EUROPEAN CENTRAL BANK

BANKING SUPERVISION

ECB-CONFIDENTIAL

DG-MS4/COI

On-Site Inspection Report

Donatello Errico
(Head of Mission)

FINAL
OSI-2018-ITMPS-3832
15 November 2018

Details of the inspection mission

REFERENCE	OSI-2018-ITMPS-3832
INSTITUTION	Banca Monte dei Paschi di Siena – SpA
TOPIC	IT RISK
PURPOSE	IT RISK
HEAD OF MISSION	Donatello Errico, Inspectorate Directorate
TEAM MEMBERS	Giacomo De Luce, Banca d'Italia, Inspectorate Directorate Francesco Abbinante, Banca d'Italia, Inspectorate Directorate (from 02.05.2018 to 15.06.2018) Mario Danza, Banca d'Italia, Inspectorate Directorate Luigi Intonti, Banca d'Italia, Inspectorate Directorate Serena Pulvirenti, Banca d'Italia, IT Department - IT Planning Directorate Giovanni Senese, Banca d'Italia, Banking Supervision 1 Directorate (from 26.03.2018 to 11.05.2018 and from 21.05.2018 to 25.5.2018)
PERIOD OF MISSION	26.03.2018-06.07.2018

Versioning follow up

STEP	DATE
Notification letter of the OSI	23.02.2018
Kick-off meeting	26.03.2018
Start of the on-site field work	26.03.2018
Location 1 of the on-site inspection	Siena
Location 2 of the on-site inspection	Milano
Location 3 of the on-site inspection	Firenze
End of the on-site fieldwork	06.07.2018
Draft report sent to the bank before the exit meeting	02.10.2018
Exit meeting with the bank's management	10.10.2018
Feedback of the bank on the draft report	23.10.2018
Final report	12.11.2018

Table of contents

FINAL
OSI-2018-ITMPS-3832
15 November 2018

Inspection Report

1 Scope and Executive Summary

1.1 Scope

1 The mission focused on IT risk, in particular on assessing: a) the consistency of the IT strategy with the overall business strategy, b) the sustainability of IT system architectures, c) the adequacy of IT security and of IT continuity and d) the Data Quality framework. The abovementioned objectives took into account the compatibilities of the cost cutting policies implemented by the bank. Moreover, the OSI checked the involvement of the management bodies regarding the management of the IT systems and processes.

2 With regards to the mentioned objectives the OSI analysed:

a) the process of definition of the new IT strategic plan (envisaged in March 2018) and IT operational plan. In this context, specific focus was placed on the initiatives to outsource the group IT function (so-called Venere project) considering the relevant strategic implications;
b) the consistency of the IT spending with the approved business plan (i.e. the 2017-2021 Restructuring Plan approved by the European Commission) and with business initiatives were evaluated;
c) the high-level governance process of the IT system architectures aimed at supporting the main business processes. The new IT strategic plan was challenged in order to verify the alignment with the IT system targets of the Bank;
d) the management (i.e. policies, processes, and procedures) of IT security, and of IT continuity. For these topics, critical incidents were analysed to appraise any structural weaknesses;
e) the effectiveness of data governance projects, as well as the appropriateness of the remedial actions in place to overcome already known shortcomings. In this context, the Data Quality framework (i.e. based on measurable metrics and KPIs) was analysed to assess its maturity grade.

3 Against this backdrop, the OSI checked the involvement of the management bodies regarding the strategic decisions on the IT systems and processes.

4 Considering the planned disposal of foreign entities and branches, the OSI concentrated on the Italian component and, in particular, on the IT services provided by the Consorzio Operativo del Gruppo Monte dei Paschi (hereinafter COG or simply Consortium) to Banca Monte dei Paschi di Siena (hereinafter BMPS) and Widiba, the online bank of the Group.

5 The main legal references are: Directive 2013/36/EU (hereinafter CRD IV); Banca d'Italia Circolare no. 285/2013. The BCBS 239 ("Principles for effective risk data aggregation and risk reporting", January 2013), The BCBS-Joint Forum "High-level principles for Business Continuity", NIST Cybersecurity Framework, ITIL (IT Infrastructure Library), ISO/IEC 27001:2013 "IT - Security techniques - Information security management systems – Requirements".

1.2 Executive Summary

6 MPS is the fourth largest Italian banking Group in terms of total assets (amounting to € 139.2 bn as of year-end 2017). The main business is the commercial banking in the domestic environment, with a focus on retail. After the failure of a € 5 bn capital raising plan in Q4 2016, BMPS applied for precautionary recapitalisation in December 2016, which required the delivery of a five-year Restructuring Plan, approved by the European Commission on 4 July 2017. As a consequence, burden sharing measures were implemented, and the Italian government subscribed the capital injection requested by ECB.

7 **Table # 1 – BMPS Group main figures at 31.03.2018 (source MPS Planning area)**

Key figures	Value
Total assets of which Loans to customers	€136,772 mln € 89,320 mln
Total risk exposure amount	€ 61,781 mln
CET1 Capital (actual/fully loaded)	€ 8,876 mln / € 7,118 mln
Net profit	€ 187.6 mln
Cet1 ratio (actual/fully loaded)	14.4% / 11.7 %
T1 ratio (actual/fully loaded)	14.4% / 11.7 %
Total capital ratio (actual/fully loaded)	15.8% / 13.1 %
Leverage ratio	4.6%
Liquidity coverage ratio	195.7%
Net stable funding ratio	106.0
Annualized ROE	7.6%
NPL ratio (gross/net)	34.2% / 14.1%
NPL ratio after securitization(gross/net)	19.7% / 9.9%

8 **Table # 2 – BMPS main shareholder at 01.07.2017 (source CONSOB web site)**

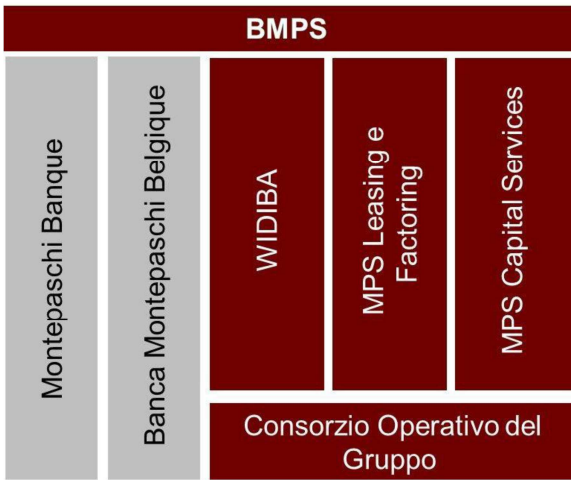
Main shareholder	Value
Ministero Economia e Finanze (MEF)	68.2%
Assicurazioni Generali S.p.A.	4.3%
BMPS S.p.A (own equity shares directly held)	3.2%

9 The IT function of the MPS Group is assigned to the internal outsourcer COG[1] that manages the overall IT platform of BMPS, MPS Capital Services, and MPS Leasing e Factoring (hereinafter MPSCS and MPSLF respectively). Widiba and the foreign banks have their own IT functions and systems, and have a functional reporting to the COG through some coordination mechanisms (e.g. sharing the IT planning at the beginning of the year) which, however, leave a large degree of autonomy on technological choices. Following the commitment of the Restructuring Plan, the foreign banks (i.e Montepaschi Banque and Banca Montepaschi Belgique) are going to be sold or closed.

10 The project of Widiba was launched in June 2013, while the bank became active starting from the end of 2014. The bank is made up of a digital platform, innovative in the national online banking sector, above all for the user experience profile, and it has acquired the network of over 600 financial advisors of MPS Group. At the end of 2017, the total assets of Widiba amounted to €2.5 bn. Widiba manages the front-end applications (e.g. Web banking, smartphone apps and financial advisor channel) and the connected hardware on its own account, while using the back-end of the COG.

[1] COG is 99.79% owned by BMPS, with the other MPS Group "Consortium Members" being Widiba S.p.A. (0.03%), MPS Leasing & Factoring S.p.A. (0.03%), MPS Capital Services S.p.A. (0.06%). Axa Italia Servizi S.p.A. (0.03%), Axa Assicurazioni Danni S.p.A.(0.03%), Axa Assicurazioni Vita S.p.A. (0.03%) are members external to the group.

11 **Figure # 1 – BMPS Group simplified structure (source IT Strategic Guidelines 17.04.2018)**



12 According to the Restructuring Plan, the MPS Group has to significantly reduce costs and investments. Cost cutting could be even more incisive in case revenues remain below the expected targets. Moreover, these constraints and the significant resizing suffered by the Group (from the end of 2009 a reduction of almost 50% in branches and of about 40% in total assets) led to a reduction in the running costs and to a careful selection of the projects to invest in. To this end, the COG has activated various levers (e.g. on the IT supplier management, management control, and organisational measures) which currently allow to comply with the cost reduction plans, and even to anticipate them in terms of cash-out.

13 The IT architecture is updated and could be open to future technological implementation to support the business activities, in a predictable horizon for a commercial bank. The bank identifies risks in the aging of the human resources and in the possible exits of valuable skills of the COG.

14 The bank is considering two strategies: a stand-alone one based, above all, on the increase in operating efficiency and another focused on the sale and externalization of the COG (so called Venere project). Until the end of the OSI, however, neither option had been framed in an overarching consideration including the critical review of the bank's business model, in the light of the role and the foreseeable evolution of IT. Moreover, the Venere project still lacks an evaluation of the implicit strategic risks and a preventive cost-benefit analysis.

15 A centralized process based on the Group Project Plan has been set up to define and oversee the project investments, in order to allow a stricter control of the top management and a strong alignment to the Restructuring Plan. However, these objectives are not adequately accomplished, considering the delay in strategic and relevant projects, the

proliferation of numerous non-strategic investments, and a consistent backlog. The MPS Group has recently introduced organisational measures to overcome these issues (e.g. on the Demand function), but further improvements are required to reduce fragmentation of responsibilities and increase the effectiveness of the overall monitoring.

16 Due to organizational and cultural factors, rather than a lack of investments, relevant weaknesses have been found in the IT security, particularly in management and monitoring of: a) privileged users; b) cyber incidents. With reference to the latter, it has been affected by relevant issues, especially regarding the traceability: the OSI team has found 13 cyber incidents which occurred in 2016 and 2017 and were not recorded in any incident management system, not escalated or formally reported, and not evaluated in their severity. Against this backdrop, the delays in implementation of IT Security projects on are relevant.

17 The IT Continuity is overall adequately managed, although it requires the implementation of a suitable component mapping to improve the effectiveness of the Operational Continuity Plan (hereinafter PCO) and to ascertain in the test phases the recovery of the critical and systemic processes within the Recovery Time Objectives (hereinafter RTO) and the restart time limits .

18 The Data Governance project is a relevant initiative to address the quality of the data with a structured approach. However, it is still at an early stage for coverage of the data perimeter, for completeness of the implementation (e.g. missing a definition of Key Quality Indicators), and limits in the coordination of the initiatives of the business functions. The development of the initiatives is envisaged in a three-year time horizon, which could entail delays and execution risks.

19 The IT Risk Management has developed a methodology to control and asses the IT Risk, but the closing of some of the gaps on IT Security, that it had raised in 2016, was baseless. The IT Audit activities are characterised by an adequate depth of analysis and assessment, but they do not cover a sufficient perimeter.

20 With regard to Widiba, it is characterised by a light structure, a strong integration between business and IT that reduces the time to market. The IT internal resources have up-to-date technological skills, in a dynamic and cohesive context. However, the strong orientation towards development determines the neglect of some risk profiles and limits in the traceability of the processes, for example in the incident management, in the monitoring of privileged user activities, in the Business Impact Analysis (hereinafter BIA). Moreover, these risks were not adequately mitigated by the local and group control functions.

21 In conclusion, the OSI identified relevant shortcomings, mainly in the IT Security, due to inadequate organizational assets, incomplete implementations of the technical solutions,

insufficient enforcement by the control functions, and shortcomings in the IT risk culture. On the other hand, the analysis of the OSI indicates 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.

2 Table of findings

22 The below table provides a list of all findings.

#	FINDING	RANKING[2]
1	Uncertainties in the definitions of the IT strategic options of the MPS Group	F2
2	Delays in strategic and relevant projects and inadequate involvement of the IT function in the group IT planning	F2
3	The gaps of the COG IT security were unfoundedly closed by the IT Risk Management weakening the effectiveness of the remedial actions	F3
4	Weaknesses of the Group IT risk assessment	F2
5	The IT Compliance function was not activated in Widiba	F2
6	The scope of the MPS Group IT Audit Plan is limited and only partially adequate to mitigate the IT Risk	F2
7	The Monte Più Sicuro and Monte Protect Shield projects have not adequately removed the weaknesses of the COG IT Security which emerged in the 2015 analysis	F3
8	Weakness in the Identity management process of the COG	F2
9	Weakness in privileged users management and monitoring process in the COG	F3
10	Defects of the security incident management of the COG	F4
11	Defects of IT security in Widiba	F3
12	The BMPS' PCOs are not complete; the continuity risk could not be mitigated	F2

[2] F1- Low impact, F2 – Moderate impact, F3 – High impact and F4 – Very high impact.

	for single process due to the inadequate application mapping	
13	Weakness in Widiba's BIA process and in the related risk assumption report	F3
14	The COG Disaster Recovery test cannot demonstrate the compliance with the restart time limits for systemic processes	F1
15	Delay in the implementation of MPS Group Data Governance project	F2

23 **Table # 3 - Table of findings**

3 Report Details

3.1 General requirements

3.1.1 Organisational framework

3.1.1.1 Governance

24 The BMPS' BoD is responsible for the direction and control of the IT, approving the overall Project Plan and the budget, the information system development strategies (the latest ones approved on 17.04.2017), the IT security policy, and the "greater importance transactions" -so called OMR- regarding IT (e.g. outsourcing of important operational functions). The BoD receives information about the COG operational trends (e.g. in the meeting held on 17.04.2017), the yearly IT risk reporting, and is notified in case of serious problems for the company activity resulting from incidents and malfunctions. The BoD, renewed on 18.12.2017, held an induction meeting on 15.01.2018 in which the managerial structure was presented and the main issues of the group were illustrated: those relating to the constraints of the Restructuring Plan and the relative repercussions on the group, the project plan, Widiba and the COG had a significant treatment.

25 The Comitato Rischi (i.e. the Risk Committee internal to the BoD) expresses its opinions on outsourcing proposals and on IT risk issues. Furthermore, in the Risk Committee and in the Board of Statutory Auditors (hereinafter BoSA) the findings emerged from the Internal Audit

(hereinafter IA) are actively discussed especially in case of high relevance gaps (for example for the Ethical Hacking[3] carried out on Widiba and on the COG).

26 The BMPS Comitato Direttivo (Management Committee hereinafter MC), led by the Chief Executive Officer (hereinafter CEO) of BMPS and composed of the group's first managerial line, is in charge of the implementation of the strategic guidelines, having a direct supervision of the Project Plan and the related strategic IT projects.

27 The head of the group IT function is the General Manager (hereinafter GM) of the COG (G. Damiani). On 01.12.2017 the CEO of Widiba (A. F. Cardamone) was also appointed as CEO of the COG. Moreover, on 17.04.2018 the Widiba and the COG hierarchical reporting lines, so far attributed to the Chief Commercial Officer and Chief Operating Officer respectively (hereinafter CCO and COO), were moved directly to the CEO of BMPS "in a logic of ever-increasing attention to technological innovation" and to "develop the digitalisation of the Bank, bringing it to the best market standards" (press release of 17.04.2018).

28 Several managerial committees are involved in the management of IT profiles in the BMPS[4] and in the COG[5.] Some of them are useful for the commitment to the IT efficiency and risk reduction (e.g. the Provided Services Committee and Risks), but the frequent need for coordination, the sharing of responsibility and the fragmentation of the processes have delayed the achievement of project objectives and weakened the direction and monitoring function (see par. 3.1.2 "Strategic Planning" and finding # 2).

29 With regard to the control functions, weaknesses emerged in the effectiveness of the IT Risk Management (see par. 3.1.3 "Risk profile, risk appetite and risk strategy" and finding # 3 and 4). The IT Compliance is extending its activities to the controlled entities, and in particular, to Widiba. (see par. 3.1.4 "IT Compliance" and finding # 5). The IT Audit does not cover relevant risk areas (see par. 3.1.5 "IT Audit" and finding # 6).

