.	Political mandate and legitimacy, budget, local data, capacity to embed participation in formal policy and planning cycles.	Fragmented responsibilities across departments and levels; exposure to political cycles and short-term funding; limited SIS expertise (Section 2.1).
2. National and European public authorities *Ministries, national legislatures and courts, national crime-prevention and security bodies, EU institutions and programmes.*	Set the legal, policy and funding framework within which local SIS operates.	Legislation, national strategies and standards, funding, and pathways to scale and mainstream successful practices.	Distance from local realities; priorities may shift towards reactive measures. Best engaged through policy dialogue and evidence.
3. Law enforcement, civil protection and emergency services *Police (national, regional, local), civil protection, fire and rescue, emergency medical services.*	Provide operational security and emergency response; co-designers of preventive and community-based approaches.	Operational knowledge, incident data, experience in crowd and event management, rapid response capacity.	Enforcement-oriented culture; trust gaps with some communities; data-sharing constraints. Joint training and mediation help.
4. Public service providers *Urban planning, mobility and public transport, social, health, education, housing and youth services.*	Address root causes of insecurity and shape the spaces and services where security is experienced.	Planning and design expertise, knowledge of vulnerable groups, everyday contact with residents.	Security is rarely part of their core remit; require cross-department coordination and clear incentives.
5. Citizens and community groups *Residents, neighbourhood associations, youth and women's groups, representatives of vulnerable or underrepresented groups (e.g. migrants, LGBTQ+ people, people with disabilities, older people), users of nightlife and event spaces.*	Partners in identifying problems and co-designing solutions, and the main beneficiaries of SIS.	Lived experience, perceptions of safety, local knowledge, legitimacy, volunteering and community networks.	Participation often dominated by a few groups; low trust and hard-to-reach populations. Need accessible formats, feedback and resources to avoid symbolic participation.
6. Civil society organisations *NGOs, foundations, community mediators, victim-support and advocacy organisations, social enterprises.*	Bridge between institutions and communities; deliver mediation, outreach, awareness and support services.	Community trust, facilitation and mediation skills, access to vulnerable groups, independent oversight.	Frequent reliance on short-term funding; risk of instrumentalisation. Need recognised roles and stable resources.

Stakeholder group	Role in SIS	What they contribute	Engagement considerations
7. Research and academia *Universities, research centres, think tanks, independent evaluation teams.*	Provide evidence, methods and independent assessment.	Diagnosis and data analysis, monitoring and evaluation frameworks, ethical (RRI) review, capacity building.	Different time horizons from practice; findings must be translated into actionable form; independence should be preserved.
8. Private sector *Private security providers, technology and IT companies, transport and mobility operators, event organisers, hospitality and nightlife businesses.*	Co-producers of security in the spaces they operate; providers of technological solutions.	Technology, operational resources, access to spaces and users, potential co-financing.	Commercial and public interests must be aligned; transparency, data protection and ethical use of technology are essential (Guideline 13).
9. Media and digital platforms *Local and national media, social media platforms, community communicators*.	Shape public perception of security and the visibility of SIS initiatives.	Reach, awareness-raising, and a role in countering misinformation.	Sensationalism and misinformation can erode trust. Engage through proactive and transparent communication (Guidelines 7–9).
10. Funders, investors and networks *EU and national funding programmes, foundations, investors, networks of municipalities, professional and peer-learning networks.*	Enable and sustain SIS initiatives and support transfer and scaling.	Funding, visibility, peer learning and replication channels.	Project-based funding undermines sustainability; funding cycles need to align with long-term institutional anchoring.

The Annex II details the role of each stakeholder for each guideline and roadmap step, as well as some general principles to apply in their engagement.

02
Challenges and enabling conditions for the adoption of Social Innovation in Security

CO-SECUR

Funded by
the European Union

The adoption of Social Innovation in Security (SIS) across European contexts is shaped by a combination of structural, institutional, social, and technological factors. While SIS offers significant potential to enhance the effectiveness, and legitimacy of security approaches, its implementation remains uneven and often constrained by systemic barriers.

This section presents a synthesis of the main challenges, opportunities, and enabling conditions for SIS adoption, based on a SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis conducted with stakeholders and project partners in the nine CO-SECUR countries. The objective is to provide a structured understanding of the context in which SIS operates, identifying both obstacles and leverage points for its successful implementation. The identified weaknesses and threats at the SWOT analysis are analysed as structural, social and emerging challenges (Section 2.1), while the strengths and opportunities are reflected as enabling conditions and favourable factors (Section 2.2).

2.1 Challenges for the adoption of Social Innovation in Security

2.1.1 Institutional challenges

One of the most significant barriers to the adoption of SIS lies in the fragmentation of governance structures. Security-related responsibilities are often distributed across multiple institutions and administrative levels, leading to coordination challenges, duplication of efforts, and inefficiencies.

In many cases, cooperation between actors depends on informal relationships rather than stable and formalised frameworks, reducing continuity and scalability.
In addition, the adoption of SIS is frequently constrained by short-term project-based funding models. Many initiatives rely heavily on temporary funding streams, particularly from European programmes, which can undermine long-term sustainability and institutional anchoring.

2.1.2 Social and governance challenges

The implementation of SIS requires strong engagement from citizens and communities. However, several barriers affect the depth and quality of participation.

In many contexts, participatory processes remain limited or symbolic, with low levels of genuine co-creation. Engagement is often dominated by specific groups, raising concerns about representativeness and inclusiveness. Reaching vulnerable or marginalised populations remains particularly challenging, especially in contexts characterised by low trust in institutions.

Trust itself emerges as a critical factor. In environments where confidence in public authorities is weak, it becomes more difficult to mobilise citizens, implement innovative approaches, and ensure acceptance of new measures.

Furthermore, sustaining engagement over time is resource-intensive, requiring continuous effort, coordination, and adaptation.

2.1.3 Capacity and knowledge gaps

The effective implementation of SIS depends on the availability of appropriate skills, knowledge, and institutional capacity. However, gaps persist in several areas.

There is often limited expertise in social innovation approaches within security-related institutions, which traditionally prioritised technical or enforcement-based solutions. At the same time, the rapid development of technological tools can outpace the capacity of organisations to adopt and integrate them effectively.

In addition, insufficient data, indicators, and evaluation frameworks make it difficult to assess the impact of SIS initiatives. This is particularly challenging in the field of security, where success is often defined by the absence of negative events or by subjective perceptions of safety.

In many cases, the implementation of security measures is not preceded by a sufficiently thorough analysis of the underlying problem. As a result, interventions may rely on generic or standardised solutions that are not adequately tailored to the specific local context, user needs, or root causes of insecurity. Strengthening diagnostic capacity, evidence-based planning, and context-sensitive design is therefore essential.

These limitations hinder learning, scaling, and the broader institutionalisation of successful practices.

2.1.4 Emerging risks and threats

The adoption of SIS also takes place in a context characterised by evolving and sometimes destabilising external pressures.

Rapidly changing security landscapes, including hybrid threats, geopolitical instability, and new forms of social tension, can shift political priorities towards more immediate and reactive measures, potentially sidelining longer-term innovation approaches.

At the same time, misinformation and polarisation can undermine trust in institutions and complicate communication efforts, affecting both the perception and effectiveness of security interventions.

There is also a risk that social innovation in security is perceived as secondary or complementary, rather than as an integral component of security policy. This perception can limit political support and resource allocation.

Persistent inequalities and territorial disparities—particularly between urban and rural areas—may also result in uneven access to and benefits from SIS initiatives.

2.2 Opportunities and enabling factors for the adoption of Social Innovation in Security

Despite these challenges, several factors create favourable conditions for the adoption and scaling of SIS.

At the European level, policy frameworks and funding programmes provide strong support for innovation, collaboration, and societal engagement. These instruments can act as catalysts for experimentation and knowledge exchange across contexts. For example, the Horizon Europe programme has supported collaborative initiatives that bring together municipalities, researchers, civil society organisations and security practitioners to co-develop and test innovative security solutions.

At the local level, municipalities are increasingly developing innovation capacities, including urban labs, digital transformation units, and participatory platforms. These structures provide fertile ground for testing and implementing SIS approaches.

Moreover, urban regeneration processes, placemaking initiatives, and renewed citizen ownership of public spaces can provide strong entry points for SIS. For example, in the "Brussels by night" initiative, one of the cases analysed by the project, local residents co-designed interventions to transform poorly perceived pedestrian tunnels through artistic installations, improved lighting, vegetation and temporary community activities. By reclaiming these neglected spaces for social interaction, the initiative contributed to enhancing both the perceived and actual sense of security.

Equally, digitalisation also offers new opportunities to enhance communication, data analysis, and coordination, provided that it is implemented in a responsible and inclusive manner. For example, participatory digital platforms and mobile applications can enable residents to report local safety concerns, contribute ideas for neighbourhood improvements, or participate in consultations regardless of time or location.

Finally, there is growing recognition of the value of learning from international experiences. The exchange and adaptation of good practices across cities and countries can accelerate the diffusion of effective approaches. The CO-SECUR project itself contributes to this process by documenting and sharing Social Innovation in Security case studies from across Europe, enabling cities and practitioners to adapt successful approaches to their own local contexts.

Table 2. **Summary of key challenges and enabling conditions for SIS adoption**

Dimension	Category	Key Elements
Challenges	**Institutional challenges**	• Fragmented responsibilities across institutions • Limited continuity of initiatives • Dependence on short-term/project-based funding
	Social and governance challenges	• Low citizen trust in institutions • Difficulties engaging vulnerable groups • Challenges in sustaining long-term engagement
	Capacity and knowledge gaps	• Limited expertise in social innovation approaches • Weak monitoring and evaluation systems • Lack of tailored problem diagnosis
	Emerging risks and threats	• Rapidly evolving security risks • Misinformation and polarisation • Unequal territorial access to innovation • Limited recognition of SIS as a strategic priority
Enabling Conditions	**Policy opportunities**	• EU policy frameworks and funding programmes supporting innovation, collaboration, and societal engagement
	Resources, skills and learning capacity	• Development of municipal innovation ecosystems (e.g. urban labs, digital units, participatory platforms) • Use of digital tools to improve communication, data analysis, and coordination
	Contextual and social enablers	• Urban regeneration processes and placemaking initiatives • Increasing citizen ownership and use of public spaces

The challenges, opportunities, and enabling conditions outlined in this section provide a comprehensive picture of the current landscape for SIS adoption. Building on this analysis, the following sections translate these insights into: strategic guidelines organised by mechanisms of action (Section 3) and a practical roadmap to support implementation at the local level (Section 4).

03

Strategic guidelines for supporting Social Innovation in Security

CO-SECUR

Funded by
the European Union

Building on the challenges and enabling conditions identified in Section 2, this chapter presents a set of strategic guidelines to support the adoption and implementation of Social Innovation in Security (SIS). These guidelines were extracted from the CAME and SWOT analysis elaborated through participatory events across the nine CO-SECUR countries.

