Development of the Business Continuity in the Information and Communication Branch (ICT) of the Judiciary

(This document name is: „Development of Business Continuity in ICT 2020 “, normal text font used is Arial 11, paragraph line spacing Single, 6 pt before and after)

Miodrag Perisic, MSEE, ICT Expert, “Support to the Justice Sector Reform” project

June 2020.

Funded by the European Union

Vladimir Polezhinovski, 22/12, Skopje,
Republic of North Macedonia
Team leader Dr. Deville: +389 (0) 70 22 40 44
E-mail: deville@planet.gr

Project implemented by NIRAS and its consortium partner Planet

Table of Contents

Abbreviations:

ICT	Information and Communications Technology
PO	Prosecution office
ITIL	formerly an acronym for Information Technology Infrastructure Library, is a set of detailed practices for ICT service management (ITSM) that focuses on aligning ICT services with the needs of business.
ACCMIS	Current Automated Courts Case Management Information System, as implemented in all courts in North Macedonia
HW	Computer systems hardware, equipment used to perform IT activities
SW	Computer systems software, programs, applications and various utilities, run on hardware
IPMS	Integrated Penitentiary Information System, used in all prisons and jails in the country
Help Desk/Support	system providing help to both computer system users and ICT staff
CIO	Chief Information Officer, top managerial position in an organization, responsible for all information services, storage and safety
"matrix" reporting structure	reporting structure in an organization, where some persons have more than one point above them to report to
ever greening process	a process of periodic replacement of ICT equipment, where each year a fixed percentage of HW is replaced with the new one, usually 20-25%
Server	a HW-based device, with processor, memory and storage, used for various computer processing functions, stored in racks with many connected servers inside

Executive Summary

This document, when completed, should become a part of the collection of different documents, proposals and frameworks, provided as the results of the specification of the Requested Services within the Terms of Reference (ToR), for the Component 3 (ICT) of the project "Support to the Justice Sector Reform"

This document, in this latest version dated June 2020, has been completed using all comments, additions and changes as proposed in the meantime by the members of the ICT Council, and as such is considered final and ready for adoption by the ICT Council.

The document has been initially designed by the project consultant, ICT Expert, after which it has been shared with a number of ICT staff across the country, distinguished members of the ICT community both at the courts and prosecution offices, who provided additional, specific comments and details, to make it fully applicable and in line with the current situation in these organizations and their future needs and possible ICT-related directions.

Besides this, the document also took into account previously expressed opinions and suggestions, as documented in the report on the Open Space training, which took part in Skopje, by end January 2020, and included over 20 representative ICT staff from various courts and prosecution offices in North Macedonia (see later for more details)

This document is presenting a proposal for to the implementation of the Business Continuity Plan within the Information and Communication branch of the North Macedonia judiciary, adjusted to the specific situation in North Macedonia justice institutions, such as the courts and prosecution offices. Wherever possible or applicable, short notes are inserted, with specific comments on situation with these institutions.

Towards the end, a specific set of measures to be taken in North Macedonia justice organizations will be proposed, based on inputs provided by the ICT Council and wider ICT community in these organizations.

1. Introduction and Definitions

Results of the polling of opinions at the ICT Open Space training

At the Open Space Training session, which our project has organized by end January 2020, for the ICT Council members and other ICT staff from various judicial institutions in North Macedonia, the attendants have been asked to provide their opinions on necessary priority actions and initiatives on several topics. In regards to the topic "ICT Organization" these were their contributions:

1. Electronic exchange of information between various institutions within the system (current issues, activities, etc.); at the moment, this is done only at the meetings of the Working Group for the Standardization of Courts Procedures, every 2-3 months;
2. Systematization & documenting of all ICT activities;
3. Creation of Help Desk/Support system for all ICT staff, for easy, available method of exchanging experience and resolving common issues (now, the only local tool is IT Forum (Bitola));
4. Definition and establishment of clear ICT hierarchy within judiciary, responsibility and area of competence at every level, creating efficient communication processes (new organization);
5. Centralized, long-term planning of all ICT needs;
6. Ensure minimum annual, compulsory ICT (certified) training for all ICT staff;
7. Justice ICT organization structure – to be clearly established, according to the best efficiency principle.

We think it is important to take these proposals into consideration, when recommending solutions for the Business Continuity in the Information and Communication Branch (ICT) of the Judiciary, using them to achieve the best possible effects.

Risk Management

Business processes are increasingly linked together via information and communication technology. This is accompanied by increases in the complexity of the technical systems and with a growing dependence on the correct operations of the technology (BSI Standard 100-2: 2005) [IT Grundshutz].

Through an organisation's Risk Management process it is likely that continuity risks will be identified. These risks can be managed to reduce their likelihood and/or impact, but it may be necessary to have plans in place to deal with the effects of the risk should it occur.

Business Continuity is the term applied to the series of management processes and integrated plans that maintain the continuity of the critical processes of an organisation, should a disruptive event take place which impacts the ability of the organisation to continue to provide its key services. ICT systems and electronic data are crucial components of the processes and their protection and timely return is of paramount importance.

