TESIM

Technical support to the implementation and management of ENI CBC programmes

Guide to developing management and information systems in ENI CBC programmes

Legal framework, standards, practices, tips and recommendations

Update June 2017

DISCLAIMER

This **non-binding document** has been developed by the TESIM project.

It does not necessarily reflect the views of the European Commission on the topic, and is presented to programme practitioners **for illustrative purposes only**.

A project funded by the European Union

Implemented by a consortium led by

particip

Table of contents

Clarification on update June 2017

The contents of the document originally delivered have been modified following the discussions which took place at the LabGroup meeting on monitoring & evaluation held in Brussels on 12-13 December 2016 and the networking event for ENI CBC Audit Authorities, held in Warsaw on 8-9 March 2017.

The modifications correspond to:

- **Removal of the conclusions of the INTERACT ENPI LabGroup held in September 2014**
- **Inclusion of INTOSAI standards on IT security in the section on applicable international standards**
- **New annex with check-list for security**
- **New annex on data structure for KEEP 2.0**

1. Aim of this guide

The **management and information systems (MIS)** are a key tool supporting programme implementation and part of the management and control systems (MCS), which need to be developed and set-up by the programme bodies and authorities.

There are specific requirements on information technology in the ENI CBC Implementing Rules, but they do not cover all the elements of the MIS. Additionally, other legislation (both European and national), as well as internationally accepted frameworks and standards are to be applied.

Therefore, in the scope of this legal framework and standards, this document aims at supporting the ENI CBC **Managing Authorities** for the design and development of MIS, **especially during the designation process** and effective and efficient programme implementation.

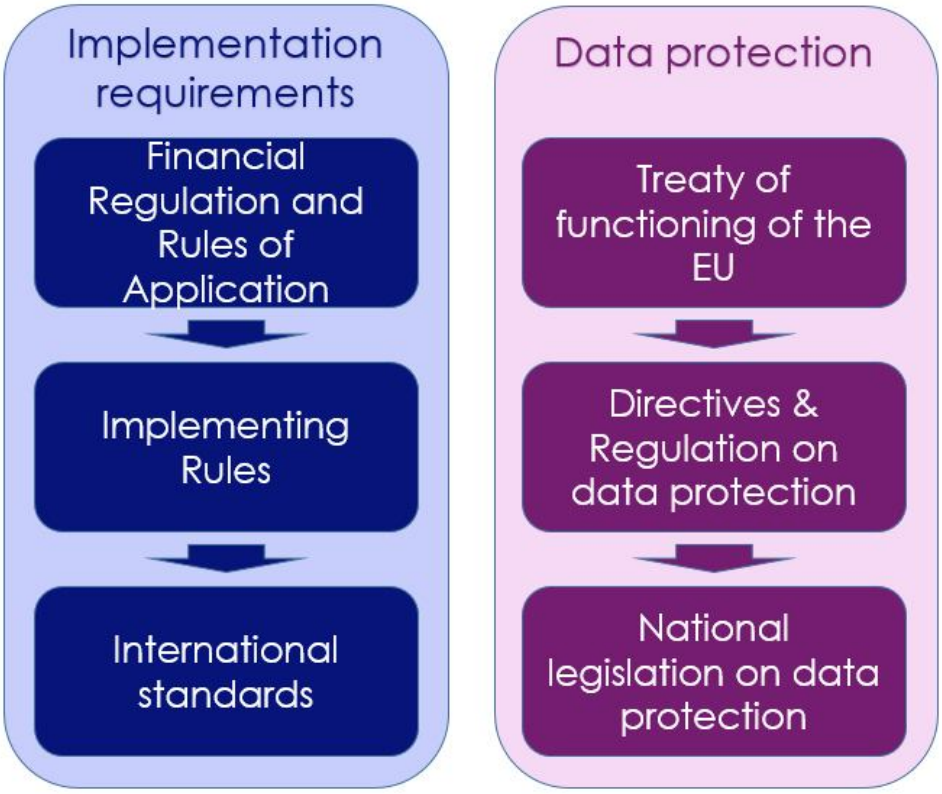
The document, which is not endorsed by EC and is therefore not compulsory, also aims at supporting the **Audit Authorities** in the **compliance assessment** during designation. It also describes the applicable framework and also some relevant practices in similar cross-border cooperation EU instruments.

On top of the key messages indicated throughout the different sections, this guidance also includes tips and recommendations. They may be taken into account during the IT policy design and implementation and may be included in the description of the management and control systems (DMCS).

This document aims at **setting the framework** and providing practices tips and recommendations for the systems to be developed by ENI CBC programmes in view of an **efficient and effective** contribution to the programme **implementation**, as well as the **compliance** with the designation criteria.

2. Legal framework

There are two main types of requirements applicable to MIS, which are regulated in different legal documents:



2.1. Requirements in the Financial Regulation

The Financial Regulation (FR, Regulation 966/2012), its Rules of Application (RAP, Regulation 1268/2012) and the ENI CBC Implementing Rules (ENI CBC IR, Regulation 897/2014) include provisions related to computerised information for programmes under shared management, which affect ENI CBC programmes.

The FR and its RAP are mainly focused on accounting, record keeping, payment authorisation and other financial procedures.

