8.16 GOVSEC - SECURE GOVERNANCE (2018.09)

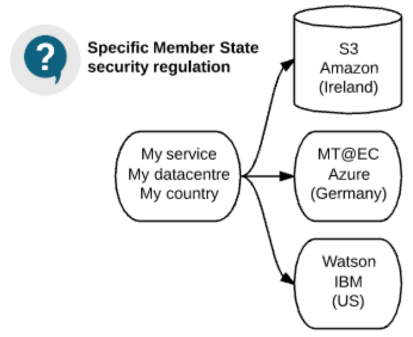
8.16.1 IDENTIFICATION OF THE ACTION

Service in charge	DIGIT
Associated Services	EU Institutions, Member States

8.16.2 EXECUTIVE SUMMARY

With the emergence of the micro-services paradigms and Cloud technologies, information system are becoming more and more independent bricks put together to deliver high value services, geographically dispatched, and implemented by various service providers at all levels.
Moreover the security regulations which apply to these various systems are not harmonised, policies varies from organisations to organisation, even within a member state. So a key disabler for inter-operable services mays in the difficulty to answer a simple question: "**Is it safe to use this service?**"

Imagine a service is using Amazon S3, Watson from IBM for sentiment analysis, and the translation system provided by Commission; hosted in Azure. The service itself has to prove compliance in terms of security of all the technical components, against a specific Member State security regulation. In this context it becomes very difficult for business stakeholder in a member state to manage the risk related to all the individual bricks which compose a service and prove compliance afterwards.


?
Specific Member State security regulation
S3 Amazon (Ireland)
My service My datacentre My country
MT@EC Azure (Germany)
Watson IBM (US)

The solution today is writing specific security compliance document, expensive to write, not reusable, and impossible to maintain. The technical security controls are usually not aligned towards these documentations.

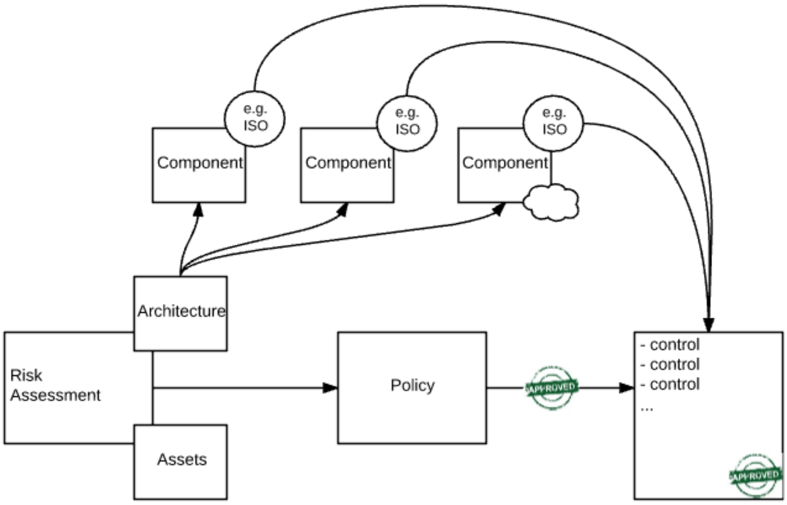
To circumvent this problem we propose in the present action to develop a **methodology**, **sustained by the appropriate IT tooling**, which will:

- Guide business stakeholders in assessing the risk in relation to their service
- Implement the governance policy of an organisation, such as a Member State, to ensure that the service
- Provide a check-list of controls and measure to be taken by the technical services to ensure that the proper security level is implemented
- Using the same check-list, help auditors to ensure that the controls are properly implemented.

The idea of the methodology is simple:

- A stage where the risk in relation to the service is analysed, to help the business stakeholder
- A stage where the risk analysis is proven against the policy of the organisation against the criteria decided by the organisation (political criticality, data sensitiveness…)
- A stage where the service is described in terms of technical bricks which are them-selves interoperable components or building blocks (i.e. databases, storage…); each building block

describes how they implement security against commonly admitted frameworks such as the one provider by ENISA or ISO.



