Information Security Management System Manual

Revision History

Version	Reference	Author	Date	Comments
1.0	M_QMS_036_E	Paula Gaspar	2014-06-25	First Version
2.0	M_QMS_036_E	Paula Gaspar	2014-09-11	Second Version : update Information Security Policy Compliance
3.0	M_QMS_036_E	Paula Gaspar	2015-01-23	Update footer
4.0	M_QMS_036_E	Paula Gaspar	2015-02-20	Update relation between ISO 9001 and 27001
5.0	M_QMS_036_E	Paula Gaspar	2015-08-05	ISMS Team update, ISO 27001:2013 Certification update
6.0	M_QMS_036_E	Paula Gaspar	2015-12-30	Update RH Responsible
7.0	M_QMS_036_E	Paula Gaspar	2016-01-18	Update WeDo Global Organization and WeDo Shareholder, update Figure 1 – WeDo Interface Management Model. Business Continuity Corporate Procedure updated.
8.0	M_QMS_036_E	Paula Gaspar	2016-01-25	Competence and Awareness updated
9.0	M_QMS_036_E	Luis Rodeia / Paula Gaspar	2016-09-07	Inclusion Annex A – ISMS Policy
10.0	M_QMS_036_E	Paula Gaspar	2016-12-14	Update Annex A – Information Security Management Policy
11.0	M_QMS_036_E	Paula Gaspar	2017-11-21	New WeDo signature replacement
12.0	M_QMS_036_E	Paula Gaspar / Luis Rodeia	2018-05-28	ISMS Security team update
13.0	M_QMS_036_E	Paula Gaspar / Luis Rodeia	2018-05-31	Global update, Managed Services Madrid and Saas Cloud inclusion
14.0	M_QMS_036_E	Paula Gaspar / Luis Rodeia	2018-08-06	Annex A updated - Privacy and Personal Data Protection Policy
15.0	M_QMS_036_E	Paula Gaspar	2019-02-18	Organization structure & Security Governance Model update
16.0	M_QMS_036_E	Cristina Pires	2019-09-24	Updated with the new WeDo brand and corporate content.
17.0	M_QMS_036_E	Lígia Sousa Marçal	2020-05-14	Updated with Mobileum brand and corporate content.
18.0	M_QMS_036_E	Paula Gaspar/ Daniela Nunes	2020-06-19	General revision and update WeDo to Mobileum Risk BU.
19.0	M_QMS_036_E	Paula Gaspar	2021-06-18	Update Scope (out of scope SaS Cloud)
20.0	M_QMS_036_E	Paula Gaspar	2022-10-14	General revision and update, Update ISMS Scope, ISMS Security team
21.0	M_QMS_036_E	Paula Gaspar	2023-11-10	General revision and update
22.0	M_QMS_036_E	Paula Gaspar	2023-12-15	Risk BU organization Chart Update

Index

Index of Images

1 Introduction

This document describes Mobileum Risk BU Information Security Management System, according to NP EN ISO 27001 Standard requirement and to the Security Management principles and vocabulary referred to in the ISO/IEC 27000 standard.

Nowadays the benefits of using Information Technologies (IT) in the organizations are undeniable. Their use makes it possible to accelerate the business strategies through new services, processes and costs optimization. However, there are also associated risks, in particular related to information security, that need to be managed.

The risks in the information security should consider the possibility of threats, such as: intrusions, internal or external attacks with the objective of stealing information, to modify or make it unavailable; sabotage, data loss caused by leak in the information system; penalties for use of illegal software; disclosure of critical information to the business; compromise the organization due to a failure of the systems, among others.

All these risks should be evaluated and the respective measures implemented. In terms of strategy the purpose is not to eliminate all the risks but to manage them to achieve the best solution for the business, to treat the risks when they become critical for the organization, to accept them when they are residual or to transfer them to a third party.

The information security should be Mobileum Risk BU main concern and responsibility at all levels including collaborators, partners and suppliers (hereafter referred to as Participants).

This security awareness will allow all to act in order to make security an integral part of Mobileum Risk BU organization and its Information, Communications and Technologies.

ISO/IEC 27001 -Information security management systems- and ISO 9001- Quality Management System- –follows a PDCA approach- Plan-Do-Check-Act, directed linked to continuous improvement and these two Management Systems are fully integrated.

It presents also Mobileum Risk BU processes, their relationships and interactions with the procedures that give substance to our business supporting activities, putting the spotlight on the following areas:

- Managed Services

- Project Management
- Product Development
- Information Technology
- Human resources

1.1 Goal of Information Security Management System Manual

Information Security Management System is applied to the following Mobileum Risk BU activities: Managed Services, Information Technologies, Human Resources.

The goal of this Manual is:

- Document all activities associated with Information Security Management System;
- Determine how the company will meet the NP EN ISO/IEC 27001-“Information Security Management Systems-Requirements”;
- Increase the effectiveness of Mobileum Risk BU Information Security Management System performance;
- An evidence that the Information Security Management System Policy are completely integrated with the Company strategic guidelines;
- Document the way Top Management is completely committed with the Information Security Management System;

This manual can be used by Customers, Suppliers, Partners, Employees and other stakeholders as evidence that the Information Security Management System is structured and implemented in order to assure that Information Security goals are established, implemented and measured every year.

1.2 Normative References, Definitions, Concepts definition

Normative References

NP EN ISO/IEC 27001 – ISO 27001 Information security management systems-Requirements;
NP EN ISO/IEC 27002 – Code of practice for information security controls.
NP EN ISO 9001 – Quality Management Systems – Requirements
NP EN ISO 9000:2000 – Quality Management Systems – Fundamentals and Vocabulary

Definitions/Acronyms

AOP	Annual Organization Planning
CFO	Chief Financial Officer
CMO	Chief marketing Officer
Excom	Mobileum Management
HR	Human resources
KPI	Key Performance Indicator
ISMS	Information Security Management System
ISP	Information Security Policy
PDCA	Plan, Do, Check, Act
QMS	Quality Management System
RDI	Research, Development and Innovation

Concepts Definition

QMS:

Quality management System (QMS) can be expressed as the organizational structure, procedures, processes and resources needed to implement Quality Management.

ISMS definition:

The governing principle behind ISMS is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.

2 About Mobileum Risk BU

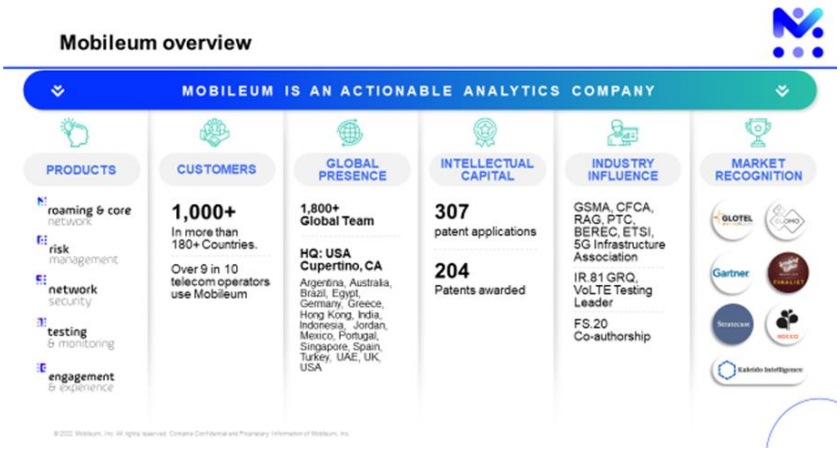
Action driven by Intelligence…

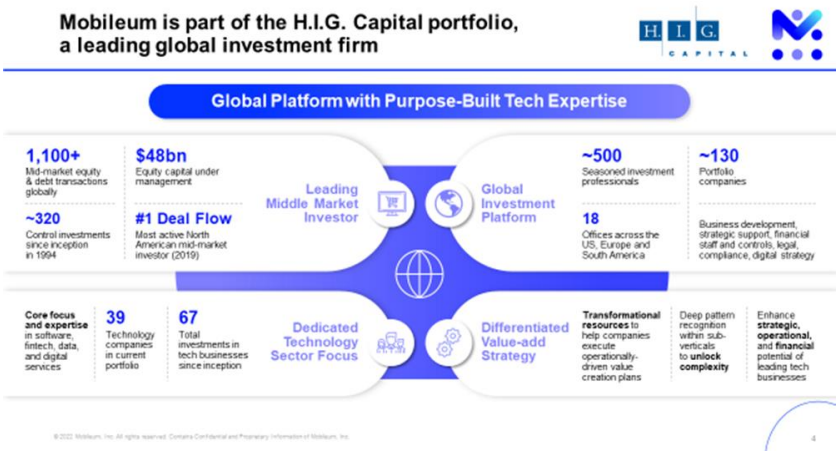
About Mobileum

Mobileum is a leading provider of Telecom analytics solutions for roaming, core network, security, risk management, domestic and international connectivity testing, and customer intelligence. More than 1,000 customers rely on its Active Intelligence platform, which provides advanced analytics solutions, allowing customers to connect deep network and operational intelligence with real-time actions that increase revenue, improve customer experience and reduce costs. Headquartered in Silicon Valley, Mobileum has global offices in Australia, Dubai, Germany, Greece, India, Portugal, Singapore and UK. Learn more in www.mobileum.com and follow @MobileumInc on Twitter.

2.1 Fast Facts

Mobileum is a GLOBAL Market leader in several areas



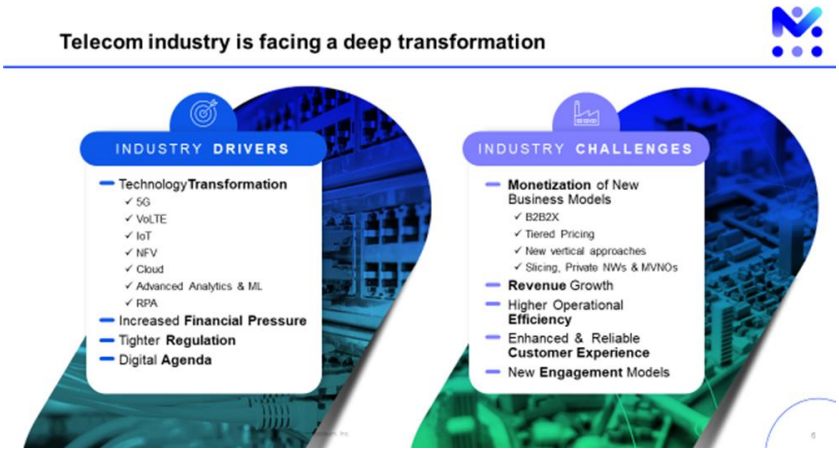


Customer References

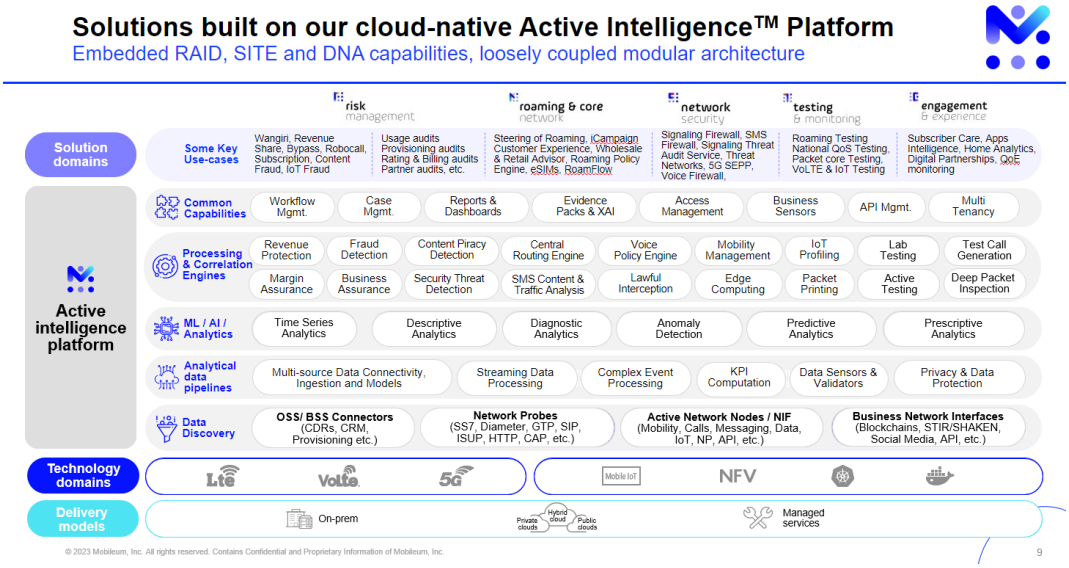
Customer Testimonials

Mobileum is highly recognized by the market and by its customers.

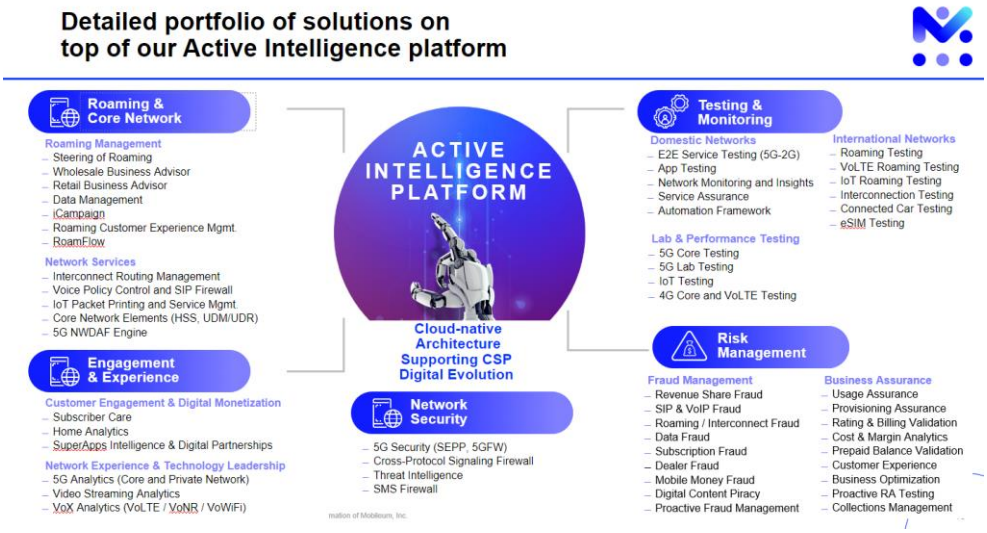
Company Overview



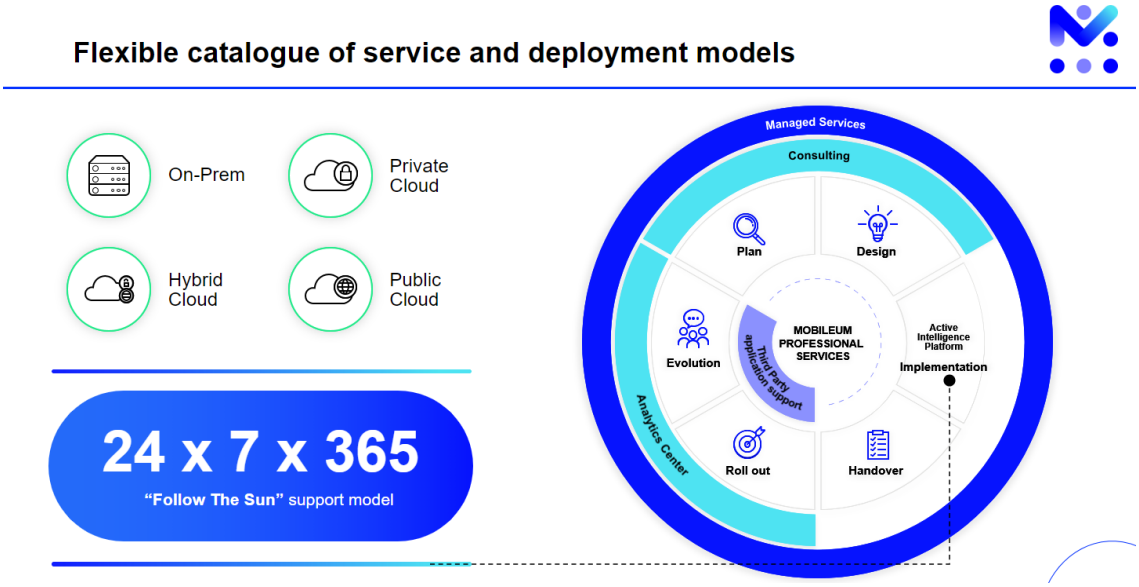
Mobileum's active intelligence platform helps customers dealing with the emerging industry challenges and opportunities.



