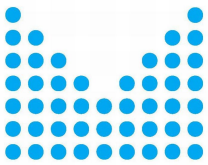
Materiál Ministerstva vnitra



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Export z Národní architektury eGovernmentu ČR

Obsah

Cooperation with other departments of the Authority and eGovernment

or **Links to related management disciplines and regulations.**

All OVS departments (including ICT itself) are existing or potential clients of the ICT service delivery unit. Working with them as clients is the most important form of inter-relationship, but this is described continuously in all other chapters of the document, not in this one.

This chapter deals with the other key interrelationships of the ICT unit with the professional and operational units in which:

1. The IT process can only be successfully executed in collaboration with these departments (economics, security and privacy, asset management, legal, HR, etc.); or
2. ICT experts have (or are to have) an important contribution to the execution of the processes of these departments (legislation, strategy, transformation - digital proxy, security, etc.).

Wherever any ICT management skill has an overlap with other office management disciplines, it is necessary to define the interfaces and focal points with ICT management in relation to these disciplines.

Similarly, wherever there is a need to respond to a new regulation or a new need in a cross-cutting way across an entire office or corporation, informatics will play a significant role, even if the management area or initiative is not primarily informatics.

Some areas of management and collaboration are already covered in separate chapters (project management, ICT economic management, ICT quality management, ICT human resource management, etc.). Others are covered here, either by brief general content, or by reference to separate materials, a summary of those materials, or the full content.

Primarily this applies in relation to ICT to the disciplines:

- collaborative care of the Authority's clients
- Collaboration in the development of strategies and legislation
- cooperation with the OVS Digital Commissioner
- ICT security management, where collaboration and competency interfaces are involved, in particular with:
    - Cybersecurity Manager (as per ZoKB) and
    - Data Protection Officer (under GDPR),
- business architecture management, modelling and management of the Authority's internal processes, i.e. active cooperation with the Authority's unit whose competence includes not only the management of the Authority's internal processes, but also e.g. data sharing,
- planning and financing ICT development (not only technology = infrastructure, but also staffing and information processes), i.e. cooperation with:
    - the finance department,
    - the Asset Management Department and
    - the HR department,
- the implementation of public procurement, both in the acquisition of technologies for assets and in the purchase of external services [1)]. In addition to administrative tasks, this requires a good knowledge of law - especially licensing law.

This chapter also includes the cooperation of the ICT unit with the relevant departments and bodies of the public corporation, if it is part of it, and with the central coordinating bodies, i.e. the Ministry of the Interior and the Government Plenipotentiary for IT and Digitalisation.

===== Support to the Authority's client services units.

Informatics will provide increasing support to the processes of delivering public services to its clients, particularly in the form of an increasing proportion of digital services. Already it is ICT services that are providing support to digital service clients.

However, in the framework of the digital transformation of authorities, new units should be created within them, which will take responsibility for common issues of client service and care, across the OVS agendas and across service channels, with an increasing share of universal service channels (CzechPOINT and PVS - Citizen Portal, or national call-centre). Such units are procedurally referred to by the English terms Front-End or Front-Office.

Part of their responsibility is to uniformly define, record, publish and promote the services of the office, especially the digital ones. In addition, they coordinate the delivery of these services by the professional services and uniformly commission and take over ICT support services to serve clients and evaluate their quality.

The role of the ICT Unit is to establish cooperation with the emerging Client Services (and Care) Unit and to find the first tangible common points in their relationship as the substantive and technical manager of the Authority's Front-Office service delivery solutions. Some of the first practical joint tasks are:

- managing the service catalogue across all service channels
- managing knowledge and providing support in all service channels, etc.

Integrated external ServiceDesk for digital services

An example of a practical collaboration with a customer care unit is a common, shared ServiceDesk for both digital and traditional service channels. The essence of the collaboration is that clients of the Authority's services, across all service channels, typically need support in two areas in particular:

- content - where and how to find the right services for life situations, what and how to fill in the submission, what and how to document attachments, etc.
- ICT - how to install and use self-service channel applications correctly, how to deal with errors or ignorance.

