mobileum

Action driven by intelligence

Information Security Management Manual

Risk BU

Document Version: 23.0

Date: 31-10-2024

The information in this document shall not be disclosed outside your organization, and shall not be duplicated, used, or disclosed in whole or in part for any purpose without prior written permission from Mobileum, Inc.

Mobileum, Inc.
20813 Stevens Creek Boulevard, Ste. 200
Cupertino, CA 95014

United States of America (USA)
Phone: +1-408-844-6600
Fax: +1-408-252-1566
www.mobileum.com

Legal Information

Revision History

Date	Version	Author	Owner	Remarks
25-Jun-2014	1.0	Paula Gaspar		First Version
11-Sep-2014	2.0	Paula Gaspar		Second Version : update Information Security Policy Compliance
23-Jan-2015	3.0	Paula Gaspar		Update footer
20-Feb-2015	4.0	Paula Gaspar		Update relation between ISO 9001 and 27001
05-Aug-2015	5.0	Paula Gaspar		ISMS Team update, ISO 27001:2013 Certification update
30-Dec-2015	6.0	Paula Gaspar		Update RH Responsible
18-Jan-2016	7.0	Paula Gaspar		Update WeDo Global Organization and WeDo Shareholder, update Figure 1 – WeDo Interface Management Model. Business Continuity Corporate Procedure updated.
25-Jan-2016	8.0	Paula Gaspar		*Competence and Awareness updated*
07-Sep-2016	9.0	Luis Rodeia / Paula Gaspar		Inclusion Annex A – ISMS Policy
14-Dec-2016	10.0	Paula Gaspar		Update Annex A – Information Security Management Policy
21-Nov-2017	11.0	Paula Gaspar		New WeDo signature replacement
28-May-2018	12.0	Paula Gaspar / Luis Rodeia		ISMS Security team update
31-May-2018	13.0	Paula Gaspar / Luis Rodeia		Global update, Managed Services Madrid and Saas Cloud inclusion
06-Aug-2018	14.0	Paula Gaspar / Luis Rodeia		Annex A updated - Privacy and Personal Data Protection Policy
18-Feb-2019	15.0	Paula Gaspar		Organization structure & Security Governance Model update
24-Sep-2019	16.0	Cristina Pires		Updated with the new WeDo brand and corporate content.
14-May-2020	17.0	Lígia Sousa Marçal		Updated with Mobileum brand and corporate content.

19-Jun-2020	18.0	Paula Gaspar/ Daniela Nunes		General revision and update WeDo to Mobileum Risk BU.
18-Jun-2021	19.0	Paula Gaspar		Update Scope (out of scope SaS Cloud)
14-Oct-2022	20.0	Paula Gaspar		General revision and update, Update ISMS Scope, ISMS Security team
10-Nov-2023	21.0	Paula Gaspar		General revision and update
15-Dec-2023	22.0	Paula Gaspar	Compliance	Risk BU organization Chart Update
31-Oct-2024	23.0	Paula Gaspar	Compliance	General revision and update.

Table of Contents

Table of Figures

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 cost optimization. However, there are also associated risks, 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 to make security an integral part of Mobileum Risk BU organization and its Information, Communications and Technologies.

ISO/IEC 27001 -Information security management systems follow 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
- Information Technology
- Human resources
- Project Management ,etc.

1.1 Goal of Information Security Management System Manual

Information Security Management System is applied to Mobileum Risk BU Business activities: Managed Services and correspondent transversal areas, such as Information Technologies, Human Resources, Legal , etc.

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;
- Evidence that the Information Security Management System Policy is 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 to ensure 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.

Definitions/Acronyms

AOP	Annual Organization Planning
CCO	Chief Compliance Officer

CFO	Chief Financial Officer
CMO	Chief marketing Officer
HR	Human resources
ISMS	Information Security Management System
ISP	Information Security Policy
PDCA	Plan, Do, Check, Act
QMS	Quality Management System

Concepts Definition

QMS — Quality management System (QMS) can be expressed as the organizational structure, procedures, processes and resources needed to implement a Quality Management. QMS is integrated in the Mobileum Compliance Department.

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

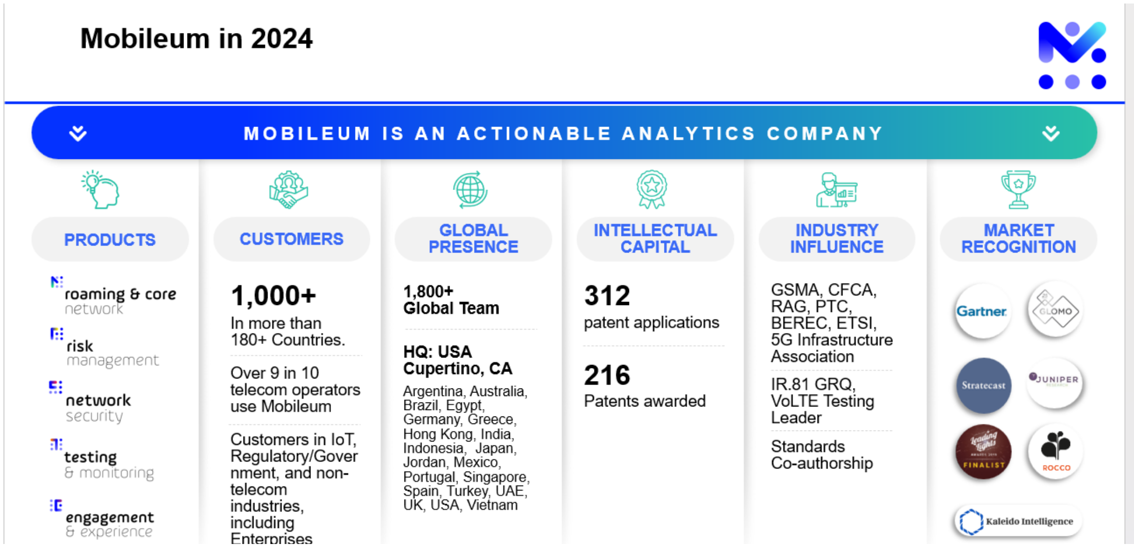
Action driven by Intelligence…

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 Mobileum Inc on Twitter.

2.1 Fast Facts

Mobileum is a GLOBAL Market leader in several areas



Mobileum in 2024

MOBILEUM IS AN ACTIONABLE ANALYTICS COMPANY

PRODUCTS

roaming & core network

risk management

network security

testing & monitoring

engagement & experience

CUSTOMERS

1,000+
In more than 180+ Countries.

Over 9 in 10 telecom operators use Mobileum

Customers in IoT, Regulatory/Government, and non-telecom industries, including Enterprises

GLOBAL PRESENCE

1,800+ Global Team

HQ: USA Cupertino, CA

Argentina, Australia, Brazil, Egypt, Germany, Greece, Hong Kong, India, Indonesia, Japan, Jordan, Mexico, Portugal, Singapore, Spain, Turkey, UAE, UK, USA, Vietnam

INTELLECTUAL CAPITAL

312
patent applications

216
Patents awarded

INDUSTRY INFLUENCE

GSMA, CFCA, RAG, PTC, BEREC, ETSI, 5G Infrastructure Association

IR.81 GRQ, VoLTE Testing Leader

Standards Co-authorship

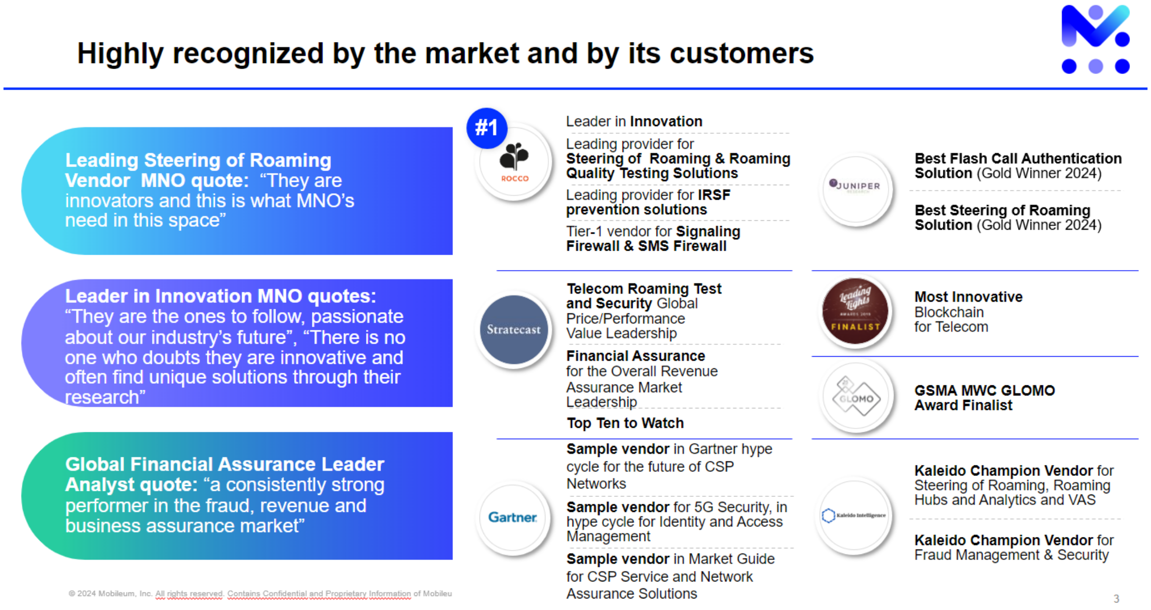
MARKET RECOGNITION

Customer References

A global footprint of 1,000 + customers

Customer Testimonials

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



Highly recognized by the market and by its customers

Leading Steering of Roaming Vendor MNO quote: "They are innovators and this is what MNO's need in this space"

Leader in Innovation MNO quotes: "They are the ones to follow, passionate about our industry's future", "There is no one who doubts they are innovative and often find unique solutions through their research"

Global Financial Assurance Leader Analyst quote: "a consistently strong performer in the fraud, revenue and business assurance market"

#1

Leader in **Innovation**

Leading provider for **Steering of Roaming & Roaming Quality Testing Solutions**

Leading provider for **IRSF prevention solutions**

Tier-1 vendor for **Signaling Firewall & SMS Firewall**

Telecom Roaming Test and Security Global Price/Performance Value Leadership

Financial Assurance for the Overall Revenue Assurance Market Leadership

Top Ten to Watch

Sample vendor in Gartner hype cycle for the future of CSP Networks

Sample vendor for 5G Security, in hype cycle for Identity and Access Management

Sample vendor in Market Guide for CSP Service and Network Assurance Solutions

Best Flash Call Authentication Solution (Gold Winner 2024)

Best Steering of Roaming Solution (Gold Winner 2024)

Most Innovative Blockchain for Telecom

GSMA MWC GLOMO Award Finalist

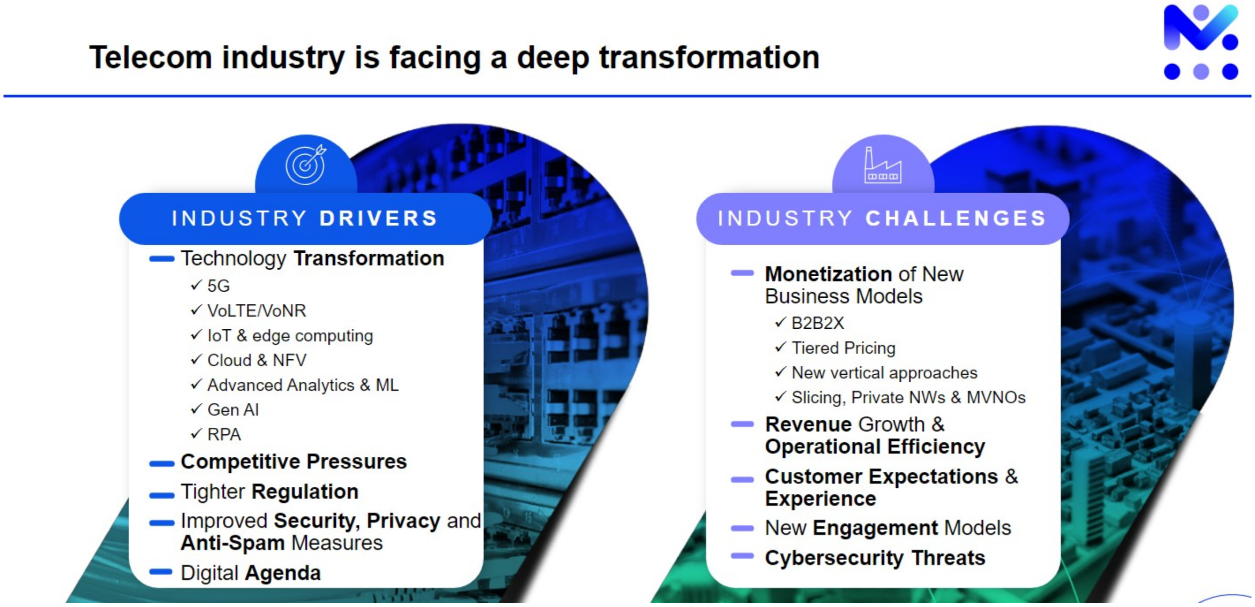
Kaleido Champion Vendor for Steering of Roaming, Roaming Hubs and Analytics and VAS

Kaleido Champion Vendor for Fraud Management & Security

© 2024 Mobileum, Inc. All rights reserved. Contains Confidential and Proprietary Information of Mobileu

3

Company Overview



Telecom industry is facing a deep transformation

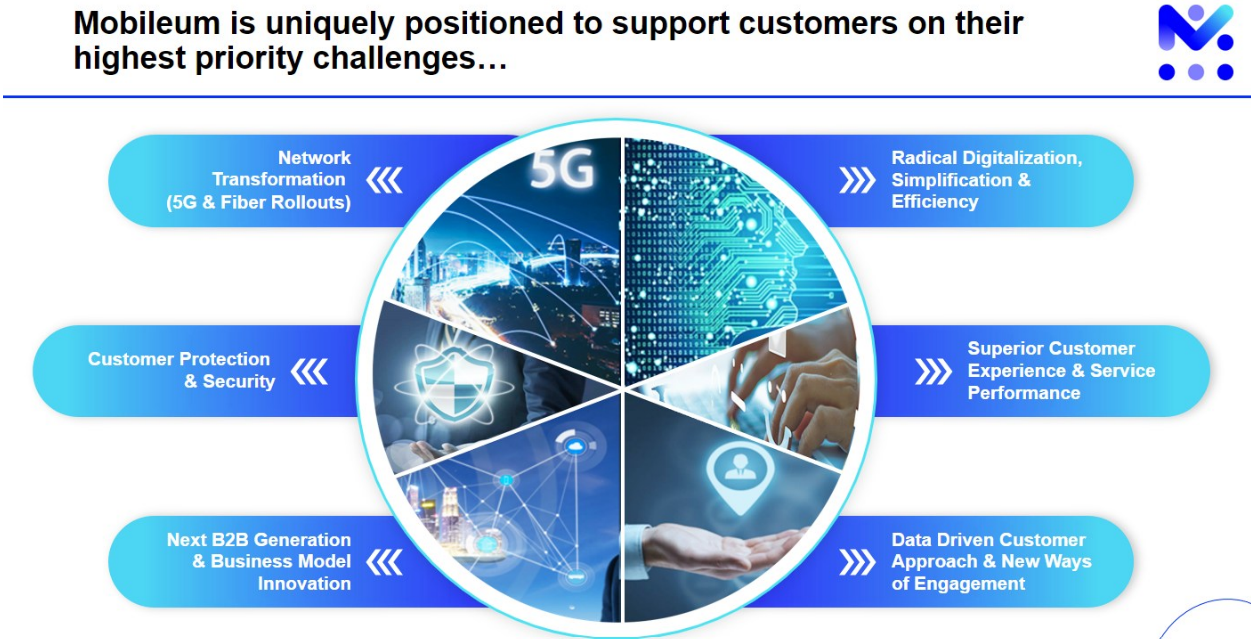
INDUSTRY DRIVERS

- Technology **Transformation**
  - ✓ 5G
  - ✓ VoLTE/VoNR
  - ✓ IoT & edge computing
  - ✓ Cloud & NFV
  - ✓ Advanced Analytics & ML
  - ✓ Gen AI
  - ✓ RPA
- **Competitive Pressures**
- Tighter **Regulation**
- Improved **Security, Privacy** and **Anti-Spam** Measures
- Digital **Agenda**

INDUSTRY CHALLENGES

- **Monetization** of New Business Models
  - ✓ B2B2X
  - ✓ Tiered Pricing
  - ✓ New vertical approaches
  - ✓ Slicing, Private NWs & MVNOs
- **Revenue** Growth & **Operational Efficiency**
- **Customer Expectations** & **Experience**
- New **Engagement** Models
- **Cybersecurity Threats**

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



Mobileum is uniquely positioned to support customers on their highest priority challenges…