The guidelines are structured according to five mechanisms of action identified in the project as key leverage points to enable and scale up SIS initiatives, namely: (i) participatory governance, (ii) cross sector collaboration, (iii) communication and awareness, (iv) environmental and urban design and (v) technological Integration. These five factors represent the core pathways through which SIS can be put in practice. They should be understood as interconnected components of a broader and holistic security ecosystem. For each one of them, a brief description is given (more information can be found in D2.3) and several concrete guidelines are outlined.

Selected case studies from the COSECUR SIS mapping are included to illustrate how these guidelines have been applied in practice across different contexts. The selected case studies reflect the diversity of thematic areas addressed in CO-SECUR (e.g. nightlife, mobility, vulnerable groups, and mass events).

An overview of the guidelines and their correspondent key mechanisms of action can be found in the table below.

Table 3. **Summary of strategic guidelines for Social Innovation in Security**

Key mechanisms of action	Guidelines
Participatory Governance	1. Institutionalise citizen participation
	2. Ensure inclusive and representative engagement
	3. Integrate mediation and trust-building mechanisms
Cross-sector Collaboration	4. Establish formal coordination frameworks
	5. Create permanent coordination structures
	6. Strengthen multi-actor ecosystems
Communication and Awareness	7. Develop proactive communication strategies
	8. Ensure inclusive and accessible communication
	9. Counter misinformation and harmful narratives
Environmental and Urban Design	10. Integrate safety into urban planning
	11. Adopt user-centred and inclusive design

Key mechanisms of action	Guidelines
Technological Integration	12. Use technology as an enabling tool
	13. Ensure ethical and transparent use of technology
	14. Promote interoperable and data-driven systems

3.1 Participatory governance

Participatory governance mechanisms enable the active involvement of citizens and stakeholders in decision-making processes related to security. These mechanisms move beyond consultation towards genuine co-creation, where participants contribute to problem definition, solution design, and evaluation.

Such approaches contribute to:

- Increased trust between institutions and communities
- More context-sensitive and accepted solutions
- Empowerment of local actors and communities

Guideline 1. Institutionalise citizen participation

Objective

To ensure stable, meaningful, and continuous citizen involvement in urban security policies by embedding participation within formal governance structures and regular decision-making processes.

Key Actions

- Establish formal and recurring co-creation platforms, such as participatory forums, citizen panels, neighbourhood assemblies, or urban living labs, where residents and stakeholders can regularly discuss security priorities and co-develop solutions.
- Integrate participatory processes into existing policy and planning cycles, ensuring that citizen input is considered at all relevant stages, including problem definition, priority-setting, implementation, and evaluation.
- Develop clear feedback and accountability mechanisms so that participants understand how their contributions have been used, what decisions have been taken, and what follow-up actions are planned.
- Ensure that participation mechanisms are adequately resourced, facilitated, and accessible in order to support sustained engagement over time.
- Promote transparency in governance processes by communicating objectives, timelines, responsibilities, and expected contributions in a clear and understandable manner.

Actors involved: Local authorities, citizens, civil society organisations.

Case Study: "Secure Neighbourhood"

Warsaw, Poland

Description: This initiative shifts urban security from a top-down administrative task to a co-produced social process. It functions through regular, multi-actor deliberative meetings that bring together residents, local leaders, the Municipal Guard, and the Police to discuss issues ranging from poor lighting to nuisance behaviour

Key elements:

- Civic Co-creation: Residents are empowered to co-decide on specific measures, such as the placement of surveillance cameras or the prioritization of patrol routes.
- Formal Coordination: The program is anchored within the Capital Safety Centre, which provides dedicated coordinators to ensure community proposals are turned into institutional actions

Impact: Increased institutional legitimacy and trust, leading to better reporting habits and a higher overall perception of safety

More information: https://cosecur.eu/case-study/the-safe-neighbourhood-project/

Guideline 2. Ensure inclusive and representative engagement

Objective

Improve inclusiveness and representativeness in participation processes. This guideline aims to ensure that engagement processes better reflect the diversity of local communities, addressing persistent gaps in inclusion and representativeness that limit the legitimacy and effectiveness of participatory approaches.

Key Actions

- Inclusive participation can be strengthened by working through trusted intermediaries such as NGOs and community organisations that already have strong links with underrepresented groups. Engagement formats should be adapted to the needs of different populations, including youth, women, migrants, and older people, ensuring that participation is meaningful rather than one-size-fits-all.
- At the same time, municipalities should actively reduce structural barriers to participation, particularly language and digital access constraints, by combining offline and accessible communication channels with simplified and multilingual materials.

Actors involved: Municipalities, NGOs, community organisations.

Case Study: "Steps for Future"

Bucharest, Prahova, Baia Mare, Vâlcea, and Arad, Romania

Description: This initiative was created to support more than one million people fleeing the war in Ukraine. It focuses on providing psychosocial support and life-skills training to help refugees integrate safely into their host communities.

Key elements:

- **Trauma-Informed Co-creation**: The program was built by listening to the specific fears and needs of refugee families rather than imposing a generic support model.
- **Vulnerability-Centred Outreach**: It specifically targets those often excluded from traditional security dialogues, such as displaced youth and mothers in high-stress environments.

Impact: Strengthened social cohesion and resilience among the refugee population, reducing their vulnerability to exploitation or secondary trauma.

More information: https://cosecur.eu/case-study/steps-for-future-life-skills-and-personal-development/

Guideline 3. Integrate mediation and trust-building mechanisms

Objective

Prevent conflicts and strengthen social cohesion through embedded mediation roles and structured dialogue processes within local governance systems, ensuring that conflict prevention becomes a continuous and institutionalised function rather than an ad hoc response. It directly responds to challenges related to low institutional trust and fragmented governance arrangements that limit coordinated responses to emerging social tensions.

Key Actions

- To put in practice this objective, community and intercultural mediation roles should be formally recognised within local governance structures, moving beyond informal or project-based arrangements. This includes defining clear mandates, competencies, and referral pathways so that mediators can act as trusted intermediaries between residents, public authorities, and service providers.
- In parallel, local authorities should establish early-warning and conflict resolution mechanisms that allow for the systematic identification of emerging tensions. These mechanisms should rely on continuous engagement with community actors, schools, neighbourhood organisations, and social services, enabling early intervention before conflicts escalate.
- These processes should be supported through coordinated work between local authorities, mediation professionals, and social services, ensuring that responses are not fragmented but instead integrated into a shared operational framework.

Actors involved: Local authorities, mediators, social services.

Case Study: "Forssa Community Dialogue"

Forssa, Finland.

Description: Following severe inter-ethnic conflicts between local youth and asylum seekers, the city implemented a community mediation model instead of relying solely on repressive police force.

Key elements:

- **Restorative Dialogue**: Professional mediators facilitated structured conversations between conflicting groups to "humanize" each side and repair relationships.
- **Shared Responsibility**: The process involved schools, social workers, and the police to create a unified support network that reinforced peaceful norms.

Impact: A rapid stabilization of local tensions and the restoration of public trust in both the police and the city's ability to manage diversity.

More information: https://cosecur.eu/case-study/forssa-community-dialogue/

3.2 Cross-sector Collaboration

Cross-sector collaboration refers to structured cooperation between public authorities, law enforcement, civil society organisations, private actors, and academia. Addressing complex security challenges requires coordinated efforts that transcend institutional boundaries.

.

Effective collaboration mechanisms:

- Reduce fragmentation and duplication
- Enable knowledge sharing and joint problem-solving
- Support integrated and holistic approaches to security

Guideline 4. Establish formal coordination frameworks

Objective
Improving cooperation between relevant actors by reducing fragmentation and ensuring clearer, more structured collaboration across institutions involved in security and social innovation.

Key Actions

- To achieve this, formal cooperation agreements should be developed between public authorities, law enforcement, NGOs, and relevant private sector actors, setting out shared objectives and working arrangements. Institutional mandates and responsibilities need to be clearly defined to avoid overlaps and gaps in implementation.
- In addition, shared governance models should be introduced to support more structured and continuous collaboration, enabling joint decision-making and more coherent operational responses across institutions.

Actors involved: Public authorities, law enforcement, NGOs, private sector.

Case Study: ANCHOR (Ankkuri)

Multiple cities across Finland.



Description: ANCHOR is a highly formalised multi-agency model designed for the early prevention of juvenile crime and domestic violence.

Key elements:

- **Integrated Multi-disciplinary Teams**: Police officers, social workers, psychiatric nurses, and youth workers operate as a single unit within a shared office.
- **Standardised Operational Protocols**: The team follows established procedures for joint home visits and risk assessments, ensuring no information is lost between departments.

Impact: Significant reduction in juvenile recidivism and faster, more coherent interventions for at-risk youth.

More information: https://cosecur.eu/case-study/anchor-preventing-youth-crime/

Guideline 5. Create permanent coordination structures

Objective
Ensure continuity of coordination beyond project-based cycles. This guideline aims to move beyond short-term, project-driven approaches by embedding coordination into permanent institutional structures that can sustain action over time.

Key Actions

- Local authorities should establish dedicated safety coordination units or equivalent stable bodies responsible for overseeing collaboration across relevant actors and initiatives. These structures should not only manage ongoing activities but also ensure continuity between projects and policy cycles.
- A key function of these units should be the preservation of institutional memory, ensuring that knowledge, lessons learned, and good practices are systematically documented and transferred across teams and time periods, reducing dependence on individual projects or personnel.

Actors involved: Municipalities, regional authorities.

Case Study: Nightlife Coordination Office

Germany (e.g., Mannheim)

Description: This office serves as a permanent governance platform that bridges the gap between the nighttime economy and municipal management.

Key elements:

- **Dedicated Institutional Liaison:** The office acts as a neutral point of contact for club owners, residents, and the city administration.
- **Conflict Prevention Architecture:** It institutionalizes regular communication channels and joint planning sessions to resolve noise or safety disputes before they escalate.

Impact: A more balanced nighttime environment where the economic vitality of nightlife is harmonized with the safety and comfort of local residents.

More information: https://cosecur.eu/case-study/night-life-coordination-bridging-nightlife-and-city-administration/

Guideline 6. Strengthen multi-actor ecosystems

Objective
Support collaborative innovation through cross-sector partnerships. This guideline aims to strengthen long-term collaboration between different sectors to overcome institutional silos and reinforce capacities for developing more effective and innovative responses.

Key Actions

- Public authorities should actively build and sustain partnerships with academia, the private sector, and civil society, moving beyond ad hoc cooperation towards structured, long-term collaboration. These partnerships should create stable spaces for knowledge exchange, enabling actors to share evidence, experiences, and methodological approaches.
- Co-design processes should be promoted as a standard practice in the development of solutions, ensuring that diverse expertise is integrated from the early stages of problem-solving and that solutions benefit from complementary perspectives across sectors.
- Ensure that security objectives are systematically integrated into broader regional strategies, including well-being, mobility, crisis management, and social cohesion policies, in order to promote policy coherence and avoid fragmented sectoral approaches.

Actors involved: Public, private, academic and civil actors.

Case Study: Brussels by Night

Brussels, Belgium

Description: A city-level program that coordinates police, prevention teams, and local venues to manage safety, intoxication, and noise in major nightlife districts.

Key elements:

- **Integrated Field Response:** Unified on-the-ground coordination between police patrols, street mediators, cleaning teams, and drug prevention specialists to defuse issues in real time.
- **Multi-Stakeholder Co-design:** Structured consultations with residents and venue operators to collaboratively plan steward presence, crowd flows, and local prevention rules.

