Funded by the European Union

Ministry of Public Administration, Digital Society and Media

UNDP

ASSESSMENT OF THE DIGITAL GOVERNANCE FRAMEWORK IN MONTENEGRO

Internal IT systems analysis

Note:

The Internal IT systems analysis was conducted within the project "E-services and digital infrastructure as a response to Covid-19" funded by the European Union, implemented by UNDP in cooperation with the Ministry of Public Administration, Digital Society and Media. The content of this Analysis is the sole responsibility of the author and does not necessarily reflect the views of the donors.

Contents

List of Acronyms	
PDC	Primary Data Center
DRS	Disaster Recovery Site (Disaster Recovery Site)
SPA	State Property Administration
UPS	Uninterruptable power supply
OS	Operating system
IaaS	Infrastructure as a service
PaaS	Platform as a service
SaaS	Software as a service
eID	Electronic identification
eDMS	Electronic document management system
AI	Artificial Intelligence
ML	Machine Learning
DMZ	Demilitarized zone

I ANALYSIS OF INFORMATION INFRASTRUCTURE IN THE PRIMARY DATA CENTER AND DRS

1 Introduction

Due to the crisis caused by the outbreak of the COVID-19 and its far-reaching impact, governments around the world have been adopting various measures to effectively combat the effects of the pandemic. Due to measures of social distancing and travel restrictions, both citizens and business organizations have experienced difficulties in accessing public services and obtaining timely information regarding their requests. The crisis has highlighted the importance of technology and the vital role of efficient, inclusive and accountable government. In this regard, the digital transformation of public administrations becomes a central issue in improving the provision of government services, both at the local and national levels.

The foundation of every IT system lies in its IT infrastructure, which is expected to allow for uninterrupted and continuous execution of IT services, provide adequate capacity and redundancy, as well as to secure the continuity of IT services in case of major incidents. Therefore, when building new or analyzing existing IT services, it is obligatory to review the "foundations" of the IT system itself, starting with the primary Data Center (PDC,) and Disaster Recovery Center (DRS) with all associated systems. After that, it is necessary to review the basic IT network and server infrastructures and communication links, which are expected to support said IT services.

1.1 Scope

Given the complexity of software systems providing public e-services and the constant need for their upgrade, maintenance, efficiency, and availability, there is a need for a very stable and reliable Data Center and IT infrastructure. To ensure that no disruption to the provision of e-services occurs in the event of a disaster, a stable and reliable backup DRS location must be provided featuring functioning IT systems, replications, and recovery procedures that are tested regularly.

Visits, interviews and data provided by the Ministry of Public Administration, Digital Society and Media resulted in a comprehensive analysis of hardware IT infrastructure presented below. The main focus of the analysis was as follows:

- Analysis of the existing Primary Data Center (PDC), including conclusions and guidelines for its further development;

- Analysis of the existing Disaster Recovery Site (DRS) to serve as a disaster recovery center, including conclusions and guidelines for its further development;
- Analysis of existing hardware and infrastructure supporting joint national systems, including conclusions and guidelines for their further development.

1.2 Limitations

Given the rather short deadlines, very limited information was obtained on the current PDC and DRS centers and the overall IT infrastructure. Documents and data received were duly analyzed and served as the basis for the preparation of this report, recommendations and guidelines for further development.

IT infrastructure was reviewed at the level of IT architecture – no detailed analysis was done in the domain of software solutions, versions and levels of functionality, nor at the level of IT security. The risks and limitations pertaining to the information obtained, and even more so to the information that remained unavailable during the preparation of this report, are high and may have implications for the decision-making processes relevant to this issue.

AUTHOR'S NOTE: Certain successes in the implementation and maintenance of the analyzed systems of the competent Ministry are evident, but the overall analysis is based on comparison with relevant standards and practices, which resulted in highlighting identified. This analysis should not demotivate employees but rather serve as an indication of existing risks and a source of recommendations for further work. The analysis does not indicate previous wrong decisions, nor does it affirm previous good decisions, as they were not considered in the given circumstances and treated as such. In addition, if there are statements in this analysis that are not adequate or properly interpreted, the author offers to provide all adequate interpretations and clarify on the basis of which information the conclusions presented below are made.

1.3 Assessment framework and methodology

At the level of the concept model and given the limitations, the overall evaluation approach focused on the information provided, visits to PDC and DRS centers, as well as orally communicated information collected on that occasion. Prior to engagement, a detailed questionnaire was sent to the competent ministry, which means that the evaluation methodology should be based on indicators for each question. However, in this particular case, this was not achieved because a number of questions were not answered directly. At the same time, most of the responses were based on comments, although many of the indicators from that questionnaire could serve as a measure of success.
To provide a complete and detailed analysis, standard and complete data collection should be used – such as surveys, questionnaires, interviews, observations, site visits and, finally, a review of updated

and complete documentation. In this case, the key data sources were incomplete documentation and visits to the PDC and DRS centers.

In the analysis itself, PDC and DRS centers were analyzed based on ANSI/TIA-942-B standards, while overall hardware and IT infrastructure was analyzed based on corporate IT standards and best practices, including ITIL, COBIT, ANSI, ITU and ISO.

2 Analysis

As already mentioned, the scope of the analysis and the focus of this report are:

- Analysis of the existing Primary Data Center (PDC),
- Analysis of the existing Disaster Recovery Center (DRS), and
- Analysis of the existing IT infrastructure supporting joint national systems.

The globally adopted ANSI / TIA-942 Telecommunications Infrastructure Standard for Data Centers provides for the minimum requirements and guidelines for the design and installation of Data Centers used in this analysis. The TIA-942 standard covers all aspects of Data Center's physical infrastructure, including:

- Location and construction works
- Electrical design
- Network architecture
- Mechanical systems
- Redundancy system for electrical, mechanical and telecommunication networks
- Fire safety
- Physical security
- Efficiency

The key objective of the TIA-942 standard is to define how the Data Center should be constructed and configured to provide the level of reliability and scalability required by its end-users.

Four ratings provide an unbiased way for Data Center owners and users to define their expectations depending on the applications and data stored in a particular Data Center:

- Tier-1: Basic IT Infrastructure – in brief: Data Center has non-redundant components and very limited protection against physical events.
- Tier-2: Primary IT infrastructure – in brief: IT infrastructure has redundant core components but no redundant distribution path serving the equipment. It has limited protection against physical events.
- Tier-3: Advanced IT Infrastructure – in brief: An IT infrastructure with redundant components and concurrently maintainable distribution channels serving the computing equipment. It is protected against most physical events.
- Tier-4: Fault-tolerant infrastructure – in brief: Data Center has redundant components and capacities, as well as active redundant distribution paths for equipment maintenance. It has protection against almost all physical events.

The Primary Data Center (PDC) represents the basic foundation of the overall IT infrastructure. In contrast, the Disaster Recovery Site (DRS) represents the foundation of business continuity. Quite often, Data Centers are a neglected part of the infrastructure. Usually, they are the weakest link as well as the cause of most system outages, especially if they are not managed properly. The present analysis treats both Data Centers (PDC and DRS) separately and in accordance with their primary functions.

The term ***IT infrastructure*** is defined in ITIL[1] as a combined set of hardware, software, networks and facilities (including all of the information technology-related equipment) used to develop, test, deliver, monitor, control or support IT services. IT infrastructure allows an organization to deliver IT solutions and services to employees, partners and/or clients. The infrastructure consists of the following components:

- Hardware: servers, computers, storage, firewalls, routers, switches and other hardware components, even Data Center hardware.
- Software: operating systems, databases, applications, ERPs, productivity applications, infrastructure software, etc.
- Network: network and Internet connectivity, firewall solutions, and security. Including path selection, routing and protection, as well as their operating systems.
- Data Centers: Server rooms and data centers. This often neglected part of the infrastructure is usually the weakest link and the cause of most system outages if not managed properly.
- People: According to the ITIL's strict definition, people are not considered part of the IT infrastructure. However, without competent and properly-qualified people in charge of managing and maintaining IT infrastructure, the capabilities of an IT organization can be significantly reduced.

The present analysis reviews the IT infrastructure at the IT architectural level. When it comes to Data Centers and IT infrastructure, all the above components are covered to a very basic extent, according to the identified risks.

[1] ITIL (Information Technology Infrastructure Library) is a set of ITSM (IT Service Management) practices for creating, improving and delivering IT operations and services, designed to standardize procedures for quality IT management. As such, it is used by some of the most prominent organizations in the world, including HSBC, IBM, NASA and others.

2.1 Primary Data Center (PDC)

As already stated, the key objective of the ANSI/TIA-942 standard is to define how the Data Center should be built and configured so that it provides the level of reliability and scalability needed by its end users. Preliminarily, according to this standard, the Primary Data Center (PDC) could probably be classified somewhere between Tier-1 and Tier-2 because it has individual components that are redundant, but not all of them. At the same time, it has limited protection against physical events, and there are identified key environmental risks. This assessment is rather inadequate for the Data Center that should enable uninterrupted and continuous operation of entire IT services pertaining to public administration. As such, it generates a risk that should not be acceptable to the Ministry and public administration as a whole.
According to the above standard, all aspects of the physical infrastructure of the Data Center were analyzed in detail:

2.1.1 PDC – Location and construction works

The Primary Data Center (PDC) of the Ministry of Public Administration, Digital Society and Media is located on the business premises of the Ministry, i.e., in the basement of the building. The space in question was primarily conceived as a server room for the needs of the Ministry. However, over time, it has grown into a Data Center that serves various IT services of public administration while retaining its fundamental advantages and risks, which were not adequately considered at the time.

The location itself does not meet the basic prerequisites for the construction of a Data Center, given that it is located deep in the business district, with rather limited opportunities for access, entry, servicing and replacement of equipment, significant risks of floods, fires and security threats that can paralyze the work of the Primary Data Center (PDC) partially or entirely. Said risks do not necessarily have to be manifested in the Data Center itself, but also in the facility itself or its immediate surroundings, but they could easily be transferred to the premises of the Data Center. The entrance to the Data Center is possible from the office building but also from the common area of underground parking (only one wall separates the PDC from these rooms), which can be used to bring the equipment in (of limited size, though, because not even a smaller truck can enter the underground garage). This also generates additional risks, bearing in mind that it is used by a large number of people and that it is relatively easily accessed.

Image 1. PDC location, in the very heart of the business district

During the construction, local standards for the construction of the business and residential facilities were followed, but not the standards for the construction of the Data Center, bearing in mind that its placement in the building was not planned at that time. In connection with this, the competent Ministry has made continuous efforts to mitigate the identified risks by upgrading the premises of the former server room. However, these efforts could not be completely successful due to the initial limitations of the location and the facility. Although significant funds and resources have been invested, the risks have been mitigated, but not to the extent necessary. Existing walls and constructions were used, security doors were installed, while there is no raised floor as one of the basic protection elements, although the floors are made of electrostatic material with connected grounding.

The walls have not been treated adequately. At the same time, the existence of plumbing installations in the immediate vicinity generates additional risks, in addition to the existing risks of flooding in the office building itself. In addition, it is important to point out that all of the construction improvements were carried out in parallel with the active operation of the Data Center, which posed an additional risk for the continuous operation of IT systems in it.

Image 2. Entrance to the Primary Data Center from the business offices and garage

2.1.2 PDC – Electrical design

The facility in which the PDC is located was not adequately designed and allocated sufficient surface area as it was not planned to be used as the Data Center, so subsequent works tried to improve the identified shortcomings. The office building, including the Data Center, was reconstructed in 2020/2021 in the context of the Energy Efficiency project. The Data Center is supplied from a single branch of the low voltage network through the 160kWA aggregate system, which comprises a redundancy for the Data Center but also for a part of the building itself, which is not in accordance with the required standards. The unit is maintained and supervised by another competent institution (State Property Administration). The Ministry staff does not have insight into its regularity or the agreement on the level of service support. However, there were problems with aggregate field failure in the past due to poor maintenance or lack of fuel in the generator unit. Following the assessment of the risks in question, the project of reconstruction of the building led to improvements in this segment. The monitoring system of the Data Center's immediate environment was also improved. The level of risk was mitigated but not reduced to the required possible minimums. As for the Data Center itself, most rack cabinets have separate UPS devices of different exploitation ages and current status. The UPS devices are not adequately monitored. The remaining equipment is connected to the central UPS system installed in 2020/2021. It supplies the main rack cabinets of the Ministry itself. The implementation of the new NN installation distribution within the Data Center was observed. However, it was not observed that many rack cabinets were still adequately connected to it. There is a detailed documentation of performed works and diagrams/schemes of new electrical installations. However, there is no projected total and measured current power, in total and by segments, nor there is information on total heat emission needs.