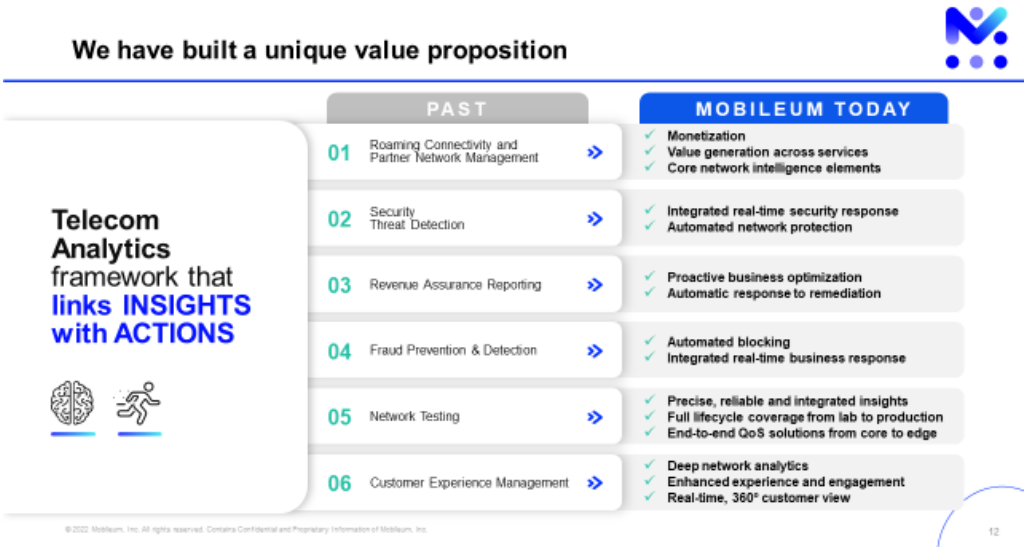
Lines of Business (LOB)

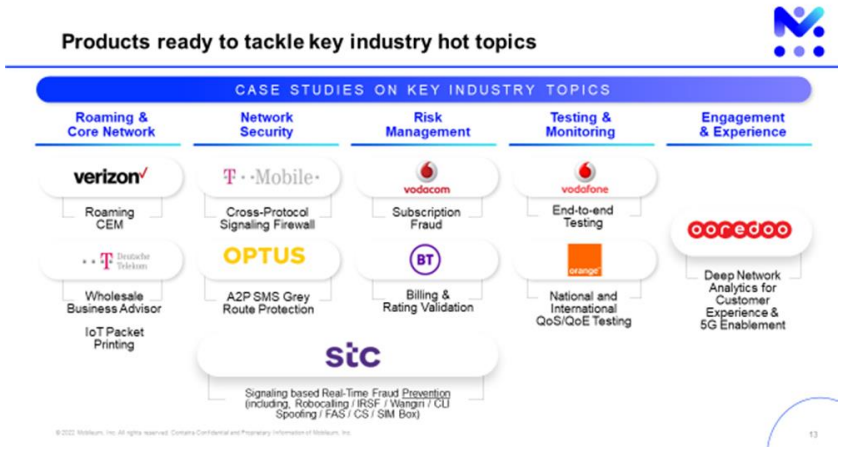


Mobileum also has a flexible catalogue of services and deployment models.

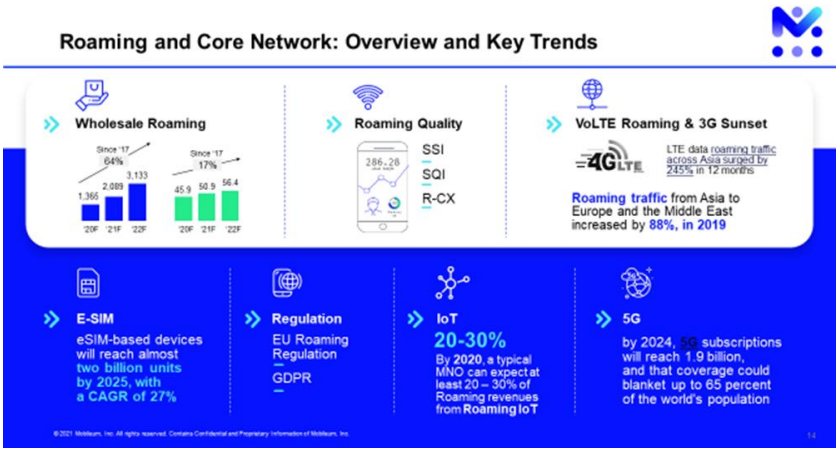


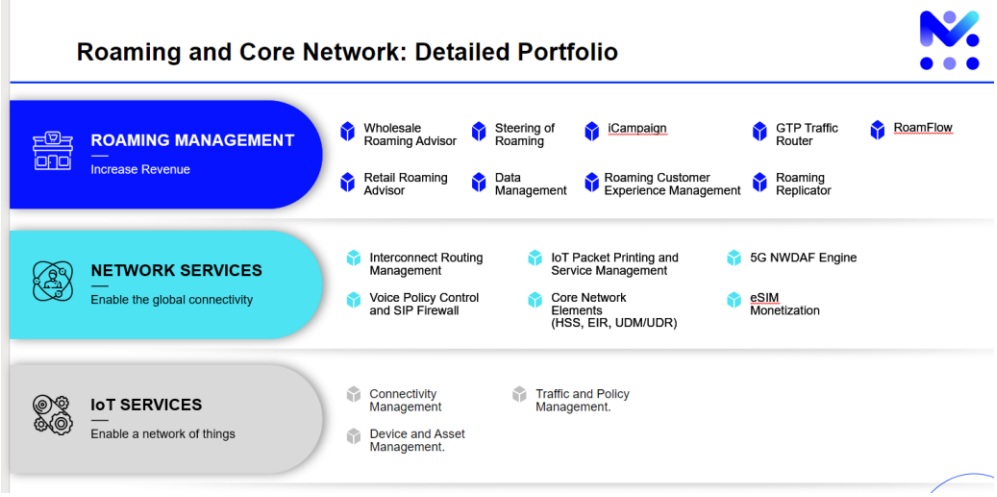
We have built a unique value proposition:

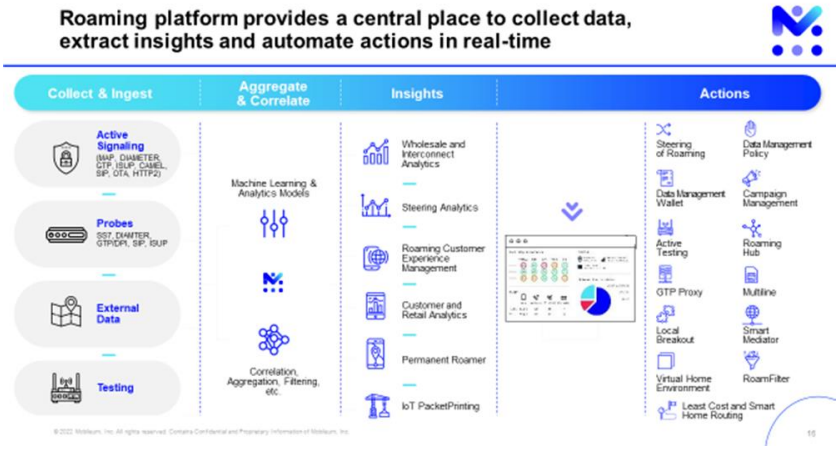


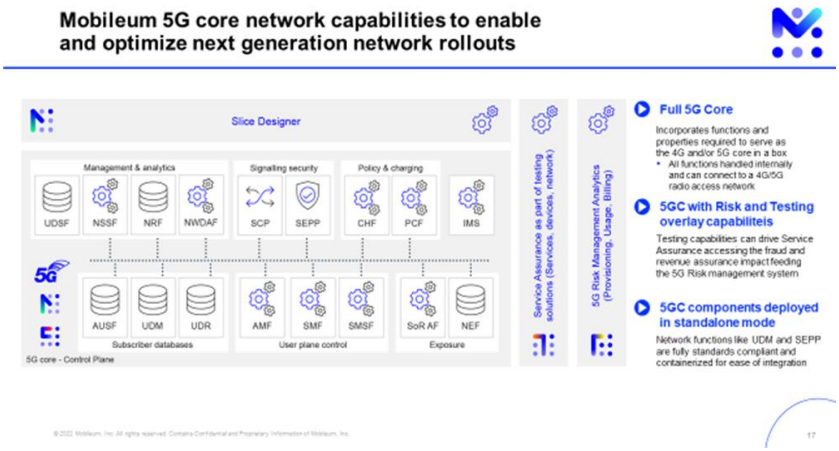


Roaming

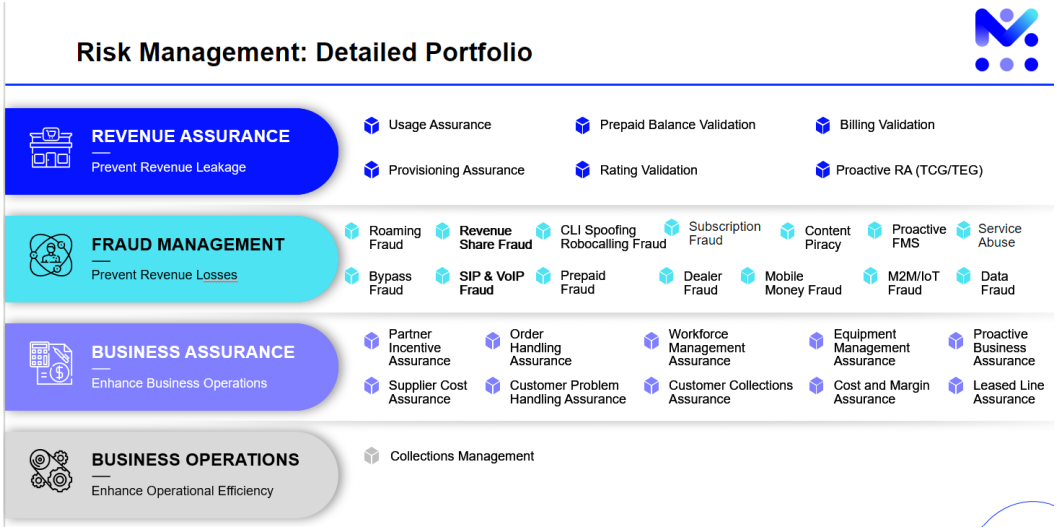



Roaming and Core Network: Detailed Portfolio
ROAMING MANAGEMENT
Increase Revenue
Wholesale Roaming Advisor
Steering of Roaming
iCampaign
GTP Traffic Router
RoamFlow
Retail Roaming Advisor
Data Management
Roaming Customer Experience Management
Roaming Replicator
NETWORK SERVICES
Enable the global connectivity
Interconnect Routing Management
IoT Packet Printing and Service Management
5G NWDAF Engine
Voice Policy Control and SIP Firewall
Core Network Elements (HSS, EIR, UDM/UDR)
eSIM Monetization
IoT SERVICES
Enable a network of things
Connectivity Management
Traffic and Policy Management.
Device and Asset Management.

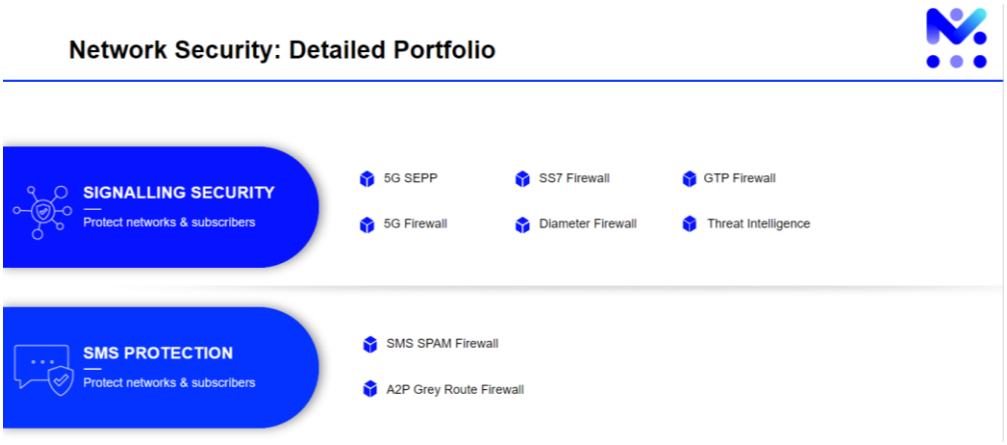

Roaming platform provides a central place to collect data, extract insights and automate actions in real-time
Collect & Ingest
Aggregate & Correlate
Insights
Actions
Active Signaling
Probes
External Data
Testing
Machine Learning & Analytics Models
Correlation, Aggregation, Filtering, etc.
Wholesale and Interconnect Analytics
Steering Analytics
Roaming Customer Experience Management
Customer and Retail Analytics
Permanent Roamer
IoT PacketPrinting
Steering of Roaming
Data Management Policy
Data Management Wallet
Campaign Management
Active Testing
Roaming Hub
GTP Proxy
Multiline
Local Breakout
Smart Mediator
Virtual Home Environment
RoamFilter
Least Cost and Smart Home Routing

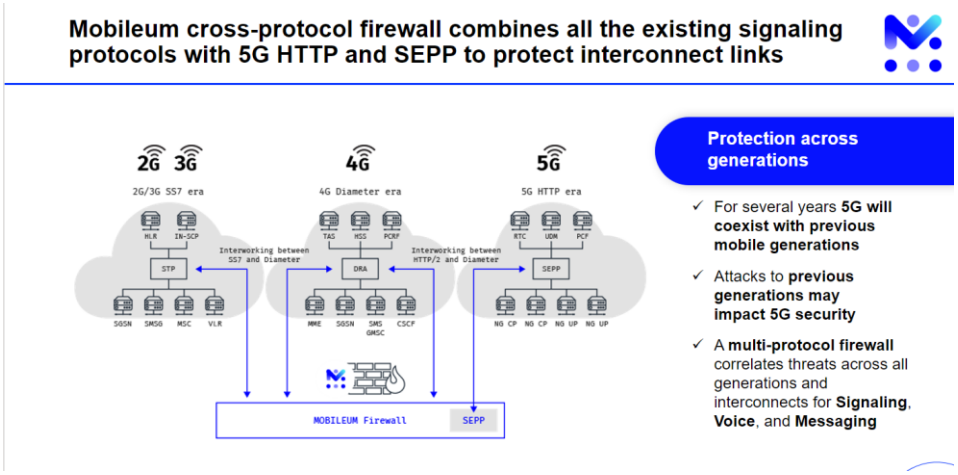

Mobileum 5G core network capabilities to enable and optimize next generation network rollouts
Slice Designer
Management & analytics
Signalling security
Policy & charging
UDSF
NSSF
NRF
NWDAF
SCP
SEPP
CHF
PCF
IMS
5G
AUSF
UDM
UDR
AMF
SMF
SMSF
SoR AF
NEF
Subscriber databases
User plane control
Exposure
5G core - Control Plane
Service Assurance as part of testing solutions (Services, devices, network)
5G Risk Management Analytics (Provisioning, Usage, Billing)
Full 5G Core
Incorporates functions and properties required to serve as the 4G and/or 5G core in a box
All functions handled internally and can connect to a 4G/5G radio access network
5GC with Risk and Testing overlay capabilities
Testing capabilities can drive Service Assurance accessing the fraud and revenue assurance impact feeding the 5G Risk management system
5GC components deployed in standalone mode
Network functions like UDM and SEPP are fully standards compliant and containerized for ease of integration