Best practice suggests that the authority should have, at least for its self-service clients, a single ServiceDesk, providing both knowledge base and staffing support in both of the above areas of concern. This requires joint coordinated management from both services.

Specifically, the ICT unit here acts both as the technical administrator of the shared solution and as a supplier of knowledge and capacity to support users in the technical aspects of the service.

Access to legislative support for the computerisation of SS

The further development of the computerisation of the SSR requires in particular the creation of new legislation and amendments to existing legislation so as to anticipate, enable and enforce the fulfilment of the architectural principles of eGovernment as set out in the ICCR, i.e. to be digitally friendly.

Since the vast majority of legislative changes involve or trigger changes in IT support for public administration, IT analysts and architects of authorities should be invited to the process of drafting amendments to agenda legislation already at the level of preparation of the legislative plan. Changes to legislation must take into account the logic, algorithmicity and parameterisation of legal regulations and the feasibility of their IT support in their wording and accompanying documents, especially by formulating a precise business specification for the corresponding IT support and a sufficient or gradually timed period for its implementation - the implementation period.

One of the irreplaceable tasks of the architecture of the authority (public administration) is to be the basis for the optimization of public administration and for the optimization of legislation. Architects and analysts must be involved in the process of developing theses and specific legislation, and in turn in the process of implementing new legislation in the authority. For more context on the involvement in the development of legislation in the Phase 2-Planning and Preparation stage of the single ISVS lifecycle, see also Management of unified ICT solutions.

It will also be essential for the further development of the computerisation of the SSR to unblock the obstacles erected by the existing legislation in the field of eGovernment, ICT procurement and in the management of ICT resources, especially human resources, see also the relationship between human resources management and the Civil Service.

It is important for the implementation of the ICCR that all new or significantly amended legislation is adapted to realistically implement the principles of the ICCR according to the benchmarks and control issues of the Digital Proper Legislation (DPL), for example at ria.vlada.cz)).

Digitally friendly legislation

The ICCR with its architectural principles and resulting rules is already harmoniously aligned with the Principles for the Creation of Digitally Friendly Legislation.

It follows that the consistent application of these Principles in the drafting of legislation, including its control by verification questions to fulfil the Principles, will significantly contribute to the implementation of the ICCR in the practice of the SSR.

Therefore, the ICCR and the MoICT lead the IT departments, i.e. the Technical Administrators of the ISVS of those offices responsible for both the preparation or commenting on legislation and the subsequent implementation of its ICT support, to:

- participate in the preparation of the substantive draft law or its amendment
- promote architectural and systems thinking as the logical basis for workable legislation
- require, as part of the terms of reference for building IT support for changes to legislation, answers to the control questions under the DPL from their respective Subject Matter Administrator from the initial plans.

One of the specific objectives (DC 4.2) of the ICCR is to establish the need to fulfil the DPL as a new obligation and an integral part of the legislative process.

IT security and data protection in the context of the Authority

IT as a systemic and holistic discipline in the Authority is a natural partner to similar and related disciplines such as Authority security, data protection, compliance, quality management, performance management and accountability.

For example, it is a well-established fact that almost all elements of the architecture of an office are simultaneously the object of protection, but also the means of protection and often a risk factor (information, technology, staff, buildings, activities, etc.). This applies to a significant extent to the elements of the Authority's architecture that are managed by the ICT Unit, i.e. primary and supporting assets.

Therefore, informatics and the office architecture method required for its strategic planning and management in the MIRCT can be very useful to the above disciplines in the office. This is because the office architecture progressively discovers, names and describes all the essential components of the structure and behaviour of the office and this knowledge is a key starting point for the work of the other disciplines. Conversely, the work of the specialised disciplines validates and complements the knowledge of the architecture of the Office and is therefore, at the very least, a very useful feedback loop.

The ICT Unit is obliged to establish a mutually beneficial open cooperation with the units responsible for the above disciplines. Some examples of cooperation are given in the following chapters, and further factual and technical additions will be included in future editions of the MŘICT and in the Knowledge base after discussion with the professional community.

