



РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА - REPUBLIKA E MAQEDONISE SË VERIUT
ДРЖАВНА КОМИСИЈА ЗА СПРЕЧУВАЊЕ НА КОРУПЦИЈАТА
KOMISIONI SHITETËROR PËR PARANADALIM TË KORRUPSIONIT

Бр.-Нр. 07-1205/2
16-03-2026 20 год.-viti
СКОПЈЕ - ШКУП

STRATEGY

FOR DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY 2026 -2029

State Commission for Prevention of Corruption (SCPC)

Prepared by:

Marina Stevanoska, Skopje, 24 September 2025



Funded by
the European Union





“This publication was funded by the European Union. Its contents are the sole responsibility of Ludwig Boltzmann Gesellschaft - Institute of Fundamental and Human Rights (LBI-GMR) and do not necessarily reflect the views of the European Union.”

Contents

1	EXECUTIVE SUMMARY	4
2	IT VISION AND STRATEGIC IT OBJECTIVES	4
2.1	IT VISION	4
2.2	STRATEGIC IT OBJECTIVES	4
3	CURRENT IT ENVIRONMENT (AS-IS ANALYSIS).....	5
4	STRATEGIC DRIVERS.....	8
5	TARGET ARCHITECTURE (TO-BE VISION).....	9
5.1	CORE FUNCTIONAL SYSTEMS.....	9
5.2	TECHNICAL STANDARDS.....	12
6	STRATEGIC INITIATIVES (2026–2029)	12
7	GOVERNANCE AND RISK MANAGEMENT	14
8	BUDGET AND RESOURCE PLAN	15
9	ANNEX: ANNUAL ACTION PLAN AND REVISION FRAMEWORK (2026–2029)	15
9.1	ANNUAL ACTION PLAN OVERVIEW	15
9.2	ACTION PLAN 2026-2029	15
9.3	ANNUAL STRATEGY REVIEW AND REVISION FRAMEWORK	17

1 Executive Summary

The mission of the State Commission for Prevention of Corruption (SCPC) is to detect and prevent corruption and conflict of interest in public institutions, enhance transparency and accountability, and foster a culture of integrity in the country. The digital transformation of the SCPC is essential for increasing the transparency, efficiency, and prompt responsiveness in preventing the corruption.

This Strategy for the Development of the Information and Communication Technology outlines the strategic vision, priority initiatives, and technical framework to support SCPC's mandate through modern, secure, reliable digital technologies, where the citizens will be actively engaged. The document aligns with the Law on Prevention of Corruption and Conflict of Interest, National ICT Strategy (2023-2030), as well as with the European integration goals.

The objective of this ICT Strategy is to improve the transparency, accountability and public trust through integrated solutions, to modernise the processes for prevention of corruption and conflict of interests, to provide for more efficient evidence and monitoring the assets status and interests of elected and nominated persons, as well as to support the implementation of the National Strategy for Prevention of Corruption and Conflict of Interests, and strengthen the personal and institutional integrity.

2 IT Vision and Strategic IT Objectives

2.1 IT Vision

To build a modern, secure, and interoperable digital environment that empowers SCPC to fulfill its mandate effectively and engage citizens in anti-corruption efforts.

2.2 Strategic IT Objectives

- **Complete digitalization of the SCPC.** This involves automating all internal processes of the Commission, through upgrading the existing and introducing new IT systems and their effective use (paperless work). In this way, the efficiency of processing citizen-submitted corruption allegations and investigating reported cases will be improved.
- **Interoperability and inclusiveness.** Existing integration frameworks will be further enhanced to ensure comprehensive and secure data exchange with all relevant government bodies and commercial entities, strengthening SCPC's ability to perform its

functions effectively. This includes full connectivity and electronic data exchange with state institutions and banks, aiming to eliminate the need for paper-based processes entirely.