Risk Management

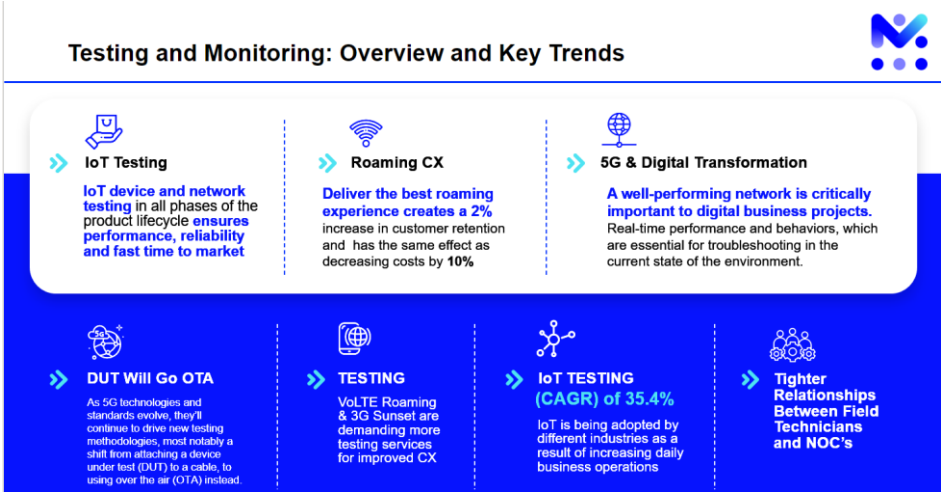


Security





Testing and Monitoring



Testing and Monitoring: Detailed Portfolio

NATIONAL QoS/QoE
Ensure Domestic N/W Experience

- 5G Testing
- Lab Testing
- Service Assurance
- Video Testing
- IMS Testing
- Core Network Testing
- IoT and eSIM Testing
- Mobile Money Testing
- Automation Framework
- Emergency Service Testing
- Voice, Data and Messaging Testing
- Smartphone and App Experience

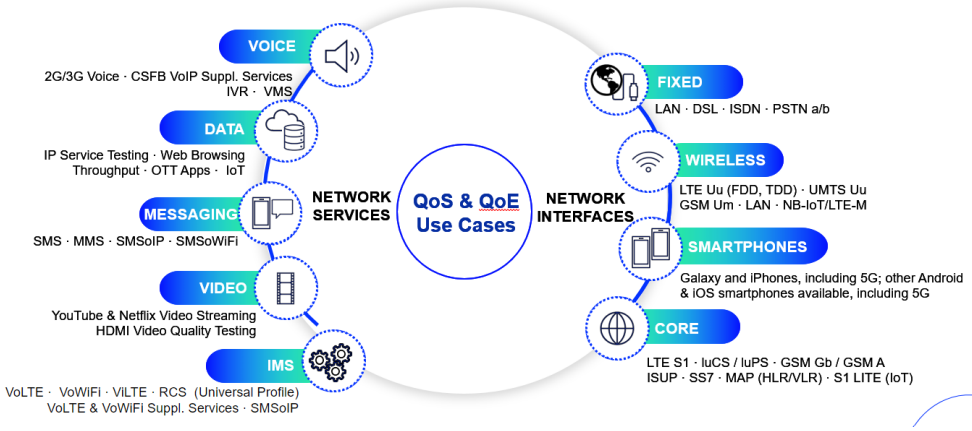
INTERNATIONAL QoS/QoE
Ensure International N/W Experience

- Roaming Quality Testing
- VoLTE Roaming Testing
- International Carrier Quality
- IoT and Connected Cars Testing
- Performance Intelligence
- Roaming Service Assurance

LAB & PERFORMANCE TESTING
Enhance Network Performance

- 5G Core Testing
- 5G Lab Testing
- 3G, 4G, 5G Functional & Compliance Testing
- 4G Core and VoLTE Testing
- Cellular IoT Testing
- dsTest Platform

Domestic Testing | Our SITE platform covers a wide range of network services and interfaces



International Testing | GlobalRoamer offers the world's largest cloud testing infrastructure for International QoS/QoE

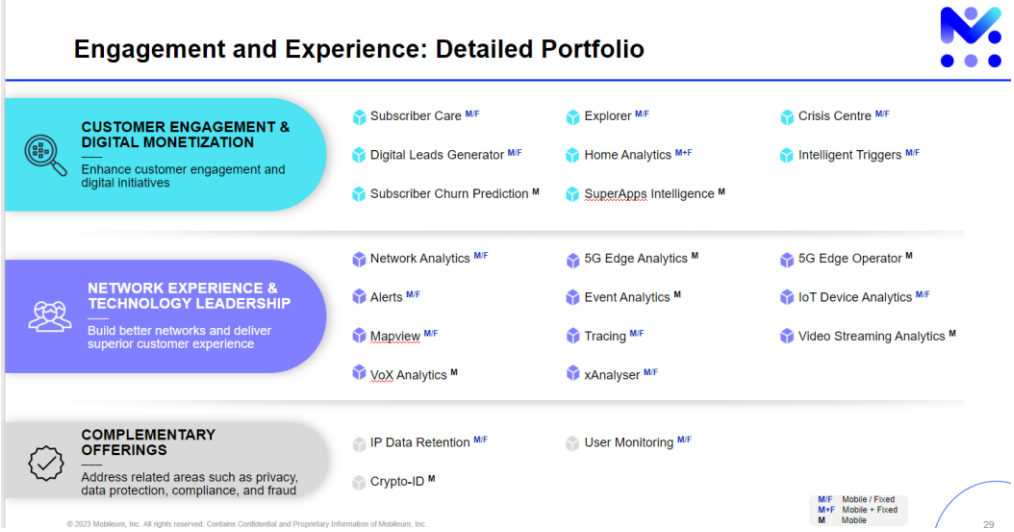
Central SIM Multiplexer with a SIM Pool from 415 MNOs

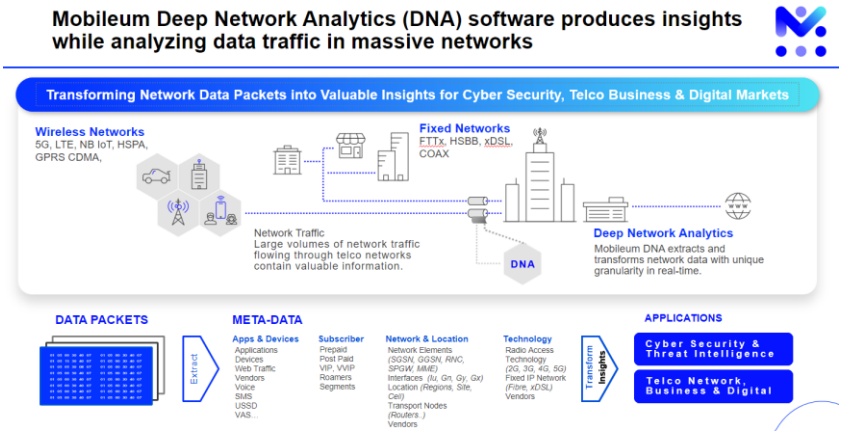
- 784 networks
- 354 locations
- 218 countries
- 606 pool SIM cards and MVNOs

- 97 calling cards
- 41 VoIP accounts
- 50 fixed line & carrier select
- 780 mobile originating networks
- 15 carrier platforms with access to 789 carrier routes

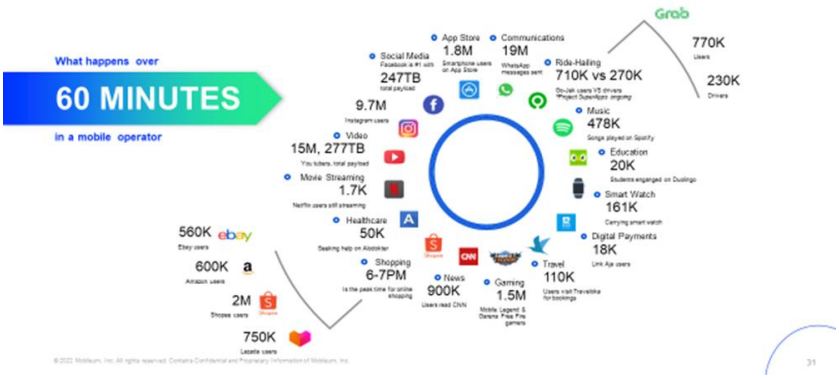
Individual routes subject to outages and linked to roadmap. Numbers stated are subject to changes.

Engagement & Experience

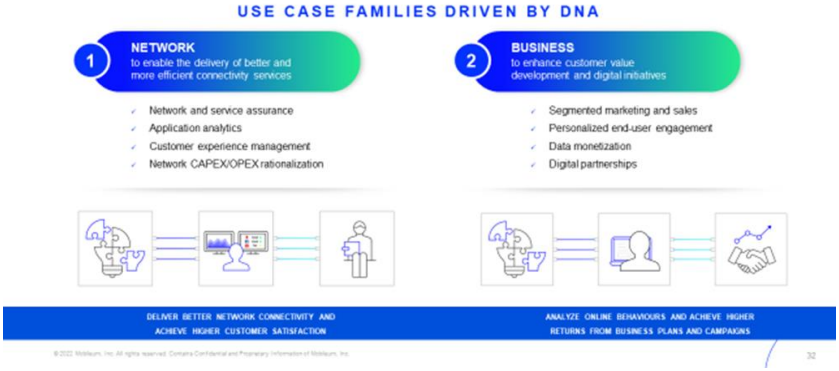




DNA generates a comprehensive picture on all end-users' interactions with data applications



DNA drives two major use case families in network operators: network and business applications

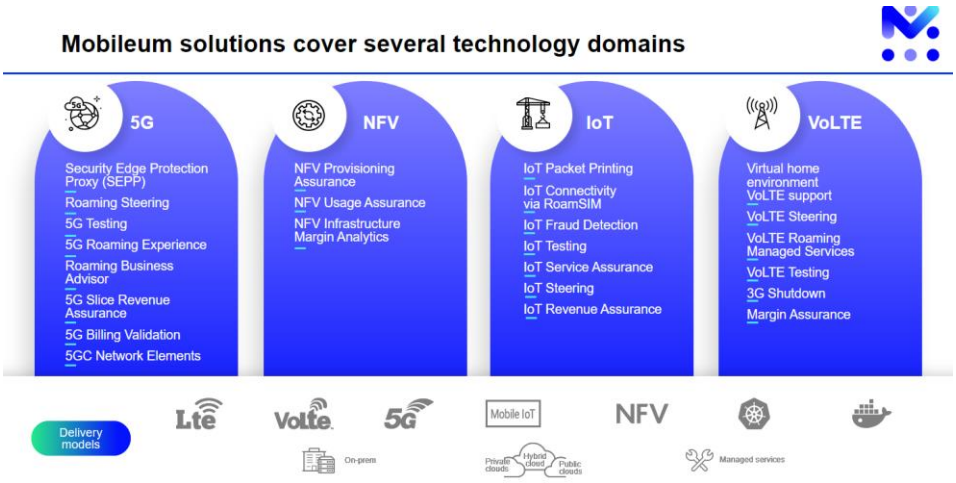


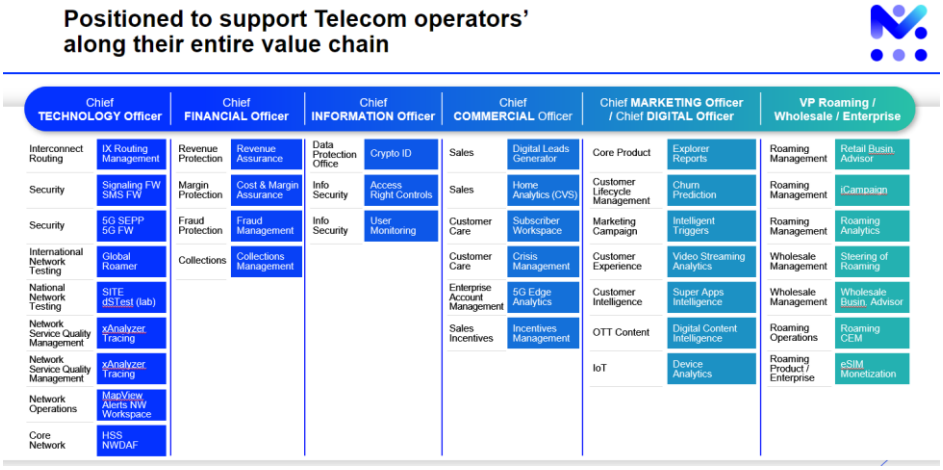
Our insights make new or better actions possible for both use case families

Use Case families	1 NETWORK	2 BUSINESS
1 INSIGHTS CONSUMED	✓ Historical & real-time network performance metrics ✓ Application-level events ✓ Correlated information (across devices, locations etc.)	✓ Historical and real-time end-user behaviors ✓ Application-level events ✓ Individualized information (for each end-user)
2 ACTIONS ENABLED	✓ Better management of network parameters & design ✓ Optimized network resource deployment ✓ Timely operational interventions	✓ Effective up-sell and cross-sell activities ✓ Digital partnerships with 3rd parties ✓ Better design of end user experiences and products
3 IMPACTS OBTAINED	✓ Higher end-user satisfaction, lower churn ✓ Cost-efficient network management ✓ Lower CAPEX and OPEX spending	✓ Higher revenues, lower churn ✓ New revenue streams through digital models ✓ Innovative products and services

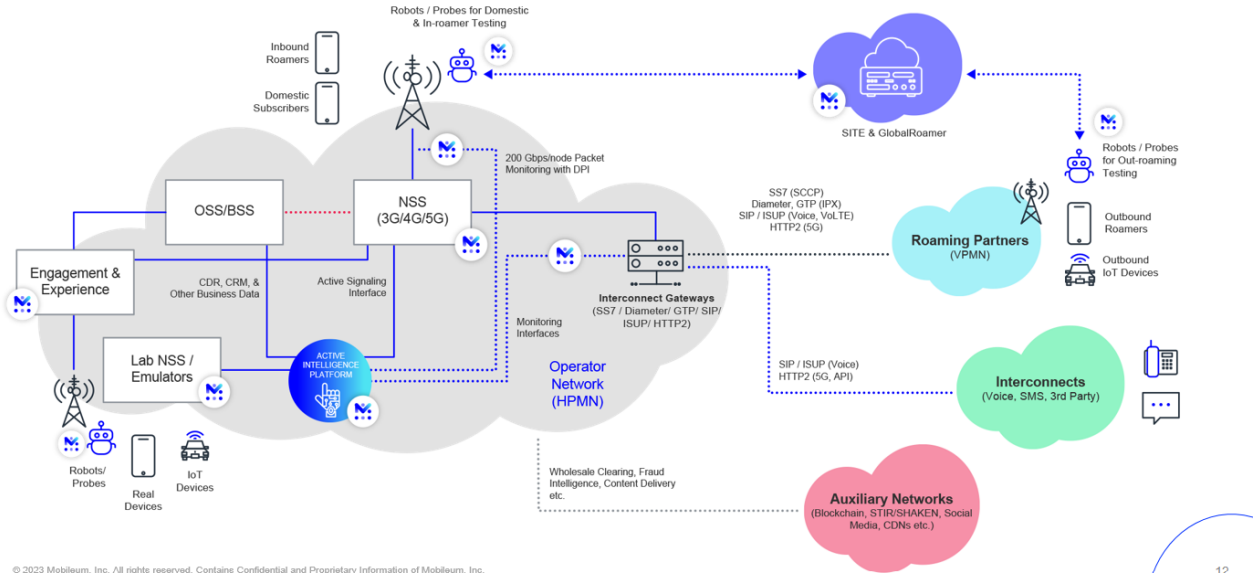
Why Mobileum?

