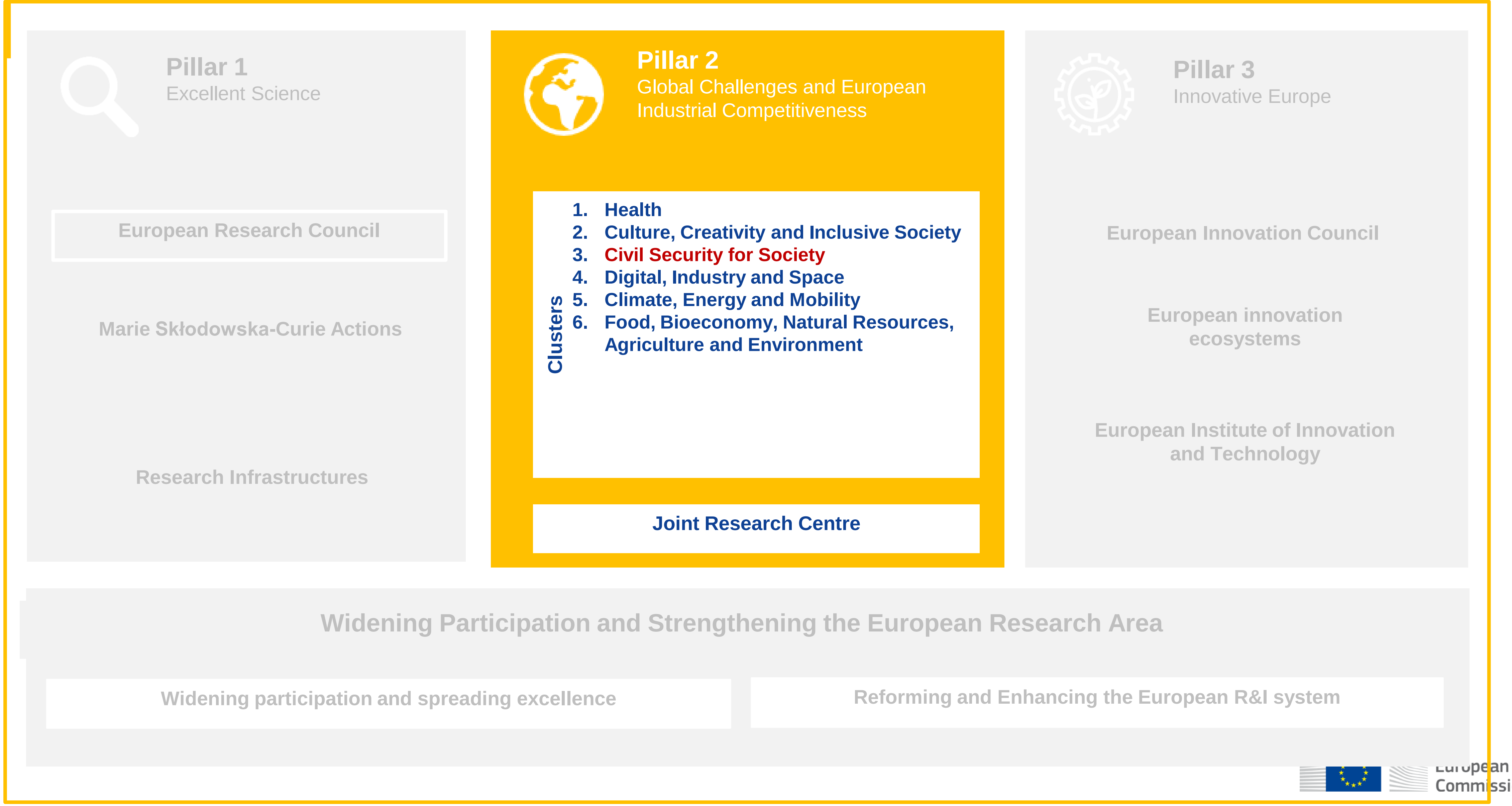
Cluster 3
‘Civil Security for Society’

European Commission

HORIZON EUROPE - CLUSTER 3



Pillar 1
Excellent Science

European Research Council

Marie Skłodowska-Curie Actions

Research Infrastructures

Pillar 2
Global Challenges and European Industrial Competitiveness

Clusters

1. Health
2. Culture, Creativity and Inclusive Society
3. Civil Security for Society
4. Digital, Industry and Space
5. Climate, Energy and Mobility
6. Food, Bioeconomy, Natural Resources, Agriculture and Environment

Joint Research Centre

Pillar 3
Innovative Europe

European Innovation Council

European innovation ecosystems

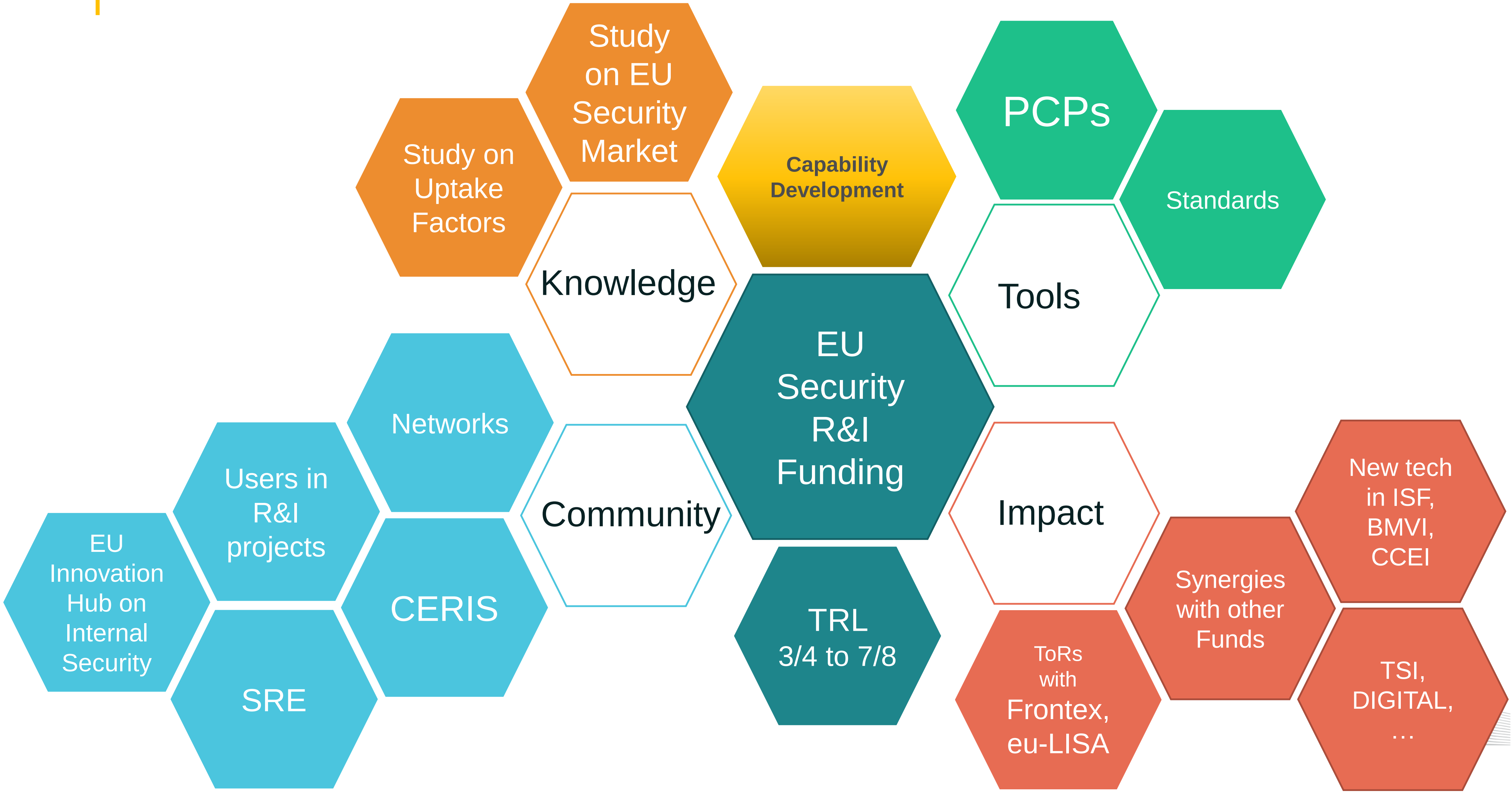
European Institute of Innovation and Technology