---

[3] Such Ethical hacking was commissioned by the IA to external providers to verify the strengthen of IT defences and discovered unknown vulnerabilities.

[4] For example: the MC on strategic projects, the Comitato Operativo Progetti (Operational Project Committee, hereinafter COP), the Demand Committees.

[5] Comitato di Direzione IT (IT Management Committee), Comitato Servizi Resi e Rischi (Provided Services Committee and Risks), Comitato Fornitori (Supplier Committee), Comitato Progetti IT (IT Project Committee), Comitato Architetture e Innovazione (Architecture and Innovation Committee).

3.1.1.2 Organisational structure and resources

30 While the IT function is mainly concentrated in the COG and Widiba, in the parent company there are significant functions for the IT management:

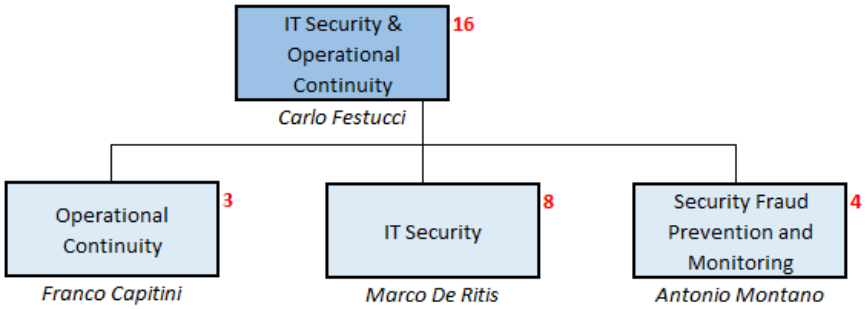
a) the control functions are all centralized, except for IT risk management units present in the COG and in Widiba that report functionally to BMPS Risk Management and cooperate in the analysis of IT Risk with the specialised unit (Rischi Informatici) in the Operating Risk Officer Area of BMPS;

b) the Chief Program & Cost Officer Area (hereinafter CP&CO), in staff to the BMPS CEO oversees the definition and management of the group Project Plan, that encompasses the IT group investments, and it ensures consistency with the Restructuring plan approved by the European Commission. The Area Pianificazione (Planning Area), under the CFO, is instead responsible for the definition of the overall budget and, in this context, for the IT budget.

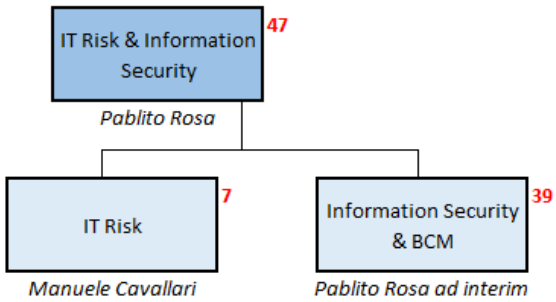
31 Administrative units are present in the COG and in Widiba with functional reporting to the corresponding structures of the Parent Company and they have an indirect but not secondary role in the IT management (e.g. in the management and control of the IT spending; in the monitoring of the IT services; in the human resources management).

32 The Logical Security and Operational Continuity function of BMPS (hereinafter LS-OC), set up in January 2017, is part of the "Area Sicurezza Integrata" (hereinafter ASI), directly reporting to the COO. The LS-OC reporting function inside the COG is the "IT Security and BCM" service (hereinafter ITS-BCM). See the following figures for the structure and resource of the two units.

33 **Figure # 2 – The IT Security and BC structure in MPS (source Organizational chart MPS dated March 2018)**

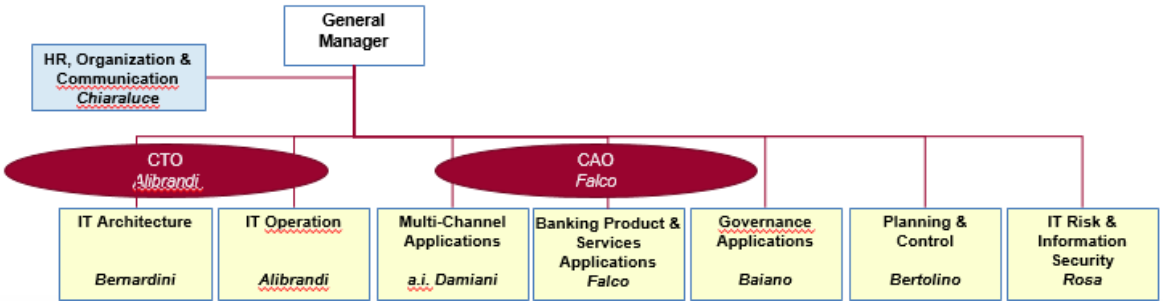


34 **Figure # 3 – The COG's IT Security structure (source Organizational chart COG dated March 2018)**



35 The COG had 862 headcount as of 31.12.2017, all seconded from MPS Group's entities and constantly reduced over the years (e.g. from December 2015 the number fell by 9%), divided among five operational areas and in staff units in six different geographical premises[6]. For the main organizational areas see the figure below

36 **Figure # 4 – COG simplified organizational chart (source Reorganization of the COG dated 20.10.2017)**



37 Due to the limited turnover, the average age is quite high (49.8 year). The COG has carried out an analysis of the compatibility of the trend of human resources envisaged in the time horizon of the Restructuring Plan, highlighting the existence of organizational levers that can be activated to maintain performance levels in line with previous years (e.g. job rotation, training, intragroup job posting, temporary assignments). However, criticalities emerged in the technological and security areas. A further analysis, based on the recognition carried out by the COG during the OSI on the staff needed by the IT area managers, has raised theoretical needs for about 40 resources: 26 in the application area, 9 in the technology and security

[6] The main are Siena and Firenze, followed by Mantova, Lecce, Padova and Milano.

area and 4 in the IT Governance; such deficits will be verified by more objective rightsizing analysis of the IT structure, following which the mentioned levers will be activated.

38 A management continuity plan has been drawn up and the critical profiles, among the unit's managers, have been identified. Anyway, the risk that critical resources leave the bank is not negligible (since 2016 almost 20 qualified skilled members of staff have left the COG), considering also the limitations on hiring, on labour costs, on incentives, and motivational factors. For example, the position of the IT Security manager is currently vacant.

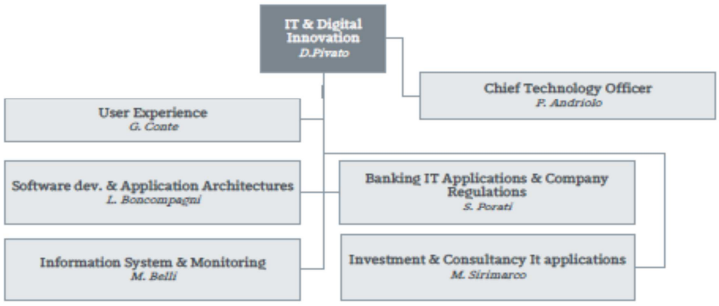
39 **Table # 4 – Envisaged trend in COG employees (source COG organisation function)**

Evolution of the COG's headcount	2017	2018	2019	2020	2021	Delta %
Number of employees	862	845	820	790	743	14%

40 The organizational model of Widiba is simpler and more compact, characterized by a light structure, a strong integration between business functions and IT that allows a reduced time to market of the business IT-based initiatives. But this strong orientation towards development often determines an inadequate level of formalization (see findings # 4, 5, 11 and 13), which makes internal processes less traceable.

41 In Widiba, the head of the IT & Digital Innovation is the Chief Information Officer, while the Chief Technology Officer is also responsible for the IT security (see next figure).

42 **Figure # 5 – The IT structure in Widiba (source Organizational chart Widiba dated 21.03.2018)**



43 About 60 internal resources are currently involved in IT, with a relatively low age (36.5 on average) and have up to date technological skills, in a dynamic and cohesive context.

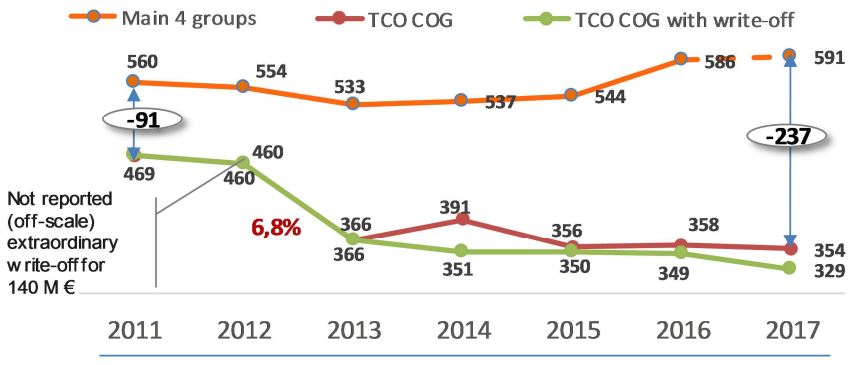
3.1.2 Strategic planning and budgeting

Strategic guidelines and the Venere project

44 In a context of rapid changes for the Bank, characterized by strong reduction in branches, employees and business volumes, the IT strategy has been aimed, above all, at increasing the efficiency, keeping a suitable level of service, according to the current needs, and taking into account the targets of the Restructuring Plan negotiated with the EU Authorities. In the MC of 23.02.2017 the CEO of BMPS requested an analysis about the future of the COG in the light of the strong downsizing of the group, evaluating the implications of a total or partial externalization. Therefore, on 23.03.2017, the CEO of BMPS informed the BoD of the strategic assessment in progress conducted by the top management through the so-called Venere project.

45 In the same meeting, an overview of the COG, its key performance indicators (KPIs) and a benchmark analysis were reported to the BoD, pointing out that the Total Cost of Ownership[7] of the IT showed a strong and persistent decline, greater than that of competitors (see next figure), especially for the component of the running costs; all the unit cost indicators (e.g. IT costs per branches and employees) were in line with or better than those of he banking system. Moreover, future scenarios and constraints were presented as a premise to strategic rationales for a change of operating model, for example: the strong downsizing suffered and further expected for the MPS Group; the challenging objectives of the new business plan in terms of costs reduction; the level of efficiency already achieved by the COG; the ageing of the human resources in an innovative context.

46 **Figure # 6 – TCO of the COG compared to the market (source COG Planning and Control)**



[7] The TCO is an aggregate of current expenses and depreciation of the IT sector collected by the CIPA (an association between Banca d'Italia and the Italian banking association with the aim to promote inter-banking IT initiatives) among the associated banks.

47 The bank's expectations are that the new model should target significant cost savings, higher service quality, risks in line or lower than today and a different mix of internal staff. Three scenarios were identified for a potential externalization: 1) the IT infrastructure (e.g. hardware and network services); 2) the infrastructure and the only applications managing banking products and services (so-called "core banking") without customer contact channels; 3) the whole infrastructure and the full application inventory. Moreover, only the third scenario has been developed in the exploring activities, driven by the idea of sharing the COG's ownership with an industrial partner backed by a financial sponsor. To this end, in the last months of 2017, a competitive tendering was arranged opening a data room to ten counterparties.

48 In February 2018, the bank received three non-binding offers (hereinafter NBOs) characterized by a high heterogeneity on the enterprise evaluation, and business model proposed[8]. None of these ensure a cost reduction compared to the target of the Restructuring plan. Moreover, the COG is anticipating such targets in its budget projections– the budget is already close to the overall 2020 target -, especially in terms of cash out, as highlighted in the following table.

[8] The bidders are the following:

	First group	Second group	Third group
Industrial partners	Engeenering IBM	Oracle TAS Group NTT Data	Cedacri group
Financial partners	Apax Partners Bergman Capital Partners	WDM Capinvest Highbridge	FSI
Advisor	Deloitte		KPMG

49 **Table # 5 –Provisional cash out trends of the COG (source COG Planning and Control)**

	Perimeter reclassified (a)		Restructuring Plan				Budget
IT Cash out	2016	2017	2018	2019	2020	2021	2018
Masterplan IT run costs	125.5	122.2	112.9	109.3	101.1	93.1	110.2
Masterplan IT run other expenses	29.7	28.9	26.3	24.9	24.4	22.5	27.9
Other costs	3.3	3.3	11.4	11.1	10.9	10.6	6.2
IT projects	130.5	138.8	134.6	129.1	128.6	123.1	118.8
Real estate projects							4.1
Total	**289**	**293.2**	**285.2**	**274.4**	**265**	**249.3**	**267.2**

(a) the perimeter reclassified excludes from 2016 the acquiring services sold in 2017.

50 On 17.04.2018, the management updated the BoD on the COG operations, strategic guidelines and possible industrial developments. The management highlighted the sustainability of the target of the restructuring plan (see table above) also in a standalone perspective. However, three strategic options were reported to the BoD: the first standalone driven by a business recovery of the MPS Group is not dependent on the IT Strategy. The other two effective strategies were a further downsizing of IT (currently pursued) and the implementation of the mentioned Venere project.

51 **Finding # 1 Uncertainties in the definitions of strategic options of the MPS Group**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, Sezione II, transposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that the body with the strategic oversight function shall be responsible on a general basis for the guidance and the control of the information system, in order to allow an optimal use of the technological resources supporting the company's strategies (IT governance). In this context, it must approve the development strategies for the information system in light of the evolution of the sector in question and in line with the existing or upcoming structure of the sectors of operation, of the corporate processes and of the company's organization.

The decrease in the budget for the IT needs, the high average age of employees, and the need to keep the IT resources in line with those of the competitors, with a low level of operational risks induced the MPS Group to review the IT strategy.

In this regard, the management is considering two options: a stand-alone strategy based, above all, on the increase in operating efficiency, and another one focused on converting the COG from captive into a market operator, providing IT services to different banks, as well as to MPS Group. Until the end of the OSI, however, at the Board's level, neither option had been framed in an

overarching consideration including the critical review of the Bank's business model, in the light of the role and the foreseeable evolution of IT. This is particularly important for the option consisting in the sale of the majority stakes of the COG, which would involve a radical organizational and operational change also with potential consequences on the Bank's broader strategies (e.g. due to a predictable long-term service supply agreement). However, this option has been pursued until non-binding offers from three associations of companies were obtained, in the absence of a preventive and fully-fledged assessment by the BoD.

Furthermore, the two strategies, reported to the BoD in the meeting of the 17.04.2018 pursue conflicting objectives. In fact, the stand-alone hypothesis focuses on the optimization of strategic and relevant projects reducing the overall investments (this approach is summarized by the catch phrases "do less to do more", "focusing on business project", "valuation of investments of the past"). On the other hand, the so-called “Venere project” pursues incremental objectives as increasing investments aimed at a currently undefined service strategy (“increase the level of investments for innovation, the development of new services and IT know-how”).

As a consequence, the “Venere project”, started in February 2017, still lacks an evaluation of the implicit strategic risks - the Risk Management function was only involved in June 2018 -, and of a preventive cost-benefit analysis As an example, the following facts that have not been adequately examined, yet:

a) only three comparable operations were conducted in Italy, two of which on the sole IT infrastructure and, only one on the entire IT system, for a bank five times smaller than BMPS; on the other hand, only the full outsourcing scenarios have been evaluated in the first round of non-binding offers;

b) the economic conditions shown to the potential partners are lean on the baseline of the Restructuring Plan while the anticipated achievement of the targets of that plan envisaged in the stand-alone strategy should be considered. Furthermore, the costs due to the retained organization needed to control the outsourcer and to manage the related risk (estimated at about 150 FTE) should be included. Moreover, the employees of the COG are seconded by MPS group, and costs might be impacted by the uncertainness about their possible return within the bank;

The flaws in the elaboration of a comprehensive IT strategy are due to the urgency of the actions implied by the Restructuring Plan that have hindered a deeper analysis of the links between IT and business in a forward-looking perspective.

The mentioned uncertainties in defining the IT Strategy could lead to a solution not consistent with MPS Group’s future business needs and business strategies.

52 The COG was previously a consortium not constituted in a corporate form, but starting from 30.06.2018 it has been transformed into a joint-stock consortium company, in order to benefit from the adhesion to the VAT Group regime of MPS Group starting from 01.01.2019[9].