The contribution of IT to the overall security of the Authority

The management of cyber risks and security of individual IS and the entire IT of the Authority must be carried out in line with the overall risk and security management of the Authority, so that the risks identified and the measures taken are part of consistent and overall processes and risk registers at the level of the whole Authority and, according to their severity, IT / cyber risks also become part of the decision-making and management of the whole Authority.

The adoption of the Cybersecurity Act has created an ideal environment for the development of ICT processes. It is the processes addressed through ICT that declare measurable savings, non-repudiation, irreversibility and many other inherent characteristics from the ICT world.

Unfortunately, these processes are not addressed comprehensively and every authority has processes with a good audit trail and processes that are without a trail. The emphasis on accountability for each area of responsibility within the defined roles under the Act has resulted in quality incremental development. However, this development is not usually accompanied by financial or organisational change. Each ICT unit respects the new rules, but at the same time tries to gradually delay each milestone as it waits for financial savings or staffing increases to implement the changes. This is what the implementation of the ICTC rules is meant to remedy, where all these contexts are already taken into account.

IT's contribution to data protection and GDPR

In the area of privacy and data protection management, all layers of the Authority's architecture and IT skills must be aligned with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, also referred to as "GDPR") and the existing Law No. 110/2019 Coll, on the processing of personal data and on amendments to certain laws, as amended, setting out the scope of personal data protection to be taken into account when creating information systems and designing systems for working with documents.

Although the primary responsibility for meeting the obligations of these regulations lies with the management of the office, the Data Protection Officer (DPO) and the subject matter administrators, the ICT unit plays an important role in analysing the status and needs of data protection, implementing IT measures, ensuring entry and exit points and respecting the various roles under the GDPR and their contractual relationships.

The GDPR regulation implies that the processing of personal data must be to the extent strictly necessary and proportionate to ensure network and information security, that is, the ability of a network or information system to withstand, at a given level of reliability, accidental events or unlawful or malicious acts that threaten the availability, authenticity, correctness and confidentiality of stored or transmitted personal data and the security of related services provided or accessed through these networks and systems. It is therefore the ICT's own responsibility to comply with these requirements.

Similar to the relationship between long-term ICT management responsibilities and cybersecurity responsibilities, in relation to GDPR and data protection, key roles need to be mapped to each other, aligning their responsibilities on the one hand and the key skills and capabilities required on the other. In particular, these roles are:

- administrator, joint administrators,
- processor,

- **trustee,**
- beneficiary,
- third party, etc.

For these roles, IT must provide or procure from suppliers the necessary IT expertise, while at the same time delegating to its suppliers, through contracts entered into by the IT department, a corresponding part of the obligations related to the stricter protection of personal data.

It is the role of the IT department as technical administrator to implement measures in all the information systems concerned to ensure the so-called mandatory requirements of the above-mentioned regulations. The formulation of specific precise requirements/implementation tasks for individual IS is the responsibility of their respective subject matter administrators in cooperation with the GDPR expert roles.

Information systems in which users handle personal data of natural persons must ensure consistent protection of such data against misuse. As a minimum security measure, it can be considered that there is a strict separation of user accounts in the system, password management, access logging, the ability to react to personnel changes in the ranks of users, setting access rights, etc. Measures must include:

- Logging to access personal data
- Encryption of personal data
- Pseudonymisation of personal data
- Anonymisation of personal data
- Functions for the exercise of the rights of subjects
- Searching personal data in the structure of databases and by hypertext.

The requirements leading to these measures, taken primarily from European legislation[2)], trigger the need to "kick-start" a new phase of development of the IS concerned with phases 1, 2 and 3. Similarly, when building a new solution, these mandated requirements must automatically be taken into account and appropriate measures included in the scope, design and roadmap of the solution, see also Architectural Principle P7 Trust and Security and the Privacy by Default and Privacy by Design principles included therein.

