Materiál Ministerstva vnitra

Export z Národní architektury eGovernmentu ČR

Obsah

Management at the level of the ICT OVS unit

The Authority's ICT management system as a cross-cutting operational capability encompasses two key process areas or functions. The most important is the joint and unified management of the development of information systems and their services to clients. But also important is the effective management and administration of its own resources and the continuous improvement of IT management processes.

This chapter covers both, but in particular summarises selected key tasks, processes and methods for managing the ICT OVS as a unified whole, while highlighting recurring methods and processes from the life cycles of individual ISs that require a unified and centralised approach (from both the OVS and government perspective).

These centralised activities at the level of the office and the state also correspond to the identified life cycle phases of individual ICT assets (IS, solutions, functional units), more in Management of individual ICT solutions and are a prerequisite for the individual activities of the management of individual assets to take place in a coordinated manner, in context and with respect for the overall interests of the OVS and the VS CR.

Key Principles of ICT Management in the Office

The rules in this chapter represent the basic common standards for line and project management of IT across other areas of (strategic, tactical and operational) management.

Despite the strengthening of the elements of sharing and national coordination, the fundamental management of informatics and informatization remains at the level of the individual OVS. In particular, the model of ICT governance and oversight at the OSS level must be built on the following key principles:

- The organization has a valid, correct and understandable Information Concept of the OVS.
- The organisation has a functional organisational structure, capacity and skills to manage the implementation of the changes formulated in the OVS IC.
- The organization develops and values the competencies of skilled personnel who bear the burden of implementing the OVS IK.
- The organisation is able to operate or manage the operation of the implemented solutions in-house and continuously improve them operationally
- The organisation respects international standards and best practices and is able to adapt its internal regulations and processes to them

Each OSS responsible for managing information technology in its own administration must be able to perform ICT lifecycle management functions effectively and correctly:

1. Developing ICT strategies and concepts, including:
    1. Contributing to the development of the Authority's ICT and eGovernment legislation
    2. managing the Authority's architecture
2. Planning and organising ICT management, including:
    1. management of ICT resources - human, knowledge, material
    2. management of ICT asset portfolios - information, application and technology components
3. ICT acquisition and implementation of ICT changes, including:
    1. managing the architecture and documentation of ICT solutions
    2. procurement management
    3. programme and project management
4. ICT operations, maintenance and support of clients and users
5. Monitoring and evaluation of ICT services (as a means of governance, i.e. oversight and control)
6. Archiving, decay, preservation and termination of solutions, with possible migration to new ones (Exit strategy)

Approach to the organisation and management of IT

The internal structure of the Informatics units must match the structure of the required roles and their competencies according to this methodology, i.e. strategic planning and management, change acquisition and implementation, operations management and service delivery, ICT governance.

Along with the developing specialisation of IT, the need to develop the structure of the ICT unit is growing. This should also include units related to architecture and the link between architecture and the other activities described and mentioned above across the Authority. Only in this way can it be ensured that ICT, as a key operational unit of the Authority, is considered as a partner already in the formulation of legislative changes, i.e. at the legislative level, and not only in the implementation of legislation at the technical level.

Also, both the role of the ICT architect (Architecture Offices, AK ICT) and the role of professional ICT project managers (Project Offices, PK ICT), both working together for the CIO of the office, need to be added or improved in each ICT unit of the VS office.

Within the framework of Strategic Informatics Management and ICT Governance, it is necessary to implement the linkage of the ICT unit to the overall structure of the Authority. This implies, among other things, that:

1. the Head of Unit (CIO) of the ICT must be part of the top management of the authority - in ministries, a deputy to inspire the development of its public services; and
2. there must be a fundamental change in the relationship of the ICT unit with other departments of the authority in the sense of Client - Supplier,
3. there must be an Architectural Office of the Authority (AK OVS) and a Project Office of the Authority (PK OVS) that propose the content of strategic changes to the architecture of the Authority and coordinate programmes for their implementation, including their ICT parts (projects).

We will discuss with other partners and the outcome will be added in the next edition.

The ICT Service's own architecture

To ensure its cross-cutting operational capability, each ICT unit has (should have) maintained its own Authority Architecture (EA), across all domains as per NAR.

This means that the ICT unit must also have and actively use a capability decomposition model or business functions (processes and services) in the form of a table and graphical map. These should be used to analyse and communicate the strengths and weaknesses of their capabilities and plan for their improvement.

Similarly, the ICT unit needs to have a map of the portfolio of application components used to support ICT processes, as well as a map of the dedicated technology, physical and communications infrastructure for these custom applications.

The ICT unit should also maintain the relevant part of the motivational architecture in all four vertical domains to share with the team and the rest of the office an understanding of its motivation and mission, its performance, its security, and its regulations and constraints.

It can be assumed that through the activity of the pilot offices in adopting these Management Methods, validated models of each domain of the ICT capability architecture will emerge and be generalized and published in NAP and in Knowledge base as reference models and accelerators for the modeling of the OVS.

Human Resources Policy and Development in Relation to ICT VS

Building human resources is one of the most important prerequisites for achieving informatization goals. Conceptual and operational plans will only come to fruition if they are implemented by a motivated, skilled and competent workforce of IT staff in the public administration.

According to the ICCR, the Ministry of the Interior of the Czech Republic will also assume conceptual, methodological and coordinating responsibility for building human resources in the informatics of the public administration as one of the means of coordinating the informatisation of the public administration according to Act No. 365/200 Coll. It will also initiate and coordinate development programmes in this area.

Nevertheless, the full responsibility for planning and managing the acquisition, retention and development of qualified IT capacity remains with the management of the individual public administrations.

The MoI will issue a Methodology (or concept) for human resources management for this area of ICT management and will publish further information and tools in Knowledge base.

Approach to Human Resource Development Informatization

The basic trends of human resource solutions in VS informatics are in-sourcing of high-end (IT strategy, architecture and management) and routine, generic IT disciplines (such as HelpDesk, field operators), use of experts from vendors (platform specialists) and, above all, efforts to recruit and retain in-house staff to manage ICT and cultivate relationships with clients, the subject matter administrators of IS.

A complementary trend is to build expert, rapidly available capacity for specific consulting tasks (office architecture, IK development, TCO calculation, OHA application support, tender documentation support, etc.) in the shared competence centres of the VS CR.

Each ICT unit is looking for a boundary to settle the needs by its own forces or by a contractor. The actual administration and management should be in their own hands, but in-house solution development is no longer required today for several reasons. One reason is the risk to long-term sustainability, whereby the loss of in-house human resources will deprive the OVS of the ability to address IS changes. The second is the 3E principle itself, where I don't have a competitive advantage given by the market when I outsource. In-house creation is suitable for selected areas where it is a simple service that will not mean re-engineering in the future or, on the contrary, a service where the assignment is completely unique.

