STANDARDS FOR OVERSIGHT AND BUSINESS CONTINUITY MANAGEMENT

National Bank of the
Republic of Macedonia

6 July 2017

10th Jubilee Conference on
Payments and Markets
Infrastructures

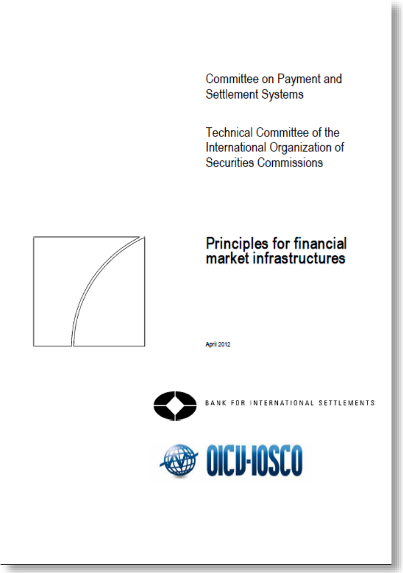
THE NBRM AND THE PFMIs

- National Bank of the Republic of Macedonia (the NBRM) has a statutory task to **establish, promote, register and oversee sound, safe and efficient payment, settlement and clearing systems**
- Committee on Payment and Settlement Systems of BIS and Technical Committee of IOSCO published Report on **Principles for financial market infrastructures** (PFMIs) in April 2012, which contain **24 principles** with standards for operation and oversight of the subjects of FMIs - payment systems, central securities depositories, securities settlement systems, central counterparties, trade repositories and **5 responsibilities** for the authorities, 18 principles applicable on payment systems, mandatory for SIPS
- The NBRM adopted the PFMIs standards and responsibilities in the bylaw regulation, following the ECB approach

- ECB's approach was also used for the **classification of the payment systems**, using the following criteria - financial impact, market share and other payment systems or securities settlement systems settle in the given payment system
- PFMIs contain **minimal set** of standards and are designed to be applied **holistically** and not on a stand-alone basis

STANDARDS

- The **main public policy objectives** are to enhance safety and efficiency in payment, clearing, settlement and recording arrangements, and more broadly, to limit systemic risk, foster transparency and financial stability, and provide guidance on identification, monitoring, mitigation and management of the full range of legal, credit, liquidity, general business, custody, investment and **operational risks**
- BIS-CPMI report **Cyber resilience in financial market infrastructures** specifies that cyber risk falls within domain of operational risk (Principle 17) and governance (Principle 2), FMIs should implement **robust business continuity plans** and consider a two-hour recovery time objective (2h-RTO)



Committee on Payment and Settlement Systems

Technical Committee of the International Organization of Securities Commissions

Principles for financial market infrastructures

April 2012

BANK FOR INTERNATIONAL SETTLEMENTS

OICU-IOSCO

- **Payment Systems Oversight Policy** is oversight framework that determines the main oversight objectives and scope, effective oversight principles, operation standards and methods, as well as reporting and transparency while overseeing payment systems
- **Decision on Criteria and Standards for Payment Systems Operations** defines classification methodology and criteria and lists the 18 PFMIs as Payment System Standards
- **Decision on the Manner and Methodology for Payment Systems Oversight** contains methodology on performing payment system oversight and actions on removing irregularities in the payment systems operations
- **Instructions for reporting by payment system operators** request reports on operational risks management, conducted tests on regular and back-up solutions and procedures, completed risk assessments and annual activity plan for the testing

OPERATIONAL RISK

- FMIs face **operational risk**, which is the risk that **deficiencies in information systems or internal processes, human errors, management failures or disruptions from external events** will result in the reduction, deterioration or breakdown of services
- Operational failures may lead to consequent delays, losses, liquidity problems, and in some cases **systemic risks**. They can reduce the effectiveness of measures that FMIs may take to manage risk, to complete settlement or monitor and manage their credit exposures
- Possible operational failures include errors or delays in processing, system outages, insufficient capacity, fraud and data loss and leakage
- Key consideration 2 of Principle 17 specifies that systems, operational policies, procedures, and controls should be reviewed, audited, and tested periodically and after significant changes
- Key consideration 6 of Principle 17 specifies that FMIs should have **business continuity plans** that will enable them to continue with the operation, even after events that cause major disruption. The plans should incorporate the use of a secondary site, should ensure that critical IT systems can resume operations within two hours following disruptive events, and enable the FMIs to complete settlement by the end of the day. FMIs should regularly test these arrangements

- More on business continuity management in the NBRM on the next slides...

Business Continuity Management Chronology

- ## 2001-2005
  - the National Bank has provided equipped offices and IT infrastructure on the reserve location in order to provide **information system continuity only**. On everyday basis, vital information from the primary information system was transferred to the information system on the reserve location, thus reducing the possibility for loss of information to maximum one day.
- ## 2005
  - the National Bank started **activities to provide continuity of the business processes in the bank as well.** The goal was to introduce a structural and regular process of planning, updating and testing of the activities and measures necessary for providing continuity of critical business processes, develop draft business continuity and disaster recovery policy,
  - for realization of the task, expert and technical assistance was provided within the Program for technical cooperation with the Central Bank of the Netherlands.
- ## 2006
  - the National Bank Council adopted the Business continuity policy, which sets the framework for efficient and coordinated activities for preserving the reputation and vital functions of the National Bank and determines the manner of providing business continuity in crisis situation.

Business Continuity Management Chronology

- the National Bank Council **established a Crisis center** as the highest management body in the NBRM during crisis,
- the Governor established **six Crisis groups** responsible for the organization of the operation in case of crisis,
- the Governor appointed a **Business Continuity Officer** competent for coordination of the process of implementation of BCP.