Widening Participation and Strengthening the European Research Area

Widening participation and spreading excellence

Reforming and Enhancing the European R&I system

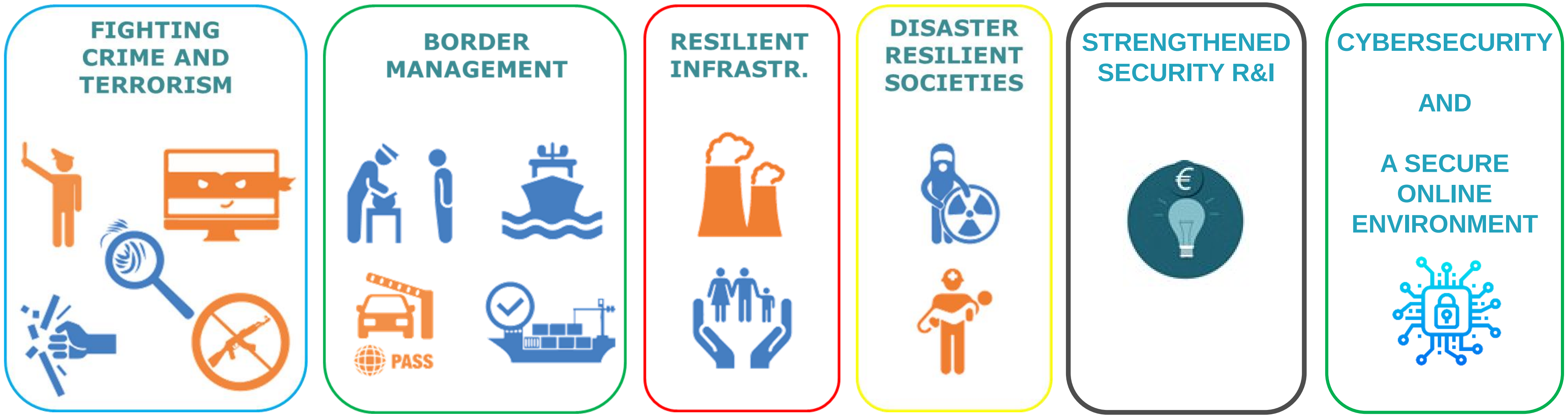
Addressing civil security innovation in the EU



European Commission

HE CLUSTER 3: Civil Security for Society

- **A work programme structured in 6 destinations**



FIGHTING CRIME AND TERRORISM

BORDER MANAGEMENT

RESILIENT INFRASTR.

DISASTER RESILIENT SOCIETIES

STRENGTHENED SECURITY R&I

CYBERSECURITY

AND

A SECURE ONLINE ENVIRONMENT

Capability-based approach

End-User oriented

Synergies and market creation

Societal dimension

Civil security for society

Key priorities/challenges addressed:

- Cluster 3 Work Programme part ‘Civil Security for Society’ will support the implementation of EU policy priorities on security, including cybersecurity, and disaster risk reduction and resilience.
- Cluster 3 focuses on projects that will improve EU preparedness and resilience in case of security threats, including cyber threats, hybrid threats, CBRN-E attacks etc.
- Cluster 3 topics also aim at protecting critical entities and infrastructures and to strengthen border surveillance.

Synergies foreseen with other funding programmes/work programme parts:

- Integrated Border Management Fund (IBMF)
- Internal Security Fund (ISF) – for law enforcement capabilities
- Digital Europe Programme
- Cohesion policy

Main horizontal policy priorities addressed:

- Within the framework of the Horizon Europe Strategic Plan 2021-2024, the Cluster 3 expected impacts will contribute in particular to the impact areas “*A resilient EU prepared for emerging threats*” and “*A secure, open and democratic EU society*” of Key Strategic Orientation D “*Creating a more resilient, inclusive and democratic European society*” and to the impact area “*Secure and cybersecure digital technology*” of Key Strategic Orientation A “*Promoting an open strategic autonomy by leading the development of key digital, enabling and emerging technologies, sectors and value chains*”.
- The Work Programme will support the European Commission policy priorities:
  - ✓ ‘Promoting the European way of life’
  - ✓ ‘European Green Deal’
  - ✓ ‘Europe fit for the digital age’.

Budget: EUR 186.60 million in 2023 (incl. missions) and EUR 196.29 million in 2024

FCT - MAIN FEATURES OF THE DESTINATION

- Related policy: Security Union Strategy, Counter-Terrorism Agenda, security dimension of the New Pact on Migration and Asylum, EU Strategy to tackle organised crime, … - stay up-to-date

- Synergies with other projects &/or calls: an asset whenever relevant and applicable

- Complementary instrument: Internal Security Fund

- ! This Destination will also promote, whenever appropriate and applicable, the proposals with:

  - the involvement of the Police Authorities in their core,
  - a clear strategy on how they will adapt to the fast-evolving environment in the area of fight against crime and terrorism (evolution of related technologies, evolution of criminal modi operandi and business models related to these technologies, etc.),
  - a minimum-needed platform, i.e. tools that are modular and can be easily plugged into another platform (in order to avoid platform multiplication),
  - tools that are developed and validated against practitioners' needs and requirements,
  - a robust plan on how they will build on the relevant predecessor projects,
  - the (active) involvement of citizens, voluntary organisations and communities,
  - education and training aspects, especially for Police Authorities and other relevant practitioners, as well as information sharing and awareness raising of the citizens,
  - a clear strategy on the uptake of the outcomes, defined in consultation with the involved stakeholders,
  - a well-developed plan both on how research data for training and testing will be obtained, in order to reach the requested Technology Readiness Levels (TRLs), and on how the specific TRL will be measured.

FCT - MAIN IMPACTS

- Modern information analysis for Police Authorities, allowing them to efficiently fight criminals and terrorists who use novel technologies;

- Improved forensics and lawful evidence collection, increasing the capabilities to apprehend criminals and terrorists and bring them to the court;

- Enhanced prevention, detection and deterrence of societal issues related to various forms of crime, including cybercrime, and terrorism, such as violent radicalisation, domestic and sexual violence, or juvenile offenders;

- Increased security of citizens against terrorism, including in public spaces (while preserving their quality and openness);

- Improved intelligence picture and enhanced prevention, detection and deterrence of various forms of organised crime;

- More secure cyberspace for citizens, especially children, through a robust prevention, detection, and protection from cybercriminal activities.

BM – MAIN FEATURES OF THE DESTINATION

- The Destination introduction and the general Cluster WP introduction apply to all topics !
- Keep up to date with relevant EU policy:
  - Security Union Strategy, New Pact on Migration and Asylum, European Border and Coast Guard, EU Maritime Security Action Plan and Research Agenda, EU Customs Union Action Plan.
- Three areas within this Destination:
  - Efficient border surveillance and maritime security;
  - Secured and facilitated crossing of external borders;
  - Better customs and supply chain security.
- Assistance from the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA).
- Central role of the European Border and Coast Guard Agency (Frontex).
- If projects use satellite-based, positioning, navigation and/or related timing data and services, beneficiaries must make use of Galileo/EGNOS (other data and services may additionally be used).
- The use of Copernicus for earth observation is encouraged.
- Develop knowledge and technologies that may be taken up by other instruments, such as the **EU Integrated Border Management Fund** (including the **Border Management and Visa Instrument, BMVI**; and the **Customs Control Equipment Instrument, CCEI**).
- The capabilities built by research and innovation in this Destination would clearly be relevant to be better prepared for potential future challenges to European internal security and crises as the ones in Ukraine in 2022.

European Commission

BM – MAIN IMPACTS

- Expected impact of the Horizon Europe Strategic Plan 2021-2024:
  - “Legitimate passengers and shipments travel more easily into the EU, while illicit trades, trafficking, piracy, terrorist and other criminal acts are prevented, due to improved air, land and sea border management and maritime security including better knowledge on social factors.”