Impact: Establishes a calmer street atmosphere, reduces physical disorder, and lowers the need for direct police enforcement, building public trust in nightlife management.

More information: https://cosecur.eu/case-study/brussels-by-night-supports-nightlife-actors-to-provide-a-better-scene-and-protects-brussels-club-culture/

3.3 Communication and Awareness

Communication plays a central role in shaping perceptions of safety, influencing behaviour, and building trust. SIS emphasises proactive, transparent, and inclusive communication strategies that go beyond crisis response.

Key aspects include:

- Clear and accessible information
- Engagement with diverse audiences
- Countering misinformation and harmful narratives

Communication is therefore not only a support function, but a core component of security governance.

Guideline 7. Develop proactive communication strategies

Objective

Strengthening anticipatory communication to support citizen preparedness and reduce uncertainty in relation to security risks and emerging situations, moving away from reactive communication approaches.

Key Actions

- Public authorities, supported by communication teams, should develop clear and accessible information on risks and appropriate behaviours, ensuring that messages are timely, consistent, and easy to understand. Communication should not only respond to incidents but also anticipate potential risks and guide citizens on preventive actions.
- To maximise reach and effectiveness, multiple communication channels should be used in a complementary way, combining digital platforms, traditional media, and community-based communication channels to ensure that information reaches diverse population groups, including those with limited digital access.

Actors involved: Public authorities, communication teams.

Case Study: Electric Castle Festival Safety Campaign

Bonțida (near Cluj-Napoca), Romania

Description: A comprehensive mass-event safety campaign combining immediate protective tools and educational initiatives to prevent harassment and substance misuse.

Key elements:

- **Discreet Help-Seeking Protocols:** The "Angel Shot" code at bars and dedicated "Safety Booths" that allow vulnerable attendees to seek immediate assistance safely.
- **Youth-Centric Education Platform:** The "G-Info Spot" (with the NGO Sexul vs Barza) providing stigma-free resources on consent, sexual health, and boundaries.

Impact: Normalizes respectful community behaviors, improves staff capacity to identify distress, and increases attendees' confidence in seeking help.

More information: https://cosecur.eu/case-study/electric-castle-festival-safer-by-targeted-messaging-and-awareness-raising/

Guideline 8. Ensure inclusive and accessible communication

Objective

Improve the accessibility and effectiveness of communication by ensuring that information reaches all segments of the population in a clear and understandable way, reducing risks of exclusion, misinterpretation, and resistance driven by unaddressed concerns or uncertainty.

Key Actions

- Municipalities, NGOs, and media organisations should develop communication materials using clear and simple language, avoiding technical jargon and adapting messages to different literacy levels. Where relevant, information should be made available in multiple languages to reflect local diversity.
- Communication strategies should also create space to acknowledge citizens' fears, concerns, and uncertainties, responding to them seriously and transparently in order to strengthen trust and reduce resistance to innovation.
- Special attention should be given to addressing digital exclusion by combining online communication with offline channels such as community outreach, printed materials, and local information points, ensuring that vulnerable groups are not left behind.

Actors involved: Municipalities, NGOs, media.

Case Study: Don't Give Up on Life - Crisis Aid on Warsaw's Bridges

Warsaw, Poland

Description: A citizen-initiated suicide prevention program that places motivational plaques on urban bridges to connect individuals in acute crisis with support services

Key elements:

- **Immediate Offline "Pause" Intervention**: Highly visible plaques offering straightforward, jargon-free emotional support and direct contact details for a 24/7 crisis hotline.
- **Integrated Crisis Response Loop**: A coordinated system linking hotline dispatchers, expanded CCTV monitoring, and River Police patrols for rapid intervention.

Impact: De-stigmatizes mental health struggles in public spaces and successfully turns high-risk bridges into proactive points of care.

More information: https://cosecur.eu/case-study/dont-give-up-on-life-crisis-aid-on-warsaws-bridges/

Guideline 9. Counter misinformation and harmful narratives

Objective

Strengthen trust in institutions and reduce social polarisation by proactively addressing misinformation and improving the quality and responsibility of public communication.

Key Actions

- Public authorities, together with media organisations and digital platforms, should develop proactive engagement strategies with the media to ensure that accurate and timely information is disseminated, especially during sensitive or rapidly evolving situations. This includes building stable relationships with journalists and communication professionals to facilitate fact-based reporting.
- At the same time, responsible communication practices should be promoted across all actors involved, encouraging consistency, transparency, and verification of information before dissemination. This helps reduce the spread of misleading narratives and strengthens the credibility of official messages.

Actors involved: Public authorities, media, digital platforms.

Case Study: REVERT (Resilience Without Violence)

Athens, Greece

Description: A collaborative project within the Athens transit system designed to combat xenophobia and rising anti-migrant narratives by fostering mutual dialogue, passenger awareness, and driver preparedness.

Key elements:

- **Anti-Stereotype Campaigns & Onboard Norms:** Implementing visible onboard communication campaigns and face-to-face community workshops to challenge public prejudice and establish mutual respect as a clear transit standard.
- **Contact-Based Coexistence:** Facilitating collaborative, informal social activities—such as sports matches between transit drivers and refugees—to dismantle "us-vs-them" polarization outside high-stress transit environments.

Impact: Successfully integrates anti-discrimination and conflict de-escalation modules into official transit driver training programs, reduces transit-based hostility, and improves daily intercultural communication.

More information: https://cosecur.eu/case-study/revert-combating-xenophobia-and-racism-in-athens-public-transport/

3.4 Environmental and Urban Design

Environmental and urban design approaches focus on how the physical environment can influence safety and behaviour. By integrating safety considerations into the design and management of public spaces, these mechanisms contribute to prevention and improved perceptions of security.

This includes:

- Designing for visibility and accessibility
- Creating inclusive and welcoming spaces
- Incorporating user perspectives into spatial planning

Such approaches are particularly relevant in urban contexts, where public space plays a key role in social interaction and security perception.

Guideline 10. Integrate security into urban planning

Objective
Integrate security considerations into urban planning processes, using spatial design to reduce risks and improve citizens' sense of security in public spaces.

Key Actions

- Urban planners and local authorities should apply safety-oriented design principles that enhance natural surveillance, improve lighting, and increase visibility in public areas, reducing opportunities for unsafe or anti-social behaviour. Accessibility should also be strengthened to ensure that public spaces are easy to navigate and usable for all groups.
- In parallel, public spaces should be designed to be inclusive and welcoming, taking into account the needs of diverse users, including women, older people, children, and vulnerable groups, so that safety is embedded not only in physical infrastructure but also in the social use of space.

Actors involved: Urban planners, municipalities.

Case Study: INSIGHT Toolbox

Germany (audits conducted in Bremen and Braunschweig during the Cutting Crime Impact project)

Description: A practical diagnostics and design toolkit developed within the EU Cutting Crime Impact (CCI) project by the State Office of Criminal Investigation of Lower Saxony (LKA Niedersachsen) to systematically analyze citizens' feelings of insecurity in public spaces. By bridging urban planning, policing, and community experience, it allows municipalities to identify safety concerns early and address them through design-led, proactive prevention rather than reactive enforcement.

Key elements:

- **Lived-Experience Diagnostics:** Utilizing participatory methods such as Emoji Mapping (allowing citizens to express spatial experiences by marking locations they enjoy, avoid, or feel unsafe in using emojis) and Walk Around Your Hood (structured on-site interdisciplinary inspections where experts and professionals evaluate physical spaces from the perspective of vulnerable users, such as the elderly or youth).
- **CPTED Spatial Analysis (Spatial Inventory):** A systematic documentation and mapping tool recording physical features—including lighting quality, benches, sightlines, visibility, and opportunities for natural surveillance—to provide urban planners with clear, experience-based data for targeted spatial improvements.
- **Heat Maps for Disorder**: A technical solution that utilizes pre-processed incident data on public order disturbances (from the Nivadis system) to generate heat maps, identifying events that disrupt neighborhood life and guiding evidence-based interventions.
- **Non-Participant Observation (Burano Method)**: A spatially grounded technique mapping human movement and presence across different times of day, weekdays, and seasons to verify behavioral patterns against perceived safety concerns.

Impact: Shifts municipal and police intervention from reactive problem-solving to proactive, safety-oriented design. It led to the permanent institutionalization of this approach through the creation of the Competence Center for Urban Security (KURBAS) within the Lower Saxony State

Police (LKA Niedersachsen), facilitating practical knowledge transfer, officer training, and the routine integration of safety assessments into urban planning.

More information: https://cosecur.eu/case-study/toolkit-security-a-crime-prevention-reference-framework-for-railway-station-areas/

Guideline 11. Adopt user-centred and inclusive design

Objective
Ensuring that security-related interventions are designed around the lived experiences and needs of diverse population groups, improving inclusiveness and relevance in security and urban solutions.

Key Actions

- Local authorities, in collaboration with citizens and NGOs, should use participatory mapping tools to identify perceptions of safety, risky areas, and everyday mobility patterns. This helps ground design decisions in real user experiences rather than assumptions.
- Design processes should systematically integrate gender and diversity perspectives, ensuring that the specific needs of different groups—such as women, migrants, children, and older people—are considered from the earliest stages of planning and implementation, rather than being added retroactively.

Actors involved: Local authorities, citizens, NGOs.

Case Study: "Shared Use Concept", Bremer Platz

Münster, Germany

Description: A park redesign near Münster's main railway station that balances public recreation with the needs of a historically rooted local open drug scene, choosing managed coexistence over repressive displacement.

Key elements:

- **Zoned Spatial Coexistence:** Dividing the square into three functional zones to minimize conflict: a southern recreation area for a nearby school, a central relaxation zone for the public, and a northern acceptance zone equipped with shelter and sanitary facilities for the drug scene.
- **Outreach Led Iterative Design:** Continuous street-level outreach by neighbourhood managers who gather design feedback directly from vulnerable users (the drug scene) and residents to adapt physical features like seating, shelters, and water access points.

Impact: Transforms a highly contested "fear zone" into a functional, socially integrated park that successfully stabilizes the area, reduces public tensions, and supports vulnerable citizens without displacing them to surrounding areas.

More information: https://cosecur.eu/case-study/bremer-platz-munster-a-shared-space-approach-for-urban-coexistence/

3.5 Technological Integration

Technological integration refers to the use of digital tools and data-driven solutions to support security objectives. Within SIS, technology is considered as an enabler that complements social and organisational processes.

Relevant applications include:

- Data collection and analysis for risk assessment
- Communication platforms and alert systems
- Simulation and scenario-based tools

Importantly, SIS promotes a human-centred approach to technology, ensuring that its use is ethical, transparent, and aligned with societal needs.

Guideline 12. Use technology as an enabling tool

Objective
To ensure that technology is used as a supportive instrument within broader social and governance strategies, reinforcing rather than replacing human-centred approaches to safety and security challenges.