- **Increasing analytical capacities.** Enhancing analytical capacities by promoting data analytics and early warning systems, while improving employees' analytical skills.
- **Development of innovative solutions and adoption of emerging trends.** SCPC will continuously explore and implement innovative IT solutions aligned with global digital trends to ensure long-term system sustainability, scalability, and effectiveness. This includes introducing new technologies (such as AI, chatbots, digital signatures, and advanced operational analytics), modernizing legacy systems and introducing user-centred improvements. The goal is to maintain the relevance and responsiveness of the SCPC's digital infrastructure in the face of evolving anti-corruption challenges.
- **Increasing transparency and citizen participation.** Ensure transparency through public-facing digital platforms and increase citizen participation through user-friendly digital reporting tools. Facilitate easier access for citizens to communicate with the SCPC, enabling them to submit reports, share information, efficiently and securely.
- **Strengthen awareness and skills.** Enhancing management awareness at SCPC about the importance of IT systems, while also developing the IT team's capabilities and improving employee skills in using these systems.
- **Infrastructure, Cybersecurity, and Data Privacy – Key Improvement Areas.** To comply fully with the personal data protection regulations, the State Commission for Prevention of Corruption must enhance its IT infrastructure and cybersecurity measures. This includes strengthening access controls with regular password updates and multi-factor authentication, improving monitoring and logging for faster incident detection, and maintaining up-to-date firewall and antivirus protections. Physical security of server rooms and secure handling of electronic media require reinforcement. Additionally, regular audits and ongoing staff training on data protection policies are essential to ensure consistent application of technical and organizational safeguards. These improvements will better protect personal data confidentiality, integrity, and availability, meeting legal requirements and best practices.

3 Current IT Environment (As-Is Analysis)

- **Systems:** SCPC manages several application systems established in the past period. Below is a list of the systems and a brief description of their purpose:

- **Communication Portal** - enables the employees of SCPC to communicate with the institutions through announcements, surveys and meetings. The system implements the process of the National Strategy for Prevention of Corruption and Conflict of Interests, where the institutions submit reports with evaluation indicators that are analysed by the SCPC and, if necessary, returned for revision. Upon completion, a draft of the annual report is generated. The portal also enables the creation and distribution of questionnaires based on the integrity methodology, receiving responses from institutions and generating reports to evaluate their performance on the national level.
- **Performance Monitoring System** - enables the monitoring of the work and the workload of the employees of SCPC, in order to improve the efficiency and the allocation of resources
- **Mobile/Beb Application for raising the awareness about the fight against corruption in SCPC** - serves to inform citizens through announcements, events and educational content, with the aim of increasing awareness of anti-corruption activities
- **Whistleblower Protected Reporting System** - enables secure two-way communication between whistleblowers and institutions, ensuring protection of their anonymity
- **Distance Learning Platform** - enables e-learning by hosting e-courses, quizzes and automatically issuing certificates for successfully completed courses.
- **Tool for anti-corruption proofing of legislation** - enables collaborative work of the employees of the SCPC for the analysis of the legal contents, creation of proposals and amendments
- **Document Management System (DMS)** – serves for document management (DMS). It enables electronic archiving, tracking of cases and documents, and distribution of digital document in SCPC.
- **System for the register of elected and appointed persons, asset declarations and interests and their monitoring** - system for personal electronic reporting of the property status of elected and appointed persons, register for appointment/termination of elected and appointed persons by the institutions, register of the elected and the appointed persons and their property situation and an administrative tool for controls and checks of the data submitted by the elected and appointed persons and institutions
- **System for Lobbyists** - enables submission and management of reports by lobbyists or lobby organizations, ensuring transparency and monitoring of their activities
- **Human Resource Management System (HRMS)** - enables integrated management of key aspects of human resources, including organizational hierarchy, training, absences and employee evaluations.

The aforementioned systems have been developed and implemented with the support by IPA projects and the Rule of Law Programme and have already contributed to the digitalisation of processes in SCPCP.

Most of the above systems have been in operation for more than two years, and additional functionalities can be implemented in them.

- SCPC uses the Information **System for Human Resources Management (ITSHRM)**, which has been implemented on central level by the Ministry of Digital Transformation and is being used by the public sector in the country for keeping a register of employees and administration of processes for calculation of salaries.
- **Infrastructure:** The SCPC's IT infrastructure supports its operations through a combination of legacy servers, network equipment, and internal connectivity systems that require modernization to meet current and future demands. The network infrastructure comprises a centralized data centre network, an access network within the premises, and a wireless network. The data centre features a main rack cabinet hosting the central router/firewall (Juniper) and switches connecting servers and aggregating the access network. The internal network is segmented into management and private VLANs. However, current architecture lacks sufficient network isolation of sensitive systems, increasing the exposure to risk and highlighting the need for subnet division and stricter access controls.

