ANNEX C1: Twinning Fiche

Project title: EU Support to Enhance Cybersecurity in Jordan

Beneficiary administration: National Cyber Security Centre (NCSC)

Twinning Reference: JO 20 ENI JH 01 23

Publication notice reference: EuropeAid/178636/ID/ACT/JO

EU funded project

TWINNING TOOL

List of Abbreviations

Acronym	Meaning
APT	Advanced Persistent Group
CNI	Critical National Infrastructure
CPS	Cyber Physical Systems
DCS	Distributed Control Systems
ICS	Industrial Control Systems
IIoT	Industrial Internet of Things
IT	Information Technology
JCCS	Jordanian Common Criteria Scheme
NCSC	National Cyber Security Center
OT	Operational Technology
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SOC	Security Operations Center

1. Basic Information

1.1 **Programme**:

Programme: Contribution for year 2020 to multiannual Measures Supporting the Implementation of the Partnership Priorities SIPP II (Reference: ENI/2020/ 042-608), indirect management with ex-ante control

For UK applicants: Please be aware that following the entry into force of the EU-UK Withdrawal Agreement[1] on 1 February 2020 and in particular Articles 127(6), 137 and 138, the references to natural or legal persons residing or established in a Member State of the European Union and to goods originating from an eligible country, as defined under Regulation (EU) No 236/2014[2] and Annex IV of the ACP-EU Partnership Agreement[3], are to be understood as including natural or legal persons residing or established in, and to goods originating from, the United Kingdom[4]. Those persons and goods are therefore eligible under this call.

1.2 Twinning Sector: Justice and Home Affairs.

1.3 EU funded budget: *EUR 1 400 000*

1.4 Sustainable Development Goals (SDGs): This twinning program will contribute to address the following Sustainable Development Goals: Peace, Justice and Strong Institutions.

2. Objectives

2.1 Overall Objective(s):

To contribute in the improvement of cybersecurity in Jordan to be in line with best international standards.

2.2 Specific objective:

Strengthen NCSC capacities to establish a Security Operation Center for Operational Technology (OT-SOC) and become National Cybersecurity Certification and Accreditation Centre.

2.3 The elements targeted in strategic documents i.e. National Development Plan/Cooperation agreement/Association Agreement/Sector reform strategy and related Action Plans:

- Cyber Security Law no. 16 for year 2019
- The National Cyber Security Strategy (2018-2023)
- **NCSC vision statement**
  Jordanian cyberspace is safe, reliable and resistant to threats.

[1] Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community.
[2] Regulation (EU) No 236/2014 of the European Parliament and of the Council of 11 March 2014 laying down common rules and procedures for the implementation of the Union's instruments for financing external action.
[3] Annex IV to the ACP-EU Partnership Agreement, as revised by Decision 1/2014 of the ACP-EU Council of Ministers (OJ L196/40, 3.7.2014)
[4] Including the Overseas Countries and Territories having special relations with the United Kingdom, as laid down in Part Four and Annex II of the TFEU.

- **NCSC Mission statement**
  "Building an effective cyber security system at the national level, developing and organizing it to protect the Kingdom from cyber threats and confront them efficiently and effectively in a way that guarantees the sustainability of work and the preservation of national security and the safety of people, property and information"

  Strategic Objectives
  - Building national capacities, raising awareness in the field of cybersecurity and developing scientific research capabilities
  - Governance of cybersecurity at the national level by strengthening the legal and regulatory frameworks for the national cyberspace and promoting compliance with them.
  - Identify National Critical Infrastructures and the requirements for their protection and sustainability
  - Responding to cyber threats by building and developing an effective and sustainable system for cyber operations.
  - Achieving a clear and comprehensive national cyber security Situational Awareness through effective management of cyber-threat intelligence information
  - Strengthening local, regional and international cooperation in the field of cybersecurity

  Operational Goals
  - Increasing national awareness of cyber security by holding educational initiatives including seminars and workshops.
  - Publishing regulations and guidelines for classifying and licensing cybersecurity service providers.
  - Contributing to the preparation and evaluation of legislations related to cyber security.
  - Forming cyber security policies and monitoring their implementation, as well as developing the required plans and programs for the implementation.
  - Determining cyber security standards and control.
  - Improving the level of cyber security for government institutions.
  - Developing monitoring capabilities to detect and respond to cyber incidents.
  - Maintaining and protecting NCSC networks and cyber operations systems.
  - Identifying critical infrastructures and establishing priorities and requirements for their protection and sustainability.
  - Issuing guidelines for protecting critical national infrastructures from cyber threats.
  - Maintaining coordination and cooperation with owners and operators of critical infrastructure.

3. Description

3.1 Background and justification

3.1.1 Background

The National Cybersecurity Centre (NCSC) was established in 2021 with the aim of oversighting the national cybersecurity functions through building an effective cyber security system at the national level, developing and organizing it to protect the Kingdom from cyber threats and confront them efficiently and effectively in a way that guarantees the sustainability of work and the preservation of national security and the safety of people, property and information.