Network Transformation (5G & Fiber Rollouts) «

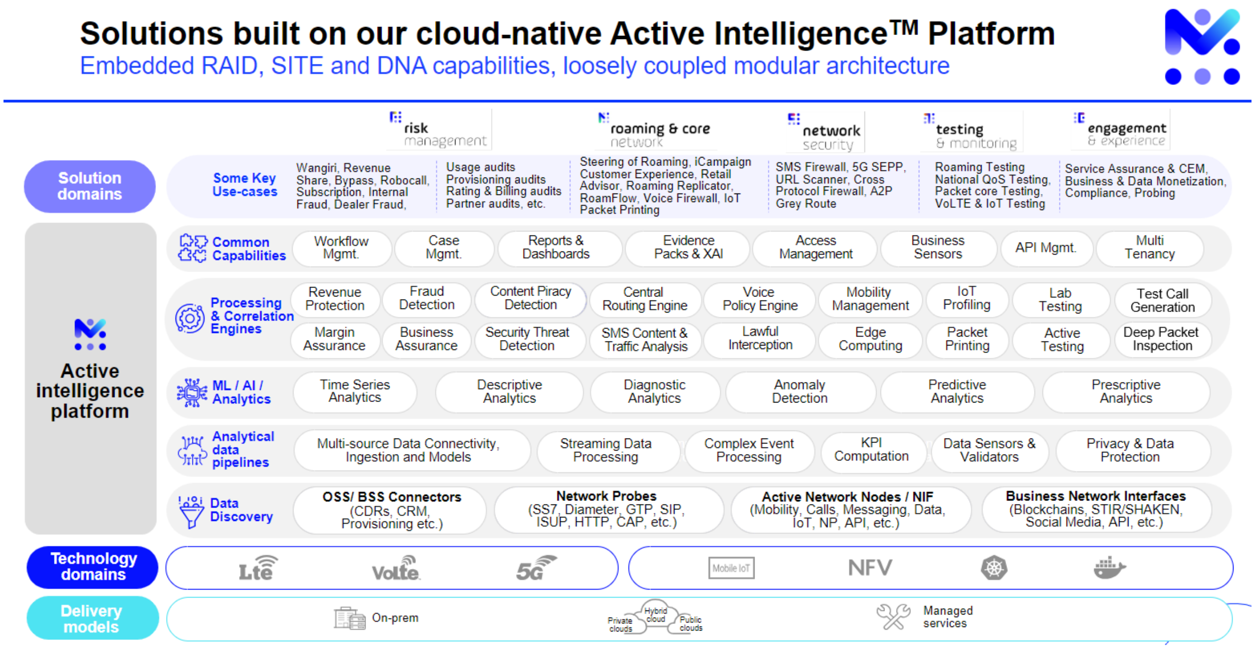
» **Radical Digitalization, Simplification & Efficiency**

Customer Protection & Security «

» **Superior Customer Experience & Service Performance**

Next B2B Generation & Business Model Innovation «

» **Data Driven Customer Approach & New Ways of Engagement**



Solutions built on our cloud-native Active Intelligence™ Platform

Embedded RAID, SITE and DNA capabilities, loosely coupled modular architecture

	risk management		roaming & core network	network security	testing & monitoring	engagement & experience
Solution domains — Some Key Use-cases	Wangiri, Revenue Share, Bypass, Robocall, Subscription, Internal Fraud, Dealer Fraud,	Usage audits Provisioning audits Rating & Billing audits Partner audits, etc.	Steering of Roaming, iCampaign Customer Experience, Retail Advisor, Roaming Replicator, RoamFlow, Voice Firewall, IoT Packet Printing	SMS Firewall, 5G SEPP, URL Scanner, Cross Protocol Firewall, A2P Grey Route	Roaming Testing National QoS Testing, Packet core Testing, VoLTE & IoT Testing	Service Assurance & CEM, Business & Data Monetization, Compliance, Probing

Active intelligence platform

Common Capabilities: Workflow Mgmt. · Case Mgmt. · Reports & Dashboards · Evidence Packs & XAI · Access Management · Business Sensors · API Mgmt. · Multi Tenancy

Processing & Correlation Engines: Revenue Protection · Fraud Detection · Content Piracy Detection · Central Routing Engine · Voice Policy Engine · Mobility Management · IoT Profiling · Lab Testing · Test Call Generation · Margin Assurance · Business Assurance · Security Threat Detection · SMS Content & Traffic Analysis · Lawful Interception · Edge Computing · Packet Printing · Active Testing · Deep Packet Inspection

ML / AI / Analytics: Time Series Analytics · Descriptive Analytics · Diagnostic Analytics · Anomaly Detection · Predictive Analytics · Prescriptive Analytics

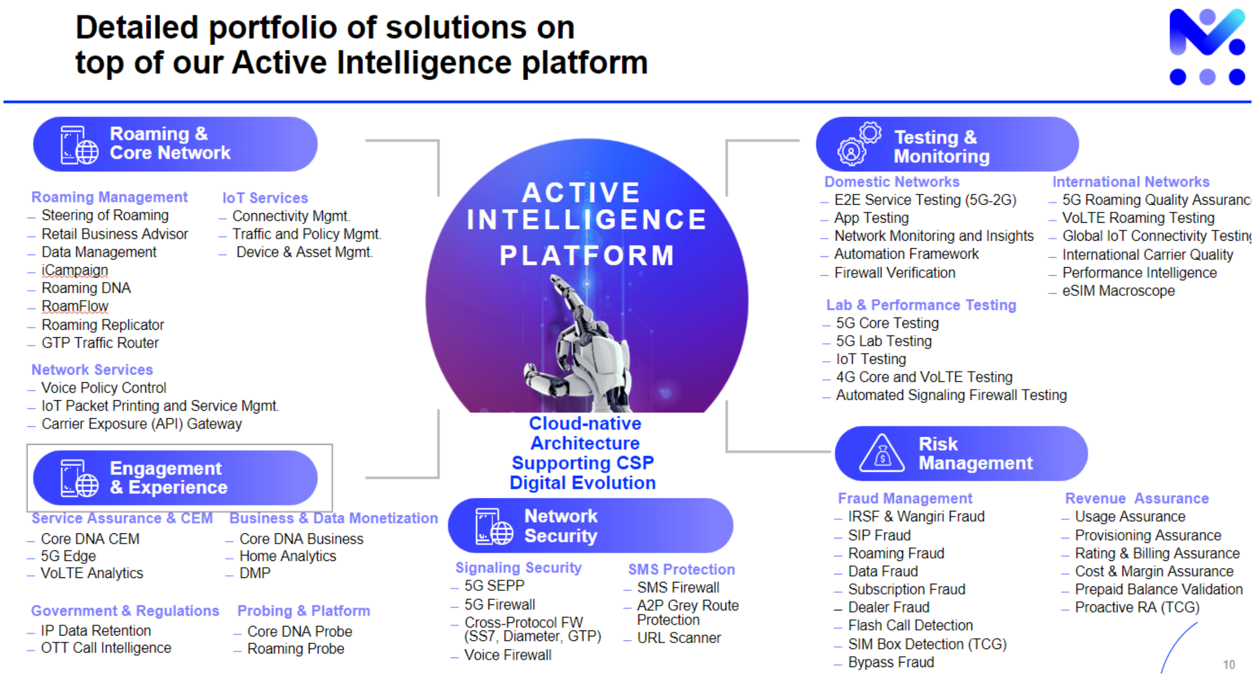
Analytical data pipelines: Multi-source Data Connectivity, Ingestion and Models · Streaming Data Processing · Complex Event Processing · KPI Computation · Data Sensors & Validators · Privacy & Data Protection

Data Discovery: **OSS/ BSS Connectors** (CDRs, CRM, Provisioning etc.) · **Network Probes** (SS7, Diameter, GTP, SIP, ISUP, HTTP, CAP, etc.) · **Active Network Nodes / NIF** (Mobility, Calls, Messaging, Data, IoT, NP, API, etc.) · **Business Network Interfaces** (Blockchains, STIR/SHAKEN, Social Media, API, etc.)

Technology domains: Lte · VoLte · 5G · Mobile IoT · NFV

Delivery models: On-prem · Private clouds · Hybrid cloud · Public clouds · Managed services

Lines of Business (LOB)



Detailed portfolio of solutions on top of our Active Intelligence platform

ACTIVE INTELLIGENCE PLATFORM

Cloud-native Architecture Supporting CSP Digital Evolution

Roaming & Core Network

Roaming Management
- Steering of Roaming
- Retail Business Advisor
- Data Management
- iCampaign
- Roaming DNA
- RoamFlow
- Roaming Replicator
- GTP Traffic Router

IoT Services
- Connectivity Mgmt.
- Traffic and Policy Mgmt.
- Device & Asset Mgmt.

Network Services
- Voice Policy Control
- IoT Packet Printing and Service Mgmt.
- Carrier Exposure (API) Gateway

Engagement & Experience

Service Assurance & CEM
- Core DNA CEM
- 5G Edge
- VoLTE Analytics

Business & Data Monetization
- Core DNA Business
- Home Analytics
- DMP

Government & Regulations
- IP Data Retention
- OTT Call Intelligence

Probing & Platform
- Core DNA Probe
- Roaming Probe

Network Security

Signaling Security
- 5G SEPP
- 5G Firewall
- Cross-Protocol FW (SS7, Diameter, GTP)
- Voice Firewall

SMS Protection
- SMS Firewall
- A2P Grey Route Protection
- URL Scanner

Testing & Monitoring

Domestic Networks
- E2E Service Testing (5G-2G)
- App Testing
- Network Monitoring and Insights
- Automation Framework
- Firewall Verification

International Networks
- 5G Roaming Quality Assuranc
- VoLTE Roaming Testing
- Global IoT Connectivity Testin
- International Carrier Quality
- Performance Intelligence
- eSIM Macroscope

Lab & Performance Testing
- 5G Core Testing
- 5G Lab Testing
- IoT Testing
- 4G Core and VoLTE Testing
- Automated Signaling Firewall Testing

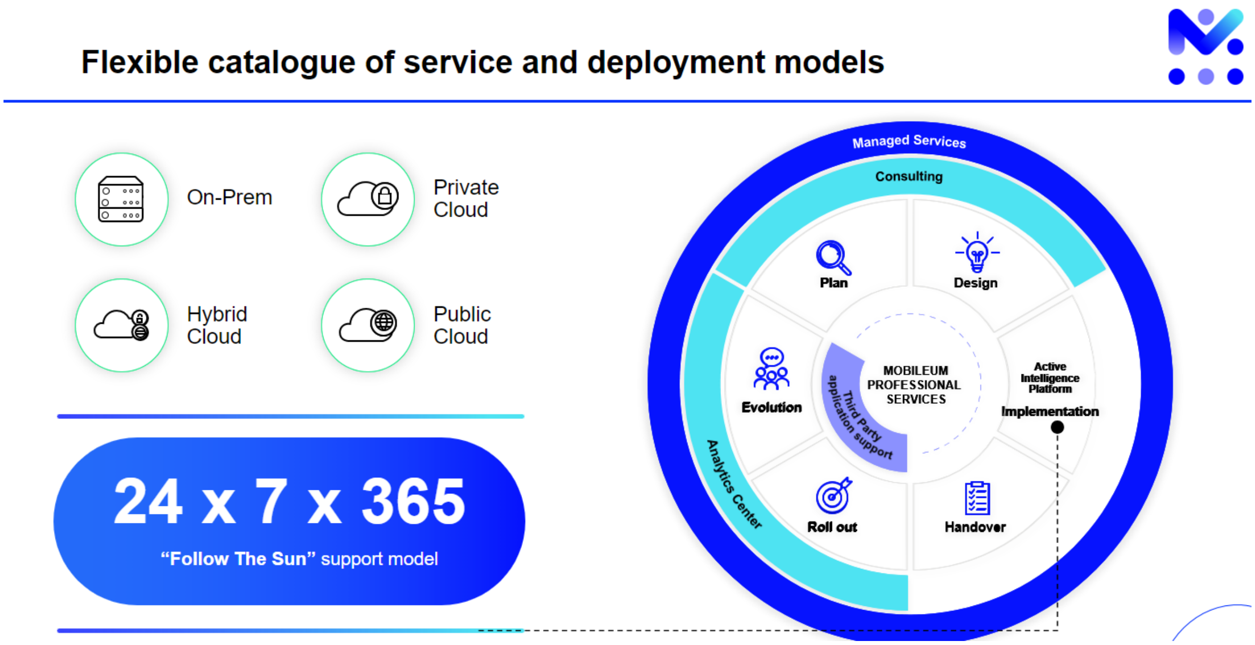
Risk Management

Fraud Management
- IRSF & Wangiri Fraud
- SIP Fraud
- Roaming Fraud
- Data Fraud
- Subscription Fraud
- Dealer Fraud
- Flash Call Detection
- SIM Box Detection (TCG)
- Bypass Fraud

Revenue Assurance
- Usage Assurance
- Provisioning Assurance
- Rating & Billing Assurance
- Cost & Margin Assurance
- Prepaid Balance Validation
- Proactive RA (TCG)

10

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



Flexible catalogue of service and deployment models

On-Prem

Private Cloud

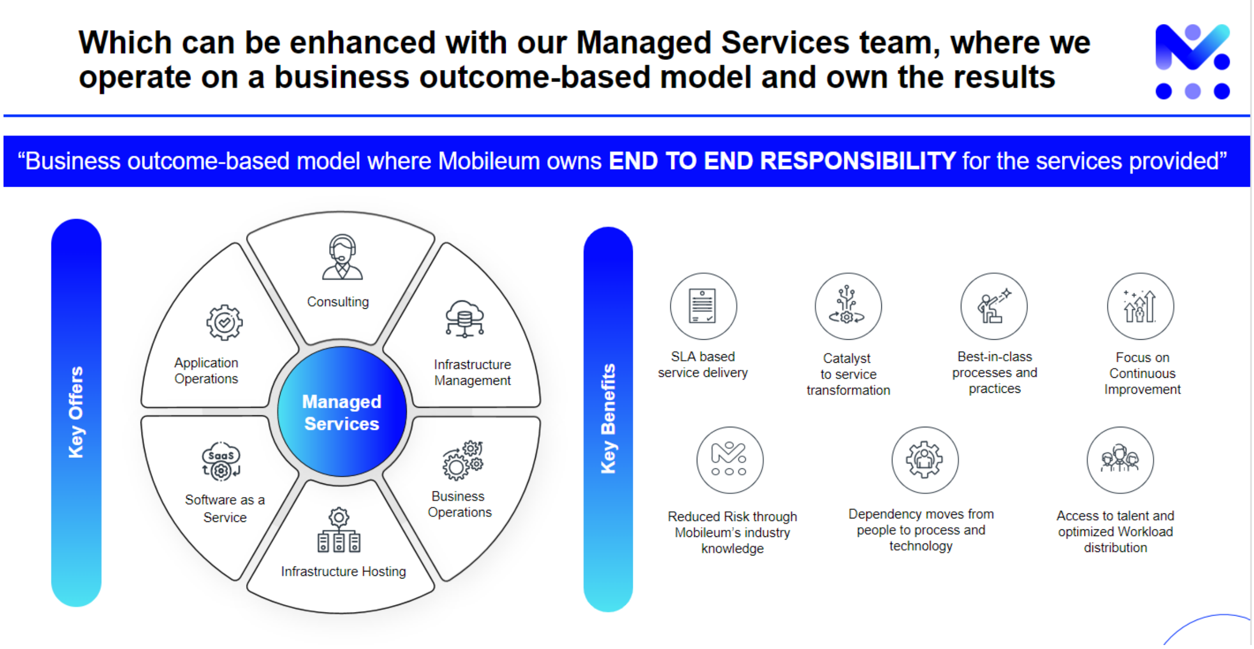
Hybrid Cloud

Public Cloud

24 x 7 x 365

“Follow The Sun” support model

Enhanced with our Managed Services Team



Which can be enhanced with our Managed Services team, where we operate on a business outcome-based model and own the results

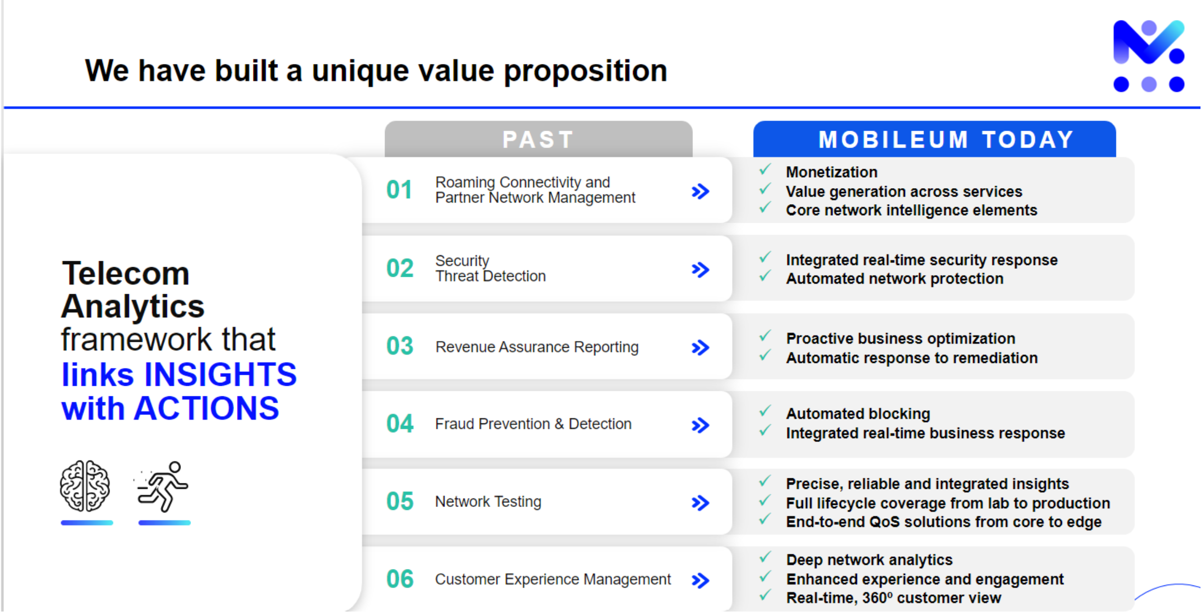
“Business outcome-based model where Mobileum owns **END TO END RESPONSIBILITY** for the services provided”

