DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Table of Contents

Management of individual ICT solutions

Act No. 365/2000 Coll. assumes that the Information Concept of the Czech Republic will also address the issue of management of public administration information systems. It is appropriate to use the recommendations of the MŘICT unchanged and thus to apply them in the full scope of the ICT portfolio (IT architecture) of the OVS. However, as with any other methodology, adaptation to specific situations is more than appropriate.

The management of each IS can be described and guidance and accelerators for it can be provided in the Knowledge base either focusing on the detail of the phases and activities in the IS life cycle stage or focusing on typical activities and methods that, although usually occurring in certain phases, may also be repetitive and overlapping (e.g. supplier selection, project management, mitigating supplier dependency, etc.).

This chapter introduces and combines both perspectives. Detailed information and accelerators, especially on deliverables and methods by IS life cycle, are provided by the forthcoming knowledge base.

All activities in the management of individual IS must be carried out in the context of the whole Authority and eGovernment of the Czech Republic and the EU, within the framework of the activities and procedures described further in Management at the level of the ICT OVS unit and Collaboration with other units of the Authority and eGovernment.

Management of information systems by stages and phases of their life cycle

The capability of ICT services (information systems and ICT infrastructure) for the purpose of safe and quality performance of public administration services cannot be effectively ensured without respecting the life cycles of change. This statement is valid both in terms of the lifecycle of technical components, the validity of contractual support from providers, and in particular in terms of changes in the needs of individual internal departments of the authority and the expectations of public administration clients.

In recent years, the number and scope of ICT services of authorities have gradually changed significantly; this increase requires a better setup of ICT administration and management and increases the demands on their service. Major milestones include work in the electronic filing service, the use of basic registers, data management obligations (security), personal data management obligations (GDPR), the possibility of transferring selected parts outside the office (Cloud) or the strengthening interest in digital public administration services. One cannot ignore the new trends and innovations in the technological part of ICT, where the primary burden on human resources is in various forms of innovative upgrades and the gradual inclusion of completely different technological approaches than a decade ago. In many cases, due to a certain obsolescence, new systems have to take into account old frameworks and technologies in their architectural designs, which costs the contracting authority increased efforts and in most cases, higher financial demands cannot be avoided.

Every information system goes through successive stages of its development, the turning point of which is always the commissioning into productive operation of a new (or significantly renewed) set of services, bringing new business values for the contracting authority. This moment brings about the completion of the work (change) of the so-called transition architecture, or for a given level of knowledge and assignment at a given time, the target architecture of the system and the entire office.

We call the period, activities and states between each two such moments of value-added service initiation one stage of the system life. A stage is thus equivalent to a single pass through all phases of the life, or development [1)] cycle of an information system, or its entire functional unit. The development of the life of each IS thus moves along a kind of permanently upward spiral, in the case of a decline in interest in the system and the gradual removal of functions, also along a subsequent downward spiral, consisting of stages.

In the same way as ISVS have their specifics compared to commercial information systems, their life cycle

necessarily has them as well, i.e. when managing the life cycle of ICT VS systems/services, it is necessary to proceed differently and to respect different legal obligations and different time limits.

To ensure the necessary addressability (who is responsible), while respecting the logic of the substantive nature of the activities in the life cycle of an ICT service / information / communication system of public administration, the course of each stage can be distinguished into the following stages [2)]:

1. STRATEGIES
2. PLANNING AND PREPARATION (including the final implementation design)
3. IMPLEMENTATION
4. PRODUCTION OPERATION (including controlled changes)
5. EVALUATION
6. TERMINATION OF SERVICE

A graphical representation of the logical sequence of these phases in the IS life cycle is shown in the following Figure:

The first and last passage through the phases of the information system life cycle stage has a privileged position among the life stages of the information system. The first stage of IS life constitutes its existence, gives it meaning, purpose and empowerment, shapes its architecture and platform in the long term. Therefore, external strategic impulses are emphasized in this cycle and internal evaluation is lacking.

The last life stage of an IS starts with the strategic decision to end the service provision/existence of the system, and ends with the physical disposal of the information system, but the whole thing is also a planned and managed implementation (archiving and disposal) project, going through planning, preparation and implementation phases.

All other stages of IS development represent the gradual addition of information system functions based on the assessment of its status and needs and/or on the basis of an external impulse - strategic and legislative changes, or its technological and platform upgrade (upgrade).

The life stages and phases of the IS life cycle correspond to the structure of planning and evaluation of their costs, see the TCO methodology.

The term 'phase' implies a specific period of similar or closely related activities, sometimes very long and unchanging - for example, the production phase. In addition, the term 'stage' means the part of the journey from start to finish, in this case from one range of productive services to a new range and value of productive services. A stage is therefore made up of phases.

The decomposition of these individual life stages into the structure: "stage" (cycle) - "phase" - "step" - "activity" - "task", necessary for the concretization of individual management activities, is based on the Methodological Manual for the needs of project management in central state administration organizations issued by the Ministry of the Interior of the Czech Republic [3)], is elaborated in the table "Scenario of the life cycle activities of the ICT service of the Ministry of the Interior of the Czech Republic" and is a part of Knowledge base**.**

The scenario of the life cycle activities of the ICT service of the Ministry of the Interior (also referred to as "scenario"), in addition to the above hierarchy of activities, also contains the individual process steps, specific documents (as defined in the Instruction of the Minister of the Interior[4)]), the standard necessary (initiating) inputs and outputs, as well as the interdependencies (conditionality of initiation) and the key roles involved in the activity.

The descriptions of each of the above stages of each IS life stage are all identically divided into the following parts for ease of comprehension:

1. Phase Framework Characteristics.
2. Phase Principles - the main features and requirements, the principles whose observance is crucial for the

proper management of the activities of this phase.
3. Recommended methods - the methods recommended for the phase.
4. Legislative anchoring - selection of legislative documents that must be respected in the performance of the activities of this phase of each stage.
5. Roles concerned - selection of roles that should be actively involved in the performance of the activities of this phase of the life stage.
6. Inputs, and resources, outputs:
    - necessary inputs - initiators of the phase - a list of actions and decisions (documents) that are necessary prerequisites = initiate the start of the execution of the activities of this phase,
    - resources necessary for the effectiveness of the activities in a given phase - resources (information, technical means, organizational measures, personnel resources, etc.) without which the performance of the activities of this phase cannot be implemented effectively,
    - the outputs of each phase serve both to document that a specific action (e.g. decision or appointment) has taken place and as input to the next action/step/phase.
7. Milestones and Steps - a brief description of the specific activities included in this phase of the IS life stage, plus the recommended methods, their major milestones (deliverables, not just deadlines) and participants (roles).
8. Process and management methods - the sequence of sub-phases, steps and deliverables of the phase, if prescribed. Along with this, the rules for joint or otherwise interrelated management within a phase, project and linear.

In this introductory edition of the MIRCT, for clarity and readability, only the sub-sections Framework Characteristics, Phase Principles and, where applicable, Sub-phases and Steps are provided for each phase. The remaining parts of the description and any extension appendices, containing the above Scenarios and other necessary accelerators for each phase, will be progressively added to the corresponding sections of KnowledgeBase.

The different parts of each phase of an IS lifecycle also have different forms of governance - linear and programmatic/project. While a substantial part of the planning, preparation and implementation of a radical change to the IS, or the termination of its service, is managed as a program and project, using project roles, the part of the strategic preparations, all operations, evaluation and continuous improvement happen in the normal line management of the departments and roles of the subject matter and technical system manager.

Phases 1, 2 and 3 of the lifecycle, leading to new value-added services, usually correspond to a single development programme, consisting of one or more sub-projects, the coordinated implementation of which will produce the benefits expected by the programme.

Each project for the implementation of a substantial change to the IS, i.e. development and implementation projects, regardless of content or size, contains the following 'project phases', represented to varying degrees but always present:

- **Project Identification, Initiation and Conception** - the future existence of the project is planned (e.g. already in the IK OVS Architectural Roadmap) and the project is roughly defined, conceived. Its objectives and basic conditions are defined. This takes place in the phase ŽC IS No. 1-Strategy.
- **Planning and preparation of the project**, after its approval and launch, including the establishment of project structures and its material and personnel support in Phase 2-Planning and preparation.
- **Project Execution**, typically after the selection of the contractor, including the establishment of joint project structures with the contractor, the target solution concept and the delivery (development, implementation) of the solution to the extent appropriate to the chosen implementation method (waterfall, agile, combination, ...), including testing.
- **Productive Operations Preparation**, including preparation including training, data migration, point of start of use and initial extended vendor support, both points in Phase 3-Implementation.
- **Project Closeout**, including final acceptance of deliverables and handover of the solution to ongoing support, at the beginning of Phase 4-Operation.
- **Ongoing project planning, monitoring and management**, in all phases of the project and in the corresponding phases 1, 2, 3 and 4 of the life cycle.

IS lifecycle phase	Implementation project phase	Key deliverables and milestones
* STRATEGY	* Identification, initiation and concept	* Strategic brief. * Information concept of the IS, containing the project. * Enterprise architecture of the project. * OHA opinion
PLAN AND PREPARATION	* Project planning and preparation	* Project definition, Project charter, Project plan. * Project architecture. * Functional and non-functional specifications. * Decision on (non)implementation of the project * Investment plan * Registration of the project at the Ministry of Finance. * Budget measure of the authority including the designation of the principal * Procurement documentation of the procurement. * Selection of the contractor / Contract with the contractor.
\ IMPLEMENTATION	* Project implementation * Preparation for productive operation	
PRODUCTION PROCESS	* Project Closeout	
Continuous - * through 1, 2, 3 and 4	* Project planning, monitoring and management.	* Project management plan, including * Resource plan * Risk register and others

Relationship between IS life cycle phases and phases of a typical implementation project.

Additional deliverables and milestones of the implementation project phases are described in the detailed Knowledge base materials for each phase of the life cycle phase and the project management methodology.

Overlapping life cycle stages. The life cycle stages of an IS may overlap with each other with a phase shift. Thus, at the same time, some IS services are routinely operated, some services from earlier stages are already being phased out and disposed of, and new services from the next stage of system development are being planned or implemented.