- Specific impacts:
  - Improved security (as well as better cost- and energy- efficient management) of EU land and air borders, as well as sea borders and maritime environment, infrastructures and activities, as well as for the EU external civilian security, against accidents, natural disasters and security challenges such as illegal trafficking, piracy and potential terrorist attacks, cyber and hybrid threats;
  - Improved border crossing experience for travellers and border authorities staff (including customs, coast and border guards), while maintaining security and monitoring of movements across air, land and sea EU external borders, supporting the Schengen area, reducing illegal movements of people and goods across those borders and protecting fundamental rights of travellers, both EU citizens and Third Country Nationals;
  - Improved customs and supply chain security though better prevention, detection, deterrence and fight of illegal activities involving flows of goods across EU external border crossing points and through the supply chain, as well as through better interoperability, minimising disruption to trade flows.

INFRA – MAIN FEATURES OF THE DESTINATION

Policy priorities:

- EC Headline ambitions
- Security Union Strategy
- Joint Framework on Countering Hybrid Threats
- Union Civil Protection Mechanism
- Measures for high common level of cybersecurity across the Union (NIS-2 Directive)
- Resilience of Critical Entities (CER Directive)

Moreover:

- The capabilities built by research and innovation in this Destination would clearly be relevant to be better prepared for potential future challenges to European internal security and crises as the ones in Ukraine in 2022.
- Where possible and relevant, synergy-building and clustering initiatives with successful proposals in the same area should be considered, including the organisation of international conferences in close coordination with the Community for European Research and Innovation for Security (CERIS) activities and/or other international events.

INFRA – MAIN IMPACTS

Expected impact of the Horizon Europe Strategic Plan 2021-2024:

- *“[…] resilience and autonomy of physical and digital infrastructures are enhanced and vital societal functions are ensured, thanks to more powerful prevention, preparedness and response, a better understanding of related human, societal and technological aspects, and the development of cutting-edge capabilities for […] infrastructure operators […]”*

Specific Impacts:

- Ensured resilience of large-scale interconnected systems infrastructures and the entities that operate them in in case of complex attacks, pandemics, natural and human-made disasters, or the impacts of climate change;
- Upgraded systems for resilience of the operators and the protection of critical infrastructure to enable rapid, effective, safe and secure response and without substantial human intervention to complex threats and challenges, and better assess risks ensuring resilience and open strategic autonomy of European infrastructures;
- Resilient and secure smart cities are protected using the knowledge derived from the protection of critical infrastructures and systems that are characterised by growing complexity.

DRS – MAIN FEATURES OF THE DESTINATION

- Investments in this Destination contribute substantially to the European Union’s objectives in terms of climate change adaptation and resilience to climate change. The funded projects are aimed at developing new technologies and solutions that can be used to understand the long-term effects of climate change, as well as to improve capacities of first responders and institutions for climate mitigation and prevention of natural disasters. Improved understanding of hazards and strengthened knowledge of the risks that these entail for human communities and their activities are cornerstones for more a resilient economy and society.

- All proposals of projects under this Destination should aim to be complementary and avoid overlaps with relevant actions funded by other EU instruments, including the European Defence Fund and its precursors (the European Defence Industrial Development Programme (EDIDP) and the Preparatory Action on Defence research (PADR)), based on the information publicly available and while maintaining a focus on civilian applications only.

- Where possible and relevant, synergy-building and clustering initiatives with successful proposals in the same area should be considered, including the organisation of international conferences in close coordination with the Community for European Research and Innovation for Security (CERIS) activities and/or other international events.

DRS – MAIN IMPACTS

- **Expected impact of the Horizon Europe Strategic Plan 2021-2024**:
  - “Losses from natural, accidental and human-made disasters are reduced through enhanced disaster risk reduction based on preventive actions, better societal preparedness, and resilience and improved disaster risk management in a systemic way.”

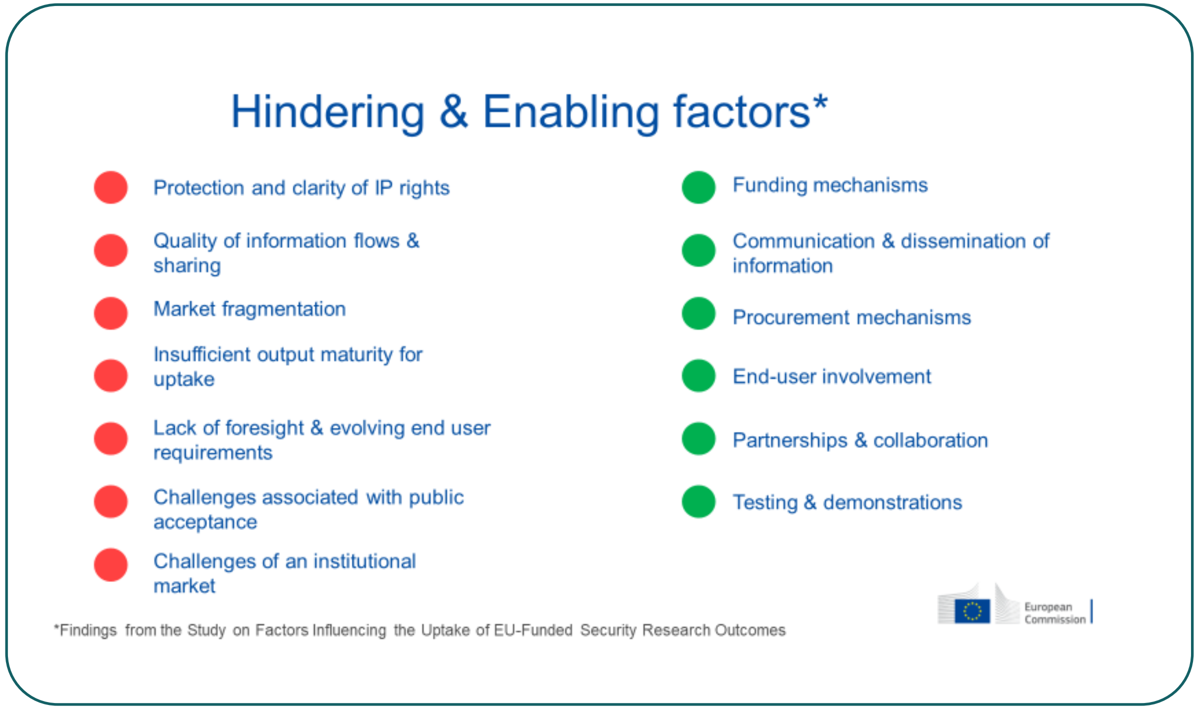
- **Specific impacts**:
  - Enhanced exploitation of the latest scientific results (e.g., from research programmes and institutions) and integrated technologies (e.g. Earth observation, in situ data collection, advanced modelling, AI) into enhanced understanding of high-impact hazards and complex compound and cascade events and improved prevention, preparedness to mitigation, response, and recovery tools;
  - Enhanced understanding and improved knowledge and situational awareness of disaster-related risks by citizens, empowered to act and involved in relevant research initiatives (including citizen volunteers) and consider innovative solutions, thus raising the resilience of European society;
  - More efficient cross-sectoral, cross-disciplines (including SSH), cross-border coordination of the disaster risk management cycle and governance (from scientific research to prevention, preparedness to mitigation, response, and recovery, including knowledge transfer and awareness of innovative solutions) from international to local levels;

DRS – MAIN IMPACTS

- **Specific impacts**:
  - Enhanced collaboration, interactions and cross-discipline dialogue and networking between the scientific community, research institutions and programmes (e.g., HE, ESA scientific activities, national science programmes, FutureEarth RIS-KAN) and first and second responders through dedicated networking and collaboration actions fostering a faster transfer of results from science into practice;
  - Support of harmonised and/or standardised and interoperability of guidelines / protocols / tools / technologies in the area of crisis management, natural disasters and CBRN-E;
  - Strengthened capacities of first responders in all operational phases related to any kind of natural and human-made disasters so that they can better prepare their operations, have access to enhanced situational awareness, have means to respond to events in a faster, safer and more efficient way, and may more effectively proceed with victim identification, triage and care;
  - Improved impact forecasting capability and scenario building for enhanced stress testing of critical entities and adaption of protection and resilience-enhancing activity accordingly;
  - Improve the capacity of institutions and professionals to respond to natural hazards, whose frequency and severity for human activities have increased and are partly resulting from climate change;
  - Improved ability to rescue and manage the first phases of emergencies that take into account extreme climatic events and/or geological hazards that may threaten urban areas (e.g. interface fires, floods, earthquakes, tsunamis, volcanic eruption etc.).