In order for NCSC to achieve its goals mentioned within Jordanian cybersecurity law, it undertakes a number of tasks and powers including granting licenses and certifications for cybersecurity services, cybersecurity service providers, and cybersecurity products.

Currently, a large number of devices are being sold to markets with poor cybersecurity requirements, and consumers are unable to make the right decisions for purchasing secure devices Hackers generally look for the easiest systems to attack that will cause the most damage. Products have been designed to optimize functionality and cost over security. As a result, many of them have little to no security features built-in. This poses cybersecurity risks such as the compromise of consumers privacy and data.

NCSC is looking forward to become the National Cybersecurity Certification Center which focuses on the evaluation, certification and labelling of cybersecurity products. As new technology products are constantly coming to market, NCSC will offer and supports the use of Certification Schemes to provide assurance to customers that the product has been assessed to be more cyber secure. NCSC will operate the needed schemes to provide the security assurance that products have been tested and examined to determine that it is securely designed, implemented, and appropriate in mitigating cybersecurity threats.

First Stage (from 2008-2012)

The Council of Ministers authorized and distributed the National Information Security and Protection Policies in 2008 and government agencies must adhere to their implementation. In 2012, the national information security and cybersecurity strategy was authorized, aimed at ensuring information and cyber security. This strategy sought to achieve comprehensive information security from by collaborating and building partnerships with stakeholders, including the government and security agencies, the private sector, and international partners. It recommended building and developing the national cyber security system, and through which strategic objectives priorities for its implementation were defined.

Second Stage: Construction (from 2015 to 2018):

The Jordanian Armed Forces-Arab Army was authorized as the national body in charge of building and devolving national capacity in the area of cyber security in 2015. It launched the national program for cyber security, and as a result, the National Technical committee was established which included representatives from the security agencies ,the

Ministry of Digital Economy and Entrepreneurship, State Institutions ,National Information Technology center , Central Bank of Jordan, as well as the Public Security Directorate and General Intelligence and was led by the Jordanian Armed Forces (department).This committee was given the responsibility of creating the National Cyber Security Program's executive road plan. The first phase of the National Security Program's implementation was finished and overseen in the years (2017–2018) by the Jordanian Armed Forces in collaboration and coordination with all pertinent national authorities.

Third Stage (2019-2021)

The Cybersecurity Law No. 16 of 2019 was passed on September 16, 2019 which governs all cybersecurity-related issues and national cyber capabilities to coordinate, manage, and guide them in a way that ensures investment efforts are used effectively. This law established the national cybersecurity center that will be responsible for security-related tasks, and it also specifies the roles, duties, and obligations on the national level with collaboration among all parties involved in cyber security and national cyber security compatibly to prevent overlapping and intersections between responsibilities. The National Council for Cyber Security was established in accordance with Cyber Security Law No. 16 of 2019 led by a president who is chosen by a royal will, and nine members representing the following national authorities:1) Ministry of Digital Economy and Entrepreneurship, Central Bank of Jordan, Jordanian Armed Forces - Arab Army, 2) The General Intelligence Department, the Public Security Directorate, the National Center for Security and Crisis Management, and 3) Three members nominated by the Council of Ministers based on the recommendation of the President of the Council for a period of two years, subject to renewal for once, two of them had to be experts from the private sector. Article (5) of the Jordanian Cybersecurity, Law No. 16 of 2019 established NCSC and assigned it to be responsible for building national capacities for cyber security.

In 2020, the system of NCSC was approved which enables the center to manage, develop and implement its strategic and operational plans required to carry out its duties and responsibilities. In order for NCSC to manage and administer its internal affairs and perform its obligations and duties, the administrative organization system of the centre No.25 of 2022 was authorized in 2021. Currently, NCSC is working on monitoring IT networks in government entities by having continuous log monitoring, log correlation, Incident response, forensics and threat intelligence that is shared between all entities. all these services are provided by a centralized Security operations centre (SOC) and we are expanding our operations to cover other governmental entities. The incident response team dealt with more than 1000 attacks in 2022 targeting governmental sectors. The SoC team was able to detect incidents and remediate them in a timely fashion, which prevented the progress of attacks and service interruption. Building an Industrial OT network will increase the attack service, especially since those networks are targets for APT groups. Attacking these networks can cause catastrophic incidents that affect the citizen’s safety.

3.1.2 Justification

OT/ICS are general terms which encompass different kind of systems that are used to monitor and control physical processes and devices in industries such as manufacturing, energy, and transportation. These systems are critical to the operation of many organizations, and disruptions or failures can have significant consequences, including financial losses, damage to equipment and property, and even harm to people and the environment. The increasing reliance on OT in CNI has made the protection of these systems a top priority for the national security.

As OT network owners and operators aim to improve operational efficiency by adopting new technologies such as CPS and IIoT, the overall cybersecurity risk is increasing due to multiple factors such as the expansion of the OT cyberattack surface and the increasing susceptibility to IT commodity malware and ransomware, which can lead to a potential disruption of physical processes.

It is important to understand that cyber security for OT has a different mission and objective than cyber security for IT. While the security professionals for IT networks focus on the confidentiality and integrity of information, OT cyber security prioritizes the safety and availability of equipment and industrial processes.