If the approach is successful, it can open the door to a common repository of component usable by the public sector which would adhere to it, and would allow aligning security policies. It would also allow sharing definition of common components such as the one of Public Cloud providers, and could be used in the scope of public Call for tenders.

The action is not overlapping other initiatives of Commission and specifically DG CONNECT in terms of certifications and code of conducts; but is complementary to them. The security assurance for the customer is coming from one hand from the fact that the Cloud provider covers most of controls (usually at infrastructure level), in a secure way, validated by certification and code of conduct. However crucial, this does not cover the controls that the customer still has to implement, with the pitfall that the border between customer and providers vary depending on the provider. The methodology allows precisely defining the border and giving assurance that either the Cloud provider or the customer covers all the controls, at a low operational level. In order to achieve this objective, the methodology will use a state of the art family of controls compatible with the standard ISO/IEC 27001, such as the ENISA Cloud Certification Schemes Metaframework[59], which is compliant with COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 of 8 September 2015 on the interoperability framework and will ensure easier portability with the member state.

A key aspect of the action is dissemination and engagement of Member States towards this methodology. The methodology had already been identified as beneficial by EU Institutions (EU Agencies, Commission) which will by default part of first pilots, but engagement of Member States and the opportunity to align Member States around security requirements, without forcing them will already be a real achievement.

8.16.3 OBJECTIVES

By providing public services with a holistic but customisable approach to manage the question of compliance of interoperable components in terms of security by putting risk assessment process and

[59] Commission is already using these frameworks as reference framework for security certification.

business impact analysis process as one of the corner stone within decision process of each public service and develop common semantics around them, the present action aims at facilitating the dissemination of these components and breaks the regulatory barriers between member states, while respecting their specificities and therefore support interaction between European public administrations and/or between Administrations Citizens and Businesses. European public services using this framework will be able to exchange security definition of their respective components to prove their compliance towards their respective regulations. This is a key enabler to develop, maintain, facilitate and even share registries of inter-operable solutions.

8.16.4 SCOPE

Large organisations, like banks, hospitals, or public sector organisation, have mature IT security governance processes aligned with the ISO27K1 standard, which require due-diligence and detailed IT security risk management, for each component in the IT infrastructure as well as the IT infrastructure as a whole.

In the past a lot of the IT components were custom-built for that organisation, but increasingly an organisation's IT is composed of standard COTS products, services, micro-services and standard components, which are then integrated and interconnected.

This means that many organisations are, independently, doing the same IT security risk assessment for the same standard COTS ICT products and components. This is inefficient and time-consuming. Sharing and re-using each other's past risk management work would save a lot of time and money. And it would allow organisations to focus on the aspects that differentiate their organisation from others. This is especially important considering the threat landscape and the shortage of IT security experts.

This action aims to develop an open platform for organisations and experts, in the public and private sector, to share and exchange IT risk management work they have done in the past about specific ICT products and/or components, using a common structure and format. The platform becomes not only an information source for risk management professionals, but it directly helps participants by allowing them to re-use each other's work.

The action will deliver a documented methodology and sustaining IT platform and the supporting actions (like training material, common repositories for key stakeholders), which will be both made available on open-source platform repositories (such as Join-up or similar). The IT platform will allow the Public administration to customise the various components to their needs. Part of the scope of the action is the engagement of Public administrations towards the methodology and tooling, which should be adapted depending on the feedback of the various interested stakeholders. During the period of the action we will provide support to the Public services deploying the methodology and tooling. It is in scope that Public services using the framework will be able to share components managed by the framework: the framework is itself inter-operable.

8.16.5 ACTION PRIORITY

This section is used to assess the priority of the proposal to become a programme's action according to Art. 7 of the ISA^2 decision[60].

