European Commission

Results and Indicators for Development

Cybersecurity

International Cooperation and Development

Results and Indicators for Development

General Introduction

This **guidance for action design** has been developed by DEVCO Unit 04 "Evaluation and Results" jointly with DEVCO Thematic Units.

It is **addressed** to all colleagues involved in the preparation of action documents and project documents and offers a handy tool to develop solid logical framework matrices. It identifies clear and measurable results statements that are in line with DEVCO policy priorities, as well as with the UN Sustainable Development Goals (SDGs), along with a range of good indicators to monitor progress. It will be updated regularly to reflect evolving priorities.

Its **main objective** is to enhance the quality of DEVCO interventions – both in terms of design as well as of monitoring and reporting in the course of implementation.

The **need for this type of guidance** was identified in the framework of the results-reporting process led by DEVCO 04, as well as through its systematic review of all action documents presented to Quality Review Group meetings.

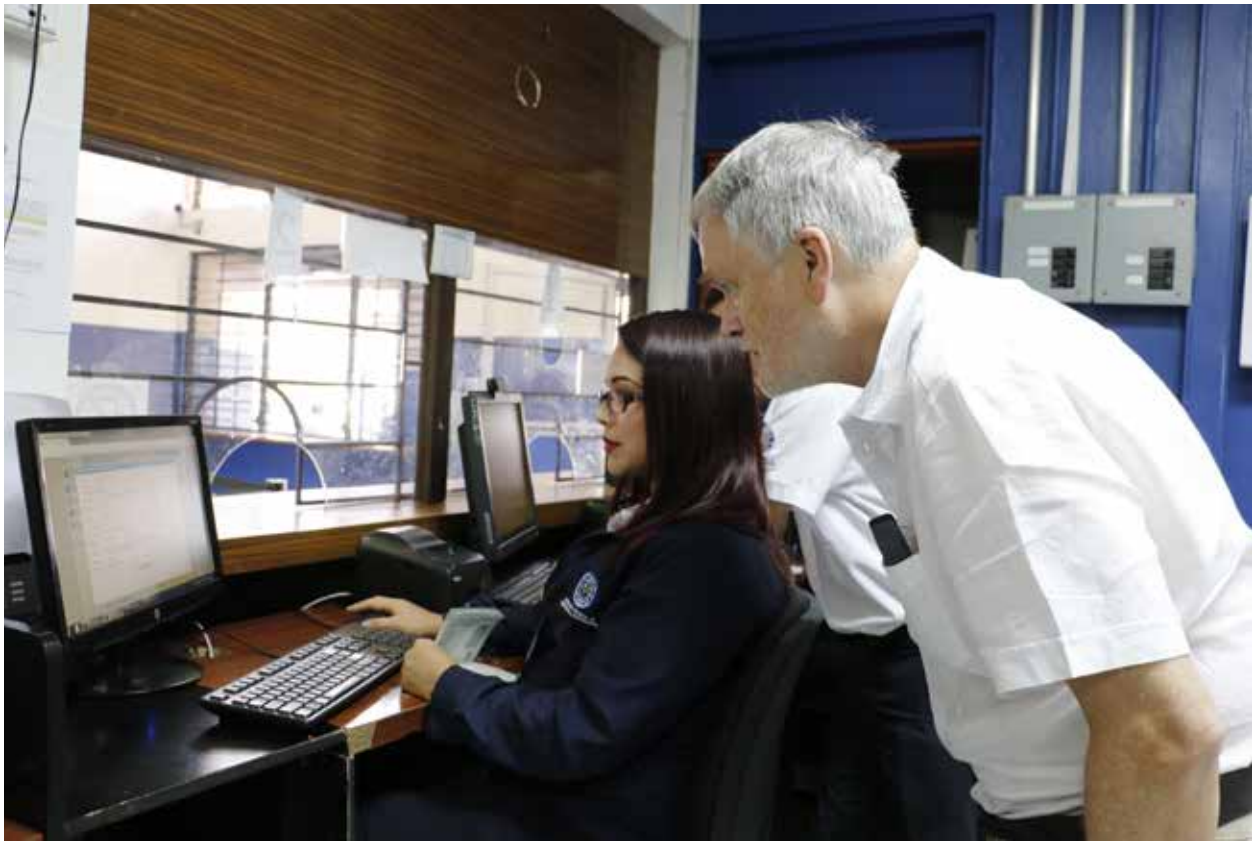
The present guidance covers DEVCO strategies in various sectors, and presents for each sector:

1. EU policy priorities: a short narrative explaining EU policy priorities and commitments as articulated in key policy and strategic documents.