SSRI – MAIN FEATURES OF THE DESTINATION

- EU investment for the development of capabilities supporting policy priorities
  - Innovation can be decisive: modernisation / effectiveness / efficiency
  - **Uptake of innovation remains a challenge**



Hindering & Enabling factors*

- 🔴 Protection and clarity of IP rights
- 🔴 Quality of information flows & sharing
- 🔴 Market fragmentation
- 🔴 Insufficient output maturity for uptake
- 🔴 Lack of foresight & evolving end user requirements
- 🔴 Challenges associated with public acceptance
- 🔴 Challenges of an institutional market

- 🟢 Funding mechanisms
- 🟢 Communication & dissemination of information
- 🟢 Procurement mechanisms
- 🟢 End-user involvement
- 🟢 Partnerships & collaboration
- 🟢 Testing & demonstrations

*Findings from the Study on Factors Influencing the Uptake of EU-Funded Security Research Outcomes

- ❯ Create a favourable environment to generate specific knowledge
- ❯ Foster a structured dialogue and coordinated action among market actors;
- ❯ Exploit catalysts of uptake
- ❯ Conduct cross-cutting security research.

SSRI – MAIN IMPACTS

Stronger pillars of security Research and Innovation

- A more effective and efficient **evidence-based** development of EU civil security capabilities built on a stronger, more **systematic** and **analysis-intensive** security R&I **cycle**

Increased Innovation uptake of security R&I outcomes

- **Increased industrialisation, commercialisation, adoption and deployment** of successful outcomes of security research reinforces the competitiveness and resilience of EU security technology and industrial base

Cross-cutting knowledge for common security solutions

- **R&I-enabled knowledge and value in cross-cutting matters** reduces sector specific bias and breaks thematic silos that impede the proliferation of common security solutions

CS – MAIN FEATURES OF THE DESTINATION

- **CL3 Increased Cybersecurity:**
  - Will support the implementation of the EU Cybersecurity Strategy**.**
  - Will support the Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centre (COM 2018(630)).
  - Supported by R&I, citizens, public authorities and companies, including SMEs, will be empowered to protect their data and online activities, via a resilient critical digital infrastructure, both private and public, that better protects the Digital Single Market and the digital life of citizens against malicious cyber activities.
  - Will strengthen European cybersecurity industrial capacities, supply chain security and increased open strategic autonomy vis-à-vis foreign technologies.
  - Will support the use of innovative digital technologies, including self-healing, artificial intelligence, cryptography, massively distributed computing and storage, as well as quantum technologies to increase data security and augment cybersecurity.
  - Will support innovations in secure hardware and software development and implementation and improve methods for cybersecurity testing and certification.

➢ All these measures aim at defending the integrity of the Digital Single Market as well as the EU’s high standards concerning rights to privacy, protection of personal data, and the protection of other fundamental rights in the digital age on the global stage.

➢ The Destination will pay particular attention to the cybersecurity of the most vulnerable organisations and individuals.

➢ In order to defend against cyber-threats, the architectural principles of ‘security-by-design’ and ‘privacy-by-design’ will be implemented in digital technologies and their applications, such as 5G, industry 4.0, artificial intelligence, Internet of Things, block chain, quantum technologies, mobile devices and connected cooperative and autonomous mobility and energy.

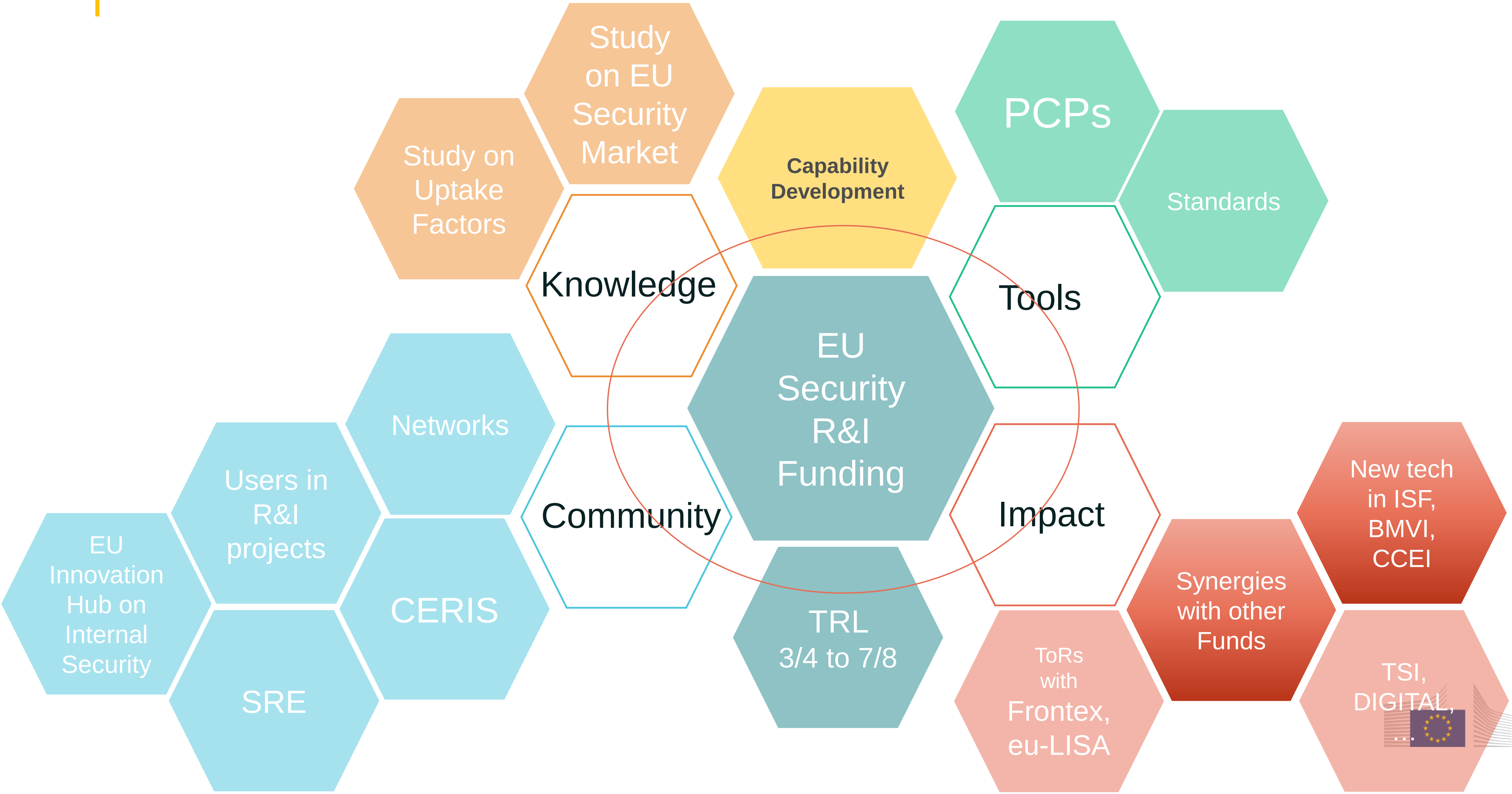
CS- MAIN IMPACTS

- **Expected impact of the Horizon Europe Strategic Plan 2021-2024:**
  - Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats.
- **Specific impacts:**
  - generate knowledge and value in cross-cutting matters in order to avoid sector-specific bias and to break silos that impede the proliferation of common security solutions;
  - strengthen key pillars of the research and innovation cycle to increase the effectiveness and efficiency of its contribution to the development of security capabilities;
  - support innovation uptake and go-to-market strategies with the aim of paving the way towards an increased industrialisation, commercialisation, adoption and deployment of successful outcomes of security research, thus contributing to reinforce the competitiveness of EU security industry and safeguard the security of supply of EU products in key security areas.