However, in-sourcing still has a strong presence in ICT, not only for staffing the Service Desk but for controlling all systems.

There needs to be a representation of operations, security and development. Each department is responsible for different activities, but they have common boundaries and cannot be separated. There was a barrier between security and operations in recent years by adopting policies, but they eventually merged again and now function more as an opportunity for exceptional representation due to the common boundary. Systems development and evolution will never be represented by operations and security, but at the same time separation is quite impossible because half of the processes are shared. Outsourcing has always been an alternative solution to providing for needs, but it became clear 15 years ago that only hybrid outsourcing, i.e. one that can be well audited, makes economic sense.

The eventual emergence of free use of the capacities of the National Data Centres or the state part of the eGovernment Cloud, as soon as possible, will undoubtedly have an impact on ICT staffing strategies and staff profiles.

Development and retention of knowledge and competences

Computer science is a knowledge-based discipline, dependent on maintaining up-to-date overview and detailed knowledge of the field. A study conducted by ICT Benchmark found that some OSCs have a paltry amount of

money set aside in their training budget for each ICT unit employee, equivalent to 1 hour to 1 day of commercial training per year.

Active ICT involvement in digital transformation and a well-written office IK must make the case for IT staff to negotiate the budget. But alongside this, it is the role of the ICT Management Unit at the MoI (IMU) to ensure more accessible training for MoS staff involved in the management and operation of ICT services, either by using the MoS Competence Centres mentioned above or by working closely with university departments for this purpose.

However, a prerequisite for developing competences is to recruit and retain the staff in the first place. Therefore, it is necessary to change the remuneration of ICT managers in the public administration so that it approaches the level of comparable professions in the private sector and is dependent on the achievement of clearly defined personal goals. This is in line with the ICCR's main objective 4 and must be implemented by central and local measures, for example by making greater use of the Key Employee Institute.

Given the difficulty of enforcing this change, the change could be gradual from key roles to less important roles. At this stage, the key roles are those that will develop the new concept of ICT management in the VS, design the architecture of VS and ICT services, formulate the sourcing strategy, formulate requests for external supplies, select the most appropriate bids and control the status of supplies.

Relationship between the ICT profession and the civil service

The basis of honest management is not to hide things and to call them by their real names. So if, according to the ICCR and the MoICT, there is a need for experts in ICT VS for roles in strategic planning and transformational change management, for example, i.e. in particular the roles of office architects or programme and project managers, then the civil service profession needs to be urgently expanded to include these roles. This change is in line with sub-objective 4.1 of the ICD.

At the same time, the professions involved in ICT management, eGovernment and strategic change must be able to draw on and transfer experience from many other sectors to the civil service. They therefore need to be very flexible in the labour market and, thanks to their expertise, they do not even need the protection of the civil service, on the contrary.

For such cases, it should be possible to employ experts in both service and employment and, regardless of this, to remunerate them in the same way as in the labour market, from where they need to be recruited and retained.

Economic and Financial Management of ICT

Budgeting, budget measures

The budget itself is key to the operation of all ICT services of an organisation and in most cases consists of many items. It is up to each representative to decide how and with what tools they will carry out, or do the actual budgeting and subsequent reporting. At the highest level, the budget is made up of mandatory[1)]) and optional (optional) expenditures. The division can also be defined as operating (OPEX) and capital (CAPEX), this designation is mainly used in private organizations, but it can also be applied semantically to public administration.

Several contexts need to be kept in mind when budgeting:

- ICT has assets under its management that need to be cared for in the long term with the care of a good manager - this means that for each item a support item needs to be accounted for and a correct decision made as to whether or not to acquire support (a long-term vision and strategy is a big help for this).

- Prices of IT commodities may decrease over time, so it is necessary to monitor and plan for their reduction, e.g. by re-competition according to the ZoZVZ [2)] etc.
- Moral obsolescence of information systems starting from the seventh year of IS makes the system more expensive (mandated expenditures are progressive), then by the tenth year there may be a marked increase. For this reason, the system needs to be upgraded or planning for renewal should be initiated.
- Many commodities can be used as a service.
- Internal resources are not the cheapest, on the contrary, they are the rarest and often unique - therefore it is inefficient to deploy these resources to fulfill commitments that we think everyone can handle - here we save the minimum on costs and we lose this human resource in most cases after some time and replacing it costs the organization a lot of money and always a drain of knowledge to an external supplier.
- New projects and requirements do not usually arise overnight, the management of the organization should have it ingrained in their culture that every new requirement is communicated to all stakeholders including the ICT department. It is more than advisable to reach out to your subject matter sponsors when budgeting, and to put in place a system of requirement gathering (to be mentioned later in the document).

Budgeting is then not meant to be a unilateral act. The requests and demands made by the ICT Unit may seem excessive, but it should be remembered that the Unit is a support unit for many internal services and services to the clients of the VS. Therefore, the budget needs to be interpreted and mutually negotiated by the economic officer to the extent that it is clear to all actors what each item means and what purpose it supports. Finally, there must be a pre-acceptance of the budget.

Final acceptance then occurs after the budget has been confirmed by the government and parliament. In the case of a request for **budget reductions**, there can be **only reductions in optional expenditure**. In this case, the ICT representative will prepare an impact analysis of which parts of ICT services will be affected by the reduction, including a definition of the risks, and will advise the Authority's management in writing.

Reductions in expenditure on mandatory (operational) items can then only legitimately take place in programme funding, i.e. in the medium and long term. This is due to the threats and high security risks associated with reductions in long-term commitments and the associated reduction in the scope, quality of availability or security of services. These reductions must be preceded by a thorough impact analysis and approval of its conclusions by the Authority's management. In most cases, long-term reductions must be accompanied by a prior one-off investment in measures to enable the reduction and/or mitigate the risks.

It should be noted at this point that any unplanned intervention in mandated expenditure (or its financial coverage) within the annual budget may result in a breach of statutory obligations (ZOKB, ZoFK, etc.). Any liability for possible damage is subsequently borne by the director who made, approved or ordered the mandated expenditure without the analysis and approval of the ICT director.

Reporting and Budget Control

Each Superior must control the use of the budget, particularly for the following reasons:

- Preliminary management control as required by law.
- Control of the fulfilment of contractual obligations.
- Budget execution, this is particularly the case for newly acquired items - this is where the plan-actual gap can be interesting.
- Comparison of 3-5 year performance in the main categories, i.e. mandated and optional expenditure.
- Tracking costs of all ICT services - this tracks items for internal staff costs (including training) and expenditure on operations and service development, e.g. costs of acquiring new ICT services

The detail of the budget is dependent on the requirements of the incumbent and his/her management style or the requirements of his/her supervisor. It is advisable to prepare own reports and in coordination with the supervisor reports for the supervisor.