The role of the ICT unit is crucial at all stages of the lifecycle of design, construction, modification and operation of new or existing solutions. Personal data is only as secure as the environment in which the personal data is processed. Therefore, from an IT perspective, it is essential to adequately secure the following areas that have a primary impact on the environment in which personal data is processed:

- Technical security:
  - ICT technologies where personal data is processed (The actual solution where personal data is processed, including all the possibilities where input/output operations take place)
  - Supporting, global or shared ICT that are used to secure the operation of the solution itself (Backend, Frontend)
  - Means and techniques by which personal data is transferred outside the primary ICT or outside ICT entirely
  - Data storage media
- Contractual security
  - Contractual relationships with all product and service providers that come into contact with the environment referred to in the Technical Security section
- Processes:
  - Development
  - Change management
  - Operations

The ideal method of security from a GDPR perspective is a combination of technical-organisational and contractual measures. It is essential to understand that one type of protection is not sufficient.

Cooperation with other operational departments

Although the IT service is exceptional in many respects in terms of its capabilities and its contribution to the Authority, it is by its very nature an operational service unit, similar and related to all the others (HR, property management, economics, knowledge management, purchasing and others).

In the transition to service-based management of the Authority, it is up to the ICT service to understand what services it provides to and receives from these services. It is important to clarify the boundaries of the collaboration at which this exchange of mutual services takes place. The manager and the staff of the IT service should be well aware of what services they are entitled to request from their 'sister' services in these operational areas.

At the same time, all operational departments should be aware that their common and only clients are all the staff of the Office. Therefore, these departments should join forces, analyze what they already have in common and how they can further converge and unify to provide their services to employees in a unified, friendly and efficient way, including employee self-service, see Collaboration with other office and eGovernment departments on the involvement of operational departments in a common shared service centre for employees.

Practical best practice examples, guidelines, templates and other accelerators for ICT collaboration areas with operational departments, mentioned in the following chapters, will be added after discussion with the expert community and published in the next issues of MŘICT and in the Knowledge base.

Cooperation with economic services

The essence of the CIO's collaboration with economic departments is that while the CIO is responsible for budget planning, for payment of contractual obligations, for cost controlling of projects and individual solutions, and for other economic operations, he or she is not and is not supposed to be an expert in this area.

He/she will provide some of these tasks, especially in larger ICT departments, with his/her economically educated staff in the roles of economist, controller, etc., but is still entitled to request adequate support with the services of economic professionals from the relevant departments.

An example of the difficulties in cooperation is the process of financing development projects. The basic problem with this process is the time that elapses between the business plan and the signing of the contract. For a new law or a comprehensive amendment to it, this involves years of work that do not impact the budget, but often it is this funding that appears in the budget. Conversely, sometimes an RIA does not have a financial burden because the change is happening in another agency. The principle of a good setup is the availability of funds that are needed to manage change. An ICT department should not have to deal with the availability of funds to run its ICT after it has been approved. The economic unit must have the right input from the ICT unit to address availability at the level of the overall budget, and the ICT unit must regularly communicate relevant changes.

Cooperation with Human Resources

The essence of the CIO's collaboration with HR departments is his need to attract, retain and intensively train his professional staff.

HR work is a natural part of any manager's job, but the ICT manager is not supposed to be such an expert at it either. He has every right to ask HR departments for support in recruiting new employees, preparing employee benefits and incentives, preparing and implementing training programs, evaluating employees and planning their further growth, etc. He has a legitimate expectation that he will receive, in particular, HR and HR-legal advice with regard to the Staff Act, the Labour Code and other regulations.

Cooperation on public procurement

The essence of the CIO's collaboration with the Legal and Procurement Units is his legitimate needs to safely, i.e. legally, manage the process of selecting a contractor under the PPL without resigning to the substantive, professional nature of the contract.

Every public procurement has at least two main aspects. The first is the need of the purchaser - they must "know what they want". It is the role of the ICT unit as the technical administrator procuring the solution for the subject matter manager to deliver a correct and understandable specification to the contract, i.e. the architecture of the solution, its functional and non-functional specification, including SLAs, part of the contractual requirements and other attributes associated with its usual role as the principal of the operation.

