Feedback from the inspected bank

Part of the report the institution wants to comment on[1]		Inspected institution's comments or remarks	HoM response
Par 51	Finding # 1 Uncertainties in the definitions of strategic options of the MPS Group	The strategic reflection on the evolution of the *Consorzio* starts with the top management's awareness that the *Consorzio* is able to set and sustain the objectives of the Restructuring Plan within a process of ongoing improvement, as defined and detailed in the IT Strategic Guidance document approved by MPS' Board of Directors on 17 April 2018. This awareness is confirmed by the updates regularly provided to the MPS BoD on cost trends (which are ahead of the plan objectives), on the focus given to important projects (strategic, relevant and mandatory) and on the increasing timeliness in the end-to-end implementation required. The same OSI IT Risk report, while highlighting a number of weaknesses and issues reported in the findings, confirms that "the current IT structure of the MPS Group can adequately support the requirements of the bank within the horizon of the Restructuring Plan, needing, however, a clear definition of the strategies and improvements in the project development". The MPS BoD is therefore in the favourable condition of not being obliged to find alternatives to the current situation and to be able to freely examine the expressions of interest put forward by some important national and international players in the IT market. MPS and these players are aware that the *Consorzio* is unique in terms of size, volumes, completeness of its features and compliance with ECB and non-ECB requirements and is not comparable with other national operations (smaller in terms of size or scope of activity), as reported in the OSI IT Risk Report. The lack of true market alternatives will allow MPS to be a "first mover" in the process to rationalise the IT market in banks and, with the right partner and the right level of risk, to obtain economic and/or qualitative benefits, for instance by sharing investments in common initiatives (such as regulations) and creating a target IT platform starting from that of the Consortium. MPS' evaluation procedure is taking place on the basis of a structured process whose timing is influenced by the definition of the restructuring plan negotiated in 2017 and by the corporate developments within the MPS Group. As of April 2018, the MPS Board has been constantly kept updated on the expressions of interest and involved in all evaluations while the internal work group has been integrated with the skills required for a business, economic, technological, legal and labour-law assessment as well as a risk assessment of the different scenarios. The same BoD of 5 September also approved the MPS Group's Digital strategy and discussed the interdependencies of the *Venere* project. The next step is expected in the BoD in November, during which the non-	

[1] Please copy the commented part of the report

		binding proposal received will be evaluated.	
Par 68	Finding # 2 Delays in strategic and relevant projects and inadequate involvement of the IT function in the group IT planning	During the process to collect the 2019 project requirements, a new approach was adopted that by directly involving the COG in assessing the proposals for projects with an IT impact, with an estimation of economic and financial resources and the preparation of a capacity plan to support the development of project activities. The project management process has been recently simplified by moving the Demand function to within the COG's scope of activity, thereby reinforcing the integration between the technical and business components - thus optimising the drafting of technical specifications (Business Requirements/BR) which are preliminary to the execution of IT measures - and reducing implementation times. The COG's Demand has adopted a timely monitoring process for the BRs in order to keep under control the times employed to cross the various stages of their lifecycle. Furthermore, as part of the recent reorganisation of the Parent Company, the Chief Program & Cost Officer Area was reallocated to within the COO Division's area of responsibility, thereby creating a functional synergy with both the organisational units as well as those managing outsourced services, which, under the new structure, also monitors the service level of the COG's demand function. The new Cost Management, Projects and Service Quality Area (*Area GCPQS)*, reporting directly to the COO, carries out all project monitoring activities as well as a direct PMO function for all Strategic Projects, supporting the project management bodies. Regarding the latter, the responsibility for project monitoring and assessments, is mainly concentrated under the Project Operational Committee (or *COP*), which fulfils these requirements for all the relevant discretionary and mandatory projects, while the Strategic Projects, (large, highly-complex Change Projects) are under the direct supervision of the Executive Committee, which uses the COP and the individual Divisions for the preliminary procedures, and receives regular updates from the GCPQS Area on the overall progress of project activities. Monitoring of strategic initiatives and the main relevant and mandatory activities has also been strengthened with the introduction of monthly Steering Committees, organised for each project owner Division, which see the participation of first-line management. Regarding Other Projects (projects with limited unit spending and low inter-functional complexity), which in the past caused a more than proportional absorption of implementation resources, their inclusion in the COP's scope of responsibility is currently being assessed (particularly with regard to the product Plans plafond and to the GAP resolution Plans, which are characterised by a high implementation priority). In this way, the discretion of the Divisions will be reduced further, and they would be responsible for a limited scope of changes required. The structure envisaged and the process changes adopted and being adopted are aimed at strengthening project planning and management processes, with the aim to better define the scope of activity, making it more compatible with cost and capacity limits, and resulting in shorter and more certain implementation times. The main procedural changes outlined above, will be incorporated in the company's internal regulations, which will be duly updated by February 2019.	