Mobileum's solutions cover several technology domains.





Mobileum Network Presence



5G Solution Strategy

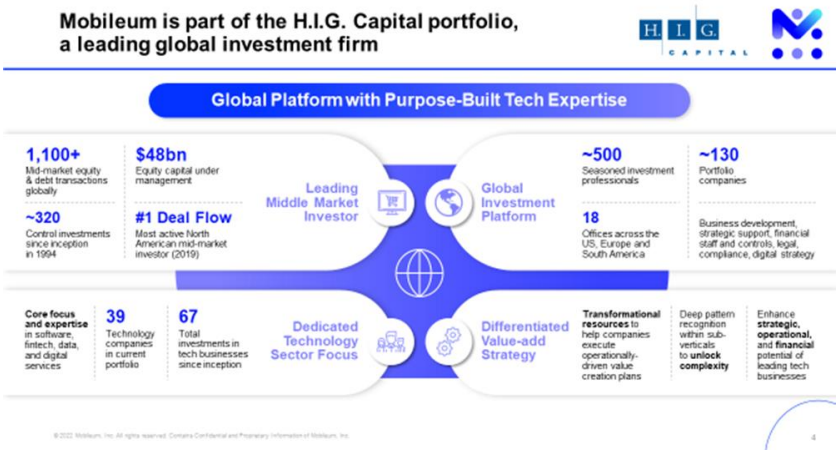
Cloud-native, Container, and Micro-service technology

	Evolution to 5G (GA 2021)		New 5G products (GA 2021)		In development
network & roaming intelligence	Traffic Steering – for 5G NSA, SA; OTA	Roaming Customer Experience Management			NWDAF++ : Network Data Analytics Function
	iCampaign (with SIP, RCS)	Wholesale Business Advisor incl BCE			UDSF : Unstructured Data Storage Function
	Roaming Replicator (piggyback roaming)	Retail Roamer Analytics and RoamWallet			Slice Designer & Manager
security intelligence	5G support in Cross Protocol Firewall	Vulnerability Assessment Services	SEPP		SCP (Service Comm. Proxy)
	Threat Intelligence for 5G				NEF (Network Exposure Function)
testing & monitoring intelligence	5G Remote Radio Testing	5G, IoT & eSIM E2E Testing	5G SA Core nw testing	CI/CD – Automation Framework	
			5G Lab Testing	5G Service Testing (Roaming, Natl., UE, IoT)	
fraud & risk intelligence	5G Provisioning Assurance	5G Service Assurance	5G IoT Assurance		5G Closed Loop Service Assurance
	5G Data Fraud Mgmt.	5G Rating and Billing Assurance			5G SLA/QoS Assurance (incl. Edge)
	Content Piracy Detection				

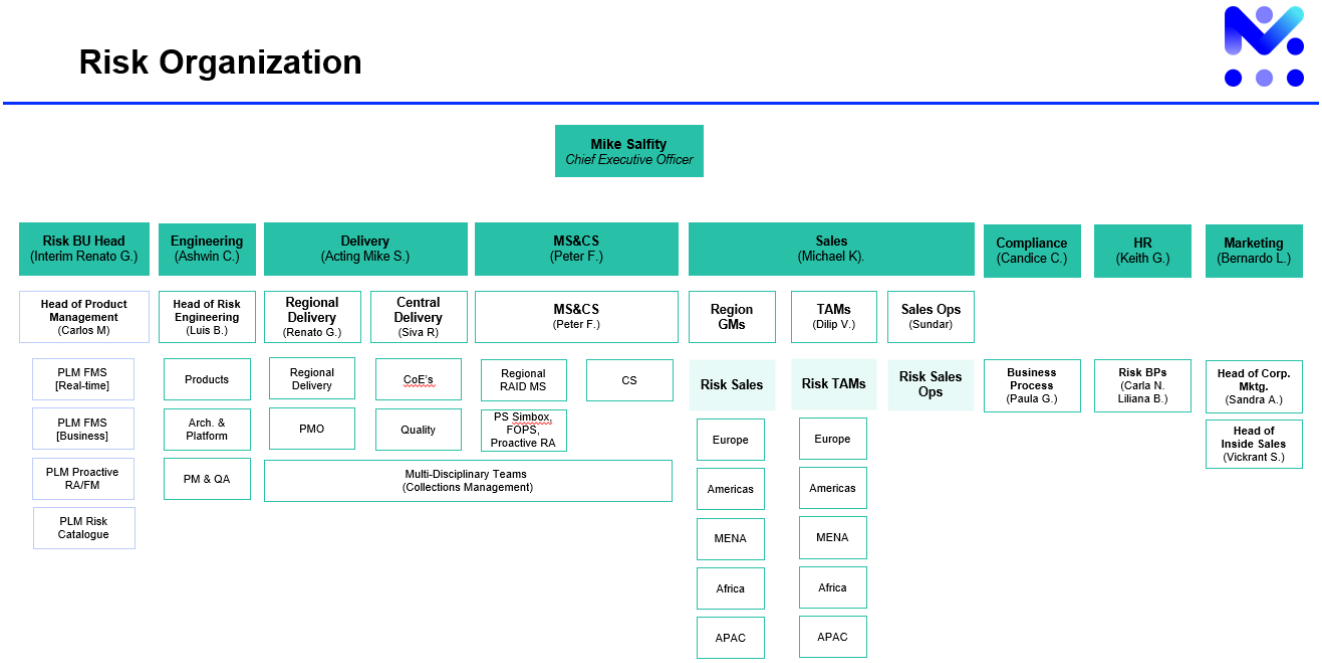
What is Mobileum's Risk BU Commitment?

The Commitment that *Mobileum Risk BU* makes to the Market is reflected by significant profitability and efficiency gains for its Customers' business, based on the design and implementation of solutions that optimize process efficiency, higher productivity levels, performance, and Customer satisfaction.

About our Shareholder



Mobileum Risk BU's Internal Organization



Certifications & Memberships

Certifications

Mobileum Risk BU Quality Management System was conceived in order to respond to all requirements of the standard NP EN ISO 9001 (International Standards for Business, Government and Society).

The certification audit took place on June 2002 and covered all activities related with software development, consulting, placement, Solution Maintenance and product management. The audit team recommended the NP EN ISO 9001 Certification;

Most Project Managers of Mobileum Risk BU are certified with the International Project Management Association (IPMA) and Project Management Institute (PMI);

Mobileum Risk BU is Certified in NP EN ISO/IEC 27001:2013 – ISO 27001 Information security management systems-Requirements, with UKAS Accreditation, since 2015;

Memberships

Mobileum Risk BU is an active Member of the GSM Association and of the TeleManagement Forum.

Alliances and Partnerships

For the past 10 years Mobileum Risk BU built a solid footprint of successfully delivered projects and technologies due to powerful solutions and strong partnerships. The company has shown in multiple projects the capability to work and support our partners during the entire sales, implementation and support cycle.

For the past 10 years Mobileum Risk BU established partnerships and alliances with major providers of information systems and integration services. The company was able to follow an internationalization strategy where working with partners with vision, complementary offer and the same approach to doing business delivered win-win-win results – for our customers, for our partners and for Mobileum Risk BU.

Through Mobileum Risk BU, the business partners gain access to leading specialists and leading technology in Business Assurance software and in niche Business Support Systems software. Partners gain the opportunity to leverage on Mobileum Risk BU world class software products.

Mobileum Risk BU is strongly committed in delivering best-of-breed services and solutions to enhance and optimize our customers' business processes. Mobileum Risk BU believes that combined expertise and technology lead to better solutions delivered to customers.

The company recognizes in our business partners a strategic contribution to our growth. The commitment to training, support and constant interactivity between partners and Mobileum Risk BU allows the creation of proposals in which the distinctive factors and the value of the solutions are clearly demonstrated.

3 Methodologies

The creation, internal diffusion and use of methodologies are critical agents for the success of projects developed by Mobileum Risk BU. To this end, a number of methodologies were created from the beginning to support the following activities:

- Managed Services, Project Management, Tests , Solution Development, Solution Maintenance, etc

To ensure the awareness and correct application of the above by all Mobileum Risk BU consultants, a continuous internal training program was established, covering all employees.

The use of methodologies enables Mobileum Risk BU:

- to have a unique way of working with any type of customer;
- to rapidly integrate new employees;
- to use a language common to all company employees;
- to expand and replace project teams;
- to easily control its projects;
- to easily communicate with all its customers;

3.1 Project Management Methodology

All Mobileum's Risk BU projects follow a common Project Management methodology that guarantees the follow-up of all project activities, from the awarding of the proposal to final project acceptance by the customer.

All the activities foreseen in this methodology aim to guarantee that:

- Customer requirements are correctly stated, implemented and tested;
- The chosen team has all the necessary skills for project execution. All projects involving software development include programmers, a testing team and people responsible for configuration management;
- The deadlines agreed on with the customer are met and the project requirements fulfilled;

- The project runs within the quality parameters specified by the applicable methodology;
- A reporting mechanism is implemented with the customer that includes periodical meetings with the customer and project status reports;
- The customer accepts the solution delivered

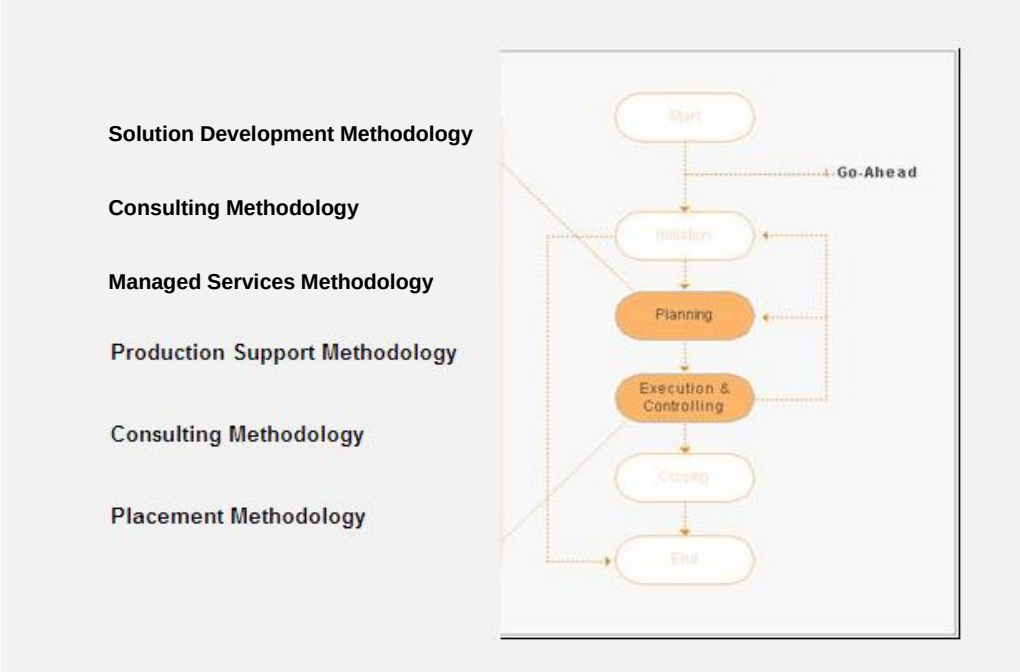


Figure 1 – Project Management Methodology

3.2 Managed Services Methodology

Managed Services Methodology is an umbrella term for third-party monitoring and maintaining of computers, networks and software. The actual equipment may be in-house, at the third-party's facilities or even at customer facilities, but the "managed" implies an on-going effort; for example, making sure the equipment is running at a certain quality level or keeping the software up-to-date.

Mobileum Risk BU follows this methodology shown in the following figure:

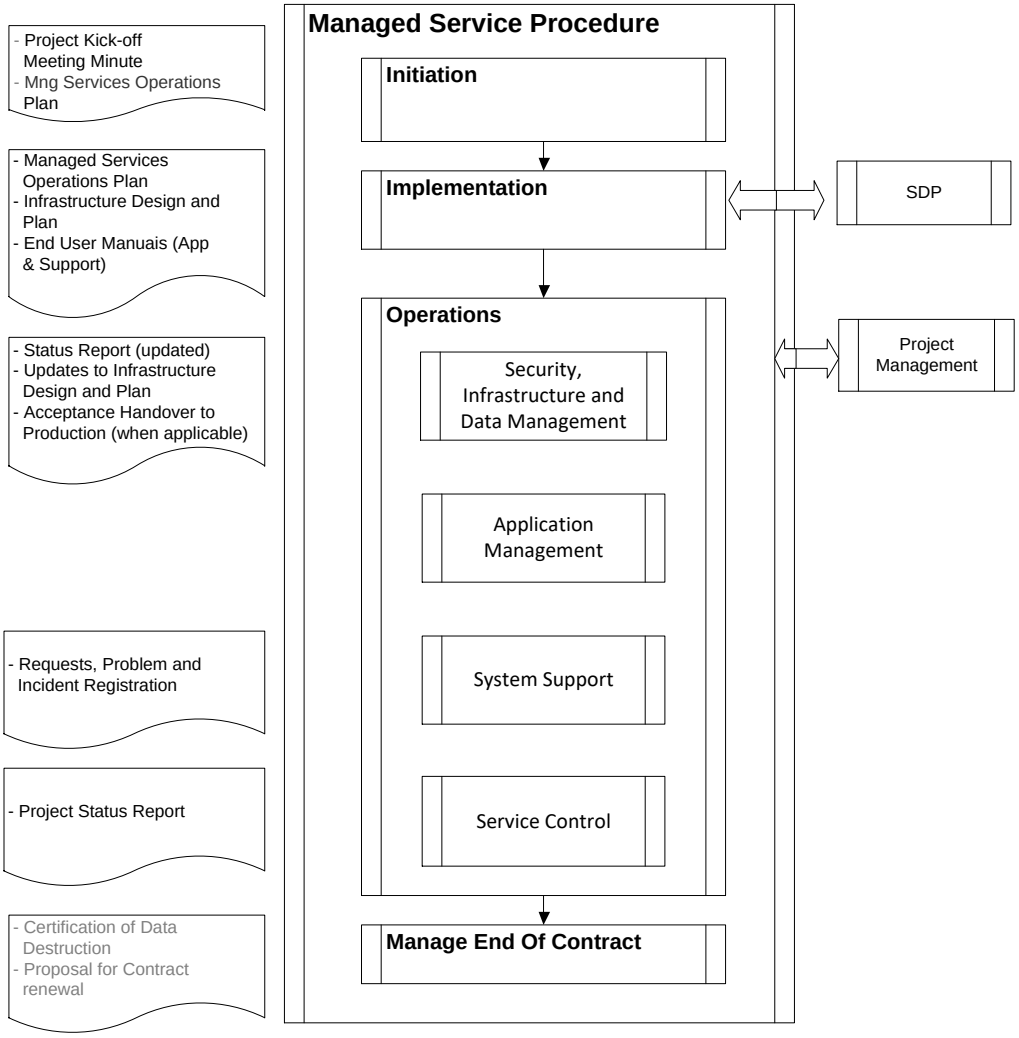


Figure 2 – Managed Services Methodology

4 Information security Management System Context

4.1 Objectives and Importance of Information Security Management System

The main objectives for the implementation of Mobileum Risk BU Information Security Management System are:

-More Business:

-Integrate Information Security in the business objectives of Mobileum Risk BU, as a distinguishable and competitive factor;

-Reliability, Safety:

-Increases reliability and safety systems;

-Increases confidence and satisfaction of Customers, Partners and Suppliers;

-Improves Operational Performance and Quality:

- Ensure business continuity always keeping the highest levels of service quality;
- Promote within staff members a culture of responsibility and accountability for Information Security;

- Compliance with Industry and Legal requirements

- Ensure compliance with industry and legal requirements in all countries where Mobileum Risk BU develops business;

-Cost reduction:

-More efficient investments;

Information is one of the most critical assets of an organization. With the generalization of information technologies and, in particular, of the Internet the volume of digital information has been increasing in an exponentially way over the last years.