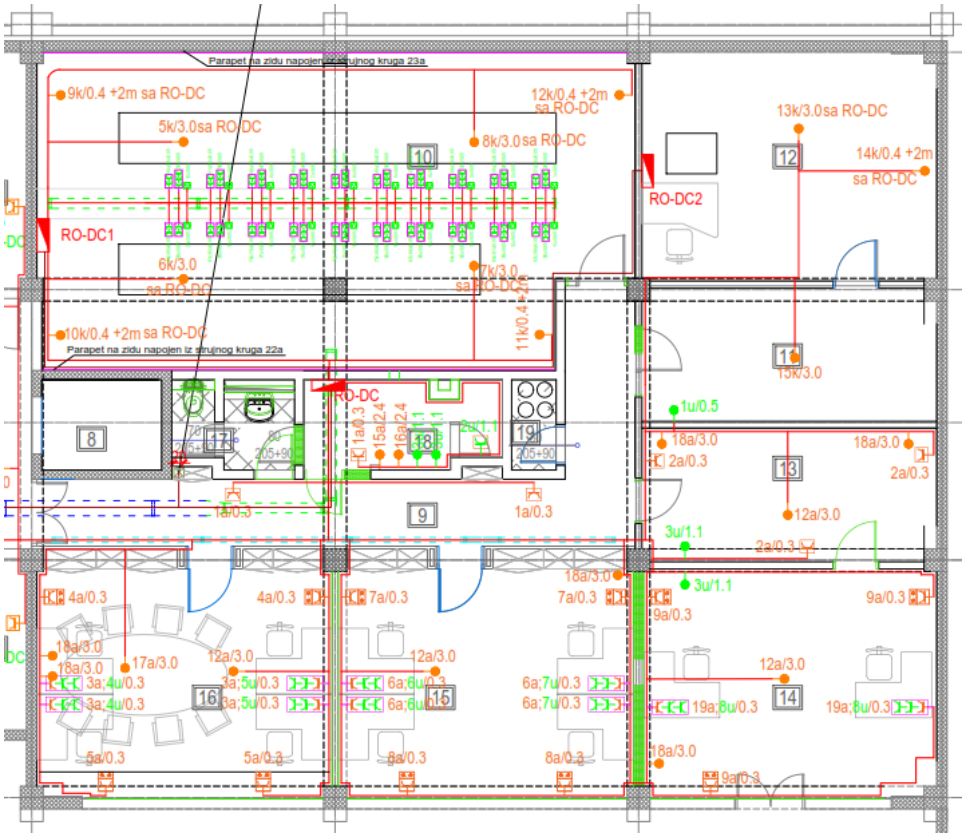

Image 3. The main electrical wiring diagram of the DC room

2.1.3 PDC – Network Architecture

Passive network architecture has not been adequately planned or implemented, which makes interventions or new implementations quite risky and inadequate. It was observed that there was a plan for passive network equipment optimization with simultaneous optimization of active network equipment that is underway and whose activity is related to the process of migration of server infrastructure. Scalability is limited by the surface area of the Data Center itself.

Image 4. One row of rack cabinets in the Data Center

WAN links have been established through two telecom providers (Telekom and Telenor) via BGP protocol using Cisco routers, backed by Checkpoint and Edge firewall, while the server segment was isolated by Juniper server firewalls. The Internet connection occurs through two telecom providers (Telekom and Telenor) via BGP protocol with assigned band 2C class ipv4 IP addresses owned by the Ministry. Also, there is an additional Internet connection provided by Telekom that is available without BGP protocol, where Telecom IP addresses (3 C class) are rented and used, provided that this connection is implemented through the same physical optical fibers as the ones mentioned. Both connections with both Telekom and Telenor are established through redundant optical fibers with different paths and routes from their Data Center.

WAN links are established via Orion Telekom (wireless) and via Telekom (optical) direct and MPLS connections. There are no redundant paths to the Data Center per provider for these connections. Redundancy is established at the level of the providers/technologies they use.

The access by most institutions takes place through the MPLS network, which is aggregated locally and terminated on the core switch system. This design is at an acceptable level, with the limitation that the configuration of the system itself, which is not the subject of this analysis, has not been adequately considered.

Image 5. Passive network installations in the Data Center

2.1.4 PDC - Thermo-technical and mechanical systems

In the context of the recent reconstruction, the Ministry has installed additional redundant air conditioners that keep the temperature at an adequate level. However, it was not observed in the documentation submitted whether the humidity of the air in the room is maintained in the same way, which can cause significant problems in the operation of the devices. Also, the lack of designated cold and hot aisles and the lack of raised floor resulted in the need for inadequate and inefficient air conditioning in the entire Data Center room. Temperature is monitored via the SMS alert/notification system. The existence of previously created alerts that were not adequately treated was noticed in the system (ACK). There is a ventilation system in the room, which is probably used for additional emergency ventilation in case of severe failure, but the adequacy of air exchange in DC rooms has not been confirmed.

Image 6. Thermo-technical and mechanical systems in the Data Center

2.1.5 PDC – Redundancy system for electrical, mechanical and telecommunication networks

Although there is a basis for the redundancy of the power supply system at first glance, the complete Data Center is powered by a single transformer station, which supplies power to the majority of other consumers in the area. The paths of power cables to and within the Data Center are not redundant. The same applies to the power and UPS power system. There are no two independent branches of electrical power, so the risks are reduced by using rack mountable UPS devices. The air conditioning system is redundant, although energy-inefficient, while no redundancy has been observed when it comes to the air-ventilation system. The degree of protection from external influences has not been determined.

The telecommunications WAN is redundant at the level of the telecom provider but probably not at the level of the technologies used or the path of the passive network that leads to and exists within the Data Center.

2.1.6 PDC – Fire safety

A NOVEC gas fire-safety system, which is not adequately managed, has been implemented in the Data Center room. Fire safety doors have been installed in the existing premises, while the walls and ceilings have been adequately treated in terms of protection from fire. Fire sensors have been installed and connected to the central alarm and control unit. However, data on testing and maintenance of this system remained unavailable at the time of compiling this report. In addition to this, certain system alarms and warnings, which were not adequately treated, were observed.

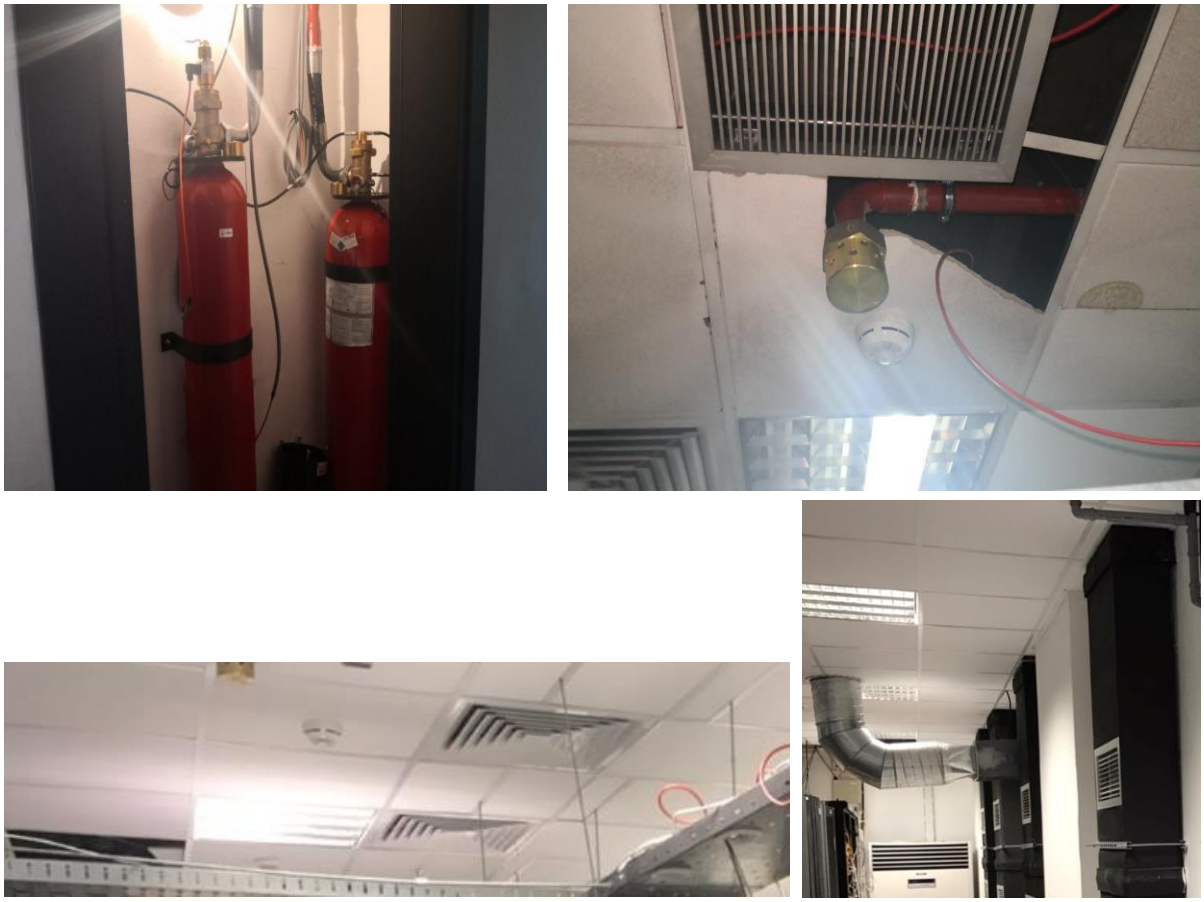

Image 7. Fire safety system and emergency ventilation

2.1.7 PDC – Physical Security

Despite the existence of security doors, video surveillance systems and physical security forces inside the office building, the security system is not at an adequate level. At a relatively short distance from the entrance to the Data Center, there is a door to the underground parking, which can be accessed relatively easily and without control. The access control system has been implemented, but certain illogicalities have been observed in the domain of granting rights and privileges to access certain premises. In addition, the malfunction of certain devices has also been noted.

In line with the established procedure, the control of the entrance to these premises is performed by the Directorate for Infrastructure and Information Security employees. Entrance to the Data Center's premises is limited in relation to the work performed by employees. The entry of any of the partners is not possible without advance notice, logging, and the presence of the Ministry employees. Each entry to the Data Center is recorded in the access control system and video surveillance. It is not recorded who is tasked with periodic supervision of this process and the supervision of external partners who access them together with the ministry's staff.

2.1.8 PDC – Efficiency

Although planned, a centralized Data Center monitoring system has not yet been established. Certain alarms and warnings were observed within the Data Center environment systems themselves. However, these are not treated adequately. Officials from the Ministry state that there are internal procedures related to monitoring the work of the Data Center, but it was evident that a number of systems have been implemented and maintained by authorities that are not under the jurisdiction of this ministry and that adequate supervision and coordination is lacking in terms of management of IT equipment and systems. According to the baseline questionnaire, there were no major incidents in the previous two years, while other documentation shows that there were problems in the work of the Data Center and that, due to lack of appropriate procedures and equipment, they could not be treated adequately, despite the additional response and prevention efforts of the employees themselves. Limited resources and clear separation of duties put additional burden on and limit the work of employees, while inadequate organization and availability of resources have a major impact on efficiency in the domains of maintenance and improvement of the Data Center.

In addition to this, major incidents recorded in the previous period were as follows:

- Water supply pipe damage and water spillage in the DC;
- A blast of a bomb planted under a car in the underground parking lot;
- DDoS attacks on the entire public administration network;
- Exchange server failure due to inability to upgrade server equipment;
- Network failure caused by overheating of the equipment due to inadequate air conditioning in the summer;
- There are no devices for uninterrupted power supply in certain parts, which leads to the termination of the work of equipment and interruption of communication.

Certainly, some of the listed risks related to the above incidents have been reduced in the previous period.

2.1.9 PDC – summary

As already mentioned, according to the self-assessment, the Primary Data Center (PDC) could probably be classified somewhere between the Tier-1 and Tier-2 categories and this classification, as such, is inadequate for the Data Center that should enable smooth and continuous operation of the entire IT services of public administration and generates a risk that should not be acceptable to the said Ministry and public administration as a whole. In this regard, and having in mind all the above findings, the last chapter brings the consolidated conclusions and recommendations, which could be considered and implemented in their entirety since resolving the above issues takes a unified and synchronized approach.

2.2 Disaster Recovery Site (DRS)

It is very important that in the event of a disaster, users of IT services ensure that significant disruptions in the delivery of e-services do not occur. For this reason, it is necessary to ensure a stable and reliable backup DRS location with regularly tested IT application systems, replications and recovery procedures. Preliminarily, according to the ANSI / TIA-942 standard, the Disaster Recovery Site (DRS) could probably be classified as the Tier-1 category since it does not have a redundant component and displays very limited protection against physical events and identified key environmental risks. This estimated classification is inadequate for the Data Center, which should enable uninterrupted and continuous operation of entire public administration IT services in the event of a disaster at the Primary Data Center (PDC) and, as such, generates the risk that should not be acceptable to the Ministry and public administration as a whole.

Primarily conceived as a temporary solution for the needs of the Ministry itself, over time, it has grown into a Data Center that serves a limited and very small number of public administration IT services. However, it was observed that there are almost no application IT systems from the Primary Data Center (analyzed above) at the Reserve Data Center (DRS). At the same time, there are backup IT systems of other competent organs (Revenue Administration, Investment and Development Fund, etc.), whose primary IT systems are not hosted in the Primary Data Center (PDC) of the Ministry of Public Administration, Digital Society and Media in Podgorica. Therefore, it was impossible to perform an adequate review of the procedures in case of recovery at the backup location.