The server infrastructure relies on 6 (six) main servers over a decade old, with limited capacity to meet growing demands and expiring warranties. The absence of network-attached storage limits virtualization options and increases the risk of data loss and reduced availability in case of outages.

- **Security:** The SCPC's IT security environment currently faces challenges related to maintenance and improvement of the system software, lack of centralized monitoring, and physical infrastructure vulnerabilities. While application software solutions generally follow modern security standards, certain legacy components and network configurations expose the organization to potential risks. Access control is implemented through a combination of local user accounts, Active Directory integration, and national single sign-on systems, with varying risk levels depending on the system. Data protection is supported by regular backups, though the absence of a **formal** disaster recovery plan and insufficient logging of administrator activities increase operational risks. Overall,

strengthening patch management, improving network segmentation, enhancing logging and monitoring, and implementing a comprehensive disaster recovery strategy are critical priorities to enhance SCPC's cybersecurity posture.

- **Interoperability:** Currently, the SCPC has established connections with other institutions through interoperability platforms and direct services, but there is a need to further strengthen and expand these integrations. Enhancing interoperability will enable more efficient, secure, and timely data exchange, reduce manual workload, improve coordination in anti-corruption efforts, and support data-driven decision-making.
- **Challenges:** Although several systems have been introduced, there are still processes that are carried out manually and can be further optimized. There is also a need for the development of a digital platform that will enable active engagement of citizens by way of electronic reporting and notification, as part of the efforts to combat corruption. The implementation and development of ICMS aims to build an integrated system for report intake, tracking, investigation, and reporting, which will improve the efficiency and transparency of the processes. In certain areas, scalability needs to be improved, and a centralized operational analytics system (e.g., Power BI) should be implemented to integrate and analyse data from all implemented systems. Another significant challenge is the under-resourced IT team.

4 Strategic Drivers

- **Legal Framework:** Law on Prevention of Corruption and Conflict of Interest, Law on lobbying, Law on protection of whistleblowers, Law on electronic documents, electronic identification and confidential services, Law on security of information systems, Law on archive material and archive activity, Law on Personal Data Protection (aligned with GDPR), Law on Electronic Governance, and Internal Policies and Security Framework (including internal rules and procedures such as Risk Analysis, Policy on Password Creation and Use, Remote Work and Telework Policy, Server Room Access Rules, DSCC Security Regulations, Incident Response Procedures, Secure Data Disposal Protocols, Backup and Recovery Policy, and Procedures for the Use and Security of IT Systems).
- **Governmental Priorities:** National ICT Strategy (2023-2030), National Strategy for Cyber Security (2023-2027), e-Government Development, Open Government Partnership, Strategy on Transparency.
- **International Obligations:** EU accession reforms, GRECO recommendations, UNCAC standards.

- **Public Demand:** Transparency in asset declarations, active engagement of citizens in the processes, real-time data access and analytics from aggregated data of the results from verifications and reports.

5 Target Architecture (To-Be Vision)

5.1 Core Functional Systems

- The existing **System for the register of elected and appointed persons, declaration of assets and interests and their monitoring** enables online submission and automated validation but requires enhancements for broader real-time verifications from multiple institutions and tracking of historical asset movements. Key improvements should focus on data cross-checking, error handling, streamlined process initiation, improved user notifications and communication, enhanced integration with DMS for case verification, and expanded conflict of interest detection capabilities.

Upon amending the Law on prevention of corruption and conflict of interests, , the requirement to print and physically submit the asset declarations should be terminated, allowing for a fully digital and paperless submission process.

- **Interoperability Layer:** Real-time integration with institutions such as the Agency for Real Estate Cadastre, Central Registry, Ministry of Internal Affairs, Ministry of Digital Transformation and Public Revenue Office. Potential cooperation with Pension and Disability Fund, Ministry of Justice, the Employment Service Agency, Ministry of Digital Transformation and the Ministry of Finance is also identified, as well as development of new services in existing institutions for obtaining and validation of additional and historical data.