He rightly expects the service from the legal and procurement experts to embed impeccable process knowledge and the other part of the contract terms and conditions into the contract, which then ensures a contractual relationship with the supplier for the CIO, representing a balanced partnership[3)].

A common example of difficulties is the lack of mutual knowledge and the ever changing environment. Just as the guarantor of an asset needs practice for their role, so do those in charge of procurement need practice and, above all, compliance with anti-corruption rules. Leakage of information prior to tendering can be significantly reduced by pre-market consultations, and the procurement process itself can often be resolved by a negotiated procedure with publication, which allows access to all suppliers and minimises the amount of additional information.

Another huge impact of the interpretation of the PPLA from previous years is the 4-year operation services, where already last year many law firms have challenged ICT departments to take longer. If the contracting authority keeps ownership of the source code with them and competes development, then there is nothing to prevent long term maintenance. The possibility of defining longer times within procurement to reflect standard practice where, for example, normal SW/HW maintenance (Maintenance) times tend to be offered at 3, 5 or 10 years should be discussed in future revisions of the Act.

Working with Property Management

The essence of cooperation with property management and maintenance is twofold:

1. The need for the ICT unit to use specific premises and associated services.
2. Significant similarity in service delivery processes for staff in the care of ICT terminal equipment and in the care of other work equipment, in addition often with the need for time synchronisation of services, both often linked to HR services (on-boarding, moving, employee departure).

The first point of cooperation should lead to the provision of property management services with SLAs similar to those associated with the delivery of services to the ICT unit's clients.

The second point of cooperation should lead to joint coordination of services provided, shared methods, procedures, tools and dispatching staff for both categories of services, with the possibility of extending to a shared operations service centre, see below.

Joint involvement in a shared services centre for staff

The common clients of operational services are the employees and managers of the Authority, all of whom have a need to draw from these universal roles to provide a set of operational services for employees, and some to add to that a set of services for managers.

Their common need is to draw on these services easily, uniformly, through the service channel of their choice, i.e. in person, in the clerk's portal or in the service dispatch call centre.

The ICT unit will play a significant role in such a shared service centre and should therefore validate such a need in their office and then facilitate the process and digital transformation of the office in the operational area by initiating and building such a shared service centre.

The long-term trend for public administration in the Czech Republic is to federate such centres with the possibility of combining local services with shared services at the corporate (departmental, regional or municipal) level and shared operational services at the national level (e.g. eLearnig).

Central Coordination of State ICT Management

As the centralization of the management of the Czech Republic's State Administration is established by law[4)]), eGovernment, which is actually VS performed in a digital (cyber) environment, must also be centrally managed. This means that the ICT departments of the authorities are obliged to follow and comply with the centrally issued documents for the field of ICT in the field of ICT in government, not only in the operation, but also in the design of the development of ICT support services (both internal and external) provided by them for the performance of government services.

That the necessity of building central competences is also perceived by the Government of the Czech Republic is also evidenced by the main objective No. 5 of the CS programme, pillar IKČR - Efficient and centrally coordinated ICT public administration, specifically sub-objective No. 5.2 - Allocation of adequate human and financial resources for the implementation of IK ČR.

In the following chapters, a set of practical recommendations for managers of ICT departments on how to implement successful cooperation with central coordination bodies will be presented in the next issues of the ICTC, after discussion with the expert community.

More detailed information, guides and other tools will be continuously updated in the Knowledge base.

Economic Coordination

In a situation of difficult or even de facto non-enforcement of even legal obligations, the only effective management tool is the central control of the state budget spending, starting from the stage of financial planning and reconciliation of appropriations to the ICT chapter, on the one hand, according to the necessity to ensure operations and, on the other hand, according to the compliance with the ICR and the contribution of individual actions/projects to the implementation of the state-prioritized strategic objectives.