- Current Situation:

The NCSC is currently working on monitoring IT networks in government entities by having continuous log monitoring, log correlation, Incident response, forensics and threat intelligence that is shared between all entities. These services are provided by a centralized SOC and which is expanding its scope of work to cover other governmental entities. The SOC dealt in 2022 with more than 1000 cyber-attacks which targeted the government sector. The SOC was able to detect incidents and remediate them in a timely fashion, which prevented the progress of attacks and service interruption. Some of these attacks were attributed to state-sponsored APT groups while others were related to cyber criminals.

- Future Plan:

The NCSC is to planning to develop an OT-SOC which is aimed to provide cyber security services to the CNI networks that are susceptible to cyber-attacks. This can include utility companies like water and electricity, which have distributed networks and relay heavily on OT systems like SCADA, DCS and PLC. The building of this SOC will involve developing the people, process and technology required to achieve the proposed capabilities.

- Services and Capabilities:

The list of proposed services will be similar to those delivered through the IT-SOC, which is covering the government sector. Some of these services are reactive in their nature while others are proactive.

- Incident Response: This includes developing the capability to conduct incident response activities and digital forensics investigations in case of suspected cyber-attacks within OT environments in the national CNIs.
- Security Assessment: This includes developing the capability to execute technical security assessment and architecture review of OT networks and provide recommendations to harden these networks.
- Threat Intelligence: This includes developing the capability to share advisories with the national stakeholders around cyber security threats affecting their OT environment.

- Real-time Monitoring: This includes developing the capability to monitor specific OT networks by deploying sensors and collection agents within the monitored OT networks to detect and respond to possible cyber breaches.
- Vulnerability Management: This capability includes developing asset inventories for the onboarded organizations and identifying vulnerabilities (tracking and scoring) associated with the discovered assets. It also provides reports and recommendations for remediations.

The Jordanian Common Criteria Scheme (JCCS) program is intended to increase the availability of certified cybersecurity products in the Jordanian market, and to provide consumers with greater assurance that the products they purchase meet a certain standard of security. By certifying products against national and international standards, the JCCS program can help to ensure that cybersecurity products are evaluated consistently and impartially, and that they meet recognized standards for security.

The JCCS program's affiliation with the Common Criteria Recognition Arrangement (CCRA) can also be beneficial for consumers, as it enables mutual recognition of evaluation and certification results across member countries. This means that products certified under the JCCS program can be recognized in other countries that are members of the CCRA, and vice versa. This can help to increase the availability of certified cybersecurity products, and give consumers a wider choice of products that have been evaluated and certified to recognized standards.

Overall, the JCCS program and its affiliation with the CCRA can play an important role in enhancing cybersecurity in Jordan and promoting greater trust and confidence in the IT and cybersecurity products available to consumers.

- Current Situation:

NCSC is the main government agency responsible for cybersecurity. The NCSC has drafted a licensing regulation for cybersecurity service providers in Jordan.

Licensing schemes are typically used to regulate the cybersecurity industry and ensure that service providers meet certain standards of quality and competence. NCSC will require service providers to obtain a license before they can offer certain services, and NCSC also will require providers to adhere to certain standards and best practices.

Such schemes can help to ensure that service providers are qualified and competent, and that they are held accountable for any failures or breaches of security.

- Future Plan:

A future plan for the Jordanian Common Criteria Scheme (JCCS) could involve several steps to further enhance cybersecurity in Jordan and promote the use of certified products. Here are some possible actions that could be taken:

Expand the scope of the JCCS program: The JCCS program could be expanded to include more types of cybersecurity products, such as cloud services, mobile applications, and IoT devices. This would help to address the evolving threat landscape and ensure that a wider range of products is evaluated and certified.

Strengthen the evaluation and certification process: The evaluation and certification process could be further strengthened by increasing the rigor of testing and analysis, and by ensuring that the testing laboratories are accredited to international standards. This would help to enhance the credibility of the JCCS program and provide greater assurance to consumers.

Promote awareness and adoption of certified products: The JCCS program could launch a public awareness campaign to promote the benefits of using certified cybersecurity products, and to encourage businesses and individuals to prioritize cybersecurity in their operations. The JCCS program could also work with industry associations, government agencies, and other stakeholders to promote the adoption of certified products.

Foster international collaboration: The JCCS program could strengthen its affiliation with the Common Criteria Recognition Arrangement (CCRA) by actively participating in its activities and collaborating with other member countries. This would help to promote mutual recognition of certification results and further enhance the availability of certified products.

Continuously review and update the JCCS program: The JCCS program could be reviewed periodically to ensure that it continues to meet the needs of the market and remains aligned with international standards. This would help to ensure that the program remains relevant and effective in the face of evolving threats and technologies.

Overall, a future plan for the JCCS program could focus on expanding the scope of certification, enhancing the evaluation and certification process, promoting awareness and adoption of certified products, fostering international collaboration, and continuously reviewing and updating the program to meet the needs of the market. By taking these actions, the JCCS program could help to enhance cybersecurity in Jordan and promote greater trust and confidence in the cybersecurity products available to consumers.