Overlapping phases of one stage. Similarly, phases of a stage may overlap or overtake each other in their activities. For example, not all the activities of closing the implementation project and the final handover of the solution to productive operation have yet been carried out, yet the services are already in productive use as outputs of the project.

Managers of the subject matter and technical administrator, the operator and the contractor must navigate and consciously manage the overlaps and overlaps between the different stages and phases.

Phase 1 - STRATEGY

Strategy Framework

The strategy phase includes activities carried out in the formulation of strategies for the development of the public administration, the OVS (its department) and its IT unit and in the corresponding changes in legislation resulting in requirements for new or changed ICT services to support the performance of public administration. The strategic phase included - due to the life cycle of one ICT service / individual VS system - the strategic

planning steps carried out jointly for all ICT services and systems of the authority, namely the creation and updating of the Information Concept of the OVS, with the simultaneous updating of its Authority Architecture (EA).

The strategy phase includes activities related to the formulation of public administration development strategies, strategies of OVS and their IT departments, and in the corresponding changes in legislation resulting in requirements for new or changed ICT services to support the performance of public administration. This is especially true in the case of central administrative authorities, which are responsible for individual legal regulations and where it is possible and necessary to participate in the development of national strategies and legal regulations from the position of IT specialists.

In the case of other authorities, especially local authorities, it is necessary to adapt their own strategies in response to changes in legislation and citizens' demands for the functioning of public administration.

The following activities are part of the strategy phase:

- Participating in the development of government strategy documents or collaborating by providing input and feedback.
- Participating in the development or amendment of legislation, and/or studying existing and forthcoming legislation and regulations, including EU standards and regulations, and analysing their impact on the ICT environment of the OVS.
- Contributing to the development of the OVS own strategic documents, including the development of the OVS ICT strategy, if the OVS is developing one, or of the department, if such a strategy is being developed.
- Analysing the needs of stakeholders, i.e. in particular the management of the Office and the needs of the specialised departments, based on communication with the subject-matter guarantors of each specialised agenda.
- Identification with the objectives and plans of the OVS and the Department, with the objectives and plans at national level (IKCR and others), with the objectives and plans at EU level and develop own ICT objectives.
- Develop and update the long-term architectural vision and overall architecture of the OVS office (EA).
- Produce an analysis containing the status now (As-Is) in subsequent periods or when changes occur then **always** produce a gap analysis with a gap assessment in the form of a separate, management summary (this summary can be attached as an appendix to the gap analysis).
- Providing other necessary inputs for the downstream preparation phase and strategic and project planning
- Preparation and updating of the OVS Information Concept and other related medium- and long-term plans for the development of the OVS ICT environment.
- Prioritization of identified objectives and preparation of medium-term outlooks and long-term financial plans for the implementation of the ICT development plans, allowing for accurate planning and budgeting, preferably in the form of annual action plans for implementation and adaptation to the objectives.

While **Stage 1 - Strategy** is an integral part of each life stage of an individual IS, it is fully applicable and dominated by the methods and means of strategic management and planning of ICT at the level of the whole department and office, in the context of eGovernment of the Czech Republic and the EU, see Management at the level of the ICT department.

To facilitate and support the processes of the strategy management phase, the Knowledge base NA VS ČR will be gradually added to the following:

1. Principles, procedures and examples to support the development of so-called digitally friendly legislation.
2. Reference model, architectural patterns, table templates and detailed guidelines for the creation and maintenance of the Authority's architecture and its vision.
3. Checklists of necessary inputs for architecture development and project planning.
4. Sample template and other aids for creating the OVS Information Concept, especially checklists for verifying compliance with the IC CR.

5. Tools and procedures for prioritizing projects before and after budget approval.
6. Tools and procedures to support budget preparation and negotiation.
7. Tools, guidelines and resources for defining objectives.
8. Draft forms of action plans.

Principles and rules of strategy formation

- **The principles of ISMS strategic planning in the context of the Authority's architecture.** For each Authority's ISMS, the Authority's Common Information Concept (also referred to as the "IC" or "OVS IC") must define what the desired target state of the ISMS is at the end of the IC planning horizon and why and by what projects or programs the necessary IS changes will be implemented and in what timeframe.
- **Linked to the overall (substantive, business) strategy and IT strategy of the authority, based on the eGovernment strategy.** The long-term management of public administration information systems must be based on the strategic objectives of the authority in the area of public administration and its information support, in the context of the strategic objectives of the authority's parent structures. It is not acceptable to develop a long-term ISMS plan in the Authority's IC without a documented and understandable reference to the development and change plans of the agencies that the ISMS supports and without the context of the planned changes to the Authority and eGovernment as a whole. It is not possible to develop or update the OVS IC without first updating its strategic inputs (agency strategy, authority strategy and IT strategy) and, conversely, after each change to these inputs, the validity of the OVS IC must be checked and, if necessary, updated.
- **ISVS Architecture.** Each ISVS subject matter manager and subject matter manager of a central eGovernment element is obliged to maintain a model of the existing, target and, where applicable, transitional architecture for this system at the level of the Authority Architecture (EA) and Solution Architecture (SA), in accordance with the methodology of the National Architecture Framework. For the purpose of requesting OHA's opinion on the programme, investment plan and project, a model of the desired state of the ISMS architecture at the level of detail of the Authority Architecture (EA)[5)]. After obtaining a positive opinion from OHA, if this is relevant in terms of the scope of the project, it is necessary to elaborate the ISMS architecture, or changes to it, for the purpose of selecting a solution and a solution provider in the form of a so-called Solution Architecture. This is then used to compile a list of functional and non-functional (meaning non-functional) specification requirements [6)]) for the purposes of the tender documentation of the tender procedure under the ZoZVZ.
- **Combination of all requirements.** The strategic planning of each ISMS at the beginning of a new phase of its development must include a combination of strategic requirements for change with mandated requirements, for example, for security (GDPR), for electronic identification and documents (eIDAS) or eGovernment objectives and standards (IKCR). For existing IS, these external requirements must be combined with internal requirements resulting from the assessment of the current state of the IS (phase 5).
- **Management periods.** Activities and deliverables in Phase 1 - Strategy are managed in continuous, periodic and Ad-Hoc mode:
    - **Ongoing** the overall (enterprise) architecture of the OVS is updated whenever any change is implemented, but also after the strategy is changed and as part of the change management implementation.
    - **Periodically**, at least once every 2 years, but also whenever strategic inputs change, the OVS Information Concept is updated.
    - **Periodically - annually**, in the period prior to the budget preparation, the project plan from the OVS IC (Roadmap) is updated.
    - **Ad-hoc** when new requirements and major incentives arise and are identified (elections, change of leadership, new legislation, etc.).

Phase 2 - PLAN AND PREPARE

Framework for planning and preparation

A phase containing steps and activities that build on the strategic direction of the individual information system established in the previous phase, elaborating this direction into a proposal for the individual changes needed, their interrelationships and timing. The phase also includes all the necessary comments, assessment and approval of the chosen solution, i.e. the Authority's ICT development plan, as a condition for initiating the related expenditure from the state budget

Public administration service change projects are increasingly relying on IT support. In addition, all projects in the Authority share a limited amount of human resources suitable for the projects. For these reasons, all informatics projects need to be demonstrably coordinated with all ongoing and planned projects across the Authority, whether together they form tightly linked development programmes or are only loosely managed as portfolios of projects.

Communication with the Accounting Service on the accounting nature of asset acquisitions and other transactions is important. Not everything that may appear to an ICT practitioner to be a fixed asset actually is from an accounting perspective. Failure to do so can lead to serious risks of breaches of budgetary discipline and other penalties.

The methods and procedures of Phase 2 - Planning and Preparation represent the implementation of the Principles and Procedures for the Acquisition and Development of Public Administration Information Systems - Part I, and the basis for updating and supplementing these principles according to §8 decree 529/2006 Coll, on the requirements for the structure and content of the information concept and operational documentation and on the requirements for the security and quality management of public administration information systems (Decree on the long-term management of public administration information systems), on the requirements for the structure and content of the information concept and operational documentation and on the requirements for the security and quality management of public administration information systems (Decree on the long-term management of public administration information systems) in the scope of questions: how to find the right solution for meeting the business needs of public service provision (and changes thereto).

The description of the phase sets out, among other things, the basic obligations on how to proceed from the position of the ICT unit in finding the most appropriate ICT solutions to optimally meet the business needs of the authority in the delivery of its public services.

In the Planning and Preparation phase, 3 work streams go side by side, complement and intertwine in time, see Table 3 for details:

- Substantive, content planning - what is to be the subject of the target solution (architecture)
- resource planning, especially human and financial (project planning)
- ensuring legitimacy of change - legislative preparation

Measure of Knowledge / Current	Plan Legislation	Plan Architecture	Plan Resources
Introductory idea	Bill of intent	Enterprise Architecture of intent	Budget and staffing requirements
Refined Idea	Final Approved Bill	Architecture of Intent	Resources Allocated
Performable Terms of Reference	Decrees and Internal Management Acts issued	Solution Design	Solution Resources issued

Overview of the relationships of the concurrent work streams of the Planning and Preparation phase.

Substantive planning, i.e., architectural preparation, occurs in steps of progressively increasing detail of knowledge, expressed in graphical models and lists of required components and their characteristics; in accordance with how these levels are defined by NAR, see the following Figure:

The basic models of the Authority's target architecture, developed in the previous Phase 1 Authority-wide Strategy and used for the release of the OVS Information Concept, are followed by the so-called "Pre-Project Start Architecture" (PSA[7]). This architecture provides a model of the future solution and its immediate context at the EA level of detail and contains, together with the basic project plan, sufficient data for the preparation of an OHA Request for Opinion.

This is followed by finding the so-called Solution Architecture, which focuses on the question of how the solution sought is to work and is expressed in terms of functional and non-functional specifications in addition to graphical diagrams. An essential part of this is the decision on the solution option. Together with the refined project plan, containing decisions on the implementation strategy, on how to provide its own, the agreement on the CBA and the decision to continue the process towards the acquisition of the solution (purchase, development or combination), the solution architecture and specification is the basis of the tender documentation.