2. Results Chain: a diagram showing the main results (impact, outcomes, outputs) that EU development interventions are expected to achieve in the sector, reflecting EU policy priorities and commitments.

3. List of Sector Indicators: examples of measurable indicators associated to each result statement are provided, that may be used in Logframe Matrices at project/ programme level.

1. EU Policy Priorities



Ever-evolving Information and Communications Technologies (ICTs) have revolutionised how we work over the past 20 years, resulting in profound global implications and scale-up of digital technologies. However, risks and challenges associated with improved access to ICTs and the growing of internet penetration are often underestimated. Therefore, cyber capacity building is crucial to promote cyber security across the globe.

Since the adoption of its Cybersecurity Strategy[1] in 2013, the EU has been leading on international cyber capacity building and systematically linking these efforts with its development cooperation funds. Moreover, in 2017 there was a clear recognition at the EU level that cybersecurity should be considered a transversal issue in development cooperation that can contribute to the realisation of the 2030 Agenda for Sustainable Development[2], as stipulated in the EU's Digital4Development[3] policy framework. In the cybersecurity sector, the desired impact/overall objective is to provide the citizens of developing countries an open, free, secure, resilient and peaceful cyberspace. Reference to this can be found as a target under SDG 9 "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation", as well as under SDG 4 "Quality education", SDG 8 "Decent work and economic growth", SDG 16 "Peace, Justice and Strong Institutions".

1. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

2. https://sustainabledevelopment.un.org/post2015/transformingourworld

3. https://ec.europa.eu/europeaid/sites/devco/files/swd-digital4development_part1_v3.pdf

The significance of efforts to build national resilience in third countries as a means of increasing the level of cybersecurity globally, with positive consequences for the EU, was also recognised in the 2017 Joint Communication on "Resilience, deterrence and defence: Building strong cybersecurity for the EU"[4].

EU interventions in this field strengthen the legislative, institutional and civil society capacities for promoting cyber security, cyber hygiene and awareness. They also help to develop new mechanisms for effective information sharing, consultation and coordination on cyber incidents.

The outcomes of these interventions include the adoption and implementation of a coherent, holistic and actionable national approach to cyber resilience; the operationalisation of cyber crisis management structures; increased trust of users, organisations, and companies in the use of cyberspace; as well as the alignment of legislation on cybercrime and electronic evidence with international standards.

The desired long-term impact is that citizens of developing countries enjoy an open, free, secure, resilient and peaceful cyberspace.

EU strategic priorities

In order to leverage the threats and challenges related to cybersecurity, EU action is structured around the following strategic priorities, as defined in the Joint Communication:

- Promoting legislative reforms and strengthening the capacity of decision-makers to design and implement cyber laws and policies in line with the Budapest Convention[5] and human rights conventions;
- Supporting an overarching strategic framework and strengthening institutional capacity to address cyber risks in a holistic way, including in public service delivery;
- Developing education, professional training and expertise in this field and improving cyber hygiene and awareness of individual users;
- Enhancing mechanisms for effective information sharing, consultation and coordination on cyber incidents between stakeholders (private sector, civil society and government bodies).

4. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN%0D

5. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

2. Results Chain

OUTPUTS

- Strengthened capacities of decision-makers to design and implement cyber laws and policies in line with the Budapest Convention and human rights conventions
- Strengthened institutional capacity to address cyber risks in a holistic way, including in public service delivery
- Skills of law enforcement, prosecutors and judges to investigate, prosecute and adjudicate cybercrime cases are improved
- Protection of critical information infrastructure is enhanced
- Mechanisms for effective information sharing, consultation and coordination on cyber incidents between stakeholders (private sector, civil society and government bodies) are in place
- Participation in international operations and/or joint investigations targeting cybercrime is promoted
- Improved cyber hygiene and awareness of individual users (e.g. employees, citizens, students)

Specific objectives - OUTCOMES

- A coherent, holistic and actionable national approach to cyber resilience is adopted and implemented
- Cyber crisis management structures are operational
- Increased trust of users, organisations, and companies in the use of cyberspace
- Legislation on cybercrime and electronic evidence is aligned with existing international legal standards and implemented

Overall objective - IMPACT

Citizens of developing countries enjoy an open, free, secure, resilient and peaceful cyberspace