Institution	Service name	Method	Service description	System where it is used/Service description
MINISTRY OF DIGITAL TRANSFORMATION	Single sign-in system	Single sign-in system	Signing in with E-id and downloading personal data of signed in user	System for asset declarations and interests of elected and nominated persons
CENTRAL REGISTER OF THE REPUBLIC OF NORTH MACEDONIA	CrmWrapperService	InvokeCrmService	Wrapper service which requires digital signature. It contains four methods that can be invoked. Downloading data of	System for asset declarations and interests for elected and nominated persons

Institution	Service name	Method	Service description	System where it is used/Service description
			trade companies and companies by EBS	
CENTRAL DEPOSITORY OF SECURITIES	Direct service GetIssue	GetHolderSecurities	Retrieval of data on securities by ISIN number.	System for asset declarations and interests for elected and nominated persons
AGENCY FOR REAL ESTATE CADASTRE	Full Property Deed	GetPropertyList	Retrieval of real estate data (parcels and buildings) based on property deed number.	System for asset declarations and interests for elected and nominated persons
		GetCadastralParcel	Retrieval of real estate data (parcels and buildings) based on parcel number.	System for asset declarations and interests for elected and nominated persons
MINISTRY OF INTERNAL AFFAIRS	Vehicles	ZemiSopstveniciNaMotornoVozi lo	Retrieval of vehicle data based on license plate number.	System for asset declarations and interests for elected and nominated persons
		ZemiMotorniVo zilaVoSopstvenostNaLice	Retrieval of a person's vehicles based on their personal identification number. Used for vehicle validation.	Admin Tool.
MINISTRY OF INTERNAL AFFAIRS	Personal Documents	ZemiPodatociO dLicnaKartaPoE mbg	Personal ID data based on personal identification number. Retrieval of data for individuals and family members using personal identification number.	System for asset declarations and interests for elected and nominated persons. Admin Tool.
	Weapon	ZemiOruzjeVoS opstvenostNaFizickoLice	Data on all weapons owned by an individual based on their personal identification number. Used for weapon validation.	Admin Tool.
PUBLIC REVENUE OFFICE	GDP_Service_v2	GetBasicDataForEmbAndYear	Income data, paid contributions, calculated and paid taxes based on personal identification number.	Admin Tool.
		GetIncomeSummaryByTypeForEmbAndYear	Summary data on income, contributions, and taxes based on	Admin Tool.

Institution	Service name	Method	Service description	System where it is used/Service description
			personal identification number.	
		GetIncomeSummaryByTypeAndPayerForEmbgaAndYear	Detailed data on payments and receipts for an individual based on their personal identification number.	Admin Tool.

Table 1. Presentation of services used in software solutions

- **Service for banks:** It is necessary to develop and implement data exchange services with all banks in the country. Currently, they are in the testing phase.
- **Improvement of the Communication Portal, in the modules for Integrity and the National Strategy:**
 - **Integrity Module** – It is necessary to improve the creation of integrity questionnaires through a dynamic and adaptable interface, as well as the generation of reports from institutions with enhanced filtering and analysis capabilities. The system should enable the creation of electronic forms and questionnaires with various functionalities, including field modeling, regional organization, and comprehensive data validations, fully managed by the user. The forms can be customized according to specific needs, with defined validation rules, evaluation mechanisms, and metrics for data analysis.
 - **National Strategy Module** – A new software solution (or a new module) needs to be developed, which will allow dynamic and adaptable creation of evaluations, fully managed by the user. Additionally, the visualization and design of the process should be improved for better clarity and user experience, along with reporting features to provide more detailed analyses and deeper insights.
- **Gift Management System** – Development of a system for managing the registration of gifts received by public officials to ensure compliance with anti-corruption regulations. This data should be publicly available in a Gift Catalogue.
- **Official Vehicles Registry** – Development of a system/registry for managing official vehicles by all institutions during election periods. Verification of the entered vehicle data should be performed against the vehicle registry of the Ministry of Interior. In the event of changes to the Electoral Code, the responsibility for this function will be transferred to the appropriate institution.
- **Development of ICMS:** It is necessary to develop an integrated system that will allow the citizens to directly submit reports for suspicions of corruption and conflict of interests. The system should provide easy access, anonymity, secure data processing and transparent monitoring the status of reports. Additionally, it will provide enable

automatic integration with the DMS System for allocation of cases and monitoring the entire procedure – from receiving the report, investigation to the final decision – as well as analytics of reports and assessment of trends.

- **Innovative digital solutions** – Implementation of modern IT system that will enable integration of new technologies, as well as Artificial Intelligence (AI) and chat-bots. The system will support automatic data analysis, identification of potential cases of corruption and conflict of interests, faster processing of reports and documents, as well as interactive communication and education of citizens, with the aim of strengthening the transparency, accountability and public trust.