The form and format of the report depends on the capabilities of the ICT unit. A recommended practice may be to keep it in the form of a spreadsheet accessible under a password on a shared drive. However, an online reporting tool with advanced visuals or portal access based on roles and identity seems to be the most appropriate way.

As mentioned above, the ICT unit budget consists of several parts, i.e.:

- operating funds for services and purchases up to 40 thousand CZK.
- investment funds, which are based on programme funding and asset replacement.
- grant titles, which although increase the budget for the approved investment at a given time, but at the same time this title locks the co-funded amount, i.e. it is necessary to reduce the budget for other costs.
- over-claims, which may sometimes be approved, but their use must then be included in the current budget, and any underspending will eventually show up in unspent claims that artificially inflate the budget for the year.
- short-term or long-term budget measures based on actual spending needs.

All of the above are implemented separately and need to be made into realistic options for cost optimisation. The basic starting point is knowledge of all commitments and precise setting of fixed payments outside the framework of legislative changes (these have a life of their own and even if a budget increase is approved, these funds are only available in the following year).

The issue of budgeting and financial management will be the subject of a separate methodology based on practice and the natural behaviour of ICT.

Concept of ICT economic management in public administration

It will be completed after discussion with the professional community and published in the next issues of MŘICT and in Knowledge base.

Contract and Supplier Management

An integral part of ICT management is the management of contractual relationships with suppliers, particularly from the following key perspectives:

- keeping track of contractual commitments and planning cash-flow spend.
- keeping track of contract expiry dates and planning for contract renewal

Contract management includes efforts to consolidate the portfolio of relationships into a manageable number of long-term partners and efforts to straighten out mismatched, usually unbalanced contractual relationships.

A separate topic is the management of the portfolio of licenses and license agreements, see the following section.

The ICT unit, often in cooperation with the economic unit, must have an error-free, preferably electronic, record of data on and from contracts so that it can use these tools to meet the needs in the above aspects. In doing so, it is also important to bear in mind the following:

- The renewal of a contract (e.g. for maintenance) can take up to two years in the process of awarding a contract and selecting a contractor according to the ZoZVZ, so it needs to be initiated well in advance.
- The IS for the registration and management of contracts with suppliers is a transactional system, it cannot be replaced by the filing service alone, but must be integrated with it.
- The IS for contracts must be linked to the management of ICT asset portfolios (catalogues) and allow management from their perspective as well.
- Contract management also includes a link to the management of risks associated with contract failure and to the management of budgets to secure contract obligations.

More practical recommendations and aids on managing contracts with suppliers will be released in Knowledge base over time.

Comprehensive License Management

Licence management is now a completely separate area of ICT that needs to have a position for the role of "licence manager" at least at a central level (meaning one person for each department, other corporation or large OVS) or a sub-role for the position of ICT manager in a smaller OVS. Part of the activities of licence managers is to set the rules and have their own licensing policy. It is in these rules that the licensing manager can confirm the platform of each department, corporation and OVS.

The primary activities of this role include managing licenses from Microsoft, IBM, Oracle, WMvare, Antivirus, Adobe and others that are used in various areas of ICT. Secondary activities then include making all other licenses of each OVS transparent and manageable.

For each license, the most important factors are its scope, time and cost. It is also important what object it relates to (how it counts) - users, processors, etc. However, what is important is the rights associated with the license, such as portability to third parties.

If the Authority decides to use an OSS/FS licence, then it must provide an alternative solution in the event of loss of support (for illustrative purposes, in the case of Open Office, it is sufficient to state the need to acquire Microsoft Office or a similar product in the event of loss of support).

On the one hand, ICT licence records must be linked to the asset records in the economic unit, then to the management of asset portfolios (Catalogues), to the management of users and permissions, to the management of knowledge and competences (Anti-Vendor-Lock-In measures), etc.

Local or corporate licence management must include a link to central government licence purchases and maximise the use of the central licences offered, see Collaboration with other offices and eGovernment departments.

OpenSource Software and Free Software

Part of the responsibility of the role of the OVS Licensing Manager is to coordinate and support decisions on the use of OpenSource Software and Free Software (also referred to as "OSS/FS") as a way of implementing individual IS, see section Management of unified ICT solutions.

Policies and measures need to be adopted at the level of the ICT unit, or the corporation and the state, which will allow, on the one hand, to take responsibility and build capacity for the support and maintenance of the OSS/FS, especially if it takes the form of a shared public administration software code, and, on the other hand, represent an exit strategy from the OSS/FS in case of loss of support.

It is also part of the licence manager's remit to have the necessary knowledge, documentation and tools to successfully handle OSS/FS throughout the IS lifecycle (solution design, tender documentation, contractual provisions, code management, documentation, sharing, etc.).

Further factual and technical additions will be included in subsequent editions of the MŘICT and updated in the Knowledge base after discussion with the expert community.

Managing ICT proprietary information systems

The ICT unit is in the case of the delivery of ICT support services for its own processes in the dual role of client

and supplier of these services. Therefore, the ICT unit needs to:

- for the sub-management of these systems, consistently split the roles of Subject Matter Administrator and Technical Administrator between two staff members, with a duplication of responsibility at the CIO level,
- for the overall management of portfolios and services, follow the same approach as for the management of applications for all other Subject Matter Administrators.

As a consequence, the applications needed for ICT management and ICT service delivery must also be fully visible in the overall architecture models of the Authority, see also Assumptions and assumptions for ICT management.

Further factual and technical additions related to the different key types of information systems used by the ICT service for internal management and delivery of its services (CMDB[3)], ServiceDesk, etc.), will be included in the next editions of the MŘICT and updated in the Knowledge base after discussion with the expert community.

Strategic planning and management of ICT OSS

A fundamental change in the management of ICT OVS, highlighted in the MŘICT, is the very introduction and consistent use of pro-active ICT strategic planning, in contrast to the hitherto largely reactive approach to implementing change and managing the operation of solutions for ISVs and other systems.

Another significant change is the effort to plan and manage with knowledge and understanding of the Authority as a whole and in the context of eGovernment in the Czech Republic and the EU, and in the context of the real needs and opportunities of the Authority's clients to draw on its mainly digital services.

Part of and supporting this changed approach is the new use of Authority Architecture as a management method to support the management of ICT and digital transformation of the Authority, in line with the objectives of the ICCR.