53 The group is conducting a simplification plan which currently provides for the integration of the subsidiaries MPSCS, and MPSL&F. In this condition, the only relevant group customers of the COG will be BMPS (more than 95% of the revenues).

54 **Table # 6 – Revenues from COG customers in 2017 (source COG Financial Statements as at 31.12.2017)**

Customer	Revenues in 2017 (€/mln)	%/Total
BMPS	320.3	90.5%
MPSCS	12.9	3.6%
MPSL&F	3.7	1.0%
Widiba	3.6	1.0%
Other	1.0	0.3%
Not MPS Group	12.7	3.6%
TOTAL	**354.1**	**100%**

55 A hypothesis to integrate the COG in the bank was discussed among the management. For example, in the IT management committee of 25.01.2018 by the GM of the COG in the following terms: “For the change of tax regime, some institutions are reintegrating the IT part in the bank and our company could also evaluate this situation if the Venus operation did not materialize”. In fact, the change in the fiscal context (e.g. the VAT group regime of MPS Group starting from 01.01.2019) and the simplification of the Group have implications on the benefits of maintaining the Consortium as a separate entity, no longer linked to fiscal savings.

56 As mentioned, in the meeting of 17.04.2018 the BoD was updated on the Consortium's operations, approving the new “Documento di indirizzo strategico dell’IT” (IT strategic guideline document), consistent with the group Restructuring Plan, and defined in a perspective of an "efficiency improvement strategy" (i.e. of further downsizing). The IT function intends to pursue the following strategic guidelines: a) increase the quality of the service, b) spend less and better, c) reduce operational risks, and d) increase the motivation of human resources.

[9] A new legislation relating to the VAT Group was introduced by Law n. 232/2016 going into effect from 01.01.2019. The option to create a Vat group should be exercised by the Parent Company and all subsidiaries by September 2018 (the "all in, all out" principle is applied). These companies constitute a single indistinct subject for VAT, with the consequence that all the transactions between these companies are irrelevant for this tax (in practice, Vat is not applied to the intra-group transactions that occur within this perimeter).

57 The document then describes which levers the COG has tactically activated and intends to use to achieve these objectives, identifying, for each area (e.g. organisation[10], human resources, supplier management), the actions to reach them and allow the support of the objectives set. The actions are monitored by KPIs.

58 However, the IT strategy reflects more general uncertainties related to the context in which the group operates and the achievement of the objectives of the Restructuring Plan in terms of revenues: if not reached, automatic cuts in costs (the maximum between € 100 mln and the missing revenue compared to the target) are provided that, reflected on IT, can entail risks in the service provisions[11].

Project planning and budgeting

59 The overall budget decision, which includes also the IT component, is a centralized process managed by two different BMPS areas: a) the "Pianificazione" (Planning, under the CFO) in charge of running expenses, and b) the CP&CO, which oversees project investments of the Group. In September 2017, the latter area was moved to report directly to the CEO, with the aim to allow both a stricter control of the top management on this strategic area and a strong alignment of the Project Plan to the Restructuring Plan.

60 The targets of the latter in terms of profit and loss indirectly set the maximum amount of investments allowed per year. In order to define the "Project Plan", the Bank's Directions submit their project initiatives, by providing, at least, a generic indication of the objectives to be achieved and a preliminary cost-benefit analysis; the level of definition of the project contents in this phase can be very variable. Subsequently, as a result of the negotiation with business units, the CP&CO selects initiatives deemed eligible for funding and allocates the available budget. This budget is then assigned to the requesting functions and included in the overall BMPS budget managed by the Planning and approved by the BoD (the latest in the meeting of 01.03.2018). A relevant quote of this budget is allocated to expenses and investments in IT projects (47% of the operative expenses -opex- and 61% of the capital

[10] For example, to gain efficiency the COG has adopted an approach that focuses the human resources on single activities of run (i.e. ordinary management of the IT services) or change (i.e. IT project development). Recently, an experiment to further strengthen this approach has been conducted, creating a specialised task force to address specific efficiency issues.

[11] At the end of April 2018, the trend of total operating costs, € 759 mln, was well below the full year target (€ 2,410 mln), but the net margin (€ 406 mln versus a target of € 1,354) was still not in line.

expenses -capex- in 2018). The budget for the projects of Widiba is managed in a single item of the Project Plan as a relevant initiative.

61 The CP&CO supervises the Project Plan, in which the projects or the programs (i.e. set of more projects linked), are classified in four categories based on their relevance: a) Strategic (projects approved and monitored by the MC); b) Relevant (projects approved by the COP); c) Others: characterized by greater discretion (evaluated and approved by CP&CO); d) Plafond: small initiatives that cannot be defined or estimated a priori, whose responsibility is directly attributed to the business owners. The mandatory projects (i.e. due to regulatory commitments) are always strategic or relevant.

62 **Table # 7 – Project plan 2016-2018 (source CP&CO)**

€/mln	Capex						Opex - ASA					
Project portfolio	2016 actuals	ow IT COG	2017 actuals	ow IT COG	2018 budget	ow IT COG	2016 actuals	ow IT COG	2017 actuals	ow IT COG	2018 budget	ow IT COG
Mandatory projects	18,3	6,2	20,9	6,4	44,0	12,1	6,7	2,1	11,4	6,6	16,6	10,8
Strategic projects	55,2	15,2	74,8	35,0	37,3	20,7	5,5	1,9	10,2	1,4	6,3	1,4
Outstanding projects	24,3	12,7	16,1	6,7	21,8	8,5	1,4	0,3	2,7	0,8	1,7	0,2
Product catalog update plan	-	-	-	-	3,4	3,4	-	-	-	-	0,7	0,7
Other project	38,1	32,8	18,9	9,0	9,2	5,2	5,5	3,2	1,1	0,8	1,0	0,5
Technical reserve	7,1	7,1	7,1	7,1	9,4	8,8	11,9	11,0	7,2	7,2	8,0	7,3
Running reserve	32,1	1,1	44,8	21,0	-	-	1,5	-	1,2	0,1	-	-
Contingency reserve	-	-	-	-	1,6	1,6	-	-	-	-	0,3	0,1
IT personnel capitalisation	20,4	20,4	17,9	17,9	17,0	17,0	-	-	-	-	-	-
TOTAL	195,5	95,5	200,5	103,1	143,7	77,3	32,5	18,5	33,8	16,9	34,6	21,0

63 Within the bank and the COG, a relevant number of Committees have been implemented to manage the definition and monitoring of projects, fragmenting the decision making and the monitoring centre (see finding # 2)[12].

[12] For example: a) the MC verifies the consistency of the Strategic projects with the overall Group's strategy; and oversees strategic projects; b) the COP manages the process of the Relevant projects, it evaluates and approves their kick off, authorizing the release of the budget, and it monitors the results achieved and reports quarterly; c) the IT Demand Committee is divided into two sessions: executive and operative. In the first the committee should decide priorities on the IT requests solving conflict situations; in the operative session, the Demand Committee approves the business requirement (hereinafter BR, see below) and defines the project internal priorities; d) within the COG the Comitato Progetti IT monitors the progress of the project plan in the the IT development phase, discussing the KPIs for the evaluation, and highlights the critical issues.

64 Once approved, projects with an IT component are implemented by the definition of several "business requirements" (hereinafter BR). Within a project, a BR is a component with full operational independence in the execution.

65 In the BR, the business function defines needs, requirements and priorities, while the IT designs the technical solution. This process is managed by a team composed of members of the business, the demand manager (see below), organisation and the IT specialist. However, the need to coordinate multiple actors have led to delays in the definition of the BRs and a lack of effectiveness in defining priorities consistent with the Project Plan (see next finding).

66 The second part of the BR lifecycle concerns the IT execution and release, and it is manly managed by the COG. The "Project Specialist" is responsible, for a single BR, for the implementation, the quality of the results, the deadlines and the budget assigned; while the "Project Manager" is in charge of the overview of BRs included in the same project.

67 Until May 2018, the Demand Management in the BMPS Organization area was in charge of coordinating the business functions, the IT and Organization to deliver the BRs of the IT projects, with the aim to have an efficient resource allocation and improve time to market ensuring the quality of the services offered. However, these objectives were inadequately achieved. In the BoD meeting of 17.04.2018, the Demand function (about 20 resources) was transferred to the COG. The new solution would reduce the organisational complexity which slows the overall process since a coordination and an agreement among several subjects is required. In fact, the reform envisages a direct interface between IT and Business to shorten the "thinking time" and create only one point of monitoring of this process in the COG's Management Control Department. In this context, the Demand Committees were dissolved (the BR is approved directly by the business manager), while the Organisation should be involved only in case the IT process requires revisions of rules and processes.

68 **Finding # 2 Delays in strategic and relevant projects and inadequate involvement of the IT function in the group IT planning**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, Sezione II, transposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that the body charged with the management function shall be responsible for ensuring the completeness, adequacy, functionality (in terms of effectiveness and efficiency) and reliability of the information system. In particular, it must establish the organizational structure of the IT function, ensuring that over time it corresponds with the strategies and architectural models established by the body charged with the strategic oversight function.

The definition and the management of the Projects Plan have been affected by shortcomings, reflected in an inefficient achievement of corporate strategies concerning the implementation of strategic and relevant IT projects. In fact, the analysis carried out by the OSI team highlighted:

a) Delays in the realization of such projects: 68% of them accumulated delays compared to the initial planning, and they were completed 6 months later than expected on average. The long-term projects (duration equal to 2/3 years) show the worst performance (e.g. EDM, Monte Project Shield; Sistema informativo filiali estere; Programma Banca Più) compared to the short-term ones, generally in line with the timing scheduled;

b) The proliferation of numerous non-strategic investments, generally of small amount on average, that accounts for 28% of the IT external expenditure, and 47% of IT projects in 2018, with a consequent failure to focus the IT function on strategic initiatives. In 2017, the business requirements (hereinafter BR) produced by the “other projects” were 69% of all ended BR, and in the first part of 2018 they are still 44%. This is also due to the plafond agreed in the Project Plan for the business units to allow them some flexibility in the budget management, in a context of inadequate monitoring;

c) a consistent backlog of BRs, in 2017, 577 BRs equal to 24% of the total, which is further growing in 2018, 671 BRs equal to 47% of the total as of end of May 2018;

d) lack of previous analysis for the estimation of IT capability. Indeed, the estimation of IT expenses within a business case is carried out by the business units and the process did not envisage a formal validation by the IT function nor a “capability” evaluation with regard to the internal IT resources (e.g. all projects are planned in the first half of the year without a prioritization). It was only after the 2018 budget approval that the IT function conducted an in-depth analysis on “IT capability” to estimate the sustainability of the project plan compared with resources and the budget available within the COG. Such analysis highlighted some errors in cost estimations and the unfeasibility of the project plan within the scheduled time; in fact , to meet deadlines set by the plan on strategic and relevant projects, the COG has planned to reallocate internal resources and to postpone the “other projects” to the second half of the year or to 2019;

e) The monitoring activities are currently focused on the BR lifecycle, however, also the time from the project kick off, from the complete definition of the relevant BR and from the BR approval and the IT execution should be monitored. Such monitoring suffers from inhomogeneous approaches of the Project Management (hereinafter PMO) to the management of the project and to the correct recording of the data of the project.

The described situations are also due to the fragmentation of the project implementation and monitoring processes, and to the multiple decision-making centres (e.g. Management Committee for strategic projects, Operational Project Committee for relevant projects, business owner for other projects, the Demand Committees executive session for the prioritisation of the execution of the project, other committees in the COG). In such a context, the Chief Program & Cost Officer (hereinafter CP&CO) who should have the central responsibility for this process, is substantially involved in the initial definition and in the final reporting (e.g. the said function does not have any access to the BR information) .

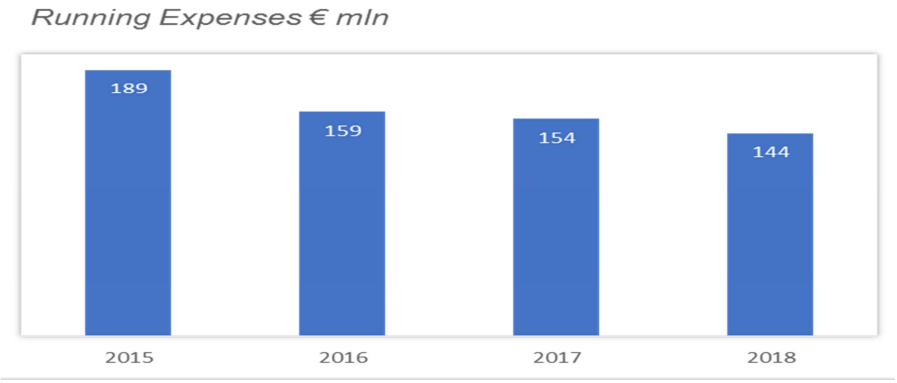
The recent reorganization of the Demand function, moving them to the COG, should ensure a partial enforcement of the Project Plan execution and a reduction in the whole chain of responsibilities. However, a simplification and shortening of the decision making process and a concentration of the monitoring processes need further steps (e.g. require the approval of the single initiatives envisaged in the "other projects and plafond" after that their contents is defined; strengthening the PMO function and on statistic collections).

Such shortcomings in the management of this process could lead to an inefficient use of the limited available resources.

69 The Group will adopt a more rigorous process for the estimation of IT costs involved in the Project Plan, performing the analysis of sustainability in the coming year simultaneously with the project plan approval. Regarding the process of implementation of a project through the BR management, the bank estimates that, on average, the definition and the IT execution of a BR require 84 days and 135 days respectively, with an overall "time to market" of 219 days in 2017. The COG is committed to a relevant lowering of these time frames (in April 2018 they were reduced to 187 days). Moreover, the bank is focusing on the reduction of the "other projects" in a strategy that would privilege the effort on the strategic and relevant ones.

70 The budget for running expenses is entirely assigned to the IT function (the COG) that negotiates it for all the entities of the Group (including also Widiba). In this case the IT function discusses with the "Area Pianificazione" office, which reports to the CFO, in order to define the budget needed to manage the ordinary workflow. The running expenses in the last years have seen a strong reduction (-24% from 2015) because the COG has pursued an aggressive costs cutting strategy, (e.g. mostly focused on suppliers).

71 **Figure # 7 – Running expenses (source elaboration of COG Planning and Control)**[13]



72 The 2018 budget for running IT operating expenses (€ 85.3 mln for the COG) has been cut by € 1.7 mln compared to the preliminary estimates of the COG. In order to achieve these further savings, the COG Management Control function is evaluating different assumptions, the main one being the renegotiation of the contract with IBM (the main supplier of hardware and services).

3.1.3 Risk profile, risk appetite and risk strategy

73 The IT risk appetite and tolerance thresholds are established annually in the RAF: if the potential risk exceeds the IT risk appetite, suitable mitigation measures must be promptly identified to contain it within the limits defined in a maximum time horizon of 12 months. The Group RAS for 2017 established that IT risk should not exceed the "Medium" level. In the cascading down of the RAS 2017, three Key Risk Indicators were defined relating to the major incidents on IT resources, serious security incidents (notified to supervisors)[14] and fraud on Internet Banking customers. As emerged in the following figure, the tolerance threshold for the serious security incidents was not met in 2017.

[13] It includes the overall COG running costs, including also non-IT components.

[14] The serious security incidents are those envisaged in the Banca d'Italia, Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, sezione 1, linked to: high economic losses or prolonged disservices, b) significant disruptions on customers and other subjects, and c) the risk of undermining the bank's ability to comply with the conditions and obligations of the law or envisaged by the supervisory regulations. The concept of security in the regulation is wider than logical or cyber security, and includes also the continuity and the compliance of the system. In general, in the present OSI report the security concept is instead referred to logical and cyber security.