A prerequisite for the substantive planning and preparation is the participation of ICT specialists in the development of the substantive plan of the relevant legislation associated with the change, in particular and in full if it is the OVS, which is responsible for the legislation in question and will be the administrator of the relevant IS. The role of ICT in this area is in particular:

- to provide the legislative team with the necessary capacity for systems thinking and the broader context of the whole authority and the eGovernment of the Czech Republic and the EU,
- to contribute to the DPL - digital friendliness of the law by knowing in particular the current technological possibilities and user habits and expectations,
- to provide a logical check and timely verification of the real feasibility of the law's impact on ICT implementation,
- provide timely information for further planning activities in ICT

Therefore, the role of ICT is most prominent at the stage of the first ideas and formulation of the substantive intent of the regulation change, but persists until the final approval of the regulation and its implementing regulations.

In project resource planning, it is essential to request and secure all types of resources in a timely manner and with a good knowledge of the pending legislation, the required scope of changes and work and their timing, through existing actions and documents (programme funding, project plan, ...). An important part of resource preparation is the acquisition of external resources, i.e. the selection of a contractor through a successful procurement process and the conclusion of a contract, ultimately combining the outputs of all three parallel planning and preparation streams.

The success and effectiveness of the Planning and Preparation phase depends to a large extent on the timing of the work in all three streams and on how the knowledge and outputs from each activity can be used together and duplication of work and documents avoided.

An important prerequisite for the success of the whole life cycle is to include the following in the scope and intent, terms of reference and contracts as early as the Planning and Preparation phase:

- Taking into account all mandated needs and rules not linked to the respective agency or operational regulations (eIDAS, security, GDPR, e-Identity, eGovernment principles from the ICCR, etc.).
- Creation of prerequisites for subsequent effective management of service quality and performance (SLA).
- Creation of prerequisites for taking over knowledge from suppliers and mitigating dependency on them.
- Creating enablers to build and ensure the Authority's ability to operate (or control the operation of) the solution and other enablers.
- Creating the enablers to evaluate measurable parameters of projects, solutions and suppliers in Phase 6.

Optimizing this confluence of planning streams, ensuring those assumptions and facilitating all activities will be the subject of documents and tools that will be part of the next edition of the MRICT and Knowledge base.

Planning principles and rules

- The planning and preparation of an individual programme or project must be done in accordance with and using programme, project and portfolio planning methods and tools at the level of the whole authority and in the context of the whole eGovernment.
- The concurrence and alignment of the three planning and preparation streams (legislative, architectural and resource).
- Involvement of IT specialists in the development of the legislative intent (if relevant to the OVS).
    - Collaboration in the specification and identification of needs,
    - Consultation and confirmation in terms of factual correctness,
    - review and approval of the final text for factual correctness.
- Phased planning of the target state with the intent of a connected functional unit through all 4 layers of architecture.
- Early planning and allocation of all necessary resources (financial, human, technical and knowledge).
- Consideration of all mandated requirements.
- Communicating with the accounting department on the accounting nature of the assets to be acquired and other transactions.
- Making assumptions for the following phases.
- Use of the principle of ex-ante control and PoC (Proof of Concept) tools, see next chapters.
- In EA models using service decomposition to create assumptions, motivators and interfaces for KPI measurement and subsequent SLA and OLA evaluation and management (SLM).
- In decomposition, always apply and plan what will be outsourced and what will be insourced, and perform impact analysis on the OVS budget (in case of UC requirements) and on internal resources and their capacity (in case of internal OLA requirements).
- In the case of using shared services, take all SLAs including shared services into account when establishing service levels (% availability) and only according to these indicators design SLAs with sponsors and design monitoring.
- Always include the requirements of all actors and key users in the SLA definition.
- Always carefully plan the capacity for implementation and subsequent operation, preferably in the form of an impact analysis, on resources:
    - Financial
    - Technical (including project support tools (PPM) and operations (ServiceDesk))
    - Human (including HelpDesk operators and resources needed for synergy)
- Always prepare a change risk matrix as an annex for documentation during implementation, the risks must be communicated at least to the ICT unit management, the subject matter sponsor and the project sponsor.
- Identify mandated contractual requirements in particular:
    - Copyright,
    - penalties and discounts,
    - catalogue SLA sheets,
    - definition of synergies,
    - exit strategies and obligations, etc.

Phase 3 - IMPLEMENTATION

Implementation Framework

The implementation phase of the planned changes to the information system represents the core of the development and implementation project planned, initiated and conceptualized in the previous phase of this stage of the solution lifecycle. Implementation is the actual delivery of standard application software, its parameterisation and software customisation and/or customised software development and/or acquisition of software as a service. For both forms of SW acquisition, the so-called "on-premise" implementation also includes the delivery of platforms and infrastructure, the building of all necessary runtime environments ("Landscape".)), with a minimum of three stages (development, testing and production), optimally for large systems four stages

(development, testing, pre-production and production), in exceptional justified cases two stages are acceptable (non-critical systems without critical data and integrations e.g. BI) and the establishment of the Authority's ability to operate and support the solution.

The methods and procedures of the implementation phase replace and develop the so-called Principles and Procedures for the Acquisition and Development of Public Administration Information Systems - Part II (implementation of a purchased solution and acquisition of a solution by development, or a combination of both). It will be a substantial supplement to the principles according to §8 decree 529/2006 Coll., on requirements for the structure and content of information concept and operational documentation and on requirements for security and quality management of public administration information systems (decree on long-term management of public administration information systems) in the area of questions: how to successfully implement the selected solution and put it into productive operation. Thus, essential and nationwide standards to the requirements of the Decree (after its expected amendment).

The project management of the implementation of individual IS must be carried out in the context of change management at the level of the entire ICT unit and the change of the entire authority, see in particular Management at the level of the ICT unit. This means in particular:

- joint management of sub-projects within the overall management of portfolios and programmes
- joint IT and non-IT change management
- joint management of large (e.g. project) and small (e.g. line, interim) changes - with shared processes, tools and resources.

In particular, to facilitate and support the processes of the implementation management phase, the following will be progressively added to the Knowledge base:

1. Recommended practices and methodologies for creating and recording analytical models at the solution architecture (SA) and solution design (SD) level
    1. Data models
    2. Process models
    3. Decomposition models
    4. Use-Case and State Models
2. Recommended standards and methodologies for project management of implementation projects (including potential development)
3. Internal development standards

Principles and rules of implementation

- Changes from a certain size, scope or nature must be managed as a project.
- Acceptance of the solution is always done by the client (contracting authority, subject matter manager) in cooperation with other stakeholders (integrated OVS, SZR, ...).
- The structure of the project steps, deliverables and methods must correspond to the chosen type of solution to be implemented (off-the-shelf software, custom development, software as a service), the implementation strategy (Big-Beng, Pilot-Roll/out) and the development strategy (Waterfall/Agile) and their possible combinations.
- Projects with higher user adaptation requirements must include adaptation activities according to the OCM methodology, which will be added to the Knowledge base.
- The activities of the implementation phase of an IS must always be carried out in accordance with the implementation management methods at the level of the whole unit/office and using common methods and tools.
- In the case of a large project being implemented by a contractor with a global best practice project and development management methodology, this methodology may be used if it is in line with the provisions of this document and its annexes and if it can be linked to the mandatory (minimum) steps and deliverables of the VS CR project management when they are issued.

Milestones / implementation steps

The implementation of a project-managed IS change in phase 3 of its life cycle, typically after the selection of the supplier, represents the implementation of the following project implementation phases according to the project management methodology:

- **Setting up project structures**, joint teams with the supplier, allocation of space, negotiation of the project calendar, commissioning of the knowledge and document sharing platform, etc.
- **Executing the project** (aka Blueprint, target concept, solution analysis and design, etc.), at least:
  - Business concept - how the solution will be used (functions, processes, services, roles, deliverables-products, etc.)
  - IT concept - how the solution will be constructed, parameterized or developed to meet the business concept, including
  - Security and privacy concept - how mandated requirements will be incorporated
  - Concept for securing all IT environments, including operational infrastructure
  - The concept of testing and validation
  - The concept of roles and permissions
  - The concept of data migration and commissioning
  - Updating the solution architecture (across all layers), or changing the EA if it is subject to change management.
- **Solution development and implementation**, i.e. creation of IT development and testing environment including OS, platforms and databases, installation, parameterization and customization of finished solutions and development of customized software solutions, including all forms of verification of required functionality - testing, Proof of Concept (PoC) and documentation of development and setup.
- **Productive Operations Preparation**, including the creation of a production IT environment, including provision of third party services, user preparation including training, data migration, point of use, establishment of the Authority's own capability to operate and support the solution (including availability and service response monitoring tools) and initial extended vendor support.
- **Project close-out**, final acceptance of deliverables and handover of the solution to ongoing support, including full development, operational and user documentation of the actual implementation of the solution.
- **Ongoing project planning, monitoring and management** - ongoing throughout all phases of the project.

A number of sub-activities, milestones and deliverables are subordinate to the individual project phases, see detailed sub-chapters in Knowledge base.

An important project activity at the beginning of implementation is the establishment of project structures and the mobilisation of its internal human and material resources.

From the moment of the productive start of the first services included in the scope of the implementation project, the latter starts to fulfil at the same time the content of Life Cycle Phase 4 - Operations, and the persons and teams responsible on the side of the customer and, where applicable, the outsourced operator, must actively participate in these project phases, starting with the preparation of the production environment and productive operations.

Phase 4 - PRODUCTION OPERATIONS

Framework characteristics of the operation

The productive operation phase is characterized by the need to ensure the delivery of the services commissioned on the previous milestone, while maintaining the parameters of quantity, quality and safety of the service and, where possible, increasing the cost-effectiveness and efficiency of the service delivery, enabled by deepening experience as well as continuous improvement of the operation without changing the service. In

short, it is about ensuring agreed service levels (SLA or OLA).

The second key characteristic of the productive operation phase is that during this phase minor changes in the scope or quality of service are implemented, mainly by continuous, line management of the ICT unit and/or the contractor, which do not require the activities of phases 2 - preparation and planning and 3 - implementation of change. In short, it is the continuous identification, qualification, planning and implementation of minor changes, i.e. requirements gathering and change management.