Approach to strategic IT management through the Authority's architecture

In the normal management of transforming organisations, and this is especially true for public administrations, there is a large gap between creatively setting strategic directions and goals and finding feasible assignments for implementing action plan projects. Most strategic changes must simultaneously include a substantial change in ICT support and leads to ICT construction projects or major changes in ICT solutions.

A completely justified need of the ICT unit in the role of technical administrator is to receive meaningful, correct, understandable and feasible terms of reference from the strategic and technical units (subject matter manager), see also the ex-ante approach Directing unified ICT solutions.

The means of bridging the gap between the chosen strategic direction and the feasible project brief is precisely the use of office architecture, in particular the development of an architectural vision and a complete individual office architecture and their application in the development of the OVS Information Concept and in the design of individual change plans.

Rules for the development of the architectural vision and the architecture of the office

Each public authority is obliged to create and maintain an individual model of the target state and planned transition states of its authority architecture in accordance with the rules of the National Architectural Framework and the ICCR as a prerequisite, starting point and part of its Information Concept.

The top and departmental level offices (see Ch 4.1.3) of the public administration are obliged to maintain an office architecture model to the extent that the office is obliged, empowered or able to directly or indirectly influence the subordinate organisations forming the public corporation together with it, whether in terms of budget, methodology, catchment, natural authority.

The NAR methodology prescribes authorities to develop individual models of their architecture in three levels of scope, as strategic, segmental and capability models of authority architecture.

The creation and maintenance of overall consistent authority architecture models is a continuous and iterative process, implementing changes in the architecture through individual specific tasks, architectural engagements[4)]. Typical architectural engagements will therefore be:

- architectural vision of the authority
- architecture for the update of the Authority's Information Concept,
- project architecture for the application to OHA,
- architecture for a feasibility assessment of a legislative change, etc.

Each architectural engagement successfully concludes with the approval of its deliverables by the Authority's Architectural Board and their acceptance by the sponsor.

The National Architectural Framework (NAR) document provides complete guidelines for the development of an architectural vision and complete individual OVS architecture. Further details and aids, especially on the different types of architectural engagements, are continuously updated in the Knowledge base.

=== Roles, processes and disciplines within the Architectural Change Authority ===.

The ability to create the maintenance and use of the Authority's architecture and its organization, should be ensured in each OVS, at least in two steps, with possible links to the architectural authorities and the roles of the parent corporation and the eGovernment CR.

In practice, this will mainly involve the division of responsibilities between the Authority's Architectural Office (AK), which together with the Authority's Design Office will be part of the Authority's management "staff", and the ICT Architecture Unit, integrated into the Authority's ICT Unit.

The Authority's Architecture Office, with the roles of Principal Architect and Domain Enterprise Architects, mainly provides the overall view of the Authority's architecture at the "enterprise" level of detail, the initial development of the strategic direction and support to the OVS Information Concept.

The ICT Architecture Office, on the other hand, is mainly responsible for the more detailed levels of executable architecture of individual solutions at the "Solution" and "Design" levels.

In the "Staff" AC, the roles of business architects are more needed, supporting the subject matter managers of the different segments of the office and their agencies in the development of business specifications, whereas in the IT Architecture Unit, the application, data and technology architects of the different platforms and solutions are more needed.

Of course, these recommended rules may have exceptions; for example, the ICT unit may temporarily substitute the competencies of the Principal and Domain Enterprise Architects.

In particular, the following processes should be defined to ensure the performance of architecture management:

- Architecture Change Management,
- Providing consultation and methodological support,
- Management of architectural standards,
- Architecture documentation management,
- Managing the repository of architectural models.

In order to distribute the responsibilities for the different components of the architecture, the architecture of an

organisation in terms of design, development and maintenance should be divided into several domains, mainly corresponding to the domains of the NAR metamodel, i.e.:

- motivational architectures, in particular strategic architecture and security architecture,
- vertical architectures of segments, agendas and capabilities and their information systems, through all layers
- horizontal architectures of the office: business architecture, application architecture, data architecture, technology architecture and network architecture
- cross-cutting architectures - the overall Enterprise architecture and its vision.

As such, the field of architecture is a subset of architecture, requiring similar specific qualifications and knowledge from the architects responsible. The role of the lead architect for the discipline is responsible for the design, management and development of the architectures in each discipline. The responsibilities and roles of these roles will be detailed in further annexes of the MŘICT in Knowledge base.

Principles, patterns and reference architectures - standards for architectural change

In the context of the above and described changes at the architectural level, it is necessary to define standards, in the form of so called architectural principles and architectural patterns and access to reference architectures, which commit the different roles and thus create an effective tool for a central unified coordination of architectural changes.

In general, the issue of principles, patterns and reference models can be viewed as follows:

- Architectural principles define the basic rules for the design of architecture in each discipline.
- Architectural patterns declaratively enumerate a list of standard and permitted technologies, their combinations and applications, methodologies and approaches to building solutions focused on specific domains and problems. The Architecture Patterns are a mandatory blueprint for the relevant parts of the Authority's architectures or individual solutions. The patterns are a reference for the architectural content.
- Architecture reference patterns represent a uniform classification in the model and the topology (location) of the elements of a domain or segment in the diagram. Reference models are the reference (reference) of order and form.

Architecture units are required to adopt national architectural principles, patterns, and reference models from NAP and NAR and apply them in their own individual models. They have the right to create their own sub-principles, patterns and reference models at the level of the whole authority or even the public corporation (department, region or municipality), as long as they do not conflict with the national ones.

It is desirable that both (state and own) principles, patterns and reference models are fully applied throughout the life cycle of individual ISVs and reflected in the standardisation and unification of architectures across the authority, including, for example, the promotion of individual standardised platforms in tender documents for the selection of suppliers under the HPAA.

Further substantive and technical additions, concerning architectural principles, patterns and reference models, will be included in subsequent editions of the NAR and NAP and updated in the Knowledge base after consultation with the professional community.

ICT Service Design by Solution Architecture and Service Management Toolkit

For the design and subsequent support of ICT services, and indeed services themselves, a combination of the systematic views of ITIL v5 and NAR (or TOGAF[5)]), or a combination of their methods.

ITIL is now the de facto standard for implementing IT service management and a collection of best practices

("best practices") in IT service management and the resulting recommendations. It offers a systematic approach to the discovery, planning, delivery and support of IT services (client VS, internal customer/key user) with the help of individual management. It covers the entire service lifecycle in the areas of Service Strategy, Service Design, Service Transition, Service Operation and Continuous Service Improvement. Managing services according to ITIL therefore means mainly setting up processes and preparing system support. Effective management of ICT services according to ITIL (SLM) and evaluation of their SLAs requires the existence of a so-called service runtime model or service tree.