5.2 Technical Standards

It is recommended that SCPC gradually adopts modern technical standards to ensure sustainability, interoperability, and compliance with international best practices. These may include:

- **Cloud-first approach**, fully harmonised with the national legislation, to enhance scalability, reduce maintenance efforts, and improve service availability.
- **Use of open standards for data sharing**, such as X-Road or similar solutions, to enable secure and standardized exchange of information with other institutions.
- **Alignment with ISO 27001** for information security management, to strengthen technical and organizational measures for data confidentiality, integrity, and availability.
- **Implementation of eIDAS-compliant authentication mechanisms**, supporting secure electronic identification and legally valid electronic signatures, especially relevant for cross-border and EU-aligned processes.

6 Strategic Initiatives (2026–2029)

Below are presented strategic initiatives in ICT area that SCPC plans to implement during the period 2026-2029, with the aim of improving the digital transformation, strengthening the integrity and improving the work efficiency.

Initiative	Description	Priority	Implementation Timeline
Gift Registry System	System for registration of gifts of officials, in order be compliant with the rules for	High	2026

	prevention of corruption and publicly available Catalogue of gifts		
Upgrade of the Digital System for Register of Elected and Nominated Persons, Asset Declarations and Interests and their monitoring	Improve user experience, larger number of verifications in real time, historical monitoring the assets, cross-checking of data, improved communication with users and generation of proposals for opening cases.	High	2026
Cybersecurity Framework	Implement access control, SIEM, incident response plan.	High	2026-2028
Improving the Communication Portal, in the modules related to Integrity and the National Strategy	Improving the user experience by dynamic creation and user template modelling	High	2027
Register of official vehicles	Register of official vehicles for management and verification of data in all institutions by connecting with the register of the Ministry of Internal Affairs.	Medium	2027
Development of ICMS	Developing an integrated system for receiving,	High	2028

	monitoring, verification and reporting on complaints.		
Artificial Intelligence (prototype, pilot phase)	Modern IT System with Artificial Intelligence for automatic analysis, interactive communication and supporting the fight against corruption.	Medium	2028
IT Capacity Building	Staff training in cybersecurity, digital forensics, and data analysis.	Ongoing	Annual

Table 2. Timeline for ICT Strategic Initiatives (2026-2029)

7 Governance and Risk Management

- **IT Governance Model:** IT Coordination Group chaired by a leading official of the institution, which also includes other officials in leading positions in the Secretariat.
- **Legal Compliance:** Ensuring compliance with all relevant laws and by-laws related to personal data protection, prevention of corruption, electronic management, security of information systems and archiving, as well as with the internal policies and security rules.

Key Risk Areas	Mitigation
Downtime of critical systems	Implementation of the Rulebook for incident reporting, response, and remediation; development of business continuity plans.
Lack of political will for development and support of ICT systems	Providing regular budget for supporting and stable financing the development of ICT systems
Insufficient level of protection and data safety	Regular testing, audit and improvement of measures for cyber security and data protection.
Lack of institutional services for interoperability with SCPC	Promotion of the interoperability and development of missing services in collaboration with relevant institutions, by concluding MoUs
Strengthening the IT capacities of the staff	Continuous training for the IT Sector staff

Table 3. ICT Risks and Planned Remediation Measures

8 Budget and Resource Plan

- Estimated Budget: €1.2–1.5 million over 4 years. The funding does not depend only on the SCPC and its initiative for obtaining budget, but also on allocations from the state budget and potential supporting international projects.
- Funding Sources:
 - SCPC core budget.
 - EU IPA funds for good governance and digital transformation.
- Potential support from international donors.

Budget breakdown:

- 45% Systems Development and Licensing
- 25% IT Security and Infrastructure
- 20% for training the staff and activities for supporting the users when introducing new systems, processes or technologies for easier adjustment and successful implementation.
- 10% - Contingency and Innovation Fund – funds reserved for unexpected situations or additional needs, such as technical issues, additional services or investing in new technologies and pilot projects which improve the efficiency and innovativeness of IT systems.

9 Annex: Annual Action Plan and Revision Framework (2026–2029)

To ensure continuous alignment of the IT Strategy with evolving institutional needs, legal requirements, and technology trends, this annex defines an **Action Plan** and a **revision mechanism** for the period 2026–2029. This will serve as a basis for monitoring progress, guiding implementation, and supporting decision-making on future IT investments.