The protection of information is therefore of vital importance, so that the trust among the several business partners may be maintained and solidified.

The availability, integrity and confidentiality of information, in a rigorous and expedite way, to support business decisions has become a competitive advantage for organizations.

If the information of an organization is disclosed, manipulated or made unavailable, the consequences can be serious and create an impact in the organization´s reputation and performance.

The information security should be monitored as a dynamic process, so that it is possible to predict and react to information security threats.

The risks resulting from information security threats have to be managed based on information made available through risk management methodologies. The result of the application of these methodologies, namely the development of risk analysis, enables objective planning of future investments in information security, as to obtain better results.

Information Security can be defined as the preservation of:

1. **Confidentiality**: assure that information is accessible to authorized personnel only;
2. **Integrity**: safeguard the correctness and completeness of information and processing methods;
3. **Availability**: assure that authorized users have access to information and associated assets when required;

Information Security Management System (ISMS) can be obtained through the implementation of a number of security controls: policies, practices, processes, organizational structures and technological solutions. These controls can be set to ensure that Mobileum Risk BU Security Policy objectives are achieved.

Mobileum Risk BU Information Security is based on the international standard ISO/IEC 27001:2013 and the controls, Annex A, are covered through the following domains:

- Security Policy;
- Organization of Information Security;
- Human Resources Security;
- Asset Management;
- Access Control;
- Cryptography;
- Physical and environmental security;
- Operations security;
- Communications security;
- System acquisition, development and maintenance;

- Supplier relationships;
- Information security incident management;
- Information security aspects of business continuity management;
- Compliance.

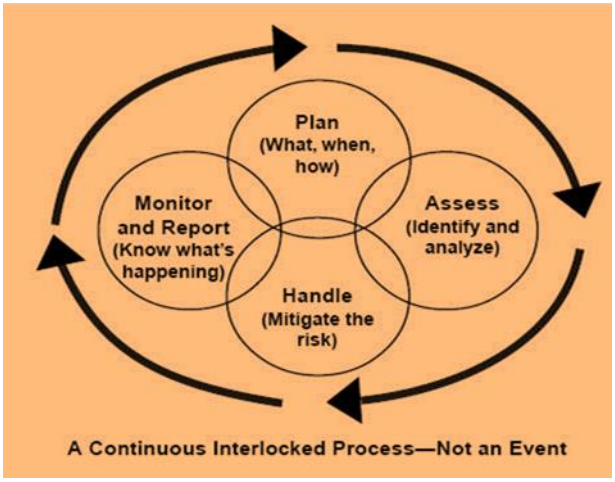


Figure 3 – PDCA

As with all management processes, an ISMS must remain effective and efficient in the long term, adapting to changes in the internal organization and external environment, therefore incorporated the "Plan-Do-Check-Act" (PDCA), or *Deming* cycle, approach:

1. The **Plan** phase is about designing the ISMS, assessing information security risks and selecting appropriate controls.
2. The **Do** phase involves implementing and operating the controls.
3. The **Check** phase objective is to review and evaluate the performance (efficiency and effectiveness) of the ISMS.
4. In the **Act** phase, changes are made where necessary to bring the ISMS back to peak performance.

4.2 Needs and expectations of interested parties

Information Systems are a decisive factor in organizational competitiveness, working as a tool that stimulates productivity and critical to the decision making process at various organization levels.
New threats targeting Information Systems rise, in part, due to today's society extensive use of the Internet. All organizations are susceptible to attacks no matter its size, nature or what IT resources and communications are currently in use.

Mobileum Risk BU intends to manage the physical and logical security, the training and awareness of all levels including all collaborators (described as Participants) that interact in the Information Security Management Scope, to guarantee the continuity of business critical processes and the quality of the rendered service.

The Information Security Management System is intended for all involved parties, like Mobileum Risk BU Participants in Mobileum Risk BU Information Security Scope, Clients, Employees, Shareholders, Partners and Suppliers, Regulators, Emergency Services, Media.

All the Participants have to assure the appropriate information security level in order to support and protect Mobileum Risk BU interests.
This will make the operation of all business units possible, thus allowing the rendering of services and the fulfillment of the mission in a safe and effective way.

Any agreements with external entities that involve access to the information processing system should take into account all relevant security requirements.

Mobileum Risk BU intends that Information Security contribute as a competitive factor and decision making supports. To achieve it is necessary that the organization observes security considerations in all aspects of business, in order to protect their assets, Participant's data privacy, while at the same time providing access to services and available information.

Information Security Management System is applied to all external partners (companies or individuals) that need to use the Information Systems infrastructure, facilities or information under Mobileum Risk BU responsibility.

Information Security risks resulting from the involvement of external entities should be identified and the appropriate controls implemented before the access is granted, in agreement with the Security management Team.

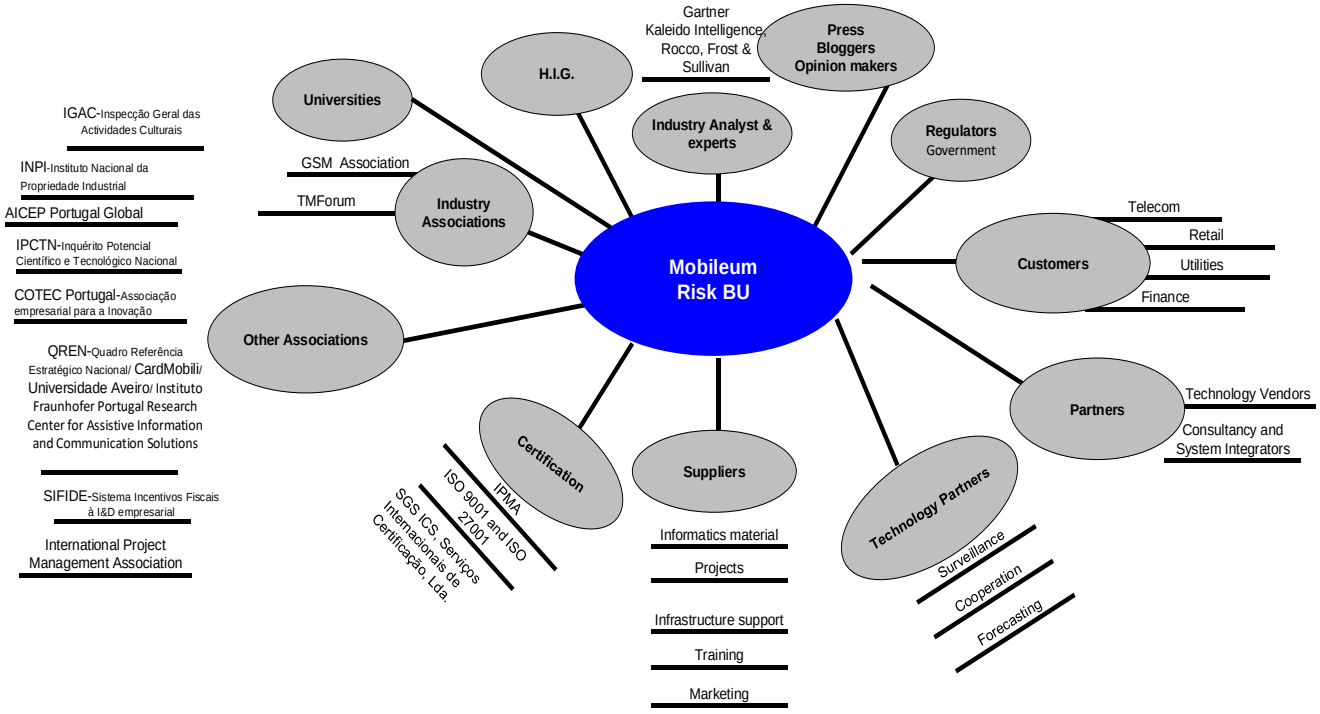


Figure 4 –Interface Management Model

Here we have the Interface Management relation model where we have all the associations, certification entities, industry associations, shareholder, partners, suppliers, customers, universities, etc, that belong to our interface management.

If the information is relevant, in the context of the activities undertaken by the company, the information is widespread and treated by the responsible for each area, that will give content to the preparation of the annual VBM (Value Based Management; part of the SPC), where proposals are made for the management of business for the future 5 years.

4.3 Information Security Management System Scope

Ensure Confidentiality of Customer data in the Systems operated by Mobileum Risk BU:

-Managed Services (Madrid Office);

Managed services are the practice of outsourcing day-to-day management responsibilities and functions as a strategic method for improving operations and cutting expenses. The managed services area is in charge of running some specific business activities for the Client.

Regarding the Infrastructure responsibility, we can have three different options: Mobileum Risk BU own systems, Subcontracted or Customer's responsibility.

Mobileum's Risk BU Managed Services is divided in 2 main categories: Business and Technological. Both service categories are independent and the customers can acquire them separately or a mix of them.

In the Business category we have **The Business Managed Services**, which is a Team leveraged by skilled people in charge of the operations and responsibilities of specific business functions (or processes) supported by Mobileum's Risk BU tools. This team has the responsibility for maintaining the Integrity and ensure Completeness and Accuracy of the system and can act as an extension of the customer team.

In the Ttechnological components we've: **Technical Managed Services, Managed Hosting and Application Solution.**

The Technical Managed Services is a group of people with comprehensive delivery, support and maintenance capabilities of a specific Mobileum Risk BU software solution running on the customer's premises or on Mobileum Risk BU managed hosting. This service includes the operation of the system, ensuring the execution of all jobs on schedule without errors and that all the reporting capabilities contracted have updated data.

The Managed Hosting is a hosting solution based on Hardware Infrastructure, necessary 3rd part Software and establishment of Communications, allowing Mobileum Risk BU Business solutions implementation.

This service includes the complete management of third party products, capacity management, Application Solution upgrades and patches. The service is operated using a three level support structure in an 8x5 local time model.

The Application Solution is a Mobileum Risk BU Business solutions based on Mobileum's Portfolio, of Raid and/or Brokers solutions, which allow the best performance of customer business activities, assuring the risks. The available modules are predefined and adjusted configuration of the main products, allowing standardize and faster implementations, and consequently a more cost effective price of the service.

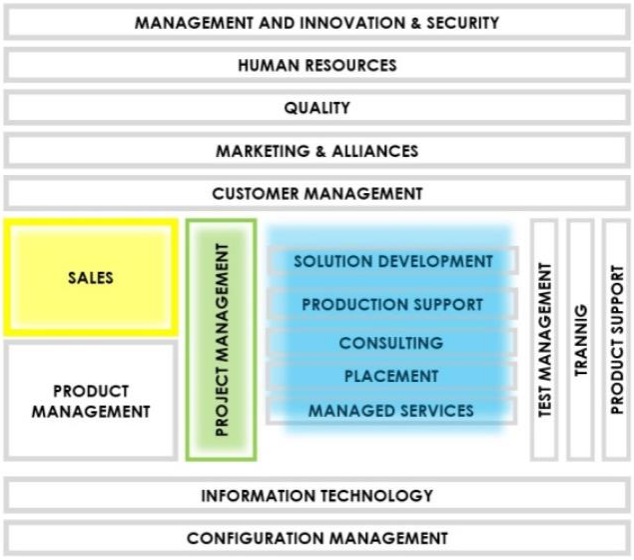
Mobileum Risk BU scope within NP EN ISO/IEC 27001 – ISO 27001 Information security management systems is applied in Managed Services - Madrid office;

4.4 Information Security Management System

ISMS is completely integrated in Mobileum Risk BU Quality Management System, that will allow Management having a better understanding of ISMS potential business benefits, while the organization is already accustomed to the PDCA approach and has this method completely ingrained in their DNA.

The system is organized by processes, as shown in the following figure.
Mobileum's Risk BU business support processes – Project Management, Solution Development, Production Support, Consulting, Placement, Managed Services are supported by particular methodologies that guarantee uniformity and quality in their execution.

Information management Security management System is incorporated in Management Process due to the Importance of this process for the organization.
Information Security Policy is defined and completely integrated in Mobileum Risk BU Annual Planning Organization Plan .



igure 5 – Mobileum Risk BU Processes Map

All documents associated to processes are in English. Support models are both in English and Portuguese.

The MANAGEMENT AND INNOVATION & SECURITY Processes comprises all activities related to:

- The strategic planning cycle;
- The Financial and Administrative Control of projects;
- The control and reporting of company performance indicators;
- Purchasing

Information Security Management System activities:

-Establish, Implement update and Operate ISMS;

-Monitor and review ISMS annually;

-Maintain, update and Improve ISMS;

-Implement ISMS Plan annually (ISMS Plan & Internal audit Plan);

-Management and measure ISMS performance indicators;

-ISMS System Revision;

The HUMAN RESOURCES process comprises all activities related to:

- Human resources planning;
- Recruitment and selection;
- Integration of new employees;
- Performance evaluation;
- Employees training;
- Skills management;
- Management of indicators related to human resources;

The QUALITY process comprises all the necessary activities to guarantee the fulfilment of NP EN ISO 9001 standard requirements, particularly:

- Process identification;
- Determining process sequence and interaction;
- Planning and revision of the quality management system;
- Definition of rules for document control;
- Definition of rules for register control;

- Quality Audits;
- Corrective and preventive actions;
- Management of quality-related indicators;

The MARKETING & ALLIANCES process comprises all activities related to:

- Relationships with analysts and press, Event Management, Offer Management, Product Management, Web-Marketing, Contact Management, Competition analysis, Campaign Management;

The CUSTOMER MANAGEMENT process comprises all the activities related to the:

- Collection and processing of Customer Satisfaction evaluation;
- Surveying of needs;
- Garnering of feedback from the projects under development

The collection and processing of the Customer satisfaction evaluation is managed by the person responsible for the quality process. Management of other activities is the responsibility of the account managers responsible for the large customers.