In contrast, Enterprise Architecture is used to implement a formal description of the organization's architecture and its key elements and links. TOGAF or ADM (Architecture Development Method.) then introduces a systematic approach to managing the service architecture as such, including its changes. Within the service design and lifecycle, the EA model is created before the service tree and the model can therefore serve as a basis for the service tree design.

Currently, the problem of service design in relation to its management is trivial, i.e., there is a complete absence and neglect in most of them, or the sponsor is not even aware that SLA or OLA will be defined in the future. It is the concisely described visual model (architecture) of the service that can quickly and effectively improve the whole matter of service design and cover future risks associated with the design of measurement and support as such. The following assumptions are necessary for a functional model of the service design and in relation to its operation:

- the EA model is stored in the organization's architecture repository
- in the EA model, each application and service is represented by a single entity at the application layer, i.e. it is a kind of application prototype
- on the technology layer all instances are already modelled in accordance with the service tree

The combination of ITIL and Enterprise Architecture methods can then be used for:

- design and implementation of services according to ITIL in an organization,
- description of the service with a visual architectural model,
- decomposition and definition of key service interfaces and definition of indicators and measurements,
- a tool for quick impact analysis in case of any change within the service, change within the whole organization i.e. what impact the creation of a new service has on the whole ICT ecosystem.

The unifier and driver in both ITIL and NAR is change. In doing so, a distinction has to be made between so-called big and small changes in terms of the choice of a way forward. Large changes are those that go beyond the existing approved Authority Architecture, represent the creation of new objects, components and services and require the involvement of the Authority Architecture (EA) update process or its IK OVS. On the other hand, small changes are those that do not involve the existence of anything new, do not require a change in the Authority's architecture, but introduce some new quality of service. Therefore, it is more appropriate to divide changes into the modification of an existing ICT service and the creation of a new ICT service.

Central repository of OVS architecture models and working with it

An architecture repository can be a very effective tool for conceptual work across all ICT service changes. An architectural repository, like for example a program code repository, performs archival and operational functions. It is a supporting information system used to describe, centrally record, manage and share the architecture. At the level of the OVS (and/or its corporation - department, county, municipality), it is created to provide consistent, mutually compatible and linkable architecture descriptions and models.

A prerequisite is the creation and maintenance of a binding architecture design and documentation methodology based primarily on the NAR methodology and the IT architecture principles and standards from the NAP. Subsequent work with the repository is performed by any Architect role (external/internal). The Architect always verifies the existence of standards - principles, patterns, and reference architectures governing architecture design in the subject area in the Departmental Model Repository System before starting the

architecture design. If the Architect does not have direct access to the repository, he/she shall request from the repository administrator an export of architectural models, principles and reference architectures related to the given issue.

The repository should not only store individual models, but more importantly have a superstructure for rapid impact and difference analysis for large and small scale changes. This superstructure should find the necessary relationships and information about the stored objects simply (preferably in a tree structure) and using queries and expressions. The objects in the repository do not have to be only architectural, it is possible to store or integrate information from other sources such as HR (org. structure), ERP (financial and asset information), PPM (information about project portfolios and projects themselves), CMDB and service catalogue (information about services and infrastructure items), etc. The repository must allow to separate the views of the whole department and office (chief architect and other roles) from the views of solutions and services (their administrators and suppliers).

The architecture of the OVS or its department must be submitted to a central architectural repository, managed by the OHA MV, to the extent specified by NAR. A prerequisite for proper functioning is a properly defined integration interface and its configuration, with mandatory use of the international ArchiMate TOGAMEFF[6)] standard. Another important prerequisite is the methodology for creating the architecture of a given OVS and its department, which must fully adapt NAR standards and principles.

OVS Information Concept

The obligation to develop an information concept is imposed by Act No. 365/2000 Coll. on all OVS that manage ISVS. This Act and its "implementing" Decree 529/2006 Coll. specify both the content structure of the information concept of the OSS and the processes associated with it.

The methodological and knowledge base of the OSS IK is the individual model of the existing and target architecture of the office. The OVS Information Concept is the official (so-called deliverable) document for the results of the work of the office architecture.

Further factual and technical additions related to the development of the OVS Information Concept will be included in subsequent editions of the NAR and NAP, issued as OHA methodological guidance and updated in the Knowledge base after consultation with the professional community.

Other methods of strategic ICT management

Additional methods for strategic planning and management of the ICT Unit, in addition to the Office Architecture and the IK OVS, will be included in subsequent editions of the MIRCT and updated in the Knowledge base after consultation with the professional community.

Change Implementation Plan (Roadmap)

The roadmap of the necessary work packages (themes, plans, projects, programmes) leading to the realisation of the differences between the current and target architecture of the Authority, especially in the area of ICT support for all its activities, is the result of architectural work and project planning.

Formally, this plan is part of the mandatory OVS Information Concept and the basis for the management of transformational change in the OVS Project Office. However, it is also subject to sharing and central coordination with the (future) eGovernment Project Office.

Management of the identification and implementation of ICT changes in the OVS

Change management is crucial for the proper functioning of ICT services and the ICT unit. Change is a big driver that affects the whole ICT environment and the organisation itself. Managing expectations or requirements is fundamental. In the vast majority, it is the requirements that can be implemented in the form of change. As indicated above, change aligns the ITIL methodology, which manages more the operation and development of existing services, and TOGAF, which focuses on new services, or is even appropriate to use in combination with the ITIL approach for major changes within existing services.

All of the above processes need to be defined consistently, including roles and responsibilities. The good practices and elaborated methods of the approach of combining ITIL and TOGAF will be part of a detailed methodology that will elaborate this topic in more detail including templates and diagrams in Knowledge base.

Furthermore, the RFC and the IT architecture need to be put into context definitively and conceptually. The abbreviation RFC, derived from the English title "Request for change", represents a request for change in the Authority's environment. RFC in the context of architecture management is a request for change impacting one or more architectural domains.

Change management process represents, in the environment of an organisation, a standard process for receiving, processing, implementing and deploying change requests. A change management process in the context of architecture management is a change management process impacting architecture and/or requiring architectural input.

Collecting, evaluating, managing and classifying change requests

A requirement is the basis for the operation and development of ICT services. Standard and consistent management ensures the ICT service is of high quality and innovative. Requirements can arise in the following categories:

- Normal operation (infrastructure, end user, key user, etc.).
- As an output of ITIL processes in particular however Incident (including Security In.), Problem, Continuity and Availability management.
- SLM - steering committees and SLA negotiation meetings
- Client service (call center, satisfaction survey, etc.)