Even though non-computerised systems are still partially allowed, these regulations set the necessary requirements for an adequate computerisation of financial management. The main provisions are:

Article	Provisions
Article 48 of RAP: Keeping of supporting documents	"*The authorizing officer shall set up paper based or electronic systems for the keeping of the original documents relating to (...) budget implementation.* *The systems shall provide for (...) registers, which **may** be computerized, to be kept identifying the exact location of such documents.* *(...) Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes.*"
Article 105 of RAP: Material form of 'passed for payment'	"*(...) In a computerised system, 'passed for payment' **shall** take the form of an electronically secured validation by the authorising officer responsible or of a technically competent member of staff, duly empowered by the authorising officer responsible.*"
Article 93 of FR: Electronic management of operations	"1. *Where revenue and expenditure operations are managed by means of computer systems, documents **may** be signed by a computerised or electronic procedure.*"
Article 235 of RAP: Organisation of the accounts	"2. *Budget revenue and expenditure **shall** be recorded in the computerised system (...), according to the economic nature of the operation (...)*"
Article 236 of RAP: Computerised systems	"*1. The accounts **shall** be kept with the help of an integrated computerised system. (...)* *3. Access to the computerised systems and subsystems shall be confined to persons included on a list of authorised users which is kept and updated by each institution.*"
Article 112 of RAP: Description of IT systems	"*Where computer systems and subsystems are used to process budget implementation operations, a full and up-to-date description of each system or subsystem **shall** be required.* *Each **description** shall define the **content of all data fields** and describe how the system treats each individual operation. It shall show in detail how the system guarantees the existence of a complete **audit trail** for each operation.*"
Article 113 of RAP: Periodical save	"*The data in computer systems and subsystems **shall** be saved periodically and kept in a safe place.*"

Article 94 of FR: Transmission of documents	"*Subject to the prior agreement of the institutions and Member States concerned, any transmission of documents between them **may** be done by electronic means.*"
Article 95 of FR: e-Government	"*1. Under shared management, all official exchanges of information between the Member States and the Commission **shall** be carried out by means indicated in the sector-specific rules. Those rules **shall** provide for interoperability of data gathered or received, and transmitted in the management of the budget.* *2. The institutions (...) **shall** establish and apply uniform standards for the electronic exchange of information with third parties participating in **procurement and grant procedures**. In particular, they shall, to the greatest possible extent, design and implement solutions for the submission, storage and processing of data submitted in grant and procurement procedures, and to this end, shall put in place a single 'electronic data interchange area' for applicants, candidates and tenderers.*"
Article 161 of FR: Court of Auditors' right of access	"*7. Use of integrated computer systems **shall not** have the effect of reducing access by the Court of Auditors to the supporting documents.*"
Article 179 of RAP: Electronic exchange systems	"*1. All exchanges with beneficiaries, including the conclusion of grant agreements, the notification of grant decisions and any amendments thereto, **may** be done through electronic exchange systems set up by the Commission.* *2. These systems shall meet the following requirements:* *(a) only authorised persons may have access to the system and to documents transmitted through it;* *(b) only authorised persons may electronically sign or transmit a document through the system;* *(c) authorised persons must be identified through the system by established means;* *(d) the time and date of the electronic transaction must be determined precisely;* *(e) the integrity of documents must be preserved;* *(f) the availability of documents must be preserved;* *(g) where appropriate, the confidentiality of documents must be preserved;* *h) the protection of personal data in accordance with the requirements of Regulation (EC) No 45/2001 must be ensured.* *3. Data sent or received through such a system **shall** enjoy legal presumption of the integrity of the data and the accuracy of the date and time of sending or receiving the data indicated by the system.* *A document sent or notified through such a system **shall** be*

	considered as equivalent to a paper document, shall be admissible as evidence in legal proceedings, shall be deemed original and shall enjoy legal presumption of its authenticity and integrity, provided it does not contain any dynamic features capable of automatically changing it. *The electronic signatures referred to in point (b) of paragraph 2 shall have the equivalent legal effect of handwritten signatures.*"

2.2. Requirements in the ENI CBC Implementing Rules

The ENI CBC IR, i.e. the sector-specific applicable Regulation, include also provisions related to information technology:

Article	Provisions
Article 4: content of JOP	"*(m) a **description of IT systems** for the reporting and **exchange of computerised data** between the Managing Authority and the Commission.*"
Article 26: functions of the Managing Authority	"2. *(d) establish and **maintain a computerised system** to record and store data on each project necessary for monitoring, evaluation, financial management, control and audit, including data on individual participants in projects, where applicable. In particular, it shall record and store technical and financial reports for each project. The system shall provide all data required for drawing up payment requests and annual accounts, including records of amounts recoverable, amounts recovered and amounts reduced following cancellation of all or part of the contribution for a project or programme.* *5. (i) **maintain computerised accounting records** for expenditure declared to the Commission and for payments made to beneficiaries*"
Article 30: General principles of management and control systems	"*1. (c) electronic data systems for accounting, storage, monitoring and reporting.*"
Annex: Designation Criteria for the Managing Authority	"*3. (v) Procedures for establishing a system to collect, record and store electronically data on each project and for ensuring that the IT systems are secured in line with internationally accepted standards.*"

The ENI CBC IR do not give details on the type of information to be recorded in the computerized systems. A source of inspiration for a detailed list of fields may be found in Annex A1 of this document, which is intended as an adaptation of article 24 and Annex III of Regulation 480/2014, supplementing ESIF Common Provisions (Regulation 1303/2013), which is not compulsory in the ENI CBC context and it would be very difficult to apply.