8.16.5.1 Contribution to the interoperability landscape

The contribution of the action to the interoperability landscape, measured by the importance and necessity of the action to complete the interoperability landscape across the Union

Question	Answer
How does the proposal contribute to improving interoperability among public administrations and with their citizens and businesses across borders or policy sectors in Europe? *In particular, how does it contribute to the implementation of:* • *the new European Interoperability Framework (EIF),* • *the Interoperability Action Plan and/or* • *the Connecting European Facility (CEF) Telecom guidelines* • *any other EU policy/initiative having interoperability requirements?*	The adoption of Cloud services and distributed systems systematically raise the question of how secured are these services in terms of IT security and data protection within EU public administration, using any kind of public cloud provider. It is urgent that public services get support to ensure compliance of their services towards one-another, but also that provider and user will be able to use same semantics. The current proposal contributes to help public administration to have a common ground in an open and transparent way, to easily solve this question, at low cost. It is fully horizontal, potentially reusable all among EU, and will help feed catalogues of interoperable solution. It will reuse with benefits all the frameworks defined by ENISA in terms of security.
Does the proposal fulfil an interoperability need for which no other alternative action/solution is available?	No similar approach identified; usually implemented by ad'hoc expensive consulting.

8.16.5.2 Cross-sector

The scope of the action, measured by its horizontal impact, once completed, across the policy sectors concerned.

[60] DECISION (EU) 2015/2240 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

Question	Answer
Will the proposal, ***once completed*** *be useful, from the interoperability point of view and utilised in two (2) or more EU policy sectors? Detail your answer for each of the concerned sectors.*	By nature, the action is being purely horizontal, the action is an enabler for any EU policy sector which involves inter-operability. Specifically the action is an enabler in the field of adoption of Cloud technologies, which multiplies the number of building blocks involved in an inter-operable service.
For proposals completely or largely ***already in operational phase,*** *indicate whether and how they have been utilised in two (2) or more EU policy sectors.*	Not applicable

8.16.5.3 Cross-border

The geographical reach of the action, measured by the number of Member States and of European public administrations involved.

Question	Answer
Will the proposal, ***once completed,*** *be useful from the interoperability point of view and used by public administrations of three (3) or more EU Members States? Detail your answer for each of the concerned Member State.*	By nature, the action being purely horizontal represents an enabler for any Member State wishing to use it. Provided Member States adopt the framework described in the action they will be able to share definition of components in terms of security. EU institutions are already interested in the methodology which represents a first set of users of the framework.
For proposals completely or largely ***already in operational phase****, indicate whether and how they have been utilised by public administrations of three (3) or more EU Members States.*	Not applicable.

8.16.5.4 Urgency

The urgency of the action, measured by its potential impact, taking into account the lack of other funding sources

Question	Answer
Is your action urgent? Is its implementation foreseen in an EU policy as priority, or in EU legislation?	Compared to the private sector, or other Public Services in the world, Europe has difficulties to embrace Cloud services, which are an inevitable enabler for inter-operable solutions. The cause mainly lies in the security aspect, since Cloud is outsourcing, performed at a massive level. Therefore it becomes urgent to provide a solution to this problem, while not making compromise in security. The present action is a solution to that problem. EU has adopted cloud strategy already 2012, but currently on the market US providers prevail, therefore we believe EU governmental cloud adoption could be wider, if supported through common approach by EU institutions.
How does the ISA^2 scope and financial capacity better fit for the implementation of the proposal as opposed to other identified and currently available sources?	By nature ISA² focuses on inter-operable solutions for Public administration, which is precisely the scope of the proposed action.

8.16.5.5 Reusability of action's outputs

The re-usability of the action, measured by the extent to which its results can be re-used.

Can the results of the action (following this proposal) be re-used by a critical part of their target user base, as identified by the proposal maker? For proposals or their parts already in operational phase: have they been re-used by a critical part of their target user base?