Programme funding

More information and the necessary accelerators to centrally coordinate ICT programmatic funding will be published in future issues of the MCICT after discussion with the technical community; more detailed information, guides and other tools will be contained in Knowledge base.

Logical framework methodology

The Logical Framework (LR, LogFrame, Logical Framework Matrix - LRM) is used as an aid in establishing the basic parameters of a project. It is part of a project design and management methodology referred to as the Logical Framwork Approach (LFA), which comprehensively addresses project preparation, design, implementation and evaluation.

Metodika logického rámce[5)]), developed by the MLSA for the European Social Fund under the Operational Programme Employment, is a proven tool for preparing an application for action registration and obtaining an

EU contribution and, based on the positive experience of the MLSA, it will be appropriate to use it for all eGovernment projects in phases 1 and 2 of their life cycle.

The logical framework identifies the objectives, benefits and outputs of the respective project, as well as the links between them. At the same time, the logical framework also contains objectively verifiable indicators and sources to verify them, which will enable the degree of achievement of the project's objectives and benefits to be determined.

More information and the necessary accelerators to the LRM will be contained in Knowledge base.

=== Investment Plan, CBA and Feasibility Study ===.

According to the current procedures, the key document for the state budget disbursement is the Investment Plan. Based on the approved budget and the funds allocated in the Authority's chapter book, it is prepared and submitted by the Authority for registration with the Ministry of Finance.

The funding requirements for VS ICT projects should always include evidence that an option has been selected:

- feasible,
- the best value for money, in terms of:

- cybersecurity,
- user-friendliness - both for the civil public and commercial entities, and for VS officials,
- usability of both the existing ICT infrastructure and the knowledge and skills of internal staff,
- long-term sustainability.

More information and necessary accelerators on Investment Plans, CBAs and Feasibility Studies will be provided in Knowledge base.

Coordinating Change Implementation and Achieving Benefits

The implementation of change takes the form of projects or programmes, for which there are a number of appropriate methodologies. From the point of view of eGovernment projects, it seems essential to coordinate them with each other, to link them to the eGovernment strategy and, last but not least, to measure the success of the implementation of the change (project/programme).

For this purpose, the logical framework methodology described above is the most appropriate, which both defines the objectives and benefits of the implemented changes and, more importantly, determines the degree of their achievement. The project logical framework should become a compulsory part of the Central Catalogue of Projects mentioned in the following chapter and should also be part of the final evaluation of the project or programme. In addition to the degree of achievement of the project's objectives and benefits, the final evaluation should include an analysis of positive experiences and, in particular, if the project has not achieved its objectives, an analysis of the reasons for failure.

The findings of the final analysis should be made available to other ODAs for use in optimising their projects, but in particular to the central Project, Programme and Portfolio Office (P3O), which will use these findings to further improve the project, programme and portfolio preparation and management processes.

It will be appropriate to implement central management also in the context of programme and portfolio management, and it is clear that, especially in the area of programme and portfolio management, cooperation between the different actors of the VS, both their IT organisations and their professional units, is necessary. A central Project, Programme, Portfolio Office (P3O), based on the PRINCE 2, MSP and MoP methodologies, will have to be implemented for coordination and management of programmes and portfolios, probably as part of the MoCR. This office must be staffed by certified experts with sufficient authority to deal with the various actors of the MoS and their organisational units at all levels of management.

Central catalogue of plans and projects

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

Licence Management and OSS/FS

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

1)
In the broader sense of ICT services, i.e. not just "mere" support / maintenance (e.g.: software updates), but also DaaS, cloud services (e.g.: SaaS, IaaS, PaaS, DPaaS), etc.
2)
GDPR
3)
In English, it would be Win/win, i.e. approximately, both parties are winners.
4)
Act No. 2/1969 Coll. - Act of the Czech National Council on the Establishment of Ministries and Other Central Bodies of State Administration of the Czech Socialist Republic
5)
https:%%//%%www.esfcr.cz/documents/21802/782328/02_Metodika_logickeho_ramce.pdf/b840b4ad-5d37-44c4-ade4-70f663f8047f