Key Actions

- Public authorities and technology providers should ensure that digital tools are embedded within broader community-based strategies, combining technological solutions with on-the-ground engagement and local knowledge. This helps avoid overly technical responses to complex social risks and strengthens relevance and legitimacy.
- At the same time, technologies should be designed and selected with a strong focus on usability and accessibility, ensuring that they can be effectively used by diverse groups, including those with lower digital skills or limited access to digital infrastructure. This reduces capacity gaps and supports more equitable adoption of solutions.

Actors involved: Public authorities, technology providers.

Case Study: National Safety Threat Map

Poland (National level)



Description: This digital platform allows any resident to anonymously report local safety concerns—such as poor lighting or vandalism—via an interactive map.

Key elements:

- **Digital Co-production:** Thousands of citizens act as "smart sensors," providing the police with real-world data that statistics might miss.
- **Low-Barrier Participation:** The technology is designed for extreme simplicity, requiring no login to encourage widespread use.

Impact: Each verified report triggers mandatory police action, leading to visible local improvements and higher public trust.

More information: https://cosecur.eu/case-study/the-national-safety-threat-map/

Guideline 13. Ensure ethical and transparent use of technology

Objective

Ensuring that the deployment of technological solutions in the security field is guided by ethical principles, reinforcing public trust and protecting fundamental rights.

Key Actions

- Public authorities and technology developers should apply Responsible Research and Innovation (RRI) principles throughout the design and implementation of digital tools, ensuring that ethical considerations are embedded from the outset rather than addressed retroactively.
- Particular attention should be given to privacy and data protection, with clear safeguards on data collection, storage, and use, as well as compliance with relevant legal and regulatory frameworks. At the same time, transparency mechanisms should be established to make it clear how technologies function, how decisions are made, and who is accountable, thereby strengthening oversight and legitimacy.

Actors involved: Public authorities, developers.

Case Study: PACTESUR

Nice, France; Liège, Belgium; and Turin, Italy



Description: A European security network that combines advanced technological tools with citizen consultation to protect crowded urban environments from security threats while safeguarding civil liberties

Key elements:

- **Transparent Technology Dialogue**: Public workshops and consultations that openly explain how surveillance tools (such as drones and CCTV analytics) function and how privacy is protected, minimizing public concern.
- **Responsible Tech Integration**: Co-designing a comprehensive technology toolbox—comprising AI video analytics, mobile reporting, and VR crisis training—using legal and ethical safeguards that ensure regulatory compliance.

Impact: Equips cities with innovative, scalable situational awareness tools, improves professional crisis preparedness, and builds public acceptance of security technologies by ensuring they align with local values and fundamental rights.

More information: https://cosecur.eu/case-study/pactesur-protecting-allied-cities-against-terrorism-by-securing-urban-areas/

Guideline 14. Promote interoperable and data-driven systems

Objective

Strengthen coordination across institutions and improve decision-making by enabling better use, sharing, and integration of data across relevant actors.

Key Actions

- Public authorities, in collaboration with IT providers, should develop interoperable digital platforms that allow different institutions to share and access relevant data in a coherent and secure way. This helps reduce fragmentation and supports more coordinated responses across organisational boundaries.
- In parallel, data analytics tools should be used to support risk anticipation and early identification of emerging issues, enabling more proactive and evidence-informed decision-making rather than reactive responses.

Actors involved: Public authorities, IT providers.

Case Study: SECUR-ED (EVALU)

Bucharest, Romania

Description: A large-scale European demonstration pilot implemented in Bucharest's public transport system to reduce fragmentation by integrating security operations, digital communications, and law enforcement agencies.

Key elements:

- **Interoperable Control Rooms:** Transport operators (RATB/STB), control centers, and police/gendarmerie forces linked their systems to exchange real-time data and coordinate immediate, joint field responses.
- **Data-Driven Hotspot Mapping:** Systematically merging and analyzing historical police records, passenger feedback, and frontline inspector reports to anticipate high-risk times and areas, shifting patrols from reactive deployment to proactive prevention.

Impact: Achieved long-term institutional coordination by permanently establishing a dedicated Public Transport Police Brigade, reducing emergency response delays, and significantly improving passenger and staff safety perceptions.

More information: https://cosecur.eu/case-study/secur-ed-securing-european-urban-transport/

While the mechanisms outlined above provide a conceptual foundation, their effective application depends on several contextual factors, including governance structures, institutional capacity, and local socio-economic conditions.

The following chapter builds on this framework by providing a practical roadmap for implementation.

04

Roadmap for implementing Social Innovation in Urban Security

CO-SECUR

Funded by
the European Union

This roadmap provides a practical framework to support local authorities and stakeholders in designing and implementing Social Innovation in Security (SIS) approaches.
Building on the challenges identified in Section 2 and the strategic guidelines outlined in Section 3, the roadmap translates these elements into six interconnected stages that support the design, implementation and continuous improvement of Social Innovation in Security initiatives (see Figure 3).

It is designed to be flexible and adaptable to different local contexts, governance structures, and levels of institutional capacity. It follows a similar rationale than the standard procedure to ensure quality in crime prevention projects, the Beccaria-Standards: Quality assurance of crime prevention projects (Winter, 2005).

Although the roadmap is presented as six consecutive milestones for clarity, Social Innovation in Security is inherently an iterative process. Insights gained during implementation, monitoring and stakeholder engagement may require revisiting earlier stages, refining objectives, or adapting actions to changing circumstances. Rather than following a fixed sequence, practitioners should use the roadmap as a flexible framework that supports continuous learning and improvement.

Each milestone includes:

- its objective;
- the main actions to be undertaken;
- the expected outputs;
- the stakeholders typically involved;
- common implementation barriers;
- recommended tools and methods;
- an illustrative SIS good practice.

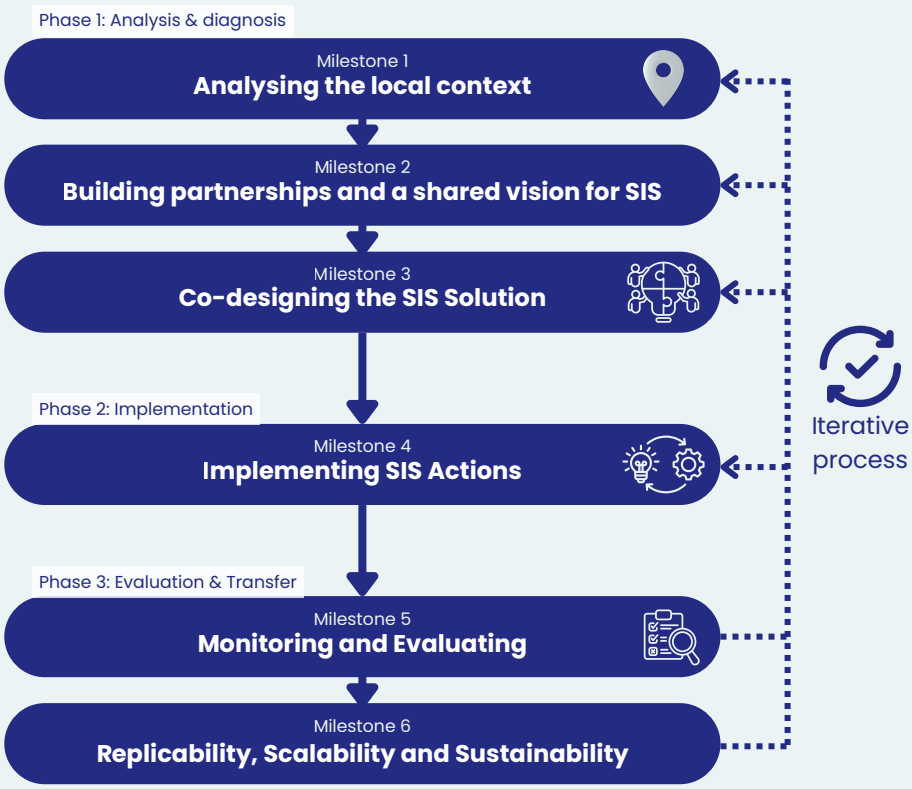

Figure 3. **Roadmap Milestones**

While the strategic guidelines provide the principles and recommendations that should inform SIS initiatives, the roadmap below translates these principles into an implementation journey. The Figure 4 shows the milestone(s) where each guideline is particularly relevant.

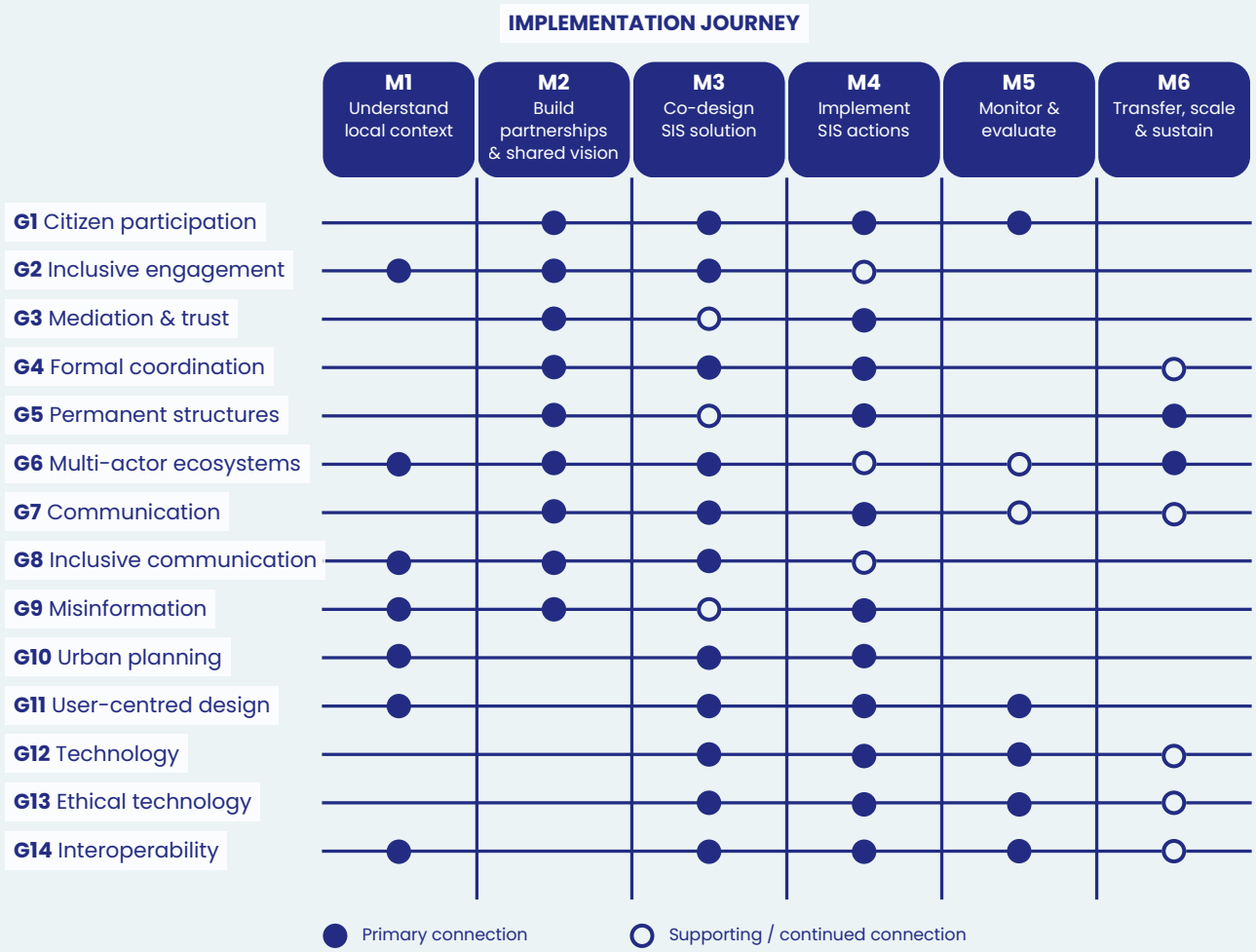

Figure 4. **Connecting the strategic guidelines (G1-G14) with the SIS Implementation Roadmap milestones (M1-M6)**

4.1. Analysis and diagnosis phase

Milestone 1: Analysing the local context

Objective
Develop a comprehensive understanding of the local security context by combining evidence, stakeholder knowledge and community perspectives. This milestone ensures that SIS interventions respond to real local needs rather than assumed problems.