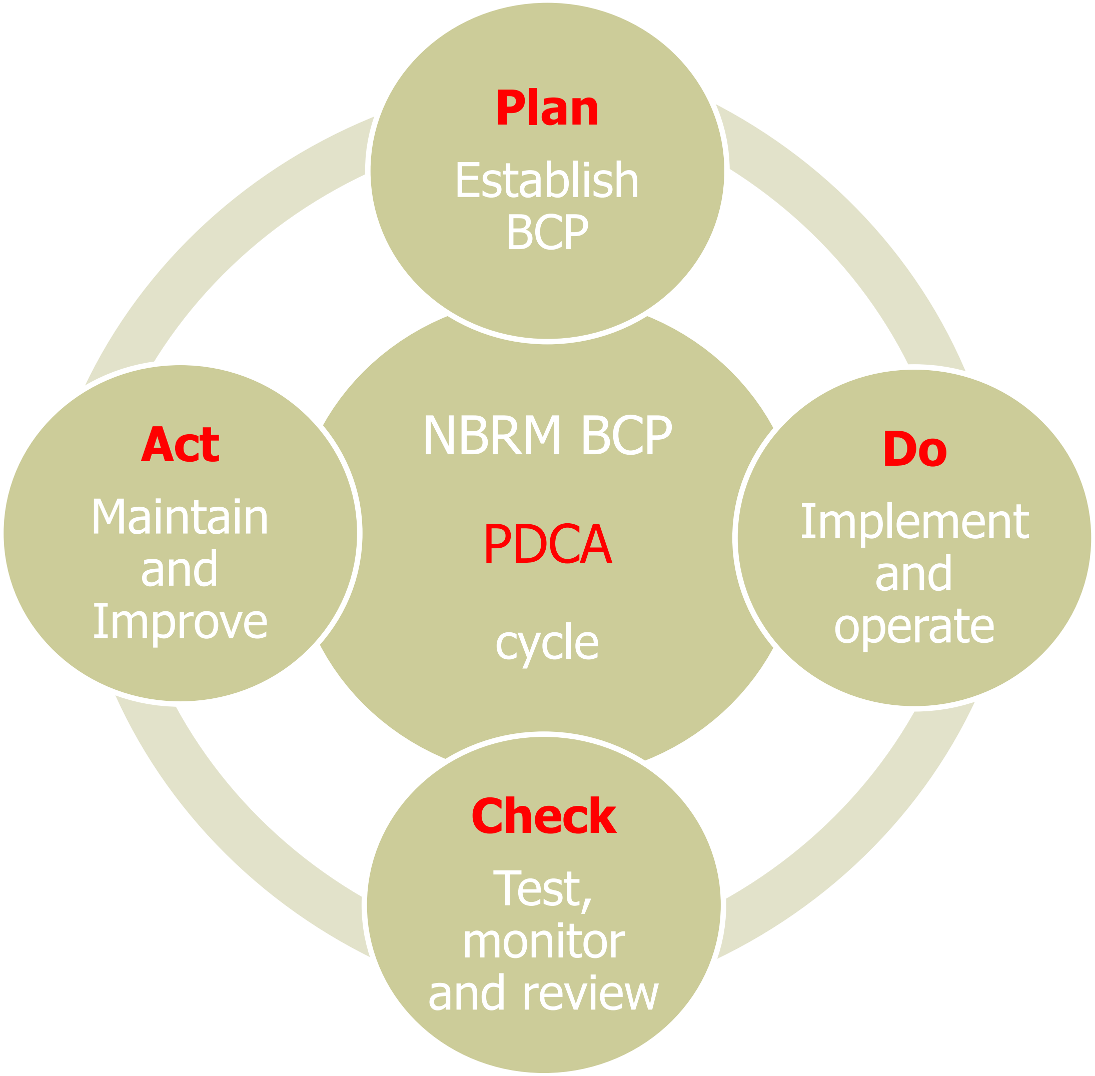
2007-2008

- uniformed standardized form for the contents of the individual plans for ensuring business processes continuity was developed, as well as an action plan for preparation of the business processes plans and their harmonization,
- **meetings**, **work-shops and seminars** from the area of business continuity were organized. All organizational units in the bank worked on the **preparation of Plans** for ensuring continuity of the business processes within their competence.

2009

- after mutual harmonization of the plans for ensuring continuity in individual business processes, a general **Business continuity plan of the National Bank was adopted**.