3.2 Ongoing reforms:

NCSC is currently drafting an updated version of national framework, and a licensing regulation for cybersecurity service providers in Jordan.

3.3 Linked activities:

Not applicable

3.4 List of applicable *Union acquis*/standards/norms:

Programming of the European Neighbourhood Instrument (ENI) - 2014-2020 - Single Support Framework for EU support to Jordan (2017-2020)

EU-Jordan Partnership Priorities JOIN (2016) 41 final ANNEX 1

EU External Cyber Capacity Building Guidelines – Council Conclusions and Operational Guidance.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive);

Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 as regards managing the risks by digital service providers posed to the security of network and information systems and determining a substantial impact of incident.

3.5 Components and results per component

Component1: Establishment of the Security Operation Centre for Operational Technology (OT-SOC).

Result 1.1: Develop roadmap and strategy for OT Cyber Security at the national level.
Result 1.2: Recommendations for cybersecurity regulations specific for OT.
Result 1.3: Develop OT-SOC Infrastructure Requirements and Architecture.

Component 2: Establishment of the National Cybersecurity Certification and Accreditation Centre.

Result 2.1: Develop roadmap and strategy for NCSC capacities for evaluation and certification of cybersecurity product.
Result 2.2: Building Jordanian Common Criteria Scheme, for certification of commercial cybersecurity products targeting Jordanian markets.
Result 2.3: Improving the capabilities of the NCSC in labelling cybersecurity products.

3.6 Means/input from the EU Member State Partner Administration(s)*:

The project will be implemented in the form of a Twinning contract between the Beneficiary Country and EU Member State(s). The implementation of the project requires one Project Leader (PL) with responsibility for the overall coordination of project activities and one Resident Twinning Adviser (RTA) to manage implementation of project activities, Component Leaders (CL) and pool of short-term experts within the limits of the budget. It is essential that the team has sufficiently broad expertise to cover all areas included in the project description.

The Member State Project Leader (PL) is expected to be an official or assimilated agent with a sufficient rank to ensure an operational dialogue at political level. This should guarantee the capacity to lead the implementation of the project and the ability to mobilise the necessary expertise in support of its efficient implementation.

Involvement of the Member State PL(s) is expected during the preparation of the Member State proposal and attendance of the PL to the selection meeting is obligatory as well as the participation in quarterly meetings of the Project Steering Committee. Participation in some communication and visibility activities is expected.
The Member State PL is supported by the RTA, who works on-site with the Beneficiary administration.

Short Term Experts will work together with the staff of the beneficiary institution under the overall direction of the beneficiary institution and the Project Implementation team. Besides providing the EU MS Twinning partner with adequate staff and other resources to operate effectively, the senior management of the beneficiary institution is expected to be involved in the development and implementation of policies and institutional change required to deliver the project results.

Proposals submitted by Member State shall be concise and focused on the strategy and methodology and an indicative timetable underpinning this, the administrative model suggested, the quality of the expertise to be mobilised and clearly show the administrative structure and capacity of the Member State entities. Proposals shall be detailed enough to respond adequately

to the Twinning Fiche, but are not expected to contain a fully elaborated project. They shall contain enough detail about the strategy and methodology and indicate the sequencing and mention key activities during the implementation of the project to ensure the achievement of overall and specific objectives and mandatory results/outputs.

The interested Member State(s) shall include in their proposal the CVs of the designated Project Leader (PL) and the Resident Twinning Advisor (RTA), as well as the CVs of the potentially designated Component Leaders-(CLs).

The Twinning project will be implemented by close co-operation between the partners aiming to achieve the mandatory results in sustainable manner.

The set of proposed activities will be further developed with the Twinning partners when drafting the initial work plan and successive rolling work plan every three months, keeping in mind that the final list of activities will be decided in cooperation with the Twinning partner. The components are closely inter-linked and need to be sequenced accordingly.

3.6.1 Profile and tasks of the PL:

Qualifications and skills:

Education:

- University degree in one of the following fields: law, public administration, computer/system/telecommunication engineering, computer science, economics or equivalent professional experience of 8 years in the sector of cybersecurity.
- Master degree in IT/Cyber Security fields is an asset.

General experience:

- Proven contractual relation to a public administration or mandated body (see Twinning Manual 4.1.4.2) responsible for cybersecurity or equivalent agency with necessary public administration experience and with a sufficient rank to ensure an operational dialogue at political level;

Specific experience:

- At least 3 years of specific experience in the area of public sector cybersecurity or equivalent.
- Previous experience in international co-operation will be considered as asset.
- Experience as a team leader or project leader in minimum 1 technical assistance or twinning projects would be considered as an asset

Language skills:

- Fluent written and spoken English.
- Knowledge of Arabic would be an asset

Tasks:

- Conceive, supervise and coordinate the overall Twinning project.
- To provide strategic advice on high level regarding reforms supported by the Twinning.
- Coordinate and monitor the overall implementation of the project including coordination and direction of the MS TW partner.
- Communicate with the beneficiary and EU Delegation.
- Guarantee from the MS administration side, the successful implementation of the project.
- Participate in quarterly meetings of the Project Steering Committee with the Beneficiary Country (BC) PL.