Business Continuity (BC) is now recognised as an integral part of good management practice and corporate governance.[1]

If we are to take the phrase "business continuity" for its surface value, the most obvious meaning would be the ability of the business or enterprise to continue operating as a going concern for a very long time. But the term actually means more than what the words literally mean.

Business Continuity Management (BCM)

The International Organization for Standardization, in ISO 22300, defined "business continuity" as the capability of an organization to continue the delivery of its products or services, at acceptable predefined levels, following a disruptive incident. It implies the responsibility of the business owners and management for the business in ensuring that it stays afloat and "on course" despite any obstacles or stumbling blocks it encounters along the way. This responsibility is incorporated into the greater management process of the business, and what is also referred to as "Business Continuity Management" or BCM.

BCM is clearly described by the ISO to provide a framework for building organizational resilience, which will allow the organization to respond accordingly, in a way that protects the business, its reputation, and all other stakeholders. As a management process, BCM involves several **key activities**:

- Identification and analysis of key products and services of the business
- Identification and analysis of the most urgent activities and processes of the business
- Identification of potential threats, and their impacts to business operations
- Devising of plans and strategies for quick and effective recovery from any disruption, and the continuation of business operations

[1] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-plan/it-service-continuity-plan

IT Service Continuity Management (ITSCM)

A number of frameworks in this area identify a purely IT aspect of BCM referred to as IT Service Continuity. IT Service Continuity Management (ITSCM) is a discipline which has evolved from IT Disaster Recovery (ITDR) but is more customer-centric. The paradigm is similar, but the underlying assumptions made by ICT as to priorities, timescales and important components are replaced with accurate data from the business units. ITSCM is the control which transforms ICT into a pro-active service organisation, meeting the needs of its customers, understanding their requirements and fulfilling these requirements. In the event of an incident the plans and systems in place should ensure a resumption of service within the agreed Service Level Agreements (SLAs) ensuring compliance and customer satisfaction as well as aiding in Business Continuity.

The Information Technology Service Business Continuity Plan is the collection of policies, standards, procedures and tools through which organisations not only improve their ability to respond when major system failures occur, but also improve their resilience to major incidents, ensuring that critical systems and services do not fail or that failures are recovered within acceptable process.

The recovery plans are organised in a hierarchy. A site loss plan details the systems which would be affected by the loss of a building. A separate plan for each service should provide detailed procedures and step-by-step guidelines for each stage of an incident so that the Recovery Teams are able to restore the services and thereby to meet the agreed process and component RTOs.

The plans should be clear and concise and expect a level of knowledge but not presume explicit local knowledge, in the event that external assistance is required to rebuild systems (the same is true of Disaster Recovery Plans)[2]. Each procedure should be self-contained so that it can be utilised to effect recovery of a single system or component (e.g. the server is running successfully but the database management system has crashed). Each document must also contain details of pre-requisites; this means that in the event of multiple component failures the correct sequence can be followed (e.g. replace failed disk, rebuild operating system, install database, configure security settings and then restore data).

In summary, the IT Service Continuity Plan should typically contain the following information:

- Details of the combined component RTOs and RPOs and inclusion of the IT Requirements Gap Analysis

---

[2] These issues and overlaps are being addressed in the latest standards and frameworks but this evolves into a complex web of procedures and policies e.g. ITIL [ITIL] is a Framework for Information Technology (IT) infrastructure with v2 being divided into 9 areas; while the idea is to utilise the areas relevant to the organisation, the existence of relationships among the areas means that taking one and not another could create deficiencies. This is also reflected in standards, where the relationships are now starting to be defined. For example, PAS 77 IT Service Continuity Management [PAS 77] acknowledges the need for Business Continuity Management (BCM) before IT Services Continuity (ITSC) plans can be developed. It also states that if there is no BC in place then a subset of the Business Impact Analysis (BIA) must be completed in order to understand the business requirements and to align IT services to business requirements.

Emerging standards (and existing ones which are evolving) reflect their roots and so the target audience for each must be known to best understand their basis. The American standard NFPA 1600 comes from the National Fire Protection Association [NFPA] and is the standard on Disaster and Emergency Management and Business Continuity Programs. Early versions are more about saving the environment than IT but the latest version (2007) moves towards BC. This contrasts with BS 25999-1, which was written purely as a BC standard to enable businesses to recover from incidents ranging from minor (outage of a few hours) to a major incident requiring relocation of services [BS 25999-1].

https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience

- IT Architecture
- Roles and Responsibilities
- Invocation Procedures
- Damage Assessment
- Escalation and process flow charts
- Detailed procedures specifying how to recover each component of the IT system
- Test Plans specifying how to test that each component has been recovered successfully
- Incident Logs
- Contact Details
- Fail-back procedures
- IT Test Plan

These plans detail the four stages:

- **Initial response:** damage assessment and invocation of the appropriate incident management teams.
- **Service recovery:** this may be staged and offer a degraded service.
- **Service delivery in abnormal circumstances:** interim measures may include relocation of services to another site or utilisation of spare equipment (often training or test servers). This is a temporary measure to provide a limited service until normal service can be resumed.
- **Normal service resumption:** returning to the usual service, fail-back from the abnormal service delivery.