It is important to classify the identified changes in terms of their size, how they are managed and their priorities. The basic priority of the technical administrator and the operator is to prevent the unavailability of system services and to meet the deadline for the implementation of service changes (especially legislative changes). Other low-priority changes should be bundled into work packages to meet the deadlines of new versions of the solution in question. This group also includes changes aimed at measurable efficiency improvements, i.e. changes bringing significant savings in resources (financial, technical or organisational). Lastly, in terms of operation, are changes that do not fulfil any of the above categories but, for example, improve the quality of service and comfort for users.

The above must reflect the relationship between the manager responsible for the delivery of information system services and the internal department or external supplier. This contractual relationship and, in general, the ability of the authority (technical administrator) to ensure efficient operation must be included in the preparation, planning and implementation phases of the creation of a new system or a major change to it. The person responsible must be empowered and competent to take decisions on the management and operation of the system and on the use of resources, including guaranteed 'mandated' resources (operating budget, mandatory internal roles, material and technical support).

Operation also means ensuring the operation of the infrastructure necessary for the delivery of application services. The acquisition and renewal of the infrastructure is governed by the rules of Phases 2 and 3 or 1 of the solution life cycle.

An important condition and part of operations management is the maintenance of up-to-date product (development), operational and user documentation of information systems, i.e. functional units in all layers of their architecture. At this stage, the asset is already in a usable condition and can therefore be accounted for as an asset and be assigned a depreciation schedule (depreciation periods). If a depreciation schedule is omitted, there is a risk of accounting impropriety.

The provision of user and technical support is crucial to support both aspects of operations (continuous service delivery and identification and implementation of changes).

For more information on the key methods used in managing operations at the level of each IS, see Managing individual ICT solutions.

In addition to activities to ensure the operation of individual information system services, it is necessary to build and use operations management capabilities centrally, across ISs, whether it is for example:

- overall management of data centres and virtualised infrastructure
- overall management of key application platforms
- overall user care
- overall solution configuration management
- overall planning and change and release management
- overall planning and resource management for operations

For more information, see the chapters on methods for operational management at the ICT unit level, Management at the ICT unit level.

In particular, the following accelerators will be gradually added to the Knowledge base to facilitate and support the processes of the operations management phase:

1. General suggestions for availability and response monitoring

2. Sample HelpDesk processes
3. Responsibilities of key roles and their competencies (as part of the overall RACI matrix)
4. Links to documents that are necessary/recommended for this phase
5. Description of backup strategy and implementation, including verification that recovery processes are operational.

Principles and operating rules

- Ensure operation of the unchanged service
- Ensure that changes are implemented to maintain the quality of the service and for its ongoing development
- Ensure that changes are implemented to improve the efficiency of the service
- Implement only "small" changes, not representing projects in phases 2 and 3 of the information system life cycle
- Create and manage a Catalogue of ICT services (currently in operation)[8)].
- To maintain and develop ICT services (systems) of the VS, for the flexible legislative development of which it is responsible as the substantive administrator of the OVS, to have its own unit or a controlled competence centre (service support unit, competence centre).
- All provided services are monitored at least at the level of End2End (business machine scenarios and scripts) monitoring.
- The operation of an individual IS is always managed in the context and executed by the means of the operation management of the entire office.
- All needs arising from the operation of the sub-unit itself must be pooled in one place and with one responsible person.
- All services must be served in a unified manner by individual ITSMs.
- There must be service quality management using SLM, regular SLA negotiation, both at the level of work teams and steering committees.
- Determination of depreciation schedule (depreciation period) for assets.
- Need to respond to security incidents involving personal data.

Milestones / steps of operation

The steps of operations management can be grouped into four areas:

- Ensuring the operational (runtime) environment (typically already designed as part of the implementation phase) and taking responsibility for the service delivery of the acquired solutions.
- Ensuring that the required service levels are maintained.
    - Operational security tasks - according to the Disaster Recovery Plan
    - Monitoring of achieved service levels including security monitoring
    - Ensuring the management of privileged user identities and access in security and operations.
    - Prevention and prophylaxis
    - HW and SW maintenance
- User support
    - HelpDesk / ServiceDesk with incident handling and management processes, problem management and initiation of change management processes
- Ongoing solution development - managing change implementation with action steps:
    - Identification and classification of incidents and change requests.
    - assessment and prioritization of change requests.
    - change planning and version control
    - change implementation and documentation.
    - Change awareness and difference training.

Phase 5 - IS Operations and Services EVALUATION

Evaluation Framework

The Operations and Services Evaluation phase includes several essential types of evaluation, in particular:

- whether the implementation project achieved the planned values (scope, time, resource requirements) and expected quality of outputs,
- whether the ICT services are being delivered at the expected level (SLA) - by the internal or external operator,
- what problems and change requirements can be inferred from reported incidents (non-conformities),
- whether the expected business benefits are achieved with the support of these ICT services, i.e. whether the parameters and benefits of the ICT investment have been met,
- whether the combination of the continuing business need for ICT services and their sustainable quality continues to warrant the maintenance or development of the solution, or conversely, the discontinuation of the provision of the system,
- what risks and mitigation measures are associated with the change project or the operation of the ICT services of the system.
- whether the suppliers are meeting the contractual expectations of quality and balanced cooperation or whether they should be excluded from further cooperation.

An important significance of the evaluation of an implementation project is if its conclusions can be used not only for better setting of internal management rules, but also for conclusions towards suppliers. At this point, such a design is already possible. The Cybersecurity Act is quite clear in its contractor management policy with regard to the quality of the solution delivered. The Public Procurement Act is quite clear with regard to security breaches. By matching these already completely identical conditions, we are able to define the quality of the bidder/supplier and, in the case of poor experience, to exclude the bidder from the tender if the non-compliance is beyond the defined threshold.

For the evaluation, a separate section (data set) will be created in the ICT catalogue, which will focus on the quality of the delivered solution. In particular, the quality of the submitted result will be evaluated against the specification, but also the quality of the client's satisfaction with the submitted result will be evaluated. It is also about the quality of the supplier and the ICT department.

Principles and rules of evaluation

- A mandatory part of all previous phases of the lifecycle phase (and project phases) must be the creation and implementation of assumptions (e.g. measurable objectives) for the evaluation of projects, operations and contractors.
- Evaluation of the achievement of targets and parameters, or mitigation of identified risks, and their interpretation into requirements and needs against small changes or major changes and the associated new life cycle phase must be a mandatory part of change projects and operations.
- In addition to specific (substantive, agenda) objectives and requirements, the fulfilment of mandated requirements (such as security, data protection, etc.) must also be evaluated.
- The risk and impact assessment also includes an assessment of the need for mandated (non-negotiable) resources necessary to maintain the current scope and service level of the information system.

Sub-stages / steps of the evaluation

Project evaluation - (non-)achievement of project objectives

- The Subject Matter Leader, together with the Technical Administrator and the Cyber Security Manager, will evaluate the level of achievement:

- project sub-objectives
- SLAs of the key parameters of the ICT service/system,

Evaluation of the investment action

- The Subject Matter Manager together with the Technical Manager will evaluate:
- achievement of objectives and planned benefits
- achievement of the schedule
- adherence to budget,

Analysis of operational data / knowledge base performance (Best Practice)

- Operator based on reports from the monitoring center (HelpDesk):
- prepare and submit an annual report to OVS management,
- continuously completes/updates the Authority's ICT knowledge base

Formulating recommendations from setup changes to further development / decommissioning

- The Subject Matter Manager together with the Technical Administrator and the Cyber Security Manager (on an ongoing basis) assess:
- proposals and recommendations for changes (functionalities and SLA parameters) sent by the User and the Operator (Supplier)
- optimization options and
- prospects for further development,
- the Technical Administrator formulates and submits to the Subject Matter Administrator:
- proposals for optimization operational measures and service development,
- comments and change requests

Decision on termination of service provision / system operation

- On the basis of the annual report, the **Agenda in Charge** shall decide whether or not to discontinue the provision of the ICT service / operation of the information or communication system.

Stage 6 - TERMINATION OF ICT SERVICE

Framework characteristics of service termination

The end of life of a system and its eventual replacement by another is a strategic decision that must be supported by architectural and economic documents and must be prepared in the IK OVS over a long period of time. The termination of a service includes the implementation of an exit plan agreed with the supplier or operator.

Therefore, the termination of service must be taken into account already when formulating the tender for the selection of the supplier, the conclusion of the contract[9)] and during the implementation process[10)]. In order to terminate the operation of the ISVS and migrate to another ISVS, the Authority must have contracted the current ISVS provider to provide all necessary cooperation, rights, data, documentation and information, to participate in negotiations with the Authority and, where appropriate, with third parties in order to ensure a smooth and orderly transfer of all activities related to the provision of services to the Authority and/or the new provider, exporting all data with comprehensive descriptions, including the creation of basic data sources for each agenda and module, which will allow the creation of sufficiently structured data based on the Authority's requirements that can be imported by another ISVS without in-depth knowledge of the database structure of the existing ISVS. Based on the data sources, it will be possible to fulfil the exit plan for the migration to another

system.

Similarly, the exit must be considered in the architecture, i.e., the solution architecture must be designed already with the need to support efficient end-of-life of the ISVS in mind.

It is desirable that those with substantive responsibility for endpoint ICT equipment consider, in accordance with 3E principles and other legislation, at the end of the ICT equipment life cycle, their retirement from the accounting records without physical disposal for subsequent effective use of the endpoint equipment within the Authority until complete wear and tear.

End of Service Principles

- The fact that the service will be terminated should be thought of in the early stages of service design, namely:
  - Technically.
  - Contractually.
  - Operationally.
  - Data/migration.
- Service termination may have reasons:
  - The financial demands of maintaining and developing the service (TCO tools).
  - Moral obsolescence and inadequacy.
  - Contractual.
  - Agenda is no longer performed, or has been amended to such an extent that the change constitutes a violation of the 3E principle.

Milestones / steps

Plan to replace the discontinued solution with a new (next generation, different system)

Verification of the usability of components:

- The Technical Administrator will prepare and submit to the Subject Matter Administrator for approval:
- analysis of the usability of the components owned by OVS (including software licenses) with a proposal for property measures (transfer to another ICT service / department, or sale / disposal of unusable ones),
- analysis of potential risks and impacts,
- qualified estimate of disposal costs,
- a realistic disposal schedule,
- Substantive agenda:
- review the Technical Administrator's proposal and either approve it or return it with specific requests for changes,
- determine which data (including operational documentation) to archive and how to dispose of.