74 **Figure # 8 IT risk Risk Appetite Assesment (source IT Risk Report 2017)**

KRI on ICT risk		unit	RAS 2017 Appetite	RAS 2017 Tolerance	Profile 2017
IT Risk	High risk IT resources (risks not mitigated within 12 months)	num (stock)	0	0	0

KRI on ICT risk		unit	RAS 2017 Appetite	RAS 2017 Tolerance	Profile 2017
IT Incidents	Major incidents on IT resources	num (flow)	12	24	10
	Major security incidents on IT resources	num (flow)	0	1	2
IB Frauds	Frauds on IB clients	%	0,0010%	0,0035%	0,0003%

75 Moreover, in the RAF the evaluation of the IT risk is integrated by a judgmental assessment driven by the adopted methodological framework based on two kinds of analysis:

a. A "Low Level" analysis carried out on a perimeter of IT assets, selected yearly on the basis of confidentiality, integrity, and availability criteria (hereinafter CIA). In 2016, about 650 IT assets were scored, and a perimeter of 370 (of which 237 had been analysed at the end of 2017) were chosen for the assessment with the low level methodology according to a three-year plan (2016-2018);
b. A "Top Level" analysis, with the aim of evaluating the comprehensive risk situation of the IT function and this applies to the single IT sector (Technological architecture Service, Application architecture Service, etc.) based on Key Risk Indicators (KRIs). The COG has implemented a specific set of KRIs for the IT Security sector that are different from those applicable to the other 38 sectors.

76 When the analysis rates "high" the risk of an IT asset or of a sector, the IT Risk Management identifies the areas for improvement and the actions (gaps) that should lower the risk to the level accepted by the RAF within a scheduled time, recording and tracking them through the RIGAM procedure. The adoption of a recommendation by the control functions is a powerful governance tool for the MPS Group, since the closing of the gaps in the scheduled time frame is strictly monitored by the control Bodies (i.e. Risk Committee and BoSA).

77 The IT Risk management approach is methodologically correct, however deficiencies emerged in the application of the IT controls and in the effectiveness of the IT Risk function in COG and in Widiba.

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**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, Sezione III, transposing artt.

74.1 and 88 of Directive EU no. 36/2013, states that the analysis of IT risk is an instrument for guaranteeing the effectiveness and efficiency of the measures adopted to protect IT resources by making it possible to graduate the mitigation measures in the various environments according to the bank's risk profile. The analysis must establish the residual risk to be submitted for formal acceptance by the system owner. If the residual risk exceeds the bank's IT risk appetite approved by the body charged with the strategic oversight function, the analysis must propose the adoption of alternative or additional risk treatment measures, drawn up in cooperation with the risk control function and submitted for approval to the body charged with the management function.

The MPS Group Risk Appetite Framework envisages that a potential IT risk cannot exceed the medium level. If this level is exceeded, mitigation measures must be promptly identified.

In 2015, the IT Risk Management function of the Parent Company and its COG functional reporting, on the basis of the analyses conducted, rated high the level of risk in the IT Security Service of the Consortium, due to several IT security weaknesses, as reported to the BoD in the meeting of 25.02.2016 in the "Relazione sul Rischio Informatico - Anno 2015" (Report on IT Risk – Year 2015). As a consequence, twenty actions were planned to overcome the related security gaps that should have been completed by the end of 2016 to reduce the risk. Such actions were included in the Monte Più Sicuro project (hereinafter M+SP).

In January 2017, the IT Risk Management certified the closure of these gaps based on the statement given by the units in charge of the remedial actions about their completion. Consequently, the risk of the sector was assessed as lower compared to the valuation of the previous year and was reduced to medium in 2017.

However, the OSI team ascertained that the closing of the following gaps was not effective, since the alleged solutions were based only on the drafting of a document about a new security process or on a software selection instead of an effective implementation of a process or an effective adoption of a security procedure:

a. Privileged user management;
b. Formalization and enforcement of the security incident management process;
c. Periodic reporting on security incidents and events;
d. Acquisition and implementation of vulnerability assessment products;
e. Review of the secure software development lifecycle.

In fact, the abovementioned security problems related to the twenty actions identified, are not substantially solved.

In addition, the gap on the organizational security sector was declared closed in January 2017 even if the organizational analysis of the security sector was completed only in April 2017.

The OSI conclusion is also supported by the fact that such activities are still planned in the M+SP, which has now become one of the four workstreams of the larger Monte Protect Shield project (hereinafter MPSP), with the overall conclusion scheduled for the beginning of 2019.

The unfounded closure of findings, without the problems being effectively overcome, has reduced the management commitment to such actions.

79 The Report on IT Risk year 2017 of the COG, highlights areas for improvement of the risk analysis linked to the weaknesses of some IT processes (e.g. incident and problem management, architectural assessment); the OSI verified the consistency and correctness of the IT Risk Management evaluations; among them, the IT Risk Management reports the lack of a security incident detection system that is one of the gaps considered already closed in the mentioned certification of January 2017 (see point b. of the above finding).

80 **Finding # 4 Weaknesses of the Group IT risk assessment**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, Sezione II, transposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that a risk control based on continuous information flows on the evolution of IT risk and a monitoring of the effectiveness of the measures for the protection of IT resources should be implemented by the second-level control functions. The management of the overall IT risk must be linked with the analysis of the individual IT resources. The assessments made must be documented and revised at least once a year in the light of the results of the monitoring process.

The Risk Management of MPS Group has defined a methodological approach for the evaluation of the IT risk that provides for the parallel operation of two types of analysis, "Top Level" and "Low Level". The OSI analysis highlighted: a) the need to strengthen the level of assessment and to improve the methodological approach of the application of the model in Widiba; b) in the COG the level of analysis already achieved, is, however, affected by the defects reported below.

With regards to Widiba, the 2017 Top Level analysis is based on a set of six indicators not sufficient to objectively measure the IT risk; in detail:

a. unlike the COG, there is no specific analysis of the security risks compared to general IT risks;
b. four indicators substantially analyzed only two phenomena; in fact, the KRIs, FRD (Sum of losses suffered by online customers for computer fraud) and CFRD (Percentage of online customers who have suffered losses, out of total online customers) monitor both the level of fraud, while GAP (weighted sum of the active gaps issued by the Control Functions on the Widiba IT Function) and PT (sum of the vulnerabilities detected by the internal vulnerability assessment and penetration test) must be aggregated because the audit did not perform any

activities in 2017, relying on the results emerged in the internal penetration test done by the same company used in the ethical hacking performed in 2016;

c. the DQM (the number of manual interventions on data in production) scale was based on the observation of only one year value (with no other benchmark) that was set to medium risk;
d. the reliability of the INCIDENT indicator (weighted sum of IT incidents) suffers from a not fully traceable process of the incident management (see finding #11);
e. indicators about both security (e.g. security offenses or incidents) and the quality of the development process (e.g. indicator about efficiency and stability of the software internally developed) are substantially missing.

With regard to the analysis carried out on each single IT asset (Low Level), different components (e.g. Software Infrastructure, Database, Infrastructural product) characterized by different technicalities, complexity and criticality were aggregated in only one asset without an adequate granularity. Moreover, the potential risks emerged from the scenario analysis were considered mitigated by controls declared by the IT function without an effective challenging of these controls by the internal IT Risk Management.

The Top Level analyses of the COG are more structured and the Low Level analyses are conducted with a more challenging approach with the IT asset owners. However, the model is not entirely robust with regards to the following:

- in the Top Level analysis of the IT security function, KRIs about the security offenses and incidents are missing;
- the adoption of the BITSIGHT indicator (a market benchmark about IT security) per se is not representative of the risk level without taking into account its components (e.g. Open ports in which the bank is valued “A” -the best grade- or Application security in which the grade is “D”, the fourth of six levels); moreover, the indicator used for the COG is contaminated by the Widiba's IP addresses;

The OSI highlighted the need to strengthen Widiba’s IT Risk Management, with a greater oversight by the group function in charge, and to increase the critical review of the indicators by the IT Risk Management of the COG.

The above reported weaknesses could hinder an objective IT risk evaluation. The formal application of the model in Widiba led the IT Risk Management to miss the opportunity to gain a deeper knowledge of the grade of controls of the innovative platform.

81 Bitsight is an entity specialised in scoring the It corporate security. By leveraging the security information available on the global network, Bitsight applies an algorithm to generate a security classification (e.g. the mentioned BITSIGHT indicator).

82 Widiba has planned an integration of the methodology for the IT Risk that envisages: a) the integration of the KRIs for the Top Level analysis (e.g. FIX1 weighted number of corrective fix), or used to improve the set of information (e.g. CYBR for the number of external cyber-attacks); b) a more analytical approach to the asset of the Low Level analysis. Such implementations are scheduled by the end of 2018.

3.1.4 IT Compliance

83 The Compliance organisation, including the IT Compliance, was reviewed starting from 2016, following the outcomes of the OSI-2015-ITMPS-32-33 on Internal Governance and Risk Management. The IT Compliance activities covered the parent company, and, indirectly the COG, while the coverage of the group entities is still incomplete.

84 **Finding # 5 The IT Compliance function was not activated in Widiba**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, Sezione II, transposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that the internal control system responsibilities must be clearly assigned for the performance of second-level controls regarding the observance of the internal rules and external provisions concerning IT (IT compliance), guaranteeing, inter alia, the consistency of organizational arrangements with external provisions, for the parts concerning the information system.

The IT Compliance function in Widiba has not been activated since its foundation at the end of 2014, nevertheless the organization and the processes of the subsidiary are based on a central role of the IT structure. It was only during the OSI, in June 2018, that the BMPS IT Compliance started the activity to verify the compliance of Widiba with the provisions of Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4 on Information System.

As a consequence, the OSI recorded the non-compliance with Banca d'Italia provisions for IT management of the policy implemented by Widiba on IT security (see finding # 11) and on IT continuity (see finding # 13).

85 In the 2018 Compliance plan the coverage of the cyber security topics is envisaged.

3.1.5 IT Audit

86 The IT Audit activities are characterised by an adequate depth of analysis and assessment, and conducted also by means of vulnerability assessments and penetration tests conducted in the COG and in Widiba (so called ethical hacking). However, a limited number of checks was carried out, only 14 interventions in 2017, without covering a sufficient perimeter.

87 **Finding # 6 The scope of IT Audit Plan is limited and only partially adequate to mitigate the IT Risk**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, Sezione II, transposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that the planning of inspections by the IT Audit must ensure adequate cover over time of the various applications, infrastructures and management processes, including any components that are outsourced. Regardless of the form chosen for carrying out the reviews, the internal audit function must be able to provide assessments of the main identifiable technological risks and of the bank's overall management of IT risk.

The number of IT audits and the topics covered in the period analyzed by the OSI (12 in 2016, 15 in 2017, 12 scheduled in the 2018) are not sufficient, considering that:

a) since its foundation, at the end of 2014, and until the end of the inspections the IT of Widiba was audited only five times. In 2017, due to the postponement of the audit on the anti-fraud platform, no IT audit was performed on the subsidiary which, given its strong focus on innovation, is characterized by a significant potential exposure to technological risks. For example, the IT Audit has not covered change management, incident management or IT continuity activities.

b) Relevant areas in the COG have not been covered by IT audits in the last three years and in the 2018 audit plan, e.g. IT outsourcing management, nevertheless, important IT functions were outsourced (e.g. mail services, first level SOC); the identity management was verified in 2014, while the incident management (in particular about cyber incidents) was not audited.

The said flaws may result in the failure to detect significant risks in the areas not covered by the IT audit.

3.2 System architecture

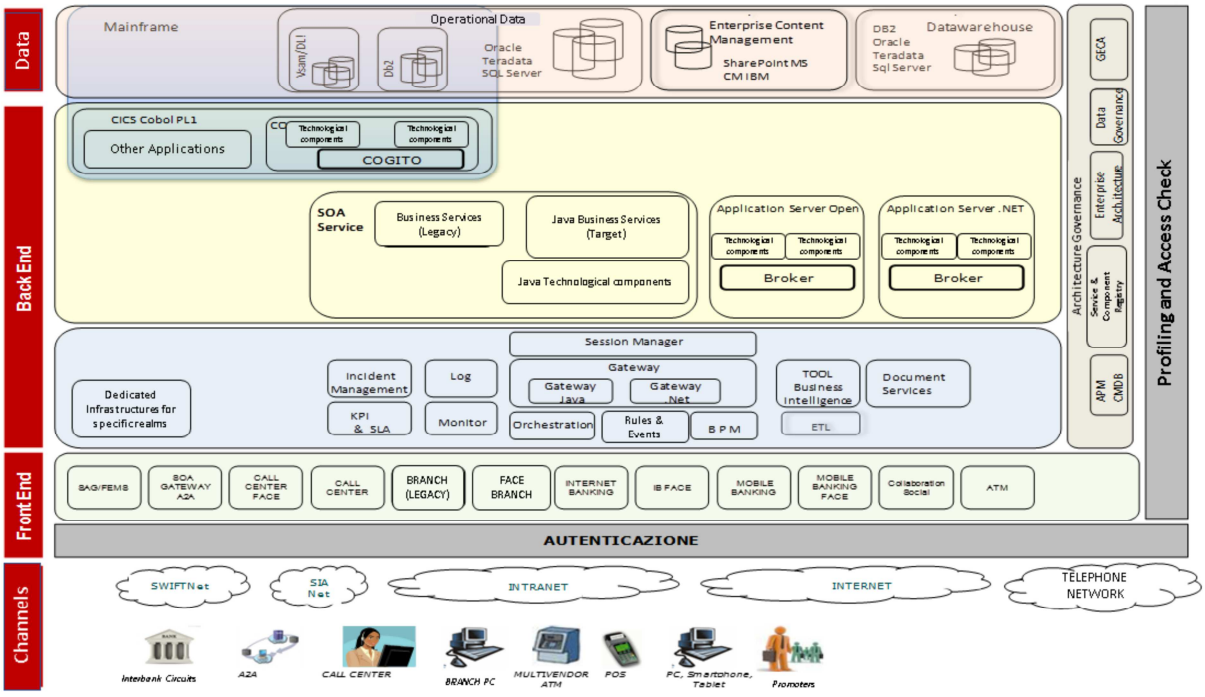
88 The IT system architecture is commensurate to the banks' (both Widiba and BMPS) business needs and could be open to future technological updating to provide support to new prospective business activities, in a predictable scenario of bank systems evolution (e.g. increasing digitalization of banking processes, mixed channel model).

89 For the COG the application and network models are documented and the configuration management database (hereinafter CMDB) is sufficiently updated. The CMDB contains the list of the applications and technological assets present in the data centres and, among other information, for each application the following data are recorded: the map of the dependency from the other applications, the name of the server where the application is running and the

list of the application software components. The technical documentation is complete and covers the application architecture, the network of data centres and the database storage area; other technical documents describe the mainframe and middleware systems' configuration (e.g. CICS, application servers).

90 The model adopted is based on the Service Oriented Architecture (SOA paradigm) with multiple presentation layers (user interfaces) based on a three-layer schema, which permits the interoperability of heterogeneous platforms (see next figure). The most important user interface present in the front-end layer is the internet banking (also named digital banking) that is implemented using J2EE technology. Widiba and BMPS are using different digital banking platforms, also if they started from the same ones, the front end of Widiba, about three years ago. In fact, the IT function of Widiba and the COG have evolved and maintained their front-end autonomously, without coordination, at least for security aspects (see finding # 7). The COG offers to Widiba a housing service to locate the front-end, but the system and the network are separated and managed independently.

91 **Figure # 9 – BMPS IT Architectural scheme (source presentation "Application Architecture – As is situation")**



92 The back-end logic is almost totally developed using mainframe technology (PL/I and Cobol language), and has been integrally coded by the COG; furthermore, most of the common components used in mainframe environment (e.g. Customer Information Control System –

CICS) have been customized to better fit the business requirements. A customized framework library (named COGITO) has been developed and incremented during the years to optimize and standardize the coding of mainframe services.