- Participate in preparation of the initial and subsequent work plans.
- Participate in preparation of both interim and final reports.

3.6.2 Profile and tasks of the RTA:

The relevant institution of MS will appoint a long-term Resident Twinning Advisor (RTA).

Resident Twinning Adviser being an official or assimilated agent from a Member State public or semi-public administration or accepted mandated body seconded to the beneficiary country to coordinate the day-to-day activities of the project.

Qualifications and skills of the Resident Twinning Adviser

Education:

- University degree in one of the following fields: law, public administration, computer/system/telecommunication engineering, computer science, economics or equivalent professional experience of 5 years in the cybersecurity sector.
- Master degree in IT fields/Cyber Security is an asset.

General Experience:

- At least 3 years of general professional experience in public administration. Engaged in cybersecurity sector or equivalent is an asset.
- Previous experience in training and mentoring in related areas will be considered as asset.
- Has worked in a managerial position.

Specific Experience:

- Experience as a team leader or project leader in minimum 1 technical assistance or twinning projects would be considered as an asset.

Language Skills:

- Fluent written and spoken English.
- Knowledge of Arabic would be an asset

Tasks:

As to the general responsibility of the day-to-day implementation of the Twinning project in the Beneficiary Country, the Resident Twinning Adviser (RTA) tasks will include:

- Provide technical advice and assistance to the administration or other public sector bodies in the BC in the context of a predetermined work-plan;
- Coordination of all project activities and experts inputs in the BC;
- Ensuring day-to-day implementation of the Twinning project in the BC;
- Ensuring smooth correlation between the activities, deadlines and the envisaged results in the Work Plan;
- Preparation of the materials and documentation for regular monitoring and reporting;
- Preparation of side letters.
- Ensure that the right quality of profile Short-Term experts are selected, mobilized.
- Supervise the STE performance and initiate appropriate action in case of quality concern.
- Organization of visibility events (kick-off and final event);
- Organization of Steering Committee meetings;
- Participation in Steering Committee meetings;
- Overseeing and managing administrative issues (e.g. assisting in reporting);
- Networking with institutions relevant to this project in Jordan and in MS;

In addition to the above, an assistant and a full time translator-interpreter shall be appointed to assist the RTA. Allowance for this must be made within the project budget. Furthermore, the assistant and translator will facilitate the training activities. Where necessary (for example, during training activities, translation of project documents/reports and materials) the project will hire an additional translator with costs covered by the project.

3.6.3 Profile and tasks of Component Leaders

Component Leaders will provide general guidance for the two Components of the project.

Qualifications and skills:

Education:

- University degree in one of the following fields: law, public administration, computer/system/telecommunication engineering, computer science, economics or equivalent professional experience of 3 years in cybersecurity.

General Experience:

- At least 3 years of general professional experience in public administration. Engaged in cybersecurity sector or equivalent is an asset.
- Previous experience in training and mentoring in related areas will be considered as asset.

Specific Experience:

- Appropriate skills and competence directly linked to the two components of the project.
  - Component1: Employed by or manage Security Operation Center for Operational Technology (OT-SOC) or equivalent department
  - Component 2: Employed by or manage National Cybersecurity Certification and Accreditation Centre or equivalent department.
- Previous experience in training and mentoring in related areas will be considered as asset.

Language Skills:

- Fluent written and spoken English.
- Knowledge of Arabic would be an asset

3.6.4 Profile and tasks of other short-term experts*:*

In close cooperation with the component leaders and upon request of the RTA, short-term experts (STE) will support specific aspects of Cybersecurity project in Jordan. In so doing, the STE are expected to maintain close cooperation with the Jordanian Cybersecurity (NCSC) experts in undertaking all activities, to advance preparation and get familiarized with relevant documentation.

STEs will provide specialised know-how for the individual tasks in the project.

- University degree in one of the following fields: law, public administration, computer/system/telecommunication engineering, computer science, economics or equivalent professional experience of 5 years in the sector of telecommunications/ electronic communications.
- At least 3 years of experience related to the subject related to the Component 1 or Component 2.
- Previous experience in training and mentoring in related areas will be considered as asset.
- Fluent written and spoken English.