9.1 Annual Action Plan Overview

Each year, SCPC will define specific activities aligned with the strategic objectives of the IT Strategy. These activities will be tracked and evaluated for impact, relevance, and completion status.

9.2 Action Plan 2026-2029

Strategic Objective	Key Activities	Responsible Unit	Timeline (quarters)	Output/Indicator
Improvement of the transparency	Development of digital Gift Registry System for management of gifts of officials, publicly available catalogue	Unit for IT Support and General Affairs + Unit for monitoring the financing of political parties, election campaigns and corruption in public procurement + International fund + Vendors	2026 Q1	Functional system with public section – Catalogue of Gifts
Improvement of the Digitalisation of Internal Processes	Adaptive maintenance and enhancement of existing systems – System for register of elected and nominated persons, asset declarations and interests and their monitoring, Document Management System and Communication Portal	SCPC + Vendors	2026 Q1 – 2026 Q3	Improved functionalities implemented in relevant systems according to technical requirements
Modernisation of asset declarations systems	Upgrade of the Digital System Register of elected and nominated persons, asset declarations and interests – improved user experience, verifications in real time, monitoring of historic data, cross-check of data, communication with users, proposals for opening cases (IPA Project)	SCPC + International fund + Vendors	2026 Q1 – Q4	Upgraded system according to technical requirements
Improved infrastructure & and increased cybersecurity	Cyber security framework – access control, SIEM, incident response plan	Unit for IT Support and General Affairs + Vendors	2026 Q1 – 2028 Q4	Strengthened security and documented incident response plan
Improvement of the Communication Portal	Improvement of the Communication Portal – modules for Integrity and National Strategy, Dynamic Creation and Modelling of Templates	Unit for IT Support and General Affairs + Unit for Strategic Planning, Cooperation, Projects, Analytics and Education	2027 Q 1 – Q4	Developed new modules for Integrity and National Strategy with dynamic creation and modelling of templates

Strategic Objective	Key Activities	Responsible Unit	Timeline (quarters)	Output/Indicator
Efficient Resource Management	Register of Official Vehicles – management and verification of data, connectivity with Mol	Unit for IT Support and General Affairs + Unit for Strategic Planning, Cooperation, Projects, Analytics and Education + International fund + Vendor	2027 Q2 – Q4	Functional register with verified data
Engagement of citizens in the fight against corruption	Development of ICMS – integrated system for receipt, review and notification of reports	Unit for IT Support and General Affairs + Unit for Prevention of Corruption + International Fund + Vendors	2028 Q1 – Q4	Functional reporting system
Innovative technologies	Artificial Intelligence (Prototype, pilot phase)	SCPC + Vendor	2028 Q1 – Q4	Prototype with automatic analysis and interactive communication
IT Capacity Building	Organize training for the staff on cyber security, digital forensics data analysis and new ICT technologies	SCPC + Vendors	Annually, Q1 – A4	Increased staff expertise and improved system maintenance. Two annual trainings were held for employees.

Table 4. Action Plan for 2026-2029

9.3 Annual Strategy Review and Revision Framework

To keep the strategy relevant and effective and the implementation of IT Systems, , an annual review process will be implemented, which includes the following:

1. Internal Review (Q1 each year)

- Led by the Sector for IT Support, General Affairs, Sessions and Public Relations in collaboration with the President and the Commissioners.
- Assess the following:
 - implementation progress of strategic objectives and key activities

- obtained outcomes in achieving the key activities
- relevance of regulatory requirements and legal changes
- system usage and efficiency reports.

2. Users' Feedback

- Information from relevant sectors and units in SCPC, according to the Action Plan
- Feedback from users (institutions, elected and nominated persons, citizens etc.)
- Data collection about user experiences and recommendations for improvement.

3. Performance Evaluation

- System efficiency evaluation and activities in relation to the set objectives
- Identify bottlenecks, underutilized systems or non-functional systems.
- Analysis of potential risks and proposals for their mitigation.

4. Revision & Action Plan Update (Q2)

- Amending the **Annual Action Plan** based on the review results and feedback information.
- Adjustments to timelines, budget allocations, or project scopes according to the new priorities.
- Approval of revised activities by the ICT Coordination Group of SCPC.

5. Documentation

- All results from the revision will be documented in a **Brief Annual ICT Strategy Review Report**.
- The Report will serve as basis for the next year's planning and improvement of the processes.