Funding priorities:

Work Programme 2023-24

Addressing civil security innovation in the EU



Cluster 3 Work Programme 2023-2024

Topics under calls 2023 (open 29 June / close 23 November 2023)

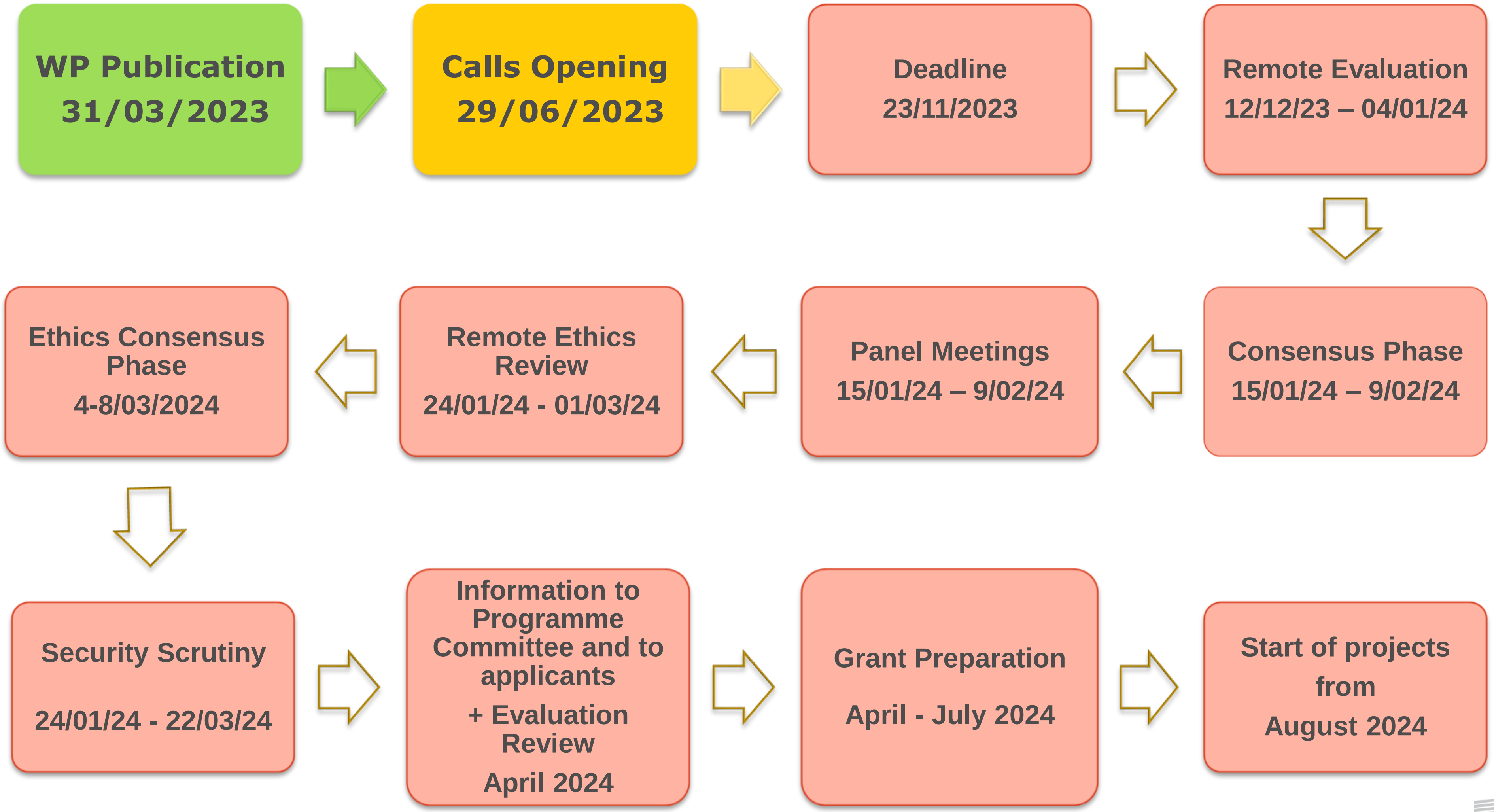
Topics under calls 2024 (open 27 June / close 20 November 2024)

FCT sub-areas	Topic	EUR (mil.)	EUR (mil.) per grant	Type of Action / TRL
Modern information analysis for fighting crime and terrorism	Processing of large, complex and unstructured datasets resulting from criminal investigations, while reconciling big data analysis and data protection	7		IA / 7-8
	Mitigating new threats and adapting investigation strategies in the era of Internet of Things	5		RIA / 5-6
Improved forensics and lawful evidence collection	A harmonized European forensics approach on drugs analysis	9	4.5	IA / 6-7
	Open topic	9	4.5	RIA / 5-7
	Lawful evidence collection in online child sexual abuse investigations, including undercover	3.7		RIA / 5-6
Enhanced prevention, detection and deterrence of societal issues related to various forms of crime	New methods and technologies in service of community policing and transferable best practices	4		RIA / 6-7
	Radicalisation and gender	3		RIA / 5-6
	Combating hate speech online and offline	8		IA / 6-7
	Open Topic	6	3	RIA / 5-6
Increased security of citizens against terrorism, including in public spaces	Open topic	4		RIA / 5-7
	CBRN-E detection capacities in small architecture	6		IA / 6-8
Organised crime prevented and combated	Crime as a service	4		RIA / 5-6
Citizens are protected against cybercrime	Enhancing tools and capabilities to fight advanced forms of cyber threats and cyber-dependent crimes	8	4	RIA / 5-6
	Tracing of cryptocurrencies transactions related to criminal purposes	6		IA / 6-7
BM sub-areas				
	Open topic	6	3	RIA / 4-6
Efficient border surveillance and maritime security	Capabilities for border surveillance and situational awareness	8	4	IA
	Identify, inspect, neutralise Unexploded Ordnance (UXO) at sea	5		RIA
	Interoperability for border and maritime surveillance and situational awareness	6	6	IA
Secured and facilitated crossing of external borders	Beyond the state-of-the-art “biometrics on the move” for border checks	6	3	RIA
	Advanced user-friendly, compatible, secure identity and travel document management	6		IA
	Integrated risk-based border control that mitigates public security risk, reduces false positives and strengthens privacy	5		IA
Better customs and supply chain security	Interoperability of systems and equipment at tactical level; between equipment and databases; and/or between databases of threats and materials	6		IA
	Detection and tracking of illegal and trafficked goods	6	3	RIA