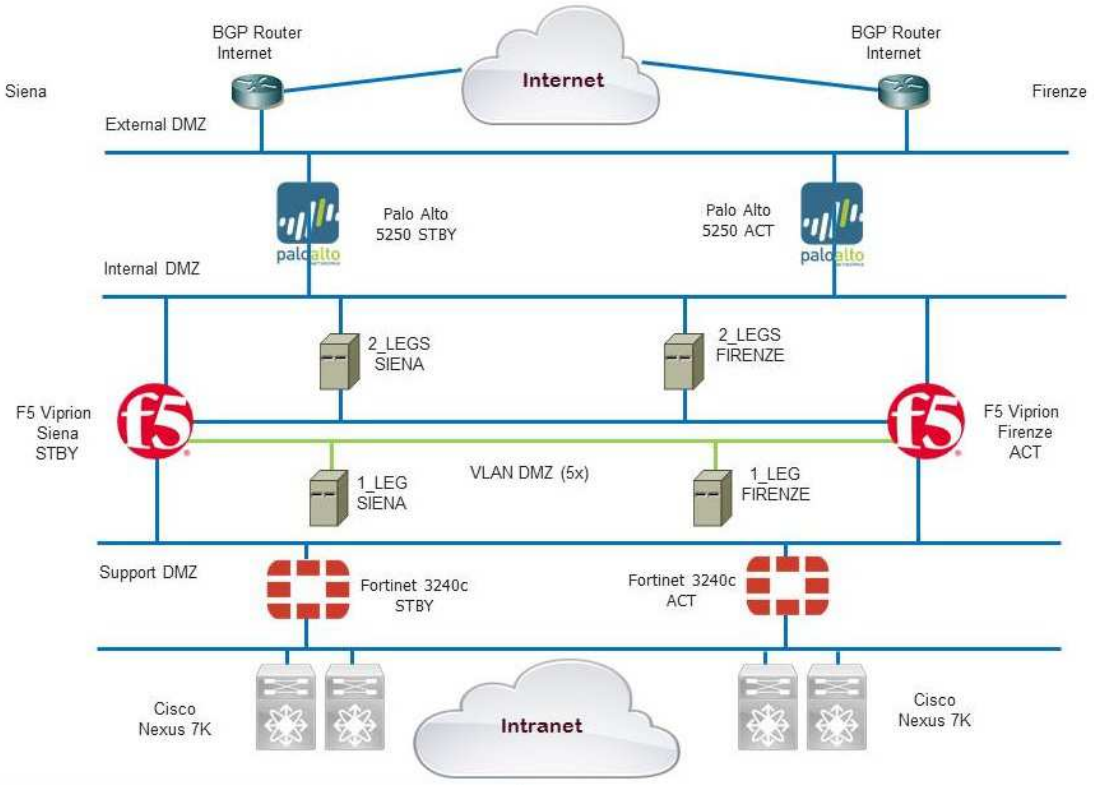
93 The services implemented in the mainframe environment are published using .NET and J2EE technologies which create the SOA service layer that is called by the front-end applications to implement a synchronous communication. SSL certificates are used to trust the communication between the front-end and back-end. A set of message queues servers provides a channel for the asynchronous communication between front-end and back-end (it is used, for example, when the front-end asks the back-end to execute a batch procedure).

94 The data centres are located in Firenze (the primary) and Siena, and with regard to the high availability, the systems that serve the front-end are configured as active/active while the back-end is configured in active/passive mode. In 2016, the geographic configuration of the two sites was evaluated as fully satisfactory for the MPS Group. In fact, the solution adopted ranked third, in terms of security, compared to the configurations of the main Italian banks, being able to boast two sites at a distance of 60 km, with synchronous replication and an extremely remote probability that they might be both compromised[15].

95 The Storage Area Network (hereinafter SAN) ensures that the transactions are simultaneously replicated with a delay of 1.2 ms in the two data centres, both for the database of the back-end and front-end layers.

[15] The impact analysis update, commissioned at the University of Siena in July 2016, showed a medium and medium-low seismic hazard (respectively for Firenze and Siena), an absent geomorphological hazard and a medium hydraulic hazard for Firenze.

96 **Figure # 10 – BMPS IT Network scheme (source presentation "Network architecture of the Data Centres")**



97 The Palo Alto device (see above figure) provides the first level of firewalling, filtering and inspecting the traffic in outbound and inbound from the Internet to the data centre's web servers. It ensures the monitoring of malicious activities coming from the Internet channel. The F5 web application firewall balances the traffic between the web servers and the application servers and the databases present in the front-end layer. At the same time, it performs specific controls on the network traffic to improve the security of communication. The communication in outbound and inbound the back-end area is controlled by the Fortigate Firewall. The said network schema is also adopted by Widiba to manage the network traffic in its front-end layer. The only difference is in the manufacturer of the firewall devices (Huawei).

98 The connection between the two data centres (Firenze and Siena) is ensured by two dark fiber provided by two carriers, and the Dense Wavelength Division Multiplexing (hereinafter DWDM) technologies supplies a bandwith up to 10Gb/s. To improve the interoperability of

the two data centres, a set of geograpichal area networks have been set as an extension of some Virtual Local Area Netwoks (hereinafter VLAN) of the two data centres.

99 Widiba designed the online banking platform (hereinafter BOL) in 2013 using an open-source model and adopting the Agile software development approach. This strategy has allowed the bank to reduce the time to market and the risk of vendor lock-in. The developers team collaborates with the open source community and has a good know-how for managing the platform's maintenance and evolution.

3.3 IT security management

3.3.1 The Monte Più Sicuro and Monte Protect Shield projects

100 In May 2015, the BMPS, through the self-assessment carried out in the ECB questionnaire on cyber-risk exposure, evaluated a high exposure to the IT Security Risk, as reported in the "Relazione sul Rischio Informatico - Anno 2015" (IT risk report – year 2015) of February 2016. As a result, a list of tasks and objectives was prepared to mitigate the highlighted risks. Therefore, a project was launched in the COG (the M+SP) with three main goals: i) to ensure compliance with regulatory standards; ii) to reduce the risk to an acceptable level, taking into account economic constraints iii) to foster a cultural transformation in the cyber security. The M+SP was presented for approval to the COP on 30.03.2016.

101 In April 2016, the COG commissioned a new IT Security assessment to Deloitte, to ascertain if the already planned mitigation activities would have been sufficient to lower the risk level. The Deloitte's analysis confirmed that the IT Security risk was high, identifying further gaps in IT security. The already planned activities, if completed on schedule - the end of 2016 - would have allowed to achieve a medium-high risk posture. To get an overall medium posture, the COG promptly integrated new mitigation activities in the said M+SP.

102 The Deloitte gap analysis assessed that important security weaknesses should have been quickly resolved:

a. Logical attacks: APT[16] and/or software vulnerability exploits; vulnerabilities on personal devices allowing an unauthorized access to information and other weak points;

[16] Advanced Persistent Threats – a special kind of hidden logging finalized to acquire a user behaviour including all its application access rights to suddenly take advantage simulating and exploiting this knowledge by movements of money to criminal associations

b. Misuse: access rights escalation; high probabilities of errors by untrained personnel; faults due to wrong application design (including secure code development lifecycle, tests and change management processes); faults in hardware assets.

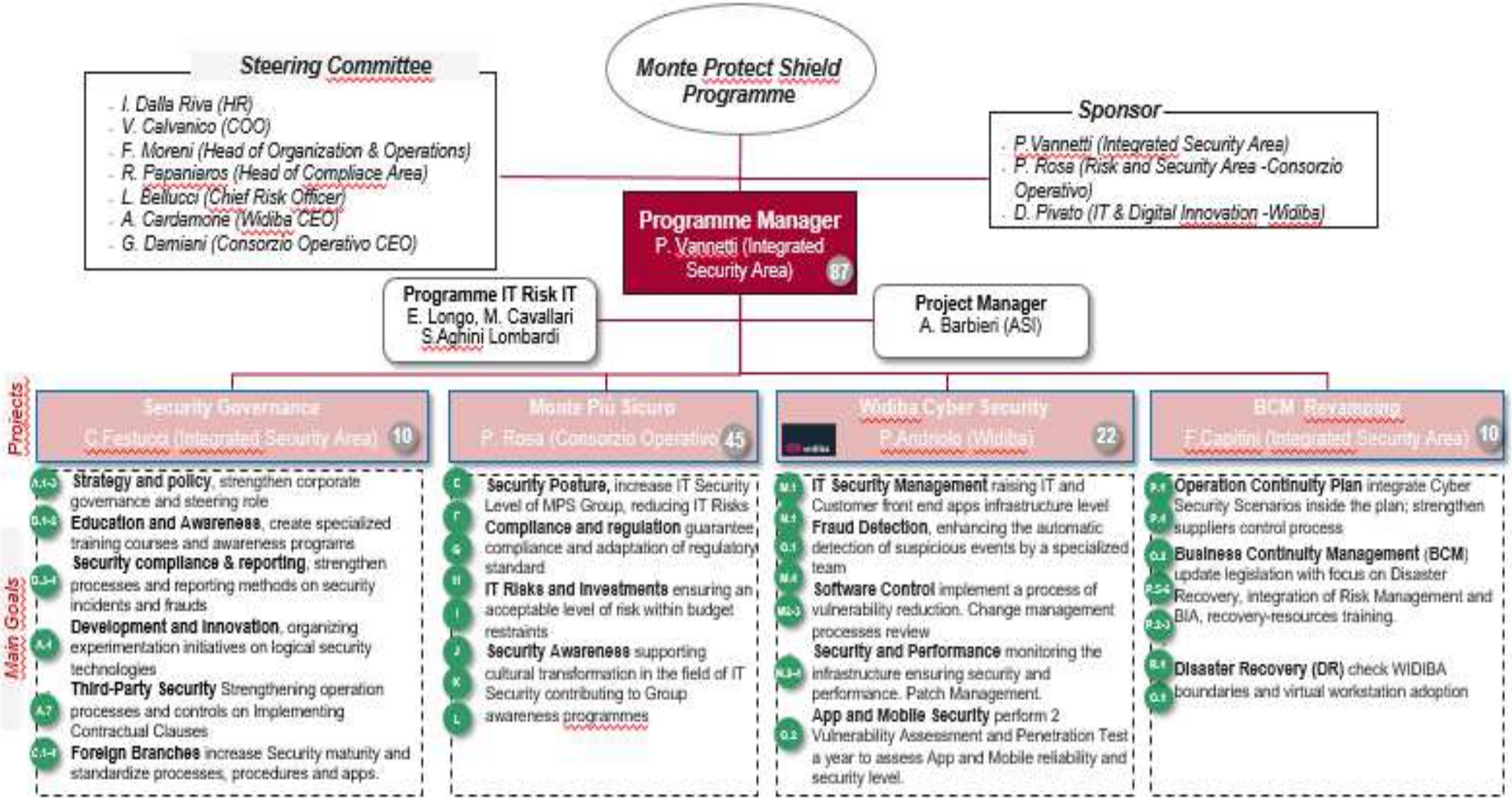
103 At the beginning of 2017, Accenture was engaged by the ASI to carry out an IT Security Maturity Assessment on the whole BMPS Group. At the end of April 2017, Accenture reported on the expected IT maturity by the end of the year 2017 and at the end of 2018[17], considering market benchmarks and regulatory requirements. Its report highlighted weaknesses mainly in the security strategy role, in the learning and awareness process, in the security compliance, in the research & development and in the supplier security compliance.

104 During the COP meeting of 05.07.2017, the M+SP status was updated and the need to postpone some planned M+SP activities was reported because of a reduction in the resources due to the Restructuring Plan. Moreover, it was reported that, according to the Accenture's benchmark, by the end of 2017, the BMPS would have achieved an adequate maturity in the sectors that have been identified and rated as weak. In October 2017, the M+SP has been incorporated in the wider MPSP project to close the gaps reported by the Accenture's assessment on Widiba, on ASI, on the COG, and on business continuity management (hereinafter BCM).

105 The MPSP (see next figure) consists of four sub-projects: i) Security Governance to enforce the role of ASI in steering the MPS Group IT security; ii) M+SP; iii) Widiba Cyber Security focused on the IT security implementation in Widiba; iv) BCM Revamping aimed at updating the business continuity management process.

[17] See "Maturity Assessment Sicurezza Logica (Accenture2017).pdf"

106 **Figure # 11 – Monte protect shield project structure (source Project presentation)**



107 The overall budget (capex and opex) used in the M+SP amounts to € 2 mln and to € 3.7 mln in 2016 and 2017 respectively. Moreover, in the last years the project has not absorbed the whole budget assigned. The 2018 budget for the M+SP amounts to € 4 mln, while the overall budget of the MPSP is € 5.3 mln.

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**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, Sezione II, transposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that the organizational structure of the ICT function is based on functional, efficiency and security criteria, clearly defining tasks and responsibilities and providing for the responsibilities and arrangements for the planning and control of the portfolio of ICT projects (including the governance of changes in the architecture and of technological innovation) and for the activities involved in the operation of the information system.

The M+SP, incorporated in the wider MPSP, has not achieved all expected benefits in the security area. The original goals to address the relevant weaknesses emerged in 2015 and at the beginning of 2016 (highlighted by the self-assessment performed in the ECB Questionnaire and by Deloitte) were inadequately pursued, showing relevant delays. In fact, the OSI team observed that:

- The activity tracking and the conclusion of the scheduled tasks of the M+SP were not correctly recorded, in a context of almost simultaneous change in M+SP management, both in the Security areas of BMPS and the COG.
- The goals mentioned in the finding # 3 (see bullet points from a. to e.) have been split in two or more sub-activities (e.g. software selection, installation, rollout), only carrying out the initial steps; for example: CyberArk was only installed but it is not used for the individual privileged user management yet; Fortify, the tool for the code development security checks, was tested in January 2017 with its first round and no longer used;
- The delays in an accountable incident management process or an effective privileged user management (see finding # 9), have not been mitigated by any tactical solutions;
- The MPSP, started towards the end of 2017, currently shows a renewed commitment; however, it still fails in the coordination of important security aspects between the COG and Widiba. For example, the COG is unaware of the Linux security weaknesses discovered by Widiba on the similar digital banking platform used by both.

In May 2017, the budget assigned to the project was cut compared to the expected needs of about 20%, limiting the possibility of reaching the expected goals. Moreover, the IT Security spending of MPS Group versus the total IT spending was only 2% in 2016, 4.1% in 2017 and is envisaged to be

5.1% in 2018, compared to the system average of 6%.

The M+SP poor management and the partial results achieved have not adequately removed the weaknesses detected, consequently, the MPS Group is still exposed to the related threats, considering also the external IT security changing scenario.

109 With regards to Fortify implementation, during the OSI the platform was adopted as a "security gate" in the software development lifecycle (i.e. a control is carried out before going into production). However, only one round has been carried out so far.

110 At the end of 2017, the BMPS took out a cyber insurance to cover up to € 20 mln damages (exceeding a minimum of € 0.5 mln per each event) to mitigate the main risks.

111 **Figure # 12 – Cyber-risk insurance (source Memo for the BoD of 14.11.2017 about the subscription of a Cyber-risk insurance)**

Type of effect and applicable coverage								
Risk Categories	Incident Management Costs	Notification Costs	Legal Fees	Direct Financial Loss	Refund Requests	Sanctions	Material Damages	Business Interruption
Confidentiality Breach - PERSONAL DATA	Cyber	Cyber	Cyber		Cyber			
Confidentiality Breach - BUSINESS DATA	Cyber		Cyber		Cyber			
Non authorized Withdrawals/Trading/Money transfers - CUSTOMERS	Cyber	Cyber	Cyber		BBB			
Fraudolent Use of Data - CUSTOMERS	Cyber	Cyber	Cyber		Cyber/ Card Frauds			
Illegal Transfer - BUSINESS FUNDS				BBB				
Banking Systems Unavailability/Interruption - NATURAL EVENTS							Elettronica	Elettronica
Banking Systems Unavailability/Interruption - CYBER ATTACKS	Cyber		Cyber		Cyber			Cyber
Disruption or Encryption - BANKING DATA	Cyber							Cyber
BANK MEDIA/WEBSITE contents	Cyber		Cyber		Cyber			

Cyber	Risk covered by Cyber Policy - to be stipulated
BBB	Risk covered by BBB Policy (Bankers Blanked Bond - Global Policy Banking Institutes) - Active
Elettronica	Risk covered by Electronic Policy (direct physical damages) - Non Active (canceled in 2013)
	Non-insurable Risk

Ensurable Effect | Non-Ensurable Effect | Non-Applicable Effect

3.3.2 Policies

112 The IT Security related policies are mainly based on two layers: a) the ASI defines the main guidelines for the topics considering also legal and regulatory bounds; b) the COG, Widiba and the other subsidiaries implement the guidelines in specific and operational aspects in their context. In this implementation, they could extend the minimum requirements expected by the guidelines. Among the mandatory requirements for Widiba and the COG, the following are envisaged: a) the security incident response must be available 24 hours for 7 days (hereinafter 24x7), and any identified threats require a risk evaluation of the current systems

and a vulnerability assessment b) the application developing and updating phases must use secure software development methodology.