Administrative action:

- The Technical Administrator shall prepare and submit to the Operator for implementation:
- a project for the termination of the provision of the ICT service / operation of the ICT system,

Technical measures:

- Operator in cooperation with the Supplier:
- uninstall the equipment and take it away for disposal,
- migrate / archive / dispose of data,

- prepare complete documentation of the disposal

ISVS Strategic Planning Principles in the context of the Authority's architecture

Ex-ante approach to planning and managing change and its benefits

Methods of translating the realization of strategic objectives into changes in the structure and behavior of the authority, i.e. into changes in its architecture, and planning interrelated feasible work packages (programs, projects) for the realization of these changes and their IT support are the task of the EA-architecture of the authority management method, which is the basic means of creating the Information Concept of the public administration authority.

ICT solutions are to be long term in nature and this can only be done in planning. Planning means knowing the commitments of the needs arising before they are implemented, i.e. the so-called **ex-ante control** of the resources spent on changing the environment. It is very inefficient to implement assignments in a superficial and non-conceptual way (e.g., improve deployment after acceptance and deployment to production). This approach is unsustainable in the long term, and above all, very costly and difficult to manage.

In the case of an ex-ante approach, where we programmatically assess the impacts of a change at the outset at design time, you can positively influence the introduction of a change on an impact-by-impact basis, primarily in the areas of cost (capital and operational, quality and architecture).

The most effective possible and at the same time the most conclusive tool to confirm or verify the suitability of the selected solution within the ex-ante control is the implementation of a Proof of Concept (PoC) project on a subset of functionalities and use cases sufficiently representing the concept of the solution of the issue in question. In order to minimize the cost of PoC implementation, it is advisable to use available open source technologies. These can then be substituted for commercial technologies with guaranteed commercial support, if necessary, within the production implementation project. A significant benefit of such a procedure is further verification and specification of requirements for individual products on open technologies and subsequent more precise targeting of production functionalities required from commercial products.

Another reason for the implementation of PoC projects is the communication of the prepared services, functionalities and their form and form towards the end users. One of the main architectural principles at the level of eGovernment of the Czech Republic is the principle of "Usability" of built applications. According to this principle, public administration services must always be designed taking into account the needs of the client - the citizen, so that he/she can, under all circumstances, handle his/her life situation in its entirety using an electronic service. At the same time, according to the principle of "Transparency" of the acquisition, operation and development of public administration services, clients - citizens should be informed about the intentions and objectives of building online public services so that they are able to use all available means to influence their direction on the basis of their legal rights and democratic principles.

In order to fulfil the above mentioned principles, the appropriate procedure for the implementation of new public administration services seems to be the verification of concepts, technologies and their functionalities in the so-called Proof of Concept (PoC) project before the actual design and construction of the target solutions. This procedure will provide users with the opportunity to test services and functionalities already at the time of their design, and therefore also the opportunity to comment on the design, or to send suggestions for changes, extensions, or optimization of the proposed services. In this way, it can be ensured that the services are designed with the expectations of the client-citizens in mind, and any possible inconsistencies, contradictions or additional requirements/expectations of the client-citizens can be captured at the outset and incorporated into the design of the newly developed service.

In the case of information systems, ex-ante control is most often associated with the expiry of a fixed-term contract, where the next tender brings with it, for example, change requirements that could not be met from

the contract. At such a time it is absolutely necessary to include in the ex-ante control a comprehensive review of the exclusive and non-exclusive licences of the solution in relation to vendor-lock effects, the possibility of using cloud and other sharing possibilities.

The ex-ante approach may thus become a simple risk mitigation tool for all ISVs in the near future. For each individual and, collectively, for all the Authority's ISVS, the OVS Information Concept will then set out what the desired target state of the ISVS is at the end of the IS planning horizon, including the reason why this is the case. That is, for what reasons arising from the intrinsic characteristics of the ISVS, from the requirements of the processes and services of the public administration of the Authority supported by it, or from what external causes, as well as by what activities the necessary changes to the IS will be implemented and by when.

Links to the business and IT strategy of the authority, the corporation and eGovernment

The long-term management of public administration information systems must be based on the strategic objectives of the authority in the area of public administration and its information support, in the context of the strategic objectives of the authority's parent structures, i.e. the public corporation of its founder (if it has such and such), the eGovernment of the Czech Republic and the EU.

It is not permissible to create a long-term ISMS plan in the IK of the Authority without a documented and comprehensible reference to the development and change plans of the agencies supported by the ISMS and without the context of the planned changes of the Authority and eGovernment as a whole.

Without specific justification (flexible response to unexpected changes in the external or internal environment), it is not acceptable to plan, prepare and implement projects that have not been identified in advance in the ISS IC. The proper way to deal with a sudden need for a major IS change is to first update the OVS IK, thus capturing all the necessary office and eGovernment context in the planning, and only then to start planning and preparing the project plan.

Enterprise architecture of the ISMS and its solution architecture

Each ISVS Subject Matter Manager and Subject Matter Manager of a central eGovernment element is required to maintain an Authority Architecture (EA) level of detail model of the existing, target and, where appropriate, transitional architecture for the system and its solution architecture model in accordance with the National Architecture Framework methodology.

The models of the target architecture of the ISMS, at all their layers and domains, are based on the overall architecture of the Authority, which they all together constitute.

The model of a certain desired state of the ISVS architecture at the level of detail of the Authority's architecture is referred to by the international abbreviation PSA[11)] and corresponds to a set of changes to be implemented on the ISMS by a development programme or project.

This level of the model is appropriate for the needs of the Authority's IC and for the need to request OHA's opinion on the program, investment plan, and project.

After obtaining a positive opinion from OHA, if this is relevant in terms of the scope of the project, it is appropriate to proceed to the development of a more detailed architecture of the ISVS, or its changes, for the purpose of selecting a solution and a solution supplier, the so-called Solution Architecture. From this, a list of functional and non-functional (meaning other than functional) specification requirements is then compiled[12)] for the purposes of the tender documentation of the tender procedure under the Public Procurement Act.

As stated elsewhere in this document, the solution architecture and its models must be an integral part of the design of the operational parameters and its visual model helps to decompose (existing and new systems) and

to accurately design the interface for service quality measurement and management (SLA/SLM).

ISVS in the Public Administration Information Concept

For each and all of the Authority's ISVS, the Authority's common Information Concept must specify what the desired target state of the ISVS is at the end of the IK planning horizon and why, i.e. for what reasons arising from the intrinsic characteristics of the ISVS, from the requirements of the Authority's public administration processes and services supported by it and from external causes, as well as by which feasible work packages (programmes and projects) the necessary IS changes will be implemented and by when.

The IK OVS combines two 'perpendicular' views of the ISMS:

- A single view of the logical ISVS (functional unit) in all four layers and four vertical domains of its architecture
- An overall view of each horizontal and vertical architectural domain that clearly shows the context of each individual ISVS.

Information System Service Management

The basic rule and recommendation of the ISTC for the ICT units of the OVS is to move to managing the relationship between providers and customers of information systems support functions through services, if they have not already done so

The next edition of the MDICT document and the ongoing additions to the Knowledge base will develop information, recommendations and tools in this area of ICT management, for example on:

- management of the Service Catalogue by department and individual organisation, possibly the Service Catalogue at eGovernment level
- the conversion of single IS functions into services and how to plan, manage and measure these services at the single IS level and how to integrate them into central service management.

ISMS Development Planning Rules

This chapter will make practical recommendations on how to effectively combine inputs from strategic planning, mandated requirements and outputs from business management and user requirements when managing the development of a single IS.

References to relevant chapters of international standards such as ITIL will also be added.

Recommendations and practical guidance tools for planning requirements for the additional resources necessary for IS development, i.e. financial and staff planning at the level of a single IS in the context of the department and the office, will be an integral part of this.

It is essential that the management of the development of a single IS must always and fully use the methods and tools for the management of the development of IT assets of the whole authority, i.e. portfolios of assets layer by layer, e.g. development plans for key platforms, see more in Management at ICT unit level.

ISVS decommissioning and migration rules

The end-of-life of a system and its eventual replacement by another is another strategic decision that must be supported by architectural and economic evidence and must be prepared over a long period of time in the IK OVS.

The end of life must be considered from the start of operations, the PSA architecture and the solution architecture must be designed with the need to support the effective end of life of the ISVS in mind. Decommissioning is also addressed in other chapters of this document. Further substantive and technical additions will be included in future editions after discussion with the technical community.

Principles for the selection and acquisition of public administration information systems

This chapter is the first part of the elaboration of the requirements: "Principles and procedures for the acquisition and creation of public administration information systems" according to §8 Decree 529/2006 Coll., on requirements for the structure and content of information concept and operational documentation and on requirements for security and quality management of public administration information systems (Decree on long-term management of public administration information systems) in the scope of questions: how to find the right solution for meeting the business needs of public service provision (and changes to them).

Rules for financing the acquisition of IT solutions

Rules for the unity of programme management of informatization development

The MDICT stipulates that the use of so-called programmes for programme funding needs and at the same time for managing the introduction of change must be aligned, i.e. they are still the same change programmes in both perspectives.

It is only possible to apply for programme funding for the development of the Authority's IT in line with how the change programmes for each ISMS have been identified in the Authority's architecture roadmap and its information concept.

It follows that it is not appropriate and possible to use programme funding and instruments for the operation and maintenance of ICT solutions, even though they are capital assets and asset enhancements, unless they are changes implemented as projects under development programmes, see below.

On the contrary, it is possible, i.e. even if an operational task (operationally funded) exceeds the capabilities of the line management unit, it will use project management methods to coordinate internal and external resources and programme management tools to coordinate changes. I.e. these tasks can also be assigned to development programmes and jointly managed.

It will be determined what is the best practice for programme funding relative to a single ISVS, so as to simultaneously tie funding to expected benefits, while leaving sufficient management flexibility, especially for small ISVS.

Rules for the economics and funding of IT solution changes

The Ministry of the Interior, with possible revision by the Ministry of Finance, will set binding rules for the ongoing sustainable and manageable financing of ICT operations over the medium term, based on a mandatory five-year Total Cost of Ownership (TCO) assessment.