BCMSystem

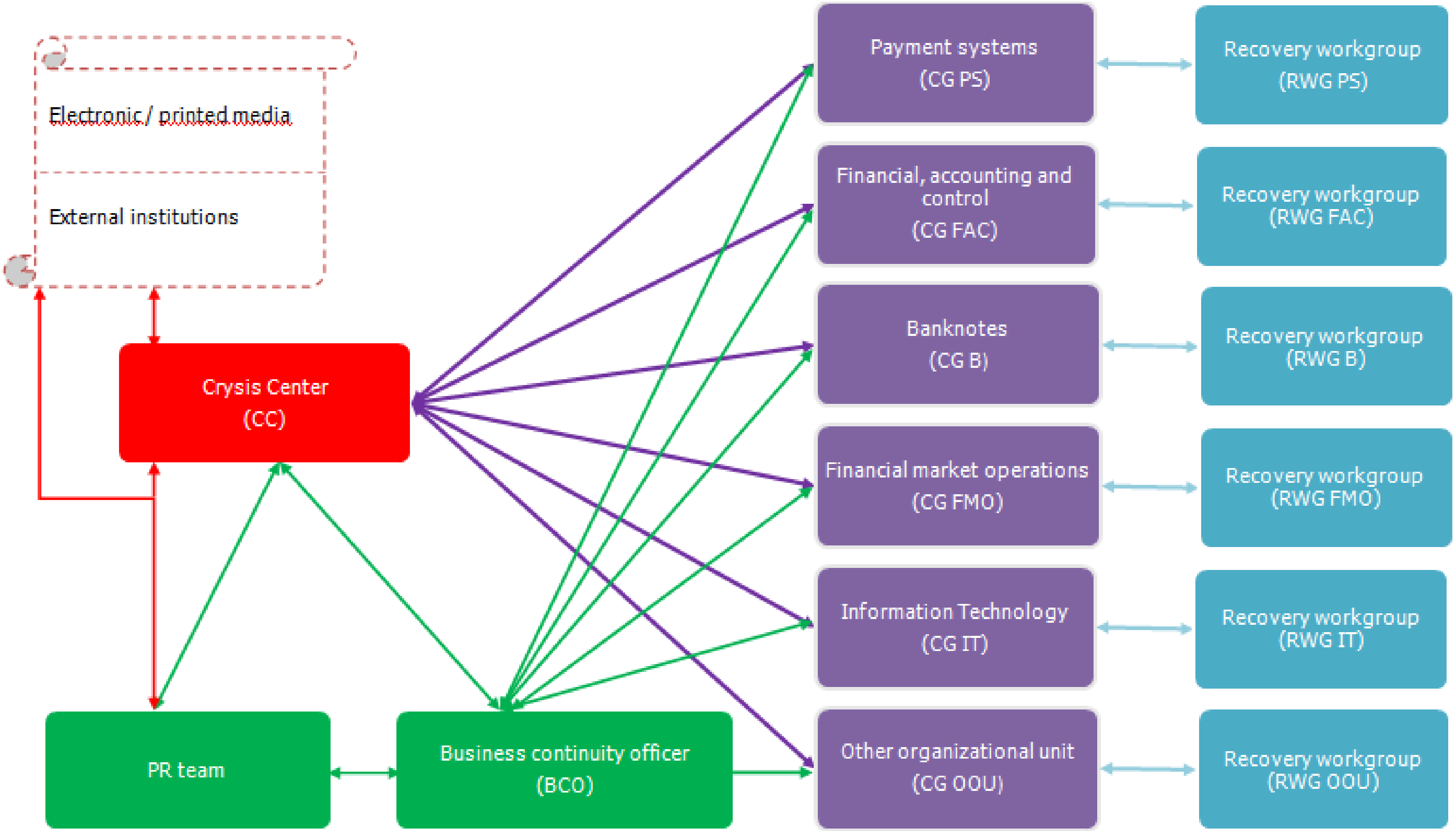


Plan - establish business continuity policy, targets, and plans in accordance with the NBRM objectives.
Do - implement and operate the business continuity policy & plans.
Check - test, monitor and report the results to management for review, determine and authorize actions for improvement.
Act - maintain and improve the BCMS by taking corrective and preventive actions, based on the results of testing, monitoring and management review.

Objective

- To preserve the reputation and the vital functions of the NBRM,
- To prevent a crisis or to mitigate its negative impacts;
- To provide protection and rescue of workers, personnel and visitors that are located in the premises of NBRM during the crisis situation, as well as protection of property, assets, values and data;
- To identify measures and actions for protection in case of immediate danger, rescue for the duration of the crisis situation and to eliminate the impact of the crisis situation;
- To establish conditions for normal execution of business processes in a reasonable timeframe.

Organization & communication



Contents of the BCPs

Each OU has a BC plan consisted of:

- business process risk analysis and determination of the maximum acceptable outage time,
- risk implications analysis,
- recovery plan in case of 4 crisis scenarios:
  a) Scenario no. 1 - "no building" - unavailability or inefficiency of the business premises of the primary location of the National Bank;
  b) Scenario no. 2 - "no computers" - work rooms are available but no accessible servers;
  c) Scenario no. 3 - "no network" - work rooms are available but the network infrastructure is unavailable (voice and / or data); and
  d) Scenario no. 4 - no sufficient staff.
- methods and measures for implementation of the plan,
- required number of employees that will be engaged in case of crisis and
- annexes to the plan that encompass data on the necessary fixed assets, small inventory, material, IT equipment, outsourcing services, contact lists etc. which will be inevitable for successful continuation of the operation in case of crisis.

Maximum outage time

The BC Plan determines five priorities for ensuring continuity of business processes with defined maximum acceptable outage time (MOT).

Priority	MOT	Processes
1	2-4 hours	28
2	1 day	10
3	2-3 days	9
4	4-7 days	5
5	8+ days	91
		143

In a crisis scenario no. 1 on the primary location of the NBRM, until the crisis situation passes, the **37** business processes with MOT 8+ will not be performed.

During imminent danger and immediately after the crisis situation arises, 7 processes (evacuation, property and persons protection, protection and rescue from fires, ruins and floods, first medical assistance, removal of the consequences and provision of transport services) will be carried out by a total of 82 persons;

During the crisis situation, the National Bank provides continuity in the operations for **99** business processes, which will be performed by a total of 185 persons in the:

- 3 reserve locations of the National Bank,
- domestic conditions or
- institutions that are subject to control by the National Bank.

RPO/RTO

- RPO - maximum targeted period in which data might be lost is a theoretical zero.

- RTO - the time frame for recovery of the RTGS and SWIFT services is a maximum of three (3) hours.

- RTO - the timeframe for recovery of all other information and communication services is a maximum of 1 (one) hour.

Update, training and testing BCPs

Updating and Training

On a regular basis, at least once a year heads of the CG and managers of OU’s are responsible for updating the BC plans and for providing training to the recovery workgroups.

BCP must be updated when significant changes in work processes are made or when new business process with priority 1, 2, 3 or 4 are introduced.

Testing

Managers of OU’s test the BC plans for business processes with a priority of 1 to 4 to

- assess their practical sustainability and enforceability;
- check the knowledge of the employees of the NBRM;
- assess possible improvement measures.

For business processes with priority 5, only the availability of vital records and other necessary resources are checked.

The Crisis Center adopts the plan for testing the continuity of business processes and it is an integral part of the Plan of Activities of the National Bank of the Republic of Macedonia for the following year.

Test approach

3 types of testing approaches are defined. All types of test can be performed in both announced and unannounced situations.

- **single business process test** - is focused on testing the continuity of the business process without the usage of required supporting means as staff and IT.

Desk test (walk through test)

The testers review the process and its logical steps on the correctness, clearness and availability of documentation and procedures that have to be used in performing the process. Part of this review will also be assessing the availability of the documentation on those locations that will be used in case the normal location isn't available.

- **single staff test** - is focused on testing the continuity measures that are only focused on staff without usage of other means like the IT, the office, etc.

Evacuation test

In order to test the orderliness of evacuations in case of disaster this evacuation test will be extended to the whole floor level and the level of the whole NBRM. Part of this test are the clearness and evacuation signals, the support of the evacuation by specific defined staff, testing whether all staff have been evacuated and arrived on the meeting location.