Name of reusable solution to be produced (for new proposals) or produced (for existing actions)	GOVSEC (Governance for Security)

Description	The proposal delivers a methodology (Business Impact Assessment, Risk management, Policy and Implementation…) and anIT supporting tool for the methodology on Information system security. It targets specifically security in the Cloud.
Reference	Return of experience of European Commission in the field of IT security, ENISA research on Cloud Security, CONNECT funded project: CloudForEurope, CloudWatch
Target release date / Status	First version and initial dissemination – 2018 Final version and end of dissemination - 2019 Documented methodology and framework – 2020
Critical part of target user base	Core users - EU Institutions and agencies Dissemination – All EU member states
For solutions already in operational phase - actual reuse level (as compared to the defined critical part)	Not applicable

[copy and use a separate table for each output foreseen]

8.16.5.6 Level of reuse of existing solutions

The re-use by the action (following this proposal) of existing common frameworks and interoperability solutions.

Question	Answer
Does the proposal intend to make use of any ISA[2], ISA or other relevant interoperability solution(s)? Which ones?	The action will use Join-up for dissemination. The action, since it aims at providing an inter-operable open-source platform, will use of support the inter-operable components necessary for its architecture such as identity and exchange of data.
*For proposals completely or largely **already in operational phase**: has the action reused existing interoperability solutions? If yes, which ones and how?*	Not applicable

8.16.5.7 Interlinked

Question	Answer
Does the proposal directly contribute to at least one of the Union's high political priorities such as the DSM? If yes, which ones? What is the level of contribution?	We are following the DSM on the intersection of two main areas (2) to protect Europe's assets by tackling **cybersecurity challenges**, and (3) to promote the **online platforms (such as joinup)** as responsible players of a fair internet ecosystem and help building common cyber-secure infrastructure across all parts of the EU so that EU governments can use same approaches in respect to IT security topics. ICTs are already widely used by government bodies, as it happens in enterprises, but eGovernment involves much more than just the tools. It also involves rethinking organisations and processes, and changing behaviour so that public services are delivered more efficiently to people. Also, when implemented well, eGovernment enables citizens, enterprises and organisations to carry out their business with government more easily, more quickly and at lower cost. How do we plan to contribute: By developing common semantics on security risk assessment by public authorities EU wide, our project will enable European usage of public clouds in more transparent way-from technical perspective open source approach will be taken and from the content perspective common semantics will be developed on security risks introduces in public authorities by using public cloud services

8.16.6 PROBLEM STATEMENT

Current state-of the-art on this field is that there exist research of this field, done by some EU funded projects (CloudWatch[61], CloudForEurope[62]), but there is no common infrastructure in place, which would enable interoperability between EU institutions and member countries, with common semantics in place for security risk analysis of public cloud offering for public authorities.

The problem of	Proving security compliance of an inter-operable service
affects	The adoption of inter-operable services
the impact of which is	Not using inter-operable service for security reason
a successful solution would be	Proving a service is compliant with a specific Member State security policy

The problem of	Adopting Cloud based services for security reasons
affects	The efficiency and costs of inter-operable services
the impact of which is	Poor adaption of inter-operable service for technical or cost reasons
a successful solution would be	Ensure compliance of these Cloud services towards a specific Member State security policy

The problem of	Cost of compliancy security analysis, which has to be made for each individual service
affects	The capacity of public services to produce new services, for budget reasons
the impact of which is	Abandoning deployment of services, for budget reasons
a successful solution would be	Minimizing the cost of security compliance analysis (one benefit of the action)

[61] http://www.cloudwatchhub.eu/sites/default/files/D3.2_Risk-Based-Decision-Making-Mechanisms-For-Cloud-Service-In-The-Public-Sector.pdf

[62] http://www.cloudforeurope.eu/documents/10179/51418/Public+administration+requirements+and+vendor+offering/045deb19-744f-4ff4-9c4d-a2e4fa1f0e29?version=1.0

The problem of	Services evolve on a constant basis
affects	The security of the whole chain, in case a change impact a security element
the impact of which is	Running unsecured services, without even knowing it
a successful solution would be	Being able to react to a change

8.16.7 IMPACT OF THE ACTION

8.16.7.1 Main impact list

[Maximum 200 words].