As in the previous case, according to the mentioned standard, all aspects of the physical infrastructure of the Data Center were analyzed as follows:

2.2.1 DRS – Location and construction works

The Disaster Recovery Site (DRS) of the Ministry of Public Administration, Digital Society and Media is located on the first floor of the office building of the sports center in Bijelo Polje. The location itself does not meet the basic prerequisites for the construction of a Data Center, given that the location within the sports and recreation center provides very limited opportunities for access, entry, servicing and replacement of equipment. There are extreme security-related threats that can paralyze the work of the Disaster Recovery Site (DRS) partially or completely, for example – riots or hooliganism after sporting events. These risks do not necessarily have to be manifested in the Data Center itself but also in the facility or its immediate surroundings. However, they could easily spread to the premises of the Data Center.

During the construction, local standards for the construction of business facilities were met, but not the standards for the construction of the Data Center, bearing in mind that its placement in the building was not planned at that time. In connection with this, the competent Ministry has made

continuous efforts to mitigate the identified risks by upgrading the premises of the former server room. However, these efforts could not be completely successful due to the initial limitations of the location and the facility. Existing walls and constructions were used, commercial security doors were installed, and the floor was raised. A suspended ceiling with built-in lighting was installed. The walls have not been treated adequately. At the same time, the existence of plumbing installations in the immediate vicinity generates additional risks and the existing risks of flooding in the office building itself. Furthermore, the Data Center is located near the river, so in addition to moisture, the river overflow may affect this location's power supply and network connectivity.

Image 8. DRS location, within the sports center

The entry to the Data Center is possible from the office building but also by common metal stairs, which can only partially be used to bring the equipment in (limited size and weight). This generates additional risks, given that the stairway is used by a large number of people and that it is relatively easily accessible.

Image 9. Entering bulky equipment in the Disaster Recovery Site

2.2.2 DRS – Electrical design

Given that the planning documentation did not envisage the placement of Data Center in this facility, all of the subsequent works tried to reduce the observed shortcomings. The Data Center is supplied from a single branch of the low-voltage network through a generator system intended for Data Center only, which is in accordance with the minimum standards. The main switchboard of the Data Center, on the other hand, is located in the common area in a public, open, and easily accessible space, meaning that unauthorized persons can easily cut off the power supply to the entire Data Center.

Image 10. DRS main switchboard

As for the Data Center itself, most rack cabinets have separate UPS devices of different exploitation ages and current status. There is no central UPS system. The implementation of inadequate distribution of LV installations within the Data Center was observed, together with the existence of

additional space for rack cabinets, for which adequate capacities are not provided. Detailed documentation of performed works and electrical installations diagrams/schemes were not submitted. Also, there is no projected total and measured current power, in total and by segments, nor there is information on total heat emission needs.

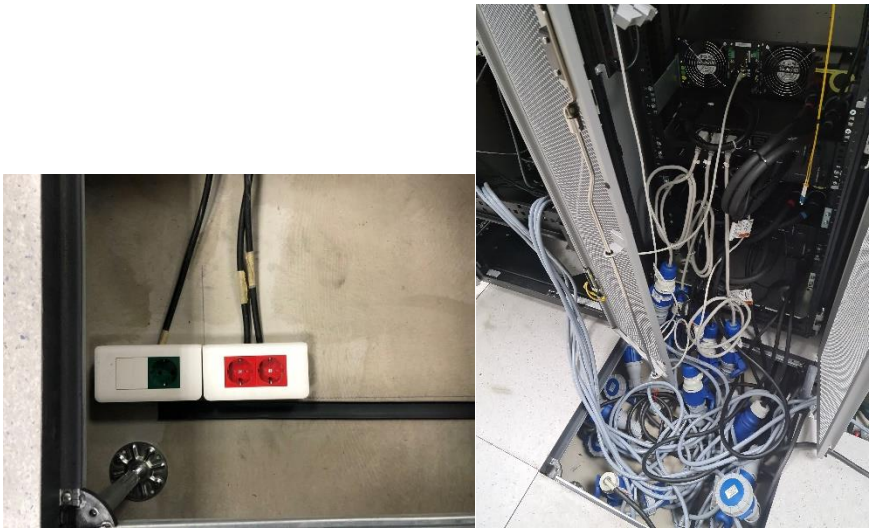

Image 11. Rack cabinet power supply in the Data Center

2.2.3 DRS – Network Architecture

Detailed documentation and network connection diagrams were not submitted during the analysis. During the site visit, it was concluded that the passive network architecture was not adequately planned or implemented and that it has been gradually implemented in accordance with needs. This approach prevents adequate capacity planning and generates additional risks for existing IT systems during subsequent implementations.

Image 12. Rack cabinets in the Data Center

2.2.4 DRS – Thermo-technical and mechanical systems

The Data Center has air conditioners, which maintain the room temperature at an adequate level in the room, but the lack of designated cold and hot aisles within the Data Center has caused inadequate and inefficient cooling of the entire room. The existence of serious warnings and notifications, which were not adequately treated, was noticed in the system. A ventilation system in the space is probably used as an additional emergency ventilation system.

2.2.5 DRS – Redundancy system for electrical, mechanical and telecommunication networks

The entire Data Center is powered by one transformer station, which supplies power to most other consumers in the area, especially the sports center, which has occasional needs for high consumption (when several events take place simultaneously), which can cause significant pressure. The paths of the power cables to and within the Data Center are not redundant, nor is the power supply system. There are no two independent branches of electrical power, so the risks are reduced by using rack mountable UPS devices.

Although energy inefficient, the air conditioning system is redundant, while no redundancy has been observed for the ventilation system. The degree of protection from external influences has not been determined.

It has been reported that the telecommunication WAN network is redundant at the level of Internet providers with a primary production optical link of 1Gbps, while the second backup link is of lower capacity. However, it has not been determined how and whether redundancy has been achieved at the level of technologies used and at the level of passive networks through which these services are delivered to and within the Data Center. Within the Data Center itself, there is currently no redundant active network equipment, but the risk in this domain has been identified and is planned to be mitigated through additional implementations or other projects (e.g., private cloud systems on DRS).

All users of IT systems, who do not use the Private Cloud system, introduce the necessary telecommunication WAN capacities individually, according to their needs.

2.2.6 DRS – Fire safety

A NOVEC gas fire-safety system, which is not adequately managed, has been implemented in the Data Center room. During the site visit, the existence of several serious alarms and warnings related to the fire safety system was established. Commercial security doors without adequate fire protection have

been installed on the existing premises. Fire sensors have been installed and connected to the central alarm and control unit. However, data on testing and maintenance of this system remained unavailable at the time of compiling this report.

2.2.7 DRS – Physical security

Despite the existence of commercial security doors, video surveillance systems and physical security within the office building, the security system is not at an adequate level. At a relatively short distance from the entrance to the Data Center, there are other offices and sports center facilities without access control, which can be accessed relatively easily. The access control system has not been implemented, but access is provided only with keys and with prior notice to the responsible staff of the Ministry. In case of disasters and emergencies, the arrival of the Ministry staff from Podgorica is required, while all works must be planned and announced in advance. It is not recorded who controls and supervises the entrance to the premises, nor in what way the external partners who access them together with the Ministry staff are registered.

Image 13. Entrance to the DRS Data Center

2.2.8 DRS – Efficiency

As with the primary Data Center, a centralized Data Center monitoring system has not yet been established. Certain alarms and warnings were observed within the Data Center environment systems themselves. However, these are not treated adequately. It was noted that a number of systems are implemented and maintained by other authorities, which are not under the jurisdiction of this Ministry. It was evident that a number of systems have been implemented and maintained by authorities that are not under the jurisdiction of this ministry and that adequate supervision and

coordination are lacking in terms of management of their systems. Additional reaction and prevention efforts of the employees themselves were noted. As in the previous case, limited resources and clear separation of duties put an additional burden on and limit the work of employees, while inadequate organization and availability of resources have a major impact on efficiency in the domains of maintenance and improvement of the Data Center.

2.2.9 DRS – summary

Given that the Disaster Recovery Site (DRS) is classified as the Tier-1 category, according to the mentioned standard, this level of classification is inadequate for the Data Center, which is expected to enable uninterrupted and continuous operation of entire public administration IT services in case of a disaster in the Primary Data Center (PDC). It generates a risk that should not be acceptable to the Ministry in question and the public administration as a whole. In addition, the Disaster Recovery Center (DRS) does not appear to be fully operational, which increases the overall risk of system downtime and reduces the possibility of business continuity. Given the very limited information on the Disaster Recovery Center (DRS), the main recommendation would be to reorganize this site the same way as the Primary Data Center (PDC) to allow operations at approximately the same level. In parallel, a redundant IT infrastructure should be set up within the Disaster Recovery Site (DRS) in parallel with the Primary Data Center (PDC), with the business continuity/disaster recovery processes developed and tested at least once a year.

During the conversation with the authorities, it was stated that the plan was to procure the necessary IT equipment and establish VMware replication through a 1Gpbs link between PDC and DRS sites.

In this regard, and having in mind all the above findings, the last chapter brings the consolidated conclusions and recommendations, which could be considered and implemented in their entirety since resolving the above issues takes a unified and synchronized approach.

2.3 IT infrastructure

The term ***IT infrastructure*** is defined in ITIL as a combined set of hardware, software, networks and facilities (including all of the information technology-related equipment) used to develop, test, deliver, monitor, control or support IT services. IT infrastructure allows an organization to deliver IT solutions and services to employees, partners and/or clients. The infrastructure consists of the following components:

- Hardware: servers, computers, storage, firewalls, routers, switches and other hardware components, even Data Center hardware.
- Software: operating systems, databases, applications, ERPs, productivity applications, infrastructure software, etc.
- Network: network and Internet connectivity, firewall solutions, and security. Including path selection, routing and protection, as well as their operating systems.
- Data Centers: Server rooms and data centers. This often neglected part of the infrastructure is usually the weakest link and the cause of most system outages if not managed properly.
- People: According to the ITIL's strict definition, people are not considered part of the IT infrastructure. However, without competent and properly-qualified people in charge of managing and maintaining IT infrastructure, the capabilities of an IT organization can be significantly reduced.

The present analysis reviews the IT infrastructure at the IT architectural level. When it comes to Data Centers and IT infrastructure, all the above components are covered to a very basic extent, according to the identified risks.

During the review, three types of IT infrastructure were defined:

- Traditional infrastructure – with traditional infrastructure, components such as Data Center, data warehouses and other equipment are owned by the organizations and within their facilities.
- Cloud Infrastructure – Describes the components and resources required for cloud computing. Rental of cloud infrastructure is a very popular method to reduce IT infrastructure and facilitate its management. Also, a private cloud can be built within an organization using resources dedicated only to that organization. The introduction of private with public clouds or within multiple private/public clouds can be managed across multiple clouds to create a hybrid cloud. There are three main categories of cloud computing service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

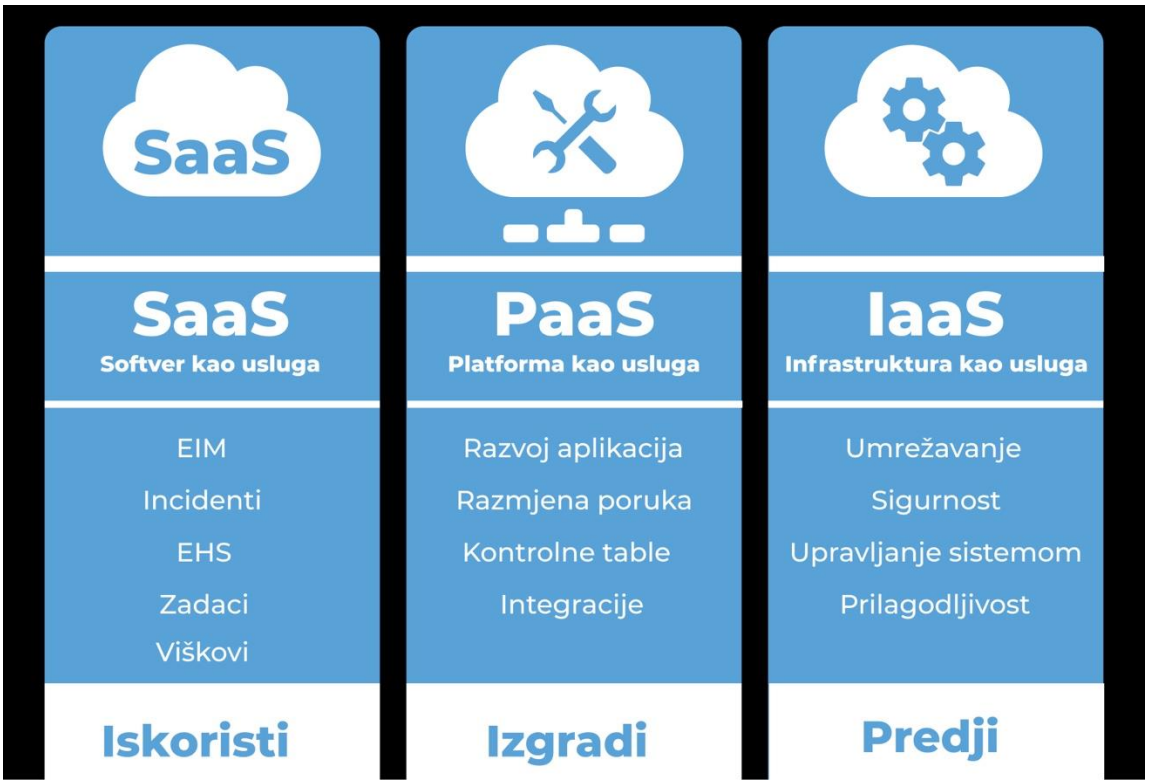

Image 14. Categories of cloud computing service models

- Hyperconverged infrastructure – allows the organization to manage computing, network and data storage resources from a single interface. Thanks to software-defined computers and bundled data storage, an organization can endure more modern workloads with scalable architectures on industry-standard hardware.