Business Continuity Planning

In recognition of the reality of the economic and business landscape being unpredictable and volatile, businesses are now taking a lot of precautions to ensure that their operations will still stand a chance against unexpected disruptions. We usually hear of these precautions in the form of disaster recovery planning, which is primarily focused on the restoration of a firm's IT infrastructure and IT operations. This view is rather limited, when you look at the bigger picture, since a business and its operations are more than just its IT infrastructure.

Thus, more attention is put on business continuity planning (BCP), which puts the company in a proactive position in planning how to ensure that it will still be able to deliver its critical products and services safely and smoothly, while meeting its legal, regulatory, and other obligations.

We can probably enumerate more than a dozen reasons why businesses should create and maintain BCP initiatives but, at the end of the day, there is only one ultimate goal or purpose for it, and that is to help ensure that the organization, business or company has the required resources, information, and capabilities to deal with emergencies and similar unexpected events, particularly their aftermath.

Benefits of Business Continuity Planning

You will probably be able to appreciate BCP even more if you have a clearer idea of what the business can gain from it.

- **BCP improves public perception and acceptance of the organization**. By displaying a proactive attitude and demonstrating the initiative to be well-prepared, users and the general public will have a favorable and positive impression of the organization. This will lead to a certain level of trust, which is likely to convert them into loyal, *trusting*, customers.

- **BCP will boost staff morale and command their loyalty to the organization**. Employees are inclined to seek stability in the organization they belong to, and a solid BCP is one way for management to give them the assurance that they are looking for. It will also give them pride in their work and motivate them to increase their productivity as members of the organization.
- **BCP enhances the relationship of the organization with other stakeholders**. Stakeholders, including the top government officials, will trust the organization enough to encourage them to keep assigning substantial budget funds, if they know that every effort to be prepared for the unexpected is made.
- **BCP improves the overall efficiency of the organization**. In the event that a crisis does arise, resulting to a disruption in operations, having a solid BCP will allow the organization to respond quickly and appropriately, keeping losses and costs to a minimum because there is already a plan in place.

Threats to Business Continuity

Risks are inherent in businesses, and the risk of being faced with potential disasters and disruptive emergencies is one of them. What are some examples of these potential risks or threats?

- **Natural disasters** (*force majeure*, or “acts of God”), such as hurricanes or typhoons, storm surges or *tsunamis*, floods, earthquakes, bushfires, blizzards, sandstorms
- **Man-made disasters** with environmental repercussions, such as oil spills, hazardous materials spills, pollution, improper disposal of chemical and other industrial wastes
- **Accidents** brought about by fortuitous events, such as fires and similar incidents in the workplace
- **Failure of utility** and other similar service providers to deliver their services, such as when power and energy providers shut down, water services are interrupted, and communication lines go out of order
- **Results of sabotage** and similar crimes (with the intention of putting the business at risk), such as arson,
- **Cybersecurity attacks**, with the information system falling prey to hacker and other similar intrusive activities

All these threats must be taken seriously, considering their various effects or impacts when they result in the disruption of business operations.

2. Steps in Developing Business Continuity Plan

Before you can get down to writing The Plan, there are several steps that must be performed.

Step 1: Identify the scope of The Plan.

As in most business planning processes, the first thing that must be done is to define the scope and objectives of the plan being made. In this case, it is the Business Continuity Plan (BCP).

In addition, there is also a need to define the assumptions that will prevail in the conduct of BCP. It is also during this phase that budgeting is conducted, with the initial program budget taking into consideration the expenses that may be incurred in the process of developing the plan. These include costs of research, trainings and seminars, and other services sought in the process of moving the plan along.

Step 2: Form your business continuity team.

There is a need to establish a governance structure within the BCP in order for management to have order and control in its conduct. This implies care and prudence in choosing the people who will be assigned the task of planning for the continuity of the business.

Usually, there is a representative for every critical process or function, as well as support processes or functions.

There is no limit to how many people should comprise the business continuity team or committee. A team could have only five people on board, or it could have as much as 20 or even 30 members. The number of people and the size of the team will largely depend on the nature of the business and the size and scale of its operations.

Step 3: Conduct a Business Impact Analysis (BIA)

Conducting a BIA is crucial since its results will be the major input in business continuity planning. Through BIA, the team will be able to predict or forecast the potential impacts or consequences of business operations. It will also aid the team in gathering information that will be helpful when it comes to developing strategies that can be adopted by the company for its recovery from the crisis.

Briefly, let us take a look at the core concerns of BIA:

- **Key business areas**, or the core operations of the business;
- **Functions and processes** of the business that are considered critical and/or time-sensitive;
- The **resources** required to ensure the continuity of these key business areas and critical processes and functions;
- The **dependencies** (and interdependencies) between and among the business areas and functions or processes;
- The acceptable or **tolerable downtimes** for each critical process or function

The BIA will facilitate the prioritization of critical processes and functions (or critical products and services) of the company, so management will have a clearer idea on which areas need more resource allocation in case of an emergency. Usually, estimates and approximations are made with respect to financial variables, such as lost revenues, additional costs, and other possible losses.