List the impacts of the action's outputs (following the proposal) on the beneficiaries to the extent possible. Some impacts are listed below – add others as needed.

Impact	Why will this impact occur?	By when?	Beneficiaries
(+) Savings in money	Yes, no need for expensive security compliance analysis (~100K€/service)	End of 2018 2019	EU Institutions Other adopters
(+) Savings in time	Yes, no need for expensive security compliance analysis (~100K€/service)	End of 2018 2019	EU Institutions Other adopters
(+) Better interoperability and quality of digital public service	Yes, by ensuring usage of Cloud technologies is safe	End of 2018 2019	EU Institutions Other adopters
(-) Integration or usage cost	No, very small system to operate		
(+) Security	Yes, ensure security at a very low level (up to security controls implementation)	End of 2018 2019	EU Institutions Other adopters
(+) End-user adoption	Yes, security drives to confidence of end users	2020	EU citizens

8.16.7.2 User-centricity

An important part of the action is called Dissemination: it consists in disseminating the principle of the present Framework to its actual users:

- The first set of users are the EU Institutions which already raise interest in the approach; this group of interest will be engaged through the various channel already available but they are a de-facto participant of the action.
- The second action will consist in disseminating the concept to other Public Services in Europe using regular dissemination channel for reusable components. The dissemination will be performed to the authorities responsible for security compliance among the Member States; the Commission and DG CONNECT and ENISA will help on that matter.
- If the interest is rising among the mentioned authorities, they will be able to be engaged from 2019: they will be able to use the framework, and a specific structure to take their feedback into account will be put in place. This structure, depending on the involvement of the pilots, can go from the active integration of requirements to the development of an open-source community.

8.16.8 EXPECTED MAJOR OUTPUTS

Output name	Methodology for Security Governance
Description	Documented generic methodology to ensure compliance of an inter-operable service using other inter-operable components such as Cloud services
Reference	Return of experience of European Commission in the field of IT security, ENISA research on Cloud Security, CONNECT funded project: CloudForEurope, CloudWatch
Target release date / Status	End 2018

Output name	Impact assessment of the methodology in MS
Description	As a result of dissemination activities among the member states, a report of the potential impact of the methodology among the Member states
Reference	Usage of an Open Source model ensures reusability of the methodology and tooling and is part of the dissemination strategy. The security controls used in the last module are by nature reusable by all users of the methodology (e.g. a description of Amazon S3 could be reused by all member states).
Target release date / Status	End 2019

Output name	Platform for Security Governance
Description	An open-source platform available on join-up, which can be deployed, installed and customised to its business

	need by a Public Service, sustaining the flow of the methodology
Reference	Return of experience of European Commission in the field of IT security governance
Target release date / Status	2020

8.16.9 ORGANISATIONAL APPROACH

8.16.9.1 Expected stakeholders and their representatives

Stakeholders	Representatives	Involvement in the action
Commission	- DIGIT	- Provider
EU Institutions	- Staff in charge of security and compliance - EU Cloud Virtual Task Force (Working Group for security), which comprises all the Institutions and agencies (Council, Parliament…); 3 to 5 Institutions as pilots	- Pilots - Pilots, Contributions
Member States	- Staff in charge of security and compliance (between 5 to 7 Member States)	Dissemination, Pilots if interested

8.16.9.2 Identified user groups

It is reminded that the action aims at:

1. Providing a supporting tool for the security policies defined by a certain organisation (e.g. Member State)
2. Helping entity which plan to develop an information system to understand the security aspects of the services he plans (e.g. business stakeholders)
3. Producing for technical services the list of controls (in a form of a check-list) that he has to implement to ensure the proper level of security, and therefore:
4. Be able to give evidence that the service he run is compliant with the security requirements established by (1) (e.g. answering to auditors)