113 The COG has implemented several policies to regulate security aspects (e.g. Incident Management policy, Cybersecurity Incident Management policy and Access Control Management). The severity evaluation in the Incident Management policy is based on a precise definition of Major Incident, in terms of assessed impacts according to economical, geographical, availability and regulatory dimensions. In the same policy, a priority evaluation is also considered based on the urgency and on the impact associated to the event. The Cyber Security Incident Management process provides for the conditions to classify a Major Incident using the same criteria specified in the Incident Management policy mentioned above.

114 In general, the BMPS policies are adequate considering all the main aspects of the security topics, while the transposal by COG and Widiba should be improved (see finding # 8, 9, 10 and 11).

3.3.3 Procedures

The Identity Management process

115 The Identity Management process starts with the assignment of a new user to an organization role by means of PaschiPeople (i.e. a customized version of People by Peoplesoft). An automatic workflow registers the user in the BMPS Windows domain. The user is then enabled to access the systems by means of his/her credentials: almost all applications (529 over 582) are enabled to be compliant with the Single Sign On (hereinafter SSO) infrastructure[18].

116 By policy, the user appointment is formalized by a document that specifies the credentials (user id and the first one-time password) handed over to the concerned person who signs it.

117 Within the COG the target platform to manage the authorisation profiles is the Oracle Identity Management (hereinafter OIM), but there are still two residual ways in place to manage them:

[18] The SSO infrastructure is one of the core infrastructure components that allows to pass identity between different technologies like Microsoft Active Directory, Linux and host based systems.

a) The Nuovo Controllo Accessi (hereinafter NCA) was developed years ago to manage, together with other components (e.g. the unified log system, the session manager), the user profile access rights of the internal developed applications. Most of the authorization management of NCA was migrated to the OIM, but it is still used for the host applications. An automatic reconciliation process is carried out between OIM and NCA.
b) the applications not integrated with OIM.

118 **Finding # 8 Weakness in the Identity management process of the COG**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, Sezione IV, transposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that the security of information and IT resources must be guaranteed by physical and logical security safeguards and procedures, whose strictness must be graduated according to the outcomes of the risk evaluation. These measures must be distributed over several layers and, among the other, must comprise: a) authentication procedures for accesses to ICT applications and systems; b) the procedures for the performance of critical operations, ensuring compliance with the principles of least privilege and segregation of duties (e.g. specific procedures of authorization and authentication, four-eyes controls and daily ex-post checks); c) the continuous management of the staff assigned to the processing of data and the performance of critical operations (e.g. by periodically verifying the lists of authorized staff).

Moreover, International standard (ISO/IEC 27001:2013 A.6.1.2 “Segregation of duties”) states that conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.

The Identity Management process, formally appointed in the IT Security function in the COG, is fragmented and only partially under the control of that function; in fact, for the applications not integrated with OIM (187 out of 582) the user management (i.e. creation and profiling, including the special user management) is informally delegated to each application responsible and is not monitored by the ITS-BCM. Moreover, a review process is not in place to verify both the user grants for applications not directly connected to the OIM and the user grants assigned inside the OIM. Among the consequences, the segregation of duties principle could be breached: the OSI team observed such violation for the antifraud engine application (RAKE), not under the OIM control, whose fraud detection configuration rules and the monitoring of suspicions transactions are carried out by the same person.

These weaknesses expose BMPS to the risk of violation of data confidentiality, integrity and availability.

119 In February 2018, a critical incident affected the ATMs networks. This incident was caused by a wrong configuration sent by a remote web console installed on the COG server by a

supplier (Fabbrica Digitale, third party of the outsourcer Bassilichi), without the COG being aware of it.

120 **Finding # 9 Weakness in privileged user management and monitoring process in the COG**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, Sezione IV, transposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that the security of information and IT resources must be guaranteed by physical and logical security safeguards and procedures, whose strictness must be graduated according to the outcomes of the risk evaluation. These measures must be distributed over several layers and, among the other, must comprise: a) authentication procedures for accesses to ICT applications and systems; b) the procedures for the performance of critical operations, ensuring compliance with the principles of least privilege and segregation of duties (e.g. specific procedures of authorization and authentication, four-eyes controls and daily ex-post checks); c) the actions of system administrators and other privileged users must be strictly controlled; d) the continuous management of the staff assigned to the processing of data and the performance of critical operations (e.g. by periodically verifying the lists of authorized staff).

Moreover, International standard (ISO/IEC 27001:2013 A.6.1.2 “Segregation of duties”) states that conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.

The activities of the privileged users, including the application administrators, are not monitored in the COG. In addition, the external resources involved in the system monitoring are also administrators of the same systems, violating the segregation of duties principle.

The OSI team asked the COG for the system administrators lists (e.g. domain, Linux, Windows servers, database, middleware), which were extracted directly from the systems. A relevant number of administrator user-ids were found: 9 for enterprise domains, more than 200 for local Windows servers, more than 200 for Linux server, over 60 for mainframe and more than 25 for departmental database servers (corresponding overall to about 300 users of which about 100 external). In such a context, a periodic review process of active administrators, both for systems and applications, is not currently envisaged in the COG policy.

However, the bank is trying to control the high number of administrators, also without a structured approach (e.g. based on checks of the COG management). During the OSI (April 2018), the COG terminated a one-off review started in January of the system administrators that revoked further about 700 users (moving from about 1,000 to the about 300 mentioned above).

Other privileged users (i.e. applications, databases) are still excluded from these initiatives.

Moreover, matching the administrator user appointments and the administered resources is not possible because the resources that would have been managed at the appointment time, were not specified. Therefore, a misuse of the administrator role cannot be verified (e.g. a mutual assignment of roles between two different server administrators not previously authorised).

These weaknesses have caused the critical incident of February 2018 where an application, running as local administrator of the ATMs, based on a Windows system, deleted most boot files affecting more than 50% of the BMPS ATMs (of which about 15% were completely out of order). Moreover, the supplier involved could remotely access this console, without any authentication, corrupting the ATMs configuration. Discovering the user who accessed such console was impossible also for the internal audit investigation.

These weaknesses entail the risk that these privileged access rights might lead to lack of data confidentiality, integrity and availability, without being promptly detected with consequent reputational and operational risks.

121 The shortcoming in the privileged user management, especially for systems, databases and major assets, is going to be partially mitigated by the full adoption of a specialized tool called CyberArk. The installation and the rollout of such tool are envisaged in the MPSP. After the mentioned project delay (see finding # 7), such implementation is now scheduled by the end of 2018.

122 Concerning Widiba, the user management process is under control, also thanks to the reduced set of assets to manage with respect to the COG. The appointment of the special user is based on a strict evaluation of trustworthiness of the administrators.

123 Moreover, the Widiba network topology allows to better control the access to the production environment. In fact, all administrators have to login to an application level proxy gateway, Balabit, before administering any production server, also for database administrators and for any other activities that require access to the servers. This single access point allows a fine privileged access control at least in the production area.

The Incident Management process

124 The Incident Management process is triggered by the systems monitoring tools in order to ensure the business continuity. The monitoring in terms of availability (hereinafter SIM –

systems incident management)[19] is distinct from the monitoring against cyber-attacks (hereinafter CIM – cyber incident management) [20].

125 Against cyber-attacks, the COG has implemented a Security Operation Centre (hereinafter SOC). The SOC collects security information (e.g. from CERTFin[21], suppliers, bulletins) and uses a Security Incident and Event Management (hereinafter SIEM, based on the IBM QRadar package) to monitor and to detect suspected activities against the BMPS systems. A SIEM usually collects data coming from log files (e.g. Microsoft Windows event log files, database logs, web servers, Linux/Unix, applications, firewall logs) and examines potential attacks on its IT systems based on rules setting native in the system or defined by technical users.

126 Both SIM and CIM processes are aimed at quickly responding to any kind of anomalies independently from their source. These processes are carried out, in both forms, with the support of an outsourcer: Mauden carries out the SIM process at the COG headquarters continuously (24x7); Accenture is remotely monitoring, out of office hours, the SIEM to ensure the overall 24x7 service.

127 **Finding # 10 Defects of the security incident management of the COG**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, Sezione IV, transposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that the security of information and IT resources must be guaranteed by physical and logical security safeguards and procedures whose strictness must be graduated according to the outcomes of the risk evaluation (classification of IT resources in terms of security). These measures must be distributed over several layers, and must comprise: a) monitoring, through the analysis of logs and audit trails, of accesses, operations and other events to prevent and manage IT security incidents; the actions of system administrators and other privileged users must be strictly controlled; b) continuous monitoring of security threats and vulnerabilities; c) rules for the traceability of actions, in order to permit ex-post verification of critical

[19] The “Servizio Erogazione” is in charge of the Incident Management process. The main ticketing system is Remedy (by BMC Software) and it is used for the registration of any anomaly detected. Any incident requires opening a ticket where all the information available to start the remediation phase is reported.

[20] The structure mainly involved is the “Sicurezza Informatica” office, that also carries out the Identity Management process.

[21] In November 2016, Banca d’Italia and ABI founded CERTFin (https://www.certfin.it/index-eng.html). CERTFin (the Italian Financial CERT) is a cooperative public-private initiative aimed at increasing the cyber risk management capacity of banking and financial operators and the overall cyber resilience of the Italian financial system.

operations; the Sezione III states that the residual risk of the IT resources should be submitted for formal acceptance by the user in charge.

The Comunicazione Banca d'Italia no.846 of 26.06.2017 defines the cyber incident type and the criteria for reporting the incident to the Banca d'Italia.

Moreover, International standard (ISO/IEC 27001:2013 A.16.1.4 "Assessment of and decision on information security events") states that information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

The overall cyber incident management (hereinafter CIM) and the related monitoring process is inadequate, because it is affected by relevant issues in the traceability of the cyber incidents, and in the coverage of the cyber monitoring tools. In detail:

a. the CIM policy does not allow to distinguish a cyber incident from a system incident (e.g. a hardware failure problem), and, in any case, it has never been applied; in fact, no cyber incidents have been so far reported, neither the relevant distributed denial of service (DDOS) incident which occurred in January 2017, and blocked the network for about 50 minutes was classified as a cyber security incident, although it was among the reasons for the subscription of a specific cyber incident insurance in December 2017.

b. Starting from the previous point observation, the OSI team asked for a new recognition of the cyber security incidents. Thus, the bank has detected 12 further cyber incidents which occurred in 2016 and 2017, not recorded in any incident management system, not escalated to the IT management and formally reported to a responsible function, and not evaluated in their severity. In addition to the said DDOS, other two of them emerged for their relevance: a) a web server attack that was followed by a forensic analysis; b) a suspicious outflow of about 8 gigabytes of data that was not investigated by the competent function;

c. Regarding the data leakage, the bank has not been able to deliver to the OSI team the information needed to delve into the event, also because the logs related to the incidents were partially unavailable, or the bank could not guarantee their reliability (e.g. the respect of the trusted chain); the Security Incident and Event Management (hereinafter SIEM) logs were deleted one month after the event although the log management policy states that they have to be retained for an adequate time period; the informal analysis of the incident at the event time was not able to clarify the content of the outflow of the data. Moreover, such analysis is not traceable (e.g. no security precautions were taken such as four eyes controls, safeguarding the inalterability of the original data);

d. The CIM policy envisaged a graduation on 5 severity levels plus the Major incident. The

severity is not based on structured criteria, e.g. those provided by the Banca d'Italia cyber incident reporting framework, by a library of threats taxonomy, or linked to a critical system/application classification in terms of confidentiality, integrity and availability. Furthermore, the first level of the SOC service contract with Accenture considers instead a classification on four levels like the one reported in the systems incident management (i.e. based on a priority calculated by means of a combination of impact and urgency, but with more detailed specifications to evaluate these two values). Moreover, the Major incident specification applied to cyber incidents expects to classify in this category any potential breach.

e. the SIEM is configured according to 11 degrees of severity that are not mapped on the severity envisaged in the CIM; the severity of the monitored events in the SIEM is not related to the potential target systems, classified in terms of their confidentiality, integrity and availability relevance;

f. a periodic review of the signals detected by the SIEM and of SIEM detection rules is not ruled and performed;

g. the SIEM collects only a subset of information logs. For example, logs are excluded for: the applications, the databases, the OIM log, the hosts, the activities of privileged users.

With regard to the latter point, the numbers of missing logs make the SIEM less effective, preventing the detection of possible offences from the excluded sources and reducing the ability to correlate events from different sources. Consequently, the controls are mainly oriented to the perimeter defense.

Finally, during the inspection, the OSI team verified that the OIM audit log registration was suspended at the beginning of 2016, preventing, among other things, a reconstruction of the records concerning authorization assigned to the users of MPS Group. However, the decision was adopted by the ex-chief of COG IT Security without a formal assumption of risk by the responsible user.

The described deficiencies in the processes expose BMPS to internal and external cyber security risks, in some cases already incurred, while the shortcoming in detection and classification of the cyber security incidents harms the bank’s ability to promptly respond.

128 Although it should have been already carried out in the M+SP, during the inspection, the COG presented a very early configuration of the next cyber incident management tool

(INCMAN by DFlab, a so called SIRP - security incident response platform[22]) that is going to be adopted, and where all relevant information about attacks, anomalies and user reported incidents will be stored. This new platform is going to be integrated with QRadar, ensuring, inter alia, the chain of trust.

129 With regards to the SIEM log retention, it has been extended to 18 months after the investigation on the data leakage incident.

130 Recently, the acquisition of a newer powerful version of the Palo Alto firewall has strengthened the external defences through the detection and the automatic reactions to the attacks; also, the new system Rake that has consistently reduced the fraud losses is effective. On the other hand, internal vulnerabilities still affect the IT security organization as reported in the previous finding.

Widiba

131 For the monitoring, Widiba has adopted NAGIOS[23]. The monitoring activity is carried out mainly by the outsourcer (Sorint). If a violation of programmed rules occurs, they have to contact the specialists in Widiba or try to investigate and solve the problem accessing directly the problem sources.

132 **Finding # 11 Defects on IT security in Widiba**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, Sezione IVtransposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that the security of information and IT resources must be guaranteed by physical and logical security safeguards and procedures whose strictness must be graduated according to the outcomes of the risk evaluation (classification of IT resources in terms of security). These measures must be distributed over several layers, and must comprise: a) monitoring, through the analysis of logs and audit trails, of accesses, operations and other events to prevent and manage IT security incidents; the actions of system administrators and other privileged users must be strictly controlled; b) continuous monitoring of security threats and vulnerabilities; c) rules for the traceability of actions, in order to permit ex-post verification of critical operations.

The Comunicazione Banca d'Italia no.846 of 26.06.2017 defines the cyber incident type and the

[22] The current ticketing platform, Remedy, is not considered suitable for such use.

[23] NAGIOS is an open source application that allows the system monitoring on the basis of a set of custom rules.

criteria the reporting the incident to the Banca d'Italia.

Moreover, International standard (ISO/IEC 27001:2013 A.16.1.4 "Assessment of and decision on information security events") states that information security events shall be assessed and it shall be decided if they are to be classified as information security incidents. Reference is also made to CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – Continuous monitoring.

The policy for Incident Management of Widiba is still in draft form and it does not provide an incident definition, a severity evaluation, and a quick and clear escalation procedure, also considering that outsourcers are involved in the process , out of the Widiba headquarters and outside of working hours.

In the used tool (NAGIOS) the defined detection rules are focused on monitoring the system availability, not on the cyber threats. Moreover, the monitoring of special user activities, (e.g. the Balabit accesses), the correlation between such and other kinds of events (e.g. suspicious data flows, configuration changing) are not considered.

The OSI team verified that, although not formalized in the policy, the incident severity assessment is based on the number of customers impacted, in particular the number of persons that contacted Widiba, reporting the anomaly. The considered thresholds do not take into account the evolution of the total number of customers (e.g. due to the migration of ex BMPS customers envisaged in the Rondine project), the criticality of the target impacted system and other economical or technical aspects.

Moreover, despite the technical solution adopted (Balabit) that would allow the monitoring by means of a single point of access to the production area, all administrators activities are not monitored and are not reviewed. Moreover, the Widiba Identity Management process does not impede infringements of the segregation of duties. In particular, this is relevant for those users (e.g. outsourcer engaged in the incident management process) that carry out system monitoring activities and are also able to access the same systems with high privileges. The same weakness is highlighted for those users that are both administrators of Balabit and of the production servers. These toxic combinations could easily result in a shutdown of any software detected alerts, if present, or remove or clean logs for unauthorized activities on the main company servers.