This implies, among other things, at least in the area of IT economic management, the introduction of a second accounting line and the recording of the consumption of the authority's resources (people, assets, energy, knowledge, etc.) in monetary terms as so-called costs by individual cost carriers. I.e. in particular dynamic cost drivers, which are programmes, projects and contracts, and static cost drivers, which are the ICT service centres, the individual components of the ICT solution, the life cycle phases of the solution and the individual

services provided.

Furthermore, this implies an update of the budget structure and budget rules.

This will move from financial expenditure management to ICT efficiency management through benchmarking and resource consumption management, see also ICT Benchmarking.

Rules for managing funding for shared ICT services

Currently, the only legal procedure for financing the establishment, operation and provision of a shared ICT service is to delegate by law to a specific OSC such a task, while allocating an appropriate budget appropriation. The resulting shared service is subsequently provided to other OSSs (or even OVMs) listed in the regulation free of charge, such as ISDS, ISZR, etc.

Proposals that shared ICT services should be covered by the General Treasury Administration chapter have not been accepted so far, instead it has been agreed that specific expenditure indicators will be set in the binding indicators of individual chapters of the state budget, which will include expenditure related to the management, operation and development of key public administration information systems, i.e. portaly_verejne_spravy_a_soukromopravnich_uzivatelu_udaju|portal of public administration]], information system through which the performance of the competences of public administration contact points is ensured, and national point for identification and authentication.

Rules for deciding how to implement ICT solutions

Any new authority IS and its services can be acquired in several ways. In terms of the way the application software is technically implemented, i.e. as:

- ASW acquired by customized development
- Type ASW (TASW[13)]))
- as an application service (SaaS[14)]))
- or a combination of all three approaches

The solution can also be implemented in varying granularity of application components included in a logical ISVS**, as:**

- **large monolithic solution,**
- **process-oriented component solution (units of components)**.
- **orchestration of microservices (App-Store)**
- **combining all three methods in different parts of the solution.**

Each sub-part of the overall **information** system solution **can be acquired in a different model of ensuring responsibility for its delivery, operation and management, namely:**

- **in-house tribal staff**
- insourcing **(supplementing missing capabilities from an external supplier while maintaining internal responsibility for the service**,
- outsourcing **or so-called cloud (contractual delegation of responsibility for the service to the supplier) * or a hybrid solution.**

If the method of acquisition and implementation [15)] of ICT services is not prescribed by law or other legal regulation, the OMS must decide on the method of acquisition (e.g. by purchasing the solution for its own management, developing the solution in-house or acquiring it as a shared service) with the responsibility of a good manager, i.e. (See the TCO methodology: TCO methodology for ICT services VS)) and other requirements relevant for the ICT service, e.g. security, timing, etc.

In making this decision, the ISVS administrator and the management of the authority must take into account not only the existing implementation options but also the options being developed by the public administration. These are in particular strategically supported forms of shared services and eGovernment cloud.

G-cloud are shared ICT services offered and operated for public administration entities either by the *government cloud* or *commercial cloud* model. The government cloud consists of shared services operated by government data centres on their infrastructure. The commercial cloud is shared services operated by commercial entities on commercial infrastructure. Both models have catalogues of services offered and an associated e-shop.

The catalogue of certified shared services publishes in the form of a public portal those offered ICT services that can be used by public administration organisations as a shared service, and also publishes financial and other conditions for their use. It is similar to the US (**http://cloud.cio.gov**) or UK (http://govstore.service.gov.uk/cloudstore) catalogues.

Criteria for using eGovernment cloud services

The decision whether or not to use cloud comes either at the moment of designing a new ISVS or of its replacement, upgrade, etc. This means that the technical administrator must always be aware of and consider the use of shared eGC services - infrastructure, platform, software and process - in the development plan of each ISVS, as they will be materially and legally available and mandatory or economically beneficial for the ISVS administrator.

In the conditions of a given OSS and its department, the following procedural steps in particular are necessary in the preparation of the ISVS for the eventual use of eGC services:

- ISVS Subject Matter Administrators shall, with the help of eGC methodologies, assess the severity of security impacts for their ISVS and determine a security impact level 1-4 (Low, Medium, High, Critical) for the whole ISVS or for its individual functional parts,
- Subject matter administrators shall identify additional services (data centres, monitoring, ServiceDesk, penetration testing, temporary data storage, mobile data sharing services, personal productivity services, end user device management services, portal services as end user interface, operations staff, consulting services, etc.) that they need to operate and develop the ISVS,
- Technical administrators shall determine the appropriate architecture for the implementation of the ISVS using eGC services
- Subject Matter Administrators, with the help of Technical Administrators and TCO eGC methodologies, identify the parts of the ISVS that would be economical to operate using eGC services,
- Subject matter administrators shall store information about their ISVs in the IS about ISVs (i.e. in the catalogue of currently operated ISVs) in the required structure, including any requirement to use eGC services.

Criteria for the use of eGovernment Cloud services, representing a combination of decision-making based on security impact assessment and determination of the required security level and on the basis of cost-effectiveness, will be updated with relevant legislation and published with detailed guidance and tools as part of the Knowledge base.

Rules for better purchasing of ICT solutions

The procurement of ICT by purchase, depending on the nature of the specific project, is governed in the public administration by the requirements of the legislation governing the management of public funds, in particular the regulations governing public procurement.

All representatives of the public administration, participating in various roles in the process of ICT procurement, are obliged by the Ministry of Public Administration to evaluate whether and what obstacles to the implementation of this concept are caused by the regulation of the management of public funds and to propose

to the Ministry of Public Administration suggestions for legislative amendments so that the principles of this regulation are fully preserved, while at the same time enabling individual purchases to fulfil the conceptual management of the information technology of the Ministry of Public Administration according to the ICCR and according to the information concepts of individual public administration bodies.

The basic problems of good purchasing of ICT solutions are in particular:

- the conflict between the overly strict provisions of the HIPAA, linked to non-discriminatory competition of one ISVS or its sub-component, and the need of the OVS as a good manager to use a shared eGovernment platform, office or shared platform common to several components of one ISVS
- the contradiction between the common legal interpretation of the OHSA in terms of the need to "re-compete" the ISVS supplier every 4 years and the realistic moral and technological sustainability of at least ASW/TASW of 10-15 years.
- the contradiction between an almost "panic" fear of dependence on suppliers on the one hand, and on the other hand the disregard of the potential of suppliers without achieving a beneficial balanced long-term partnership with ISVS suppliers or their components.

As good practice, basic approaches can be recommended for OSSs and their ministries. In particular, in the future they should use the following tools to increase transparency in the preparation and execution of contracts for the supply of information systems:

- **Marketing market research** - presents the organisation's intentions to the public and allows them to comment on the requirements and the required solution concept.
- **Preliminary (individual) market consultation** - historical experience shows that individual communication with business entities or the public is a suitable way of implementing market consultation. In the course of market consultations carried out in the past, it often turned out that consultations carried out with the participation of several participants, especially business entities, hinder open dialogue. Each party in such a market consultation is vigorously defending its know-how against potential competitors. The recommended form is therefore individual market consultations with proper documentation of their conduct and outcomes.
- **Project of Confirmation (PoC)** - has been described under the ex-ante control approach in the previous chapters.

Further substantive and technical additions will be included in future editions after consultation with the professional community.

Basic measures against supplier dependency in design and procurement

The basic nature of the phenomenon of supplier dependency (also Vendor-Lock-In) stems mainly from four factors, namely:

- the inability of the authority to develop the ISMS because it has not built up such competence itself in its implementation and subsequent maintenance, i.e. sufficient qualified human resources and sufficient knowledge, information and skills;
- the impossibility of acquiring such resources because, as a rule, the Authority is not contractually entitled to do so by the original supplier on the basis of an inappropriate setting of rights and obligations towards the supplier;
- the inability to compete among multiple suppliers of services to the product because of the uniqueness of the development or operational environment or the absence of multiple suppliers of services to the product in the marketplace;
- the characteristics of a product that is delivered without a development environment (compiled, executable only), without source code, model and documentation, so that it cannot be changed even with the best will.

This implies the following rules for the preparation, implementation and development of ISVs:

1. The Authority may not enter into a contract associated with an information system that does not contain a licensing arrangement entitling the Authority to provide all deliverables (source code, development environment, data model, documentation of the work, training materials, user manuals, etc.) obtained under the contract to any third party entity of its choice for support, maintenance, development or decommissioning and replacement of the information system.
2. The Authority shall not be entitled to conclude contracts which are unilaterally disadvantageous, either for itself or for the supplier. Even a substantial disadvantage of the contracts to the supplier will eventually backfire on the contracting authority, for example by increasing risks, in particular related to the supplier's inability to meet disproportionate obligations.
3. The Authority may not enter into a contract associated with an information system that is so unique that there are no multiple suppliers/service providers capable of developing, modifying or operating such a system.
4. In the case of application software, those IS solutions that do not assume or allow for any modification (data model, program code) or addition of add-on modules, i.e. they are delivered only in executable, compiled form, without source code and without a development environment (e.g. Antivirus or parts of Office), it must also be the case that all outputs associated with, delivered with or generated by the project must be contractually available to any third party or the public, except for the actual right to use the solution.

Other standard (boxed, COTS, TASW) application software for the solution, which OVS in turn expects to need to tailor, not only in terms of parametric changes (e.g. user dials) but also changes to the data model and programming functions and any bespoke software developed:

- must be contractually and physically delivered in a form that allows the Authority to maintain and develop the work freely on its own or with the help of third parties,
- they must never be delivered merely already compiled into an executable environment (Run-Time), but must include full support for the change phase (Design-Time), i.e. the development environment with all models, libraries, source code, development documentation, etc.

Also, all application and operational software, developed at the request and with the funds of a public authority of the Czech Republic or the EU, must be delivered with an open license, allowing its use, or the use of its parts, by any public authority of the Czech Republic - Open Source and EUPL license.

Further detailed information on Anti Vendor-Lock-In is provided here, and will be further added and continuously updated in Knowledge base.