Key Actions

- Analyse local security challenges using both objective data (crime statistics, socio-economic indicators, service gaps) and subjective dimensions (perceptions of safety, trust, fear, inclusion).
- Assess existing initiatives, programmes, and policies already addressing security-related issues.
- Conduct a participatory context self-assessment to identify strengths, weaknesses, opportunities, and barriers (SWOT analysis) within the local security ecosystem.
- Map key stakeholders, including public authorities, law enforcement, NGOs, community groups, private actors, researchers, and citizens.
- Identify governance structures, decision-making processes, and coordination mechanisms.
- Detect underserved groups, territorial inequalities, and emerging risks requiring targeted responses.

Expected outputs:

- A local security context assessment.
- A stakeholder map.
- A governance and institutional capacity assessment.
- A summary of key challenges, barriers and enabling conditions (SWOT analysis).
- A baseline of quantitative and qualitative indicators.
- A preliminary understanding of local priorities for SIS.

Stakeholders involved

- Local and regional authorities.
- Law enforcement agencies.
- Urban planning and mobility departments.
- Civil protection and emergency services.
- Social and health services.
- Civil society organisations.
- Community groups.
- Researchers and universities.
- Private sector organisations.
- Citizens, with particular attention to vulnerable and underrepresented groups.

Common implementation barriers

- Fragmented responsibilities across institutions.
- Limited availability or sharing of local data.
- Insufficient understanding of citizens' perceptions of security.
- Difficulties engaging vulnerable or hard-to-reach groups.
- Low institutional trust.
- Limited organisational capacity.
- Limited recognition of SIS as a strategic priority.

Tools and methods

Tool/method	Purpose	Recommended resource
Initiatives on Social Innovation in Security	Checking already existing SIS initiatives for inspiration or potential replication	CO-SECUR Booklet: Inspirational use-cases on Social Innovation in Security https://cosecur.eu/wp-content/uploads/2026/09/D2_2_Booklet-SIS-Case-Studies-1-1.pdf CO-SECUR use-cases database platform: https://cosecur.eu/case-studies/
SWOT Analysis	Synthesize the diagnosis and prioritise strategic actions.	CO-SECUR tool: Using SWOT and CAME for Assessing Social Innovations in Safety and Security: https://cosecur.eu/resources/
Community Needs Assessment	Identify the main security needs, vulnerabilities and priorities within the community.	OECD Guidelines for Citizen Participation Processes https://www.oecd.org/en/publications/oecd-guidelines-for-citizen-participation-processes_f765caf6-en.html
Participatory Mapping	Collect citizens' perceptions of safety and identify place-based issues.	Map-based platform for collecting and analysing spatially referenced public input: Maptionnaire [1] https://www.maptionnaire.com/
GIS & Spatial Risk Mapping	Analyse objective spatial patterns of crime, mobility and environmental risks.	Open-source QGIS Training Manual https://docs.qgis.org/3.44/en/docs/training_manual/
Stakeholder Mapping	Identify key actors, their roles and potential contributions to the SIS process.	CO-SECUR Stakeholder map: https://cosecur.eu/resources/
Vulnerability Mapping	Identify the population that may experience disproportionate exposure to security risks or barriers to participation.	Disaster Resilience Scorecard to assess Cities disaster resilience https://mcr2030.undrr.org/disaster-resilience-scorecard-cities

1 Maptionnaire is a private-sector company whose tool is recommended by the CO-SECUR project team as a suitable option for participatory mapping. This recommendation is based on the team's assessment of its relevance and does not imply any formal affiliation with the company.

Tool/method	Purpose	Recommended resource
Governance Self-Assessment	Evaluate institutional capacities and readiness to implement SIS.	UN-Habitat Governance Assessment Framework (GAF-MTR) https://unhabitat.org/governance-assessment-framework-for-metropolitan-territorial-and-regional-management-gaf-mtr

Case Study: INSIGHT Toolbox

Bremen, Braunschweig, and Essen, Germany

Description: A diagnostics methodology developed under the EU Cutting Crime Impact (CCI) project that integrates residents' subjective lived experiences with professional planning and policing perspectives to understand how safety is perceived in public spaces.

Key elements:

- **Citizen-Centred Emoji Mapping**: Residents mark locations on a physical or digital map using simple emotion-based symbols (emojis) to quickly identify hidden zones of discomfort, poor lighting, or high stress.
- **Interdisciplinary "Walk Around Your Hood" Inspections**: Planners, police officers, and municipal staff walk through neighborhoods together, adopting the specific roles of vulnerable users (e.g., seniors, young women, children) to assess spatial safety in real conditions.

Impact: Shifting local security planning from reactive policing to proactive, CPTED-led spatial improvements. The methodology has been institutionalized within the Lower Saxony State Police (KURBAS) to routinely guide urban safety assessments and municipal planning.

More information: https://cosecur.eu/case-study/insight-toolbox-a-collaborative-toolkit-for-analysing-perceptions-of-safety-in-public-spaces/

Milestone 2: Building partnerships and a shared vision for SIS

Objective
Following the context analysis, municipalities should work collaboratively with stakeholders to develop a shared vision that reflects local priorities, aspirations and capacities. This vision should provide a common direction for the SIS initiative and establish the foundations for collaborative implementation and long-term sustainability.

Key Actions
- Co-create a shared vision for the SIS initiative with relevant stakeholders by defining common objectives, priorities and expected outcomes.
- Ensure the meaningful participation of citizens, particularly vulnerable and underrepresented groups.
- Align the vision with existing policies, initiatives and local priorities.
- Agree on governance principles, roles and responsibilities.
- Consider long-term sustainability and institutional ownership from the outset.
- Document the shared vision to guide subsequent implementation.

Expected outputs:
- A shared vision statement for the SIS initiative.
- Agreed strategic objectives and implementation priorities.
- A preliminary governance framework, including key roles and responsibilities.
- A stakeholder commitment to support the implementation process.
- A long-term sustainability perspective, identifying opportunities for institutional ownership and future scaling.

Stakeholders involved
- Local and regional authorities.
- Law enforcement agencies.
- Civil society organisations.
- Community representatives.
- Citizens, including vulnerable and underrepresented groups.
- Researchers and academic institutions.
- Private sector organisations.
- Policy-makers and elected representatives.

Common implementation barriers
- Different stakeholder priorities and expectations.
- Limited political commitment or institutional leadership.
- Low levels of trust between organisations and communities.
- Unequal participation and representation.
- Limited understanding of the SIS approach.
- Short-term planning and uncertainty regarding future resources.

Tools and methods

Tool/method	Purpose	Recommended resource
Visioning Workshops	Facilitate the co-creation of a shared vision, objectives and long-term aspirations among stakeholders	UN-Habitat – Participatory Planning: https://unhabitat.org/topic/planning-and-design
Facilitation Methods	Support collaborative discussions, consensus-building and conflict management during co-design sessions.	Participatory Methods Toolkit – practitioner's manual https://ist.vito.be/en/publications/enpublications/toolkit.html
Conflict Mediation Approaches	Help reconcile different interests and build agreement where priorities diverge	Berghof Handbook for Conflict Transformation https://berghof-foundation.org/library/berghof-handbook-for-conflict-transformation

Case Study: Brussels by Us

Brussels, Belgium

Description: A citizen-led urban revitalization initiative that transformed neglected, unsafe underpasses and tunnels into attractive public spaces by developing a shared, community-backed vision for the area.

Key elements:

- **Living Lab Partnership & Co-design:** Bringing together municipal authorities, researchers, local NGOs, and residents to jointly map safety concerns and co-create solutions as equal partners.
- **Multifaceted Spatial Reclamation:** Activating the physical space through a coordinated blend of artistic installations, improved lighting, urban greening, and temporary community activities that encourage positive social interaction.

Impact: Reclaims problematic "fear zones," fosters deep community ownership, and successfully increases both actual and perceived safety without relying on repressive security measures.

More information: https://cosecur.eu/case-study/brussels-by-us/

Milestone 3: Co-designing the SIS solution

Objective
Translate the shared vision into a concrete, feasible and locally adapted implementation plan through collaborative design processes.

Key Actions
- Co-designing solutions that address the priorities identified during the previous milestones;
- Selecting and prioritising actions based on local needs, available resources and expected impact.
- Identifying the resources, capacities and partnerships required for implementation.
- Define a monitoring and evaluation framework, including a balanced set of Key Performance Indicators (KPIs) and qualitative indicators aligned with the objectives of the SIS initiative.
- Assessing ethical, legal and data protection considerations where relevant.
- Preparing an implementation plan, including timelines, responsibilities and monitoring arrangements.
- Validating the proposed intervention with key stakeholders before implementation.

Expected outputs:
- A co-designed SIS intervention or action plan.
- An implementation roadmap, including timelines, clearly defined roles and responsibilities, and resource needs.
- A preliminary monitoring and evaluation framework. (See Milestone 6)
- Stakeholder agreement on the proposed intervention.

Stakeholders involved
- Local and regional authorities.
- Law enforcement agencies.
- Urban planners.
- Civil protection and emergency services.
- Social and health services.
- Civil society organisations.
- Community representatives.
- Researchers and technical experts.
- Private sector organisations.
- Citizens, particularly those directly affected by the identified challenges.
- Legal experts (data, privacy, ethics).
- Communication and social media experts.

Common implementation barriers
- Difficulties translating broad objectives into concrete actions;
- Limited financial or human resources;
- Unclear governance arrangements and responsibilities;
- Insufficient coordination between departments and organisations;
- Conflicting stakeholder expectations;
- Legal, ethical or data governance constraints;
- Resistance to organisational change.