Cluster 3 Work Programme 2023-2024

INFRA sub-areas	Topic	EUR (mil.)	EUR (mil.) per grant	Type of Action / TRL
Improved preparedness and response for large-scale disruptions of European infrastructures	Facilitating strategic cooperation to ensure the provision of essential services	5		IA / 6-8
	Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures	9.5	4.75	IA / 6-8
	Open topic	5		IA / 6-8
Resilient and secure urban areas and smart cities	Resilient and secure urban planning and new tools for EU territorial entities	6		IA / 6-8
	Advanced real-time data analysis used for infrastructure resilience	5		RIA / 5-6
DRS sub-areas				
Societal Resilience: Increased risk Awareness and preparedness of citizens	Improving social and societal preparedness for disaster response and health emergencies	8	4	RIA
Improved Disaster Risk Management and Governance	Design of crisis prevention and preparedness actions in case of digital breakdown (internet, electricity etc.)	4		RIA
	Prevention, detection, response and mitigation of chemical, biological and radiological threats to agricultural production, feed and food processing, distribution and consumption	8	4	RIA
	Open topic	6	3	RIA
Improved harmonisation and/or standardisation in the area of crisis management and CBRN-E	Operability and standardisation in response to biological toxin incidents	6		RIA
	Internationally coordinated networking of training centres for the validation and testing of CBRN-E tools and technologies in case of incidents, with consideration of human factors	4		IA
	Harmonised / Standard protocols for the implementation of alert and impact forecasting systems as well as transnational emergency management in the areas of high-impact weather / climatic and geological disasters	6	3	IA
Strengthened capacities of first and second responders	Robotics: Autonomous or semi-autonomous UGV systems to supplement skills for use in hazardous environments	8	4	RIA / 6-8
	Increased technology solutions, institutional coordination and decision-support systems for first responders of last-kilometer emergency service delivery	3.5		RIA
	Hi-tech capacities for crisis response and recovery after a natural-technological (NaTech) disaster	4		RIA / 5-7
	Cost-effective sustainable technologies and crisis management strategies for RN large-scale protection of population and infrastructures after a nuclear blast or nuclear facility incident	6		RIA / 6-8
SSRI sub-area				
Increased innovation uptake	Open grounds for pre-commercial procurement of innovative security technologies	2	1	CSA
	Accelerating uptake through open proposals for advanced SME innovation	4.5	1.5	IA / 6-8
	Demand-led innovation through public procurement	10.5	5.25	PCP / 6-8
	Accelerating uptake through open proposals for advanced SME innovation	6	1.5	IA / 6-7
CS sub-areas				
Systems Security and Security Lifetime Management, Secure Platforms, Digital Infrastructures	Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)	28	4-6	IA
	Approaches and tools for security in software and hardware development and assessment	37	4-6	IA
Privacy-preserving and identity technologies	Privacy-preserving and identity management technologies	15,7	2-4	IA
Cryptography	Post-quantum cryptography transition	23,4	4-6	RIA
Secured disruptive technologies	Security of robust AI systems	15	4-6	RIA

2023 Call evaluation - Timeline of main steps



WP Publication
31/03/2023

Calls Opening
29/06/2023

Deadline
23/11/2023

Remote Evaluation
12/12/23 – 04/01/24

Consensus Phase
15/01/24 – 9/02/24

Panel Meetings
15/01/24 – 9/02/24

Remote Ethics Review
24/01/24 - 01/03/24

Ethics Consensus Phase
4-8/03/2024

Security Scrutiny
24/01/24 - 22/03/24

Information to Programme Committee and to applicants
+ Evaluation Review
April 2024

Grant Preparation
April - July 2024

Start of projects from
August 2024

Who is eligible for funding?

EU COUNTRIES

- Member States (MS) including their outermost regions
- The Overseas Countries and Territories (OCTs) linked to the MS

NON-EU COUNTRIES*

- Countries associated to Horizon Europe (AC)
- Low and middle income countries: See HE Programme Guide
- Other countries when announced in the call or exceptionally if their participation is essential

SPECIFIC CASES

- Affiliated entities established in countries eligible for funding
- EU bodies
- International organisations (IO): International European research organisations are eligible for funding, Other IO are not eligible (only exceptionally if participation is essential), IO in a MS or AC are eligible for funding for Training and mobility actions and when announced in the call conditions

* Eligibility exception (Article 22.5): HORIZON-CL3-2023-INFRA-01-01: Facilitating strategic cooperation to ensure the provision of essential services" limited to legal entities established in Member States only.

General eligibility conditions

Consortium composition (collaborative projects) for RIA/IA

- ➢ at least **one** independent legal entity established in a **Member State**, and
- ➢ at least **two** other independent legal entities each established either in a different **Member State** or an **Associated Country**

Consortium composition (collaborative projects) for CSA

- ➢ at least **one** independent legal entity established in a **Member State or in an Associated Country** (HORIZON-CL3-2023-SSRI-01-01)
- ➢ For this type of actions, third Countries and International Organisations are not eligible for (exceptional) funding!

Evaluation criteria

Excellence - **Impact** - **Quality and efficiency of the implementation**

- Evaluation criteria are **adapted** to each **type of action**, as specified in the WP
- Each criterion includes the '**aspects to be taken into account**'. The same aspect is not included in different criteria, so it is not assessed twice
- **Open Science** practices are assessed as part of the scientific methodology in the excellence criterion
- **New approach to impact**: Key Impacts Pathways (KIPs)
- The assessment of the **quality of applicants** is assessed under 'implementation', rather than as a separate binary assessment of operational capacity
- Assessment of **management structures** has been removed

Evaluation Criteria (RIA/IA)

Excellence

- ✓ Clarity and pertinence of the **project's objectives**, and the extent to which the proposed work is ambitious, and goes beyond the state of-the-art.
- ✓ Soundness of the proposed **methodology**, including the underlying concepts, models, assumptions, inter-disciplinary approaches, appropriate consideration of the **gender dimension** in research and innovation content, quality of **open science practices** including sharing and management of research outputs and engagement of citizens, civil society and end users where appropriate

Impact

- ✓ Credibility of the **pathways** to achieve the expected **outcomes and impacts** specified in the work programme, and the likely scale and significance of the contributions due to the project.
- ✓ Suitability and quality of the **measures to maximize expected outcomes and impacts**, as set out in the dissemination and exploitation plan, including communication activities.

NB: New approach to impact: Key Impacts Pathways (KIPs)

Quality and efficiency of the implementation

- ✓ Quality and effectiveness of the **work plan**, assessment of risks, and appropriateness of the effort assigned to work packages, and the resources overall.
- ✓ Capacity and role of each **participant**, and extent to which the **consortium** as a whole brings together the necessary expertise

NB: The quality of applicants is assessed under 'implementation', rather than as a separate binary assessment of operational capacity. Assessment of management structures has been removed.

Evaluation Criteria (CSA)

Excellence

- ✓ Clarity and pertinence of the project's objectives.
- ✓ Quality of the proposed coordination and/or support measures including soundness of methodology.

Impact

- ✓ Credibility of the **pathways** to achieve the expected **outcomes and impacts** specified in the work programme, and the likely scale and significance of the contributions due to the project.
- ✓ Suitability and quality of the **measures to maximize expected outcomes and impacts**, as set out in the dissemination and exploitation plan, including communication activities.

NB: New approach to impact: Key Impacts Pathways (KIPs)

Quality and efficiency of the implementation

- ✓ Quality and effectiveness of the **work plan**, assessment of risks, and appropriateness of the effort assigned to work packages, and the resources overall.
- ✓ Capacity and role of each **participant**, and extent to which the **consortium** as a whole brings together the necessary expertise

NB: The quality of applicants is assessed under 'implementation', rather than as a separate binary assessment of operational capacity. Assessment of management structures has been removed.

Ethics review

Same criteria as in H2020

For all activities funded, ethics is an integral part of research from beginning to end, and ethical compliance is essential to achieve real research excellence. An ethics review process is carried out systematically in all Horizon Europe proposals, based on a self-assessment included in the proposal.

Adapted following lessons learnt

Possible simplification of the process by

- Focusing mainly on complex/serious cases
- Optimising the number of ethics requirements in funded projects

Security scrutiny

New in Horizon Europe

Security issues will be checked systematically in all Horizon Europe proposals (in H2020 only proposals submitted to topics flagged as ‘security-sensitive’ were checked). The checks are based on a self-assessment included in the proposal.