Connectivity test

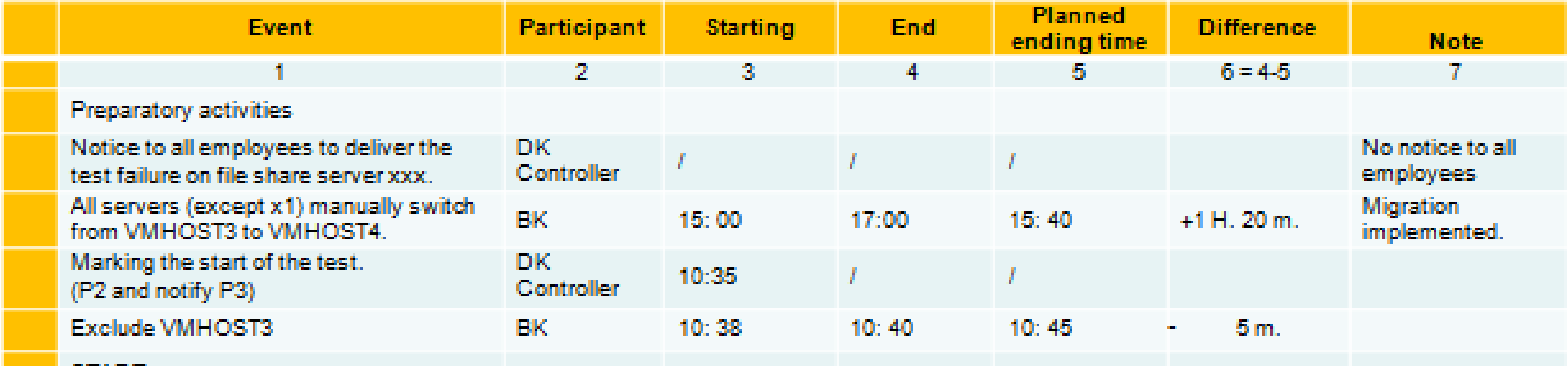
This test will be focused on the correctness and completeness of the contact lists, the contacting of the staff itself, the availability of the contact list and the knowledge regarding what they are required to do based on BC plans. Based on the way it is organised, connectivity test can be performed in call trees format or by one person.

Test approach

- **combined testing - includes staff and the supporting means**

  This kind of test can be performed for one or more interconnected processes, with a limited or wider scope, depending of the defined scenario.

Testing sample



	Event	Participant	Starting	End	Planned ending time	Difference	Note
	1	2	3	4	5	6 = 4-5	7
	Preparatory activities						
	Notice to all employees to deliver the test failure on file share server xxx.	DK Controller	/	/	/		No notice to all employees
	All servers (except x1) manually switch from VMHOST3 to VMHOST4.	BK	15: 00	17:00	15: 40	+1 H. 20 m.	Migration implemented.
	Marking the start of the test. (P2 and notify P3)	DK Controller	10:35	/	/		
	Exclude VMHOST3	BK	10: 38	10: 40	10: 45	- 5 m.	

TESTING REGISTER

No.	OU	Test ID	Test No.	Description	Date and time test begins	Date and time test ends	Result	Identified defencies	Measures for improvement	Deadline for applying measures for improvement
10	IT	IT001	1	Failure of file share server	11.11.2014 10:35:00	11.11.2014 11:45:00	successful	none	3 measures are determined for improvement. 2 of them are already implemented in the plan.	I quarter 2015
13	IT	IT002	2	Failure of the DW system (SQL Server service, SharePoint services for DW infrastructure)	13.08.2015 11:00	13.08.2015 11:45	successful	none	1 measure identified	IV quarter 2015

Test 2016

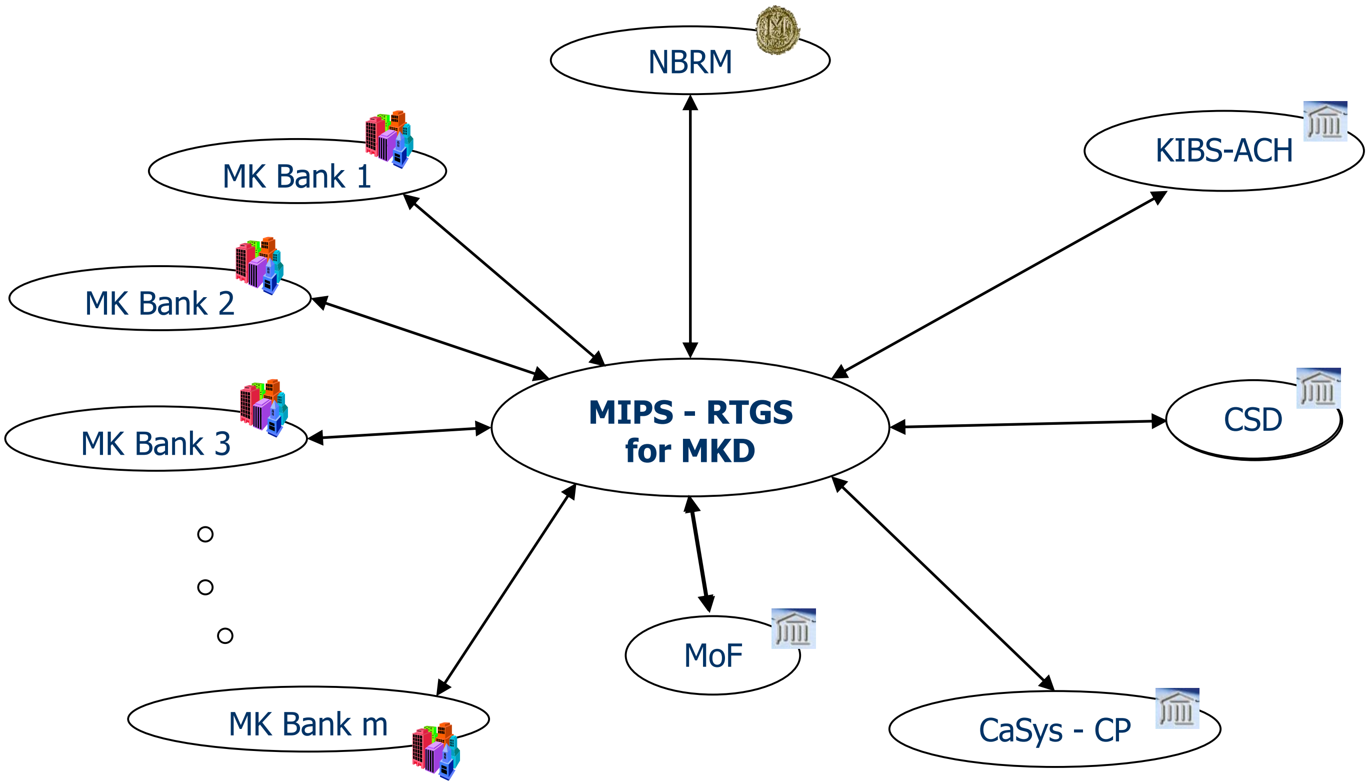
On 26.11.2016 (Saturday) – large scale testing was held.