The SALES process comprises all activities from the identification of a business opportunity to the awarding of the proposal by the customer.

The PRODUCT MANAGEMENT process encompasses all activities related to Mobileum's Risk BU product management namely the planning of the conception and evolution of WDT products.

The PROJECT MANAGEMENT process encompasses all operational activities from the start of the project until its acceptance by the customer, namely:

- Establishment of the project team;
- Project planning;
- Management of the team and planned activities;
- Management of the relationship with the customer;
- Project status control and reporting;
- Guarantee of the garnering and implementation of all the customer's requirements.

The responsibility of fulfilling all steps of the process is incumbent on each project director.

The MANAGED SERVICES process defines the methodology to be applied by Mobileum Risk BU consultants in all projects involving the delivery of solutions on a Managed Services Model.

These solutions may be delivered with different service layers:

- Technical Managed Services;Business Managed Services; Managed Hosting and Application Solution

Depending on the service level layer Mobileum Risk BU will provision the customer in the Managed Services infrastructure and will operate the system in terms of Security, Infrastructure and Data Management, System Support and Service Control.

The SOLUTION DEVELOPMENT process defines the methodology to be applied by Mobileum Risk BU consultants in projects implying software development or package customization.

The responsibility of fulfilling all steps of the process is incumbent on each project director.

The CONSULTING process defines the methodology to be applied by Mobileum Risk BU consultants in projects that imply information surveying activities, recommendations, information transmission, process surveying and improvement and impact analysis.

The responsibility of fulfilling all steps of the process is incumbent on each project director.

The PLACEMENT process defines the methodology to be applied by Mobileum Risk BU consultants in projects involving the placement of skills during a determined period of time.

The responsibility of fulfilling all steps of the process is incumbent on each project director.

The PRODUCTION SUPPORT process defines the methodology to be applied by Mobileum Risk BU consultants in all projects involving system production support, whether or not the systems are developed by Mobileum Risk BU.

The responsibility of fulfilling all steps of the process is incumbent on each project director.

The TEST MANAGEMENT process defines the methodology to be applied by Mobileum Risk BU consultants in software testing activities.

The responsibility of fulfilling all steps of the process is incumbent on each project director.

The PRODUCT SUPPORT process is applicable to all situations where Mobileum Risk BU assumes a contractual commitment with a customer to supply Maintenance services for products developed by Mobileum Risk BU Soft.

The TRAINNING process defines the methodology to be applied by Mobileum Risk BU consultants in all projects involving the training of Human Resources in the solutions developed by Mobileum Risk BU.

The responsibility of fulfilling all steps of the process is incumbent on each project director.

The INFORMATION TECHNOLOGY process comprises all the activities needed for the company's physical resources management, namely:

- Backups;
- Workstation definition and installation;
- Security;
- Anti-virus Maintenance;
- Register of software licences;

The CONFIGURATION MANAGEMENT process comprises the activities of:

- Version management;
- Changes management;
- Configuration management;
- Baselines creation;
- Packaging of the solution to be sent to the customer

A structure exists with persons responsible for processes, who guarantee that all NP EN ISO 9001 standard requirements are consistently complied with, implemented and monitored.

The garnering of feedback, changes and the monitoring of processes, as well as their documentation and maintenance, is the responsibility of each process manager.

Mobileum Risk BU Quality Management System (NP EN ISO 9001:2015) covers some of the NP EN ISO 27001 - Information Security Management System requirements.

4.5 Value Chain

Mobileum's Risk BU value chain is shown in the following figure, reflecting the linking of processes.

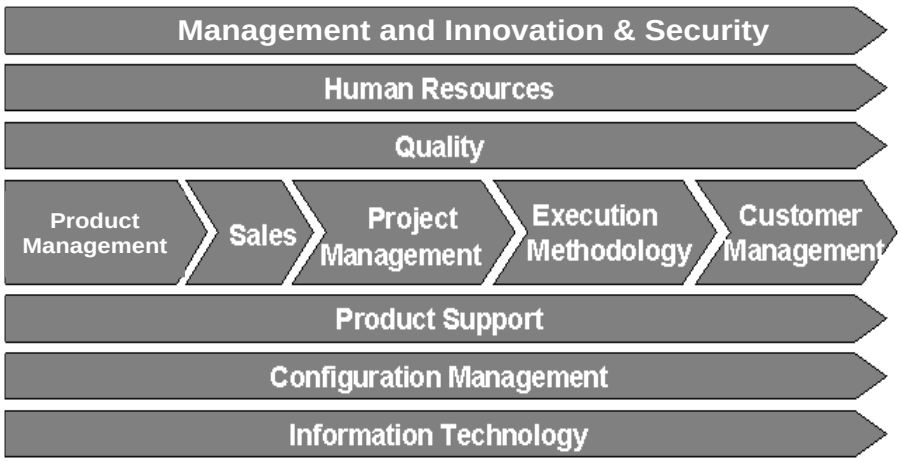


Figure 6 – Value Chain

4.6 Relation between processes

The processes described below support Mobileum's Risk BU activities in an integrated way. The sequence of processes and the information flow between them is shown in the figure below.

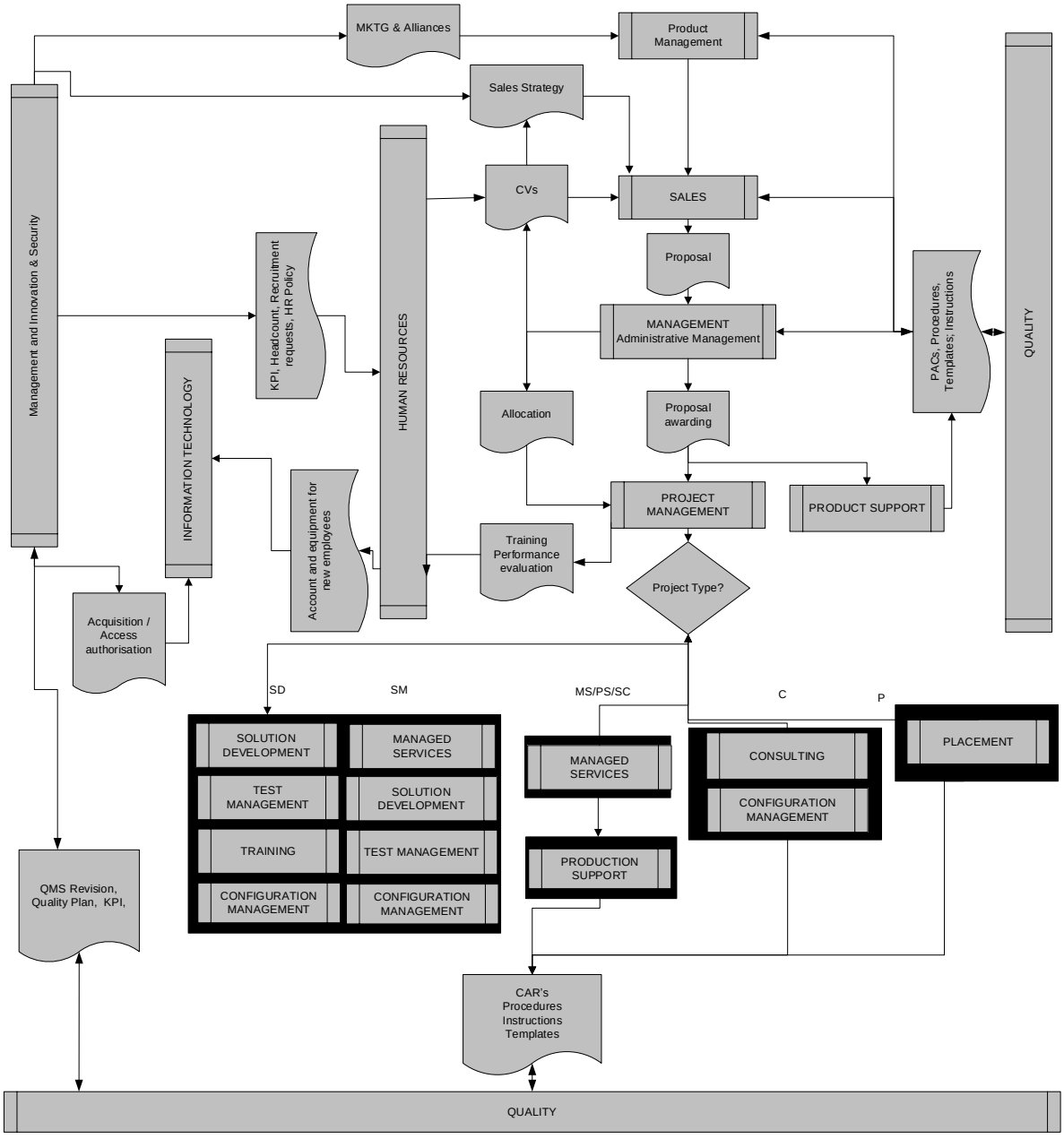


Figure 7 – Relation between processes

4.7 ISMS requirements for Business Continuity

Business Continuity Plan is adapted to each project. All the rules defined in T_QMS_386_E - Business Continuity Plan referring Datacenter rules and policies and also accomplishing what was defined in the contract with the customer.
Mobileum Risk BU also has a Business Continuity Plan in a corporate point of view related with ISM scope in Headquarters and Madrid (P_QMS_047_E - Business Continuity Plan Corporate).
Also we have I_QMS_156_E - Legal Contractual and Business Requirements and I_QMS_156_S - Legal that have the legal requirements.

Important Contact in Portugal :

SUPERVISION AND REGULATORY ENTITIES:

ACT - Autoridade para as Condições do Trabalho

http://www.act.gov.pt/

Autoridade Nacional de Protecção Civil (National Authority for Civil Protection)

http://www.proteccaocivil.pt/Pages/default.aspx

http://www.prociv.pt/en-us/Pages/default.aspx

Comissão Nacional de Protecção de Dados (CNPD)

http://www.cnpd.pt/

Entidade Reguladora dos Serviços Energéticos - ERSE

http://www.erse.pt/pt/Paginas/home.aspx

https://www.erse.pt/

Associação Portuguesa de Direito Intelectual

Http://www.apdi.pt

https://www.apdi.pt/

CYBERCRIME POLICY:

- Organização Portuguesa de combate ao cybercrime (OPCC):

  opcc@europe.com

  https://www.policiajudiciaria.pt/unc3t/

Important Contact in Spain:

- Boletín Oficial del Estado ("BOE") – www.boe.es
- Agencia Española de Protección de Datos ("AEPD")– www.aepd.es
- http://europa.eu/eu (Unión Europea)
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=PT

- Communicaciones Electronicas

Diretiva 2002/58/CE

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002L0058&from=PT

EMERGENCY SERVICES PORTUGAL:

- Help national number: **112**
- Poisoning: **800 250 250**

HOSPITALS PORTUGAL:

- Curry Cabral: **217 924 200**
- Egas Moniz: **21 043 10 00**
- Estefânia: **21 312 66 00**
- Hospital de Braga: **253 027 00**
- Júlio de Matos: **217 917 000**
- Maternidade Alfredo da Costa: **21 318 40 00**
- Miguel Bombarda: **213 177 400**
- Pulido Valente **21 754 8000**
- Santa Maria: **21 780 5000**

- Santa Marta: **21 359 40 00**
- Santo António dos Capuchos: **21 313 63 00**
- São José: **21 884 10 00**
- São Francisco Xavier: **21 043 10 00**

HEALTH CENTERS PORTUGAL – Emergency:

- UCSP Sete Rios: **21 042 32 60**
- Lapa: **21 393 12 50**
- UCSP Lumiar: **21 752 71 10**
- Braga: **253 20 92 30**

CRUZ VERMELHA PORTUGAL:

- Ambulances: **213 913 900**
- Hospitals: **217 714 000**

FIRE DEPARTMENT PORTUGAL :

- HELP LINE: **213 422 222**
- PHONE: **213 924 700**

POLICE PORTUGAL

- GNR – Comando: **213 217 000**
- GNR - Brigada Fiscal: **218 112 100**
- Polícia de Segurança Pública: **213 466 141**
- Polícia Municipal: **217 268 022**

EMERGENCY SERVICES:

Help national number: 112 (Portugal & Spain)

Poisoning: Spain 098

Red Cross Spain :

Ambulances: **91 473 93 61**

Emergencies: **91 522 22 22**

FIRE DEPARTMENT Spain:

Madrid and Móstoles: **080**

Community of Madrid: **085**

POLICE Spain

National: **091**

Municipal: **092**

Guardia Civil: **062 - 91 514 60 00**

Protección Civil Madrid: **91 537 31 00**

Cruz Roja Madrid: **91 522 22 22**

Seguridad Social y Urgencias SAMUR Madrid: **061**

Ambulancias Madrid: **061 - 91 479 93 61**

Bomberos Madrid: **080 – 085 – 092**

Atención al Ciudadano: **010**

5 Leadership

5.1 Leadership and Management commitment

The decision to implement an Information Security Management System was taken by the Management Commission, and all means were made available forthwith for the execution of a project that would enable the fulfilment of this objective.

The revision and adaptation of the Information Security Management System have been backed by the Management Commission on a periodic basis, in accordance with the company's internal needs and strategic changes.

It is incumbent on the Management Commission to review and approve the Information Security Policy, described in this Manual:

- Suits the organization's objectives;
- contemplates the fulfilment of the Information Security Management System's requirements and the continuous improvement of its efficacy;
- Supplies a framework for the establishment and review of the objectives of Security;
- Is communicated and understood within the organization;
- Strong collaboration with Partners, Regulators and with the environment where the company is incorporated ;
- Employees as part of Information Security Management System ;
- Focus on internal training ;
- Encourage, promote communication and constant feedback between employees and Top Management;
- Promote continuous improvement of the effectiveness of the ISMS;

Mobileum Risk BU Top Management presents to Mobileum Risk BU the Company strategic plan, each year to all employees.
Mobileum Risk BU Information Security Policy is completely connected with those company strategic guidelines.

Mobileum Risk BU guides its innovative activity on the grounds of its mission and strategic vision, which continually seeks to add value to their customers and partners.
The mission of Mobileum Risk BU is reflected in the commitment to contribute to the business sucess of its customers.

Guarantees it together with its partners, through aligning their solutions with the business challenges of clientes and through his own knowledge.

Customer satisfaction allied with the motivation and excellence of Mobileum's Risk BU people are key for an effective and results driven management of Information Security Management System.

Mobileum Risk BU strategy from start included an agressive internationalization based on the competitive advantage resulting from this innovative, distinctive and competitive range of products and solutions, which led the company to become a global market leader in Telecom Revenue Assurance Software.
Mobileum's Risk BU strategic vision of being a global market leader in Business Assurance solutions will allow the company to reach a new development stage and maintain the innovation path.
Mobileum's Risk BU target industries (originally Telecommunications, but currently investing in its expansion into the Retail, Energy and Financial) are highly dynamic and high tech driven industries where the capacities to innovate and to keep up with the market are key success factors for any solution provider.

Based on them, Mobileum Risk BU draws up its technological evolution plan that periodically is re-evaluated and adapted to external conditions, always aligned with ISMS principals and with Mobileum Risk BU strategy.

5.2 Information Security Policy

Information Security Policy can be defined as the preservation of:

1. Confidentiality: assure that information is accessible to authorized personnel only;
2. Integrity: safeguard the correctness and completeness of information and processing methods;
3. Availability: assure that authorized users have access to information and associated assets when required;

5.3 Importance of Security Policy

Information is one of the most critical assets of an organization. With the generalization of information technologies and, in particular, of the Internet the volume of digital information has been increasing in an exponentially way over the last years.