The information obtained during the analysis of the IT infrastructure was incomplete. Such information was expected to give a detailed overview of the existing hardware and IT infrastructure, its current and required capacities, current status and utilization, etc. On the other hand, the level of information on the Private Cloud system can be praised since it is well managed in the domain of available capacities. The plans for future migrations to this environment have been recorded and the organization's focus on this system.

Based on the submitted information, it can be concluded that the overall strategy of the Ministry has recently focused on private cloud infrastructure and optimization of the overall government IT infrastructure on this private cloud, which is considered a very good and cost-effective approach. Virtualization is a technology that allows the creation of multiple simulated environments or dedicated resources from a single physical hardware system, while clouds represent IT environments that abstract, consolidate, and share scalable resources within a network. Infrastructure as a Service (IaaS) very often represents a private cloud computing model. Another key reason for the increased interest in setting up and managing private clouds in Europe is the significant amount of uncertainty regarding potential EU regulations on privacy, security, location and ownership over data.

The process of optimizing the entire IT infrastructure on the existing private cloud is underway. However, there is no envisaged timeline or comprehensive plan by the authorities. In addition, an adequate private cloud infrastructure environment has not been implemented in the Disaster Recovery Site (DRS), nor have disaster recovery procedures been developed, although there are plans to perform this task. This is particularly true when the needs of other ministries and government agencies are taken into account, bearing in mind that part of their infrastructure is or should be hosted at the Primary Data Center (PDC) in the near future. A review of the migration of these systems in private clouds is underway. Currently, VMware Private Cloud covers 11 government institutions that operate 39 information systems hosted on 122 virtual servers.

Given the main components of the IT infrastructure, additional information still needs to be provided, such as:

- Hardware – a complete list of hardware, including its detailed description, year of implementation, main purpose, capacity, use, etc., was not provided during the assessment period. According to the Ministry staff, there is a lot of leftover hardware which is no longer used. Maintenance is mainly related to the warranty period of the equipment, after whose expiration it is largely not adequately implemented/contracted.
- Software – a complete list of software, including OS/DB/APP with specification details, software hosting details, versions, year of implementation, main purpose, capacity, use, etc., was not provided during the assessment period.
- Network – a brief overview of the current and desired configuration was presented. For security reasons, a complete list of established network connections, including network plans, IP segmentation, network/security devices used, and pertaining specifications, versions, year of implementation, main purpose, capacity, use, etc. were not provided.
- Staff – information on the organizational chart, duties and responsibilities of employees was provided. Nevertheless, such information requires improvement, especially in the area of management and maintenance of the Primary and Disaster Recovery Sites (PDC and DRS) and maintenance of IT infrastructure. It should be kept in mind that inadequate daily operation and maintenance of the system are considered the main risks in modern IT operations. At the same time, the lack of human resources can easily undo all investments that are made.

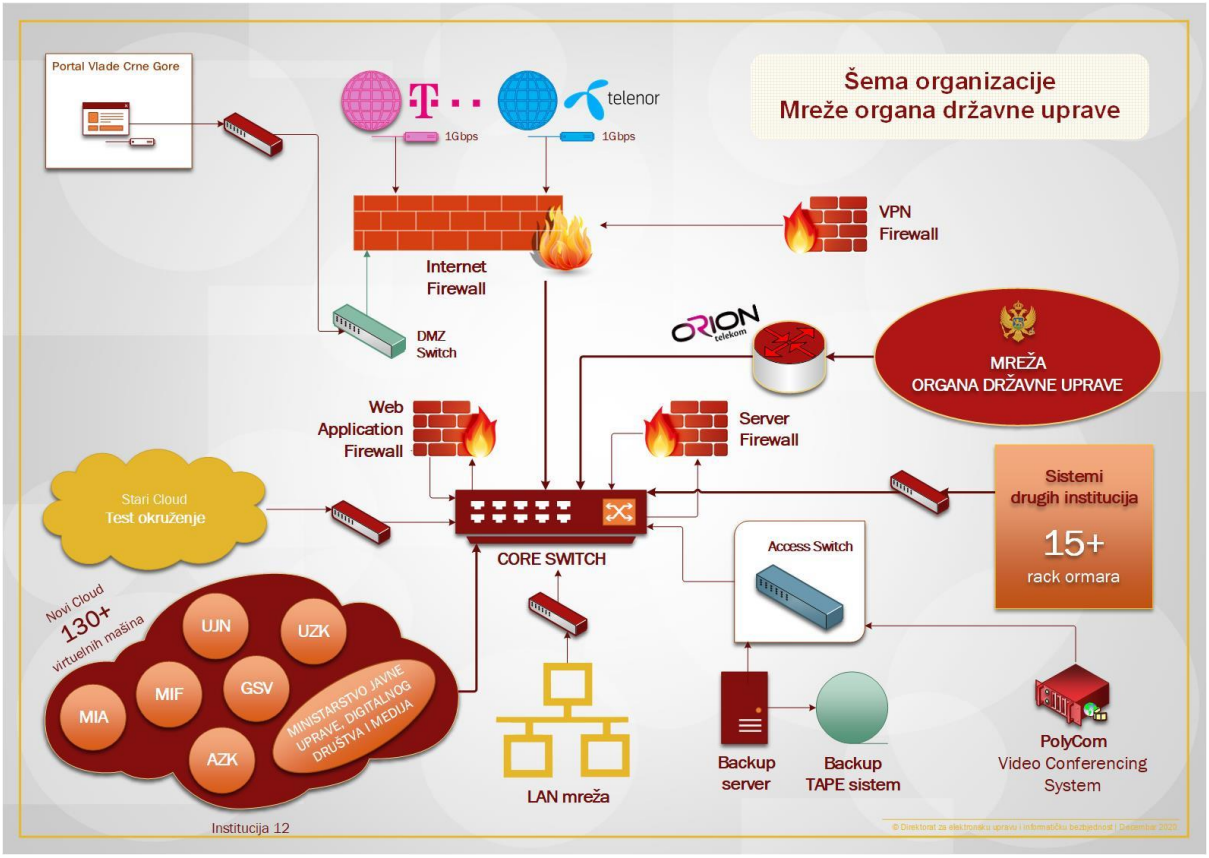

Image 15. The basic scheme of IT infrastructure

The main focus of the current strategy of the Ministry is to reduce the number of physical servers, and it appears that some good results have already been achieved by migrating part of the system to the cloud environment. Building a centralized virtualization platform can lead to certain savings but also generate major operational risks. Instead, a multi-virtualization platform in the private cloud is recommended. Even a hybrid cloud could be considered – to include some less important servers, such as simple web pages – which are categorized as sites that are not considered particularly critical and with no or low customer interaction. Servers need to be changed from time to time in line with available support and warranty conditions, which is something that does not seem to have been adequately done in the past.

The IT infrastructure features a SAN (Storage Area Network), which is considered a highly redundant system in the strategic plan. In reality, however, it contains some non-redundant parts (such as the backboard) in addition to the main redundant parts (controllers, memory, power supply, RAID, etc.). With this in mind, it is recommended to use multiple storage devices within the SAN infrastructure. Previously, the full capacity of the Private Cloud system was planned for 10 years for storage, which is good, but it should be harmonized with the system usage plans (currently, 60TB of the available 360TB is used). As for the Private Cloud system servers, the plan covers a 5-year period. At the same time, certain requirements of virtual production servers, for which the rationalization is performed, were observed as unjustified or underutilized. The system itself is scalable, which is an approach that allows for the flexibility of the IT infrastructure in question, which is highly recommended.

Current capacities and the use of the environment were also presented, and the use of CPUs seems to be at a low level, while memory and storage are used more and provide room for growth.

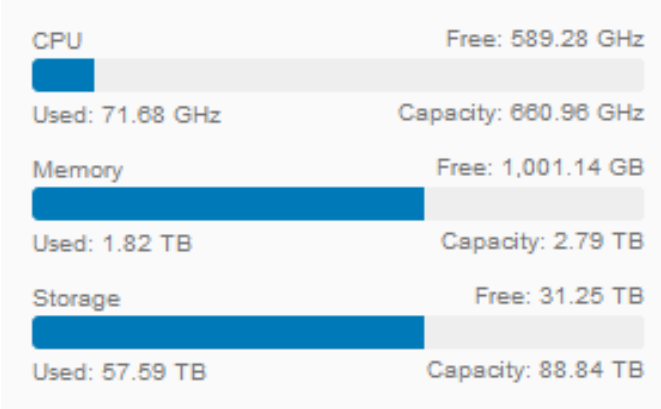

Image 16. Degree of utilization allocated virtual environments (source: MPADSM)

Although there seems to be a general plan, the desired configuration has not yet been achieved. Many aspects of the IT infrastructure require an update since the obsolete equipment needs to be replaced. Currently, remote locations are directly connected to L3 switches (located in a separate WAN zone). It is necessary to better understand the network configuration of the security system to improve security and performance and continue the application of further network and server segmentation. The initial DMZ was created. In order to further increase the security of the network of state bodies, it is planned to procure and implement a new Internet firewall with an IPS function by the end of 2021.

WAN links are realized through two providers via BGP protocol on Cisco routers backed by Checkpoint and Edge firewall, while the server segment is isolated by Juniper server firewalls. Institutions access through MPLS network that is aggregated locally and terminated at the core switch system, whose replacement is underway. According to the plan, expected occupancy after migration should be at the maximum level of 40% of network capacity (there is currently no data on system occupancy and load), while the complete system is scalable and supports further expansion by adding new chassis to the stack. Migration of all services to BGP addresses is currently underway with the aim to ensure full redundancy in that domain as well.

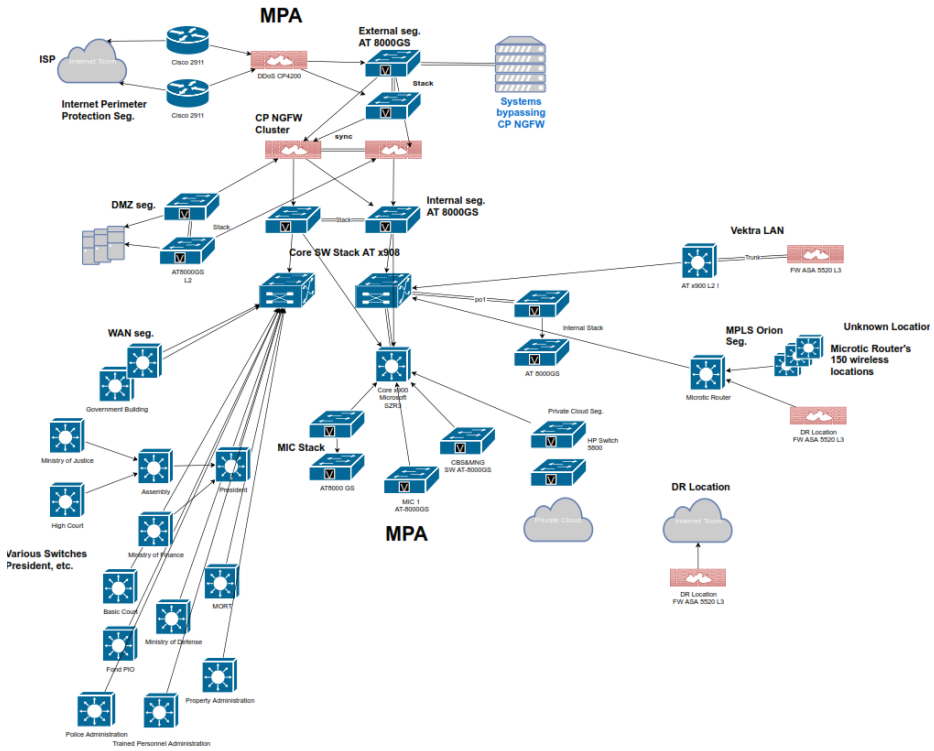

Image 17. Network segmentation diagram

Additionally, the hardware within the Primary Data Center (PDC) belongs to various institutions over which the Ministry has no control. However, the Ministry plans to offer these institutions the option to move to their private clouds to improve redundancy and facilitate system maintenance.