Step 4: Strategizing and Planning

Based on the results of BIA, the team will then identify response and recovery strategies and plans to address the effects of the disruption, and present them in detail. It is in this phase where the team will provide details on the arrangements and measures that the company will undertake in order to mitigate threats and risks.

For every critical function, process, service, or product, there should be corresponding continuity responses, measures or plans. Cost estimates should also be included. That is how detailed this phase should be.

It should also talk about the readiness procedures that must be implemented, and how they will be implemented.

Step 5: Compilation and Documentation

This involves the writing of the Business Continuity Plan. Usually, there will be a first draft, since the succeeding steps involve testing the recovery plans and strategies, making adjustments and re-testing until such time that The Plan can be finalized.

Also, it is important to note that BCP is an ongoing process. That means that The Plan must be tested frequently, and updated when necessary. Thus, The Plan is subject to changes, as applicable.

Step 6: Implementation and Testing

The prevention and mitigation strategies formulated in Step 4 will now be implemented. This involves communication of the plan to all members of the organization, making them aware of their part in it. This involves training them on their roles if the event does happen. External stakeholders should also be made aware of the plan.

The emergency response and recovery strategies will undergo testing, mostly through drills and scenario exercises that will require the participation of the concerned employees or members of the organization. Through testing, the business continuity team will be able to assess whether the plan will be effective or not. This is their opportunity to make the necessary adjustments and corrections.

Testing and evaluation must be done periodically in order to take into account the ever-changing nature of businesses.

Step 7: Adjustments and Improvements

The program may need to be adjusted due to the following:

- Evaluation and testing of the strategies may reveal that they are ineffective or inefficient
- There may be deficiencies in the strategies
- Some roles and responsibilities are vague and need clarification
- Change in the roles and members of the business continuity team
- Introduction or occurrence of new or additional factors or circumstances, such as new equipment, opening of a new branch, relocation of operations, and new technology or system that modified critical processes.

Since testing and evaluations are done periodically, there is an equal chance that the program has to be adjusted several times. It follows that the Business Continuity Plan will have to be rewritten to accommodate or reflect these adjustments.

3. Writing the Business Continuity Plan

After performing the first three steps mentioned above, you are now ready to compile and document your business continuity planning activities in the Business Continuity Plan, modifying it for finalization purposes after testing and audit. Basically, everything that you performed in BCM will be documented in The Plan.

Depending on the nature of the business, The Plan may have special features or additional parts. But generally, a Business Continuity Plan has the following sections:

1. Program Administration

Usually, this comes in the form of a Mission Statement which contains the following:

- The purpose of the plan, stated to benefit and involve the organization as a whole and not in parts
- The scope, goals and objectives of the organization's BCP
- The methods of evaluation that will be employed
- The budget, specifically the anticipated and estimated costs that will be required
- Other resource requirements
- Anticipated timeline of the conduct of BCP
- Compliance with any relevant legal and/or regulatory requirements

North Macedonia Judiciary Specifics (Program Administration):

Some specific comments and suggestions regarding situation with this theme are entered here, provided by some of the North Macedonia ICT staff at courts:

The plan for the business continuity for the services in the field of ICT is a set of policies, standards, procedures and tools, out of which the following are the rules and procedures already adopted by the highest management of the institutions and they are applied in the North Macedonia judicial system. With some additional processing and adjustments, depending on the needs, they could be used in the preparation of the plan for continuity in business operations.

In accordance with the obligations provided by the Law on Personal Data Protection, all courts have prepared the following acts, approved by the Directorate for Personal Data Protection, basically stating that according to its content they are in accordance with the existing regulations:

1. Rulebook on technical and organizational measures for ensuring confidentiality and protection of personal data processing
2. Rulebook on the manner of performing video surveillance
3. Procedure for the process of making a security copy, its archiving and storage, as well as for the return of the stored personal data
4. Procedure for the process of destruction of documents, as well as for the destruction, deletion and cleaning of the media
5. Procedure for the reporting, reacting and repairing incidents
6. Procedure for determining the obligations and responsibilities of the court clerk-ICT staff, who administers the information system

Every three years, the Directorate for Personal Data Protection performs regular inspections in all courts, after which it submits to the courts a decision on possible established violations, with the obligation to take actions and activities to remove them within the given deadline, otherwise fines follow.

Each court is obliged to conduct an annual internal audit of the work of the judicial ICT officer, who administers the information system as well as to check the registration of the authorized access and the authorized persons when accessing the cases, for which he prepares a report containing possible established irregularities and the proposed measures for their removal.

It is especially important to point out that during the preparation for the fulfillment of the envisaged obligations with the Law on Personal Data Protection, trainings and workshops were organized with the presence of representatives of the Directorate for Personal Data Protection who gave directions, prepared templates for preparation of the necessary documentation, etc.