The long-term goal is to provide added value in the operation of information systems and applications by optimising the arrangement of links between systems or applications and by using shared application functions. In a narrower technical sense, it is the integration of various technical parts of an information system (even of varying maturity and obsolescence), i.e. systems or applications, into a single entity, mainly by means of integration and orchestration tools.

The aim is to build an information systems architecture that effectively supports processes and agendas within the OVS and its department. Furthermore, this approach enables a significant increase in interoperability and flexibility, while reducing the risk of dependency on a particular vendor (vendor lock-in). This will be achieved in particular by creating application components that provide services shared by multiple applications.

This objective will significantly simplify the existing architecture and reduce the cost of modifying existing systems and applications. In addition to reducing the cost of implementing and integrating new systems and applications, there will be greater automation of processes, resulting in reduced costs and increased processing speed. Last but not least, easier integration with systems of external entities will be possible.

In order to successfully achieve the presented approach, the following measures should be implemented:

- Transition to a service-oriented and orchestrated architecture - construction of an ESB/BPM platform
- Gradual transition of individual applications (systems) to service-oriented architecture

- Maintaining documentation of IS and ICT services in models that comply with TOGAF and ArchiMate standards.

Further factual and technical additions will be included in future editions and in the Knowledge base after discussion with the professional community.

Achieving long-term balanced partnerships with suppliers (avoiding Vendor-Lock-In)

The ISTC and the Knowledge Base will help to establish and maintain a long-term balanced partnership between ICT services and their suppliers by publishing a series of guides and tools, such as model contracts and tender documents or standards and how-to guides. Consideration will also be given to a model whereby the sub-contracts of individual PSCs will refer to the general terms and conditions of the public administration, issued in agreement with the MoI or the MMR.

Each PSC would still have a choice or modification, but the terms and conditions would already balance the rights of both parties. There may be a separate annex reflecting both the State Property Directive and the provision of knowledge to information systems.

Further factual and technical additions will be included in future editions after discussion with the professional community.

Principles of Open Source Software Acquisition

Open Source Software and Free Software (OSS&FS) has been an integral part of ICT for many years. From a security point of view, these products have long been proven to be safe. Unfortunately, many products have historically changed from OSS to paid versions. Further, many products have stopped being supported and almost all OSS projects have the assumption that we have to make the changes ourselves.

Therefore, purchasing OSS is definitely risky if we do not consider all the implications. In any case, using OSS does not give us management and administration for free. The long-term sustainability of OSS is not dependent on a short-term solution. The primary view must be the life of the information unit over its 5+ year lifetime, with a clear strategy for how to continue to operate it beyond the baseline 5 years (relevant to TCO).

A separate methodology will be developed for the use and suitability of integration of each OSS product. It will focus not only on the integration of OSS elements into information units, but also on the possibility of sharing successful products such as a filing cabinet or anonymiser. More information on this topic will be published in Knowledge base.

Rules for valuation of IS development or modification

For better determination of the maximum price of the work or for comparability of solution variants with different degree of software customisation, it is necessary in ICT VS CR to use a unified methodology for valuation of software development (or customisation) for OSS, based e.g. on the function point method according to ČSN ISO/IEC 20926.

This methodology should be developed and issued as another standard of the OŘI MV unit, see Introduction, and published in Knowledge base.

Contractual security

In practice, ICT managers have to deal with many types of contractual relationships (development, operations,

support, licensing,...) without adequate support.

An important step is to unify the types of contracts according to content, length, scope, etc., i.e. to bring uniformity and order to the contractual system in the management of ICT relations with suppliers. Furthermore, it is necessary to gather experience and transform it into an expression of best practice in the form of guaranteed contract templates, including their possible combination with general terms and conditions, see above.

One of the objectives of the next edition of the MRICT and the continuous updating of the Knowledge base is to provide additional information, documents and tools to support safe and effective contracting in public administration ICT.

Concepts for managing the successful implementation of proposed ICT change projects

This chapter is the second part of the elaboration of the requirements: "Principles and procedures for the acquisition and creation of public administration information systems" according to §8 of the current Decree 529/2006 Coll., on the requirements for the structure and content of the information concept and operational documentation and on the requirements for the management of security and quality of public administration information systems (Decree on the long-term management of public administration information systems) under the heading of questions: how to successfully implement and put into productive operation the selected solution. It contains essential and nationally applicable standards to the requirements of the Decree (after its expected amendment).

Program and project management rules for individual ISVs

Informatics in the Authority serves its internal clients, informatics projects are intended to contribute to the achievement of Authority-wide goals, and public service change projects increasingly rely on informatics support. In addition, all projects in the Authority share a limited amount of project-appropriate human resources. Therefore, all individual ISMS projects need to be coordinated with each other within the ICT Unit, then more broadly across all projects across the Authority and, in the future, the eGovernment of the country.

The coordination of projects, their linking to programmes and the management of project portfolios is a service of the Project Office of the Authority (also referred to as "PK"[16)]). It builds on the work of the strategic units and is knowledgeably supported by the services of the Authority's overall architecture unit, the Architectural Office (also referred to as "AK"). For more information on joint project and programme management at the office level, see Management at the ICT unit level.

ISMS development programme management

All projects that are related to each other in time, subject matter or otherwise, must be managed as a programme to ensure that together they deliver greater value and with greater certainty than if they were managed separately.

Whereas project management is primarily focused on achieving planned outputs while maintaining consumption of planned resources, programme management is primarily focused on meeting strategic objectives and achieving expected benefits. From this perspective, it is recommended that each individual project should also be managed using both project and programme principles. More on programme management Management at ICT unit level.

ISVS project management as part of a portfolio

Very often a large number of projects are managed simultaneously in the ICT unit and across the office. The responsibility for their management is divided among several project directors with the support of project managers. A group of projects with a common responsibility of one project director or project manager, or conversely a group of projects similar in content, functional unit, supplier, shared resources or other criteria, is called a portfolio.

The basic feature of a portfolio is that someone specific is responsible for it and reports the progress of all projects in his/her portfolio to someone.

For each individual ISMS project, it follows that it must be clearly assigned to one director or manager and thus become part of his/her portfolio, his/her responsibility and his/her reporting to the SC and the management of the office.

For more information on project portfolio management techniques, see Management at ICT unit level.

=== Rules for managing individual ISVS implementation projects ===.

For any IT activity that meets the definition of a project or, depending on the scope of its implications, the ICCR stipulates that it should be consistently managed as a project from the outset, i.e. using project management methods, responsibilities and tools.

There are several definitions of a project which differ slightly from each other, but all express the same essence:

- A project is a time, cost and resource constrained set of activities leading to the promotion of development strategic objectives, change and innovation (excluding operations, but including large-scale maintenance, repair, renewal and purchase of services or tangible and intangible assets).
- A project is a time-limited effort undertaken to create a unique product, service or result. This means that a project has a defined beginning and end. It results in the creation of a unique product or the ability to provide a service, as opposed to operational activities which are repetitive and have no defined end.
- According to another definition, a project is "*a unique process, limited in time, cost and resources, undertaken to produce defined outputs in terms of quality, standards and requirements*".
- A project brings about a one-time (step) change in the quality of its object, in this case primarily a change in the characteristics of the ISVS, a qualitative change in the ICT infrastructure, or a change in the capabilities of the IT department; it has a fixed goal, i.e. the extent of the change, which must be implemented within a specified time and using a planned range of resources (financial, human, material,...).

The obligation to apply project management is established for projects (at least one of them):

- whose value of expenditure is greater than 10% of the development and innovation part of the Authority's annual IT budget (not the operational part of the budget),
- where the level of involvement of human resources (internal and external, IT and professional together) exceeds 10% of the Authority's own annual internal IT unit capacity - capacity criterion,
- the preparation and implementation of the change takes more than 3 months - time criterion,

where changes to the ICT solution or infrastructure may impact on its resilience to cyber risks or its ability to deliver public services - risk criterion.

After the experience from the practical application of these rules, the next edition of the document may further limit the project management boundaries to accommodate small authorities, especially local governments.

For each project meeting the above conditions, the authority is obliged to include an adequate number of internal staff in the project team before the project starts, to ensure that the know-how applied or created in the project remains available as knowledge and skills (not just documentation) in the authority. This is one of several prerequisites to defend against an undesirable level of dependency on suppliers (Vendor Lock-In). In this

context, we need to ensure that:

- employees of the Authority whose assignment to the project exceeds 10% of their working time (4 hours per week) are released for the project[17)] and a corresponding part of their normal work and responsibilities were (formally and de facto) transferred to other employees of the Authority.

To the extent of their integration into the project, * the employees were subject to the project management, i.e. their direct supervisor is the head of the project team, who, inter alia, approves the employee's statements of work and awards remuneration for work on the project. The escalation levels are the project manager and the steering committee. This can be handled by means of delegation decrees, see below.

- in case of external contractor participation, the tender documentation and contract required as an integral part of the performance the activities, outputs and way of working (approach) leading to an effective transfer of knowledge and active skills (for example: system setup or filling in the dials in the system is not done by an external consultant but by an internal employee under the guidance of a consultant, ...).

The section of the MCIT on the approach to the management of IT services describes the minimum roles and positions that the office and the IT service must have (In/Out) in order to fulfil the above requirements. At a minimum, specific human resources (by name) must be assigned to the following roles to ensure quality and safe management of ICT change projects:

- Project Sponsor - a statutory member of the management of the Authority[18)])
- Project Director - the operation sponsor, (for cross-departmental projects, a government appointment is required)
- Project Manager - project management expert
- Solution architect (domain and platform)
- Analyst - internal consultant, able to parameterize and develop solutions
- IT services group manager ("trader" of IT services for internal clients - specialist departments)
- ICT Operations Manager
- External services buyer
- IT economist (project budget manager) - capable of controlling the department, projects and components
- IT Auditor - providing IT governance functions to ICT management and other components of the office
- and others

In the Knowledge base a table of expected job and service roles for each project role will be prepared.

Appointments must be made in writing, via a letter of appointment signed by the appointee and the supervisor/manager. In doing so, it is clear that the Authority may use external service providers for the implementation of these roles, but this does not absolve it of the obligation to have internal staff assigned to the roles, "shadowing" - controlling external staff, with clearly defined responsibilities. The roles of project sponsor, project director and IT economist (project budget manager) cannot be outsourced.