Par 78	Finding # 3 The gaps of the COG IT security were unfoundedly closed by the IT Risk Management weakening the effectiveness of the remedial actions	The Operational Risk Function incorporates the inspection findings in its assessments and checks regarding the level of security posture compliant with the risk tolerance established in the RAF. During the assessment of the closure of the individual gaps, the analysis will be repeated to verify the residual risk following the mitigation measures.	
Par 80	Finding # 4 Weaknesses of the Group IT risk assessment	<u>WIDIBA</u> A review of the Top Level indicators is currently in progress. In addition, the inventory of IT resources subject to Low Level analysis was also revised, with an increase in the level of granularity of the infrastructural components. Finally, we intend to improve the methods for conducting the analyses of assets with specific attention being given to any security aspects and a greater level of investigation. The activities carried out have been agreed on between Widiba and the Parent Company. The closing date estimated is within the first quarter of 2019. Some of the implementations carried out will be used for risk analysis by year-end. The new indicators on security incidents and corrective fixes on software will be introduced subsequent to the start of the Incident process and its tuning according to the deadlines indicated in finding #11 below. <u>Consorzio</u> In June 2018, the *Consorzio* began to track security offenses and incidents through the new IncMan platform; the set of information regarding the incidents tracked, as well as the severity classification criteria still need to be fine-tuned (as identified in finding #12). A risk indicator based on this monitoring will be introduced in 2019. As regards the BitSight indicator, the Operational Risk Function and the *Consorzio* have already agreed on a new rating scale, with more conservative thresholds, which will be applied as of January 2019. Additional corrective measures will be evaluated in 2019, based on positioning with respect to the individual risk vectors which BitSight includes in the calculation of its rating. With regard to the finding concerning the failure to analyse all the critical assets in the business continuity perimeter, it should be noted that the classification of such critical resources has been taken as a priority factor in the selection of assets included in the annual risk analysis perimeters: out of 86 critical assets, 70 were already analysed between the end of 2015 and 2017; 12 are in the process of being analysed within the 2018 perimeter; 4 have not been analysed since they are going to be dismissed or because similar to others already analysed (the reports on the four critical applications cited as not analysed are available to the Inspectors).	
Par 84	Finding # 5 The IT Compliance function was not activated in Widiba	Although the title of the finding does not reflect the current situation, the detailed description provided in the inspection report (paragraph 3.1.4) is acceptable and already recognises the fact that activities have been started. The detailed plan for the controls cycle has been shared with Widiba's local Compliance referent, according to the duration identified on the basis of available resources.	
Par 87	Finding # 6 The scope of IT Audit Plan is limited and only partially	No specific comment or remark on the paragraph. The finding will be addressed within the 2019 and 2020 audit plans in order to provide full assurance, as required, about the assessment of the main technological	

	adequate to mitigate the IT Risk	risks and of the bank's overall management of IT risk over the overall 3-year audit cycle (2018-2020).	
Par 108	Finding # 7 The Monte Più Sicuro and Monte Protect Shield projects have not adequately removed the weaknesses of the COG IT Security emerged in the 2015 analysis	The establishment of the Monte Protect Shield Project, which encompasses the Monte Più Sicuro Project, introduced, in the course of 2018, a rigorous and orderly approach in the project's management, which gave a decisive impulse to the implementation of the plan's initiatives. More specifically, the: - adoption of group rules on project management through the involvement of a Steering Committee made up of first line managers and a structured monitoring process according to project management rules. - stable and profitable integration between Parent Company and IT skills - increased accountability resulting from a risk-oriented approach, with the inclusion of the Risk function in project management. have led to all key deliverables being achieved on time. These include the: - extension of the 24H first level SOC Service to under Accenture's SOC - revision and implementation of data masking of the Central System test environment - activation and implementation of the system for the detection and management of security incidents (offenses and/or incidents) - assessment of application components on the departmental systems (ATM, Server Linux, Server Windows) which use together with: the activation of a quarterly control process; the revision of Security standards; the implementation of the Architectural and Security Monitoring process. - activation, on a representative sample, of the solution for detection of Authorisations on documents present within the Team Site and network files - revision of the Architecture of the authorisation system for the branch front-end application (Paschiface) - revision and implementation of the perimeter defence system with the application of new security rules - activation of new solutions for identifying the Vulnerabilities present in our systems and control activities - activation of the security control gate within the DevOps cycle for applications with external exposure via internet - revision of network architecture for securing the technical-application infrastructure of the Digital Banking and Paschi Azienda Online systems. Under completion by the end of the year: - Extension to BMPS of new Internet browsing infrastructure - Monitoring of System Administrators for departmental environment - Update for the new Identity Management infrastructure for the entire production environment - Activation of the PC encryption function (Bitlocker) for most of the General Management Division - Activation of the NAC (Network Access Control) solution for controlling the Laptops of externals connected to the corporate network from BMPS locations To be completed in 2019: - Extension of encryption to Branches and completion for General Management Division (March 2019) - Extension of monitoring of System Administrators that	