Key Offers

Key Benefits

- SLA based service delivery
- Catalyst to service transformation
- Best-in-class processes and practices
- Focus on Continuous Improvement
- Reduced Risk through Mobileum’s industry knowledge
- Dependency moves from people to process and technology
- Access to talent and optimized Workload distribution

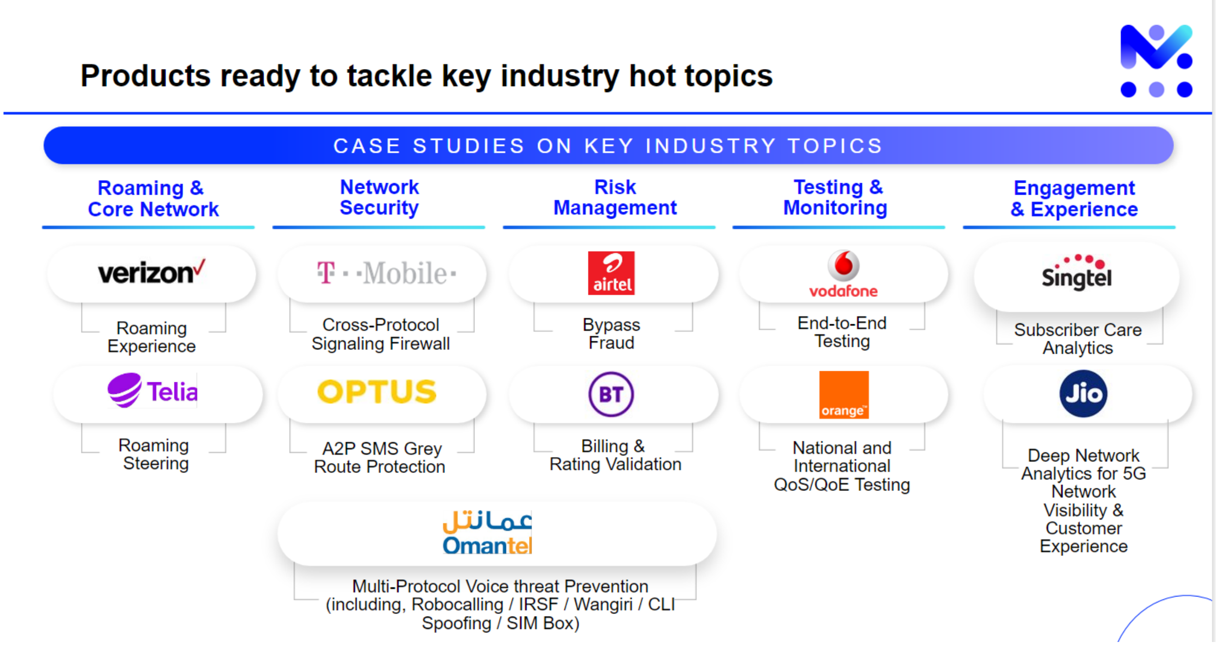
We have built a unique value proposition:



We have built a unique value proposition

Telecom Analytics framework that **links INSIGHTS with ACTIONS**

PAST	MOBILEUM TODAY
01 Roaming Connectivity and Partner Network Management	✓ Monetization ✓ Value generation across services ✓ Core network intelligence elements
02 Security Threat Detection	✓ Integrated real-time security response ✓ Automated network protection
03 Revenue Assurance Reporting	✓ Proactive business optimization ✓ Automatic response to remediation
04 Fraud Prevention & Detection	✓ Automated blocking ✓ Integrated real-time business response
05 Network Testing	✓ Precise, reliable and integrated insights ✓ Full lifecycle coverage from lab to production ✓ End-to-end QoS solutions from core to edge
06 Customer Experience Management	✓ Deep network analytics ✓ Enhanced experience and engagement ✓ Real-time, 360° customer view

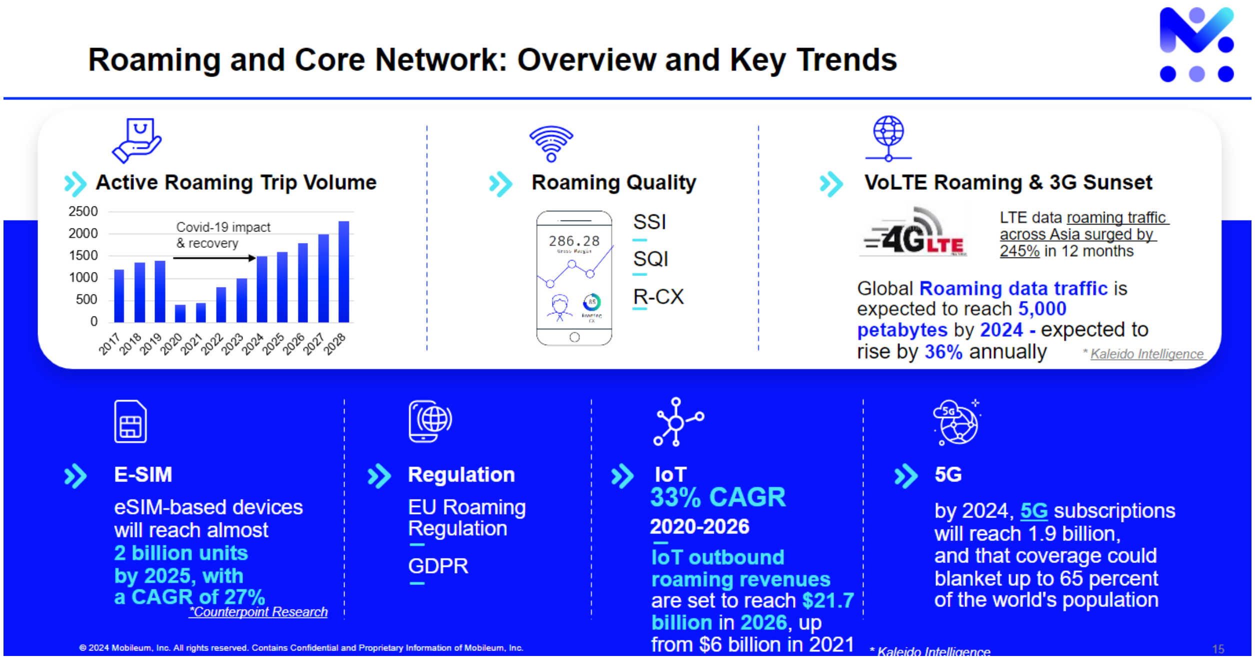


Products ready to tackle key industry hot topics

CASE STUDIES ON KEY INDUSTRY TOPICS

Roaming & Core Network	Network Security	Risk Management	Testing & Monitoring	Engagement & Experience
verizon – Roaming Experience	T-Mobile – Cross-Protocol Signaling Firewall	airtel – Bypass Fraud	vodafone – End-to-End Testing	Singtel – Subscriber Care Analytics
Telia – Roaming Steering	OPTUS – A2P SMS Grey Route Protection	BT – Billing & Rating Validation	orange – National and International QoS/QoE Testing	Jio – Deep Network Analytics for 5G Network Visibility & Customer Experience
	عمانتل Omantel – Multi-Protocol Voice threat Prevention (including, Robocalling / IRSF / Wangiri / CLI Spoofing / SIM Box)			

Roaming



Roaming and Core Network: Overview and Key Trends

Active Roaming Trip Volume

Roaming Quality

SSI

SQI

R-CX

VoLTE Roaming & 3G Sunset

LTE data roaming traffic across Asia surged by 245% in 12 months

Global **Roaming data traffic** is expected to reach **5,000 petabytes** by **2024 -** expected to rise by **36%** annually ** Kaleido Intelligence*

E-SIM

eSIM-based devices will reach almost **2 billion units by 2025, with a CAGR of 27%**

**Counterpoint Research*

Regulation

EU Roaming Regulation

GDPR

IoT

33% CAGR

2020-2026

IoT outbound roaming revenues are set to reach **$21.7 billion** in **2026**, up from $6 billion in 2021

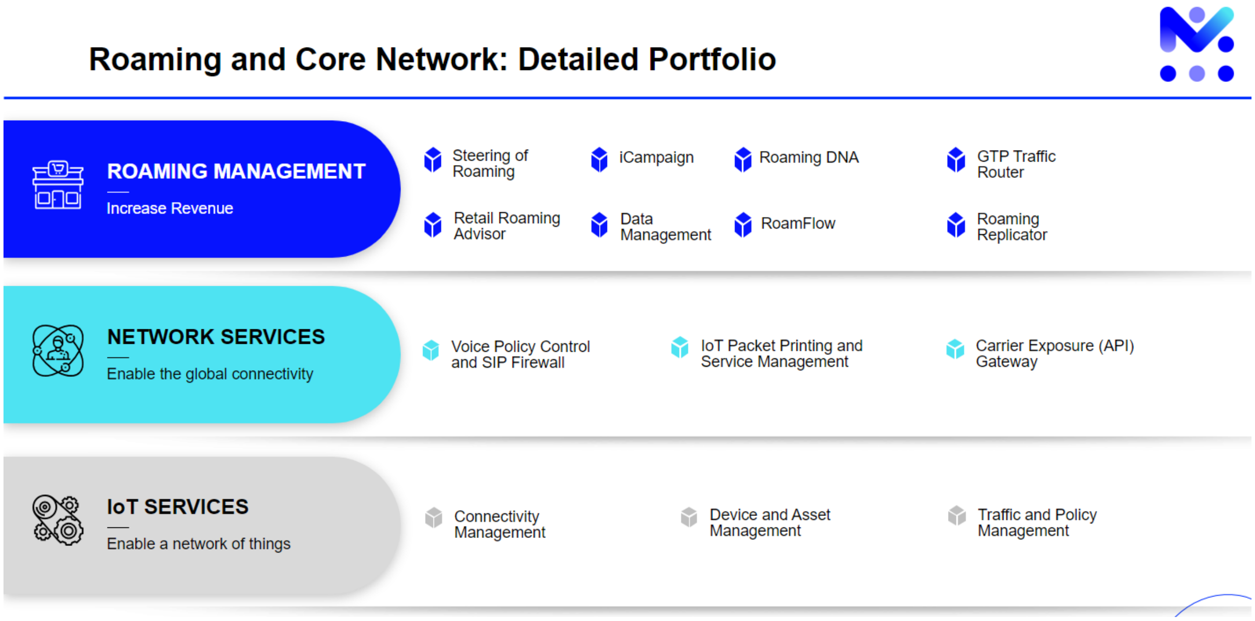
** Kaleido Intelligence*

5G

by 2024, 5G subscriptions will reach 1.9 billion, and that coverage could blanket up to 65 percent of the world's population

© 2024 Mobileum, Inc. All rights reserved. Contains Confidential and Proprietary Information of Mobileum, Inc.

15



Roaming and Core Network: Detailed Portfolio

ROAMING MANAGEMENT

Increase Revenue

- Steering of Roaming
- iCampaign
- Roaming DNA
- GTP Traffic Router
- Retail Roaming Advisor
- Data Management
- RoamFlow
- Roaming Replicator

NETWORK SERVICES

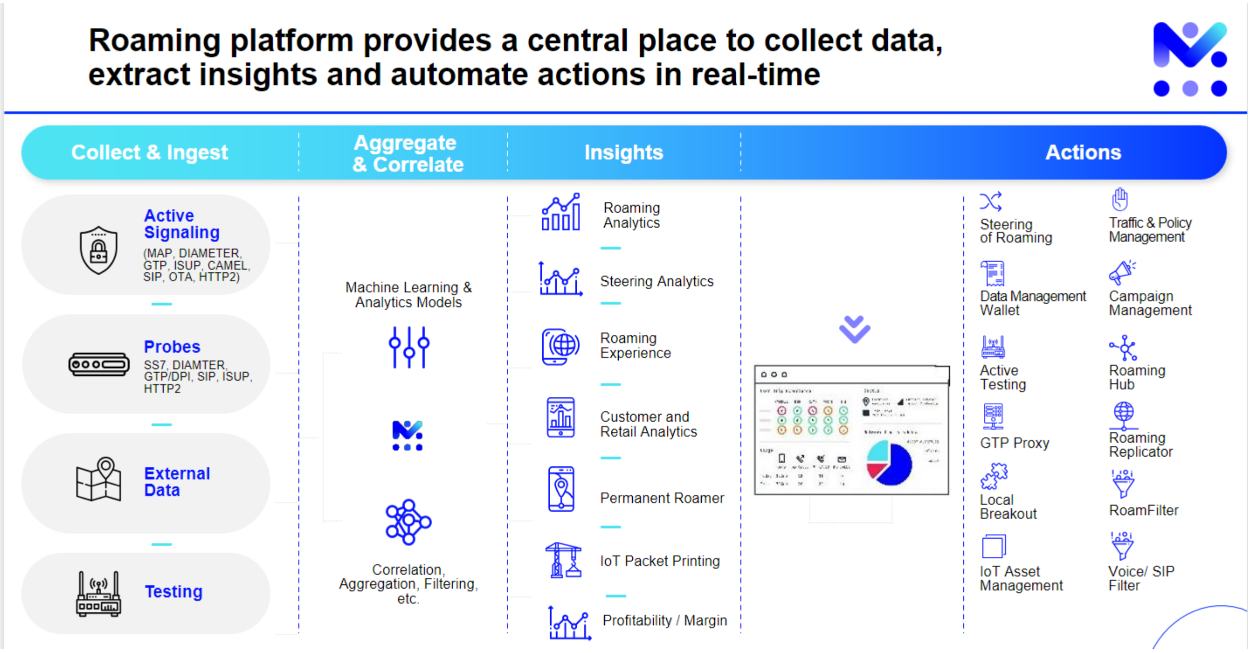
Enable the global connectivity

- Voice Policy Control and SIP Firewall
- IoT Packet Printing and Service Management
- Carrier Exposure (API) Gateway

IoT SERVICES

Enable a network of things

- Connectivity Management
- Device and Asset Management
- Traffic and Policy Management



Roaming platform provides a central place to collect data, extract insights and automate actions in real-time

Collect & Ingest

Active Signaling
(MAP, DIAMETER, GTP, ISUP, CAMEL, SIP, OTA, HTTP2)

Probes
SS7, DIAMTER, GTP/DPI, SIP, ISUP, HTTP2

External Data

Testing

Aggregate & Correlate

Machine Learning & Analytics Models

Correlation, Aggregation, Filtering, etc.