Key message:
When using Annex III of the Regulation 480/2014 as a source of inspiration, we took into account that the list of fields is linked to the information exchange system used by DG REGIO, which is not used by DG NEAR, who will use KEEP instead, and this for specific purposes only. **Any legal reference indicated in the annex to Regulation 480/2014 is not applicable in ENI CBC. Therefore, not all fields nor all information contained in its description are necessarily useful in the ENI CBC context. A proposed adaptation is annexed to this document (see annex A1).**

2.3. Summary of legal provisions in the Financial Regulation and the ENI CBC Implementing Rules

In summary, the different applicable regulations contain the following provisions on information technology affecting the programmes:

Compulsory Provisions	Source
Electronic secured validation for authorizing procedures	RAP
Computerised accounting system, including a list of authorized users	RAP & IR
Description of computerized accounting system	RAP & IR
Periodical saving and keeping of information in a safe place	RAP
IT system for the reporting and exchange of computerized data with the EC[1]	FR & IR
Interoperability of financial data in official exchange with EC[2]	IR
Electronic exchange of information with third parties participating in procurement and grant procedures to the greatest possible extent	FR
Ensured access to Court of Auditors to supporting documents in integrated computer systems	FR

[1] As in the ENI CBC Implementing Rules, which require in Article 4 "*IT systems for the reporting and exchange of computerised data between the Managing Authority and the Commission*".

[2] Further explanation of these requirements is provided in Article 26.2.(d) of the Implementing Rules.

Procedures for establishing a system to collect, record and store electronically data on each project	IR
IT system is secured in line with internationally accepted standards[3]	IR

Optional provisions	Source
Electronic original documents and computerized register for exact location of documents	RAP
Electronic signature for management of operations	FR
Electronic transmission of documents between EC and Member States	FR

2.4. Data protection

Data protection is a fundamental right in the EU. The applicable legislation on data protection derives directly from the Treaty of Functioning of the European Union (Lisbon Treaty):

Article 16 of TFEU
(ex Article 286 TEC)

1. **Everyone has the right to the protection of personal data concerning them.**
2. **The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.**

These provisions are further explained in the Directive 95/46/EC (Data protection directive), which defines how protection of the personal data has to take place and sets limits on collection and use of personal data.

[3] COBIT & ISO standards, further explained in the chapter 3 of this Guide.

It defines that the "*personal data*" is information related to an **identified or identifiable natural person**, that is, information allowing to either establish the identity of the person (identified natural person) or identify, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (Identifiable natural person).

Other legal rules at EU level are Regulation (EC) No 45/2001 and the e-Privacy Directive 2002/58/EC. Moreover, all these principles for the use of personal data have been implemented in the Member States through the national data protection law.

Key message:

The MIS needs to comply with the applicable national legislation on data protection for information relating to any natural person (applicants and beneficiaries, project participants, staff of the programme bodies and authorities, staff of national authorities).

The compliance with this legislation shall be checked at least by the Audit Authority in the context of the systems audit, as it is not a blocking requirement for designation.

2.5. Web accessibility

On the 26th October 2016, the European Union published a Directive on the accessibility of the websites and mobile applications of the public-sector bodies, which will affect the websites and on-line applications of the ENI CBC programmes by the end of the programming period, but not during the designation process. Therefore, the provisions of the Directive are not yet applicable to any software developed in 2016 or 2017.

The accessibility requirements set out in the Directive describe what must be achieved in order for the user to be able to perceive, operate, interpret and understand a web-site, a mobile application and related content.

The four **principles** of accessibility are:

- **Perceivability**, meaning that information and user interface components must be presentable to users in ways they can perceive;

- **Operability**, meaning that user interface components and navigation must be operable;
- **Understandability**, meaning that information and the operation of the user interface must be understandable;
- **Robustness**, meaning that the content must be robust enough to be interpreted reliably by a wide variety of user agents, including assistive technologies.

An **European standard** is compulsory - EN 301 549 V1.1.2 (2015-04) - even though **national standards** are accepted, as defined by article 4 of Regulation 1025/2012. Therefore, the programmes must check if there is applicable legislation in the Member State hosting the Managing Authority. **ISO/IEC 40500** standard may also be used, in absence of specific national ones.

Member States shall apply this Directive by 23rd September 2020 for web-sites of the public sector published before 23rd September 2018.

Key message:
MIS needs to comply with the applicable national legislation on web accessibility. **The compliance with the new Directive is recommendable, as the programme web-sites and on-line applications will need to be in line with it before the end of the programming period, with the exception of the ones for the submission of proposals.**

2.6. In view of the designation

Compliance with IT requirements is a key challenge for designation, as it is one of the cornerstones of programme management needing a very technical work, in order to make it comply with the applicable requirements.

There are several **pillars** in the designation criterion 3 (v) concerning IT:

Type of requirement	How to comply
Content	Minimum information required in the different articles

	of the ENI CBC Implementing Rules
Security	Requirements in international standards, such as INTOSAI, ISO 27000:2013 or COBIT. Additional requirements are needed for internet-based modules, such as OWASP guidelines (see section 3 of this document)
Data protection	Respect of the national legislation of the Member State hosting the Managing Authority

These elements are included in the questions 3.34 and 3.35 of the proposed check-list for compliance included in the TESIM guide for designation. However, the check-list includes other questions, inspired in the check-list for EGESIF programmes:

- A **description of the MIS**, including a flowchart, showing the different elements (or modules), the links between them and the indication whether they are internet-based or networked (see section 4 of this document);
- An indication of which parts of the system have been used in the **previous programming period**, as some modules may be the same, others upgraded and others brand new;
- A confirmation of the adequate **segregation of functions** in the use of MIS (see section 4 of this document);
- An assessment of the modules which are already **operational** and which ones are being developed, under test or yet to be developed. A reliable planning of the non-operational parts is essential for designation.

3. Applicable international framework and standards

As previously mentioned, the annex of the ENI CBC IR specifically stipulates the respect of internationally accepted standards.