4. Budget

Maximum Budget available for the Grant

1.4 Million Euro

5. Implementation Arrangements

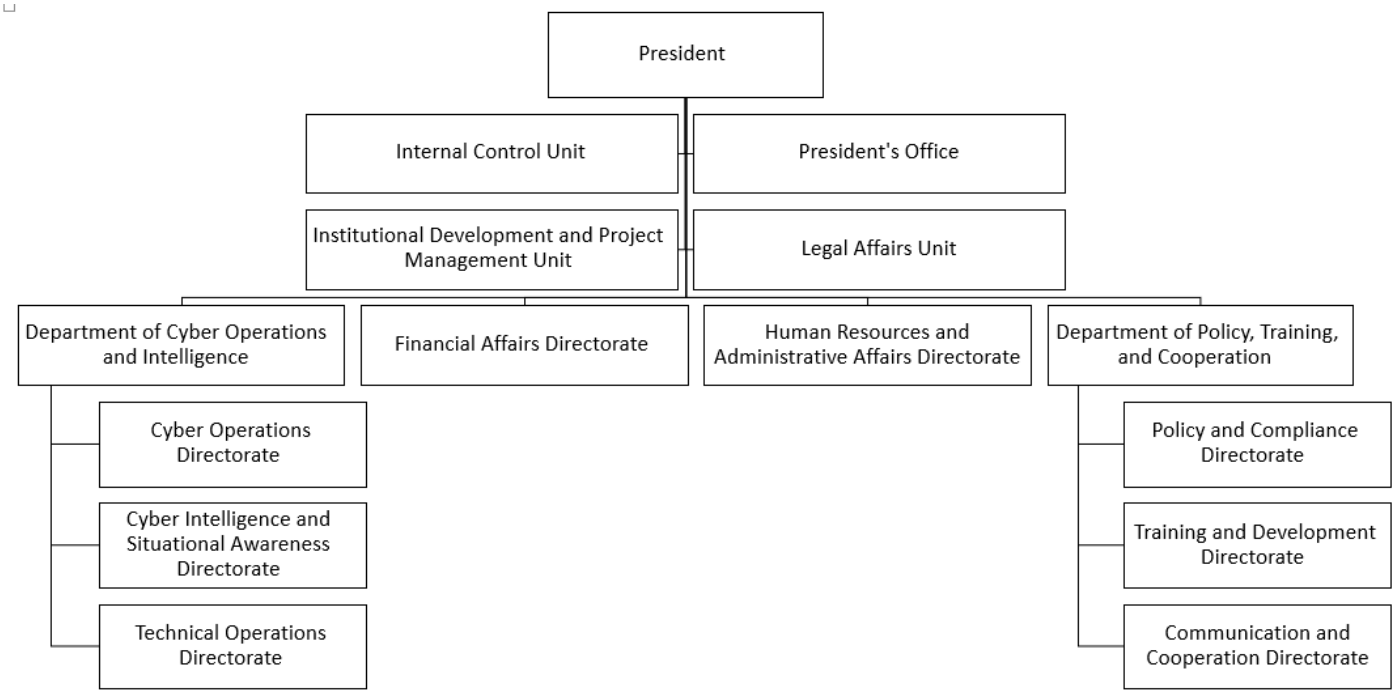
5.1 Implementing Agency responsible for tendering, contracting and accounting

The Ministry of Planning and International Cooperation is the Contracting Authority for the twinning project under which The Programme Administration Office (PAO) coordinates of all the related activities and the administrative management of the funding Programme. The PAO will be the responsible institution for the management of this twinning project.

Contact details of PAO responsible of the contract:
Ministry of Planning and International Cooperation
Ms. Areej AlHadeed
Programmes Administration Office
Ministry of Planning and International Cooperation
P.O. Box 555 Amman, 11118 Jordan
Telephone Number: +962 6 46 444 66 ext. 506
Email: Areej.Alhadeed@mop.gov.jo

5.2 Institutional framework

The NCSC consists of two main departments: the Department of Operations and Cyber Intelligence and the Department of Policy, Training, and Cooperation. The NCSC comprises a total of 90 employees who are allocated across all the directorates and units within the organization. For further information, please refer to the organizational chart provided below.



5.3 Counterparts in the Beneficiary administration:

5.3.1 Contact person:
Rasha Darwish
Officer at Institutional Development and Project management unit at NCSC.
Postal address: Jandaweel, Abdallah Rajab Hakouz Street, Amman, Jordan
Email: rasha.darwish@NCSC.JO
Phone Number: +962786472231

5.3.2 PL counterpart
Bassam Al-Maharmeh
President of National Cyber Security Center
Postal address: Jandaweel, Abdallah Rajab Hakouz Street, Amman, Jordan
Email: bassam.maharmeh@ncsc.jo
Phone Number: 0790799990

5.3.3 RTA counterpart
Heba Abu Zaid
Institutional Development and Project Management Director
Postal address: Jandaweel, Abdallah Rajab Hakouz Street, Amman, Jordan
Email:Heba.abuzaid@ncsc.jo
Phone Number :+962) 79 970 1964

6. Duration of the project

24 Months of Implementation Period.

7. Management and reporting

7.1 Language

The official language of the project is the one used as contract language under the instrument (English). All formal communications regarding the project, including interim and final reports, shall be produced in the language of the contract.

7.2 Project Steering Committee

A project steering committee (PSC) shall oversee the implementation of the project. The main duties of the PSC include verification of the progress and achievements via-à-vis the mandatory results/outputs chain (from mandatory results/outputs per component to impact), ensuring good coordination among the actors, finalising the interim reports and discuss the updated work plan. Other details concerning the establishment and functioning of the PSC are described in the Twinning Manual.