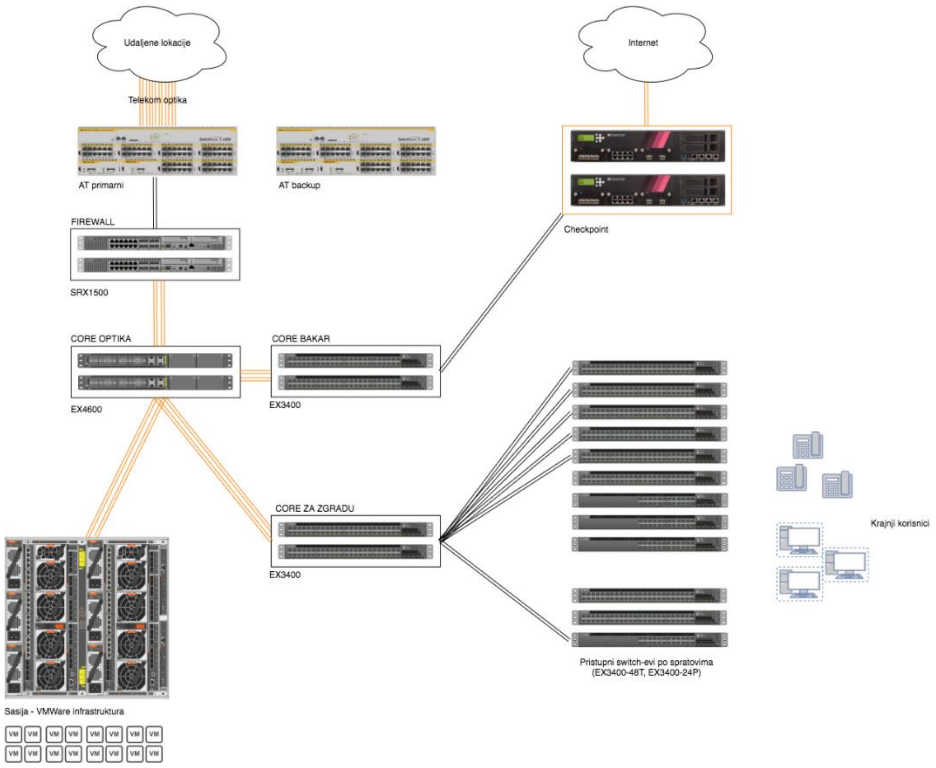

Image 18. Plan for the future configurations

Even though IT security is not the focus of this report, it seems that there is awareness of the importance of this issue among the competent authorities in the Ministry. They plan to consider this issue in more detail and deal with some of the threats identified in the previous period (such as DDoS attacks, etc.). This is very important for the overall IT infrastructure but is not part of this report.

Backup tape-library devices are used to create data backups. These should also be improved by using cheap storage systems for storing and replicating data on the DRS site (offline backups). In this way, faster recovery can be ensured in case of need. For other systems that are not virtualized and are not under the jurisdiction of the Ministry, the backup procedures are performed by the institutions themselves independently. Currently, there is no data provision system other than standard restrictions in terms of access rights. It is planned to pay particular attention to the procurement of special systems for data protection and encryption in the coming period.

Also, it has been observed that many of these systems are still running on very old OSs (such as Windows Server 2003/2008), which are no longer supported. This means that the migration to the private cloud should include the virtualization of these servers and the upgrade of these systems during a migration. It should entail contracts for maintenance of the systems after migration and regular updates and patches of both operating systems and applications. Regular maintenance and application of system patches should also be established (both at the level of procedures and at the operational level).

Also, there is a plan to procure a system for monitoring and supervising the entire IT infrastructure and services, as well as to procure a system for monitoring system administrators and users with special privileges, as well as the system for monitoring third parties that perform system administration.

Currently, the documentation in the domain of IT service management is incomplete. Several policies and procedures – such as procedures for monitoring, managing and creating changes to the system, records of changes and problems, as well as reporting and monitoring incidents – are being developed. Currently, there is no systematic approach to work. Still, it is planned that the procedures will be based on and in accordance with ITIL, COBIT 5 and 27001 standards. When it comes to the adopted procedures, the following were said to exist (although they were not shared with the authors of the report):

- Security policy
- Incident reporting procedure
- Backup procedure
- The system recovery plan and basis for BCP
- Physical security plan

Particular attention should be paid to the IT staff of the Ministry, who should be very well trained, bearing in mind the importance of the IT systems they manage. The organization and separation of

duties should be adequately established. There is no clear organization or persons who are designated as responsible for notifications and first response in incident situations. This is especially important in the periods outside working hours (7am-3pm). The entire IT service management should be defined in accordance with contemporary principles of practice.

3 Conclusions and recommendations

The main conclusions/recommendations within the framework of this analysis are not listed individually according to the identified risks due to the fact that they strive for a new approach because additional investments in existing locations and IT infrastructure would not adequately address the risks listed above. Upon analyzing the IT infrastructure within the Primary Data Center (PDC) and the inadequate Disaster Recovery Site (DRS), it is evident that there are high risks in the domain of the environment that supports the main government IT systems.

In this regard, the final conclusions are divided into several categories:

1. Further investments in the Primary Data Center (PDC) would not allow for an adequate improvement of this facility. Previous multiple investments in the active Data Center environment have increased the availability of IT systems but at the same time created additional risks for the systems in question (a serious extent of work has been carried out next to active IT systems, which is planned in future as well). The existing Primary Data Center environment poses a serious threat to the availability of IT systems it hosts. It is recommended that the Ministry conduct an analysis that should include the possibility of building a special building for the Primary Data Center in Podgorica in accordance with the Tier-4 standard or leasing a facility with adequate capacity from commercial service providers.

2. In order to ensure stable business continuity, in parallel with the Primary Data Center (PDC), a Disaster Recovery Site (DRS) should be established following the same standard. Further investments in the Disaster Recovery Site(DRS) would not yield an adequate improvement of this facility. Given the small number of systems hosted at this facility, it is recommended that the Ministry conduct an analysis that should include the possibility of building a designated building for the Disaster Recovery Site (DRS) with associated facilities in accordance with the minimum Tier-3 standard or leasing such facilities from commercial service providers. At the same time, based on adequate analysis, it is necessary to consider other cities in the northern region, especially the ones with adequate road and communication infrastructure (e.g., Bijelo Polje, Nikšić, Berane, etc.).

The definition of preconditions and requirements for the needs of the Primary and Disaster Recovery Sites (PDC and DRS) should be carried out in accordance with the relevant standards (striving toward the Tier-4 category). It is necessary to provide all the necessary IT rooms and staff offices within the mentioned premises.

3. A very detailed review and analysis of the required IT infrastructure capacities of the entire public administration is needed. A private cloud establishment strategy is still recommended.

However, it is very difficult to predict future needs without adequate capacity analysis and plan. Also, the scalability of the system should be enabled in an easy and accessible way. Simultaneous implementation of the private cloud should be carried out on both PDC and DRS sites, with the establishment of minimal replication and recovery procedures. In addition, it is desirable to create a geo-cluster between these two sites allowing high availability of IT systems. IT infrastructure should be built as very scalable and highly accessible in both locations, and in parallel, active replication and business continuity plans should be developed.

If the Ministry opts to develop new PDC and DRS locations and the associated IT infrastructure, without adequate analysis and planning of the necessary capacities, it could easily revert to the current situation with inadequate spending.

4. It is necessary to significantly improve the organization and level of training of staff, which should be able to adequately manage Data Centers and IT infrastructure. A clear definition of responsibilities and segregation of duties would also enable a clear definition of responsibilities and expectations regarding system maintenance and improvement.

If the decision is made to start the development of new PDC and DRS locations and the associated IT infrastructure, it is recommended to consider the possibility of separating this part of the competencies into a separate organizational unit or administration with clearly defined expectations and competencies towards all public institutions that should deliver services according to the state-of-the-art IT service principles. The organization should be established according to the most modern IT service management standards. In the future, it should provide services to all authorities and strategic state-owned organizations, optionally and preferably on a commercial basis.

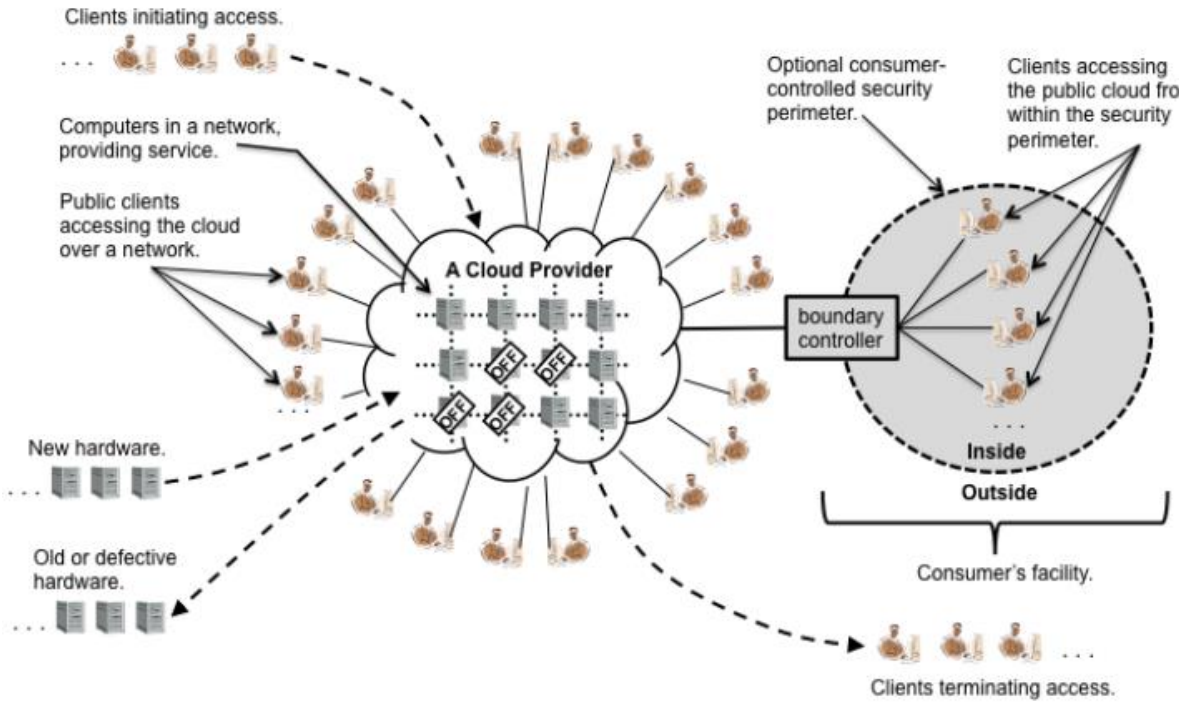

Image 19. An example of organizing a private cloud solution

Although this appears as a strategic, very demanding and expensive plan, at first sight, detailed analyses combined with the Ministry's strategic commitments would show that it probably does not exceed the level of current investments. If adequately planned and rolled out in several annual phases, it can be very feasible and affordable. If one takes into account the cost of unavailability of the system, the reputational risks and the reputation of government agencies, the analysis could show whether these investments would prove to be very justified. Of course, the investments themselves must be accompanied by adequate organizational and human capacities because otherwise, they would lead to inadequate implementations and waste of funds and resources while maintaining the same risks.

Strengthening the capacity of the Ministry of Public Administration, Digital Society and Media to develop detailed technical documentation/plans and update them on a regular basis should be a strategic focus. Having detailed technical documentation on the overall IT infrastructure and Data Centers is crucial for any good analysis and subsequent decisions. Detailed plans should include detailed technical analysis and costs to ensure future savings and highly accessible operations and services. Furthermore, a strategic plan should be developed for the introduction of an adequate organizational part to serve as an internal provider of IT infrastructure in the private cloud for the needs of all other authorities, based on modern IT service management. This process demands the involvement of all stakeholders and future users from its very beginning to define and ensure common goals. After that, a strategic IT infrastructure plan should be developed to include the Primary Data Center (PDC) and the Disaster Recovery Site (DRS) with the corresponding IT infrastructure in the private cloud. In doing so, it should be kept in mind that wrong decisions based on inadequate analyses

or incomplete data could have significant negative technical and economic consequences in the later stages of the plan. In order to ensure efficiency, the scalability of the proposed solutions must be guaranteed and based on a pay-as-grow model. Overall, the proposed model should be based in part on a holistic approach in modern IT, putting customer needs ahead of all other needs. Also, it should be based on a detailed analysis that envisages creating a strategic plan and meeting and maintaining anticipated needs starting from the bottom (Data Centers) all the way to the top (IT services and application systems).

To achieve all this, the following standard IT principles can be applied:

1. Developing the strategy of the Data Center (PDC and DRS) and the private cloud in it;
2. Developing the management of organizational and business process changes;
3. Organizing modern IT service management for governing and delivering these IT services;
4. Defining technological principles and strategies. In doing so, it is necessary to focus on data, solutions and customer needs.