Idea management should be mentioned as an innovative process entering its requirements.

In public administration, in many cases other sources of requirements have to be taken into account:

- Legislation (laws and sub-laws, EU Community law)
- Political leaders (Government and its programme, Minister and political leadership of the OVS, party programme)
- Minutes of the meetings of the individual sections and of the meetings of a given OVS

As far as channels are concerned, the number of channels making requests should be kept to a minimum and, as far as possible, be under the control of one particular organisational unit.

The most common variant for handling requests is the ServiceDesk. The ICT unit should strive to use all available tools to force actors and processes to enter their requests here. This is the least demanding way of servicing requests in terms of organisation and resources. As mentioned above, a good level of request handling is the basis for increasing the quality of ICT services and the satisfaction of their clients and users.

Request handling is the next logical part. In general, it can be stated that the servicing and coordination of most

requests is handled, by definition, by the ServiceDesk (also referred to as "SD") or the HelpDesk function and the servicing roles of the SD. Both SD technical tools and ITIL best-practices can be fully leveraged in these activities. For project requirements, the PPM (Project Portfolio Management) tool can be used, and methodologically, industry best-practices such as PRINCE 2, etc.

In order to increase the transparency of the preparation of new services of the OVS and its department and to make the resulting solutions more efficient, it is advisable to use pilot projects when building new services, with the possibility of involving the expert public in the design and testing of solution concepts, thus verifying the need, suitability, functionalities and other aspects of the proposed solutions. This procedure provides users with the opportunity to test services and functionalities already at the time of their design, and at the same time the opportunity to comment on the form of 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 clients - citizens in mind, and any possible inconsistencies, contradictions or additional requirements/expectations of the VS clients are captured at the outset and incorporated into the solution concept of the newly developed service. Another indisputable benefit of the implementation of verification projects is the specification of the requirements for the target solution and expected functionalities. In the context of possible public procurement for the delivery of whole or parts of services, a precise set of clearly defined functionalities can already be requested. This minimises the risk of inefficiently requesting functionality that will not be used in the future and the risk of a large number of change requests for optimisation or customisation of the services used.

More detailed information, guides, procedures and tools will be issued as a separate methodological document and as a continuously updated part of the Knowledge base after consultation with the expert community.

Project and Programme Management Office

The IT of the Public Administration Office serves both its internal users for the execution of public administration agendas and external clients.

Therefore, even at the local government level, any public administration ICT projects, i.e. even support services (e.g. electronic filing service project or attendance records) should not be purely single-purpose, but should contribute to the objectives of the whole authority as part of the whole eGovernment.

All the Authority's projects, including IT projects, must be coordinated alongside budget planning and spending, at least in the following aspects:

- the contribution of the project to the achievement of the Authority's objectives - there must be an overview of which projects fulfil which objectives and vice versa, which objectives are fulfilled by which projects,
- common changes in the architecture of the Authority - time and functionally aligned implementation of changes to individual components of the architecture, with a clear preference for unification and use of common solutions,
- coordinated consumption of resources by individual projects, especially human resources - there must be a central overview of the Authority's staff allocated part-time to individual projects, both in terms of projects and in terms of individual staff capacity.
- coordinated use of the Authority's other physical and property resources, such as common areas, computing capacity, time available for downtime and outages, etc.

The coordination of projects, their linking to programmes and the management of project portfolios is a service of the Project Management Office (also known as "PMO"[7)]). It builds on the work of the strategic units and is supported by the knowledge services of the Authority's overall architecture unit, the Architectural Office (also referred to as "AK"). Both forms together should preferably be part of the so-called "staff" of the Authority's management.

At a second, lower level, already exclusively for ICT projects, this coordination and management takes place in the project management, strategy and IT architecture units within the ICT unit of the Authority.

Further factual and technical additions on the whole issue of project and programme management will be included in the next editions of the MŘICT and updated in the Knowledge base after consultation with the professional community.

Categorisation of programmes and projects

To facilitate the orientation and application of programme and project management methods, these should be categorised according to various factors:

According to the position and responsibility of the investor, in particular its place in the hierarchy of public administration:

- national projects, entrusted by the government to a single authority (supplied by the director)

According to the size or importance of the project

- strategic
- normal
- small

By impact and method of implementation

- Individual (central or local), always in a single office
- Fan-shaped (centre → territory)
- Gradual (Pilot/Roll-Out) spread of the same (type)
- Combined

Program 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 more value and with greater certainty than if they were managed separately.

Programmes of change can be identified both within an individual OVS and across multiple VS organisations. In this case, the programme definition must clearly identify which OSC will manage the programme.

While 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 not only project but also programme principles.

The basic seven principles of programme management[8)]) are:

- Be aligned with the Authority's strategy and with cross-departmental strategies
- Be a leader of change
- Communicate the desired better future state of the Authority
- Focus on the benefits and potential threats
- Deliver measurable value for change
- Design and build a cohesive (coherent) capability for the Authority
- Continuously learn from experience.

Change agendas can be identified both within an individual OVS and across multiple VS organisations. In this case, the programme definition must clearly identify which OVS will drive the programme.

All future change programmes, somehow related to IT, must be identified in the updated OVS IC. All funding

programmes under programme funding must have their antecedents in the relevant substantive change programme identified in the ICR; the formal creation of programmes for funding purposes only is not permitted under the ICR. At the same time, however, the budget financing rules must preserve sufficient room for flexible managerial decision-making to reallocate the allocated funds according to the changing conditions of the Authority and eGovernment (re-prioritisation).

All ODAs for which projects can be identified (see following chapters) that are interrelated and jointly contribute to the achievement of benefits need to put in place programme management processes, albeit to a practical minimum extent.

For supra-ministerial programmes, the establishment of an organisational structure by the Government is necessary, including the nominal designation of specific persons managerially responsible for programme management (programme director) and authorised to directly assign and require the performance of tasks by stakeholders from other ministries.

More information and rules on the management of IT development programmes, including links to programme funding, will be issued by the MoI in cooperation with the MoF in the form of the Methodology for the Management of IT Development Programmes, which will also include the basic structure of the programme.

Project portfolio management

Active management of one or more of the Authority's project portfolios is a means of making effective decisions about these projects in relation to each other and to the Authority's objectives and available resources. This is particularly important in a public administration IT environment where a number of projects seemingly or actually consume a lot of resources without delivering the expected benefits.

In the area of project human resource management, the Authority needs to lead a development plan for selected staff to become project resources, i.e. to be able to take responsibility for project leadership (including project managers on the client side), for specific roles in the project staff such as project architect, for leading project teams and for 'shadowing' key contractor specialists, i.e. for working independently on the project under the direction of the contractor and for taking on know-how within the project. This designation must necessarily be reflected in the job descriptions of the staff concerned.