7.3 Reporting

All reports shall have a narrative section and a financial section. They shall include as a minimum the information detailed in section 5.5.2 (interim reports) and 5.5.3 (final report) of the Twinning Manual. Reports need to go beyond activities and inputs. Two types of reports are foreseen in the framework of Twining: interim quarterly reports and final report. An interim quarterly report shall be presented for discussion at each meeting of the PSC. The narrative part shall primarily take stock of the progress and achievements

via-à-vis the mandatory results and provide precise recommendations and corrective measures to be decided by in order to ensure the further progress.

8. Sustainability

The achievements of a Twinning project (from results per component to impacts) should be maintained as a permanent asset to the Beneficiary administration even after the end of the Twinning project implementation. This presupposes inter alia that effective mechanisms are put in place by the NCSC administration to disseminate and consolidate the results of the project.

This Twinning project emphasises the aspect of sustainability with particular regard to areas related to awareness raising, training, monitoring and evaluation:

- The internal needs assessment of the NCSC, which has been conducted prior and during the formulation of this fiche, illustrated that NCSC needs assistance to strengthen its operational and institutional governance framework to be able to improve its performance and better measure the impact of the TWG project foreseen attained results.
- A monitoring and evaluation system will be developed and implemented in close cooperation with NCSC. By ensuring for its appropriateness in the NCSC-context, the M&E system is supposed to sustain and be used after the Twinning Project activities were accomplished.
- It is expected that this project by its nature will inspire NCSC to adopt EU and international best practice and standards, adapt relevant ideas and mechanisms in the light of Jordan's situation, and improve NCSC's capacities in relation with cyber security. It is assumed that the support of this twinning is very practical and thus evident for NCSC's development efforts.
- Establishment of the Security Operation Center for Operational Technology (OT-SOC) with the help of the TWG intervention should be kept operational and running. It means the enhanced skills and competency of the staff as well as the budgetary plan should include sufficient resources to ensure that the skills attained will be kept in the long term.
- NCSC becoming the National Cybersecurity Certification and Accreditation Centre result should be sustained in the long run by provision of sufficient annual budget to keep the center up and running and be able to host and organise numerous and various regional cyber security trainings, workshops,. Basically ensure the knowledge transfer internally and externally.
- At the end of the project the NCSC will be in the position to master and to perform the necessary tasks independently with no assistance. The project will lead to improved institutional framework, enhanced training programmes, and efficient impact measurement tools. The Project will provide appropriate development strategies and action plans to enable the CNCS to prevent and act on any cyber security related threat with greater sufficiency.

9. Crosscutting issues *(equal opportunity, environment, climate etc…)*

This project will ensure equal treatment and opportunity to all persons of interest regardless of their gender, age, race, colour, disability, religious view, ethnicity, marital status, and social classes, as guaranteed in the constitution of the Hashemite Kingdome of Jordan. Moreover, the project pursues a "do-no-harm" approach and avoids activities that could have adverse effect or impact on the environment.

10. Conditionality and sequencing

This project will be implemented through a twinning arrangement. Consequently, the NCSC will be required to allocate sufficient, suitable experienced staff and all necessary material resources for the efficient implementation of the Twinning Project.

The commitment and participation of Senior Management of the NCSC is indispensable, both qualities are intrinsically involved in developing and implementing the policies as well as facilitating any institutional changes required in delivering the project results and ensuring the sustainability of project actions after the completion of the project activities.

11. Indicators for performance measurement

- Result 1.1: Develop roadmap and strategy for OT Cyber Security at the national level.
- Result 1.2: Recommendations for cybersecurity regulations specific for OT.
- Result 1.3: Develop OT-SOC Infrastructure Requirements and Architecture.
- Result 2.1: Develop roadmap and strategy for NCSC capacities for evaluation and certification of cybersecurity product.
- Result 2.2: Building Jordanian Common Criteria Scheme, for certification of commercial cybersecurity products targeting Jordanian markets.
- Result 2.3: Improving the capabilities of the NCSC in labelling cybersecurity products.
- Based on the joint work of development of the rolling work plan the Logical Framework Matrix needs to be developed with respective indicators (qualitative and quantitative) regularly updated during project implementation and used as a management performance measurement tool.

12. Facilities available

The beneficiary will host the EU twinning project team and will provide the following facilities for RTA, RTA Assistants and the two component leaders:

• Office space (10 m2 /staff), including functional desk and shelves

• If possible and applicable additional office space for the pool of STEs (normally 2-4 experts)

• Land lines for national telephone.

• WLAN with internet connection for all project team office environment.

• Access to training rooms in the beneficiary's premises, including audio-/video-equipment.

• Access to meeting rooms in the beneficiary's premises.