The check-list for compliance assessment prepared for designation in EGESIF context explicitly mentions **COBIT** framework and **ISO** standards, so TESIM guidance on compliance refers to the same ones. Additionally, as it is mentioned in the EC Regulation on on-line security, we provide some information about **OWASP** guidelines. These last guidelines are already used by INTERACT's eMS software. Also **INTOSAI** provides two related standards on audit of IT, including IT security, as well an information document.

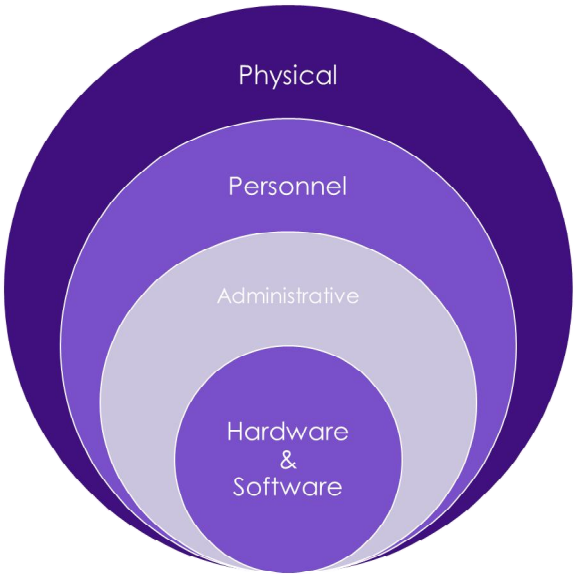
During the designation process, the auditors will need to assess whether international standards are observed in the case of already developed software and/or whether the MA has taken into account relevant international standards for the update and/or development of the systems.

3.1. INTOSAI

INTOSAI issued two standards related to IT:

- ISSAI 5300 Guidelines on IT audit
- ISSAI 5310 Information System Security Review Methodology

These standards define several layers of IT security to be checked:



Additionally, **INTOSAI** Capacity Building Committee published in 2015 a document called "***Managing Information Communications Technology***". The document is aimed as a support for Supreme Audit Institutions and confirms the same **standards** indicated by EGESIF for security issues as an **option** for ensuring it, but not an obligation. The document adds to them the **Information Security Forum** (https://www.securityforum.org/) as a source of good practices.

In particular, INTOSAI identifies the following **aspects of IT security**, which should be considered[4]:

a. **IT Security Policies**: the organisation should have sufficient policies which specify to staff what systems and data should be secured and what is acceptable and unacceptable behaviour when using the organisation's systems and data.
b. **Asset Management**: the organisation should have the systems in place to track the IT assets it has acquired and in particular to enable it to ensure that disposals are authorised and don't allow data to be lost or stolen.
c. **IT Risk Management**: the organisation should have procedures and processes in place to identify and monitor IT risks and manage issues as they arise. These should be included in the organisation's overall risk management process and escalated depending on the nature and scale of the threat which they pose to the organisation.
d. **Compliance**: the organisation should ensure that procedures and processes are in place to monitor and ensure compliance with IT security policies and procedures.
e. **Physical Security**: this applies to any premises with access to systems and data and includes locks on doors and windows, visitor/contractor escort and CCTV surveillance, proximity cards/readers on doors, turnstyle doors, etc., depending on the type of data center (either subcontracted or own)
f. **Environmental Security**: this applies primarily to data centers and computer/communication rooms and includes air conditioning, fire and flood prevention/detection systems, UPS (uninterruptible power supplies), fireproof safes for back-up and archive media, etc.

[4] A **check-list** based on them can be found in annex A2.

g. **Network Security**: this applies to the LANs and WANs used/operated by the organisation. (...) they include the physical and logical security of network equipment, firewalls and servers, and of network access points.
h. **Operating System Security and Database Security**: systems and databases should be configured and administered so that access is restricted to those system administrators whose job it is to support the applications used by the organization and unauthorised access is prevented. Direct access to databases should be restricted to database administrators; any reporting should ideally be run on a mirrored management information database.
i. **Desktop Security**: user account maintenance, password/login security settings, system access rights.
j. **Application Security**: user account maintenance, password/login security settings, access rights to system functions and segregation of duties.
k. **Data Security**: data security classification, back-ups/restores, encryption, two-factor authentication, user access rights.
l. **IT Service Security**: the organisation should determine the data recovery and business continuity arrangements required to ensure continuity of service.

A short explanation on the content of the standards recommended by INTOSAI and EGESIF and the link to the main documents are found below.

3.2. COBIT

The main international framework applicable to Information Technology (IT) recognized by the European Commission is issued by an organization called **ISACA** (http://www.isaca.org).

ISACA developed and maintains the internationally recognized COBIT®. (http://www.isaca.org/COBIT). The latest version, called COBIT5[5], defines a **framework for the governance and management of information technology** in companies and institutions, covering a range of tools, resources and guidance in the following areas:

[5] A free copy of the Framework is accessible at the same website.