The testing was conducted:

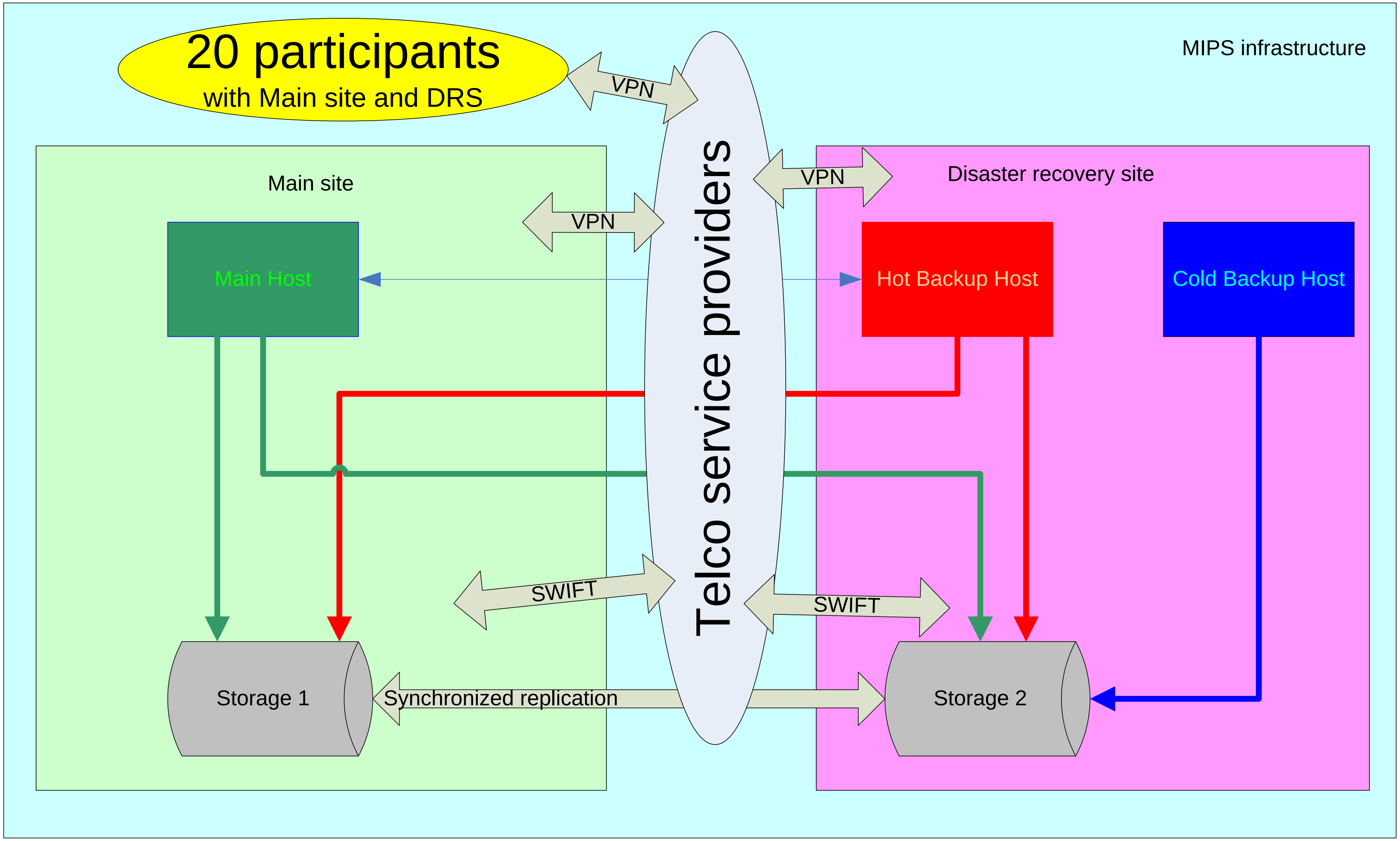
- for 15 critical work processes,
- under the responsibility of 6 organizational units,
- a total of 98 people participated in the testing:
    - NBRM - 42,
    - commercial banks - 53,
    - MF - 3
- test codename: ПС003-ФП002-ВСЛ002-ИТ005-ФСК001-ТООА002
- scenario:
    - the access to several streets and buildings in Skopje is blocked,
    - The primary locations of the NBRM and 2 largest banks are blocked, there is no possibility of access to them, the systems are non-functional and they continue their operations from their reserve locations,
    - The primary location of other banks are available and they continue to operate from their primary locations,
    - Due to technical problems in connection with the reserve location of the NBRM, the Ministry of Finance submits the payment orders on the magnetic medium. Also, until the functional system of the reserve location is established, one bank delivers the urgent payment orders of her large clients on a magnetic medium.