		access the mainframe, which account for 20% of the reference perimeter (April 2019). - Extension of the new Identity Management infrastructure to the development and testing environments (April 2019). Finally, as far as the assigned budget is concerned, the financial resources absorbed for project initiatives are believed to be in line with the goals to be achieved.	
Par 118	Finding # 8 Weakness in the Identity management process of the COG	A solution has been provided for that is broken down into technical, organisational and regulatory areas. It has already been put underway with the establishment of a mixed Parent Company/COG work group, which has identified the following areas of intervention: - As a priority, the regulations will be updated with the rules and responsibilities which all users responsible for applications outside the OIM perimeter must strictly comply with, and will identify the methods for monitoring and controlling the behaviours applied. This activity is expected to be completed by the end of the current year. - In parallel, work will begin on the implementation of a technical-organisational solution to verify and control the authorisation profiles on applications not integrated with OIM, and, at the same time, an analysis will be carried out on the possibility of integrating other currently out-of-scope applications will also be analysed. This activity is expected to be completed by 30 September 2019.	
Par 120	Finding # 9 Weakness in privileged user management and monitoring process in the COG	In this case too, a solution has been provided for that is broken down into technical, organisational and regulatory areas. It has already been put underway as part of the mixed Parent Company/ COG work group. Note, however, that in this area, as noted by the Supervisor, control crash activities have already been regularly carried out along with a "clean-up" of users no longer necessary. More specifically: - As a priority, the current regulations regarding rules and responsibilities will be updated and more precisely identify the types of controls and responsibilities to be assigned. This activity is expected to be completed by the end of November 2018. - In parallel: Privileged user access will be secured, identified and tracked through the implementation of the tool, CyberArk (its deployment is part of the Monte Più Sicuro Project). This implementation will be divided into two steps, as shown in finding #7: ○ Access to the departmental systems (70% of the total) will be integrated in CyberArk by the end of this year ○ Residual access to the mainframe will be integrated in CyberArk by 30 April 2019.	
Par 127	Finding # 10 Defects of the security incident management of the COG	The mixed Parent Company/COG Work Group provides a structured solution, as described below: - the revision (within the Cyber Incident Management process) of the classification of the criteria underlying the distinction between "system incident" and "cyber incident" will be completed by the end of November 2018. - The project "*Evoluzione SIEM*" will define the	

		classification of severity of the offences and incidents based on the type of asset and critical nature of the processes to which they refer. The new classification framework (criticality/impact) will be unique for all structures involved in the process and provides for the implementation of a structured review of rules on a regular basis. This is expected to be completed by 30 April 2019. - Completion of the "*Evoluzione SIEM*" initiative will enable the activation and storage of logs currently not included in the scope of the SIEM analysis. This activity is expected to be completed by 30 April 2019. - Finally, a review of the save and information storage procedure will be put in place. This activity is expected to be completed by 30 April 2019. Moreover, as of June 2018, data on the offenses identified will be stored for at least one year.	
Par 132	Finding # 11 Defects on IT security in Widiba	<u>Incident</u> A project to review Widiba's Incident process has been included in the Masterplan expiring in December 2018 so as to make it operational by January 2019 with a first phase of tuning. The main activities being analysed are as follows: 1. Determination of Incident by type (e.g. IT, Security, Fraud, Data quality) and method of assigning severity calculated on objective data and not just from customer reports. 2. Publication of IT Incident, Major Incident policy, with various escalation processes. 3. Management of incident management owners with coordination of outsourcers 4. Tracking of changes made in fix with matching to the incident of reference. 5. Monitoring of written code with a focus on the SW's stability and on the changes to critical components. 6. Reporting for greater usability of data and KPIs for IT Incidents. All activities are expected to be completed by March 2019 – we estimate 3 months of Tuning in production for the development of the process for both the application and organisational components. <u>Monitoring</u> Correlations were introduced in September between security threats (external attacks) and the monitoring of systems: currently, alerts are highlighted in the monitoring dashboard and managed by suitably trained staff. Additional control will be added to correlate IT threats with automatic alerts, so as to also cope with any growth in volumes. All activities are expected to be completed by March 2019. <u>Privileged users</u> By May 2018, Widiba had taken steps to make corrections to the monitoring of Admin users, with a system of alerts in the case of changes to monitoring tools. More specifically: 1. assignment of Balabit administration privileges to non-system administrators for segregation of roles – disabling of Balabit administrator privileges to current system administrators; 2. automatic sending of emails to mail group (bala-sec@widiba.it) for all accesses to production and	