The Supreme Court, the Judicial Council and the four appellate courts have ISO 9001: 2015 certifications, within which additional procedures in the field of ICT have been prepared and adopted by the top management.

Specifically, at the Supreme Court, the following ICT-related procedures have been adopted and are being applied:

1. Procedure for access to the premises where the ICT systems are located
2. Procedure for participation, elaboration and monitoring of ICT projects for the courts of the Republic of Macedonia and the Judicial Council of the Republic of Macedonia
3. Procedure for the maintenance of ICT projects and coordination with IT departments in the courts of the Republic of Macedonia and the Judicial Council of the Republic of Macedonia
4. Central nomenclature update procedure
5. Procedure for installation, configuration, administration, monitoring and maintenance of the ICT systems in Supreme Court (SC)
6. Procedure for use, upgrade and renewal of the ICT systems in SC
7. Procedure for reporting, reacting and repairing an ICT incident
8. Procedure for creating and managing backups
9. Internet and e-mail use security procedures
10. Procedure for granting user privileges

Once a year, internal and external control is performed by an authorized company in order to determine possible inconsistencies, after the removal of which follows the extension of the certificate for the next year.

Adopted procedures are continuously supplemented and changed depending on the needs and problems that arise.

It is important to note that during the ISO certification process, an authorized company was hired to conduct training, provide guidance, develop the necessary documentation and manage the overall certification process.

The following is a list of identified risks in the judicial system of RSM:

1. Lack of sufficient number of professional IT staff employed in the Center for Informatics of the Supreme Court (SC). Due to the specifics of the work performed, these jobs should be filled with professional and properly educated IT persons.
2. Lack of appropriate and continuous education in authorized educational centers of IT persons employed in the judicial system of RSM
3. Lack of additional (backup) internet links (in case of a drop in the internet link, to continue the functionality of the ICT systems)
4. Lack of disaster recovery site according to the model active - active
5. Lack of High-availability clusters at the level of each court
6. Lack of timely and continuous HW and SW upgrade or renewal according to the depreciation period or after the end of the life cycle
7. Lack of workstations for newly hired court clerks
8. Lack of appropriate equipment and software for centralized monitoring of all servers in SC and all servers in the courts of RSM
9. The lack of service by an authorized company for storage of media with security copies for SC in a remote location, for the other courts is provided dislocated storage of unsupported data in the Center for Informatics of SC
10. Lack of training to raise security awareness among all employees
11. Lack of appropriate and / or timely information in regards to: possible physical access of an unauthorized person to the ICT equipment, possible problem or an ICT incident occurred
12. Insufficient observance of all security aspects when using the given authorizations to work with the ACMIS system
13. Insufficient compliance with security rules by Internet and Email users

The goals of BCP/ ITSBCP will be to increase the efficiency, transparency and accountability of information systems in the judiciary, to increase accessibility, timeliness and ease of use of judicial services for all users, to improve data quality and to ensure the smooth operation of a centralized IT system as a whole.

To make a functional analysis and assessment of possible risks (which are already provided in the ISO documentation in the judicial institutions where this certificate is implemented) by defining the degree of each of the risks, the probability of their occurrence as well as regular monitoring and updating of the table with potential risks.

"The Information Technology Service Business Continuity Plan is the collection of policies, standards, procedures and tools" (page 2)

We can talk about one general BCP only as an ITSBCP, with emphasis on the most important Disaster recovery procedures in case of: data loss, server and network failures, security attacks…

All existing ISO procedures with defined strategic goals and risks, other internal procedures and lot of other acts should be processed and adapted, according to the rules of proposed ITSCM, taking care of compatibility with the Court Rules of Procedure and other legally prescribed rules.

Parallel existence and continuous maintenance of two (or more) independent systems – ISO and ITSBCP would be pointless.

2. Governance

This will detail the formation of the business continuity team. Emphasis must be placed on the following information:

- The **team members**, their titles or designations, as well as their roles and responsibilities as members of the BCP team. Include their contact details.
- The **lines of authority** and succession of management, clearly demonstrating the delegation of authority and accountabilities.
- **External entities** or organizations that the business will interact with in the conduct of BCP. They include vendors, distributors, contractors, suppliers, and the like.

Presentation of this section is reinforced by including an organizational or functional chart showing the lines and interconnections among the members of the team and external parties.

North Macedonia Judiciary Specifics (Governance):

The BCP in general must include list of external suppliers who have entered into a contract for the maintenance of hardware equipment with courts and for every supplier the exact delivery time of all spare hardware parts in case of hardware disaster should be precisely defined.

All possible plans are related to the existing central budget planning, led by the Judicial Budget Council.

For a lot of ICT problems and incidents the courts are dependent on higher instances and external entities, so most of the ICT planning in the courts is closely related to the centralized ICT planning.