Related SDGs and Targets

Main impact

4. Quality education

8. Decent work and economic growth

9. Industry, innovation and infrastructure

16. Peace, Justice and Strong Institutions

3. List of Sector Indicators

Result	Indicators
Impact **Citizens of developing countries enjoy an open, free, secure, resilient and peaceful cyberspace**	◤ Country score in the ITU Global Cybersecurity and Cyberwellness Index (Score) *data source* Global Cybersecurity and Cyberwellness Index website ◤ Country score in the World Economic Forum's Network Readiness Index (Score) *data source* Network Readiness Index ◤ Country score in the Freedom on the Net - Freedom House (Score: 0=Most Free, 100=Less Free) *data source* Freedom on the Net Report 2017 Report https://freedomhouse.org/report/freedom-net/freedom-net-2017 ◤ Existence of independent national human rights institutions in compliance with the Paris Principles (Qualitative) *data source* Secondary
Result	**Indicators**
Outcome **A coherent, holistic and actionable national approach to cyber resilience is adopted and implemented**	◤ Extent to which cybercrime is mentioned in a national strategic framework / cyber strategy (Qualitative) *data source* Analysis of the national strategic framework to be commissioned by the Action ◤ Status of a comprehensive national strategic framework on cybersecurity (Qualitative) *data source* National Strategy on Cybersecurity adopted by the Government ◤ Status of an implementation plan (or roadmap) for delivering on the strategic commitments in the field of cybersecurity (Qualitative) *data source* Roadmap document adopted by the government ◤ Status of a cybercrime/high-tech crime units in the relevant government institutions (Qualitative) *data source* Project reports ◤ Number of locally-based organisations that contribute to dialogue with central authorities and cybersecurity actors (Number of) *data source* Expert survey/mapping to be commissioned by the Action (at the beginning and end of the implementation)

Result	Indicators
Outcome **Cyber crisis management structures are operational**	◤ Existence of a cyber-related budget line (in particular linked to CERT/CSIRT) in the national budget (Qualitative) *data source* National budget ◤ Amount of the national budget allocated to agencies with cybersecurity competence (EUR) *data source* National budget (a specialized study may need to be commissioned by the Action) ◤ Status of national body mandated with cyber crisis management (Qualitative) *data source* National legislation ◤ Status of policy provisions defining the responsibilities and resources of institutions competent for prevention, protection and recovery from cyber attacks and/or accidental failures (Qualitative) *data source* National legislation and policies ◤ Status of cyber-related inspection and/or audit services within the individual institutions and bodies responsible for incident and crisis management (Qualitative) *data source* National legislation and policies

Result	Indicators
Outcome **Increased trust of users, organisations, and companies in the use of cyberspace**	◤ Percentage of users / organisations / companies that report trust in the use of the cyberspace (Percentage) *data source* Surveys of users / organisations / companies to be commissioned by the Action ◤ Percentage of internet penetration in the country (Percentage) *data source* https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=AF ◤ Percentage of population that expresses confidence in the capacity of the law enforcement and judicial bodies to tackle cybercrime effectively (Percentage) *data source* Public perception surveys to be conducted at the start and the end of the project (disaggregated by sex and age) ◤ Number of individuals (disaggregated by sex), companies, and organisations falling victims to cyber attacks (Number of) *data source* National reports or survey to be commissioned by the Action

Result	Indicators
Outcome **Legislation on cybercrime and electronic evidence is aligned with existing international legal standards and implemented**	◤ Status of legal provisions / regulations on cybercrime and electronic evidence (Qualitative) *data source* National legislation and policies ◤ Status of the accession to/ratification of the Budapest Convention (Qualitative) *data source* National legislation ◤ Number of domestic and/or international prosecutions and cases adjudicated on cybercrime (Number of) *data source* Reports from the Ministry of Justice ◤ Percentage of cybercrime complaints that are investigated (Percentage) *data source* Reports by cybercrime units and prosecution offices