The small dimension of Widiba, compared to the whole MPS Group and the separation of the two platforms, mitigate the risk. However, the weaknesses in the prompt detection of cyber offenses and in the monitoring of privileged users activities expose Widiba to the potential risk of violation of confidentiality, integrity and availability.

133 During the OSI, the Widiba management started a review of the processes in order to mitigate the issues reported in the above finding. For example, the definition of an objective methodology to assign the level of severity to the incident and the introduction of a mail-based monitoring for the Balabit privileged users. The completion of the activities is scheduled by the end of 2018.

3.4 Business continuity management-contingency plans

3.4.1 Background and policies

134 The BCM perimeter was defined in the setting up phase of the BCM System (hereinafter BCMS) more than ten years ago, and has been updated in accordance with the requirements listed in the Banca d'Italia Circolare no. 285, Parte I, Titolo IV, Capitolo 5 – "Business Continuity". The companies of the group belonging to the perimeter are: BMPS, MPSCS, MPSL&F, the COG and Widiba.

135 The organizational model of the MPS Group states that:

- The parent company issues the guidelines and manages its own BCMS, coordinating the other companies;
- The companies in the BCM perimeter manage their own system;
- The COG - in addition to managing its BCMS - manages the recovery rooms and the Disaster Recovery Plan;
- Widiba, managing autonomously its IT infrastructure, is responsible for its own Disaster Recovery Plan.

136 As established in the internal policies, the processes with an estimated high impact within 72 hours from the occurrence of their interruption are defined critical[24]; moreover, on the basis of the Comunicazione Banca d'Italia no.0377116 of 07.04.2014, the MPS Group has been confirmed as one of the institutions managing processes of systemic relevance, that are: a) those related to money and financial instruments settlement systems (e.g. Target2, Espress II), b) market access services to regulate liquidity, and c) retail payment services with a widespread public use.

[24] The analysis evaluates, for different time bands (1-4 hours, 4-8 hours, 8-24 hours, etc.), the impact level (high, medium, low) from an economic, regulatory and reputational point of view.

137 The scenarios elaborated by the bank in the Operational Continuity Plan (hereinafter PCO) are compliant with the regulations. Furthermore, a cyber-attack scenario was included in the policy during the OSI, and it will be considered in the next PCO. A specific plan for the “Vesuvio Emergency” is going to be evaluated.

138 The PCO of the MPS Group and the related Management System are defined by: a) a Group policy which defines the methodologies, models and rules adopted by the Group; b) three group directives, two of which are in progress that define the organizational model adopted by the Group; c) the “Rules on Business Continuity” that gathers all the management aspects for the preparation and maintenance of the PCO.

139 The policy framework is overall complete but it suffers from redundancies that make it difficult to maintain and to easily refer to . Therefore, the bank is proceeding in its revision with a view, among other things, of streamlining it.

140 For all the suppliers involved in the processes included in the BCM perimeter, BMPS acquires a copy of the relevant PCOs. Among them, the outsourcer Fruendo has a significant importance in terms of the number, relevance and extension of the processes managed on behalf of the MPS Group. Moreover, the supervisory and control mechanisms of external suppliers, involved in critical processes, are being further strengthened.

3.4.2 Procedures

The Operational Continuity Plan (PCO) and Disaster Recovery procedures

141 The PCO of MPS Group consists of two main documents:

- Volume 1: "Continuity Strategies and Management of the Crisis", approved by the BMPS BoD on 17.7.2014 and implemented by the other group companies within the perimeter.
- Volume 2: "Operating procedures for critical and systemic processes" that defines the crisis operational management procedures of individual processes. The document is prepared, and revised annually by the companies within the perimeter that, through the BIA, detect critical or systemic processes.

142 In 2017, as in 2016, several modifications of the Bank's organizational structure impacted on business continuity updating (e.g. changes of the operating units and of the related processes). Moreover, the exodus of personnel envisaged in the Restructuring Plan, in addition to the normal turnover which occurred in 2017, have changed the human resources allocated to the critical processes. The aforementioned events produced the results indicated in the following table.

143 **Table # 8 – Occurred changes in critical processes, and related recovery resources, between 2016 and 2017 (source PCO volume 2)**

Company	Critical processes[1]		Systemic processes of critical processes		Primary human resources[3]		Recovery human resources[3]		Work station in the recovery rooms [4]	
	Y'17	Y'16	Y'17	Y'16	Y'17	Y'16	Y'17	Y'16	Y'17	Y'16
Banca MPS[2]	43	45	12	12	179	187	56	77	45	45
Consorzio Operativo[2]	15	16	8	8	163	172	86	74	23	22
Widiba[5]	1	1	0	0	5	6				
MPS CS	12	12	1	1	73	69	20	34	39	23
Totali	**71**	**74**	**21**	**21**	**420**	**434**	**162**	**185**	**107**	**90**

(1) "process / service" pairs are counted as "processes", even when the process is the same.

(2) after the BIA carried out in 2017, 3 processes, 2 of BMPS and 1 of the COG, were considered no longer critical.

(3) primary and recovery human resources have been designated - sometimes - in greater numbers than the minimum required for the process. If a primary resource also performs recovery activities, it is counted only once.

(4) more critical processes (carried out in different sites) can be attested on the same recovery work station, in order to optimize the use of the rooms.

(5) recovery solution that involves the intervention of a supplier.

144 In 2017, all BoDs of the Group companies, belonging to the BCM perimeter, approved the update of their PCO after the annual BIA cycleIn 2017, all BoDs of the Group companies, belonging to the BCM perimeter, approved the update of their PCO after the annual BIA cycle. After these approvals, minor changes have been performed autonomously by the BCM Responsible for the MPS Group.

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**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 5, Allegato A, Sezione II transposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that the BIA, preliminary to the drafting of the PCO and periodically updated, identifies the level of risk related to the individual business processes and highlights the consequences of the interruption of the service. Moreover, for each critical process, the IT support procedures and the technological and communication infrastructures used should be identified. Also, according to BCBS-Joint Forum "High-level principles for Business Continuity", an effective BCM includes a recovery strategy that sets out recovery objectives and priorities based on the BIA (e.g. most plans sequence the recovery of operations coherently with their business impact, focusing first on an organisation's critical operations).

The IT Risk Management has evaluated the risk of the applications, also in terms of availability, in the context of the Low Level risk assessment. The perimeter of the critical applications in the IT

Risk Management analysis was partially different from that identified by the BIA 2017. In fact, the OSI team observed that 81 out of 111 critical applications, classified in the two most critical levels in the risk analysis, were not present among those identified in the BIA 2017 (e.g. “Gisco Bonifici”: management and control application for sending and receiving relevant amount cash transfers, “Internet Banking” and “Trading online Web”, “CBI - Paskey Aziende Online": application for the flows exchange management with the Consorzio Triveneto). Moreover, in the BIA 2017, for 35 out of 74 critical processes, the supporting applications were not specified.

Furthermore, B-Safe - the software for the BIA analysis and the PCO production that registers the applications connected to critical processes- receives by the COG’s asset inventory (CMDB) the list of the applications but it is not integrated with the list of dependencies among the IT assets contained in the CMDB; consequently, the criticality of a component or an infrastructure cannot be associated to the critical process it supports. The said information absence could hamper the decision-making process, setting the correct priorities (i.e. the recovery strategy) in the recovery of infrastructures and applications related to the criticality of the processes, to their dependencies, and to possible cut-off dates (e.g. deadlines for tax payment).

Against this backdrop, a full recovery strategy (i.e. Disaster recovery) cannot offset the lack of continuity measures and recovery procedures for each process.

Such situation is due to the lack of integration of the systems involved and to the missing coordination of the IT risk analysis and of the BIA analysis.

The inconsistency between the outcomes of the risk analysis and the BIA entails the risk that critical applications for the Business Continuity are not considered. On the other hand, the lack of an adequate component mapping impacts on the effectiveness recovery capacity of single process. All this could result in the failure to meet the established Recovery Time Objectives.

146 Following the audit survey (no. 202/2017 on the Disaster Recovery Test), on 23.01.2018 BMPS provided the census of the applications missing in the BIA 2017. Lastly, the MPSP sub-project "BCM Revamping" envisages , within the year, to integrate the risk analysis methodology with the BIA's one.

147 Within the same "BCM revamping" sub-project, the revision of the COG Disaster Recovery Plan is envisaged, in order to make the related procedures more usable in case of emergency and to guarantee the completeness with respect to the Widiba perimeter.

148 The Widiba Disaster Recovery plan focuses only on the front-end production systems (as mentioned earlier, the back-end is ensured by the COG). The active-active configuration between the data centres of Firenze and Siena ensures an automatic response in case of a

disruptive event; the Plan provides a series of ex-post checks to confirm the correct functioning of the alive site. In view of infrastructural changes, the Plan envisages to carry out tests and simulations to ensure the effectiveness of the said configuration. The internal systems, instead, linked to the office and development areas, are hosted in Milano at the Banca Widiba headquarters and replicated in the server farm in Firenze.

149 **Finding # 13 Weakness in Widiba's BIA process and in the related risk assumption report**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 5, Allegato A, Sezione II transposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that the BIA, preliminary to the preparation of the business continuity plan and periodically updated, identifies the level of risk related to individual business processes and highlights the consequences of service interruption. Resource allocation and intervention priorities are related to the risk level. The processes related to corporate functions particularly relevant for the impact resulting from their unavailability, require high levels of business continuity to be achieved through preventive measures and with business continuity solutions to be activated in the event of an accident. Furthermore, the body with control function is responsible for monitoring the completeness, adequacy, functionality and reliability of the business continuity plan. The activity carried out and the decisions taken are adequately documented.

The BIA 2017 of Widiba is incomplete: many fields in the impact assessment questionnaire, envisaged by the group policies, were not filled in (e.g. impact level over time after service interruption and related description); in addition, the information recorded was inconsistent (e.g. high economic impact within four hours for "Organization of team building training activities in the Media Center" process). Considering such inconsistencies of the above-mentioned BIA exercise, the responsible for Widiba BCM decided both to ignore the BIA's results and to consider critical only the process of "Incident management" (specifically the incident monitoring and control sub-process) as in 2016. The reasons behind this choice are not adequately documented: in fact, this approach is not explained in the adequacy report nor in other formal documents reported to the Widiba and BMPS BoD.

Therefore, the continuity of Widiba processes is based exclusively on the continuity measures applied to the incident monitoring process (i.e. the outsourcer's PCO and the on-call availability of the IT managers), and on the high availability of the Widiba production systems.

Since Widiba is an online bank, the unavailability of the web site or part of its functionality is subject to significant reputational impacts (e.g. the process of securities buying and selling has an RTO of four hours), but it is not possible to guarantee continuity of intervention on critical

applications (e.g. a software fix installation) in case of unavailability of the development and testing systems, located in Milano and, therefore, not in the disaster recovery configuration. In fact, the restoration of such systems on the alternative site of Firenze may require up to 12 hours.

The said weakness of the BIA process are due to: a) the lack of awareness of the personnel responsible for the BIA assessment; b) the inadequate supervision by the group function responsible (ASI) for ensuring the congruence of PCO; c) the Widiba census of business processes is too granular (504 functional processes and 869 operational processes), implying a heavy burden in completing the questionnaires; d) the lack of an IT compliance function (see finding # 5).

The absence of an effective identification of critical processes and related continuity measures could result in the failure of Business Continuity risk mitigation.

150 The Widiba processes will be remapped and codified using the same taxonomy adopted by the group (using the application "ARIS") and, starting from 2019, the bank will make use of the same procedure as BMPS – B-Safe – to manage directly its BIA cycle.

Testing strategy and execution

151 The Bank adopted a three-year test plan on Operational Continuity Measures for the period 2015-2017 with the aim of strengthening the methods of supervision of the BCM tests. This plan provides realistic tests of the systemic processes over a three-year period and partial procedures every year. The processes identified as critical for business continuity purposes were tested with three-year rolling tests (even partial). Moreover, as a response to the 2016 audit findings, more realistic modalities have been adopted (i.e. unexpected tests) starting from the second half of 2017.

152 The BCM test plan can be considered adequate and was substantially complied with in the 2015-2017 period; the same guidelines have been confirmed for the 2018-2020 test plan (BoD of 05.04.2018).

153 The test of the Disaster Recovery plan, managed by the COG, is performed on a yearly basis. In December 2016, the simulation was done in "third copy" mode[25]. Such a smaller and less realistic scenario was adopted because the secondary data centre of Siena was the primary site until the swap with the one located in Firenze in September 2016, and no

[25] The simulation was performed through the creation of an isolated testing system with access to a database resulting from the copy of production data, restored after the abrupt and unordered closing of the synchronous data flow between primary and secondary databases.

technical changes had occurred in the meantime. In 2017, on the other hand, a more realistic test was carried out with the provision of services from the secondary site on Saturday 2 December and the participation, among the other stakeholders, of two BMPS branches that operated regularly and transparently in relation to the supply site.

154 In 2017, Widiba carried out the BCM test on its own critical process and participated in the COG Disaster Recovery test to check the proper functioning of its front-end, in case that back-end services are provided by the recovery site of the COG.

155 **Finding # 14 The COG Disaster Recovery test cannot demonstrate the respect of the restart time limits for systemic processes**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 5, Allegato A, Sezione IItransposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that, at least once a year comprehensive tests must be carried out, based on scenarios that are as realistic as possible, of the operational recovery of critical processes in crisis conditions, observing the ability of the organization to carry out the measures laid down in the business continuity plan in accordance with the time schedule established. Furthermore, the special requirements for the systemic relevance processes (Sezione III), state that the restart time (i.e. the time required, excluding the decision time, for the implementation of the technical and organizational interventions in order to restore the services availability in safe conditions) does not exceed two hours.

The Disaster Recovery test in 2016, carried out on a restricted and isolated scenario ("third copy" mode with the exception of distributed systems), resulted in an overall restart time of 2:34 hh/ mm. Moreover, the "Paschi Face" application did not restart due to a misconfiguration of the test environment. The Disaster Recovery test in 2017, designed to provide all services from the secondary site for 24 hours, highlighted a restart time of almost four hours for the overall systems (while only the ATM service were recovered in about 1:40 hh/mm). In both the 2016 and 2017 tests, it was not possible to establish if the systemic processes were available before the complete restart because, except for the ATM service, the user testing procedure started at the end of the whole recovery process.

The COG Disaster Recovery solution is based on the duplication of almost all the IT infrastructures between the primary and secondary data centre, but the recovery strategy is not consistent with the business impact analysis since it was developed before the introduction of the BCM and not subsequently reviewed, in order to distinguish critical technological resources from those of lower importance by mapping dependencies between application software components and critical business processes (see finding # 12). By consequence, the testing procedures (apart from the ATM operational tests) have not been designed to ascertain the recovery of the critical and

systemic processes within the respective restart time limits.

Therefore, it is not possible to guarantee that in the event of a real disaster, systemic processes will be restored within the restart time of two hours provided in the regulation.

156 At the end of the OSI MPS has been excluded from the list of operators having to comply with the most strict requirements for systemic processes. Even so, MPS can further take part in the CODISE activities as part of the second-level systemic operators[26].

Continuous improvement

157 BMPS, along with the COG and Widiba, have processes in place to overcome the issues arising from the BCM and Disaster recovery tests, from the audit findings, from the Accenture's Maturity Assessment (commissioned at the end of 2016, from which the "BCM Revamping" plan was born), as well as the lessons learned from accidents. Among them could be mentioned:

- New operating instructions, issued by the parent company in September 2017, to improve the effectiveness of the recovery rooms (e.g. monitoring and maintaining the recovery workstations) and virtual workstations adoption allowing to overcome the constraint of the current recovery stations, physically located mainly in Siena and Firenze;
- Online course on the basic concepts of the BCM, updated at the end of 2017 and provided to the roughly 250 primary and recovery resources of BMPS;
- Integrated test execution between Fruendo and BMPS;
- Specific monitoring measures to correctly detect the restart time of critical and systemic processes (envisaged by the end of the year).