A project which is unable to assemble project teams and fill the estimated required capacity of internal project staff from the available vacancies of the Authority's pool of qualified staff representing potential project resources (see mandatory internal filling of project roles) must not be started until the appropriately qualified resources are again available. Such a project would carry an unacceptably high risk of failure from the outset. On the other hand, the Authority's project resources must not be overstretched beyond the legal limits of the Staff Act and the Labour Code, forced to work in their spare time. This, in addition to the risks of error, leads to a permanent loss of these Authority resources in the long term.

In a situation where planned changes in the Authority and its ICT lead to more programmes and projects than the Authority's available financial, human and material resources, a process of 'project prioritisation' must be demonstrably applied. This should be done at least once a year, in the context of budget planning, or whenever concurrently running or planned projects hit the limits of the Authority's resources. The prioritisation process consists of allocating the available resources and allocating them only to projects that make the greatest contribution to the Authority's objectives or that are required by legislative changes. Projects that, due to their currently lower priority, do not reach the Authority's resources will not be started or will be stopped until their priorities are raised or the Authority's available project resources are increased. The process described above is the responsibility of the Authority's Project Office. The Project Office must be informed of all projects from the time pre-project preparation begins.

More information and rules on the management of IT project portfolios, including links to human resources management, will be issued by the MoI in the form of an update to the Methodology for the Management of IT Projects and Diverse Accelerators in Knowledge base.

Management of individual IT projects

The management of individual ICT projects, see in more detail Management of unified ICT solutions, must be centrally coordinated both from the perspective of the "small" project office of the ICT department, the PK of the authority and eventually from the perspective of the future central PK of the state or eGovernment, once it is established.

Implementing small changes - continuous improvement

In many cases this is done, but it is not recommended that the implementation of small or small changes is managed by the Change Manager. In the case of small changes, so-called coordination is preferable, where the execution is carried out by the Change Coordinator. In the case of simple coordination, a given change management role does not have as many formal documentation and management responsibilities as the Project Manager role, and in most cases coordinates multiple changes and reports more succinctly at the Operations Management level of operations in some cases this tends to be the Project Development level.

Change management will be added after discussion with the technical community and published in future issues of MŘICT and in Knowledge base.

IS Operations Management and Service Delivery

Managing support for clients and users of ICT services

The management of support to clients and users of ICT services will be completed after consultation with the professional community and published in future issues of the MŘICT and in Knowledge base.

ICT Operations Management

The required operational parameters of the requested systems and services should be defined as part of each OVS service operation unit and its department. Operational parameters mainly include service or system availability indicators for end users and response time indicators. Both types of parameters should be designed taking into account the importance of the services provided and the interfaces through which the services are provided. The values of the operational parameters should then be taken into account in the design of the architecture of the target solutions, in particular in the part of ensuring continuity and performance of the solution, and contractually supported in the service and information systems operating agreements (SLAs).

In the environment of OVS and its department, an approach to the definition of contractual parameters of services in so-called service data sheets should be gradually introduced. The basic idea of the approach is that services are provided through one or more interfaces and each interface is classified in terms of importance according to the categories "Gold", "Silver" and "Bronze". Shared catalogue sheets can then be created for each service category and application-specific services can be addressed within concise, dedicated catalogue sheets if required. This approach can be applied in the preparation of any contract with the character of delivery of operation and support services.

The management of ICT operations at the level of the whole Authority will be completed after consultation with the technical community and published in future editions of the MŘICT and in the Knowledge base.

Monitoring ICT Operations and Services

Each system, application or service must be designed and implemented in such a way that it can be integrated into the monitoring system of the OVS and the departmental organisation. The monitoring system must cover the metrics that are identified as automatically monitored in the Service Level Agreements (SLAs) and monitor these metrics in accordance with the procedures and parameters defined in the SLAs. In addition to the metrics so marked, the monitoring must monitor and evaluate other metrics common to the type of system or application.

Detailed methodologies and technical proposal regarding monitoring tools will be completed after discussion with the expert community and published in future issues of the MŘICT and in the Knowledge base.

Risk and Security Management in the ICT Unit

The main objective in the organisation and management of security in the Authority and its ICT Unit is to establish and use management processes to effectively enforce and control the security of information systems and technologies.

For Cyber Security and Risk Management, it is recommended to use the provisions of Act No. 181/2014 Coll. on Cyber Security (including the Decree) not only for systems falling under the purview of this Act, but also for other information systems, as this regulation sets out appropriate methods for managing cyber security.

Risk Management in the ICT Unit

Once an ICT unit is given a task that goes beyond the use of existing resources, it should at least conduct a risk analysis before starting to perform the task and create a risk map that - when properly completed - serves as a control for the entire management.

The risk map should also take into account risks from outside the scope that may cause the task to be suspended or cancelled. The main risk areas may include:

- cyber security
- Financial
- organisational
- political (taking into account possible political decisions affecting the task)
- Legislative area (consideration of potential changes in legislation and its interpretation affecting the accomplishment of the task)

The individual risks must be named and their relevance to the task must be justified. They must then be assessed to determine how they can be mitigated as part of the risk management process.

Each risk has an owner, i.e. a person or entity with the responsibility and authority to manage the risk and the actions that can be taken to mitigate or eliminate it. The level of action taken to mitigate risks should be consistent with the outcome of the risk assessment. However, in this respect it is important to note that achieving 100% elimination of all risks is not possible even with unlimited resources. It is therefore up to the management of the organisation to determine an acceptable level of risk and to provide the resources (not only financial, but also personnel, competence, etc.) necessary to achieve it.

A combination of technical and organisational measures is appropriate for optimum effectiveness of risk mitigation. Most risks must be considered before the actual implementation of the task or in the preparation of contractual documentation with suppliers.

In addition to risk management at the level of individual IS, their design, development and operation, see also Management of uniform ICT solutions, the focus of risk and security management lies on activities at the level of the entire office, implemented by the IT department in cooperation with other security structures of the office, such as physical security, GDPR officer, OHS, etc, See Collaboration with other Authority and eGovernment

entities.

The methodology issued by the NCIB, consisting of the main activities, can be used for cybersecurity risk assessment:

- Asset mapping and registration
- Risk analysis
- Risk management process
- Risk Management Plan,
- Risk assessment
- Controls and audits

It will be good to link this methodology with the risk management methods from the project standards (PMI, Prince2) and the TOGAF framework, together with financial risk management etc. so that they can all contribute together to a single register and process for managing all risks at authority level. MRICT supports in reducing or eliminating risks recommendations and guidance materials produced by NCIB:

- Minimum-Safety-Standard
- Security Standard for Videoconferencing
- Guidelines for impact assessment

Risk map type annexes including the legend, supporting questions and impact measurements, and other factual and technical additions will be published in future editions of the MRICT and in the Knowledge base after discussion with the expert community.