Some specific comments and suggestions regarding situation with this theme are entered here, provided by some of the North Macedonia ICT responding staff:

Annually, the Supreme Court of the Republic of Northern Macedonia conducts centralized public procurement for the maintenance of the following ICT equipment intended for the needs of all courts:

- Maintaining the software for the ACMIS system in the courts, including all functional upgrades integrated in it
- Maintenance of ICT equipment and software solution for Web portals and their integration with ACMIS systems of all courts
- Maintenance of the system for precise air conditioning in the ICT system room of the Supreme Court of RSM where the entire ICT equipment for the court and parts for all courts of RSM are located
- Maintenance and software renewal of devices for protection of all courts of RSM
- Maintenance of ICT equipment, virtualization platform, operating systems, databases, Active Directory architecture, etc. intended for the functioning of the ACMIS system in all courts of RSM
- Maintenance of the system for centralized backup / restore intended for protection of the ACMIS databases of all courts of RSM
- Procurement of anti-virus and anti-spam licenses intended for all courts of RSM
- Maintenance of the e-mail system intended for the Supreme Court of RSM
- Maintaining the software for recording events by correcting logs from ICT devices located in the Supreme Court of RSM
- Maintenance of the system for uninterrupted power supply (UPS) located in the building of the Supreme Court of RSM

After concluding a maintenance agreement with a specific company, the SC Center for Informatics will notify the IT staff in the courts of the contact address of the help desk of such company, where they should apply for a problem or request help. In order to control the promptness and response time of the companies, a copy of the report of the problem as well as a copy of the undertaken activity is submitted to the e-mail account of the SC Center for Informatics.

The experiences so far are mostly positive in terms of the diligence and response of the companies. In case of malfunction of the entire server, the maintenance company replaces it with a backup server, while in case of malfunction of a hardware part, the company replaces it with a backup and additionally procures spare parts. In case of a serious problem with the system software, the companies in coordination with the support of the manufacturers and the court IT staff successfully overcome the problem and return the functionality as soon as possible.

Reporting a problem or seeking help from the company that maintains the ACMIS system takes place through a ticketing system so that IT staff in the courts have experience working with such a system.

3. Business Impact Analysis

Document all the results of the BIA conducted by the team. Again, be as detailed as you possibly can.

Results of any prior risk assessment procedures undertaken by the company should be included, as these will figure greatly in the conduct of BIA. By identifying the vulnerabilities of the company and their potential impact on its operations, the company will be able to determine its state of readiness and responsiveness in the event a disaster does happen that may cause disruptions.

Other points that must be highlighted in this section are:

- **Recovery Time Objectives (RTO) for business processes and functions**, in case of disruption. This is basically the estimate of the maximum duration or length of time that disrupted processes and functions must be recovered or restored, before the continuity of the business is seriously threatened.
- **Recovery Point Objective (RPO) for data restoration.** This is the maximum length of time in which data in an organization's IT infrastructure or database might be lost or inaccessible because of an emergency or disaster. When system designers and analysts are called in to work on recovery or restoration of data, they will know how much time they are given to accomplish that.

North Macedonia Judiciary Specifics (Business Impact Analysis):

Some specific comments and suggestions regarding situation with this theme are entered here, provided by some of the North Macedonia ICT responding staff:

In order to achieve the shortest possible down time, it is especially important when planning and purchasing the necessary ICT equipment to give preference to new technologies such as High-availability clusters, Disaster Recovery site according to the model active - active etc.

In the SC Center for Informatics, the ICT equipment on which the decision for Criminal Records is placed is configured as High-availability clusters, while Disaster Recovery site, reserve location is configured in the Basic Criminal Court and refers to the ICT equipment on which the solutions for Web portals and Electronic Delivery are located. In other courts, ICT equipment is outdated and lacks the stated capabilities.

This is top critical risk, so recovery time for processes and data restoration is very short. Thus, it is also important to estimate the time required to put the system back into operation in the event of a fall.

A procedure for retrieving data from backups should be described in detail, with precisely defined parameters for the performance of the returned data.

We must have efficient recovery plan, e.g. in case of this incident the future Central Case Management System must provide immediate full service delivery, until the recovery of normal services is completed.

This may suggest the existence of two physical servers, instead of just virtual ones, in every court, so that the second one can take over in case of the primary server failure! This measure could be possible with the upcoming massive purchase of new servers.

4. Business continuity strategies and requirements

All the plans, measures, procedures and arrangements, as well as the resources and other requirements to implement them, must be documented in this section, in great detail.

Take note that BCM is an ongoing process, which means planning strategies that will be employed before, during, and after a disruptive event.

Examples are **detailed strategies and resource requirements** for:

- Implementation and execution of **prevention and control strategies**, or the activities that will be undertaken before the event takes place. Examples are:
    - Installing physical protection facilities, systems and measures, such as emergency generators and storm shutters.