Tools and methods

Tool/method	Purpose	Recommended resource
Lessons learnt from similar initiatives	Understand the barriers and lessons learnt from previous experiences	D2.3. Lessons learnt from CO-SECUR on how to implement SIS involving citizens https://cosecur.eu/wp-content/uploads/2026/09/D2_3_Lessons-learnt-on-how-to-implement-SIS-involving-citizens-1-1.pdf
RACI Matrix	Clarify who is Responsible, Accountable, Consulted and Informed for each governance task.	European Commission, PM² Project Management Methodology Guide — RAM (RASCI): https://op.europa.eu/en/publication-detail/-/publication/97cc2f12-c648-11ee-95d9-01aa75ed71a1/language-en
Toolbox on Crime prevention through community engagement	Overview of citizen engagement initiatives and related challenges	European Crime Prevention Network (EUCPN) https://eucpn.org/sites/default/files/document/files/2502_ENG_Toolbox_BE_Crime%20prevention_LR.pdf
Living Lab Methodology	Co-design and test solutions with users and stakeholders in real-life settings.	European Network of Living Labs (ENoLL): https://enoll.org
Co-design Workshops	Develop and refine solutions collaboratively with all relevant actors.	Design Council – Double Diamond: https://www.designcouncil.org.uk/our-resources/the-double-diamond/
Privacy & Ethics Checklists (GDPR/Data Protection by Design)	Ensure that SIS actions involving personal data or digital technologies comply with privacy, ethics and fundamental rights requirements.	European Data Protection Board (EDPB): https://www.edpb.europa.eu/
Design Sprint / Rapid Prototyping	Test and refine proposed solutions before full-scale implementation.	Google Design Sprint Kit: https://designsprintkit.withgoogle.com[2]
Urban diagnostics	Combine spatial, socio-demographic and community-generated data to identify place-based risks, vulnerabilities and opportunities for intervention.	EU Local Digital Twin Toolbox: https://interoperable-europe.ec.europa.eu/collection/ldttoolbox/solution/eu-ldt-participate/solution-overview

2 Google Design Sprint Kit is a private-sector company whose tool is recommended by the CO-SECUR project team as a suitable option for participatory mapping. This recommendation is based on the team's assessment of its relevance and does not imply any formal affiliation with the company.

Tool/method	Purpose	Recommended resource
Tactical urbanism pilots	Use temporary, low-cost and reversible interventions to test co-designed solutions in real-world settings.	Nacto Urban Street Design: https://nacto.org/publication/urban-street-design-guide

Implementation Readiness Checklist

Before launching the implementation phase, it is recommended to carry out a final readiness check. This helps ensure that the proposed actions are feasible, supported by stakeholders and backed by appropriate governance and resources.

□ Have the proposed SIS actions been co-designed with relevant stakeholders?
□ Have implementation responsibilities been clearly assigned?
□ Are the necessary resources and capacities available?
□ Have ethical, legal and data protection aspects been addressed?
□ Has the implementation plan been agreed?
□ Have monitoring arrangements been defined?

Case Study: Safer Leiria (UrbSecurity)

Leiria, Portugal

Description: An urban security initiative that addressed rising feelings of insecurity in Leiria's historic center by using a "Quintuple Helix" collaborative planning model to co-design local physical and social interventions.

Key elements:

- **CPTED Principles**: Gamified Co-Design ("Serious Games"): Utilizing interactive planning games to engage citizens, municipal planners, academics, and local business owners as equal partners in co-designing the city's Integrated Action Plan.
- **CPTED-Driven Spatial Redesign**: Integrating Crime Prevention Through Environmental Design principles directly into the co-designed plans, focusing on eliminating blind spots, activating underused public areas, and improving street lighting.

Impact: Substantially improves residents' feelings of safety in the historic center and ensures that municipal urban interventions are directly aligned with the real, lived needs of the community.

More information: https://cosecur.eu/case-study/safer-leiria-a-collaborative-intervention-method/

4.2. Implementation phase

Milestone 4: Implementing SIS Actions

Objective
Testing and deploying integrated interventions based on SIS principles.
Implementation should be regarded as an adaptive process rather than the execution of a fixed plan. Continuous learning, stakeholder feedback and emerging evidence may require revisiting earlier decisions and refining interventions throughout the implementation process.

Key Actions
- Putting the implementation plan into practice, ensuring clear responsibilities, timelines, resources and monitoring arrangements;
- Combining social, spatial, technological and organisational interventions (guidelines and mechanisms of actions explained in Section 3) to develop integrated and mutually reinforcing solutions;
- Testing, reviewing and refining actions through pilot activities and continuous stakeholder feedback before scaling successful solutions;
- Documenting progress and lessons learned throughout implementation, including monitoring data and stakeholder feedback;
- Adapting interventions where needed and mitigating any unintended negative impacts to ensure that solutions remain effective, inclusive and adapted to community needs.

Expected outputs:
- SIS actions implemented in accordance with the agreed implementation plan.
- Effective coordination among stakeholders throughout implementation.
- Refined interventions, adapted in response to monitoring results and stakeholder feedback.
- A solid evidence base to support the evaluation, sustainability and potential scaling of the SIS initiative.

Stakeholders involved
- Local and regional authorities.
- Law enforcement authorities.
- Urban planners.
- Mobility planners.
- Civil society, community representatives.
- Vulnerable groups.
- Research and academia.
- Private sectors, where relevant.

Common barriers for implementation
- Limited resources, budget or implementation capacity.
- Unclear governance, ownership or responsibilities.
- Actions that are not sufficiently based on local needs or stakeholder priorities.
- Exclusion of vulnerable or underrepresented groups during implementation.
- Scaling interventions before they have been properly tested or gained community support.
- Limited monitoring and learning, reducing the ability to adapt and mitigate unintended negative impacts.

Tools and methods

Tool/method	Purpose	Recommended resource
Agile Project Management (PM² Agile Practices)	Support iterative implementation, adaptive planning and continuous improvement throughout the delivery of SIS actions.	European Commission PM² Methodology: https://commission.europa.eu/funding-tenders/how-apply/pm2-project-management-methodology_en
Prototyping procedures	Approach to developing, testing and improving an idea at an early stage	Nesta prototyping framework: https://www.nesta.org.uk/toolkit/prototyping-framework/
"Do No Harm" ethics risk analysis	Anticipate unintended negative effects of security interventions on specific groups before piloting or scaling them.	CDA Collaborative Learning Projects, The "Do No Harm" Framework for Analyzing the Impact of Assistance on Conflict: A Handbook — https://www.cdacollaborative.org/publication/the-do-no-harm-framework-for-analyzing-the-impact-of-assistance-on-conflict-a-handbook/
Digital Collaboration Platforms	Assess interoperability requirements and identify existing standards, and reusable solutions for the implementation of digital public services.	Interoperable Europe Portal - Solutions: https://interoperable-europe.ec.europa.eu/interoperable_solutions

Case Study: Pol'and'Rock Festival

Czaplinek–Broczyno, Poland

Description: One of Europe's largest open-air music events that successfully manages high-demand safety, environmental, and crowd risks by combining a multi-agency professional response with a deeply embedded peer-to-peer safety culture.

Key elements:

- **Multi-Agency Joint Command**: Establishing a unified command structure where the festival organizer, regional authorities, police, fire, medical, and rescue services work side-by-side, sharing real-time information and conducting daily joint briefings to adapt safety actions on the ground.
- **Peer-to-Peer Normative Regulation**: Utilizing the "Pokojowy Patrol" (Peaceful Patrol)—a massive corps of trained volunteers who use first aid, communication, and de-escalation to guide behavior, promote prosocial norms, and manage conflicts before they require police intervention.

Impact: Successfully minimizes response delays, eliminates institutional blind spots, and shifts large-scale event security from a purely punitive enforcement model to a highly trusted, community co-produced safety ecosystem.

More information: https://cosecur.eu/case-study/polandrock-festival/

4.3 Evaluation and Transfer phases

Milestone 5. Monitoring and Evaluating

Objective
Assess the implementation and outcomes of the SIS initiative to understand what worked, what could be improved and how lessons learned can inform future actions.

Key Actions
- Collecting evidence from multiple sources including operational data, stakeholder feedback and citizens' perceptions of safety and inclusion (through surveys, interviews, participatory feedback methods, etc).
- Evaluating both the implementation process and the results achieved, identifying strengths, challenges and unintended impacts.
- Assess the longer-term social impact of the initiative, including changes in trust, social cohesion, perceptions of safety and community resilience where possible.
- Assess how the initiative has influenced institutional collaboration, governance practices and organisational readiness for future SIS initiatives.
- Documenting and sharing good practices and lessons learned to facilitate knowledge exchange and replication.

Expected outputs:
- An evaluation report assessing both the implementation process and the outcomes achieved. Evaluation should combine objective indicators (e.g. implementation progress, participation rates or accessibility improvements) with perception-based indicators (e.g. feelings of safety, trust in institutions or stakeholder satisfaction).
- Evidence on the effectiveness and impact of the SIS actions.
- Lessons learned and recommendations, including good practices and transferable knowledge for improving future interventions.

Stakeholders involved
- Local and regional authorities.
- Evaluation and monitoring teams.
- Law enforcement and public service providers.
- Civil society organisations.
- Citizens and community representatives.
- Researchers and academic institutions.
- Policy-makers and funding organisations.

Common barriers for implementation
- Limited availability or quality of monitoring data.
- Focusing only on quantitative indicators while overlooking qualitative outcomes, such as trust, social cohesion or perceptions of safety.
- Limited stakeholder participation in the evaluation process.
- Insufficient time or resources for meaningful monitoring and reflection.
- Failure to translate evaluation findings into improvements for future actions.

Tools and methods

Tool/method	Purpose	Recommended resource
Indicators	Objective and perception-based indicators to monitor and evaluate the action.	CO-SECUR Illustrative monitoring indicators for Social Innovation in Security (SIS) https://cosecur.eu/resources/
Evaluation Frameworks	Structure the evaluation process and assess both implementation and outcomes.	OECD DAC Evaluation Criteria: https://www.oecd.org/dac/evaluation/daccriteria.htm
Monitoring Indicators	Measure implementation progress and outcomes using quantitative and qualitative evidence.	European Commission Better Regulation Toolbox, TOOL #43. Monitoring arrangements and indicators https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en
Monitoring Systems and Dashboards	Visualize and track indicators in real time to support timely, evidence-based decision-making.	Platforms such as: • DevResults (https://www.devresults.com/) • Kobo Toolbox (https://www.kobotoolbox.org/)
OECD Well-being Framework	Measuring social outcomes, trust, inclusion and quality of life using a combination of objective and perception-based indicators.	OECD Well-being Framework https://www.oecd.org/en/topics/measuring-well-being-and-progress.html
Social Return on Investment (SROI)	Assess the wider social value created by SIS initiatives beyond immediate security outcomes.	Social Value International: https://www.socialvalueint.org/
Theory of Change Canvas	Build shared understanding of the causal pathway from actions to long-term outcomes/impacts.	UNEP – *Theory of Change Approach for evaluation*: https://www.unep.org/evaluation-office/building-capacity-evaluation
Before/After Spatial Perception Mapping	Compare residents' perceived safety in a specific space before and after the intervention, capturing subjective experience alongside physical/environmental factors.	Efus – Methods and Tools for a Strategic Approach to Urban Security: https://efus.eu/topics/audits-methodology/methods-and-tools-for-a-strategic-approach-to-urban-security-publication/ *(complementary: Safetipin Safety Audit — https://safetipin.com/)*

Tool/method	Purpose	Recommended resource
After Action Reviews (AARs)	Reflect on implementation, identify lessons learned and improve future interventions.	NATO Joint Analysis & Lessons Learned Centre (JALLC): https://www.jallc.nato.int/
Feedback Loops and Learning Reviews	Enable continuous, real-time adjustment of the initiative based on ongoing evidence and stakeholder input.	USAID Collaborating, Learning & Adapting (CLA) Framework: https://usaidlearninglab.org/cla

Case Study: LETS-CROWD

Madrid, Spain (and various European pilot cities)

Description: A European-wide security initiative that developed a comprehensive risk-assessment and monitoring toolkit to assist Law Enforcement Agencies (LEAs) and organizers in evaluating crowd dynamics and security readiness before and during mass events.