The protection of information is therefore of vital importance, so that the trust among the several business partners may be maintained and solidified.

The availability, integrity and confidentiality of information, in a rigorous and expedite way, to support business decisions has become a competitive advantage for organizations.

If the information of an organization is disclosed, manipulated or made unavailable, the consequences can be serious and create an impact in the organization´s reputation and performance.

The information security should be monitored as a dynamic process, so that it is possible to predict and react to information security threats.

The risks resulting from information security threats have to be managed based on information made available through risk management methodologies. The result of the application of these methodologies, namely the development of risk analysis, enables objective planning of future investments in information security, as to obtain better results.

Information Security Management System (ISMS) can be obtained through the implementation of a number of security controls: policies, practices, processes, organizational structures and technological solutions.
These controls can be set to ensure that Mobileum Risk BU Security Policy objectives are achieved.

Mobileum Risk BU Information Security is based on the international standard ISO/IEC 27001:2013 and the controls, Annex A, are covered through the following domains:

- Security Policy;
- Organization of Information Security;
- Human Resources Security;
- Asset Management;
- Access Control;
- Cryptography;

- Physical and environmental security;
- Operations security;
- Communications security;
- System acquisition, development and maintenance;
- Supplier relationships;
- Information security incident management;
- Information security aspects of business continuity management;
- Compliance.

6 Objectives and Principals of Information Security Policy

Information Security Policy presents the main **objectives** to ensure that all information assets have the required protection and specifies the control objectives that should be seen as a regulatory requirement. The objectives are applied independently of the locations and technologies used:

Objective 1:
Integrate Information Security in the business objectives of Mobileum Risk BU, as a distinguishable and competitive factor;

Objective 2:
Ensure compliance with industry and legal requirements in all countries where Mobileum Risk BU develops business;

Objective 3:
Ensure business continuity always keeping the highest levels of service quality;

Objective 4:
Promote within staff members a culture of responsibility and accountability for Information Security;

The implementation of top policies allows the coordination of all efforts, provides dynamism to the implementation of information security and, at the same time, optimizes resources and competences.

Information Security Policy is aligned with the nine **Principles** for the systems and networks Information Security defined by OECD (Organization for Economic Co-operation and Development).

The nine principles presented hereafter were created with the objective of promoting security among all the Participants and are complemented amongst themselves, so they should be considered as a whole. The principles are directed to the Participants of all levels (administrative and operational), and their responsibilities depend on their roles. All the Participants will benefit from awareness, education, share of information and training that leads to a better understanding of information security matters and the adoption of best practices in this domain.

The efforts to strengthen the systems security and the information networks should respect the values of a democratic society, especially the need of free and open circulation of information, as well as the **basic principles** of respect for the individuals' private life:

1) Awareness
All the Participants should understand the need of the existence of secure information networks and systems and their role in the maintenance and increase of security.

2) Responsibility
All the Participants should answer for the systems and network security.

3) Action
All Participants should act swiftly and cooperatively to prevent, detect and answer to security incidents.

4) Ethic
Each Participant should respect the interests of the other Participants.

5) Democracy
All Participants should make the security of the information systems compatible with the essential values of a democratic society.

6) Risk Evaluation
All Participants should regularly evaluate the risks of the systems and information networks.

7) Security Conception and Implementation
All Participants should incorporate security as an essential element of the systems and information networks.

8) Security Administration
Each Participant should manage security using a global approach that involves all Participants in a coordinated and integrated way.

9) Re-evaluation
All the Participants should re-evaluate and review the security of the systems and information networks and this re-evaluation can be an input to modify, adapt security policies, norms, procedures and manuals.

Based on this principles, Mobileum Risk BU draws up its technological evolution plan and ISMS Policy, that periodically is re-evaluated and adapted to external and internal conditions. Always aligned with ISMS objectives and with Mobileum Risk BU strategy.

6.1 Information Security Policy Framework

Mobileum Risk BU Information Security Policy is detailed in this Manual and belongs to the first Level of Mobileum Risk BU Documentary Model (Figure 1).
This Model has an increasing level of detail from top to bottom. The documentation associated to each level is in compliance with the higher level documentation and provides requirements and expectations for the objectives of the lower levels documentation.

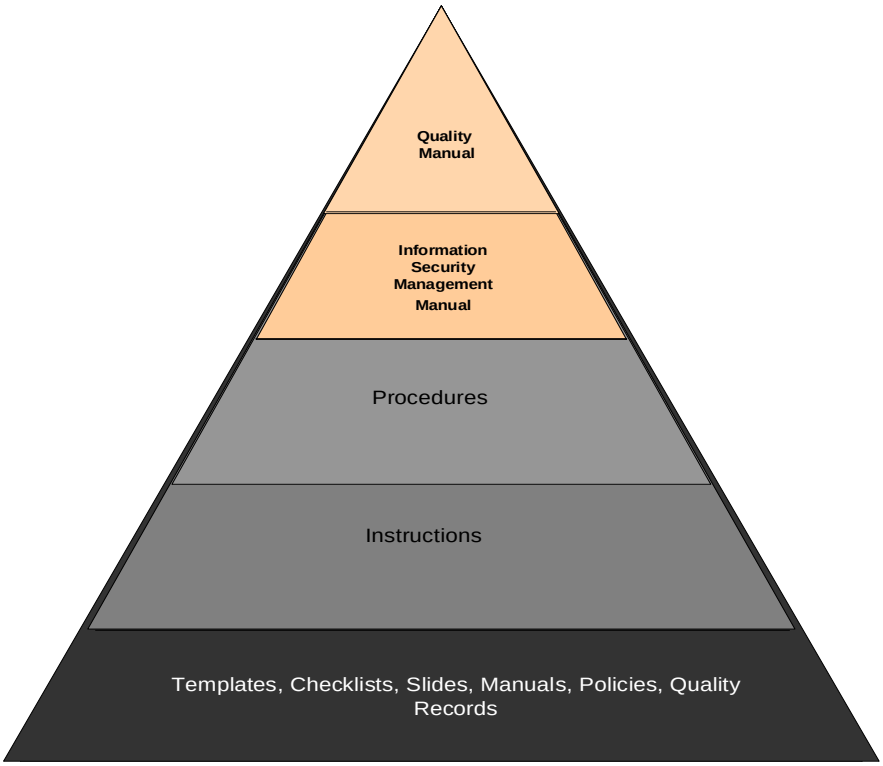


Figure 8 –Mobieum Risk BU ISMS Documentary Structure

The ISM system documentation is organized according to the above figure.

All documents are created, classified, revised, approved and published according to the layout of procedure *P_QMS_004_E – Document Management*.

Documentation supporting the company core business is written in English, whereas the support models are in both Portuguese and English. Internal instructions and activity support procedures can be found in Portuguese or English.

Standards and Procedures should be created addressing people, processes, technologies and organization. These documents should be viewed as guides to the implementation of the rules defined in the Information Security Policy. The development of these documents should be rigorous since they are specific for each asset and temporal implementation.

6.2 Information security Policy Guidance

The implementation and maintenance of the requirements of the Mobileum Risk BU Information Security Policy is guided by ISO/IEC 27001 Information security management systems (requirements) and practices of the security industry, namely the ISO/IEC 27002 – Code of practice for information security controls.

ISO/IEC 27001 Annex A, is distributed in 14 domains and it supports the implementation and maintenance plan, using key controls to guarantee conformity, to formulate documentation of policies, to distribute security responsibilities, to execute risk analyses and to define and implement security and access controls.

6.3 Information Security Policy Compliance

Non-compliance of what is in the rules and guidelines has serious consequences, which will be analyzed by Mobileum Risk BU Management, Human Resources and Legal Department.

Exceptions to ISMS rules must be analyzed by Mobileum Management.

6.4 Organizational roles and responsibilities

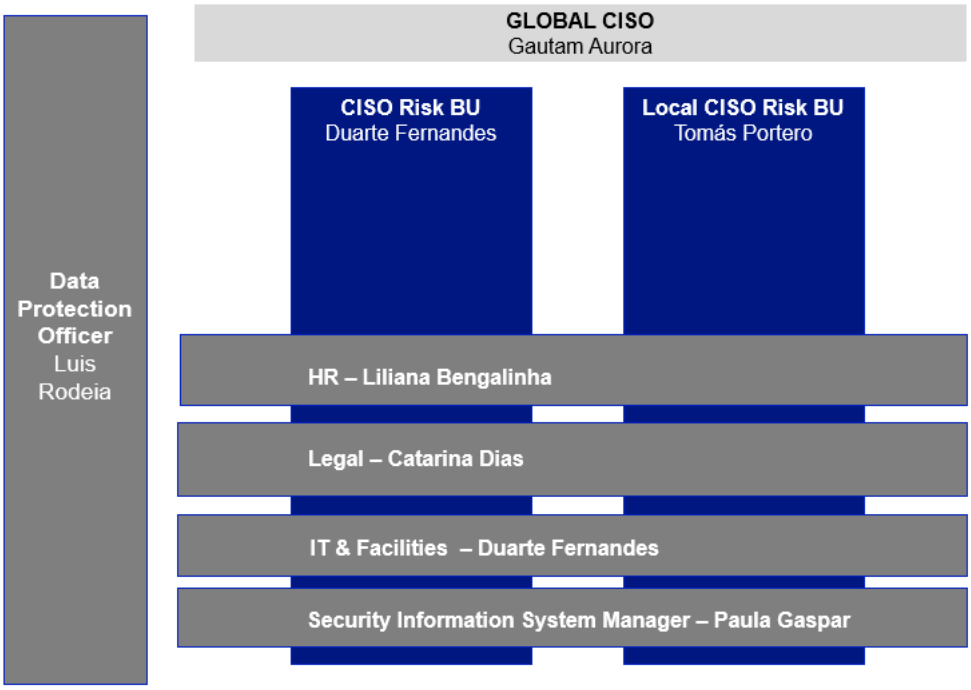


Figure 9 –ISMS Organization Model

Information Security has particular importance to Managed Services and Projects, systems and users of Mobileum Risk BU that handle with this scope. Information Security is not confined to one department or small group of people, it is, therefore, important to clearly define responsibilities that guarantee that all relevant and important aspects will be taken into account and that all tasks will be adequately fulfilled.

ISMS Objectives, Policy, Plan and procedures are completely aligned with Mobileum Risk BU Strategic Plan guidelines.

Mobileum Risk BU strategic Plan is defined within Management and Innovation & Security Process by Mobileum Risk BU Management.

The Management Commission deliberated that Information Security Management system is one of the concerns of Mobileum Risk BU, and has selected a team responsible for guaranteeing the maintenance and continuous improvement of the ISMS.

ISMS Organization Model consists in a Security Team (ISO 27001) with different roles:

-Chief Information Security Officer (CISO):

GLOBAL	- Mobileum Risk BU Management Level, direct report to CFO – Administrator, Member of Mobileum Risk BU Executive Commission; -Assures the Operational, Maintenance an improvement of the System; - Assures implementation of Training and awareness programs for all participants in ISMS; -Definition of Information Security policy; -Define and review all ISMS policies and procedures in order to protect the organization's digital assets, from information to infrastructure and more; - Management and direction of the information security team, namely the local CISO's and the transversal areas' representatives - Responsible for compliance (ISO27001); - Define ISMS security strategy aligned with the company strategy guidelines;
RISK BU CISO	- Mobileum Risk BU Experience or Senior Manager, Management level in a Mobileum Risk BU Business area; -Assures the Operational, Maintenance an improvement of the System; - Assures implementation of Training and awareness programs for all participants in ISMS; -Review and update Information Security policy; -Contributes and update policies and procedures to protect the organization's digital assets, from information to infrastructure and more; -Responsible for compliance (ISO27001); - Developing a complete strategy that covers prevention, detection, and response security incidents; -Coordinates the IT & facilities Mobileum Risk BU area completely aligned with ISMS Strategy;
LOCAL CISO	- Mobileum Risk BU Experience or Senior Manager, Management level in a Mobileum Risk BU Business area; -Assures the Operational, Maintenance an improvement of the System;

- Assures implementation of Training and awareness programs for all participants in ISMS;

-Review and update Information Security policy;

-Contributes and update policies and procedures to protect the organization's digital assets, from information to infrastructure and more;

-Responsible for compliance (ISO27001);

- Developing a complete strategy that covers prevention, detection, and response security incidents;

-Security System Manager:

- Mobileum Risk BU Manager, assures operation, maintenance, review, monitoring and improvement of the Security System;

-Assures that ISMS follows and applies ISO 27001 Policy guidelines;

-Elaborating and proposing to the Executive Commission security procedures to adopt in agreement with best practices and in accordance with the international policies and standards recognized in this domain;

-Advising the Executive Comission regarding the security of information.

-Management and measure of ISMS performance Indicators

- ISMS System Revision;

-Operation Team:

- Mobileum Risk BU Business area (ISMS scope) and transversal areas;

-Assures ISMS EN ISO 27001 compliance;

-Assures that ISMS follows and applies ISO 27001 Policy guidelines;

-Assures ISMS EN ISO 27001 compliance;

-Developing training and awareness programs for the Participants of ISMS;

-Feedback about Best practices in the Business;

Mobileum Risk BU has defined a career plan for its employees. A detailed description of each function's responsibilities can be found in instruction I_QMS_012_E – Job Descriptions. Both documents are published on the intranet and are accessible to all employees.

It is incumbent on the person responsible for Security Management to elaborate the ISMS plan, identify changes in the process, and ensure that the ISM system meets all the requirements of the EN ISO 27001 assuring its integration in Mobileum Risk BU Quality Management System.

The Security System Manager must guarantee the performance of internal audits and respective corrective measures.

Information management System belongs to Management & Innovation and Security Process in Mobileum Risk BU Quality Management System.

The Process owner is a Management commission member.

7 Planning

Information Security Management System (ISMS) can be obtained through the implementation of a number of security controls, such as policies, practices, processes, organizational structures and technological solutions. These controls can be set to ensure that Mobileum Risk BU Security Policy objectives are achieved already described in section 4.1 of this Manual.

In order to reach these objectives, described in the ISMS Policy, a Risk Management Methodology was conceived, and is revised with the aim of guaranteeing the fulfilment of the annually defined company objectives and the follow-up of the company's strategy, as well assures fulfillment of ISO 27001 Standard requirements.

The goal of Mobileum Risk BU Risk Assessment Methodology

- Determination the criteria for Risk acceptance;
- Identification of assets;
- Identification of Vulnerabilities and threats;
- Evaluation the size of Risks;
- Identification and assessment of Risks treatment options;
- Selection of controls for Risk management;
- Identification Management approval for residual Risks;

8 ISMS Support

8.1 ISMS Resources

The main goal of Mobileum Risk BU is the constant improvement and optimization of the Information managements System and to accomplish this goal we have full commitment of Mobileum Risk BU Top Management.

Mobileum Risk BU Executive Management Commission provided and approved all necessary Human, Technological and Financial resources for the establishment, implementation, maintenance and continual improvement of the Information Security Management System.

The annual resource plan per business unit results from the strategic planning cycle.

The selection and recruitment of new employees are carried out in accordance with the content of procedure P_QMS_008_E – Hiring and Selection.

The integration of new employees is carried out in accordance with the content of procedure P_QMS_007_E- New Hires Integration.