    - Diversification of resource providers and expanding the supply chain, maybe by looking for other alternative suppliers and vendors so as to not be entirely dependent on a single source.
    - Setting up off-site facilities as backups or alternates for servers, storage and warehousing, among other things (Disaster Recovery site)
- Implementation and execution of **emergency response strategies**, or the activities during the event. Examples of these emergency responses are:
    - Set up of an incident response command center
    - Evacuation procedures
    - Information dissemination to the media and the general public
    - Delivery of notifications and status updates to suppliers, vendors, distributors and customers
- Implementation and execution of **recovery strategies**, or activities after the event has taken place and efforts are made to resume operations. Example strategies are:
    - Relocation or transfer of operations to another geographical area
    - Alternative methods or processes, such as manual workarounds, or temporary methods employed or used by the company to facilitate the continuation of critical processes and functions in the absence of normal systems and personnel
    - Data restoration, especially when the company's information technology units received the brunt of the disruption.

North Macedonia Judiciary Specifics (Business Continuity Strategies and Requirements):

Some specific comments and suggestions regarding situation with this theme are entered here, provided by some of the North Macedonia ICT responding staff:

Regarding the prevention and control strategies, appropriate measures are taken within the possibilities:

- The building in which the Supreme Court is located is equipped with a generator and UPS devices, to which all of the ICT equipment located in the Supreme Court is connected.

- The server room located in the Supreme Court of RSM meets the prescribed standards for spatial, climatic, energy and safety conditions: area of over 50 m2, with no windows, double antistatic floor, independent power cables, professional redundant cooling system, metal door, magnetic card entry control only for IT staff and judicial police in case of unforeseen situations.

- In the other courts, the prescribed standards for spatial, climatic, energy and safety conditions are either fully or partially observed.

A Disaster Recovery team must be formed that will act quickly according to a pre-prepared plan in case of disaster. It is also important to provide Disaster Recovery site.

The server rooms are not fully equipped in all courts, but they are gradually being equipped in accordance with the funds provided by the Judicial Budget Council. *Where completed, server rooms' security is already at high level: metal door and antistatic floor, independent power cables, double air conditioning, locked, with court police and camera supervision, with court police controlled courts entrance.*

There are existing ISO procedures for: server room access control, physical protection and video supervision, records of persons entering the court…

Some Recovery strategies and testing environments are highly dependable of higher instances.

Although regulations do exist today prescribing these measures, in many cases there is not enough space in the server rooms, especially where more institutions are under same roof.

5. Training, Testing and Evaluation

With respect to Training, the Plan should include details of the following:

- Training program or curriculum that will be followed by the members of the business continuity team and the other members of the organization.
- Timeline or training schedule of the team members and other personnel

When evaluating the planned strategies, the following should be in The Plan as well:

- Testing procedures for the recovery and response strategies
- Testing schedule or timeline for the conduct of the procedures
- Forms and documents that will be used in the testing and evaluation
- Description and the finer details on the exercises that will be conducted

North Macedonia Judiciary Specifics (Training, Testing and Evaluation):

Pursuant to the obligations under the Law on Personal Data Protection (Procedure for the making a security copy, archiving and storage, as well as for the return of stored personal data), each court has the obligation to check the functionality of security copies for personal data reconstruction at least 2 - 4 times a year.

The courts in RSM are not able to check the functionality of the security copies because they do not have sufficient resources on the existing ICT equipment, nor do they have training to perform the said check which is not simple at all.

Only the Supreme Court most regularly performs either a check on the functionality of the backups or a real reconstruction of parts of the ICT system and restores the backed up data depending on the needs. In the past period, the SC Center for Informatics, in cooperation with the external company in charge of maintaining the equipment for the Criminal Record, performed a complete reconfiguration of it due to a logical disorder, restored the backed up data and re-established the functionality. For all performed checks or real data reconstruction, minutes are duly prepared in which the undertaken activities are noted and they are attached when regular inspections are performed by the Directorate for Personal Data Protection.

The plan must be tested in predefined schedule time, because it could be at risk during an actual emergency. Tests should be performed after prescribed disaster recovery actions taken to calculate the expected recovery time of the system or data, and to ensure that we will get the expected result.

Also, backups made according to currently applicable regulations should be tested in predefined schedule time to ensure consistency and functionality of data, as well as to determine the time for which this data would be returned to the system.

6. Program Maintenance

The Plan will also serve as a historical record or reference to trace how the business continuity management process went about. Thus, when writing about updates or adjustments made, there should be a reference on the deficiencies or issues that were addressed by the adjustments or corrective actions.

The Business Continuity Plan is essentially the Bible of the company during times of crisis or when it has to deal with the fallout of a disaster. Usually, people have trouble thinking straight during such major events and upheavals, and The Plan will serve as the guide that will steer the company in the right direction.

When writing a Business Continuity Plan, accuracy is of high importance, from the personal information of all individuals and entities involved to their roles and responsibilities. It should also remain relevant at all times, and that can be achieved by making sure that it is kept up to date. Finally, when writing The Plan, do it in such a way that it can be easily understood by everyone who reads it, from senior management to the lowliest employee in the organization. It won't be of any use if trying to make sense of what it written on it becomes a hardship.

North Macedonia Judiciary Specifics (Program Maintenance):

Some specific comments and suggestions regarding situation with this theme are entered here, provided by some of the North Macedonia ICT responding staff:

Business Continuity Plan (BCP) should be managed by the top court leadership (President, administrator), but because this plan refers to ICT content, ICT persons should be deeply involved in its creation and management.