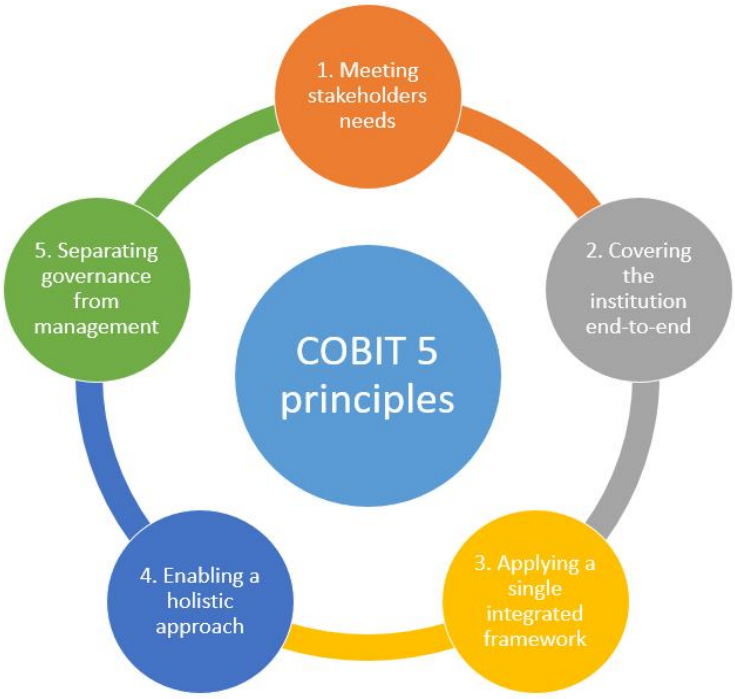
particip

The framework is based on the assumption that "*information is a key resource for all enterprises, and from the time that information is created to the moment that it is destroyed, technology plays a significant role. Information technology is increasingly advanced and has become pervasive in enterprises and in social, public and business environments*". As a consequence, the institutions need to strive to:

- Maintain high-quality information to support decision-making,
- Achieve strategic goals with the support of IT-enabled investments and the effective and innovative use of IT,
- Achieve operational excellence through the reliable and efficient application of technology,
- Maintain IT-related risk at an acceptable level,
- Optimise the cost of IT services and technology,
- Comply with relevant laws, regulations, contractual agreements and policies.

COBIT 5 provides a comprehensive framework that assists institutions in achieving their objectives for the governance and management of enterprise IT in a holistic manner, based on **5 principles.** Together, these five principles enable the enterprise to build an effective governance and management framework that optimises information and technology investment and use for the benefit of all stakeholders.

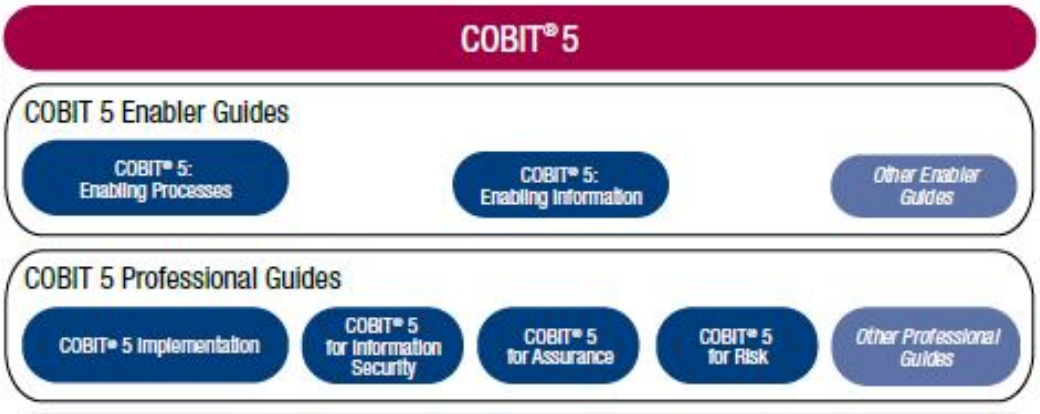
Se the 5 principles in the chart below:



Key message:

The MIS cannot be programme-body-oriented; it has to respond to the needs of all concerned stakeholders (applicants/beneficiaries, project selection committee and assessors, national authorities, programme bodies and authorities & European Commission)

On top of the global principles, COBIT has a set of more specific standards, among which there is one on security:



The one on information security may be used for ensuring the compliance with the security requirements mentioned in the designation criterion, together with ISO and OWASP.

3.3. ISO/IEC

The main international standards applicable to security are developed by the **International Organization for Standardization (ISO)**, in particular ISO 27001:2013 (http://www.iso.org/iso/iso27001), which is explicitly mentioned by the guidance documents from DG REGIO.

The ISO 27000 group of standards helps organizations keep information assets secure, such as financial information, employee details or information entrusted to by third parties.

In particular, ISO/IEC 27001 is the best-known standard, providing requirements for an **Information Security Management System (ISMS)**. An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

A specific check-list on ISO 27001:2013 is attached to this document, including the following aspects:

- Information security policies
- Organization of information security
- Human resources security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management

It is important to remark that some key questions on security are not strictly technical and cannot be outsourced to any software development company. Elements such as information security policies or human resources security policies are linked to the organization. Adequate description needs to be included in DMCS, either directly or with reference to the relevant documents of the hosting institutions.

Key message:

The programme has a wide range of stakeholders and needs to put in place some of the MIS in an internet-based platform, as well as some internal modules, such as authorization, payment and accounting.

As MIS is containing sensitive information, ensuring data security becomes a key requirement for designation.

3.4. OWASP

OWASP is the acronym for Open Web Application Security Project (http://owasp.org). Even though it is not recognized as an international standard, the **OWASP Top 10 project** provides an overview of the most critical web application security risks as well as tools for addressing these risks; the technical specifications therefore draw upon the findings of this project.