		changes to configuration to the Balabit platform (include the sending of a notification email); 3. group email alert to bala-sec@widiba.it on direct access to firewall by system administrators. Each access is notified to other persons in the group bala-sec@widiba.it 4. disabling of SSH service with notification to mailbox bala-sec@widiba.it in order to centralise all access to Balabit only from the web platform; 5. optimised mail already existing for notification to the systems group for all alerts signalled by the monitoring systems including switch-off of alerts (manual or automatic): extension to admins for reciprocal checks.	
Par 145	Finding # 12 The BMPS' PCOs are not complete; the continuity risk could not be mitigated for single process due to the inadequate application mapping	A solution has already been put under way and is structured along two lines of activity: - Mapping of critical/systemic processes and related assets: the update was completed in September 2018 and takes account of the restore times established by Bankit regulations (RTO). The output was shared with the *Consorzio Operativo*. The Disaster Recovery test scheduled for the weekend of 14 October will also verify the restart times of the applications identified in the BIA (Business Impact Analysis) relating to the system processes being tested (*see* also finding # 14). - Correlation with Risk Management: a process has been identified that provides for a structured exchange of information flows between the Parent Company/BCM Security function and the Risk Management function in order to align the results of the respective assessments. Furthermore, in order to rectify any discrepancies already present in 2018, the Parent Company/BCM Security Function will carry out the appropriate checks with the individual process owners and align the other function involved on the results. This last activity will be concluded by the end of this year.	
Par 149	Finding # 13 Weakness in Widiba's BIA process and in the related risk assumption report	As at 31 May 2018, Widiba had concluded its preparation of a backup environment on Siena's servers with the replication of the development environment in order to enable activation of the critical development process in a short time in the event of a CED fault in *Via Messina* (Milan) with connection of resources in VPN to emergency locations (e.g. MPS *via Rosellini*, Sorint Bergamo or other locations in Milan or Siena). Moreover, the BIA content was fully revised in the first half of the year, leading to the identification of critical processes and assigning a new assessment of importance and risk to all the Bank's functions. By the end of the year, all the supporting documents for all the solutions implemented will be produced and the Business Continuity Plan (BCP) will be reviewed. Only the Incident Management process was considered in the BCP since all the applications are on 2 geographical sites in Active-Active mode and therefore with mitigation of business continuity risk. This decision will be reported in the "IT Strategic Guidance" which Widiba will submit to the Board of Directors by the end of 2018, together with the new BIA and BCP solutions. All documentation and methodology will be shared with the appropriate Parent Company Functions, including the ICT Compliance Function. Furthermore, it has been agreed with the Parent Company that Widiba will adopt the application solution which manages Business Continuity at group level. As a preliminary step to adopting the solution, the processes will be registered in	

		Aris; taking account of their high number, the first to be registered will be those in the BCM environment, to allow the execution of BIA from as early as 2019. It is expected that all activities will be completed by the end of 2018, except for the revision of the granularity of the registration of processes which will be revised in the course of 2019, together with the mapping of processes in ARIS according to the Parent Company taxonomy.	
Par 155	Finding # 14 The COG Disaster Recovery test cannot demonstrate the respect of the restart time limits for systemic processes	The Disaster Recovery plan has been updated to include the results from the 2018 BIA, which reports the classification of processes and applications relating to each of them. Each systemic process has the recovery times and RTO (Recovery Time Objective) associated to it. During the next disaster recovery test (13-14 October) the restart times of applications relating to systemic processes will be measured. All activities are expected to be completed by November 2018.	
Par 169	Finding # 15 Delay in the implementation of Data Governance project	As of July 2018, the Data Governance Function has changed its approach with the use of a more stringent definition of “Relevant Output”, now limited to those reports with a structure bound by regulatory provisions. At the same time, a “Data Driven” approach was launched through the identification of the so-called “Relevant Data Bases”, a Data Governance action plan was established for 2018-2019 and a request was made for the launch of two project activities (generally communicated to the supervisory authority as “new project initiatives”): - DataGov Evolution - New Data Quality infrastructure for regulatory reporting (SISBA3) The acquisition of the new Data Discovery and Lineage systems has also been communicated. In addition to what is known to the Bank of Italy, the Data Governance Function is also preparing two new Group Directives: - Acquisition and use of external data sources - Production and distribution of Divisional and Network Reporting	