Therefore the main group of end-users of your solutions are:

- Staff in charge of the security policies and compliance: they get support through a platform which allow them to implement their policies and expose it to the business stakeholders
- Business stakeholder of a system: they are helped to be explained which security rules have to be put in place, which hosting solution is valid, etc.…
- IT Technicians: they are provided with a checklist of security controls to implement
- Security auditors: they have a checklist to which they can refer in case of audits

8.16.9.3 Communication and dissemination plan

The dissemination is a formal work package of the action; the draft action plan is:
An important part of the action is called Dissemination: it consists in disseminating the principle of the present Framework to its actual users:

- The first set of users are the EU Institutions which already raise interest in the approach; this group of interest will be engaged through the various channel already available but they are a de-facto participant of the action.
- The second action will consist in disseminating the concept to other Public Services in Europe using regular dissemination channel for reusable components. The dissemination will be performed to the authorities responsible for security compliance among the Member States; the Commission and DG CONNECT and ENISA will help on that matter.
- If the interest is rising among the mentioned authorities, they will be able to be engaged from 2019: they will be able to use the framework, and a specific structure to take their feedback into account will be put in place. This structure, depending on the involvement of the pilots, can go from the active integration of requirements to the development of an open-source community.

8.16.9.4 Key Performance indicators

Provide a list of KPIs allowing the measurement of the progress and completions of milestones and the action. In case of an on-going action with already identified metrics[63] indicate the current values.

Description of the KPI	Target to achieve	Expected time for target
Number of organisations using the framework	4 Institutions 10 Institutions	End 2018 End 2019
Number of building block described and reusable	20 building blocks 50 building blocks	End 2018 End 2019
Number of organisation participating to dissemination	20 public services	End 2018 2019

8.16.9.5 Governance approach

The action will be organised as follows:

- The supplier team: document the methodology, develop the platform and organise dissemination activities. The supplier team will work in agile mode using the SCRUM methodology. It is reminded that this methodology divides the time in fixed period of activities called sprint (few weeks). Deliverables are defined at the beginning of the sprint, and delivered at the end of the sprint.

[63] For examples see the ISA2 dashboard https://ec.europa.eu/isa2/dashboard/isadashboard , **effectiveness** tab.

- The project will be steered by a Project Management Board, which will be involved in:
  - Definition of the content of a sprint
  - Debriefed systematically at the end of the sprint; opportunity will be taken at the end of each sprint to list risks and issues related to the project
  - At any moment the Project Management Board will have access to the progresses of the project, through a public SCRUM board which shows the progress in real time
- End-users of the platform will be involved though a collaborative platform, where they will be able to exchange with the Provider and the PMB. Escalation of end-users will be organised through this channel.

8.16.10 TECHNICAL APPROACH AND CURRENT STATUS

The action relies on the development of an information system (IS). Today a very early version approach and methodology is being prototyping using office automation tools, proven promising but not sufficient in terms of efficiency.

Technically speaking the IS does not represent a challenge in terms of architecture, since it basically consists in managing a database of information provided by the various stakeholders, a database of building blocks, and workflows to manage the transitions.

Therefore this information will be perfectly served using a MDM[64]/BPM[65] approach. The information system will therefore need a database technology as repository, a workflow engine to manage transition, and a decent presentation layer for a decent usability of the IS. The IS itself must be inter-operable, so it will expose its key interfaces through Web Services.

Additional requirements to take into account are: respect the principle of open source development for its publication, and easiness of deployment in constraint environments of users of the platform (e.g. Member states and Institutions); therefore attention should be given not to give technical constraints or 3rd parties dependencies.

Al last it is also more than likely that parts of the methodology are already covered in the Member States or Institutions: this will be visible only after the phase of engagement of the other Member States or group of interest. So it is important that the IS is modular to allow such integration, or can obviously reuse an existing contribution if applicable.