Key elements:

- **Dynamic Crowd Evaluation Models**: Integrating real-time crowd sensors, spatial density trackers, and safety checklists to monitor crowd flows and evaluate potential stress points during large-scale gatherings.
- **Simulation-Based Performance Monitoring**: Utilizing digital crowd simulations and evacuation scenarios to evaluate the effectiveness of local security protocols, enabling police and organizers to continuously audit and refine their response plans.

Impact: Establishes a standardized, data-driven framework for crowd safety, improving coordination between municipal authorities and emergency responders while shifting mass event planning from intuitive assumptions to structured, evidence-based evaluation.

More information: https://cosecur.eu/case-study/lets-crowd-law-enforcement-agencies-human-factor-methods-and-toolkit-for-the-security-and-protection-of-crowds-in-mass-gatherings-eu-project/

Milestone 6: Replicability, scalability and sustainability[3]

Objective
Ensure that successful SIS initiatives can be sustained and replicated beyond their original context.

Key Actions
- Embedding successful SIS practices into local policies, strategies and governance structures to ensure long-term continuity;
- Developing a sustainability strategy, identifying long-term funding opportunities, strategic partnerships and the resources required to maintain successful actions over time;
- Preparing a replication and scaling roadmap, identifying which elements of the initiative can be transferred while adapting them to different local contexts;
- Sharing knowledge, tools and lessons learned through peer-learning activities, communities of practice and cross-regional collaboration networks;
- Reviewing the long-term impact of the initiative, including its contribution to institutional change and community resilience;
- Regularly updating the SIS approach in response to emerging risks and evolving community needs.

Expected outputs:
- A long-term action plan for the continuous development and improvement of SIS initiatives.
- A replication and scaling roadmap identifying opportunities to transfer or expand successful practices.
- Documented good practices, lessons learned and transferable tools to support knowledge exchange.
- Recommendations for integrating SIS approaches into local policies, governance structures and organisational practices.
- Strengthened partnerships and peer-learning networks supporting future collaboration and replication.

Stakeholders involved
- Local and regional authorities.
- Policy-makers.
- National and European public authorities.
- Civil society organisations.
- Community representatives.
- Researchers and academic institutions.
- Networks of municipalities.
- Funding bodies and investors.
- Private sector partners.

Common barriers for implementation
- Limited political commitment to continue SIS initiatives beyond the initial project.
- Insufficient long-term funding or organisational capacity to sustain successful actions.
- Replicating solutions without adapting them to local contexts and community needs.
- Weak knowledge-sharing and collaboration networks, limiting opportunities for peer learning and replication.
- Limited documentation of lessons learned and evidence, making it difficult to transfer successful practices.

3 **Sustainability** refers to maintaining successful SIS actions over time through appropriate governance, resources and institutional commitment. **Scalability** is the ability to expand successful interventions to reach a wider population or territory within the same system. **Replicability** refers to adapting and implementing successful approaches in different contexts while preserving their core principles.

Tools and methods

Tool/method	Purpose	Recommended resource
Initiatives on Social Innovation in Security	Sharing the initiative in an interactive platform	CO-SECUR use-cases database platform: https://cosecur.eu/case-studies/
Scaling up toolkit	Assess conditions and pathways for scaling social innovations	European Commission – Scaling-up Social Innovation: Seven Steps https://employment-social-affairs.ec.europa.eu/scaling-social-innovation-seven-steps-using-esf_en
Knowledge-sharing Platforms and Communities of Practice	Facilitate peer learning, exchange of good practices and collaboration across municipalities and regions.	European Urban Initiative: https://www.urban-initiative.eu/
Funding and Investment Strategies	Identify suitable funding sources and financing mechanisms to ensure long-term sustainability.	EU Funding & Tenders Portal: https://ec.europa.eu/info/funding-tenders/opportunities/portal/

Replicability, Scalability and Sustainability Checklist

Before concluding the SIS process, municipalities should assess whether successful interventions are ready to be sustained, expanded or transferred to other contexts.

□ Have successful practices been clearly documented and evaluated?
□ Have long-term funding and governance arrangements been identified?
□ Have SIS approaches been integrated into local policies or organisational practices?
□ Has a replication and scaling roadmap been developed?
□ Have knowledge, tools and lessons learned been shared with other municipalities or networks?
□ Are mechanisms in place to regularly review, adapt and improve the initiative over time?

Case Study: Time for Change in Alytus

Alytus, Lithuania

Description: A municipal safety initiative that institutionalized youth preventive work and multi-agency partnerships to steer at-risk youth away from anti-social behavior, transitioning local security from reactive enforcement to sustainable community support.

Key elements:

- **Policy-Embedded Cooperation**: Legally integrating county police, school boards, and municipal social services into a permanent, locally funded interdisciplinary team, ensuring the initiative's long-term operational continuity.
- **Scalable Restorative Models**: Establishing standardized youth behavioral mentoring and parent-coaching modules designed to be easily replicated and adapted in other Lithuanian municipalities facing similar juvenile safety challenges.

Impact: Successfully embedded youth safety and preventative care protocols directly into Alytus's local strategic development plans, creating a stable, locally funded governance framework that reduced youth-related public nuisances and increased trust in local safety institutions.

More information: https://cosecur.eu/case-study/time-for-change-in-alytus/

05
Conclusions

CO-SECUR

Funded by
the European Union

This report has explored how Social Innovation in Security (SIS) can support the development of more inclusive, effective, and resilient security approaches across European urban contexts. Building on the conceptual foundations, empirical evidence, and stakeholder engagement activities developed within the CO-SECUR project, it provides a structured framework to support the adoption of SIS in practice.

The analysis confirms that security challenges are increasingly complex, interdependent, and context-specific. Traditional approaches based primarily on top-down or reactive measures are often insufficient to address issues related to trust, perception of safety, social cohesion, and emerging risks. In this context, Social Innovation in Security offers a complementary paradigm, emphasising participation, collaboration, prevention, and responsiveness to societal needs.

The findings of the SWOT/CAME analysis, enriched through iterative stakeholder engagement processes, highlight a set of persistent challenges. These include fragmented governance structures, limited institutional capacity, insufficient inclusion of diverse social groups, and difficulties in evaluating and sustaining initiatives over time. At the same time, the analysis identifies significant opportunities, including growing policy support at the European level, increasing local innovation capacities, and the availability of diverse practices across cities.

In response to these insights, this document proposes a set of strategic guidelines structured around key mechanisms of action: participatory governance, cross-sector collaboration, communication and awareness, environmental and urban design, and technological integration. These mechanisms reflect the need for integrated and multi-dimensional approaches, combining social, spatial, organisational, and technological components.

The integration of case studies from the CO-SECUR mapping demonstrates that SIS is already being implemented across a wide range of contexts and thematic areas, including mass events, nightlife, mobility systems, and the protection of vulnerable groups. These examples illustrate the feasibility and adaptability of SIS approaches, while also highlighting the importance of context-sensitive design and implementation.

To support the transition from strategy to practice, the report provides a roadmap for implementation, outlining key steps from the analysis of the local context to the development of sustainable and scalable interventions. This roadmap emphasises the importance of stakeholder engagement, clear governance structures, continuous learning, and long-term commitment.

Overall, the results underline that the successful adoption of SIS depends not only on specific tools or interventions, but on the creation of enabling conditions. These include political commitment, institutional coordination, adequate resources, capacity-building, and the ability to adapt to local contexts. Importantly, SIS should not be considered as a complementary or optional approach, but as an integral component of modern security policy.

Looking forward, further efforts are needed to strengthen the evidence base, develop robust evaluation frameworks, and support the scaling and transferability of successful practices across different contexts. Continued collaboration between public authorities, communities, researchers, and practitioners will be essential to fully realise the potential of Social Innovation in Security.

In this regard, CO-SECUR contributes to advancing both the conceptual understanding and the practical implementation of SIS, offering a foundation for future policy development and innovation in the field of European security.

06
References

CO-SECUR

Funded by
the European Union

- Dantas, C., op den Akker, H., Bello, P., Machado, N., Marinho, A., Fornes, G., Llop, L., Mekri, M., Hecker, M., Rau, A., Cristea, L., Dec, B., Kamińska, A., Woch, M., Nikolaidis-Konstas, D., Jaržemskis, A., Girdvainienė, L., Kalašnikovaitytė, E., Papadimitriou, A., Montaldo, M., Monge, G., Lucas, R., & Ferrando, M. (2022). Database of Social Innovation in Security Cases (**CO-SECUR Deliverable D1.2**). CO-SECUR project. https://cosecur.eu/wp-content/uploads/2025/11/D1_2_Database-of-Social-Innovation-in-Security-cases.pdf

- Llop, L., Fornés, G., Laakso, K., Mekri, M., Hecker, M., Rau, A., Bello, P., op den Akker, H., Dantas, C., Machado, N., Marinho, A., Cristea, L., Dec, B., Kamińska, A., Woch, M., Nikolaidis-Konstas, D., Jaržemskis, A., Girdvainienė, E., Kalašnikovaitė, I., Papadimitriou, A., Montaldo, M., Ballina, V., Lucas, L., & Ferrando, M. (2025). Literature review on Social Innovation for Security Perception and Security Behaviour (**CO-SECUR Deliverable D1.1**). https://cosecur.eu/wp-content/uploads/2025/11/D1_1_Literature-review-on-Social-Innovation-for-Security-Perception-and-Security-Behaviour.pdf

- Llop, L., Garcés, J., Mekri, M., Hecker, M., Rau, A., op den Akker, H., Machado, N., Dantas, C., Cristea, L., Andrei, L., Marin, M., Woch, M., Nikolaidis-Konstas, K., Trochidis, I., Girdvainienė, I., Venskūnaitė, E., Tanriverdi, A., Santini, G., Hylander, A., García-Lepetit, N., & Ferrando, M. (2026). Lessons learnt on how to implement SIS involving citizens (**CO-SECUR Deliverable D2.3**). CO-SECUR project. https://cosecur.eu/wp-content/uploads/2026/09/D2_3_Lessons-learnt-on-how-to-implement-SIS-involving-citizens-1-1.pdf

- Winter, I. C. (2005). Beccaria-Standards: Quality assurance of crime prevention projects. https://www.beccaria-standards.net/Media/Beccaria-Standards-englisch.pdf

- Woch, M., Kamińska, A., Dec, B., Tuchowski, D., Llop, L., Mekri, M., Hecker, M., Rau, A., op den Akker, H., Bello, P., Machado, N., Dantas, C., Cristea, L., Andrei, L., Marin, M., Nikolaidis-Konstas, K., Trochidis, I., Girdvainienė, I., Venskūnaitė, E., Tanriverdi, A., Santini, G., Hylander, A., Monge, G., García-Lepetit, N., & Ferrando, M. (2026). Booklet of SIS Case Studies (**CO-SECUR Deliverable D2.2**). CO-SECUR project. https://cosecur.eu/wp-content/upl

Annexes

CO-SECUR

Funded by
the European Union

Annex I.