Result	Indicators
Output **Strengthened capacities of decision- makers to design and implement cyber laws and policies in line with the Budapest Convention and human rights conventions**	◤ Status of the national strategic framework on cybersecurity (Qualitative) *data source* Draft National Strategy on Cybersecurity, Action's progress reports ◤ Status of legislation and/or regulation addressing cyber risks (Number of) *data source* Draft laws, Action's progress reports ◤ Status of legislation and/or regulation addressing Critical Information Infrastructure Protection (CIIP) (Number of) *data source* Draft laws, Action's progress reports ◤ Status of cyber risk management framework/ guidelines for national authorities (Qualitative) *data source* Draft Guidelines, Action's progress reports ◤ Number of decision-makers trained by the Action on the importance of cyber policies, design and implementation of national cybersecurity strategies (disaggregated by sex) (Number of) *data source* Database of training participants maintained by the Action (disaggregated by sex) ◤ Status of constitutional, statutory, policy guarantees for cybercrime and electronic evidence legislation (Qualitative) *data source* Action's progress reports ◤ Status of regulations on the cybersecurity technical standards in line with the international best practices (Qualitative) *data source* Action's progress reports ◤ Status of assessment of existing legislation for compatibility with the Budapest Convention (Qualitative) *data source* Assessment to be commissioned by the Action ◤ Extent to which provisions promoting cyber hygiene and technical standards in line with international best practices are integrated in draft/revised laws, regulations and government tenders (Qualitative) *data source* Assessment of legislation and regulations to be commissioned by the Action; draft laws and regulations produced with the Action's support ◤ Number of staff in Ministries/ Parliament mentored by the Action on legislative/ regulatory measures on cyber risks (disaggregated by sex) (Number of) *data source* Database of training participants maintained by the Action (disaggregated by sex) ◤ Extent of application of the national cooperation framework/guidelines in case of large scale cyber incident or crisis (Qualitative) *data source* Study to be commissioned by the Action

Result	Indicators
Output **Strengthened institutional capacity to address cyber risks in a holistic way, including in public service delivery**	◤ Number of institutions and organisations participating in periodic cyber risk assessments with support of the Action (Number of) *data source* Action's progress reports ◤ Number of cyber risk assessments conducted with support of the Action (Number of) *data source* Action's progress reports ◤ Number of government representatives trained/mentored by the Action on cyber hygiene practices and technical standards (disaggregated by sex) (Number of) *data source* Database of training participants maintained by the Action (disaggregated by sex)

Result	Indicators
Output **Skills of law enforcement, prosecutors and judges to investigate, prosecute and adjudicate cybercrime cases are improved**	◤ Number of requests handled by national 24/7 points of contact with support of the Action (Number of) *data source* Action's progress reports ◤ Number of table top exercises or mock operations supported by the Action (Number of) *data source* Action's progress reports ◤ Number of cybercrime units participating in domestic and international investigations thanks to support of the Action (Percentage) *data source* Action's progress reports

Result	Indicators
Output **Protection of critical information infrastructure is enhanced**	◤ Status of the list of national critical infrastructure (Qualitative) *data source* Infrastructure list compiled by the Action ◤ Status of governance framework for CIIP and cyber incident management (Qualitative) *data source* Action's progress reports ◤ Extent to which the national CERT/CSIRT has established parameters for organizational structure, human resources, tools and processes with the support of the Action (Qualitative) *data source* Action's progress reports ◤ Number of incident management/response cases monitored and handled by national CERT/CSIRT thanks to support of the Action (Number of) *data source* Action's progress reports ◤ Number of CERT/CSIRT employees mentored/trained with the support of the Action (disaggregated by sex) (Number of) *data source* Database of training participants maintained by the Action (disaggregated by sex)

Result	Indicators
Output **Mechanisms for effective information sharing, consultation and coordination on cyber incidents between stakeholders (private sector, civil society and government bodies) are in place**	◤ Number of MoUs between key private sector entities (CII operators, vendors) and governmental bodies signed with support of the Action (Number of) *data source* MoU documents ◤ Membership in FIRST and TF.CSIRT/TI certification obtained thanks to support from the Action (Qualitative) *data source* Action's progress reports ◤ Number of stakeholders participating in public consultations organised by the Action on the development of national cybersecurity strategic framework (disaggregated by sector and sex of participant) (Number of) *data source* Action's progress reports

Result	Indicators
Output **Participation in international operations and/or joint investigations targeting cybercrime is promoted**	◤ Number of joint operations and/or investigations conducted with support of the Action (Number of) *data source* Action's progress reports ◤ Number of international agreements/MoUs on combatting cybercrime signed between the private sector and CSOs with support of the Action (Number of) *data source* MoU documents ◤ Number of international police-to-police requests prepared with the support of the Action (Number of) *data source* Action's progress reports ◤ Status of public/public-private reporting mechanisms developed with the support of the Action (Qualitative) *data source* Action's progress reports

Result	Indicators
Output **Improved cyber hygiene and awareness of individual users (e.g. employees, citizens, students)**	◤ Extent to which cyber hygiene and awareness is mentioned in a national strategic framework (Qualitative) *data source* Action's progress reports ◤ Status of the Cyber Awareness Month campaign *data source* Action's progress reports ◤ Number of institutions, organisations, and individuals reached by the campaign promoting cyber hygiene and awareness (Number of) *data source* Action's progress reports ◤ Number of persons reached by the cyber awareness raising campaigns/training implemented with the support of the Action (Number of) *data source* Action's progress reports