ANNEXES TO PROJECT FICHE

1. The Simplified Logical framework matrix as per Annex C1a (compulsory)
2. Links for :
    a. National Cyber Security Strategy 2018-2023
    b. Cyber Security Law no. 16 for year (2019)
    c. National framework

Annex 1: Simplified Logical Framework

	Description	Indicators (with relevant baseline and target data)	Sources of verification	
Overall Objective(s)	To contribute in the improvement of cybersecurity in Jordan to be in line with best international standards	• NCSC operations are enhanced and expanded.	• Satisfaction surveys. • Quality check. • Statistical information of cyber attacks • Annual report	
	Description	**Indicators (with relevant baseline and target data)**	**Sources of verification**	**Risk**
Specific Objective	Strengthen NCSC capacities to establish a Security Operation Centre for Operational Technology (OT-SOC) and become National Cybersecurity Certification and Accreditation Centre	• The enhanced Security Operation Centre for Operational Technology (OT-SOC) is established. • National Cybersecurity Certification Evaluation Scheme is drafted • Jordanian Common Criteria Scheme is drafted • Cybersecurity Labelling Scheme is drafted	• Official reports, statistics, studies. • Project reports and data. • Interviews with the beneficiary and other target groups • Experts mission reports.	• Lack of cooperation and dedication. • Insufficient capacity for absorption
Component 1	Establishment of the Security Operation Centre for Operational Technology (OT-SOC)			

Sub results for Component 1	**Result 1.1** Develop roadmap and strategy for OT Cyber Security at the national level	• A baseline assessment methodology for critical national infrastructure and developing a national cyber technical risk model is developed • Recommendations on for cybersecurity OT at the national level are developed and presented to NCSC's management • National policies and framework for assessing cybersecurity resilience in National Critical Infrastructure are developed. • National strategic model to OT Cyber Security are developed • Roadmap and strategy are drafted. • Training programs for institutional development and project management unit employees are devised.	• Periodic project report • Minutes of Meeting with key stakeholders	• Facing difficulties in obtaining objective and reliable information • Lack of stakeholders' awareness.

Sub results for Component 1	**Result 1.2** Recommendations for cybersecurity regulations specific for the OT-SOC	• Related regulations are assessed and revisions are drafted. • NCSC processes and procedures are assessed and revised to account for the establishment of OT-SOC • Recommendations are drafted for the enhancement of: o response and security assessments for OT/ICS environments o cyber incident response to vulnerability management and protective monitoring capacity o the capabilities of employees in (Cyber Operations Directorate, Cyber Intelligence and Situational Awareness Directorate, Technical Operations Directorate)	• Reports • Committee minutes of meetings	• Lack of cooperation and dedication. •
Sub results for Component 1	**Result 1.3** Develop OT-SOC Infrastructure Requirements and Architecture	• Assessment of the existing situation on the national level is drafted. • The requirements for Incident Response, Security Assessment, Threat Intelligence, Real-time Monitoring, Vulnerability Management are formulated	• Reports	• Implementation delays • Data not being available • Insufficient capacity for absorption
Component 2	**Establishment of the National Cybersecurity Certification and Accreditation Centre.**			

Sub results for Component 2	**Result 2.1** Develop roadmap and strategy for NCSC capacities to evaluation and certification of cybersecurity products	• assessment of the current situation and the future situation and identifying gaps for to evaluation of cybersecurity products and certification of cybersecurity products • Developing a national policies and framework for to evaluation of cybersecurity product and certification of cybersecurity products • Developing the evaluation methodologies for NCSC to evaluation of cybersecurity product and certification of cybersecurity products • provide training courses and internships for professionals to learn more about certification processes and evaluation methodologies, and to perform evaluation at the highest assurance level. • Provide requirements to become the NCSC member of the Common Criteria Recognition Arrangement (CCRA)	• Assessment report • Minutes of meetings • Draft of the roadmap • Reports	• Insufficient capacity for absorption • Implementation delays

Sub results for Component 2	**Result 2.2** Developing Jordanian Common Criteria Scheme, for certification of commercial cybersecurity products targeting Jordanian markets.	• Policies and instructions to Jordanian Common Criteria Scheme for commercial cybersecurity products are drafted • Specifications and standards for the approval of commercial cybersecurity products for commercial cybersecurity products are drafted • The National Assessment Plan, the Joint Jordanian Standards Scheme, for the accreditation of commercial cybersecurity products are drafted • A plan for continuous review and updating of the Jordanian common Standards Scheme system is devised.	• Minutes of meetings • Reports	• Data not being available
Sub results for Component 2	**Result 2.3** Improving the capabilities of the NCSC in labelling cybersecurity products	• Guidelines for standards and specifications for product classification (software and hardware) are devised. • Product labelling evaluation methodology is drafted. • Training courses to raise awareness on the labelling of cyber security products are developed.	• Minutes of meetings, • Final reports	• Lack of cooperation and dedication. • Data not being available

Annex 2 :

National Cyber Security Strategy 2018-2023. (https://modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/national_cyber_security_strategy_2018_2023.pdf)

Cyber Security Law no. 16 for year (2019) (http://ncsc.test.jo/documents/Cybersecurity-Law-Ar-No-16-of-2019.pdf) , (https://www.lob.gov.jo/?v=1.15&lang=ar#!/LegislationDetails?LegislationID=3268&LegislationType=2&isMod=false)

National framework

(https://ncsc.jo/Manager/OPSHandler/OPS_Auth.asmx/GetAttachment?Type=Form&ObjectID=10285&RowID=30&ColumnName=Attachment&FileName=4794&IsThumb=false)