More about the organization of the test, test results and lessons learned – on the next slides…

Macedonian interbank payment system (MIPS) in 2016 as RTGS for Macedonian denar



MIPS infrastructure



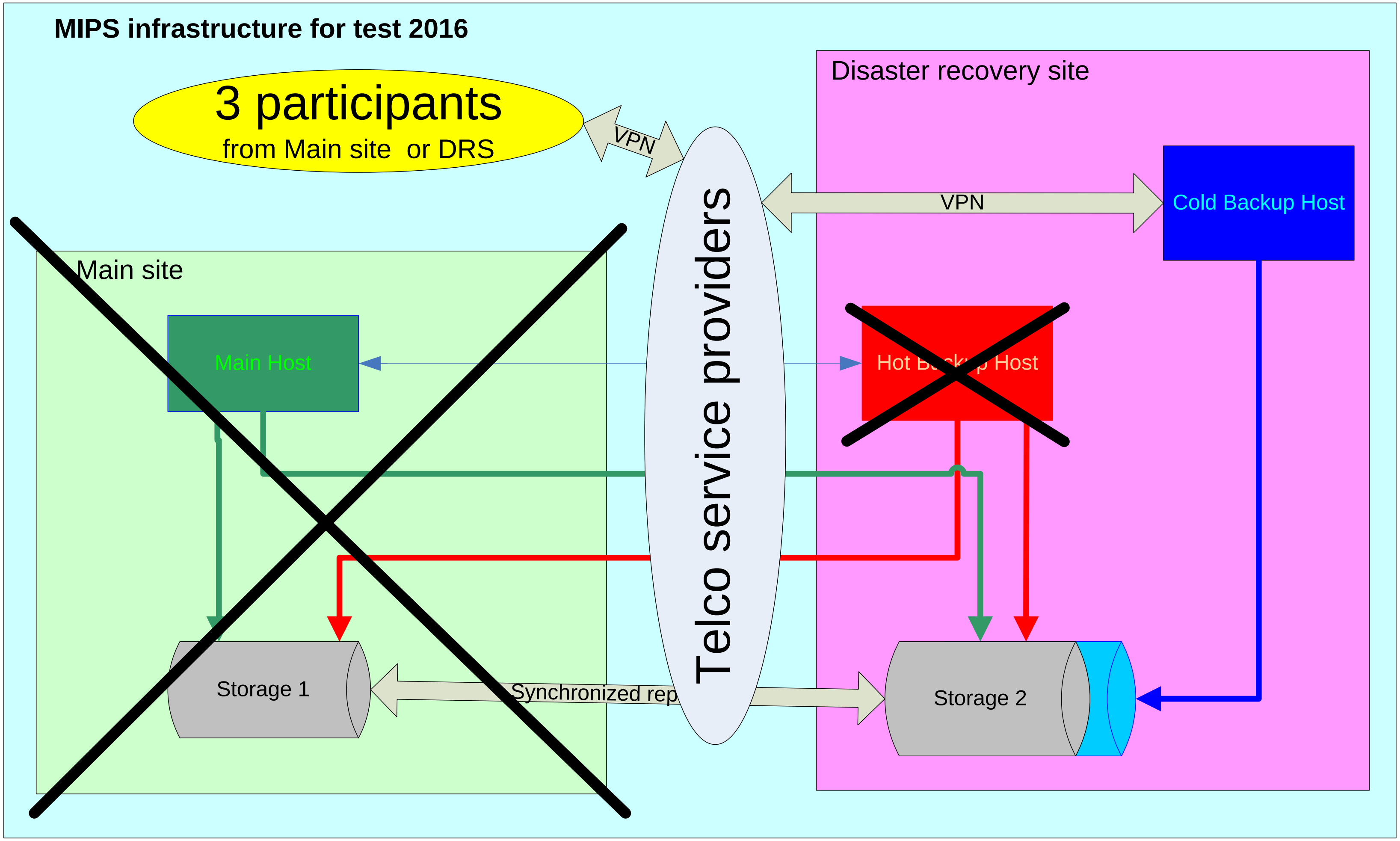
Main objectives from the testing of the BCP of MIPS (1/5):

- *check the time-need* and effectiveness in communication (**call tree**) and transferring information for declare the crisis from the NBRM to the participants from NBRM
- *time estimation* necessary for establishing an **active payment system in crisis** and operationalization of the processes that are subject to this test at DRS location define potential areas for improvement
- *check the efficiency* of the processing of **payment orders** submitted by the institutions on the **magnetic medium** (USB or CD)

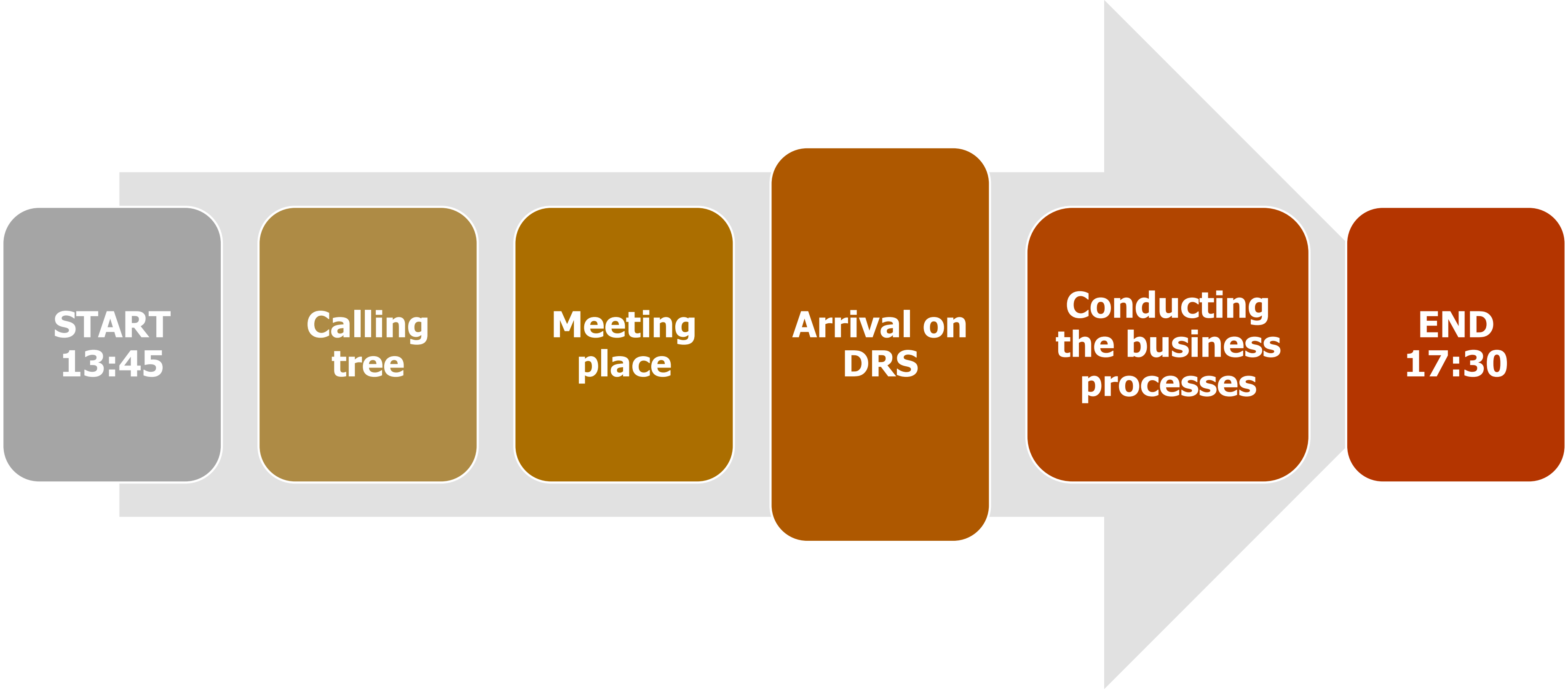
Main objectives from the testing of the BCP of MIPS (2/5):