Taken in consideration all these requirements, but having as target a functioning and proven methodology, the action will follow the following staged approach:

Stage 1: **Drafting** and **Designing** *(year 1)*	- Drafting the methodology, using a prototype of the application developed with a RAD[66], such as Grails, using open source databases as repository and Activity as workflow engine - While engaging the Member States and other stakeholders, designing the future application architecture
Stage 2: **Implementing**	- Once the methodology is proven enough, and the candidate testers (e.g. Member States engaged), implementing the final version of the system

[64] MDM: Master Data Management

[65] BPM: Business Process Management

[66] RAD: Rapid Application Development tool

and **Testing** *(year 2)*	(building blocks listed below) - Testing each building blocks as the arrive, on the basis of the priority of the stakeholder
Stage 3: **Packaging** and **Deploying** *(year 3)*	- Packaging the IS in a form deployable by potential users, and deploy it in an open source repository - Deploying the IS at customer's site where they will be operated in production

The building blocks of the IS are:

BIA (optional)	Flow managing the Business Impact Assessment of similar process
Risk Assessment	Flow managing the Risk Assessment methodology
Policy/Governance	Flow managing the Governance process, implementing the policy rules
Controls Generator	Modules generating the security controls

The data assets managed are:

BIA, Risk Assessment	Information, Questionnaires filled by stakeholders, brick's database
Policy/Governance	Rules of Governance, Decisions
Control Generator	Database of controls per bricks, Check-lists

During the *Drafting and Designing* phase, only a partial implementation of the building will be achieved, following Agile practices to best fit the need of drafting the methodology and performing presentation to the stakeholders.

8.16.11 COSTS AND MILESTONES

8.16.11.1 Breakdown of anticipated costs and related milestones

Only activities directly in relation with Member States are requested for funding by ISA (e.g. dissemination, publication of the methodology, and customisation capabilities of the information system); specific tasks that would be in the interest of the EU Institutions are funded directly by DIGIT.

Phase: Initiation Planning Execution Closing/Final evaluation	Description of milestones reached or to be reached	Anticipated Allocations (KEUR)	Budget line ISA/ others (specify)	Start date (QX/YYYY)	End date (QX/YYYY)
Initiation	Drafting	200 k€	0 k€	Q1/2018	Q3/2018
Initiation	Initial Dissemination	50 k€	50 k€	Q1/2018	Q2/2018
Planning	Designing	150 k€	100 k€	Q3/2018	Q3/2018
Execution	Implementing	450 k€	150 k€	Q4/2018	Q2/2020
Execution	Dissemination	50 k€	50 k€	Q4/2018	Q2/2019
Execution	Pilot Testing (EUIs)	50 k€	0 k€	Q2/2018	Q3/2020
Execution	Pilot Testing (others)	150 k€	150 k€	Q3/2019	Q3/2019
Execution	Packaging	300 k€	50 k€	Q3/2020	Q4/2020
Closing	Methodology (final)	150 k€	50 k€	Q3/2020	Q4/2020
Closing	Deploying	100 k€	50 k€	Q3/2020	Q4/2020
	Total	1.650 k€	650 k€		

8.16.11.2 Breakdown of ISA^2 funding per budget year

Only activities directly in relation with Member States are requested for funding by ISA (e.g. dissemination, publication of the methodology, and customisation capabilities of the information system); specific tasks that would be in the interest of the EU Institutions are funded directly by DIGIT.

Budget Year	Phase	Anticipated allocations (in KEUR)	Executed budget (in KEUR)
2018	Drafting and Designing Initial dissemination	400 k€ (100 k€ ISA) 50 k€ (50 k€ ISA)	
2019	Implementing and Testing Dissemination Pilot Testing	500 k€ (150 k€ ISA) 50 k€ (50 k€ ISA) 100 k€ (100 k€ ISA)	
2020	Packaging and Deploying Pilot Testing (continuation) Publication of methodology	400 k€ (100 k€ ISA) 50 k€ (50 k€ ISA) 150 k€ (50 k€ ISA)	