Business continuity plan (BCP) which ensures contingency functioning, should be the result of the combined efforts of the President of the Court , Court Administrator and ICT leaders in the organization; it should also be maintained and constantly monitored by all key people involved in all processes, in order to maintain the BCP up to date. It is quite possible that most maintenance activities will become another set of mandatory voluminous duties, added to the already long list of ICT staff duties.

4. North Macedonia Specific Circumstances Summary

Considering the role that judiciary holds in every civilized society today, one must note the specific circumstances that planning and management of the ICT Business Continuity in North Macedonia judiciary must consider:

- As with other similar systems in the countries in transition within CEE, there is a lot of attention devoted by the EU to proper, efficient and independent functioning of the national judiciary systems, as key precondition for rule of law; this is clearly visible through a large number of high-value projects financed by EU in this area
- With today's role of ICT in providing the backbone of an efficient national judiciary, the ability of ICT to function uninterrupted under crisis caused by potential disasters and/or disruptive emergencies, becomes of paramount importance
- Thus, a properly planned, written and implemented Business Continuity Plan, including Disaster Recovery, can go a long way towards ensuring continuous operations of ICT in judiciary, as well as increase in confidence, both within the judiciary staff and judiciary clients (citizens, legal entities, etc.)
- Today, there are no crisis management plans for the basic courts, individually or collectively
- Relevant ISO standards education has been done only for appellate courts, not for the basic courts
- There are no specific procedures in case of crisis for the protection of personal data at the basic courts

5. Action Plan

This is the set of recommendations presented in the document, with further actions proposed:

ICT Council:

This document, which has already been expanded by using comments and suggestions collected from various ICT staff across the country, will be sent by our project to the ICT Council, for their further actions. We expect the ICT Council to proceed with the following actions:

a. Review the document, considering further extensions or improvements, in their next monthly meeting;

b. Assign one of the members as a rapporteur to manage the process of completing this document;

c. The ICT Council should, during its examination of this document, consider the Action Items as defined in the document, and their ramifications to the future ICT Strategy plans, as well as necessary changes to ICT Strategy, timing and financial needs;

d. Once this is done, the Council should include this document as part of the ICT strategy and send the completed document, together with proposed activities, timing and financial expectations, for further consideration to Ministry of Justice and other relevant bodies/institutions;

Recommended Process:

Considering all of the above, there seems to be a clear process on improvement of business continuity, both at the courts and at prosecution offices:

1. Constitution of the Business Continuity Management Team, at the level of Judicial Council or Supreme Court (for judiciary), or at the level of State Prosecution Office (prosecution);
2. The team should create appropriate plan for all institutions, as described in this text, with perhaps specific details for different types of institutions;
3. The plan should be the source for specific procedures, with clear assignments of duties;
4. In addition, control procedures must be designed, to provide a guaranty that the process will be respected and regularly tested;
5. Set of training courses should be established, and regularly repeated at the Judicial Academy premises;
6. Procedures and readiness must be regularly checked and reports to the governing body created based on these checks, in pre-determined time periods.
7. On top of this, please consider the “North Macedonia Judiciary Specifics” at the end of each chapter, for further, more detailed instructions.
8. The persons and/or institutions to be involved in the above plan are listed within these recommendations, for each element of the Business Continuity/Disaster Recovery Plans.
9. The costs of creating such plans are difficult to estimate, considering that they should be created both centrally and at each court, but they mostly contain the costs of time spent by the people in judiciary assigned to perform these actions.

Disaster Recovery Site:

As previously discussed with Mr. Jane Stojanov, Head of Telecommunication Sector at the Ministry of Internal Affairs (MIA), there exists a realistic opportunity for the North Macedonian justice ICT branch to establish its own Disaster Recovery site, within the perimeters of the MIA’s own, new disaster recovery facility, in the city of Prilep.

By November last year, this facility has already completed its Phase 1, the physical building and complete, redundant, dedicated power supply station; by this time, according to the project plan, Phase 2 should be completed, with full computer equipment data centre, divided into two separate spaces, with 42 racks to accept servers, drives and all communication and security equipment. One of these spaces is reserved for MIA, while the other is available to all other government departments (including potentially justice ICT equipment); some departments have

already booked space, such as Ministry of Finance, for its Revision, Public Income and Customs departments. The site should be fully completed and operational by July 2020.

The Ministry of Interior offers two models of financing these external users: one is basically “free of charge”, if the government agrees to take on its financing, while the other is subject to signed memorandum of Understanding, signed between MIA and the department requesting the use of the center.

This site is expected to be fully connected to the users in Skopje, using both microwave and high-speed optical connection, which is being currently built.

Addendum 1: Business Impact Analysis

Business Impact Analysis: Essential services/functions ranking

Service/business unit: _____

Areas affected and degree of influence:

Level of importance of essential ICT business service	Finance	Employees	Clients	Suppliers / business partners	Legal/ regulatory	Public/ community	Other	Total score (prioritize and draw up the list of services)

1 = weak negative influence ***10 = strong negative influence***