- *checking the functionality* of the **parts of the payment process** (making a transfer order for payment, control, approval and settlement of the payment in MIPS)
- *check the functionality* of **electronic communications** and the functionality of the **equipment of COLD MIPS** system
- *checking* **LAN** (local area network) for NBRM employees on DRS and the **printers**
- *checking* **PBX** (private branch exchange) **telephone system** and **phones on DRS**

MIPS infrastructure for test in 2016



Testing is conducted in the following stages (NBRM view):



START 13:45

Calling tree

Meeting place

Arrival on DRS

Conducting the business processes

END 17:30

Scope of the test:

- NBRM (6 departments and 42 persons)
  - Department of Off-Site Supervision and Licensing (2 working processes)
  - Financial Market Operations Department (2)
  - Payment Systems Department (3)
  - Financial, Accounting and Control Department (1)
  - Information Technology Department (5)
  - Technical Maintenance, Security and Archive Department (2)
- 3 Major Banks (53 persons)
- Ministry of finance (3 persons)

Day for testing:
Working day – Saturday

State of the MIPS:
TEST messages on the LIVE infrastructure

Test results about success of messages sent to MIPS:

Participant	Sent messages	MT 920	Settled messages	Rejected messages in working hours (until 17 hour)	Rejected messages after closing the MIPS system
Participant 1 (main)(N*)	1003	1	803	199	1
Participant 2 (DRS)(N+MM**)	809		204	0	605
Participant 3 (MM)	805	1	804	0	1
Participant 4 (DRS) (N)	800		800		
NBRM	40		34	0	6
Total	**3457**	**2**	**2645**	**199**	**613**

*** N – means executing payments through the network**

**** MM – means executing payments from the premises in NBRM by transfer the payments on magnetic medium (USB stick or CD)**

Conclusion (1)

- All 15 processes within the jurisdiction of the 6 organizational units in NBRM were successfully tested and the planned activities were fully implemented.
- Communication and coordination between the National Bank and external participants in the testing, as well as communication and coordination within the participants, the National Bank is assessed as fast and efficient.
- Transport services to and from DRS had a high level of efficiency and good coordination, according to the timeframe foreseen.

Conclusion (2)

- The working premises and working conditions (heating, clean rooms, etc.) are in accordance with the needs.
- The time for realization of the envisaged processes was shorter than the maximum acceptable interruption defined in the BCP of the National Bank.
- All processes of criticality category 1 (with a recovery time of 2 to 4 hours) started to run on the DRS for a much shorter time than planned.
- The organizational units will use the experiences from this testing when planning the next testing, as well as improving of the BCP.

Next test of BCP in November 2017

Scope of the test:

All participants in MIPS from their DRS

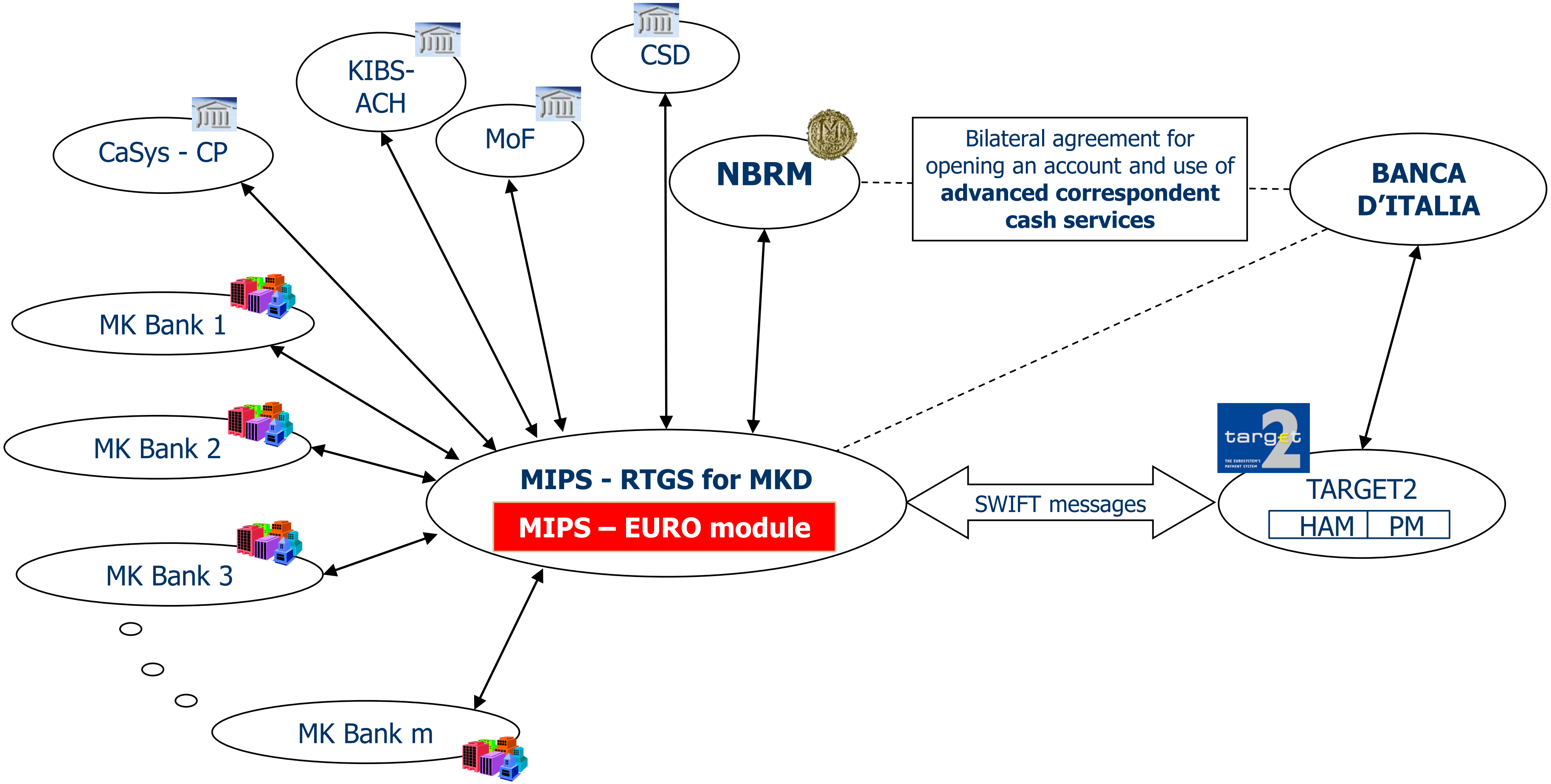
Day for testing:

Working day – Friday

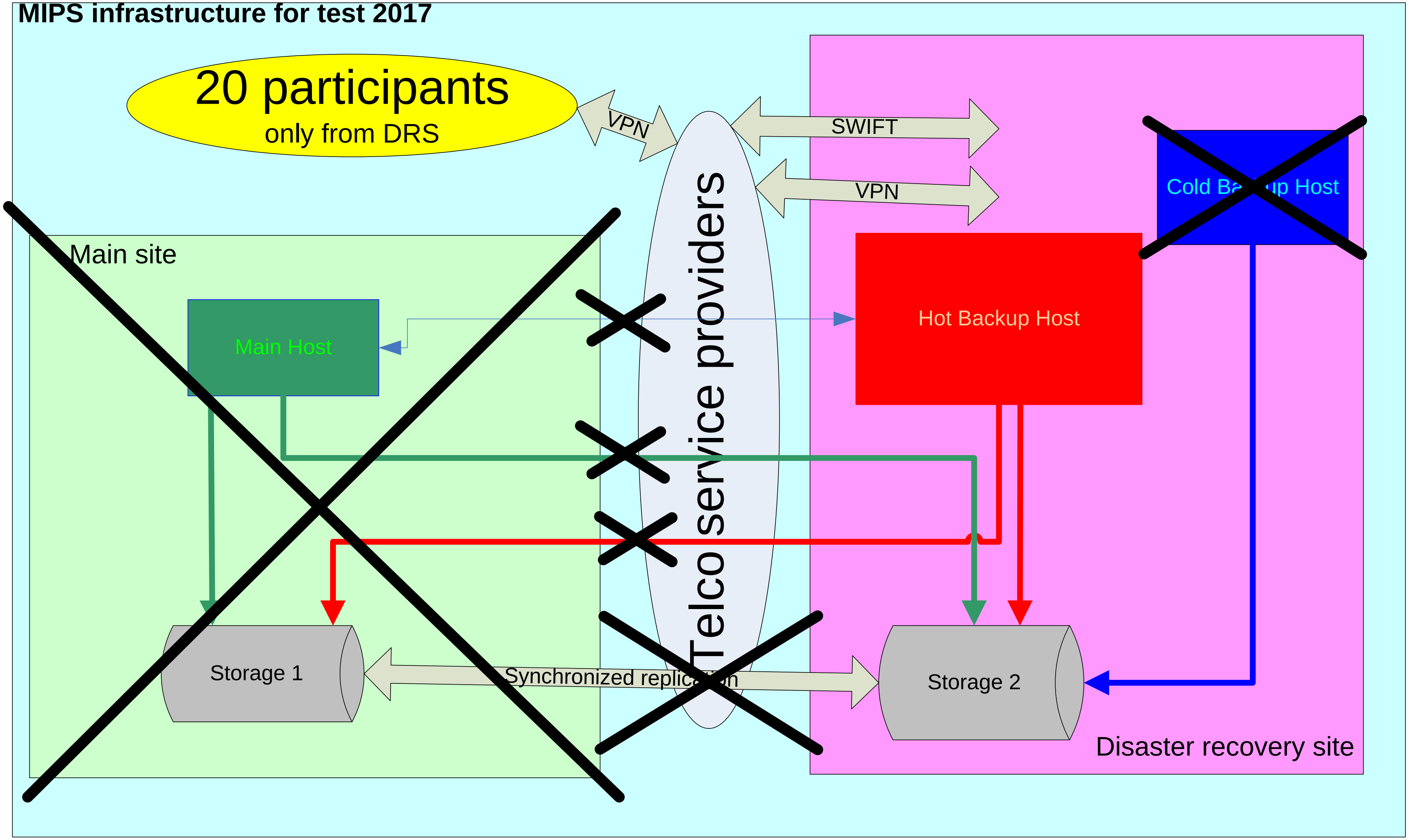
State of the MIPS:

LIVE

Macedonian interbank payment system in 2017 as RTGS for Macedonian denar + Euro Module



MIPS Infrastructure for test in 2017



Thank you!

Lihnida@nbrm.mk

GacovB@nbrm.mk

GeorgievZ@nbrm.mk