3.4.3 Reporting

158 Every year the BMPS BoD is informed, through the adequacy report of the Group BCM Manager, on the effectiveness of the BCM system, the tuning and improvement activities, the tests' results and the management of human and instrumental recovery resources. Moreover, the BoD yearly approves the PCO, previously shared with the Operational Risk Management, and submitted to the Risk Committee.

[26] The CODISE is the coordination structure of the operational crises of the Italian financial market. The MPS Group participates in the CODISE tests (the latest in June 2017).

3.5 Data quality management

3.5.1 Background and Policies

159 In 2015, the Institution, in order to be fully compliant with the requirements listed in the Banca d'Italia Circolare no. 285, Part I, Title IV, Chapter 4 – "Information System", setup a project with a multi-year horizon, the "Data Governance" project, in order to implement a formal and documented data governance and data quality framework at group level, called "Standard di Data Governance" (Data Governance Standard, hereinafter DGS)[27].

160 The regulatory framework, which is considered adequate by the OSI team, is composed of the policy, adopted in September 2016 ("Data Governance Policy") that defines principles and high-level data governance model, and of three directives, adopted in June 2017 which defines: a) the organizational model implemented in terms of responsibility for the Data Management System; b) the perimeter of information (which is composed of business information related to the relevant outputs defined within the Data Governance Project); c) and the data quality management framework. The implementation of the said project is currently focused exclusively on BMPS.

161 The overall Data Governance Process is managed by the Data governance and Reporting Management Service (placed under the Planning Area within the CFO Direction), which is led by the Chief Data Officer (hereinafter "CDO"), currently identified in the Head of Planning area, and in charge of addressing strategic activities in this sector. The organizational framework adopted by the bank envisages a strong cooperation between the business units that oversee the management and production of data, and the IT function, responsible for the management of the Data Governance platform and the development of technical controls.

3.5.2 Procedures

162 The criteria chosen by BMPS to define the relevant perimeter of data to be involved in the Data Governance system were defined considering the more sensitive information areas subject to regulatory requirements (e.g. Anti-money laundering, compliance, risks, credit, financial statements, banking supervision). For each information area, BMPS selected some

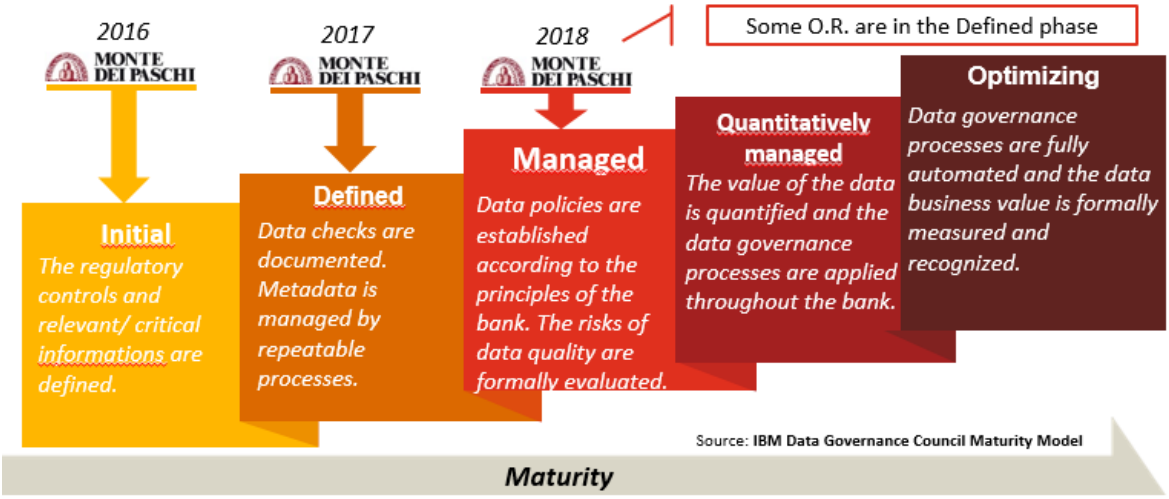
[27] The TRIM-2017-ITMPS-2939 reported in the chapter 2.3 Data Quality Process information on the mentioned project focused on the application to the perimeter of the model credit risk parameter and raised the finding # 3 "Data quality framework; data quality dimensions and controls¸ data quality roles and responsibilities" already reported to BMPS. The OSI team did not overlap in its observations with the issues raised in the mentioned finding.

"Relevant Outputs" (hereinafter RO), i.e. reports, information, databases, whose importance involves both the Bank's internal reporting (e.g. commercial monitoring) and the external ones (e.g. LCR, Finrep). In 2016, over 400 RO were initially identified by the bank. Given the complexity of the scope and the limited resources, the Institution decided to concentrate its efforts on a limited perimeter, defined on the priority of intervention criteria, of about 46 RO.

163 The perimeter currently covers only the Parent Company areas; according to the CDO, a "sufficiently" large perimeter should be reached in at least 36 months with an estimated investment effort of € 4 mln. In the future, the bank would gradually extend the perimeter based on the priority needs recognized, in the following areas: audit; commercial; Customer Relationship Management (CRM); human resources; customer database and other customer data.

164 With reference to the RO the bank wants to increase the data governance maturity, being currently positioned according to the scheme of the figure below.

165 **Figure # 13 – BMPS data governance maturity chart (source 2017 annual report on Data Governance)**



166 For the operational application of the Data Governance system, three main tools have been implemented by the bank: a) Business Glossary: it is the catalogue that collects all the elements of the Data Governance System (e.g. Areas, Roles, Relevant Outputs). For 61% of 46 RO, about 10,000 Business Data Element (hereinafter BDE[28]) were registered and

[28] A business information element which constitutes or contributes to the production of a Relevant Output

mapped in the Business Glossary; b) Piattaforma controlli**:** in this application (Irion DQ was the platform selected) the Data Quality Controls available on the RO are registered (Data Control Dictionary); for those directly codified in the platform, the checks are automatically executed, summarized at various levels of aggregation and reported. Other controls, automatic and manual checks, are only mapped in the platform and executed in other processes/procedures. As of 31.12.2017, about 800 data quality checks had been developed directly on the platform; c) Remediation: fails in the checks could activate a remediation process through the IT ticketing platform (Remedy); the data governance platform automatically opens a ticket towards the IT function and it allows the monitoring of its life cycle. The ticket is managed with the same tools used in the Incident Management process (Remedy) that starts a workflow towards a responsible owner. Currently, the ticketing process is managed only by the IT function without a clear identification and definition of Data Quality incidents in the Group's system and the involvement of the bank network in remediation, for example in the case of incorrect data entry (see finding # 15). The bank expects to overcome these criticalities in 2018.

167 To analyse the effectiveness of the Data Governance project the OSI focused on findings and recommendations about data quality issues emerged consequently to ECB inspections; two of such issues were sampled from two OSIs on credit risk: a) Recommendation no. 12 of OSI-2015-ITMPS-34-35 follow-up letter, according to which, the Institution should upgrade and update the database to include all relevant information about collateral; b) Finding no. 3 of OSI-2016-ITMPS-12-38, according to which, among other things, for a significant number of properties the cadastral data are partially or totally missing. In this regard, in 2016 the bank setup the project "Argo" with the aim to include the information and the documentation related to mortgages granted after 01.01.2012 (approximately 380,000). As of 31 December 2017, the bank estimates that anomalies in the cadastral values arise in 1.44% out of 380,000 properties (source elaboration on DWH). However, the remedial actions were followed only by the Data Owner function (i.e. the Chief Lending Officer), without a coordination mechanism with the CDO function and with the Data Governance project (see next finding).

168 The design of the process and of the procedures is, in general, adequate, but the state of the art is still at an early stage; for example the missing definition of Key Quality Indicators (hereinafter KQIs), implementation issues, or limits in the coordination of the initiatives give rise to criticalities, highlighted in the following finding.

169 **Finding # 15 Delay in the implementation of Data Governance project**

Banca d'Italia Circolare no. 285/2013, Parte I, Titolo IV, Capitolo 4, Sezione V, transposing artt. 74.1 and 88 of Directive EU no. 36/2013, states that a company standard for data governance must be instituted, defining the roles and the responsibilities of the functions involved in the use and processing of corporate information for operational and management purposes and, in relation to the importance of data sets for the information system, mechanisms to measure and guarantee data quality, e.g. through a key quality indicator system, that should be periodically reported to business users, to control functions and to the management body. The identification, measurement, assessment, monitoring, prevention and mitigation of the risks associated with data quality must be part of the risk management process.

Moreover, BCBS 239 principles 1-11 about Overarching Governance and Infrastructure, Risk Data Aggregation Capabilities, and risk Reporting Practices ask institutions to implement an effective data quality framework with several specific requirements.

The Data Governance project in BMPS started in April 2016, but the activities were based only on the publication of an ineffective group policy successively replaced. Also due to such delay, the project is still at an early stage. As a consequence, a scant perimeter has been covered both from a horizontal and a vertical view:

1. from a horizontal perspective, the complexity and the vastness of the perimeter still require many activities, considering that on about 400 Relevant Outputs (hereinafter RO) initially identified in half of the information areas (e.g. commercial, audit, customer database are excluded), the Institution selected only a perimeter of 46 of them. Regarding these 46 RO, the coverage is incomplete (e.g. missing the mapping of the existing controls of Sisba, the main application for regulatory reporting, in the Irion DQ platform). In the activities only the Parent Company and the COG are involved, while the other entities of the Group are excluded;
2. from a vertical point of view, a data quality indicators system (e.g. based on key quality indicators) was not in place, preventing an effective monitoring; this implies that performances metrics are not available, in order to objectively measure the overall data quality and that of the RO (i.e. a synthetic indicator that informs the Institution's Senior Management about the data quality risk). Moreover, metrics or judgmental evaluation of the completeness of the Data Quality Controls, with respect to the information area in scope, are not implemented or formalised.

The ticketing process currently involves only the IT function, without the engagement of the Data Owners able to organize the remediation, also through the contribution of the customer managers

in the network.

Moreover, the Chief Data Officer (hereinafter CDO) has not been involved to address findings on data quality issues emerged during ECB OSIs. Consequently, remediation actions were developed to clean anomalies in the cadastral values in the database of the immovable properties, but such data are not included in the RO and not managed in the new Data Quality framework (e.g. implementing automatic controls to avoid future degradation of such cleaned-up information, or to monitor the effectiveness of the follow up activities), highlighting a not integrated approach to the addressing of data quality issues in the bank.

Finally, in the first five months of 2018, Data Governance and data quality topics were never discussed in other Board or managerial committees, despite the abolition of the Data Governance Committee previously in charge of the data governance coordination.

The Data Governance project, considering the need for a three-year time horizon and not bringing perceivable benefits given the abovementioned limits, entails an increasing execution risk, i.e. to not achieve its goals in terms of coverage of the perimeter and in terms of maturity. Moreover, a risk of fragmentation and coordination of the initiatives concerning data developments is concrete, given that the bank has adopted a decentralized approach and is conducting other initiatives (data expansion, closing of ECB findings) that are managed outside the Data Governance perimeter.

170 A prototype of KQIs based on balanced scorecards was drafted in May 2018. It covers 7 RO, mainly in the internal model area, and it summarizes the results of the controls, the remedial actions and a qualitative indicator based on a self-assessment.

3.5.3 Reporting

171 Starting from 2017, the Data Owners, for each covered area for which they are responsible, produce a Data Quality Report related to the RO in their perimeter. The overall outcome of such reporting is quarterly summarized to the CDO. The reporting process is carried out for the most part through qualitative "self-risk assessment" filled in standard forms by the data owner, and, for others, through the centralized control platform (Irion DQ). Currently the reporting on the RO is focused not only on the data quality outcomes but also on the activities linked to the project (e.g. data modeling).

172 The CDO function yearly publishes a report for the CEO named “Rapporto di Sintesi Annuale di Data Governance”, in which it summarizes the activities carried out during the year and it presents the priorities for the coming year.

3.5.4 Other connected projects

173 In the second half of 2017, the Institution, launched a project ("Risk Reporting according to PERDAR") focused on the Risk Reporting target model, and on the highest-level reports to Corporate Bodies and senior management, in order to comply with the principles 7-11 about risk reporting practices of the BCBS 239. In this context, on 05.01.2018 the BoD approved the "Direttiva di Gruppo in materia di Integrated Risk Reporting" (Group Directive on Integrated Risk Reporting) defining the related organizational model. It outlines the risk reporting framework, the governance, the risk reporting model, the relevant risk flows, and roles and responsibilities. Some parts of the directive are not yet implemented and the project is at an early stage.

174 The Swiffer initiative is a regular activity implemented by the COG at the end of 2016, for the execution of massive technical controls (e.g. presence of control characters in strings; checks on dates) on the data warehouse (hereinafter DWH) system that is one of the most important data base for the reporting. In 2017, the controls had about 1.5 mln executions; 44,282 columns (4.5% of the total DWH columns) were examined on priority basis, and about 1.3 bn values were checked. Since the activation of the initiative, remediation actions have been undertaken that have led to a considerable reduction in the anomalies (from 567 mln to 33 mln occurrences in absolute terms, from 535 anomalous items out of 1 mln to 26 out of 1 mln).

4 Detailed table of contents

5 Table of tables

6 Table of figures

7 Annexes

7.1 Annex 1 – Abbreviations

ABBREVIATION	MEANING
AIRB	Advanced Internal Rating Based Approach
ASI	Area Sicurezza Integrata / Integrated Security Area
BCBS	Basel Committee Banking Supervision
BCM	Business Continuity Management
BCMS	BCM System
BDE	Business Data Element
BIA	Business Impact Analysis
BOL	Banking Online
BMPS	Banca Monte dei Paschi
BR	Business Requirements
bps	Basis points
BoD	Board of Directors
BoSA	Board of Statutory Auditors
CEO	Chief Executive Officer
CCO	Chief Commercial Officer
CET1	Common Equity Tier 1
CDO	Chief Data Officer
CFO	Chief Financial Officer
CIA	Confidentiality, Integrity and Availability

CIM	Cyber Incident Management
COG	Consorzio Operativo di GruppoMontePaschi (Operational Consortium Monte dei Paschi Group)
COO	Chief Operating Officer
COP	Comitato Operativo Progetti (Operational Project Committeee)
Corep	Common Reporting
CMDB	Component Management Database
CP&CO	Chief Program & Cost Officer
CRR	Capital Requirement Regulation (Regulation 575/2013/EU)
CRD IV	Capital Requirement Regulation (Directive 2013/36/EU)
DGS	Data Governance Standard
DWDM	Dense Wavelength Division Multiplexing
DWH	Data Warehouse
D-SIB	Domestic Systemically Important Bank
EBA	European Banking Authority
ECB	European Central Bank
Finrep	Financial Reporting
GM	General Manager
KQI	Key Quality Indicator
KRI	Key Risk Indicator
IA	Internal Audit
IEC	International Electrotechnical Commission
IM	Identity Management
ISO	International Organisation for Standardization
IT	Information Technology

ITIL	Information Technology Infrastructure Library
ITS-BCM	IT Security and BCM
LS-OC	Logical Security and Operational Continuity
MC	Comitato Direttivo (Management Committee)
MPS Group	Banca Monte dei Paschi Group
MPSLF	MPS Leasing e Factoring
MPSCS	MPS Capital Services
M+SP	Monte più Sicuro Project
MPSP	Monte Protect Shield Project
NBO	Non-Binding Offers
NIST	National Institute of Standards and Technology
NCA	Nuovo Controllo Accessi (New Access Control)
OIM	Oracle Identity Management
OMR	Operazioni di Maggior Rilievo (greater importance transactions)
OSI	On-site Inspection
O-SII	Other Systemically Important Institutions
Q&A	Questions and Answers
PCO	Operational Continuity Plan
PMO	Project Management
RO	Relevant Output
RTO	Recovery Time Objective
SAN	Storage Area Network
SIM	Systems Incident Management
SIEM	Security Incident and Event Management
SOC	Security Operation Centre

SSO	Single Sign On
VLAN	Virtual Local Area Network
24X7	24 hours for 7 days

Feedback from the inspected bank

Part of the report the institution wants to comment on[29]		Inspected institution's comments or remarks	HoM response
E.g. Para 50	*Text ABC from Para 50*		

[29] Please copy the commented part of the report