ICT Security Management

An essential part of the long-term sustainable operation and development of the ICT of a given OSS is the enforcement of cyber (information) security. For this purpose, each OSC must implement a stabilized information security management system according to the ZoKB and the ISO/IEC 27001:2013 standard. This system continues to ensure the security of the IS included in the ISMS through the operation and improvement of the information security management system. In addition, emphasis should be placed on greater involvement of the organisational units of the OSS in security activities, streamlining of surveillance and monitoring activities and deepening the security assurance of the OSS IS.

Operations and security are linked through several aspects. It is primarily availability, where security is as interested in system availability as operation. In many respects, information from monitoring tools can be used interchangeably.

The linking of the Service Catalogue and security assets seems to be very appropriate, where thanks to the link to another ITSM tool, i.e. the Configuration Database, risks can be projected onto individual items and thus the effects of e.g. outages on the organisation's assets can be seen very quickly. The linking can happen both at the service level - as its next attribute, or specific configuration items again at the attribute level.

There is also a tool for linking Incidents within a single ITSM tool, i.e. ServiceDesk. In this case, there is a symbiotic effect of servicing one Incident, where in the case of a Security Incident, there is only a change of category, where this change automatically assigns the resolution of the Incident to a different group of resolvers. It is appropriate here to take measures to ensure higher information security, both for the Incident and for the individual information generated within the solution. These measures are technical restrictions on the visibility of this information within the tool (specific roles in the security department see everything, others e.g. only SLA parameters and the solver).

Another pervasive issue is change and its handling. For example, security consumes the institute of standard and emergency change. Standard or so called pre-approved change significantly shortens the resolution of security Incidents, or their remediation exactly in the diction of the Incident, i.e. the highest priority solution leading to the rapid removal or elimination of the possible negative impact of the Incident (violation of integrity,

availability, confidentiality). It should be noted that a Security Incident is any event that leads or may lead to a breach of confidentiality, availability or integrity of information within the OVS and its department. A Security Incident is any violation of the general obligations outlined in the OVS Security Guidelines for which an exemption has not been granted. Events that may constitute a security incident and that affect the security of information may occur in the context of personnel, administrative, technical and physical security.

To ensure higher operability and availability, security monitoring technology called SIEM is deployed in the OVS. OVS should have not only a system for storing and standardizing security logs, but also advanced functionality i.e. log correlation. This system should have not only events from network elements and network, but mainly events from applications and services.

In the context of monitoring work, it is proposed to build the analogy of service trees (ITSM concept) in the context of security monitoring. Realistically, such trees are then built similarly (configuration database = asset database (or CMDB with security information) over security information. Both monitoring systems (operational and security) can then escalate their critical events (operational = fault, security = safety critical events) to each other. The last area of security monitoring in relation to IT operations is the access of privileged users to assets or technical nodes (devices) in a given organization's environment. This access is critical and its monitoring must be an area unique and closed to the OVS security department. Privileged user access must be escalated to OVS security monitoring and reported regularly, there must be no unwarranted privileged access to network equipment.

The inclusion of OVS security in the ICT department is not detrimental if critical and risky assets are fully under the audit and methodological supervision of the KB department. The advantages of a joint organisational assignment are:

- Jointly managing changes and projects or risk reduction activities on security assets.
- Shared budget.
- Sharing of analytical resources.
- Sharing project and coordination resources.
- Further substantive and technical additions will be included in future editions after discussion with the technical community.

IT Asset Management

Managing the overall service portfolio

To be added after discussion with the expert community and published in future editions of MŘICT and in Knowledge base.

Application Portfolio Management

To be added after consultation with the expert community and published in future issues of MŘICT and in Knowledge base.

Technology Portfolio Management

To be completed after consultation with the expert community and published in future issues of MŘICT and in Knowledge base.

Management of OVS Data Collections

To be completed after discussion with the expert community and published in future issues of MŘICT and in Knowledge base.

A different approach to the acquisition and management of ICT commodities

To be completed after consultation with the expert community and published in future editions of MŘICT and in Knowledge base.

Approach to indirect management and oversight of informatization (governance)

To be completed after consultation with the expert community and published in future editions of MŘICT and in Knowledge base.

Introduction of service quality management

To be completed after consultation with the expert community and published in future issues of MŘICT and in Knowledge base.

Reporting for ICT management and governance

To be added after discussion with the expert community and published in future issues of MŘICT and in Knowledge base.

ICT Controlling and Benchmarking

A methodology for calculating *total cost of ownership (TCO)* or, for externally operated ICT services, a de facto *total cost of use* methodology for ICT services has been developed for the evaluation of project plans, for comparing different ICT project solution options with each other, for monitoring and managing the service costs of currently operated ICT solutions and for other management purposes in the public administration of the Czech Republic.

The absolute amount of TCO and the derived (relative) indicators belong to the so-called Key Performance Indicators (KPIs) or form part of the calculation (Value Tree) of some aggregate KPIs.

Currently, TCO indicators are already applied or at least recommended for use in the following management areas within the Czech Government for the support of ICT management:

1. Analysis and cost comparison of existing information systems across the central government, i.e. **benchmarking** between chapters and central administrative offices.
2. Determining the **efficiency of investment** of multiple solution options for newly planned ICT projects.
3. **Economic performance** in the OHA's request for an opinion on an ICT project.
4. Comparing the cost of an existing ICT service solution with the cost of an ICT service solution through **eGovernment cloud**.
5. Development of **controlling** public administration ICT services.

Further information on ICT controlling and benchmarking will be discussed with the professional community and published in future issues of MŘICT and in Knowledge base.

Standardisation in ICT management

A comprehensive and challenging chapter on standardisation in ICT will be added after discussion with the professional community and published in future issues of MŘICT and in Knowledge base.

1)
(also referred to here somewhere as part of the so-called mandated resources.
2)
Act No. 134/2016 Coll. on public procurement.
3)
Configuration Management DataBase
4)
Engagement - unfortunately not a suitable fixed translation.
5)
The National Architecture Framework (NAR) was developed based on a combination of TOGAF 9.2 and ArchiMate 3.1.
6)
The OpenGroup ArchiMate Model Exchange File Format.
7)
In English Project Management Office - PMO.
8)
According to the MSP (Managing Successful Programmes) methodology, for example (Williams, 2004).