Insights

Roaming Analytics

Steering Analytics

Roaming Experience

Customer and Retail Analytics

Permanent Roamer

IoT Packet Printing

Profitability / Margin

Actions

Steering of Roaming

Traffic & Policy Management

Data Management Wallet

Campaign Management

Active Testing

Roaming Hub

GTP Proxy

Roaming Replicator

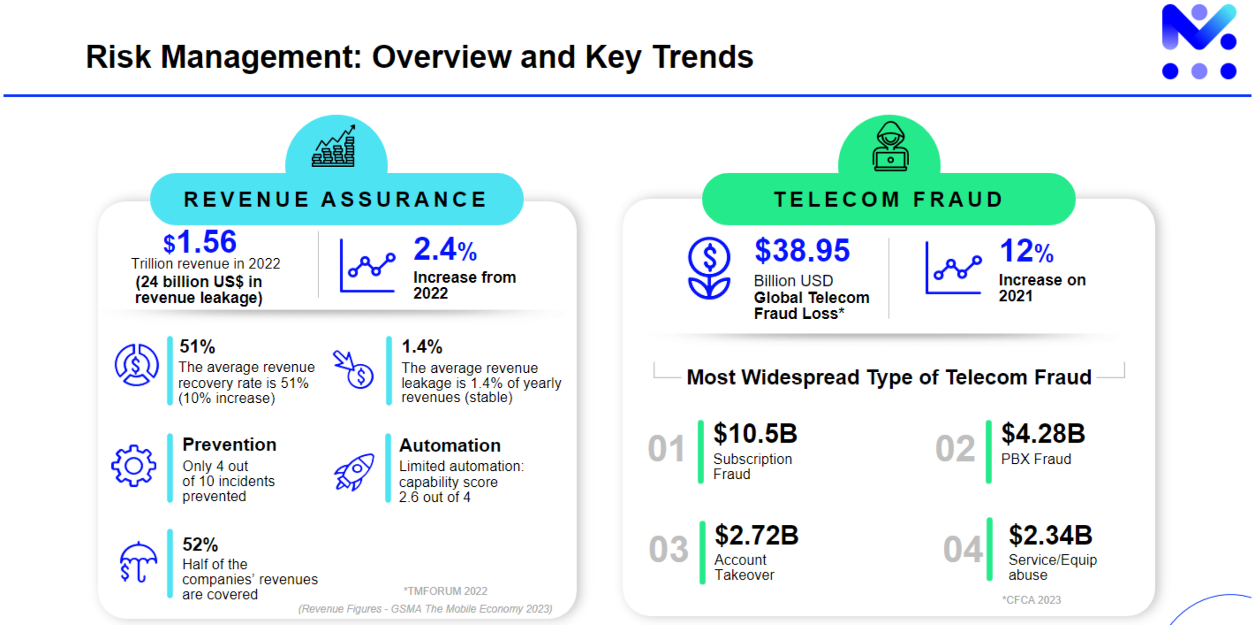
Local Breakout

RoamFilter

IoT Asset Management

Voice/ SIP Filter

Risk Management



Risk Management: Overview and Key Trends

REVENUE ASSURANCE

$1.56
Trillion revenue in 2022
(24 billion US$ in revenue leakage)

2.4%
Increase from 2022

51%
The average revenue recovery rate is 51% (10% increase)

1.4%
The average revenue leakage is 1.4% of yearly revenues (stable)

Prevention
Only 4 out of 10 incidents prevented

Automation
Limited automation: capability score 2.6 out of 4

52%
Half of the companies' revenues are covered

*TMFORUM 2022

(Revenue Figures - GSMA The Mobile Economy 2023)

TELECOM FRAUD

$38.95
Billion USD
Global Telecom Fraud Loss*

12%
Increase on 2021

Most Widespread Type of Telecom Fraud

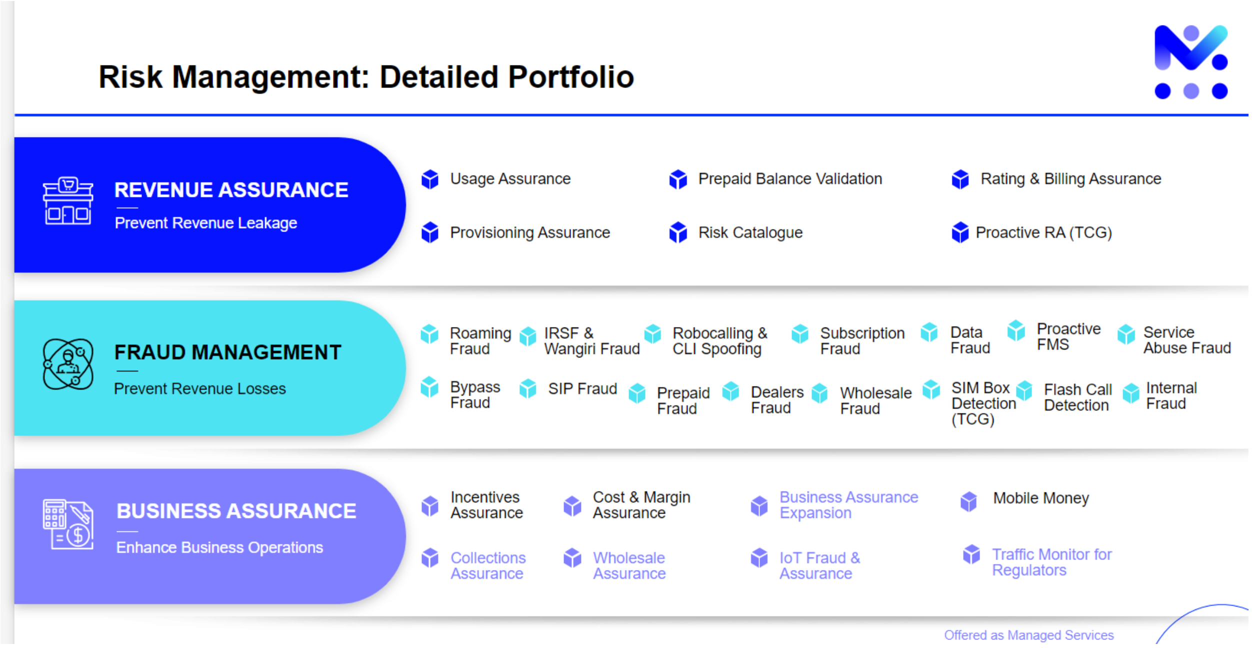
01 $10.5B Subscription Fraud

02 $4.28B PBX Fraud

03 $2.72B Account Takeover

04 $2.34B Service/Equip abuse

*CFCA 2023



Risk Management: Detailed Portfolio

REVENUE ASSURANCE
Prevent Revenue Leakage

- Usage Assurance
- Prepaid Balance Validation
- Rating & Billing Assurance
- Provisioning Assurance
- Risk Catalogue
- Proactive RA (TCG)

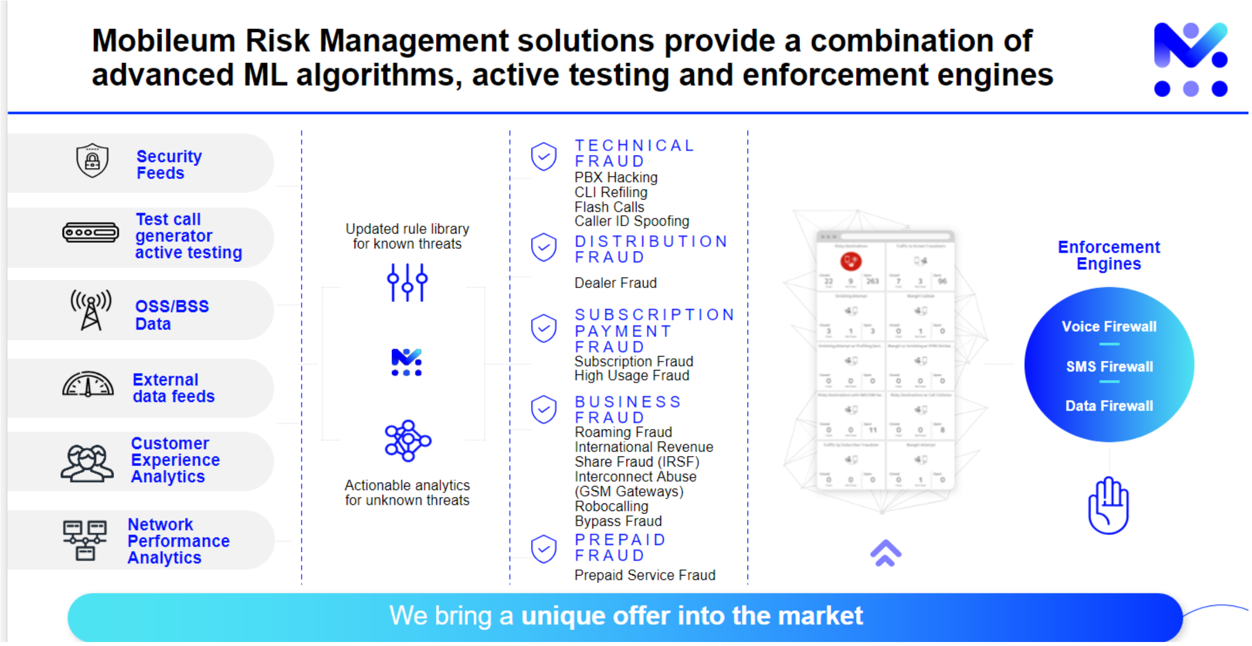
FRAUD MANAGEMENT
Prevent Revenue Losses

- Roaming Fraud
- IRSF & Wangiri Fraud
- Robocalling & CLI Spoofing
- Subscription Fraud
- Data Fraud
- Proactive FMS
- Service Abuse Fraud
- Bypass Fraud
- SIP Fraud
- Prepaid Fraud
- Dealers Fraud
- Wholesale Fraud
- SIM Box Detection (TCG)
- Flash Call Detection
- Internal Fraud

BUSINESS ASSURANCE
Enhance Business Operations

- Incentives Assurance
- Cost & Margin Assurance
- Business Assurance Expansion
- Mobile Money
- Collections Assurance
- Wholesale Assurance
- IoT Fraud & Assurance
- Traffic Monitor for Regulators

Offered as Managed Services



Mobileum Risk Management solutions provide a combination of advanced ML algorithms, active testing and enforcement engines

Security Feeds
Test call generator active testing
OSS/BSS Data
External data feeds
Customer Experience Analytics
Network Performance Analytics
Updated rule library for known threats
Actionable analytics for unknown threats

TECHNICAL FRAUD
PBX Hacking
CLI Refiling
Flash Calls
Caller ID Spoofing

DISTRIBUTION FRAUD
Dealer Fraud

SUBSCRIPTION PAYMENT FRAUD
Subscription Fraud
High Usage Fraud

BUSINESS FRAUD
Roaming Fraud
International Revenue Share Fraud (IRSF)
Interconnect Abuse (GSM Gateways)
Robocalling
Bypass Fraud

PREPAID FRAUD
Prepaid Service Fraud

We bring a **unique offer into the market**

Security

Network Security: Overview and Key Trends

58%
Of Enterprises (and 52% of consumers) would leave or consider leaving their operators because of a security breach

73%
Of Enterprises (and 62% of Consumers) would want to use 2FA less, stop using or have an alternative

3rd
Most likely reason to churn after price and coverage

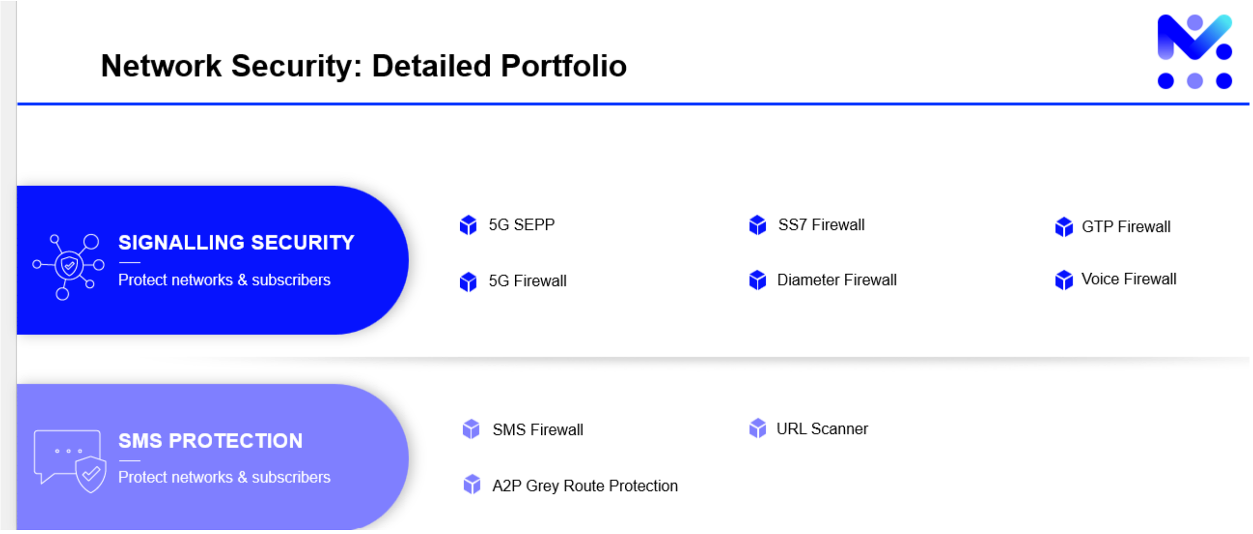
For $500, this site promises the power to track a phone and intercept its texts

German researchers discover a flaw that co listen to your cell calls.

Germany drops inquiry into claims NSA tapped Angela Merkel's phone

Prosecutors say they can find no actionable evidence to support claims German chancellor's mobile phone was tapped by US National Security Agency

European risk report flags 5G security challenges



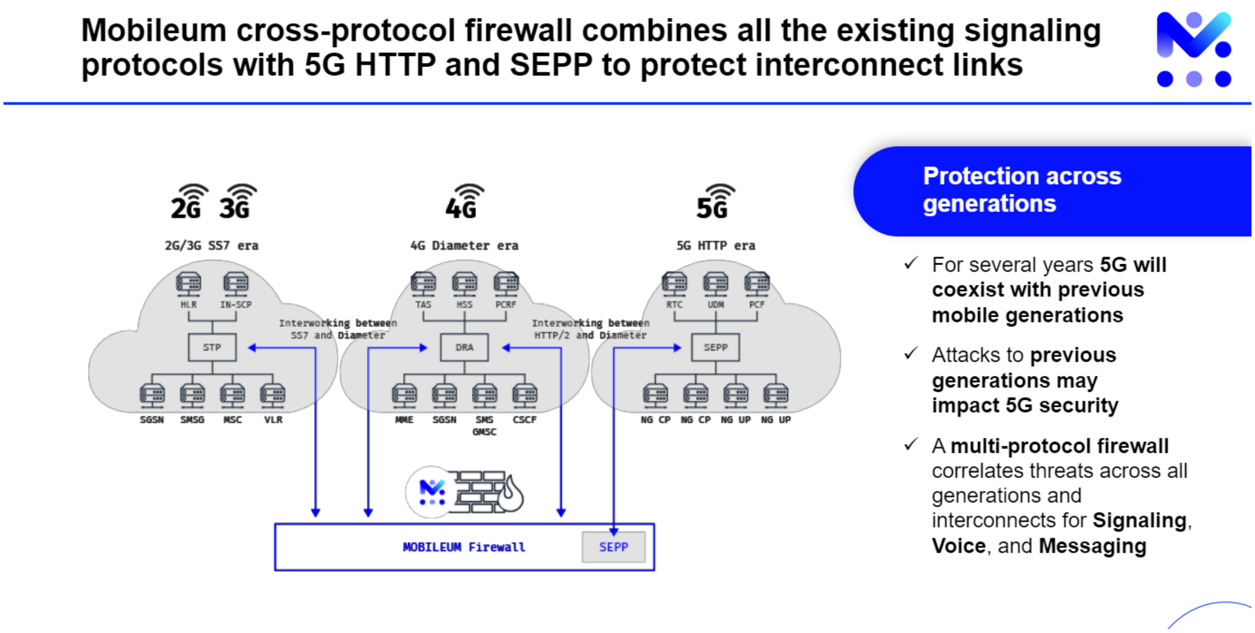
Network Security: Detailed Portfolio

SIGNALLING SECURITY
Protect networks & subscribers

- 5G SEPP
- 5G Firewall
- SS7 Firewall
- Diameter Firewall
- GTP Firewall
- Voice Firewall

SMS PROTECTION
Protect networks & subscribers

- SMS Firewall
- A2P Grey Route Protection
- URL Scanner

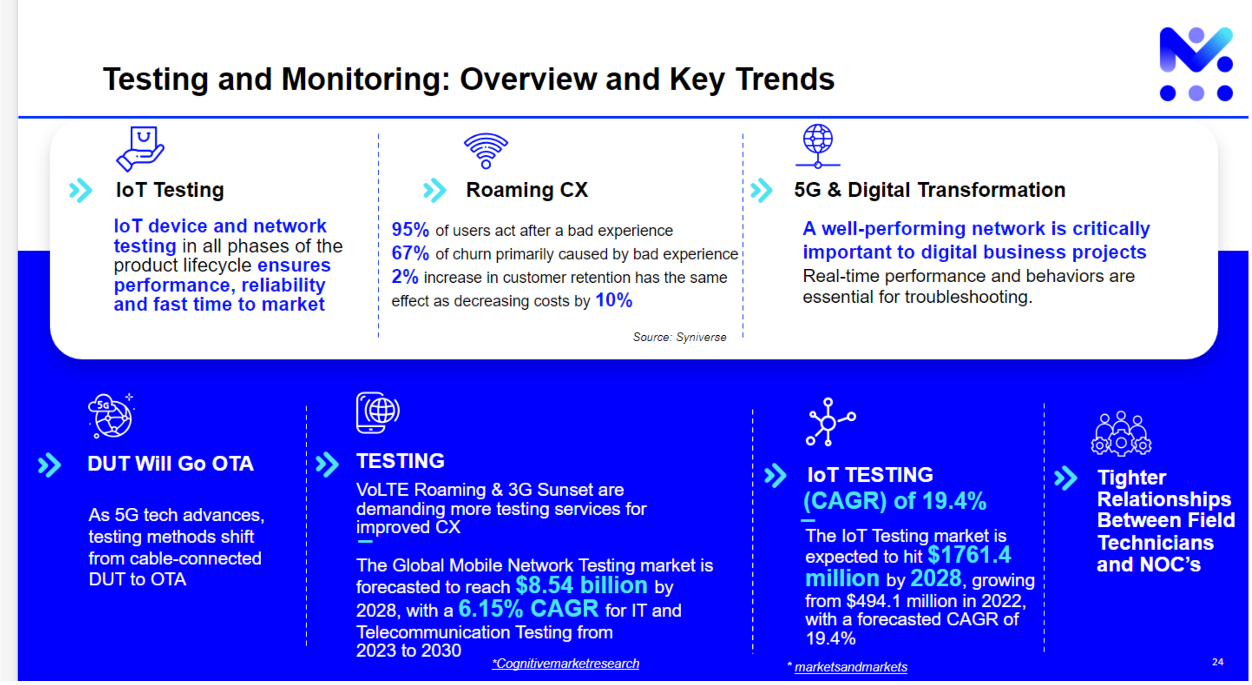


Mobileum cross-protocol firewall combines all the existing signaling protocols with 5G HTTP and SEPP to protect interconnect links

Protection across generations

- ✓ For several years **5G will coexist with previous mobile generations**
- ✓ Attacks to **previous generations may impact 5G security**
- ✓ A **multi-protocol firewall** correlates threats across all generations and interconnects for **Signaling**, **Voice**, and **Messaging**

Testing and Monitoring



Testing and Monitoring: Overview and Key Trends

IoT Testing

IoT device and network testing in all phases of the product lifecycle **ensures performance, reliability and fast time to market**

Roaming CX

95% of users act after a bad experience
67% of churn primarily caused by bad experience
2% increase in customer retention has the same effect as decreasing costs by **10%**

Source: Syniverse

5G & Digital Transformation

A well-performing network is critically important to digital business projects
Real-time performance and behaviors are essential for troubleshooting.