8.2 Competence & Awareness

In order to fulfill Information Security Policy, following ISMS Policy objectives and guidelines, a Training program was established before the creation of ISMS organization Model:
Mobileum Risk BU trained most of the team in order to have the largest number of people Certified by IRCA - The International Register of Certificated Auditors – has Information Security Management Systems Lead Auditors. The goal is to provide skills in order to optimize most as possible Information Security performance.
The rest of the team was trained by an external company expert in Information Security training, to guarantee a level of knowledge commensurate with the challenges and opportunities to be faced.

The updating and management of skills is carried out in accordance with procedure P_QMS_015_E – Skills Management.

The identification of training needs is carried out during performance appraisal, as described in procedure P_QMS_022_E – Performance Appraisal.

The elaboration of the annual training plan results from the consolidation of the information obtained in relation to each employee's individual performance.

The activities of training management and the gathering and processing of appraisal results from training sessions are described in P_QMS_006_E – Internal Training.

Registers of training sessions are stored by HR. The register of the training sessions attended by each employee is maintained and managed by the person in human resources responsible for training.

Concerns with the identification and adaptation of the employees' skills to Mobileum's Risk BU business begins with the process of selection and recruitment of new employees, and continues after they have joined the company, through a continuous training process which is described in procedure P_QMS_006_E – Internal Training.

Training is an instrument for garnering and to retain Talent in the company, annually Mobileum Risk BU Training Plan is approved by Mobileum Management and is published in Mobileum Risk BU intranet available to all employees.

Mobileum Risk BU trainings are provided to the persons within the security scope, giving awareness of ISMS Policy, rules and guidelines with the goal of involving all employees, in information Security Management System, also to clarify the importance of their contribution to the effectiveness of ISMS, including the benefits of an improved Information Security performance:

1) Security Training

   Owner: ISM Security System Management Team

   Distribution List: ISMS scope (Managed Services)

This Training has also the objective of warning that all people have an active and important role in ISMS.

8.3 Communication

ISMS documentation is classified following P_QMS_004_E- Document Management, that establishes what and to who should be communicated.

Responsibilities and roles are completely identified and communicated in this Manual –section 6.4–and available internally thru intranet to all employees.

This manual can and should be used by Customers, Suppliers, Partners, Employees and other stakeholders as evidence that the ISMS is structured and implemented in order to assure that ISMS policy and goals are established, implemented and measured every year.

8.4 Social Media

Mobileum Risk BU believes that his presence in the social media is essential and acknowledges the importance of its employees, partners and suppliers and shareholders as active players of a global information society.
The principles described below aim to guide Mobileum Risk BU employees and partners, suppliers, shareholders, with the intended conduct when performing in a professional context or when representing Mobileum Risk BU.
Mobileum Risk BU seeks to ensure its good reputation without jeopardizing its employees, partners, suppliers, shareholders, etc., right to freedom in the personal sphere.

Mobileum Risk BU believes that the best way for its employees and external parties to be in the virtual world is to follow the principles that guide them in real life-wise judgment and good common sense, living company values and following Conduct Code guidelines and all other applicable policies.

For the purpose of this Manual, Social Media is Technology and Sites that require and involve the discussion and publication of contents, namely: Blogging, micrologging (e,g.twitter), video sharing (You Tube, Vimeo), networking (Facebook, Linkedin).

8.5 Fundamental principles for Mobileum Risk BU presence in Social Media

Transparency
Transparency is a Mobileum Risk BU value. Mobileum Risk BU defends a transparent attitude in the Social Media and doesn't recommend the manipulation of information; nor the deception of followers through "fake" destinations or posts designed.
The company must ensure that it clearly identifies its own brand's Websites;

Safeguarding Privacy

Safeguarding privacy of customers, partners, etc, must be compliant with privacy and data protection policies, applicable laws and information security policies (P_QMS_004_E-Document Management);

Respect for copyrights, trademarks, advertising rights and third-party parties
This guarantee in Social Media depends on each case, so Legal coordination is required to ensure well informed and appropriated decision-making;

Use of best practices
Listen to the online community and act according to the applicable good practices, in order to ensure that the social network principles reflect the most updated and appropriate behavior standards;

These Fundamentals guidelines are part of the ISMS training content delivered to all Mobileum Risk BU employees.

8.6 ISMS documented Information

ISMS is completely integrated in Quality Management System as described in this Manual – Section 4.4- Creation, reviewing, approving, publishing, archiving and extinguish rules of ISMS documentation is described in P_QMS_004_E-Document Management.

The way to generates codes and names for all information items that need to be stored electronically, like software, project documentation, quality related documents, etc., is described in I_QMS_001_E-Convention Names.

9 Performance evaluation

9.1 Monitoring, measurement analysis and evaluation

As described in section 6.4 of this Manual, the ISMS Security Manager activities are related with monitoring, measurement of ISMS:

It is incumbent on the person responsible for Security Management to elaborate the ISMS plan, identify changes in the process, ISMS annual Revision and ensure that the ISM system meets all the requirements of the NP EN ISO 27001 assuring its integration in Mobileum Risk BU Quality Management System.

The Security System Manager must guarantee the performance of internal audits and respective corrective measures, evaluates the effectiveness of the Information Security Management System In the annual ISMS Revision.

ISMS Key Performance Indicators are documented in P_QMS_034_E-Measuring Analysis and Improvement and monitored in T_QMS_442_E - ISMS Security Metrics and Goals.

9.2 Internal audit

Internal audits are carried out with the frequency defined in the ISMS plan and in accordance with procedure P_QMS_013_E – Quality Audits.
Internal audit results are processed in accordance with the layout of procedure P_QMS_017_E – Corrective and Preventive Actions.

9.3 Management Review

In order to assure ISMS continuing suitability, adequacy and effectiveness the ISMS plan should be updated and reviewed annually.
Information Security Policy should be reviewed by Executive Commission in order to guarantee is compliance with Mobileum Risk BU Strategic Plan.

The annual revision of the Information Security Management System can be triggered by one of the following events (inputs):

- Changes in company strategy

- Changes in ISMS Policy
- Review of the supply of products and services
- Interface Management analysis;
- Regulators and external environment;
- Customer Feedback analysis;
- ISMS Analysis & management :

  -Internal Audits results (P_QMS_013_E – Quality Audit, P_QMS_017_E – Corrective and Preventive Actions);

  -Results from Mobileum Risk BU Management System analysis – ISMS Management System Revision;

ISMS system revision is made by the Security Information Manager in order to analyse the essential key points for Strategic Plan Cycle of the company.

Information Security Management System review is presented and approved by Mobileum Risk BU Management commission.

As outputs of the ISMS System review is considered:

- Actions to be implemented with the aim of improving the effectiveness of ISMS Management System;
- Possible need for Human resources, financial or technology resources to ensure the adequacy of the ISM System to the Company practice and adequacy with the NP EN ISO 27001 standard;
- Changes in Policies, goals, key performance indicators, processes or other elements associated with the implemented ISM system;

10 Improvement

10.1 Non conformity, Corrective and Preventive actions

Non Conformities, Corrective and Preventive actions are identified and implemented in accordance with the layout of procedure P_QMS_017_E – Corrective and Preventive Action.

10.2 Continual Improvement

Mobileum Risk BU strives to continuously improve the efficacy of its ISMS system through the use of the ISMS policy, the performance analysis of the company KPI, audit results, the analysis of relevant data, corrective and preventive actions and through management revision.

11 Annex A

Information Security Management Policy

As described in P_QMS_053_E – Information Security, Privacy and Personal Data Protection Policy

Information is one of the most critical assets of an organization. With the generalization of information technologies and, in particular, of the Internet the volume of digital information has been increasing in an exponentially way over the last years.

The protection of information is therefore of vital importance, so that the trust among the several business partners may be maintained and solidified.

The availability, integrity and confidentiality of information, in a rigorous and expedite way, to support business decisions has become a competitive advantage for organizations.

If the information of an organization, including Personal Data, is disclosed, manipulated or made unavailable, the consequences can be serious and create an impact in the organization´s reputation and performance.

Mobileum Risk BU top management is committed to maintain the continual improvement of the information security management system. The information security should be monitored as a dynamic process, so that it is possible to predict and react to information security threats.

Information Security Policy can be defined as the preservation of:

1. Confidentiality: assure that information is accessible to authorized personnel only;
2. Integrity: safeguard the correctness and completeness of information and processing methods;
3. Availability: assure that authorized users have access to information and associated assets when required.

Mobileum Risk BU defined four objectives to ensure that all information assets have the required protection and specifies the control objectives that should be seen as a regulatory requirement:

Objective 1:
Integrate Information Security in the business objectives of Mobileum Risk BU, as a distinguishable and competitive factor;

Objective 2:
Ensure compliance with industry and legal requirements in all countries where Mobileum Risk BU develops business;

Objective 3:
Ensure business continuity always keeping the highest levels of service quality;

Objective 4:
Promote within staff members a culture of responsibility and accountability for Information Security;

Mobileum Risk BU follows security best practices as defined in the General Data Protection Regulation. This Security Policy applies to Mobileum Risk BU, in all of its organization. Therefore, Mobileum Risk BU defined a general set of policies, which assures information security, including personal data:

- Backups Policy;
- Acceptable Use of Assets;
- Cryptography;
- Information Transfer;
- Clear Desk and Screen Policy;
- Passwords Policy;
- IT_Helpdesk_Facilities_Policy;
- Mobileum Risk BU Site Data Protection, Privacy and Cookies Policy.

Mobileum Risk BU is ISO 27001 certified for a subset of our services, which scope is:
The Information Security System for Managed Services Process related with Madrid Office.

The implementation and maintenance of the requirements of the Mobileum Risk BU Information Security Policy is guided by ISO/IEC 27001 Information security management systems (requirements) and practices of the security industry, namely the ISO/IEC 27002 – Code of practice for information security controls **for ISO 27001 certified scope**.

Mobileum Risk BU Information Security in ISO 27001 scope is covered through 14 domains (Security Policy; Organization of Information Security; Human Resources Security; Asset Management; Access Control; Cryptography; Physical and environmental security; Operations security; Communications security; System acquisition, development and maintenance; Supplier relationships; Information security incident management; Information security aspects of business continuity management; Compliance) and it supports the implementation and maintenance plan, using key

controls to guarantee conformity, to formulate documentation of policies, to distribute security responsibilities, to execute risk analyses and to define and implement security and access controls.

Privacy and Personal Data Protection Policy

The protection of privacy and personal data of all persons who somehow relate to Mobileum Risk BU (clients, users of the services, employees, partners and others) is a fundamental commitment of our Company.
Personal data is essential for the activity of Mobileum Risk BU, in particular, for the marketing of its products and services, for the provision, monitoring and improvement of the quality of the services made available by Mobileum Risk BU, for the management of Mobileum's Risk BU human resources and for the fulfilment of legal obligations, with the challenges that are associated to the processing of personal data for the said purposes being very strongly influenced by the technological, economic and social developments.

Our commitment is to work every day in order to ensure the privacy and protection of personal data for which we are responsible in compliance with the applicable legislation, regulations and guidelines on such matters.

This commitment is executed, namely, by the adoption and implementation of policies and standards of privacy, including, for that purpose, the Privacy Policy of the Company, as well as our Information Security Policy.

In order to better carry out our commitment, we have appointed a Data Protection Officer (DPO), which is responsible for advising Mobileum Risk BU, monitoring Mobileum's Risk BU compliance of the personal data processing with the said policies and standards, as well as applicable law, and is the point of contact for the Data Subject and the relevant Supervisory Authority.
In addition, Mobileum Risk BU have a security team within the organization responsible for, among other aspects, the maintenance, development and supervision of information security, policies and standards, as well as security awareness through training and communication.
With this Statement of Commitment, we want to make clear Mobileum's Risk BU commitment to privacy, security and personal data protection and ensure that all those processing personal data under their relationship with Mobileum Risk BU are bound and act in accordance with the underlying principles.

Personal Data Processing Principles and Data Subjects Rights

The processing of personal data by our Company complies with the following fundamental principles:

- Lawfulness principle
- Purpose limitation principle
- Transparency principle
- Adequacy and data minimisation principle
- Need to know principle
- Integrity and confidentiality principle
- Privacy by design and by default principle

In addition to complying with the said applicable principles, Mobileum Risk BU is committed to ensure the respect of Data Subjects rights, in particular, the right of access and information to personal data being processed by Mobileum Risk BU, the right to rectification, the right to erasure ("right to be

forgotten"), the right to data portability, the right to restriction of processing, the right to withdraw consent, the right to object, the right not to be subject to a decision based solely on automated processing, including profiling, and the right to lodge a complaint.

A) Lawfulness principle

The personal data will be processed only if and to the extent that it is grounded on one of the conditions laid down for lawfulness, namely (i) when consent is given by the Data Subject or when the processing is necessary for (ii) the performance of a contract to which the Data Subject is a party, (iii) compliance with a legal obligation, or (iv) the purposes of the legitimate interests pursued by Mobileum Risk BU or by a third party.

B) Purpose limitation principle

The personal data will be processed exclusively for the purposes that determined its collection and will only be processed when legally permitted and by providing the due information to the corresponding Data Subject.

C) Transparency principle

Data subjects will be informed in a clear and concise way of the relevant aspects related to the processing of their personal data, namely, regarding the processing purposes and possible transmission to third parties.

D) Adequacy and data minimisation principle

Only personal data that is adequate, relevant and limited to the necessary personal data for the relevant purposes will be processed and for the time strictly necessary.

E) Need to know principle

Only employees and partners of Mobileum Risk BU whose functions require it will have access to the relevant personal data processed.

F) Integrity and confidentiality principle

The personal data will be processed in such a way as to guarantee its security, namely, (i) protected against unlawful or unauthorized access or disclosure, (ii) protected against unauthorized modification, loss or destruction of personal data or accidental loss of such personal data, and (iii) ensured that personal data will be available when necessary and permitted, without undue delay.

G) Privacy by design and by default principle

Mobileum's Risk BU products and services, their support systems, and their procedures will be developed with the concern of protecting your privacy and personal data.

Personal Data Protection

Mobileum Risk BU respects best practices in the field of protection of personal data and information, and has adopted a program of policies and standards to ensure confidentiality, integrity and availability of the information it is dealing with and that is under its responsibility, which is known to all employees and partners of Mobileum Risk BU.

Mobileum's Risk BU Information Security Policy establishes a wide range of set of technical and organizational measures, organized in several security areas, including:

(i) **Logical security measures**, such as the use of firewalls and detection of intrusion, the existence of a policy of access to information and logging;

(ii) **Physical/organizational security measures**, among which a strict access control to the physical installations of our Company, by employees, partners and visitors, as well as very restricted access, permanently monitored, to the essential technological infrastructures of our Company;

(iii) **Other measures** such as masking, encryption, pseudonymization and anonymization of personal data, as well as a set of measures which aim to execute the principle of privacy by design and by default. Where Mobileum Risk BU uses subcontractors or third parties, Mobileum Risk BU will assure that its subcontractors and third parties are be bound by obligations in order to comply with the applicable legislation and security measures considered necessary by Mobileum Risk BU for the relevant purposes, as well as to ensure that: (i) the sharing of personal data obeys the applicable laws as amended from time to time, (ii) the transmission is securely made, and that (iii) the subcontractors or third parties are contractually obliged to observe confidentiality duties and to ensure the security of personal data, which, to that end, may be transmitted to them, with the restriction not to be able to use such data for any other purpose, for their own benefit or that of third parties, nor to correlate them with other data that is in the said subcontractors and third parties possession.

Compliance with information security policies, security standards and protection of personal data is subject to periodical scrutiny, audit and control, complemented by a demanding program of information and training of Mobileum's Risk BU employees and partners.