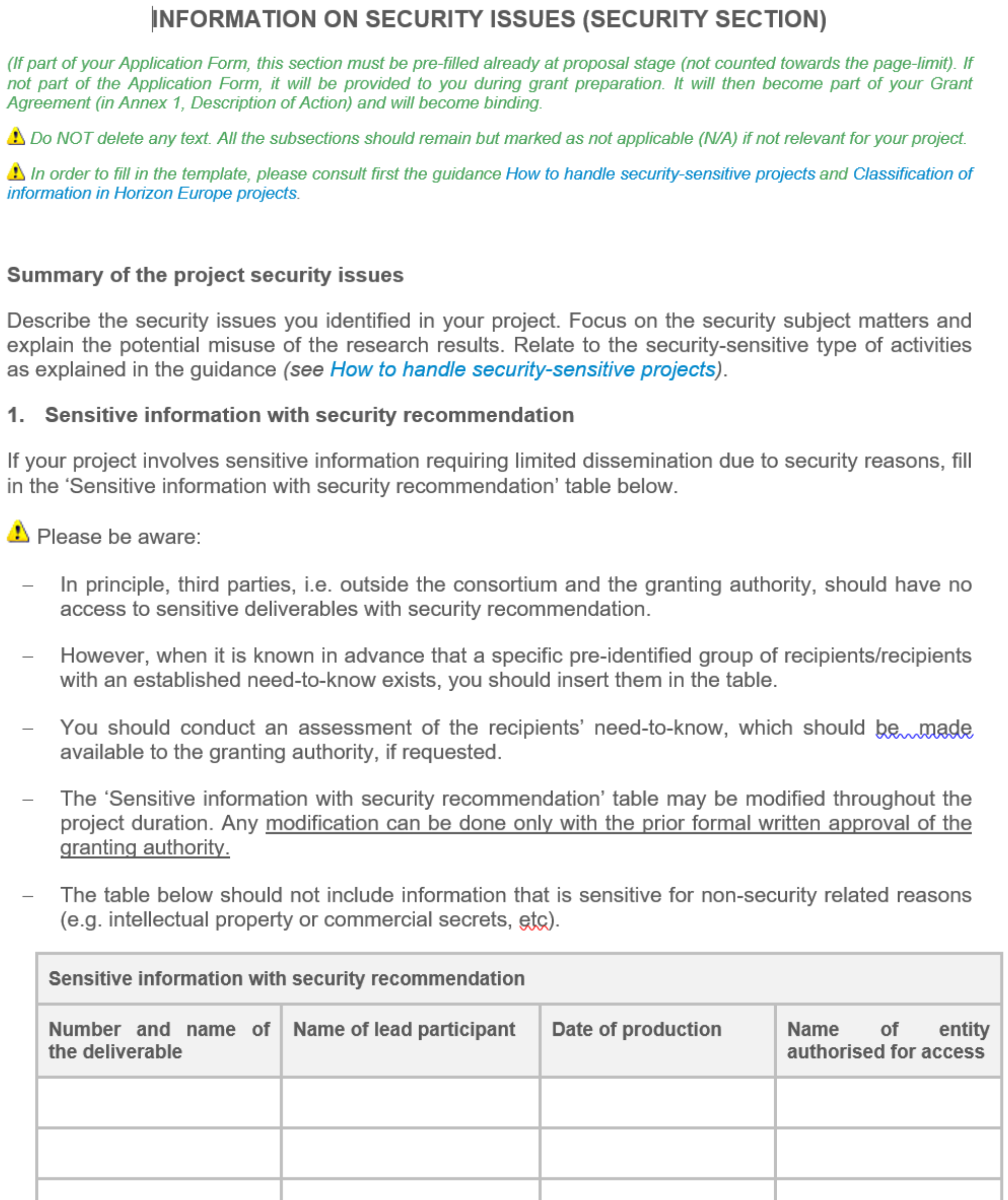
The checks based on the self-assessment may trigger an in-depth security scrutiny

Security scrutiny – Annex

Annex to fill in and include in your proposal (mandatory)

The focus is on:

- Whether the proposal uses or generates **EU classified information**
- Potential of **misuse of results** (that could be channeled into crime or terrorism)
- Whether activities involve information or materials **subject to national security restrictions**



INFORMATION ON SECURITY ISSUES (SECURITY SECTION)

(If part of your Application Form, this section must be pre-filled already at proposal stage (not counted towards the page-limit). If not part of the Application Form, it will be provided to you during grant preparation. It will then become part of your Grant Agreement (in Annex 1, Description of Action) and will become binding.

⚠ *Do NOT delete any text. All the subsections should remain but marked as not applicable (N/A) if not relevant for your project.*

⚠ *In order to fill in the template, please consult first the guidance How to handle security-sensitive projects and Classification of information in Horizon Europe projects.*

Summary of the project security issues

Describe the security issues you identified in your project. Focus on the security subject matters and explain the potential misuse of the research results. Relate to the security-sensitive type of activities as explained in the guidance *(see How to handle security-sensitive projects)*.

1. Sensitive information with security recommendation

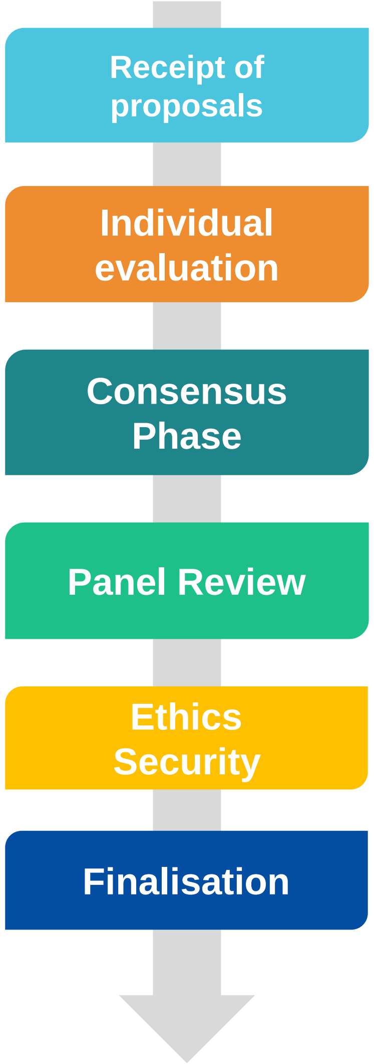
If your project involves sensitive information requiring limited dissemination due to security reasons, fill in the 'Sensitive information with security recommendation' table below.

⚠ Please be aware:

- In principle, third parties, i.e. outside the consortium and the granting authority, should have no access to sensitive deliverables with security recommendation.
- However, when it is known in advance that a specific pre-identified group of recipients/recipients with an established need-to-know exists, you should insert them in the table.
- You should conduct an assessment of the recipients' need-to-know, which should be made available to the granting authority, if requested.
- The 'Sensitive information with security recommendation' table may be modified throughout the project duration. Any modification can be done only with the prior formal written approval of the granting authority.
- The table below should not include information that is sensitive for non-security related reasons (e.g. intellectual property or commercial secrets, etc).

Sensitive information with security recommendation			
Number and name of the deliverable	Name of lead participant	Date of production	Name of entity authorised for access

Standard evaluation process



Receipt of proposals

Admissibility/eligibility check
Allocation of proposals to evaluators

Individual evaluation

Experts assess proposals **individually** (Minimum of three experts per proposal)

Consensus Phase

All individual experts discuss together to agree on a **common position**, including comments and scores for each proposal

Panel Review

The panel of experts reach an **agreement** on the scores and comments for all proposals within a call, checking **consistency across the evaluations**, if necessary, resolve cases where evaluators were unable to agree. Rank the proposals with the same score

Ethics Security

The proposals potentially selected for funding go through the Ethics screening and Security Scrutiny

Finalisation

The Commission/Agency reviews the results of the experts' evaluation and puts together the **final ranking list**

European Commission

Dual use and Exclusive focus on civil applications

- The assessment on **‘exclusive focus on civil applications’** aspects is carried out by the technical evaluators in the form of additional question
- For ‘**dual use**’, no additional question for experts in the evaluation. The declaration mentioned above will be sufficient with no further checks in evaluation or grant management
- **Opinion of experts indicating if removing the activities that do not have an exclusive focus on civil applications would lead to lower evaluation scores.**

Artificial intelligence

Under Horizon Europe, the technical robustness* of the proposed AI based systems is evaluated under the excellence criterion.

- Experts must answer an additional question on whether the activities proposed involve the **use and/or development of AI-based systems and/or techniques**.
- The aim is to bring to **experts' attention** that they must **assess the technical robustness** of the proposed AI-system as part of the excellence criterion (if applicable).
- Also the answer to this question aims at ensuring a **proper follow-up** of any aspects related to **Artificial Intelligence** in projects funded under Horizon Europe.

(*) Technical robustness refers to technical aspects of AI systems and development, including resilience to attack and security, fullback plan and general safety, accuracy, reliability and reproducibility.

HORIZON EUROPE
CIVIL SECURITY FOR SOCIETY

CROSS CUTTING ASPECTS

“Cross-cutting issues”

Gender dimension in R&I content

Addressing the gender dimension in research and innovation entails taking into account sex and gender in the whole research & innovation process

Social Sciences and Humanities

Assessing the effective **contribution of social science and humanities disciplines** and expertise as part of the scientific methodology of the project.