DUT Will Go OTA

As 5G tech advances, testing methods shift from cable-connected DUT to OTA

TESTING

VoLTE Roaming & 3G Sunset are demanding more testing services for improved CX

The Global Mobile Network Testing market is forecasted to reach **$8.54 billion** by 2028, with a **6.15% CAGR** for IT and Telecommunication Testing from 2023 to 2030

**Cognitivemarketresearch*

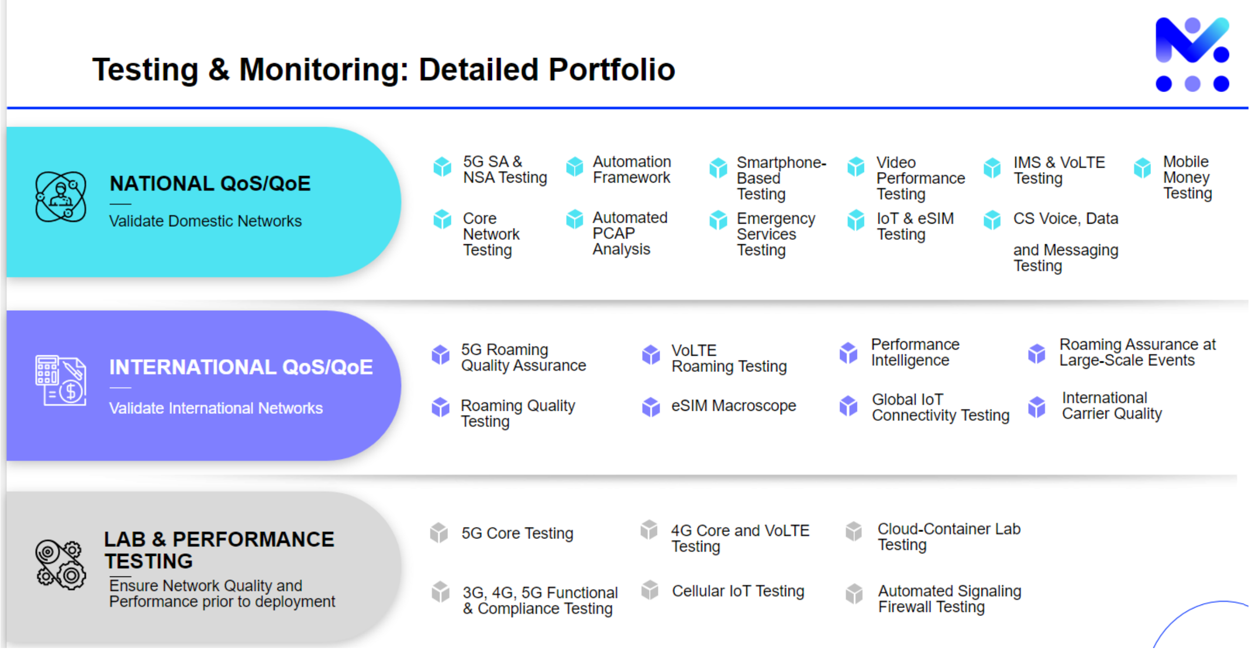
IoT TESTING (CAGR) of 19.4%

The IoT Testing market is expected to hit **$1761.4 million** by **2028**, growing from $494.1 million in 2022, with a forecasted CAGR of 19.4%

** marketsandmarkets*

Tighter Relationships Between Field Technicians and NOC's

24



Testing & Monitoring: Detailed Portfolio

NATIONAL QoS/QoE

Validate Domestic Networks

- 5G SA & NSA Testing
- Core Network Testing
- Automation Framework
- Automated PCAP Analysis
- Smartphone-Based Testing
- Emergency Services Testing
- Video Performance Testing
- IoT & eSIM Testing
- IMS & VoLTE Testing
- CS Voice, Data and Messaging Testing
- Mobile Money Testing

INTERNATIONAL QoS/QoE

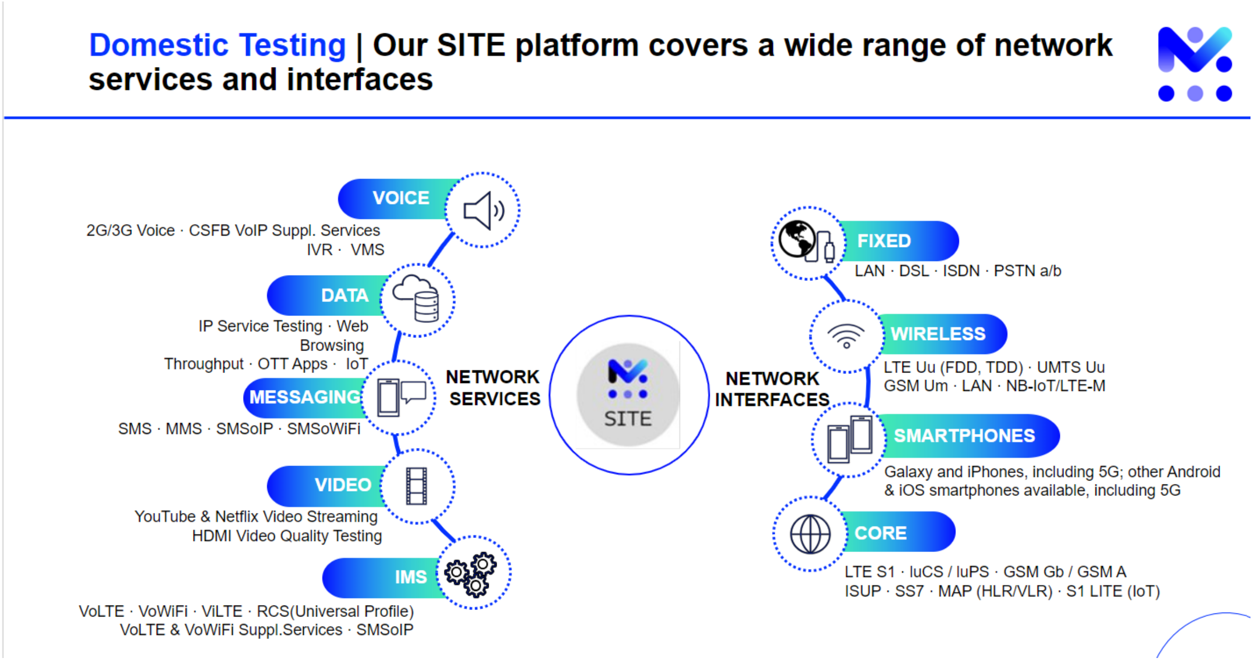
Validate International Networks

- 5G Roaming Quality Assurance
- Roaming Quality Testing
- VoLTE Roaming Testing
- eSIM Macroscope
- Performance Intelligence
- Global IoT Connectivity Testing
- Roaming Assurance at Large-Scale Events
- International Carrier Quality

LAB & PERFORMANCE TESTING

Ensure Network Quality and Performance prior to deployment

- 5G Core Testing
- 3G, 4G, 5G Functional & Compliance Testing
- 4G Core and VoLTE Testing
- Cellular IoT Testing
- Cloud-Container Lab Testing
- Automated Signaling Firewall Testing



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

VOICE: 2G/3G Voice · CSFB VoIP Suppl. Services IVR · VMS

DATA: IP Service Testing · Web Browsing Throughput · OTT Apps · IoT

MESSAGING: SMS · MMS · SMSoIP · SMSoWiFi

VIDEO: YouTube & Netflix Video Streaming HDMI Video Quality Testing

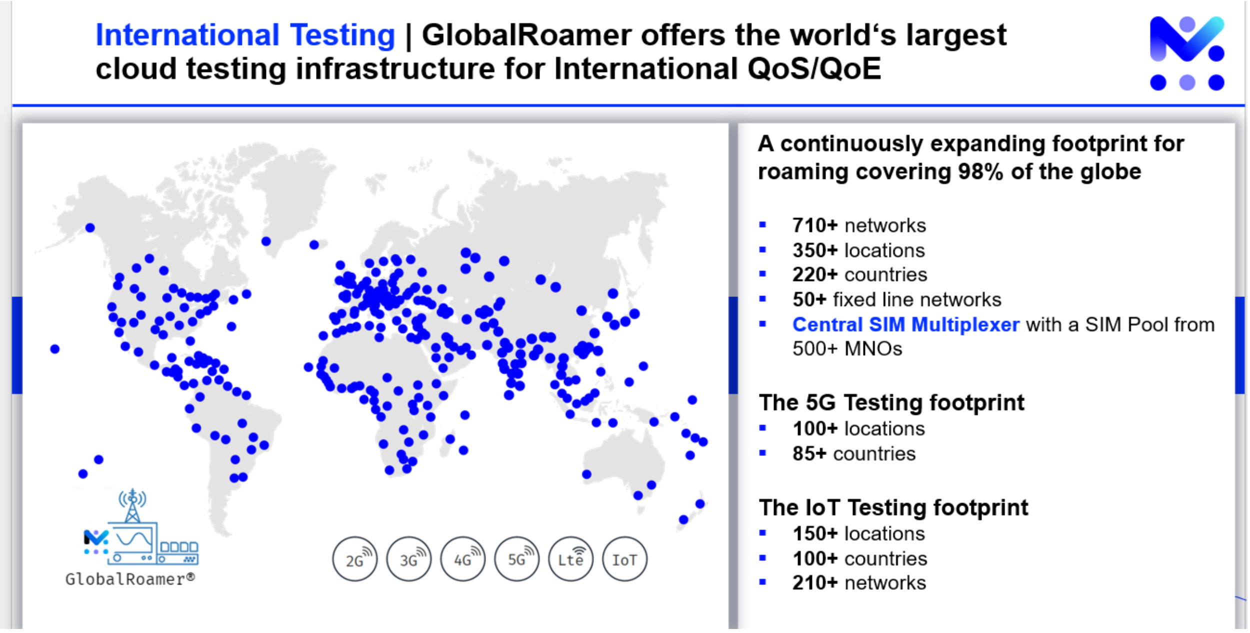
IMS: VoLTE · VoWiFi · ViLTE · RCS(Universal Profile) VoLTE & VoWiFi Suppl.Services · SMSoIP

FIXED: LAN · DSL · ISDN · PSTN a/b

WIRELESS: LTE Uu (FDD, TDD) · UMTS Uu GSM Um · LAN · NB-IoT/LTE-M

SMARTPHONES: Galaxy and iPhones, including 5G; other Android & iOS smartphones available, including 5G

CORE: LTE S1 · IuCS / IuPS · GSM Gb / GSM A ISUP · SS7 · MAP (HLR/VLR) · S1 LITE (IoT)



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

A continuously expanding footprint for roaming covering 98% of the globe

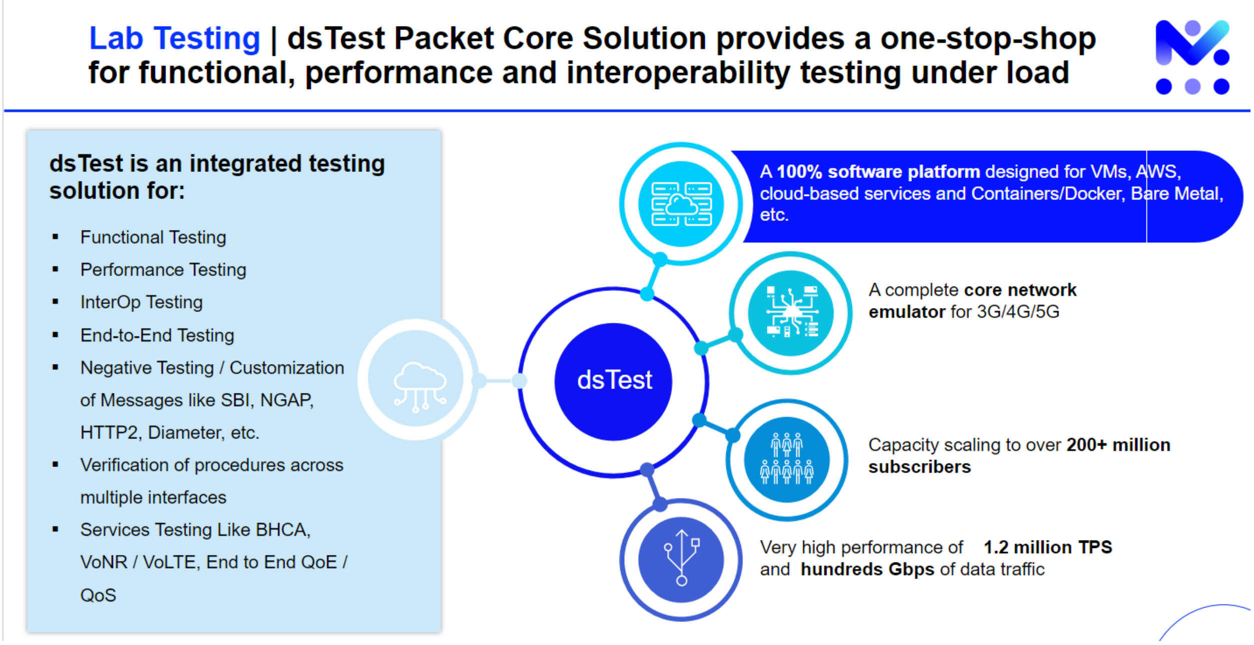
- **710+** networks
- **350+** locations
- **220+** countries
- **50+** fixed line networks
- **Central SIM Multiplexer** with a SIM Pool from 500+ MNOs

The 5G Testing footprint

- **100+** locations
- **85+** countries

The IoT Testing footprint

- **150+** locations
- **100+** countries
- **210+** networks



Lab Testing | dsTest Packet Core Solution provides a one-stop-shop for functional, performance and interoperability testing under load

dsTest is an integrated testing solution for:

- Functional Testing
- Performance Testing
- InterOp Testing
- End-to-End Testing
- Negative Testing / Customization of Messages like SBI, NGAP, HTTP2, Diameter, etc.
- Verification of procedures across multiple interfaces
- Services Testing Like BHCA, VoNR / VoLTE, End to End QoE / QoS

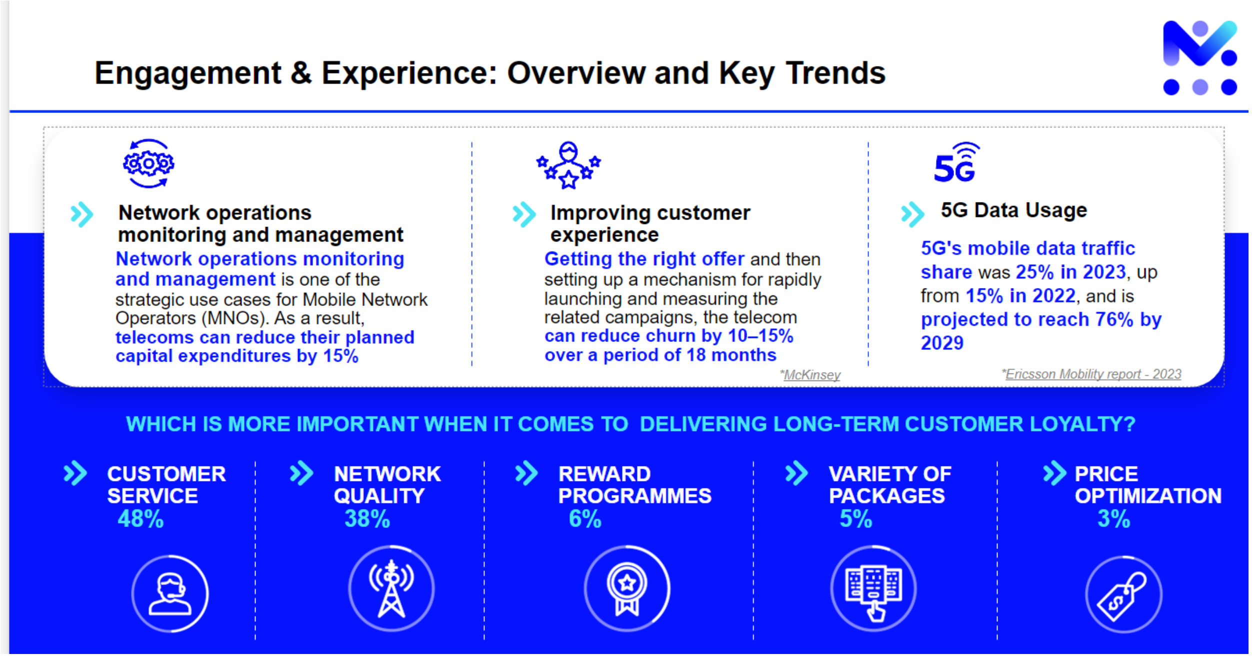
A **100% software platform** designed for VMs, AWS, cloud-based services and Containers/Docker, Bare Metal, etc.