4 Framework action plan

Based on the drawn conclusions, and in order to provide initial assistance in their implementation, an initial action, which can be used by the Ministry to define a framework for a further action plan, is proposed below. This action plan can be expanded or changed in accordance with the Ministry's needs and strategies.

No.	Recommendation	Recommendation details	Expected objectives
1	Analysis of current and required capacities of IT infrastructure at both PDC and DRS	a) Development of inventory methodology for all services b) List of all services, regardless of whether they already exist or should exist in the Primary Data Center (PDC) c) Technical inventory and description of all previous services, necessary preconditions and requirements – current/required situation d) Development of methodology and categorization of all previous services according to the level of their criticality and BCP/DRP needs e) Decision making in the domain of IT infrastructure capacity management strategy at PDC and DRS	All services pertaining to the future IT infrastructure are listed, technically described and categorized in accordance with methodologies. Decisions are made in the domain of capacity management strategy.
2	Analysis with IT infrastructure development plan	a) Preparation of basic technical documentation of IT infrastructure, with the definition of structure, capacity and capabilities b) Preparation of detailed technical documentation of all defined services with the plan of necessary IT infrastructure elements at PDC and DRS c) Analysis containing a proposal for the development of IT infrastructure while enabling the necessary scalability of capacity and needs d) Based on the defined necessary IT infrastructure elements, it is necessary to conduct an analysis of the model of development/migration of IT infrastructure from the "as-is" to the "to-be" state	Defined future IT infrastructure structure, capacities, and capabilities, with detailed technical documentation. Analyzed models of IT infrastructure development with models of migration to the "to-be" state.

		e) Decision making in the domain of IT infrastructure development strategy at PDC and DRS	Decision made in the domain of IT infrastructure development strategy at PDC and DRS.
3	Primary Data Center (PDC) Analysis and Development Plan	a) Defining Primary Data Center (PDC) requirements and capacities b) Development of the preliminary design of the Primary Data Center (PDC) with all its requirements c) Comparative cost analysis for building and maintaining own Primary Data Center (PDC) and renting a commercial Data Center (TCO for a longer period of time, e.g., 10–20 years) d) Decision making in the domain of Primary Data Center (PDC) strategy NOTE: Based on the decision, a detailed action plan for the implementation of the strategy shall be developed. The report itself shall provide conclusions and recommendations the Ministry should take into account.	The preliminary design of PDC with all necessary requirements and comparative analysis of construction and maintenance models are developed. Decision made in the domain of primary data center development strategy (PDC).
4	Disaster Recovery Site (DRS) Analysis and Development Plan	a) Defining the requirements and capacity of the Reserve Data Center (DRS) b) Development of a conceptual solution for the Reserve Data Center (DRS) with requirements c) Comparative analysis of costs for building and maintaining own Disaster Recovery Site (DRS) and renting a commercial Data Center (TCO for a longer period of time, e.g., 10–20 years) d) Decision making in the domain of Disaster Recovery Site (DRS) strategy NOTE: Based on the decision, a detailed action plan for the implementation of the strategy shall be developed. The report itself shall provide conclusions and recommendations the Ministry should take into account.	The preliminary design of DRS with all necessary requirements and comparative analysis of construction and maintenance models are developed. Decision made in the domain of Disaster Recovery Site (DRS) development strategy.

5	IT service management Analysis and Development Plan	a) Training of employees for IT service management b) Defining the methodology for establishing IT service management c) Defining the models and objectives of IT service management with organizational model, structure and resources d) Analysis of the current situation with the plan of development/migration to the adopted model of IT service management e) Decision making in the domain of IT service management strategy NOTE: Based on the decision, a detailed action plan for the implementation of the strategy shall be developed. The report itself shall provide conclusions and recommendations the Ministry should take into account.	Employees who participated in defining the methodology and plan for establishing IT service management, including organizational model, structure and resources, are trained. Decision made in the domain of IT service management development strategy.
6	The strategy for the development of the entire IT infrastructure	a) Consolidation of all previously defined decisions and analysis/harmonization of the consolidated IT infrastructure b) Defining the strategy of IT infrastructure development c) Strengthening the legislative framework in the domain of IT infrastructure, harmonization with existing legal solutions, and drafting normative legal acts, as well as internal procedures in the domain of IT infrastructure management d) Development of a framework action plan based on the IT infrastructure development strategy	Adopted the IT infrastructure development strategy, harmonized with existing legal solutions, and developed internal procedures. Adopted an action plan based on the IT infrastructure development strategy.
7	Organizational development	a) Training of employees in accordance with the guidelines of the strategy of the development of the entire IT infrastructure, including both IT infrastructure system administrators and system administrators of specific services b) Development of performance measurement model and continuous training of employees c) Development of a minimum system availability model and defining a framework agreement with external system users (SLA, RTO, RPO, etc.)	Employee training delivered, and a performance measurement model developed. The model of minimum system availability and framework agreement with external system users was adopted.

		d) Development of a model for measuring the performance, availability and capacity of the system e) Implementation and maintenance of IT service management (preferably certification), including improvement of existing business processes, organization and organizational practices f) Defining categorized services required for business continuity (BCP/DRP) and establishing standardized requirements for implementation	Model for measuring system performance, availability and capacity adopted. Implementation of the adopted IT service management model. Development of the main BCP and DRP plans.
8	IT infrastructure development	a) Development of a detailed technical and functional plan for the development of IT infrastructure, based on the IT infrastructure development strategy, including planned migration and migration procedures b) During the implementation of a detailed action plan for the development of IT infrastructure, mandatory development and maintenance of detailed technical documentation of all elements of IT infrastructure c) Development of detailed business continuity plans with regular annual tests NOTE: Based on the decision, a detailed action plan for the implementation of the strategy shall be developed. The report itself shall provide conclusions and recommendations the Ministry should take into account.	A plan for the development and migration of IT infrastructure is developed on the basis of the adopted strategy. During the implementation of the plan, detailed technical documentation of all elements of the IT infrastructure is prepared. Detailed business continuity plans are adopted and successfully tested.

ANALYSIS OF JOINT PUBLIC ADMINISTRATION SYSTEMS AND SERVICES

INTRODUCTION

The most significant effect of the ongoing COVID-19 pandemic when it comes to the domain of work, both in public administration and in private companies, was the mass transition from office to work from home mode, which required major changes in the organization of communication with public officials, different approach to the content they work with, but also different communication with interested members of public. The ability to adapt to the unprecedented circumstances using agile information systems was a substantial challenge for the public administration, which suddenly had to support a large number of workers working from home, communicating with users from their homes, and providing services electronically. Inevitably, content management software is, generally speaking, evolving rapidly, and new technological trends, such as artificial intelligence (AI) and machine learning (ML), are increasingly being built into platforms to provide additional insights into content and user behavior patterns. In addition to this, much work is also being done in relation to features that improve the level of security of content on these platforms, given that many actors of recent cyber-attacks and other malicious threats have perceived remote access to systems as their chance to intercept such communications.

Having all the above in mind, together with the clear commitment of the new Government of Montenegro to intensify digital transformation efforts and the almost inevitable future pandemics or other unforeseen scenarios that will require new and different ways of working and access to public administration, below is a brief description the most important existing systems that are used commonly by all authorities, as well as recommendations for improvements that would ensure better preparedness for said circumstances.

1. The www.eUprava.me web portal

1.1. Introduction

The eUprava.me (e-Government) web portal is a central web-based portal for receiving electronic form submissions that enables the provision of services electronically, through the generation of electronic services and the processing of electronically submitted requests. The electronic manner of communication between public administration and citizens and the business officially started on April 7, 2011, when five state institutions began providing 12 electronic services. Ten years later[2], there are 530 active services on the eUprava.me web portal, of which 162 are electronic services and 368 information-provision services.

All services on the web portal feature one out of five levels of sophistication, as follows:

- Level 1 – Information-provision services (description of the administrative procedure) – 221;
- Level 2 – One-way interaction (forms are available for download and manual filling, but it is not possible to upload them to the portal) – 147;
- Level 3 – Two-way interaction: electronic forms can be filled in by the user, while the system allows submitting a request with electronic identification (authentication) – 162;
- Level 4 – Transaction, allowing the entire service to be delivered electronically – including filling in forms, electronic identification, making the payment, and delivery
- Level 5 – State-of-the-art e-services, allowing proactive (automated) delivery of services in a way that warns and informs the user about relevant facts – the user is required to provide their confirmation or consent only.

The legal basis for the delivery of services through the e-uprava.me web portal is provided for in the Law on Electronic Administration[3], which entered into force on July 5, 2020, and the Law on Electronic Identification and Electronic Signature[4], which entered into force on January 3, 2020.

The Law on Electronic Administration, among other things, stipulates the adoption of 17 bylaws, of which 15 ordinances and two decrees[5].

---

[2] The data was updated on October 27, 2021.

[3] **"Official Gazette of Montenegro", no. 072/19 of December 26, 2019**

[4] **"Official Gazette of Montenegro", no. 031/17 of May 12, 2017 & 072/19 of December 26, 2019**

[5]

1. Rulebook on the requirements that must be met by facilities, i.e. spaces for accommodation and operation of computing and communication equipment;
2. Rulebook on the standards of accessibility;
3. Rulebook on the manner of opening, suspending and revoking accounts in the active directory and unique official addresses for electronic communication of state administration bodies;
4. Rulebook on technical requirements and security standards for access to the unified electronic data exchange system;

The Law on Electronic Identification and Electronic Signature prescribes the adoption of nine bylaws[6].

Although several thousand applications (around 8000 or more) are communicated through this web portal every year, which is a number that remains relatively stable from year to year, this trend does not correspond to the growing interest in new technological concepts and the digitalization of public administration. Even the outbreak of the Covid-19 pandemic, which was expected to lead to an exponential increase in the use of e-government services, did not change the trend of stagnation in

5. Rulebook on the manner of granting unique licenses;
6. Rulebook on the appearance and content of forms for submitting data on electronic registers and information systems, as well as on the content and manner of keeping the meta-register;
7. Rulebook on the content and appearance of the application form for obtaining consent to the conceptual design, i.e. project documentation for the establishment, i.e. improvement of the information system of state administration bodies;
8. Decree on the manner of management and other issues of importance for the functioning of the Unified System for Electronic Data Exchange;
9. Rulebook on technical and other requirements for the use of a unified information system;
10. Rulebook on the manner of managing the unified information system, and the development and improvement of the unified information system;
11. Rulebook on the manner of determining the fulfillment of conditions for the use of a unified information system;
12. Rulebook on the manner of obtaining consent for the provision of e-government services through the system;
13. Rulebook on the criteria of portability and responsiveness the competent body is expected to meet when providing e-government services;
14. Decree on technical and other requirements for access to the unified information network, as well as the manner of managing the information and communication network;
15. Rulebook on the manner of management of the information systems;
16. Rulebook on the manner of development and improvement of the information system;
17. Rulebook on the manner of auditing information systems in state administration bodies.

*** Note: regulations 9 to 17 have not been adopted yet, so minor changes in their name or content, which may occur in the process of harmonization with the Secretariat for Legislation, are possible in the coming period.

[6]

1. Rulebook amending the Rulebook on measures and activities for the protection of electronic signature and electronic seal certificates;
2. Rulebook on the minimum amount of liability insurance against liability for damages resulting from the provision of electronic trust services;
3. Rulebook on the detailed content and manner of keeping records of electronic trust service providers and the register of qualified electronic trust services providers;
4. Rulebook on the manner of performing electronic trust services and qualified electronic trust services for state administration bodies;
5. Rulebook amending the Rulebook on the manner of assessing the conformity of qualified means for the production of electronic signatures and electronic seals and the content of the list of certified qualified means for the production of electronic signatures and electronic seals;
6. Rulebook on detailed conditions that must be met by a qualified electronic trust services provider;
7. Rulebook on technical and operational requirements related to the node – the place of connection of the electronic identification schemes and the process of establishing a framework for the interoperability of the electronic identification system;
8. Rulebook amending the Rulebook on the minimum technical standards and accompanying procedures in relation to which the level of security of the electronic identification system is determined;
9. Rulebook amending the Rulebook on detailed requirements that must be met by a qualified service of registered electronic delivery.

the number of submitted applications. One of the reasons for this situation is the fact that the technical warranty on the portal expires at the end of 2021, which is why there have been very few innovations in terms of functionality, user experience, usability and other technical and user-related aspects of its operation over the past 10 years. Contrary to the Law on Electronic Government obligations, various institutions sporadically decided to build their own electronic service portals. Thus, special portals for students belonging to the Ministry of Education, Science, Culture and Sports, the portal of the Revenue and Customs Administration, the portal of the Ministry of the Interior, the portal48.podgorica.me of the Capital City, the eInnovation portal of the Ministry of Economic Development and many others isolated "islands" in the of electronic public administration services ecosystem were developed.