Methodological approach

This report builds on previous research and analytical work carried out within the CO-SECUR project, ensuring coherence and continuity across project outputs.

First, the conceptual foundation of the analysis is informed by a *Literature Review on Social Innovation for Security Perception and Security Behaviour* (CO-SECUR Deliverable D1.1), which provides a comprehensive overview of existing knowledge on the role of social innovation in shaping security outcomes and citizens' perceptions.

Second, the empirical grounding of the report is supported by the mapping of Social Innovation in Security (SIS) initiatives developed in the *published Database with 180-225 SIS Cases* (CO-SECUR Deliverable D1.2). This database offers a broad overview of practices implemented across Europe, capturing a diversity of contexts, actors, and thematic areas.

Building on this mapping, *the published booklet D2.2 Inspirational Use-cases on Social Innovation in Security* (CO-SECUR Deliverable D2.2), provides a curated selection of 20 case studies, which have been used in this document to illustrate concrete applications of SIS approaches. These examples are integrated throughout the guidelines to demonstrate the practical relevance and transferability of the proposed actions.

Furthermore, the identification of the mechanisms of action underpinning this document are based on *the publication D2.3. Lessons learnt on how to implement SIS involving citizens* (CO-SECUR Deliverable D2.3). This framework defines key domains of intervention—such as participatory governance, cross-sector collaboration, communication, urban design, and technological integration—which are used to organise the strategic guidelines presented in this document.

Finally, the content of this report is informed by a participatory and iterative process involving project partners and external stakeholders. In this context, a SWOT/CAME analysis was conducted as part of a broader series of engagement activities, including co-creation sessions, and stakeholder consultations carried out in the nine CO-SECUR countries. The results from the SWOT analysis were reflected in Section 2 as challenges and enabling conditions, whereas the CAME inputs were incorporated in the guidelines of Section 3.

Finally, an open consultation collected feedback from eleven external stakeholders and four members from CO-SECUR Advisory Board.

This approach ensures that the guidelines and recommendations presented are both evidence-based and practice-oriented, reflecting challenges and opportunities across different European contexts.

All referenced materials are publicly available on the COSECUR project website: https://cosecur.eu/resources/

Table 4. **D3.1 Societal Development Plan Methodology**

Analytical & participatory process	Description	Outcome
Identification of key concepts and evidence	Analysis of 46 peer-reviewed and 62 grey literature studies.	**D1.1. Literature review on Social Innovation for Security Perception and Security Behaviour**
Mapping of practices and contexts	Mapping of 183 cases.	**D1.2 Database of Social Innovation in Security cases**
Selection of illustrative examples	20 case studies analysed and showcased	**D2.2 Inspirational Use-cases on Social Innovation in Security**
Identification of mechanisms of action and conceptual framework	Five mechanisms of action identified	**D2.3 Lessons learnt on how to implement SIS involving citizens** **D2.1. CO-SECUR conceptual framework and theoretical model**
Participative workshops to validate results	Three rounds of workshops in each of the nine CO-SECUR countries (27 workshops in total, 278 participants)	Nine **SWOT analysis** (one per country) and one cross country **CAME analysis.** Validated **D2.2** and **D2.3**
Open consultation, including External Advisory Board	Feedback received from eleven external stakeholders and four members of CO-SECUR External Advisory Board	Co-designed and validated **D3.1 Societal Development Plan**

Limitations

Several limitations should be considered when interpreting the findings and recommendations presented in this report. First, the evidence base encompasses Social Innovation in Security (SIS) initiatives that differ substantially in terms of geographical and institutional context, scale, maturity, target groups and thematic focus. As a result, the cases are not directly comparable, and the database and selected use cases should be understood as illustrative rather than statistically representative of SIS practices across Europe.

Second, the transferability of SIS approaches is inherently context-dependent. Institutional arrangements, regulatory frameworks, social and cultural factors, local needs and available resources can significantly influence how an approach is implemented and with what results. The guidelines should therefore be understood as adaptable principles rather than standardised solutions.

Third, although the participatory process involved stakeholders from nine CO-SECUR countries and incorporated co-creation activities, consultations and SWOT/CAME analysis, the perspectives gathered cannot fully represent the diversity of European cities, regions and stakeholder groups. In addition, participatory and qualitative methods necessarily involve a degree of subjectivity and may reflect the experiences and priorities of the participants involved.

Finally, the availability of evidence on the longer-term impacts of SIS initiatives remains limited. Many initiatives are still developing, meaning that robust evidence of sustained changes in security perceptions, behaviour or other societal outcomes is not always available. The recommendations therefore place greater emphasis on enabling conditions, mechanisms of action and practical implementation than on establishing causal relationships between specific interventions and outcomes.

These limitations do not undermine the value of the guidelines but rather highlight the importance of interpreting and applying them in light of local contexts, available evidence and the evolving nature of Social Innovation in Security.

Annex II.

Stakeholder roles across the guidelines and the roadmap

The involvement of each group changes along the SIS process. Sections 3 and 4 use the group names in Table X and a simple notation to indicate roles:

L (Lead) groups coordinate or take primary responsibility; **S (Support)** groups are active partners that co-design or co-deliver actions; and **C (Consulted)** groups provide input, data or feedback at specific points. A dash indicates that the group is not typically involved at that stage. These roles are indicative and should be adapted to local governance arrangements; for example, a civil society organisation or a research team may lead specific actions in some contexts.

Table 5. **Indicative roles of stakeholder groups in the six milestones of the roadmap**

Stakeholder group	M1 Local context	M2 Partnerships	M3 Co-design	M4 Implement	M5 Monitoring	M6 Replication
Local and regional authorities	**L**	**L**	**L**	**L**	**L**	**L**
National and European public authorities	–	–	–	–	C	**S**
Law enforcement, civil protection and emergency services	**S**	**S**	C	**S**	**S**	–
Public service providers	**S**	–	**S**	**S**	**S**	–
Citizens and community groups	C	**S**	**S**	**S**	C	C
Civil society organisations	**S**	**S**	**S**	**S**	**S**	**S**
Research and academia	**S**	C	C	**S**	**S**	**S**
Private sector	C	C	C	**S**	–	**S**
Media and digital platforms	–	–	–	C	–	C
Funders, investors and networks	–	–	–	–	C	**S**

L = Lead; S = Support; C = Consulted; – = not typically involved. Milestones are described in Section 4.

Table 6. **Indicative lead and support roles by strategic guideline**

Guideline	Lead	Support
1. Institutionalise citizen participation	Local and regional authorities	Citizens and community groups; civil society organisations
2. Ensure inclusive and representative engagement	Local and regional authorities	Civil society organisations; community groups
3. Integrate mediation and trust-building mechanisms	Local and regional authorities	Civil society organisations (mediators); public service providers (social services)
4. Establish formal coordination frameworks	Local, regional and national authorities	Law enforcement; civil society organisations; private sector
5. Create permanent coordination structures	Local and regional authorities	Law enforcement; civil society organisations; research and academia
6. Strengthen multi-actor ecosystems	Local and regional authorities	Private sector; research and academia; civil society organisations
7. Develop proactive communication strategies	Local and regional authorities	Law enforcement; media and digital platforms
8. Ensure inclusive and accessible communication	Local and regional authorities	Civil society organisations; media
9. Counter misinformation and harmful narratives	Local and national authorities	Media and digital platforms; law enforcement; civil society organisations
10. Integrate security into urban planning	Local and regional authorities (urban planning)	Public service providers; law enforcement; citizens
11. Adopt user-centred and inclusive design	Local and regional authorities	Citizens and community groups; civil society organisations
12. Use technology as an enabling tool	Local and regional authorities	Private sector (technology providers); research and academia
13. Ensure ethical and transparent use of technology	Local and national authorities	Private sector (developers); research and academia; civil society organisations
14. Promote interoperable and data-driven systems	Local, regional and national authorities	Private sector (IT providers); law enforcement; public service providers

Guidelines are described in Section 3.

Principles for engaging stakeholders

Regardless of the local context, the following principles, derived from the guidelines and from Responsible Research and Innovation (RRI), should inform stakeholder engagement throughout the roadmap:

- **Start from the local context**. The relevant stakeholders, their interests and their relationships differ from place to place. Mapping them is the first task of the roadmap (Milestone 1) and should be revisited as the initiative evolves.

- **Treat citizens as partners**. Citizens and communities are co-designers, not only consulted or informed (Guideline 1). Reaching vulnerable and underrepresented groups requires accessible formats and trusted intermediaries (Guidelines 2 and 3).

- **Recognise different interests and address tensions openly**. Typical tensions include privacy versus surveillance, enforcement versus community trust, commercial versus public interest, and short political cycles versus long-term change. Transparent and, where needed, mediated dialogue helps turn these tensions into shared decisions.

- **Clarify roles and commitments early**. Agreeing who leads, who supports and who is consulted, and recording it in a governance framework or coordination agreement, reduces fragmentation and duplication (Milestone 2; Guidelines 4 and 5).

- **Sustain engagement over time**. Providing feedback on how contributions have been used, resourcing facilitation and keeping stakeholders involved in monitoring and evaluation maintain trust and support long-term institutional ownership (Milestones 5 and 6; Guideline 1).

Annex III.

List of contributors

The following contributors were involved in the review and consolidation of this document. This list is not exhaustive and includes only those who have agreed to have their names publicly acknowledged:

CO-SECUR Consortium Members

- Kveloce
- University of Valencia
- Saferglobe RY
- Deutsch-Europäisches Forum für Urbane Sicherheit e.V. (DEFUS)
- Shine 2Europe Ltd.
- European Integrated Projects
- Evalu Sp. z o.o.
- Tero Monoprosopi IKE
- Smart Continent
- Digital Europe

CO-SECUR Advisory Board – Represented Organisations

- ICONS Innovation Strategies
- Wilfrid Laurier University – Viessmann Centre for Engagement and Research in Sustainability (VERiS)
- Epoka University
- University of Patras – SCYTALE Group

External Stakeholder Organisations

- University of Greenwich
- Geospatial Information Initiative Association
- Barcelona Supercomputing Center (BSC)
- Leibniz University Hannover
- ISAR Germany (International Search and Rescue)
- INNVOCAM
- City of Geel
- IASIS NGO
- Information Technologies Institute (ITI), Centre for Research and Technology Hellas (CERTH)



CO-SECUR

Co-creating urban security solutions

CO-SECUR is a 3-year Horizon Europe project (2023-26) that aims to **improve citizens' security perception and behaviour in public spaces**, especially at large events and crowded areas, by actively engaging them to co-create innovative security solutions.

Visit our website: cosecur.eu

Scan me

Subscribe to the Newsletter

Follow us on LinkedIn

Follow us on YouTube

Funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them. Grant Agreement no. 101121325