A complete **core network emulator** for 3G/4G/5G

Capacity scaling to over **200+ million subscribers**

Very high performance of **1.2 million TPS** and **hundreds Gbps** of data traffic

Engagement & Experience



Engagement & Experience: Overview and Key Trends

Network operations monitoring and management

Network operations monitoring and management is one of the strategic use cases for Mobile Network Operators (MNOs). As a result, **telecoms can reduce their planned capital expenditures by 15%**

Improving customer experience

Getting the right offer and then setting up a mechanism for rapidly launching and measuring the related campaigns, the telecom **can reduce churn by 10–15% over a period of 18 months**

*McKinsey

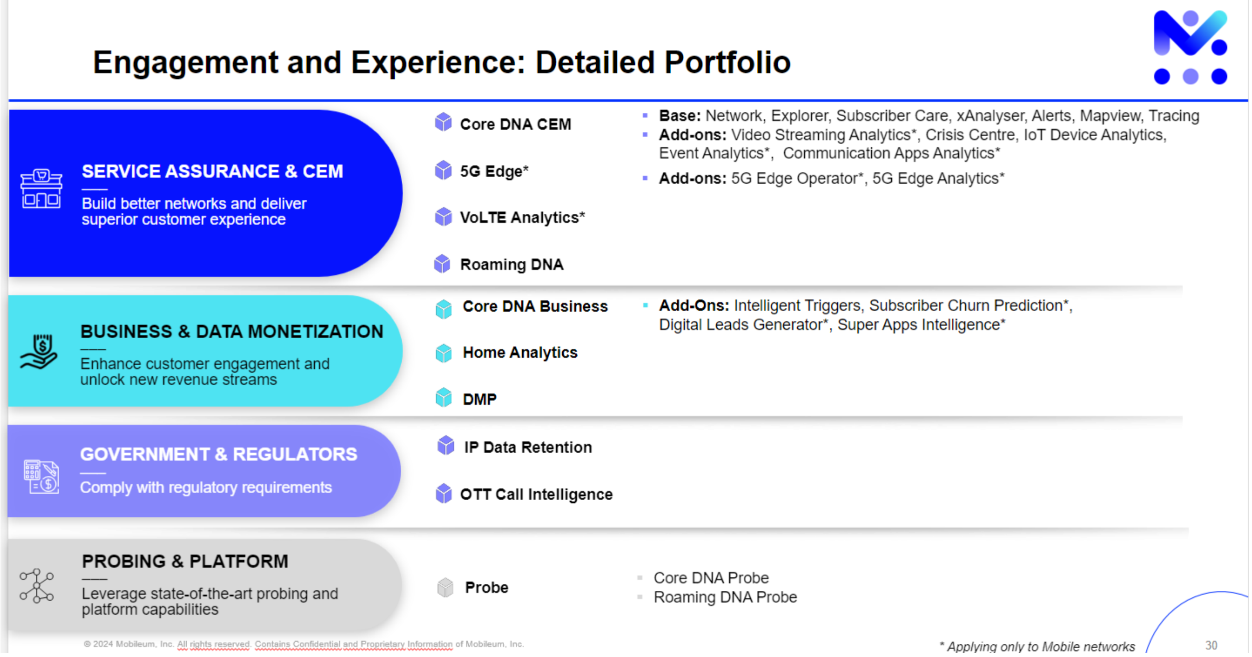
5G Data Usage

5G's mobile data traffic share was **25% in 2023**, up from **15% in 2022**, and is **projected to reach 76% by 2029**

*Ericsson Mobility report - 2023

WHICH IS MORE IMPORTANT WHEN IT COMES TO DELIVERING LONG-TERM CUSTOMER LOYALTY?

CUSTOMER SERVICE	NETWORK QUALITY	REWARD PROGRAMMES	VARIETY OF PACKAGES	PRICE OPTIMIZATION
48%	38%	6%	5%	3%



Engagement and Experience: Detailed Portfolio

SERVICE ASSURANCE & CEM

Build better networks and deliver superior customer experience

- **Core DNA CEM**
  - **Base:** Network, Explorer, Subscriber Care, xAnalyser, Alerts, Mapview, Tracing
  - **Add-ons:** Video Streaming Analytics*, Crisis Centre, IoT Device Analytics, Event Analytics*, Communication Apps Analytics*
- **5G Edge***
  - **Add-ons:** 5G Edge Operator*, 5G Edge Analytics*
- **VoLTE Analytics***
- **Roaming DNA**

BUSINESS & DATA MONETIZATION

Enhance customer engagement and unlock new revenue streams

- **Core DNA Business**
  - **Add-Ons:** Intelligent Triggers, Subscriber Churn Prediction*, Digital Leads Generator*, Super Apps Intelligence*
- **Home Analytics**
- **DMP**

GOVERNMENT & REGULATORS

Comply with regulatory requirements

- **IP Data Retention**
- **OTT Call Intelligence**

PROBING & PLATFORM

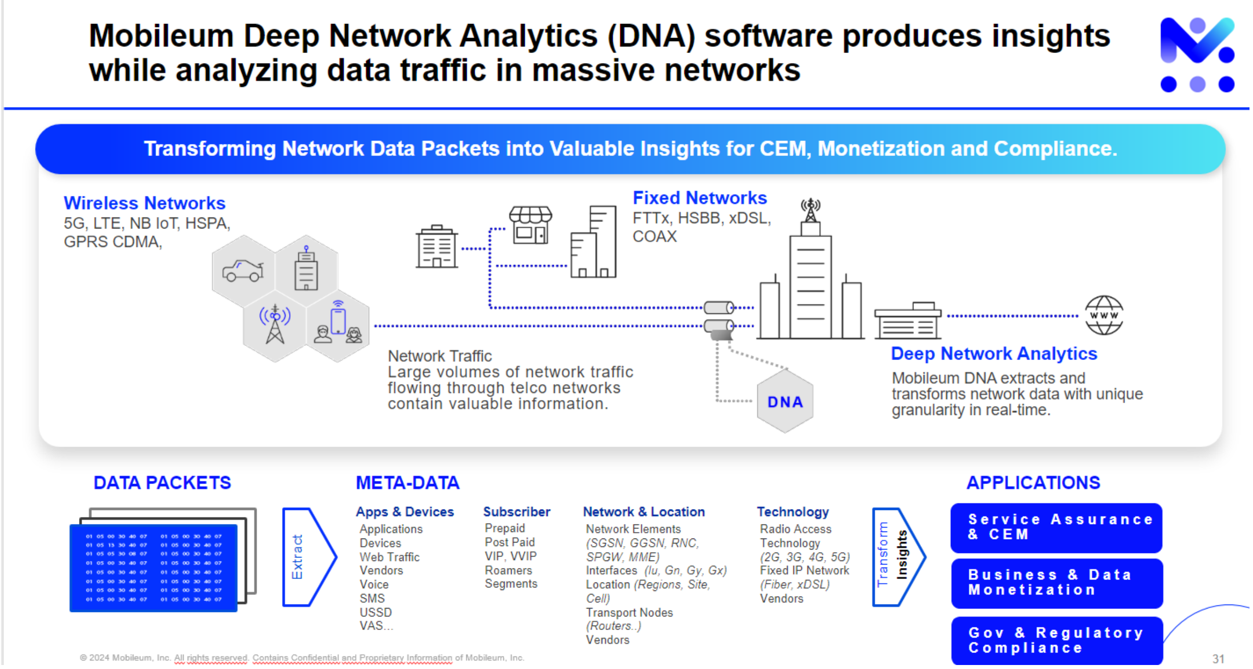
Leverage state-of-the-art probing and platform capabilities

- **Probe**
  - Core DNA Probe
  - Roaming DNA Probe

© 2024 Mobileum, Inc. All rights reserved. Contains Confidential and Proprietary Information of Mobileum, Inc.

* Applying only to Mobile networks

30



Mobileum Deep Network Analytics (DNA) software produces insights while analyzing data traffic in massive networks

Transforming Network Data Packets into Valuable Insights for CEM, Monetization and Compliance.

Wireless Networks
5G, LTE, NB IoT, HSPA,
GPRS CDMA,

Fixed Networks
FTTx, HSBB, xDSL,
COAX

Network Traffic
Large volumes of network traffic flowing through telco networks contain valuable information.

Deep Network Analytics
Mobileum DNA extracts and transforms network data with unique granularity in real-time.

DATA PACKETS

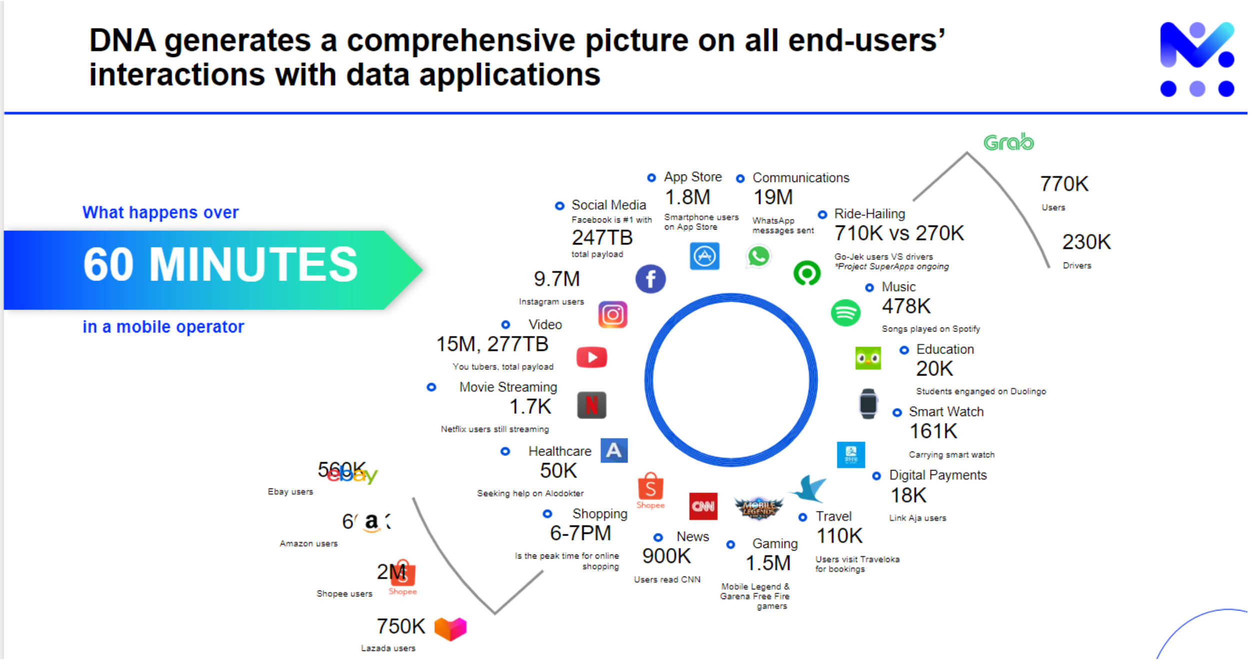
META-DATA

Apps & Devices	Subscriber	Network & Location	Technology
Applications Devices Web Traffic Vendors Voice SMS USSD VAS…	Prepaid Post Paid VIP, VVIP Roamers Segments	Network Elements *(SGSN, GGSN, RNC, SPGW, MME)* Interfaces *(Iu, Gn, Gy, Gx)* Location *(Regions, Site, Cell)* Transport Nodes *(Routers..)* Vendors	Radio Access Technology *(2G, 3G, 4G, 5G)* Fixed IP Network *(Fiber, xDSL)* Vendors

APPLICATIONS

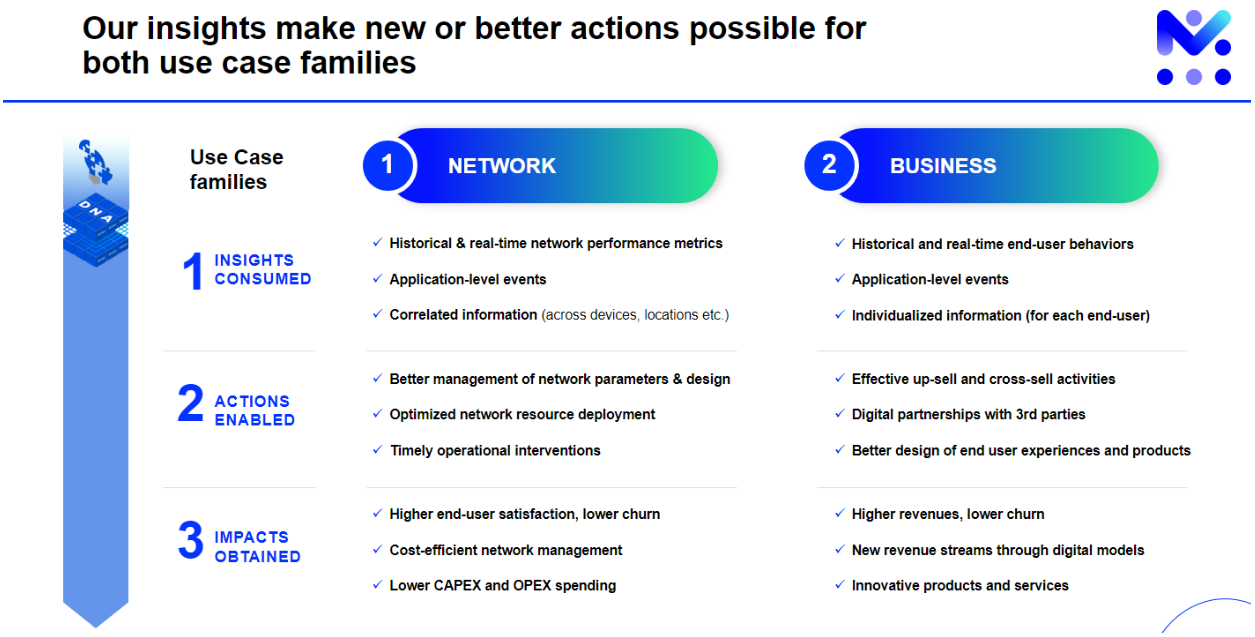
- Service Assurance & CEM
- Business & Data Monetization
- Gov & Regulatory Compliance

31



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

What happens over
60 MINUTES
in a mobile operator

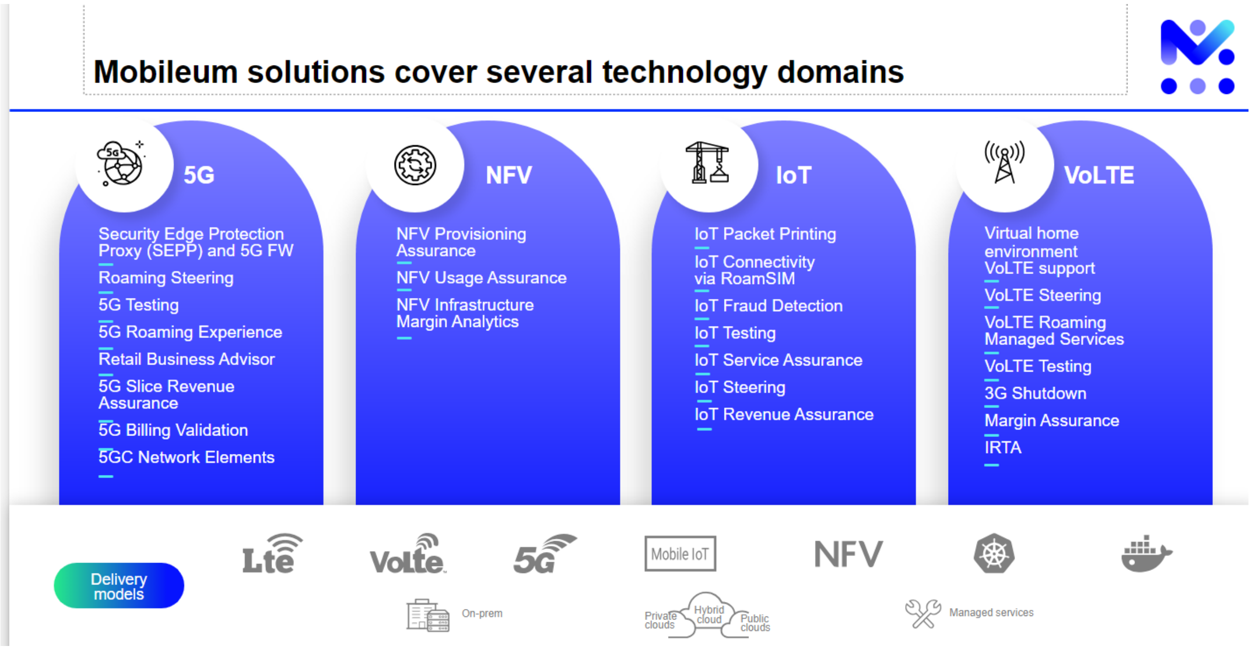


Our insights make new or better actions possible for both use case families

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 solutions cover several technology domains