Another important reason for the insufficient popularity of this web portal is that the perception of fully functional electronic services differs depending on the perspective from which they are viewed. While citizens and businesses perceive electronic services as "end-to-end" services that remove the need to visit the counter and wait in lines, the authorities consider electronic services to be even those with partially digitized steps of a process. The reasons for this discrepancy in views are numerous. One of the most common is the non-compliance of regulations with the digitization requirements, which is why the technological solutions try to cover only segments of the business process for which there are no implicit legal barriers. Several illustrative examples of this situation can be found in some of the most used services on the e-Government portal, such as the e-service for announcing vacant job positions within the Vocational Training Program for persons who acquired higher education or the e-service for applying for student loans. Specifically, after the employer fills in the data on the company and the data on available jobs for this Program, and after they receive an e-mail confirming the successfully submitted application – they are obliged to print, sign, stamp and take the attachment from the e-mail to the local the counter of the National Employment Agency of Montenegro. After that, the employee is asked by the public servant to copy the data from the form to the form of the Bureau, which is to an extent different from the one from the e-Government portal and submit it for the purpose of recording.

The experience of those who used some of the recently developed information systems, including the new Public Procurement portal (https://cejn.gov.me/), indicates that the eGovernment portal remains a system that generates a number of problems due to the time in which it was created. Specifically, the bidders can register on this portal electronically by entering data about the company, authorized persons, as well as all other relevant data. It is not clear why the contractors did not make use of the public API through which, thanks to electronic identification, they could automatically withdraw all data from the Central Register of Business Entities. Once the registration is completed, the user is not able to log in to the system until they download certain Form 1 from the portal of the Directorate for Public Procurement Policy, which contains identical data as those from the electronic registration form. Once they download the form, they are expected to fill it in, sign it and send it to the business address of said Directorate. After this, if the data in both places match, the portal administrator approves the registered account, allowing the user to use the portal.

A similar experience comes from using the subvencije.me web portal (subsidies and financial incentives portal), which this year promoted exclusively electronic submission of applications within the Program for Improving the Competitiveness of the Economy for 2021. Namely, after registration on the portal, which means entering all data about the company, i.e., applicant (it is not clear why the public API with crps.me was not used). It is worth noting that this process is not protected by an SSL certificate despite the form that involves sending data to the server. After the entry in question, the user is redirected to download between 5 and 15 .docx files depending on the selected program line. After filling in the multiple documents with multiple identical entries about the company (in the first chapter of each downloaded document), all .docx files should be signed electronically and, together with additional accompanying documentation (which is partly under the jurisdiction of other authorities and could be exchanged via JSERP), uploaded to the server via a form. Several iterations with representatives of the Ministry follow, during which changes in the submitted application may be requested, after which the application will be rejected or accepted.

This example alone also shows that digitalization has brought additional steps that users must follow instead of removing the need to follow a number of existing ones. This indicates the need to change regulations and optimize business procedures and practices rather than changing the platforms offering electronic services because the functionality of the most modern portals and systems do not stand a chance with users as long as business procedures are complicated and involve duplicate and redundant steps.

In addition to all the above, the data from The research on the attitudes towards and the use of e-services among citizens and businesses in Montenegro, implemented by Ipsos and funded by UNDP, shows worrying results. As many as one-third of Montenegrin citizens have never heard of electronic services (33%), while just over two-fifths of them have heard of the term “e-services” but know almost nothing about them (45%). Only one-fifth of respondents consider themselves mostly familiar with electronic services (19%), while only 3 out of 100 citizens (3%) report that they have full knowledge of the concept. These data show that, apart from technical and user shortcomings, the electronic services system does not have an adequate communication system with the target public. This is evidenced by the information obtained during the interviews with those responsible for carrying out digitization activities in the Ministry of Public Administration, Digital Society and Media. Such information relates to the virtually non-existent involvement of citizens in designing and developing an electronic service, as well as an almost complete absence of the system for receiving and analyzing user feedback in order to improve the user experience with e-services of public administration (with the exception of the basic rating system).

1.2. Functional units and technical aspects

The eUprava.me web portal is a custom-made solution built on the .NET technology stack, including the MS SQL Server 2008 R2 database running in the background. It is hosted on 64-bit servers under

Internet Information Services 7.5 (IIS 7.5), which relies on the Windows Server 2008 R2 installation. It was designed and implemented using the SOA (Service-Oriented Architecture) concept, which should provide easy scalability, new functionalities, decentralized updating option and secure communication.

The Content Management System (CMS) developed for the needs of this web portal was built using the C# coding language. The front-end segment of the portal, i.e., the user interface, was developed using the following technologies:

- ASP.NET
- JavaScript + jQuery framework
- AJAX
- HTML + CSS for structure and styles.

The portal consists of several interconnected subsystems, as follows:

1. System for managing the Portal content (Content Management System) – designed and implemented according to Web Content Accessibility Guidelines 2.0, XHTML 1.0/1.1 standard.

2. Electronic services generation system – this system uses a wizard to enable the creation and maintenance of electronic services, including the generation of electronic forms and the definition of relevant parameters.

3. Electronic services delivery system – enables the submission of requests using specific forms that guide the user through the entire process.

4. Electronic services processing system – this system allows:

- finding and retrieving submitted requests and attached documentation;
- sending an email from the person processing the request to the end-user;
- the processor to upload a document that is the result of an electronic service;
- returning the request to the applicant for additional.

5. Electronic identity and signature management system – enables electronic identity verification, electronic signing, and electronic signature validation. The portal supports electronic user identification, depending on the type of public service required. Also, electronic signing of all electronic requests through the e-government portal is provided in the case that was one of the requests in the process of creating the electronic service. At the time of making this analysis, the e-government portal supported the acceptance of certificates issued by MPADSM (for public administration officials, state bodies officials, etc.) and certificates of the Post of Montenegro.

6. System for electronic public hearings titled *eParticipacija* – which provides the possibility of publishing calls for public hearings, commenting on a particular topic and submitting documents by registered users. Those working in public administration bodies may initiate public hearings on any issue of public importance, a legislative proposal, etc.

7. System for users – Moja eUprava (engl. My eGovernment) – allows personalization by the users of the Portal, based on their personal profile. It is a central place for all registered Portal users allowing them to personalize content, view submitted requests, change information in their profile and more. This subsystem still does not have the capacity to interact with the user proactively. However, those in charge of digitalization activities in the Ministry are aware that the process should go in that direction, and these functionalities are part of plans to build a new e-government portal.

8. eObavještenje (eNotification) – system notification to end users on all activities related to a specific request they made, system notification to administrators on new requests received through the e-government portal, as well as a system notification on the profile page of the end-user of the Portal.

9. The system that allows integration with available electronic payment systems – ePlaćanje (ePayments) – a service that enables electronic payment and integration with competent institutions that provide electronic payment services. The service was implemented in 2013 as a completely independent part of the information system. However, it has never been widely used due to organizational and legislative barriers.

10. eZakazivanje (eAppointments) – electronic scheduling service – an integral part of the system for generating, executing and processing electronic services. A system that provides the possibility of electronic scheduling of appointments, submitting requests for services whose one or more steps cannot be performed electronically in their entirety, as well as a system that allows scheduling appointments.

11. eAnkete (eSurveys) – electronic surveying system – with defined administrator's rights to create and review surveys, create reports and export them in one of the formats allowing further processing of data in professional programs for the purposes of mathematical and statistical analyses. The creator of the survey has the ability to determine the survey target population: anonymous or registered users.

12. Web services for integration with external systems – The Portal is open for access to other information systems in order to download data from the web services of the Portal. In that sense, a register of all systems has been provided, which allows access to and download of data with predefined rights and a set of data to be downloaded.

All registered users of the eGovernment Portal are enabled to submit their questions and suggestions related to e-government provided by the Portal. In this way, the user's communication with the public administration is simplified so that the user, by filling out the form located below the information about the service, can send a question or suggestion to the competent institution regarding the service of interest. In addition to the above, users also have the opportunity to vote on whether the service was useful or not.

1.3. Conclusions and recommendations

The implementation of the system providing the highest-level e-services implies automated exchange of data from the key registers between institutions while dealing with all the challenges related to interoperability. Without this precondition, all electronic services in Montenegro will be limited to Level 3 in terms of sophistication. This is, however, only one of the many centralized systems necessary for digital transformation. In addition to this, there is a need for electronic payment systems for administrative fees, electronic delivery systems, improvement of the existing electronic identification and signature system, etc. In addition to the above, the existing euprava.me web portal is based on outdated technologies, which over time has become an aggravating and limiting factor for its upgrade and maintenance. Therefore, in order to improve this system, the team of authors proposes the following activities:

1. Reengineering of administrative procedures, which is a project that involves the selection (prioritization) of 10-15 administrative procedures that have the greatest coverage in the domain of target groups, and re-engineering them, in accordance with applicable regulations, best global practices, accompanied by an openness to change special legal solutions which prove to be obstacles to change. It is possible to have good digital services only if analog administrative processes are good.
2. Developing a new eGovernment portal as a state-of-the-art technical solution based on "one-stop-government" principles built around the so-called "digital enablers" such as electronic identity (eID), integration of data from the basic registers of all state administration bodies (JSERP), NS-NAT and e-Delivery systems, which, in addition to less sophisticated ones, will also contain fully digitalized fourth and fifth level services. The new web portal should be user-oriented, offering an adequate user experience, intuitive, supportive of diversity, inclusiveness and equality in the broadest sense of the word, and it should motivate users to complete procedures electronically instead of going to the counter. Also, the portal should be responsive, i.e., adjustable to all devices and screen sizes, including mobile phones. The construction of native mobile applications should be considered in the next phase. A special aspect of this project is cyber security, in which, in addition to taking measures to protect the IT infrastructure on which it will be hosted, the principles of web system protection at the

application level should be incorporated during construction[7]. An example of good practice is the Estonian e-Government portal https://www.eesti.ee/en

3. Establishing an integrated policy (standards) for the development and delivery of electronic services as one of the policy instruments for strengthening the coherence, effectiveness and sustainability of the Montenegrin public sector's efforts to provide high-quality services to citizens and businesses. Once developed and established, these standards need to be applied to all public administration bodies, and the following aspects must be insisted on:
    - "single point of contact," the idea that all public administration services, regardless of the bodies participating in their provision, are located in one place or, if this is not possible, that services are at least accessed through a user identification service - Single sign-on (SSO).
    - Classification of services through life cycle events, which allows services to be approached intuitively through identification with the real-life stages of the individual (for example, the birth of a child, finding a job, starting a company, etc.). Good examples of this approach are the Estonian and British national e-service portals.
    - Unifying the service provision between different communication channels. Procedures must look identical when the service is provided through a web portal, mobile phone, over the counter, through a digital kiosk, telephone, and other ways.
    - Implementation of the "once&only" principle that promotes the exchange of data and information at all levels and between all institutions and eliminates the possibility of requiring citizens and companies to submit evidence or documents already owned by the authorities.
    - Establishing a "user engagement and citizen-driven" approach when designing and creating services, i.e., putting users at the very center of the process of creating and improving services, which must be based on the principles of usability, usefulness, empathy and inclusiveness (so-called "look and feel" principles).
4. Developing a system for advanced reporting on user behavior patterns when using the portal and other indicators important for business decision-making. Such a system should be based on BI principles (three-layer storage architecture: OLTP, DWH, OLAP, optional and data mining systems for predictive and prescriptive analyses[8]). When adequately planned and built, such a system can provide, among other things, monitoring of the following indicators: Customer Satisfaction Score, Breakdown based on the so-called levels of customer satisfaction, Satisfaction trends over time, user outflow predictions, Net Promoter Score, the share of anti-promoters, passive users and promoters, NPS trend over time, employee productivity or utility rates, employee commitment indicators, statistics on transactions over time etc.

[7] https://owasp.org

[8] Predictive analytics applies mathematical and statistical modeling and techniques to historical data, and shows what can be expected, with some degree of probability. Prescriptive analytics involves collecting data, designing activities in different scenarios, and predicting the impact they will have, in order to facilitate and automate decision-making by choosing the best of the options offered.

5. Improving the existing or design and developing a new system for receiving and analyzing euprava.me portal user feedback, with the aim to improve the user experience of e-government services, better and more intensive communication with users, and greater visibility of e-services at all levels. This recommendation may include several known mechanisms for collecting user feedback, such as: online panels, humanoid robots, customer satisfaction systems and web portal service ratings, mobile applications, kiosk feedback systems, and internal feedback systems. By collecting and analyzing this information, all individual interactions, as well as their sequences, are stored and reviewed – including information about what users clicked, what they did not click, what they said, whether they were bothered by something or liked something in particular, and how they felt during interactions with service providers and the like. Examples of good practices for each of the above mechanisms can be found both in EU countries and globally. Some of the best known are:
    - Online panels: Ireland's "Your Dublin, Your Voice," "City of Provo" in Utah, USA, or "Service Victoria," also in the USA.
    - Humanoid robots: ASAN xidmət in Azerbaijan and VITAL shared services in Singapore.
    - Web portal user feedback: two examples from the UK, the National Library of Medicine and healthcare.gov. Also, integration with social networks is recommended in this segment.
    - Mobile applications: RAS Mobile app and MyGov in India, but also National Super App in Malaysia.
    - Kiosk-feedback systems: ASAN centers in Azerbaijan.
    - Internal feedback systems: Fraser Health, British Columbia, USA.