The Top 10 application security risks are:

1. Injection
2. Broken authentication and session management
3. Cross site scripting (XSS)
4. Insecure direct object references
5. Security misconfiguration
6. Sensitive data exposure
7. Missing function level access control
8. Cross site request forgery (CSRF)
9. Using known vulnerable components
10. Unvalidated redirects and forwards

Regulation 1179/2011, laying down technical specifications for online collection systems stipulates in art. 27.6 that a proper security configuration in place requires, at least, that: (...) "*(e) security settings in the development*

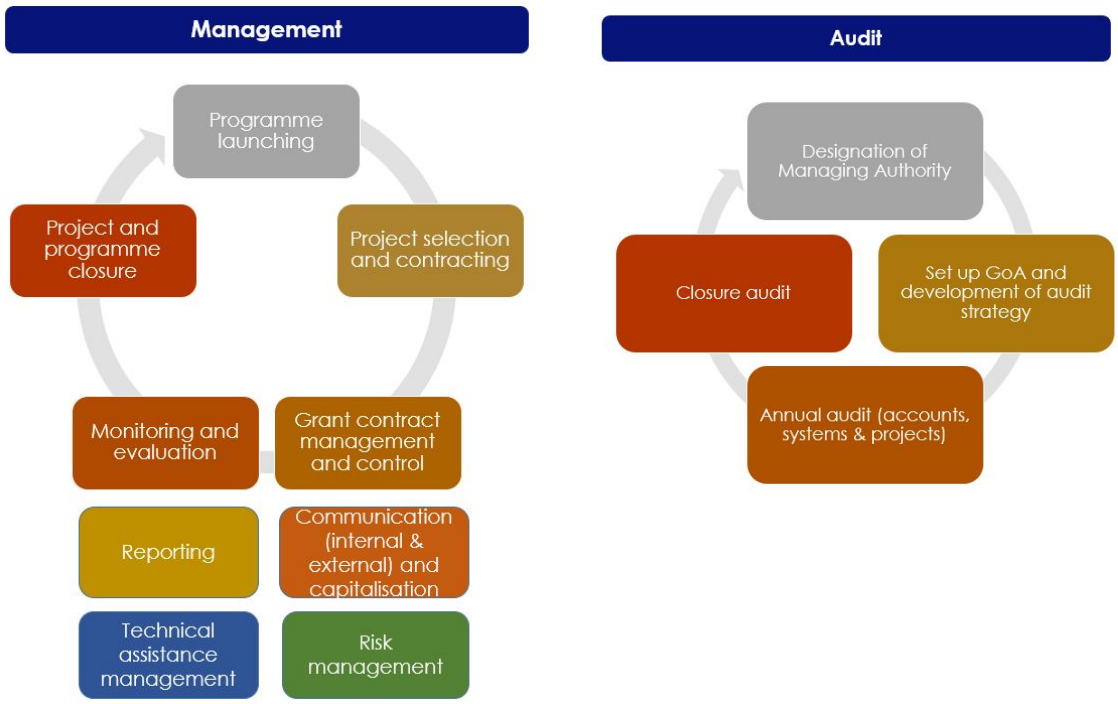
frameworks and libraries are configured in accordance with best practices, ***such as the guidelines of OWASP****.*"

Therefore, even though these guidelines are suggested by the EC, other similar ones may be applied, provided that they are clearly identified in the DMCS.

4. Programme processes in ENI CBC

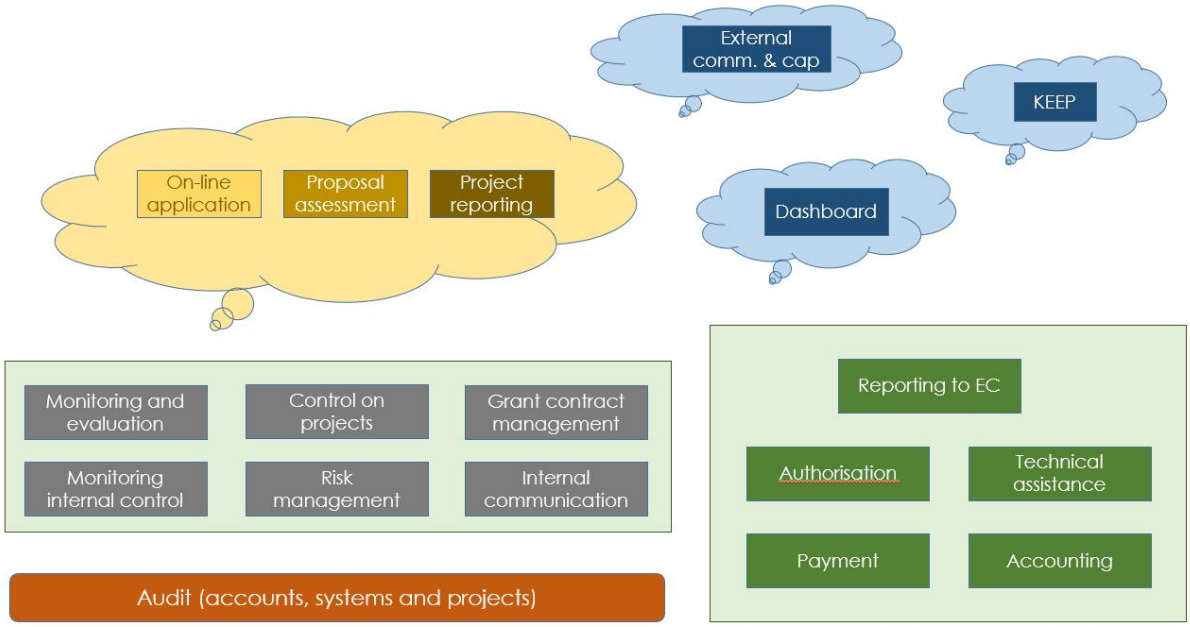
The holistic approach proposed by COBIT, including the institution end-to-end, may be translated to the ENI CBC context as the need to take into account **all the processes** which will take place during all the programme cycle, as well as **all the concerned stakeholders**.