International Cooperation

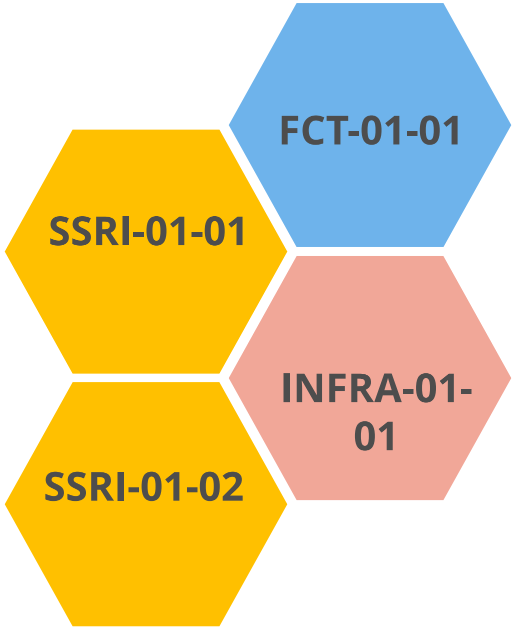
To achieve the right balance between the need to exchange with key international partners (including with relevant international organisations) while at the same time ensuring the protection of the EU security interest

Gender dimension in R&I content

Addressing the gender dimension in research and innovation entails taking into account sex and gender in the whole research & innovation process

The integration of the gender dimension into R&I content is **mandatory**, unless it is explicitly mentioned in the topic description

Topics flagged as not gender relevant



General eligibility conditions

Gender Equality Plan

Moreover, participants that are public bodies, research organisations or higher education establishments from Members States and Associated countries **must have a gender equality plan**, covering minimum process-related requirements.

- A self-declaration will be requested at proposal stage (for all types of participants)

- Included in the entity validation process (based on self-declaration)

Social Sciences and Humanities (SSH)

Assessing the effective **contribution of social science and humanities disciplines** and expertise as part of the scientific methodology of the project.

When the integration of SSH is required, **applicants have to show the roles of these disciplines or provide a justification if they consider that it is not relevant for their project**.

A proposal without a sufficient contribution/integration of SSH research and competences will receive a lower evaluation score.

CL3 Topics flagged as SSH relevant

FCT-01-03

DRS-01-04

DRS-01-01

INFRA-01-02

DRS-01-05

DRS-01-02

International Cooperation

To achieve the right balance between the need to exchange with key international partners (including with relevant international organisations) while at the same time ensuring the protection of the EU security interest

Cooperation can include sharing knowledge, experiences, expertise and mutual learning

International cooperation is explicitly encouraged only where appropriate and specifically supporting ongoing collaborative activities

Topics where International Cooperation is envisaged

DRS-01-04

DRS-01-01

DRS-01-05

DRS-01-02

Lump Sum topics

Lump sum evaluation and grant agreement follow standard approach with the same:

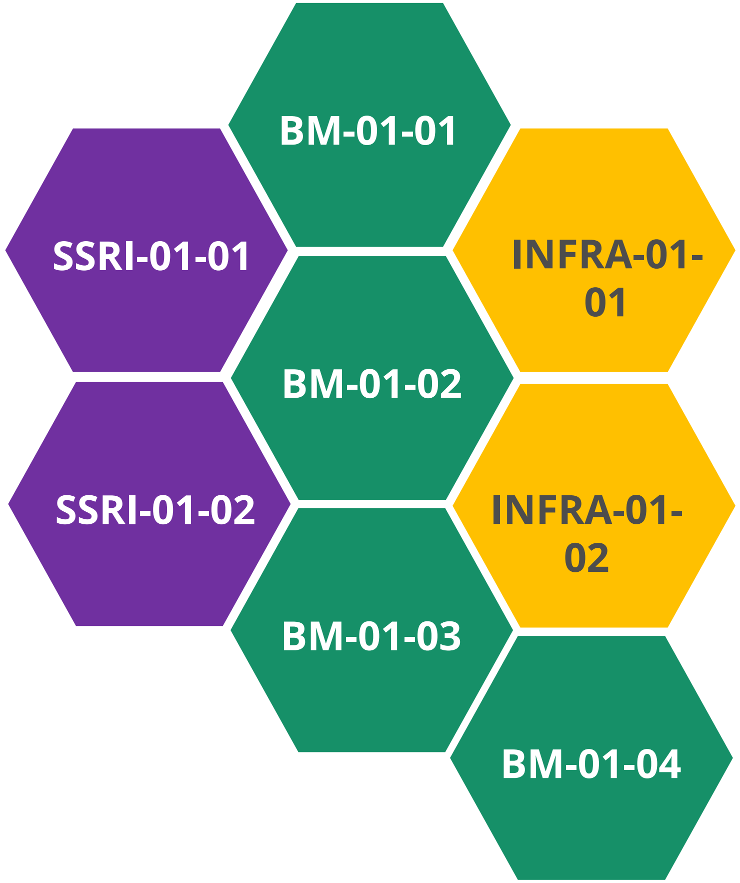
- ✓ Evaluation criteria
- ✓ Pre-financing and payment scheme
- ✓ Reporting periods and technical reporting, **though focusing on completion of work packages**

One lump sum share is fixed in the grant agreement for each work package:

Work package completed payment

- Payments do not depend on a successful outcome, but on the completion of activities
- Work packages can be modified through amendments (e.g. to take into account new scientific developments)

CL3 Topics flagged for Lumps SUM



BM-01-01

SSRI-01-01

INFRA-01-01

BM-01-02

SSRI-01-02

INFRA-01-02

BM-01-03

BM-01-04

HORIZON EUROPE

Lump Sum Topics

European Commission

Why using lump sum funding?

Significant simplification potential:

- Despite all simplification, funding based on reimbursement of incurred costs stays complex and error-prone
- Lump sum project funding removes all obligations on actual cost reporting and financial ex-post audits – i.e. a **major reduction of administrative burden**
- **Access to the programme becomes easier**, especially for small organisations and newcomers

Focus on performance:

- Shift from focus on financial management and checking costs to **focus on scientific-technical content** of the projects

European Commission

Basic principles of lump sum topics

✓ Applicants **define the lump sum** in their proposal. The type of lump sum is specified in the text of the topic

✓ In setting the lump sum, they are **free to define the amount** necessary to carry out your project

✓ The lump sum chosen must be **justified by the resources mobilised**

✓ Proposals are evaluated according to the **standard Horizon Europe evaluation procedures by independent experts**

✓ Proposals are assessed in terms of **Excellence, Impact and Quality and efficiency of the implementation**

Final Tips!

✓**Check carefully (including additional!) admissibility and eligibility conditions**

✓**Read carefully the topic description ("scope", "expected impact")** – will your proposal match the expectations?

✓**Fill in the proposal templates** by following the instructions

✓Fill in properly the mandatory annexes!

✓**Address thoroughly the selection and award criteria**

✓Respect the **page limits**

✓**Clearly describe what** you will achieve **and how** you will do it

✓Choose your **consortium based on your project needs** (e.g. no duplications or partners without clear responsibilities,...)

✓**Describe carefully the impact** (expected, societal, economic [IA: business analysis, market potential,..])

✓**Submit (a first version) well before the final deadline**

Research Enquiry Service

For questions about research and Horizon Europe, you can contact the Research Enquiry Service via the webform:

Research Enquiry Service (europa.eu)

More Information and resources

EU Innovation and Industry for Security

Community for European Research and Innovation for Security (CERIS)

Annual Security Research Event

National Contact points for EU security research

@EUHomeAffairs
#EUSecurityResearch #SecureSocieties

EUHomeAffairs

Enhancing security through R&I CSWD(2021)422

Frontex on EU research

Eu-LISA on EU research

EU Innovation Hub for Internal Security

Horizon Europe Cluster 3 “Civil Security for Society” (2023-2024 Work Programme)
&
Cluster 3 Info Day and brokerage event 2023

EU Funding & Tenders Portal

Thank you