5G

- Security Edge Protection Proxy (SEPP) and 5G FW
- Roaming Steering
- 5G Testing
- 5G Roaming Experience
- Retail Business Advisor
- 5G Slice Revenue Assurance
- 5G Billing Validation
- 5GC Network Elements

NFV

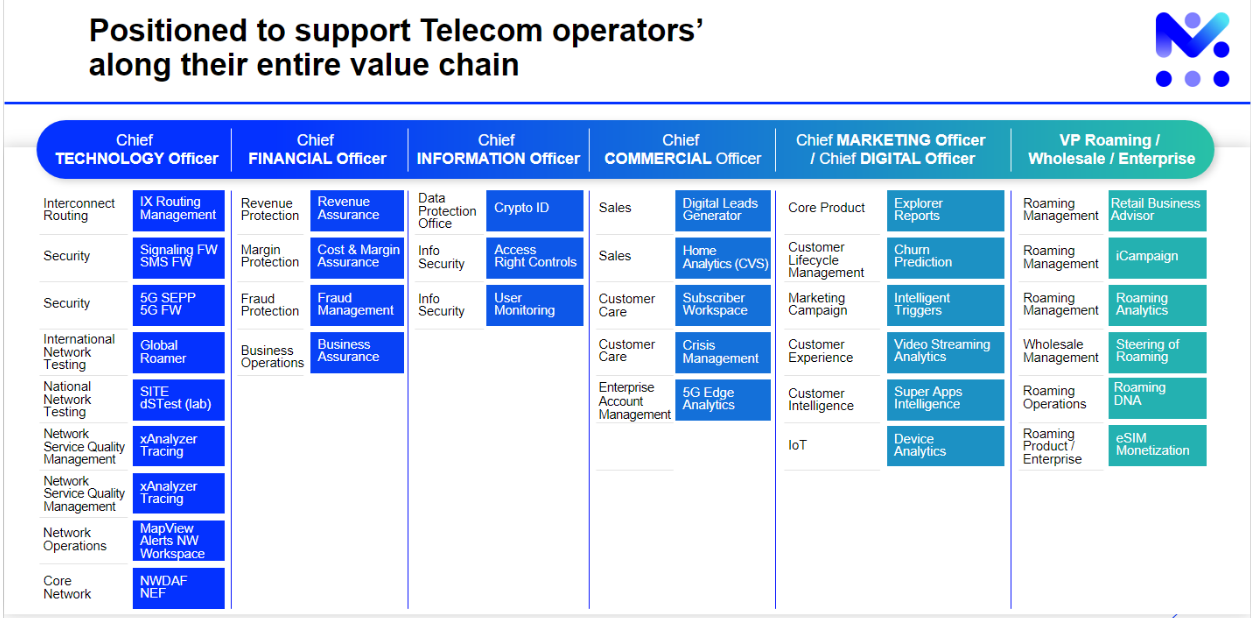
- NFV Provisioning Assurance
- NFV Usage Assurance
- NFV Infrastructure Margin Analytics

IoT

- IoT Packet Printing
- IoT Connectivity via RoamSIM
- IoT Fraud Detection
- IoT Testing
- IoT Service Assurance
- IoT Steering
- IoT Revenue Assurance

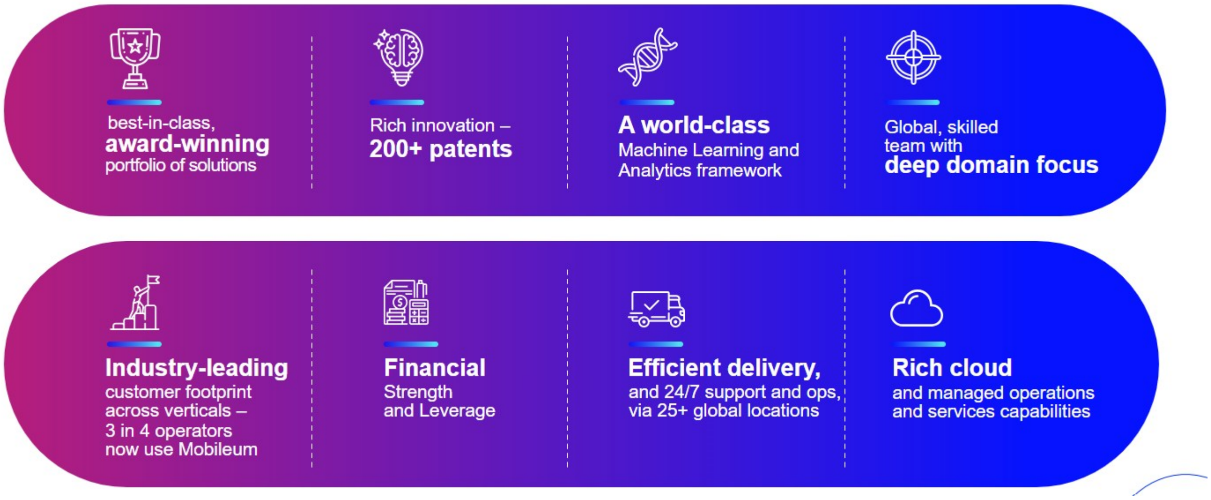
VoLTE

- Virtual home environment VoLTE support
- VoLTE Steering
- VoLTE Roaming Managed Services
- VoLTE Testing
- 3G Shutdown
- Margin Assurance
- IRTA



Positioned to support Telecom operators' along their entire value chain

Chief TECHNOLOGY Officer		Chief FINANCIAL Officer		Chief INFORMATION Officer		Chief COMMERCIAL Officer		Chief MARKETING Officer / Chief DIGITAL Officer		VP Roaming / Wholesale / Enterprise	
Interconnect Routing	IX Routing Management	Revenue Protection	Revenue Assurance	Data Protection Office	Crypto ID	Sales	Digital Leads Generator	Core Product	Explorer Reports	Roaming Management	Retail Business Advisor
Security	Signaling FW SMS FW	Margin Protection	Cost & Margin Assurance	Info Security	Access Right Controls	Sales	Home Analytics (CVS)	Customer Lifecycle Management	Churn Prediction	Roaming Management	iCampaign
Security	5G SEPP 5G FW	Fraud Protection	Fraud Management	Info Security	User Monitoring	Customer Care	Subscriber Workspace	Marketing Campaign	Intelligent Triggers	Roaming Management	Roaming Analytics
International Network Testing	Global Roamer	Business Operations	Business Assurance			Customer Care	Crisis Management	Customer Experience	Video Streaming Analytics	Wholesale Management	Steering of Roaming
National Network Testing	SITE dSTest (lab)					Enterprise Account Management	5G Edge Analytics	Customer Intelligence	Super Apps Intelligence	Roaming Operations	Roaming DNA
Network Service Quality Management	xAnalyzer Tracing							IoT	Device Analytics	Roaming Product / Enterprise	eSIM Monetization
Network Service Quality Management	xAnalyzer Tracing										
Network Operations	MapView Alerts NW Workspace										
Core Network	NWDAF NEF										



best-in-class, **award-winning** portfolio of solutions

Rich innovation – **200+ patents**

A world-class Machine Learning and Analytics framework

Global, skilled team with **deep domain focus**

Industry-leading customer footprint across verticals – 3 in 4 operators now use Mobileum

Financial Strength and Leverage

Efficient delivery, and 24/7 support and ops, via 25+ global locations

Rich cloud and managed operations and services capabilities

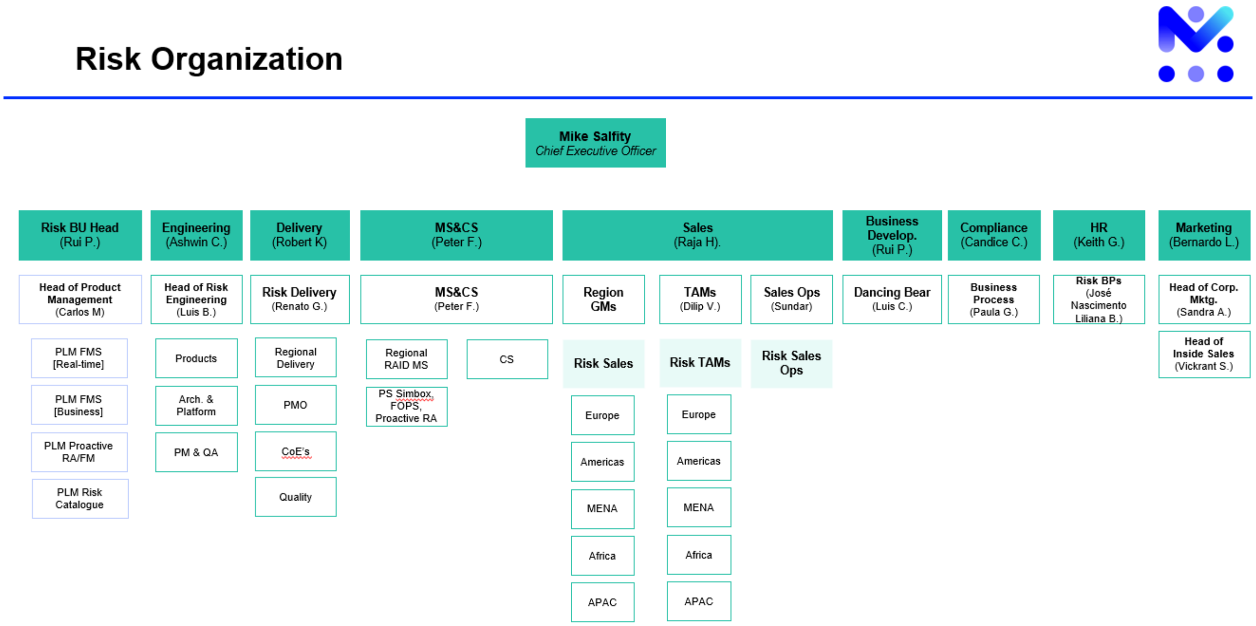
What is Mobileum’ s Risk BU Commitment?

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 and Executive team:

Please go to Mobileum site: **Executive Team | About | Mobileum**

Mobileum Risk BU’s Internal Organization



Risk Organization

Mike Salfity
Chief Executive Officer

Risk BU Head (Rui P.)
- Head of Product Management (Carlos M)
- PLM FMS [Real-time]
- PLM FMS [Business]
- PLM Proactive RA/FM
- PLM Risk Catalogue

Engineering (Ashwin C.)
- Head of Risk Engineering (Luis B.)
- Products
- Arch. & Platform
- PM & QA

Delivery (Robert K)
- Risk Delivery (Renato G.)
- Regional Delivery
- PMO
- CoE’s
- Quality

MS&CS (Peter F.)
- MS&CS (Peter F.)
- Regional RAID MS
- PS Simbox, FOPS, Proactive RA
- CS

Sales (Raja H).
- Region GMs
- Risk Sales
- Europe
- Americas
- MENA
- Africa
- APAC
- TAMs (Dilip V.)
- Risk TAMs
- Europe
- Americas
- MENA
- Africa
- APAC
- Sales Ops (Sundar)
- Risk Sales Ops

Business Develop. (Rui P.)
- Dancing Bear (Luis C.)

Compliance (Candice C.)
- Business Process (Paula G.)

HR (Keith G.)
- Risk BPs (José Nascimento Liliana B.)

Marketing (Bernardo L.)
- Head of Corp. Mktg. (Sandra A.)
- Head of Inside Sales (Vickrant S.)

Certifications & Memberships

Certifications

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 GSMA .

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 Mobileum Risk BU world class software products.

Mobileum Risk BU is strongly committed to 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 being 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, several methodologies were created from the beginning to support the following activities:

- Managed Services, Project Management, Customer support , 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 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.

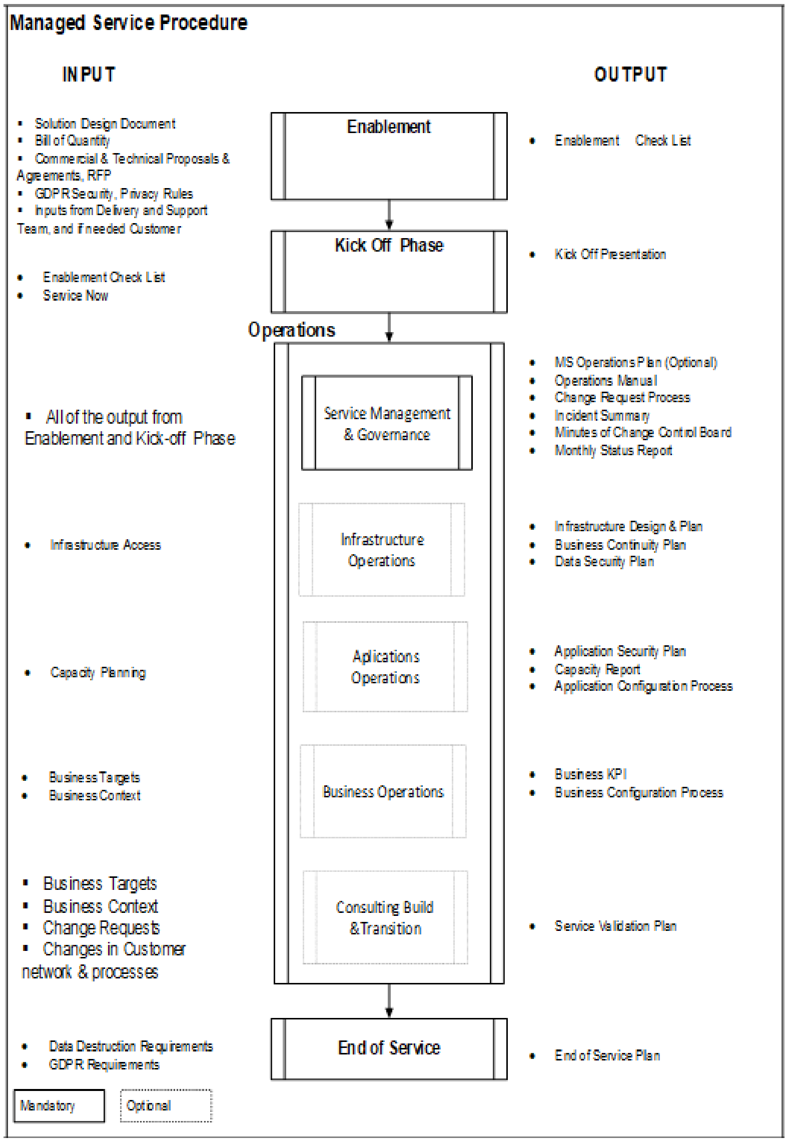


Figure 1- Managed Services Methodology

4. INFORMATION SECURITY MANAGEMENT SYSTEM CONTEXT

4.1 Objectives and Importance of Information Security Management System

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

More Business:

1-Integrate Information Security and Cybersecurity in the business objectives of Mobileum as a distinguishable and competitive factor;

Improve Operational Performance and Quality:

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

3- Ensure business continuity always keeping the highest levels of service quality.

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

Reliability, Safety:

5-Ensure that all data, albeit customer data, employee data and company data that is deemed sensitive in nature is protected from unauthorized access and disclosure;

6-Physical and logical security controls are in place to protect sensitive information;

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

The protection of information is therefore of vital importance, so that 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 on the organization´s reputation and performance.

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.

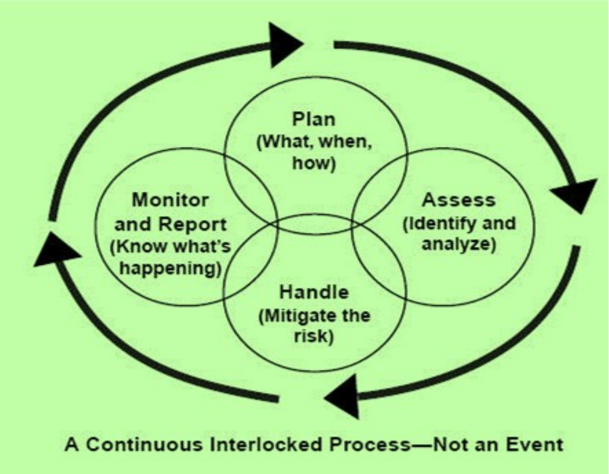

Plan (What, when, how)
Assess (Identify and analyze)
Handle (Mitigate the risk)
Monitor and Report (Know what's happening)
A Continuous Interlocked Process—Not an Event

Figure 2 - 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 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 is critical to the decision-making process at various organization levels. New threats targeting Information Systems rise, in part, due to today's society's 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 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 service rendered.