Each project must have these roles arranged in an organizational structure containing a hierarchy of authority and responsibility:

- A Project Steering Committee (also referred to as the "PSC"), headed by a Chairperson and including at least the Project Sponsor and Project Director, and a statutory representative of the Authority if neither the Project Sponsor nor the Project Director.
- The Project Core Team (also referred to as the 'HTP'), led by the Project Director and including at least the Project Manager, the Project Manager for the Contractor, the Project Administrator, the Principal Project Architect and the Project Team Leads. The core project team shall include support roles for the Project Director as required, such as a technical and substantive project manager, a lawyer, an economist (project budget manager), a quality manager and a project publicity manager.
- Project management teams (also referred to as "PMs"), led by the PM team leaders and including at least team members from the Authority side and, where appropriate, team members from the contractor side.

For very small projects[19)], roles and responsibilities in the project management plan can be reduced accordingly, for example by having a separate Project Director (who must never be absent) take on part of the Steering Committee's roles and responsibilities, with the Authority's management as a whole taking on the remainder of the RCP's responsibilities, the Project Manager taking on part of the Core Team's roles and responsibilities, and the HTP taking on the remainder of the HTP's roles and all of the roles of the project teams. Redundancy is at the discretion of the project office or office management, where there is not already a PC.

Each ICT project, regardless of content or size, contains a minimum set of phases of its life cycle with fixed deadlines as defined by the methodology.

Regardless of the project management methodology used (Prince2, PMI, etc.), the project must pass at least a mandatory, methodology-specified minimum set of control milestones or interim activities aligned with both the need to deliver quality ICT solutions and the requirements of the financial control and procurement processes.

From the mandatory and extended set of milestones, intermediate activities and project deliverables, milestones, activities and deliverables relevant to the specific project are selected in a justified manner during the initial project planning. Non-selection, omission of a mandatory milestone, activity or output must be clearly justified in the project documentation.

A project managed in compliance with these ICRC rules must produce and use at least the minimum set of deliverables/working documents specified by the methodology. Each project must have, at a minimum, a project plan during project preparation, a project management plan during implementation and a project progress report at completion.

The project management mechanism must include mandatory reporting to the management of the Authority, for example through the project office or the project steering committee, once a month, containing a minimum set of data as defined by the methodology.

Project management must include active engagement with key stakeholders, their legitimate needs and expectations.

Project management must include an ongoing and final evaluation of the results and benefits achieved, and a guided learning of lessons learned.

More information and rules on the management of ICT projects and their portfolios, including links to human resources management, will be issued by the Ministry of the Interior of the Czech Republic in the form of an update of the Methodology for IT Project Management, which will also be published as part of the Knowledge Base.

Risk and security management in implementation projects

An important and non-negotiable part of project management is, besides managing the scope, time and resources of the project (budget, people and technology/assets), also managing risks and taking appropriate measures to mitigate them.

Project risk and security management includes the management of cyber risks and security in accordance with their management methods and using tools at the level of the entire ICT unit and office, Management at the level of the ICT unit.. The optimal risk management method is a combination of practices from standard project management methods, the TOGAF framework and the issued recommendations of the NCIB. It is planned to release a set of accelerators in the Knowledge base to support best practice in this area.

Other principles such as "Security by design" and methods such as secure software development must be applied in the project.

Approval of projects by the HA Department of the Ministry of Interior

The process is managed in accordance with the OHA's continuously issued Methodological Guidelines and their corresponding forms, see the OHA website, which together with other guidance and tools will be continuously updated in the Knowledge base.

=== Principles for documenting the actual implementation of an IT solution ===.

Knowledge of the current state of configuration items of the ICT application and technology architecture is a prerequisite for its effective management. However, this knowledge often does not include the current documentation of ICT systems, or accepted documentation of the actual implementation of the required change (e.g. setting access rights for individual user roles) or new ICT service, including knowledge of the current contractual support (maintenance), or contractual SLAs (what they are, until when they last, ...).

The responsibility for reflecting accepted changes in the current documentation should always be clearly identified for individual ICT systems.

Optimally, this activity should be included as an integral part of the acceptance processes and the responsibility for it should be assigned to the organisationally competent Technical Administrator.

Standards, templates and typical examples of such documentation will be progressively updated in the Knowledge base.

Documentation of program modifications

In the last two years, software management has advanced significantly with the possibility of self-deploying the Gitlab portal, which not only manages all software versions, but more importantly, machine checks can be set up for this deployment method. It is also possible to roll back between versions and also check the described source code. In the commercial world, the deployment of systems via Gitlab has changed very quickly, because such deployment does not require human interaction and there is a complete audit trail of the changes made.

Solution architecture and office architecture updates

Architecture updates should have a set milestone of once a year or a maximum of a two-year cycle for small in-line changes. In the case of project-implemented changes, an update of the subject solution architecture models at all levels of detail (EA-PSA, SA and SD[20]) must be completed and submitted together with the documentation of the actual implementation as part of the acceptance of the project deliverables.

The datasheets shall also have a record of all changes and subsequently all changes from the datasheets shall be propagated to the architecture models at a given milestone.

Policies for acceptance of project deliverables and transition to productive operation

Careful acceptance of the results of the change implementation and verification of the successful transition of the new IS services into productive operation is one of the key project milestones and a milestone in the information system life cycle.

Proper acceptance of the deliverables is also directly related to the so-called Ex-ante approach to planning and change management (see Management of unified ICT solutions), as it allows to verify the achievement of the planned indicators of the selected solution method.

It is the intention of the MŘICT to follow the types of contracts concluded (Management of unified ICT solutions),

the different ways of implementing the solutions of the implemented changes (Management of unified ICT solutions), the Methodology of IT project management (Management of unified ICT solutions) and other aspects of the acquired solution, to prepare and update in Knowledge base a set of guidelines and accelerators to facilitate and make more consistent the proper acceptance of the delivery of implemented changes.

Rules for effective management of operations and service delivery, service procurement and continuous improvement

Corresponds to the ITIL processes of part Service Design, part Service Transition, full Service Operation and Continuous Service Improvement, as well as the COBIT 5 processes of Deliver, Service and Support.

We will discuss with other partners and the result will be completed.

Building and maintaining competencies to operate and develop IT solutions

Building monitoring, defining monitoring and building a department to support and develop ICT services, including mechanisms for follow-up on datasheets and SLAs.

We will discuss with other partners and the outcome will be completed.

Example of a rule: The Authority is obliged to build its own competence centre (competence centre) for the maintenance and development of IS for which it is responsible as a subject matter manager for the flexible legislative development during the implementation of a new solution or after the effectiveness of this ICD for solutions for which it has not done so in the past. It can replace its own competence centre by securing such competence from another public administration or state-owned entity, either by contract or by law, but it must be competent capacity, independent of the original supplier, which the authority can dispose of as if it were its own staff.

A competence centre must be maintained for the solutions and platforms of these solutions.

Policies and procedures for the operation of public administration information systems

We will discuss with other partners and the outcome will be completed.

Principles for the care of clients and users of information systems services

Sub-recommendations related to the ServiceDesk knowledge base: the handling of every life situation in the ICT world must be measurable, as 90% of all life situations are recurrent and the knowledge base makes the service management system faster in all cases. Each incident takes days to resolve the first time, hours the second time and the next time the same incident is resolved the same day.

If you use an information system, centralise all requests in one place and have a team responsible for dealing with them, then the subsequent classification of these requests will quite naturally speed up their settlement.

Other methods of ISVS client care will be included in future editions of the MIRCT and updated in the Knowledge base after discussion with the professional community.

ISVS Indirect Governance Rules

ISVS indirect governance methods will be included in the next editions of the DGICT and updated in the Knowledge base after consultation with the expert community.]

1)
Corresponding to the acronym SDLC - Software Development Life Cycle
2)
Other authors also use the terms: steps, stages or phases, but these terms are retained for other purposes.
3)
https:%%/%www.google.com/url?client=internal-uds-cse&cx=015489265366623571386:izzrwg3bmqm&q=https:%%//%%www.mvcr.cz/sluzba/SCRIPT/ViewFile.aspx%3Fdocid%3D21793567&sa=U&ved=2ahUKEwjo65mCpbbjAhVKR5oKHbPUBvQQFjAAegQIABAC&usg=AOvVaw0pSuoaLR5IWUWODLfvqk
4)
Instruction of the Minister of the Interior No. 5/2017 of 25 January 2017, which establishes the project office and regulates the management of projects in the field of competence of the Ministry of the Interior
5)
(From the Project Start Architecture, a model of the system for a future project at the level of Enterprise Architecture.
6)
(Functional & Non-functional Specification.
7)
From the Project Start Architecture
8)
As evidenced by published experience from e.g. the USA and the UK, the Catalogue is one of the key tools for ICT management in public administration. It builds on the catalogue of public administration services and records all ICT services (SaaS, DaaS, PaaS, IaaS) that are currently operated both for the internal needs of authorities and offered as e-services to citizens and companies.
9)
The contract should avoid disadvantageous provisions (Vendor-Lock-In), cf: . https:%%//%%www.mvcr.cz/soubor/hlavni-architekt-egovernmentu-dokumenty-typicka-nevyhodna-ujednani-ve-smlouvach-na-dodavku-ict-produktu-metodika-anti-vendorlock-in.aspx.
10)
The term "exit plan" or "exit strategy" is also used.
11)
Project Start Architecture, (rather than the Czech PAS - Project System Architecture or SAP - System Architecture Project)
12)
Functional & Non-functional Specification.
13)
The English abbreviation is COTS (Commercial off-the-shelf
14)
The English acronym is Software-as-a-Service
15)
from English: deployment, deployment
16)
Project Management Office - PMO.
17)
It should be possible for an employee to be released for the project without his/her consent and without the consent of his/her immediate superior, for example, by using Section 47 of the Service Act, No. 234/2014 on transfer. It would be useful to push for legislation to regulate the maximum period of transfer without the employee's consent to 120 days per calendar year and with the employee's consent for up to the duration of the project.
18)
unless it is the Project Director or the Subject Matter Leader of the change (agenda
19)
The definitions of small project and very small project are still being sought.
20)
Enterprise architecture, solution architecture and solution design.