We may summarize the main processes during the programme cycle as follows:



These **processes** need to be **integrated in the MIS** through a set of different modules and software, with different users and access methods. The modules may be developed *ad hoc* for the programme (or a group of programmes) or acquired in the market (e.g. for accounting, audit, etc.).

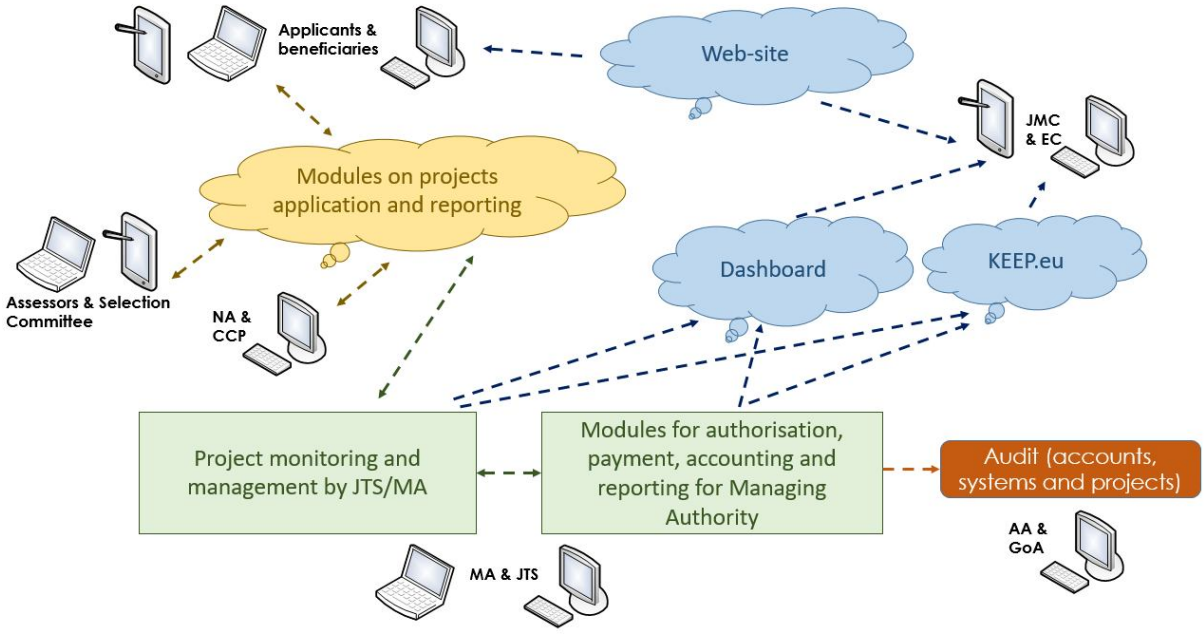
Some of the modules shall be accessible "*on the cloud*" and others will be "*classical*" management software of the bodies hosting the Managing Authority or the Joint Technical Secretariat. See an example in the chart below.



The different modules may be fully or partially connected. Nevertheless, a full connectivity between all systems in an automatic way is not possible, in particular for certain modules embedded in the usual procedures of the hosting organization for the Managing Authority, such as authorization and payments.

Key message:
The MIS should cover all the key programme processes, even if there are several software packages (with or without capacity of exchanging data amongst them).
The DMCS needs to include also the description of the MIS and how they are embedded into the procedures.

All the programme stakeholders should get access to these modules, with different levels of intensity and access rights, depending on their needs. See below an example of the type of accesses and the flows of information.



The description of the MIS in the DMCS has to include the type of access for each profile of stakeholder, showing that an adequate segregation of functions is respected.

Not all the modules need to be available from the beginning of the programme cycle. Some will be already available from the previous periods, while others will be adapted or updated during the launching phase, in accordance with the needs.

Either available or planned, all the modules and the type of software to be used, adapted or developed, should be identified in the initial DMCS used for the designation process. In the case of non-operational modules, a detailed reliable planning needs to be developed and referred to in the DMCS.

5. Monitoring requirements and reporting needs of the European Commission for 2014-2020 (KEEP 2.0)

The intention of DG NEAR is to use the KEEP database as a source of information on the contracted projects supported by the ENI CBC 2014-2020 programmes, as most of this information shall be available in KEEP.

Instead, the annual implementation report will rather focus on the outputs and results produced by the programme, use of programme indicators, examples of successful projects and good practices, as well as information on their monitoring and communication activities and use of the programme financing. The annual report shall be transmitted by e-mail.

The most important change planned for KEEP 2.0 is the **automatic transfer of data from the programme MIS**. KEEP selects the information needed for each project through fields describing it, e.g. project name, project summary, thematic objective, budget, etc. This information shall be transferred through an **XML file**[6], which should be generated automatically by the programme MIS. The data structure of the file is annexed to this document (annex A3), but also highlighted in annex A1.

The information required by KEEP includes the name of the project contact person. It is important to ensure that data protection rules are respected, as this name shall be available in the KEEP database, if the project is approved.

The data structure annex also includes some fields related to the calls for proposals, not to the projects.

[6] File is available upon request to TESIM.

6. Practices in cross-border cooperation

The results of the questionnaire sent to all ENI CBC programmes show the following results:

6.1. Practices in ENPI CBC 2007-2013

As lessons learned from the previous programming period, the programmes identify the following changes needed:

- introduction of online application and reporting forms;
- availability of all documents and reports in the system;
- possibility to generate evaluation reports from the system;
- availability of results of the on-spot checks;
- administrator rights for the MA;
- access rights for the lead beneficiaries and viewing rights (or full access);
- improvements of user-friendliness of the system;
- improving printing option from the system;
- improvement of the statistics generation from the system.