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 must 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 agreement with external entities that involve access to the information processing system should consider all relevant security requirements.

Mobileum Risk BU intends to contribute as a competitive factor and to decision-making supports. To achieve it is necessary that the organization observes security considerations in all aspects of business, 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 access is granted, in agreement with the Security management Team.

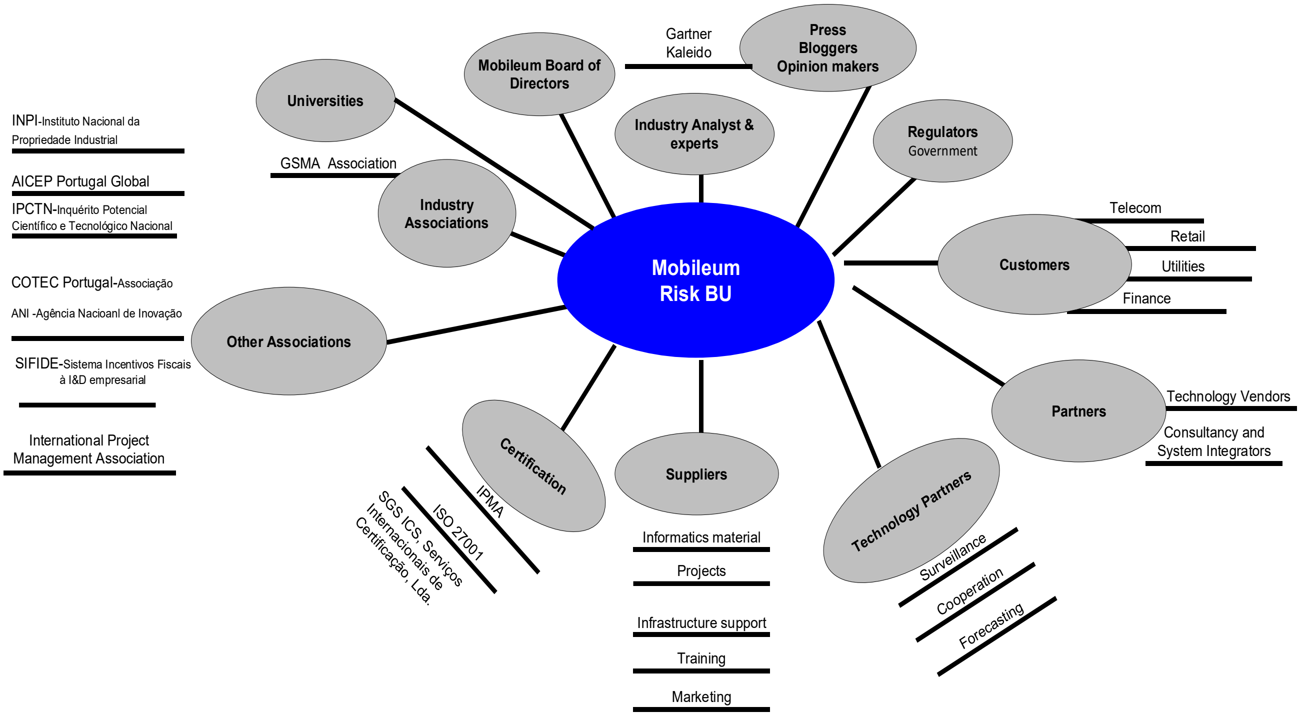

INPI-Instituto Nacional da Propriedade Industrial
AICEP Portugal Global
IPCTN-Inquérito Potencial Científico e Tecnológico Nacional
COTEC Portugal-Associação
ANI -Agência Nacioanl de Inovação
SIFIDE-Sistema Incentivos Fiscais à I&D empresarial
International Project Management Association
Universities
GSMA Association
Industry Associations
Other Associations
Mobileum Board of Directors
Gartner
Kaleido
Press
Bloggers
Opinion makers
Industry Analyst & experts
Regulators
Government
Mobileum Risk BU
Telecom
Retail
Utilities
Finance
Customers
Partners
Technology Vendors
Consultancy and System Integrators
Certification
IPMA
ISO 27001
SGS ICS, Serviços Internacionais de Certificação, Lda.
Suppliers
Informatics material
Projects
Infrastructure support
Training
Marketing
Technology Partners
Surveillance
Cooperation
Forecasting

Figure 3- Interface Management Mode

Here we have the Interface Management relation model where we have all the associations, certification entities, industry associations, Board of Mobileum Directors, 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, that will give content to the preparation of the Annual Operation Planning (AOP) and Strategic Plan Cycle of the company.

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 into 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 Technological 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 into Mobileum Risk BU Quality Management System (Compliance), 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, Product Management , Managed Service, Customer Support, are supported by 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 into Mobileum Risk BU Quality Management System.

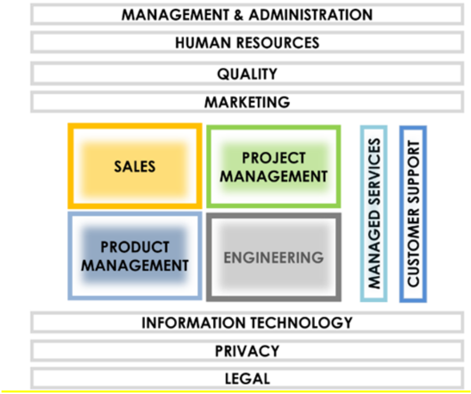


Figure 4 – Mobileum Processes Map

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

The Management and Administration Processes comprise all activities related to:

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

And it has integrated the 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 Quality Management System in the company, such as :

- Process identification;

- Determining process sequence and interaction;
- Definition of rules for document control;
- Definition of rules for register control;

The Marketing 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 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 the garnering and implementation of all the customers' 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.

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

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 license's;

Customer support Process:

Our customer support team is dedicated to building and strengthening relationships with our telecom clients who rely on our products and services, by working closely with them to identify and reduce network operating expenses and ensure customer satisfaction.

Legal process:

Legal department is responsible for keeping company's operations compliant with all the relevant laws and regulations in force. It is staffed by lawyers and legal experts, who can be considered the company's legal counsel.

4.5 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.

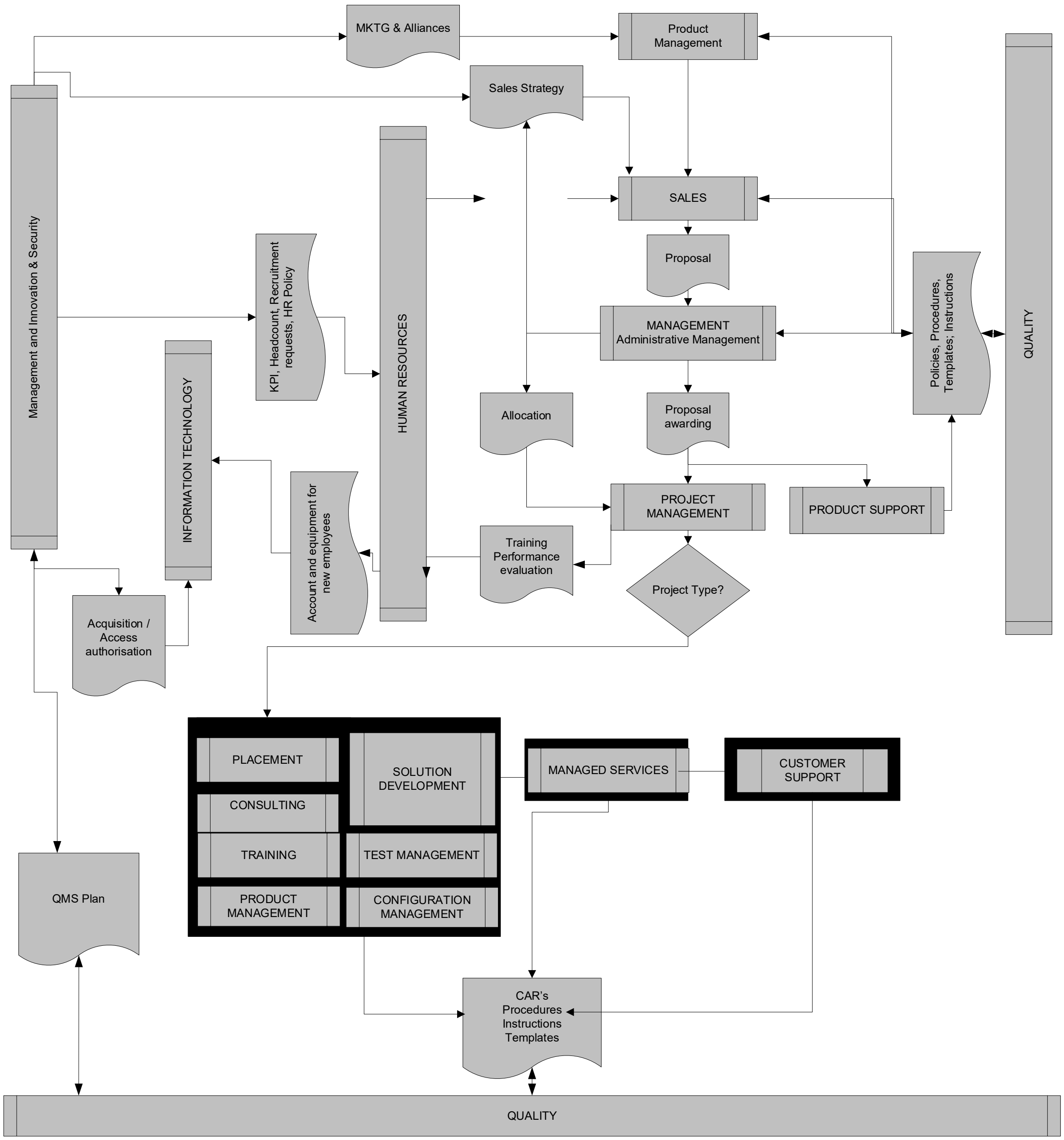


Figure 5 -Relation between processes

4.6 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 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 Emergência e Protecção Civil (National Authority for Civil Protection)

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

Comissão Nacional de Protecção de Dados (CNPD)

http://www.cnpd.pt/

Entidade Reguladora dos Serviços Energéticos - ERSE

https://www.erse.pt/

Associação Portuguesa de Direito Intelectual

Http://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**
- 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 Sta Clara e Lumiar: **210519790**
- Braga: **253 20 92 00**

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, 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 has been backed by the Management on a periodic basis, in accordance with the company's internal needs and strategic changes.

It is incumbent on the Management 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;
- It is communicated and understood within the organization;
- Strong collaboration with Partners, Regulators and with the environment where the company is incorporated in;
- 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 following the Global Mobileum Policy defined in P_MQMS_105_E-Mobileum Security Policy and completely integrated with 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 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;

As clearly identified in Mobileum Security Policy : P_MQMS_105_E-Mobileum Security Policy.

5.3 Importance of Security Policy

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

The protection of information is therefore of vital importance, so that 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.

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 specify the control objectives that should be seen as a regulatory requirement. The objectives are applied independently of the locations and technologies used:

Objectives :

More Business:

1-Integrate Information Security and Cybersecurity in the business objectives of Mobileum as a distinguishable and competitive factor;

Improve Operational Performance and Quality:

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

3- Ensure business continuity always keeping the highest levels of service quality.

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

Reliability, Safety:

5-Ensure that all data, albeit customer data, employee data and company data that is deemed sensitive in nature is protected from unauthorized access and disclosure;

6-Physical and logical security controls are in place to protect sensitive information;

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 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) Ethics
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 these 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 8).

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 level's documentation.

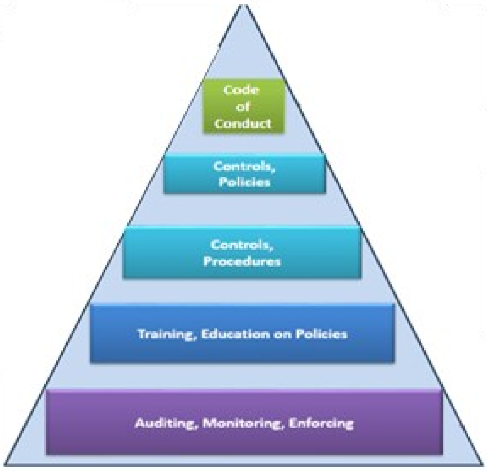

Code of Conduct
Controls, Policies
Controls, Procedures
Training, Education on Policies
Auditing, Monitoring, Enforcing

Figure 6- Information Security Policy Framework

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

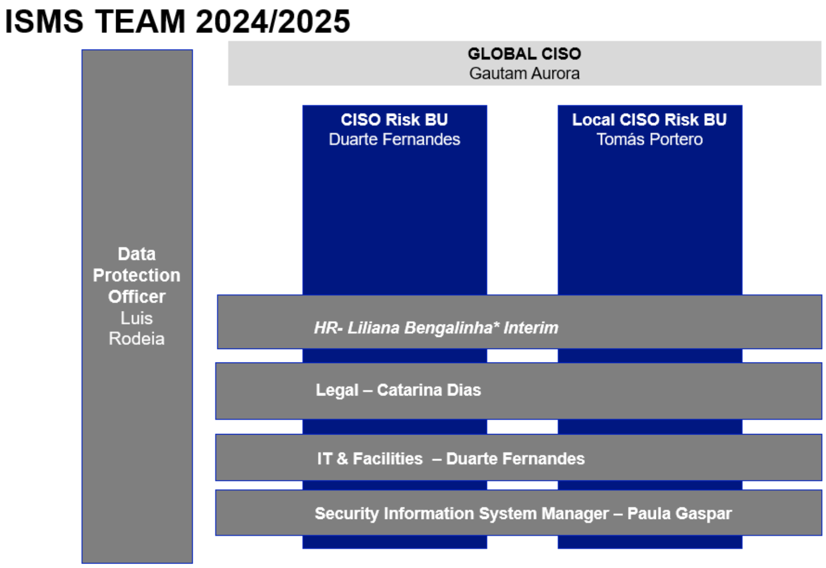


Figure 7- ISMS Organization Model

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 considered 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 Management team 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 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.

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 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 of 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 to Mobileum Risk BU Top Management.

Mobileum Risk BU Executive Management 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_MQMS_032_E – Hiring and Selection Procedure

The integration of new employees is carried out in accordance with the procedure P_MQMS_031_E- New Hires Integration Procedure.

8.2 Competence & Awareness

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 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 as much 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_MQMS_034_E – Performance Overview Procedure.

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_MQMS_030_E – Internal Training Procedure.

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_MQMS_030_E – Internal Training Procedure.

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 training is provided to the people 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:

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 whom should be communicated.

Responsibilities and roles are completely identified and communicated in this Manual 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 ensure that ISMS policy and goals are established, implemented and measured every year.

8.4 Social Media

Mobileum Risk BU believes that its presence in 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 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, microblogging (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.

Creation, reviewing, approving, publishing, archiving and extinguish rules of ISMS documentation is described in P_QMS_004_E-Document Management.

The way to generate 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 this Manual, the ISMS Security Manager activities are related with monitoring and 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_MQMS_045_E – Mobileum 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_MQMS_045_E – Mobileum Audits, 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 Team (BU and Security Management Team).

As outputs of the ISMS System review are considered:

- Actions to be implemented with the aim of improving the effectiveness of ISMS Management System;
- Possible need for Human resources, financial or technological 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 Nonconformity, 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 results, audit results, the analysis of relevant data, corrective and preventive actions and through management revision.

11. ANNEX A- PRIVACY AND PERSONAL DATA PROTECTION POLICY

11.1 Privacy and Personal Data Protection Policy

The protection of privacy and personal data of all people who somehow relate to Mobileum Risk BU (clients, users of the services, employees, partners and others) are a fundamental commitment of our Company.

These practices are described in P_MQMS_026_E – Mobileum Employees Privacy Policy and in P_MQMS_069_E - SDP - Personal Data Protection Policy.

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 Mobileum 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 has 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.

11.2 Rights of MOBILEUM' Employees, as Data Subjects

The Mobileum Employees rights are described in P_MQMS_026_E – Mobileum Employees Privacy Policy.

The Employee can exercise their rights through the following e-mail: dataprotection@mobileum.com

11.3 Employee Obligations, as Data Subject

The Mobileum Employees obligations are described in P_MQMS_026_E – Mobileum Employees Privacy Policy.

MOBILEUM has policies, standards and internal procedures in place related to information security management, computer equipment usage, MOBILEUM' Client's information processing, and Quality management, among others, effectively communicated to its Employees.

It is the duty of the Employee to know and apply the said procedures, policies, and standards in the performance of their work activity, ensuring, in particular, at all times the maximum confidentiality and integrity of MOBILEUM' proprietary information.

Failure to comply with the mentioned policies, standards and procedures by the Employee may lead to disciplinary proceedings, without prejudice to possible civil and/or criminal liability of the breaching Employee.