It is encouraging that those responsible for the digitalization activities in MPADSM have already recognized the importance of this activity in the plans for the next period and in the Public Administration Reform Strategy for the period 2022-2026, as one of the operational goals included the establishment of a system for assessing customer satisfaction with electronic services in public administration.

2. eDMS

2.1. Introduction

The Electronic Document Management System (eDMS), whose implementation for the needs of the line ministries in the Government of Montenegro and the Secretariat General of the Government began in 2011, is primarily intended for electronic office operations, which includes not only proper recording and electronic archiving of documents produced in the course of business administration but also document management throughout its life cycle, as well as conducting business procedures.

The key difference from the traditional way of working is the participation of all public servants in the process of keeping records of cases. Instead of being the exclusive responsibility of the records management office, thanks to eDMS, all clerks who participate in the processing of cases shall be obliged to personally record changes in the cases they process. In this way, according to the "authority" matrix, eDMS, provides insight into the state of documents: to whom the case was assigned, the status of the case and a large number of content reports with data on the number of processed cases, work efficiency of the sectors and individuals etc. By integrating eDMS with other e-government software solutions, an operational information base will be created for the development of new electronic services.

The legal basis for implementing the project of introducing eDMS in state administration bodies is primarily found in legal documents that regulate the issues such as office operations and the use of electronic documents, electronic signatures, and electronic administration.

The introduction of the eDMS system has been recognized as an important goal in the Public Administration Reform Strategy for the period 2016-2020, as well as in the Strategy for the information society development 2016-2020, which represent comprehensive strategic frameworks for improving the situation in the field of digitalization of public administration in Montenegro. Also, some of the strategic goals in new strategies for digital transformation and public administration reform, which are in preparation, will address the topic of eDMS.

So far, the system has been used only in the part of office operations within each of the institutions, although it supports the functionality of electronic documents exchange between institutions. This option has been enabled from the very beginning, but only at the level of several ministries as well as at the level of exchange of documents with the Secretariat for Legislation for the purposes of publication in the Official Gazette of Montenegro.

2 .2. Technical assumptions

The eDMS system in the Government of Montenegro was implemented to integrate a custom-made web interface implemented in ASP.NET technology (Origami.net), Opentext Documentum Content Server as a repository and central segment the system, and installed supporting modules from the Opentext ECM group. In 2017, Open Text acquired the Documentum product group from Dell EMC, starting a new phase in the development of these platforms.

The structure of the eDMS system allows users, within their permissions on the system, to independently define business rules, operating procedures and procedures in accordance with their specific needs. The central module of the system is the Archive, containing all documents, objects and files and allowing reliable storage of archives of the institution in electronic form, as well as efficient search and access to desired documents and objects. This archive is designed to accommodate and store many documents and meets all relevant international standards related to this field.

In addition to this, the Documentum platform includes Trusted Content Services to resolve security situations that go beyond the authentication and authorization mechanisms, as needed by the application.

In terms of architecture, eDMS uses a three-tier (MVC) architecture, a modern technological trend in web-based software.

The eDMS solution is built on the following technologies:
Origami.net:

- HTML, Javascript, JSON, Ajax, ActiveX
- Silverlight (for advanced file upload),
- ASP.NET MVC2,
- Spring.NET,
- NHibernate.

Back-end components:

- EMC Documentum,
- Adlib Express Recognition Server OCR,
- Adlib Express Conversion Server.
- Microsoft and Oracle DB servers

The system is hosted in the Primary Data Center of the Ministry of Public Administration, Digital Society and Media.

The entire infrastructure is built on available private cloud virtualization resources with dual key components in order to ensure the high availability of key components of the system.

Users from line ministries can use the PKI infrastructure for user authentication only. All additional security management requirements are part of the software solution and managed internally through the Origami application and its integration with Documentum Content Server and, particularly, safe system resources of the Content Server that preserve the integrity of the content located in the repository. Since the integration with MS Active Directory, which is also a centralized common system used by all ministries in the Government of Montenegro, has been performed, logging in to eDMS is done using the same credentials as those intended for logging in to client computers. Such access is, of course, possible only if the user performs access from the network belonging to state bodies.

2.3. Usage

The implementation of the eDMS system in the institutions of the Government of Montenegro began in 2011 when the scope of implementation of the first phase was defined. This phase involved all ministries in the then Government and the Government's Secretariat General. Eight years later, the second phase included additional state bodies:

- Police Directorate
- Secretariat for Legislation
- Protector of Property and Legal Interests
- Human Resources Management Authority

At the time of writing, eDMS is used by a total of 16 institutions.

So far, the system has been used only in the part of office operations within each of the institutions, although it supports the functionality of electronic documents exchange between institutions. This option has been enabled from the very beginning, but only at the level of several ministries (Ministry of Public Administration, Ministry of Justice and Ministry of Economy), as well as at the level of exchange of documents with the Secretariat for Legislation, for the purposes of publication in the Official Gazette of Montenegro.

2.4. Conclusions and recommendations

Keeping in mind the adoption of the innovated Decree on office operations[9], which entered into force on January 1, 2020, and the Instruction on the manner of conducting office operations[10], the need for digitalization of office operations becomes the need of all institutions and bodies in local self-government units. To this end, the MPADSM organized an assessment of the needs of local self-government units regarding the use of electronic document management systems. Thanks to it, it was learned that in 40% of the total number of municipalities, there is a system in which electronic records of data or documents are kept, while the remaining municipalities do not have developed systems, meaning that they keep records in the traditional way using auxiliary log books in paper form.

Also, from their answers, it can be concluded that municipalities which do not have an information system of this type do have an awareness of the need to establish information systems that would digitize business processes. There is also a strong awareness of the benefits of the system already in use in ministries. Municipalities mostly cite technical and financial challenges when it comes to key reasons for the non-existence of such a system.

Recommendations:

1. Improve the functional and visual aspects of the eDMS system through partial or complete refactoring
2. Integrate eDMS and the new eGovernment portal, as well as other systems in public administration bodies whose workflow includes the exchange of documents
3. Promote the use of eDMS systems at the level of local self-government units
4. Build native mobile applications for eDMS
5. Promote eDMS as one of the tools for measuring efficiency and performance indicators

[9] "Official Gazette of Montenegro", No. 47/19
[10] "Official Gazette of Montenegro", No. 59/19

3. OTHER SHARED SYSTEMS AND SERVICES

By implementing shared (centralized) information systems in public administration, the establishment of the highest level of services for citizens and the economy is achieved. If institutions are focused only on their narrow and individual goals, data exchange and all other joint services will become secondary, and processes will become sub-optimal, which will reflect in the time the administration procedures take away from users and their satisfaction with public administration services. Montenegro has been committed to building shared systems for years, but the lack of financial resources, vision, and often the mentality of people who were not ready for digitalization have slowed down these processes.

Now that digital transformation has been set as one of the priorities in the Work Plan of the Government, it is the right time to accelerate the development of these systems again, above all:

1. Electronic Data Interchange System (JSERP)
2. Electronic Identification and Signature System (eID)
3. Electronic System for the Payment of Administrative Fees (NS-NAT)
4. Electronic document delivery system (e-Delivery)

4. Framework Action Plan

Based on the drawn conclusions, and in order to provide initial assistance in their implementation, an initial action, which can be used by the Ministry to define a framework to define detailed activities, is proposed below. This action plan can be expanded or changed in accordance with the Ministry's needs and strategies.

No.	Recommendation	Recommendation details	Expected objectives
1.	Reengineering of administrative procedures	a) Selecting 10-15 administrative procedures that have the greatest coverage in terms of target groups b) Conducting in-depth "as-is" analysis, which, among other things, includes the application of Business Process Modeling Notation or some other appropriate methodology, as well as activity-based analysis c) Conducting in-depth "to-be" analysis taking into account the so-called SMART criteria (Specific, Measurable, Attainable, Relevant, Time-bound), as well as the analysis of current legal solutions which could be obstacles to changes d) Conducting a GAP analysis with transition-related recommendations e) Creating a change management strategy that should support the changes in processes and provide sustainability f) Conducting training programs and allowing relevant actors to get acquainted with new roles in accordance with the recommended changes	Selected procedures are improved in accordance with appropriate methodologies. Decisions in the field of change management strategy are made. The process of change in organizational patterns in public administration started.
2.	Development of a new eGovernment portal	a) Development of project and development plans b) Development of a "source-to-target" dictionary and data migration plan from the aspect of changing the structure of the database c) Development of the system according to the established plan and functional specification	Technically improved eGovernment portal, which implements the principles from Recommendation 3, with the development of new modules and expansion/modification

		d) Development of unit and functional tests e) Migration of data from existing structures f) Putting the system into production g) Development of system documentation and user instructions h) Delivery of training to all users to prepare them for work on the new system, according to the training plan i) Establishing a model for maintaining a new information system in order to support stable operation, improve performance and functional extensions or legally-motivated extensions if the need arises	of the database so that it supports business processes in new functionalities. Contract on maintenance and continuous improvement of the system that covers at least 3 years is signed.
3.	Establishment of integrated policies (standards) for the creation and provision of electronic services and binding all public administration bodies to apply them with appropriate legal solutions	a) Establishment and promotion of "single point of contact" principles, i.e., access to all services through a single digital platform or single sign-on (SSO) b) Development of a model for the classification of services through life cycle events, especially those yet to be established on the new eGovernment portal c) Unification of service delivery procedures, which should be compatible with the reengineering of Objective 1 procedures. d) Implementation of the "once&only" principle, with the establishment of mechanisms for reporting problems every time the user is asked to submit a document that could be the subject of exchange between institutions e) establishing a “user engagement and citizen-driven” approach when designing and creating services	Standards for creating and providing services in public administration are established. Process monitoring with clear indicators of progress is established.
4.	Development of an advanced reporting system	a) Development of project and development plans b) Defining indicators relevant for business decision-making in the domain of service digitalization	Advanced reporting system developed. Contract on maintenance and continuous improvement of the

		c) Development of the system according to the established plan and functional specification d) Development of the integration layer e) Development of modules with automatic and manual data synchronization f) Development of unit and regression tests g) Putting the system into production h) Development of S2T dictionaries and user manuals i) Delivery of training to all users to prepare them for work on the new system, according to the training plan j) Establishing maintenance of the BI system in order to support stable operation	system that covers at least 3 years is signed.
5.	Improving the existing or developing a new system for receiving and analyzing feedback from users	a) Designing a model and developing an online feedback panel b) Putting humanoid robots in the use in facilities where public administration services are provided. Such places will be determined by means of an analysis whose task will be to identify the busiest service provision facilities. Attention must be paid to the multi-correlation of predictors. c) Upgrading the functionality of the new eGovernment portal with options for service evaluation d) Establishing a feedback system via mobile phones e) Installing Kiosk-feedback systems in the busiest locations in cities f) Establishment of a system of obtaining feedback from public administration employees in, because employees also have the opportunity to perceive services offered as citizens/users	A system for collecting feedback, or some of the proposed modalities, is developed. Contract on maintenance and continuous improvement of the system that covers at least 3 years is signed.

6.	Improving the functional and visual aspects of the eDMS system	a) Preparation of a feasibility study for potential improvements and definition of the refactoring project plan b) Development of the system according to the established plan and functional specification c) Putting the system into production d) Delivery of training to all users to prepare them for work on the new system, according to the training plan	The eDMS system improved in accordance with the findings of the feasibility study. A system for continuous improvement has been formed Training programs delivered.
7.	Integration of eDMS systems with other systems in public administration	a) Preparation of a feasibility study of potential integrations with other systems, with the analysis of technical and organizational perspectives, opportunities, constraints and risks b) Development of the project plan and technical documentation of the API after the decision on which integrations are justified c) Development of integration modules according to the established plan and functional specification d) Putting the system into production e) Delivery of training to all users to prepare them for work on the new system, according to the training plan	Integration of eDMS with other systems where procedures require the exchange of documents and in accordance with the findings of the feasibility study is completed.
8.	Promotion of the use of eDMS systems in local governments	a) Analysis of the necessary technical preconditions for the use of eDMS at the local level b) Development of a user acquisition plan c) Implementation of the system for local self-government units d) Putting into production e) Delivery of training to all users according to the training plan	eDMS system is in active use in all municipalities in Montenegro.
9.	Development of native mobile applications for eDMS	a) Analysis of required functionalities b) Analysis of security aspects	iOS and Android apps launched on Google Play and AppStore

		c) Analysis of preconditions in the context of identity verification d) Designing applications for iOS and Android platforms according to the principles of UX/UI design e) Prototype development and testing f) Application and API development g) Testing h) Putting the system into production i) Establishment of maintenance and upgrade systems	
10.	Promotion of eDMS as one of the tools for measuring efficiency and performance indicators	a) Designing and establishing a model for measuring employee performance according to eDMS data b) Promoting a change in organizational culture and habits while analyzing the process of receiving, signing, processing and closing requests, which may indicate the presence of "bottlenecks" in government organs c) Establishing an electronic system for monitoring and analyzing performance over time	A model for measuring efficiency and performance indicators over time is established. The sustainability of such a system is ensured