Even though some of these aspects may be similar to the requirements indicated in e-Cohesion documents, they may be a source of inspiration, but they are not compulsory in the ENI CBC legal framework.

Few programmes will upgrade the systems used in 2007-2013, two will use eMS from INTERACT, while most of them have decided to develop new software.

6.2. Practices in ENI CBC 2014-2020

The main new features included in the 2014-2020 MIS, as stated in the questionnaire, are the following:

- on-line application will be made possible for most programmes, and thus more data will be uploaded online by applicants directly into the MIS;
- reduction of paper documents, especially on the stage of the application and concerning project reporting;

- more programme bodies will have access to the system and will be able to benefit from the information stored there;
- more programmes will provide access rights to the MA for the lead beneficiaries and the beneficiaries.

The modules included in the MIS are the following for the programmes having answered the questionnaire:

	EERU	LVRU	KAR	KOL	LLB	ROUA	ROMD	ITTU	PBU
Applications and project data	x	x	x	x	x	x	x	x	x
Assessment and selection	x	x	x	x		x	x		
Contracting	x	x	x	x		x	x		
Monitoring	x	x	x	x	x	x	x	x	x
Reporting	x	x	x	x	x	x	x	x	x
Payments	x	x	x	x	x	x	x		x
Technical assistance						x	x	x	x
Accounting		x				x	x	x	
Statistics	x	x	x	x	x	x	x	x	x
System administration	x	x	x	x	x	x	x	x	x

The roles and the rights are allocated to each user specifically based on their role in the programme:

MA and/ or JTS	• administration rights • can introduce and modify information in the system
Branch Offices	• reading rights • in few cases can also introduce information to a limited extent
Control Contact Points	• usually have reading rights • possibility to upload the expenditure verification reports directly into MIS to be explored
Auditors performing expenditure verification	• reading rights • usually have access to the project applications
JMC members	• reading rights
External project assessors	• reading rights • possibility to upload evaluations
Audit Authority and members of the Group of Auditors	• reading rights
Lead beneficiaries	• in the programmes that have the on-line application, have right to upload, view, correct information
Beneficiaries	• in the programmes that have on-line application, right to view and add information

Additionally, most programmes will benefit from:

- automatic calculations,
- system-generated alerts,
- on-line status tracking,
- availability of history of the files
- exchange of data with KEEP.

On security issues, the programmes state:

- Several of them will use encrypted channels (protected by **SSL** protocol) for the communication between the system and its users
- Security measures of several systems following the guidelines developed by the "Open Web Application Security Project" (**OWASP**)

Example of the Romania – Ukraine ENI CBC and the Romania – Rep. of Moldova ENI CBC programmes:

The system is secured at the following levels:

Security at the network level
The application server will be installed inside a secured network. Firewall systems will assure network security over various network types of attacks.

Security at transport level
Transport of the information over the internet is made over secured SSL channel. The application server is configured with a SSL certificate and such, all the traffic between the application server and the user is made through encrypted channel.

Security at the application level
The application has its own identity management and authorization module. User groups and roles were created according to the business process needs. Users have access rights to specific view perspectives and information only according to their authorization. User authorization is considered though their associated roles.

Anti-robot security
User registration and user authentication is protected by captcha codes to block exploiting of such functions by automated tools. User registration may complete only after validation of and email address.

Development framework level security
During the development process, security measures were taken to mitigate top ten security flaws according to OWASAP https://www.owasp.org/

Security tests
Security test, with dedicated security tools, were executed against the application.

- User identification will be done in all programmes using a login and a **password**. Several programmes mentioned that they will define their own security requirements for the passwords

7. Conclusions, tips and recommendations

As final conclusions, here are some tips and recommendations for a successful set-up of a compliant MIS:

1. **MIS requirements** in the new period are much wider than in the previous ones. A simple update of the approach of the previous period may not be enough;
2. A **dedicated team** with adequate technical support is needed for the development of the MIS part of the DMCS. This team has to ensure good knowledge of the organisations hosting the different programme bodies, the needs of all stakeholders, good knowledge of legal requirements and of the applicable international standards;
3. The **new responsibilities by countries** and their co-ownership in the definition of the MCS, the compliance with **new legal requirements** in the Financial Regulation and the ENI CBC Implementing Rules, and the need of a better **beneficiary-oriented MIS** are some of the **key cornerstones** for the new period;
4. Important decisions may need to be taken at organizational level to adapt its usual policies to the new requirements. The **commitment from the top management** level is essential from the beginning;
5. The **full MIS shall not be developed and operational** at designation phase, but a compliant initial design and a detailed planning are needed.

Annexes

A1: detailed check-list for data on projects

This detailed check-list aims at identifying a list of recommended minimum requirements for the IT systems in detail. Annex III of the Regulation 480/2014 is our source of inspiration, with the necessary adaptations to the specificities and legal requirements of ENI CBC.

It takes into account the specificities of ENI CBC and provides details on the content of the IT system, as a complement of the general check-list for designation developed by TESIM on the first part of the key question for this designation criterion, that is "**procedures for establishing a system to collect, record and store electronically data on each project**".

A2: check-list on security

It serves as a guidance to the compliance on security issues, as stipulated in INTOSAI documents. It is also a complement of the general check-list for designation developed by TESIM on the second part of the key question for this designation criterion, that is "**procedures for ensuring that the IT systems are secured in line with internationally accepted standards**".

A3: KEEP 2.0 data structure

It contains the list of fields to be transferred to KEEP, together with a description ensuring a shared understanding on the information contained in each one. The fields included in this document, prepared by INTERACT, are highlighted in annex A1.