

# COMPANY PROFILE

—  
NOV  
22







Obiettivo is specialized in information and cyber security service



### Cross-industry Experience

More than 10 years of experience serving major companies in

- Automotive
- Defense
- Communications & Technology
- Utilities
- Financial and Insurance Services
- Industrial Products & Services
- Health & Life Sciences
- Retail



### Core competencies

Our advisors transfer the skills gained in different markets

- Information & Cyber Security Strategy and transformation
- Information Risk Management
- Information Risk Governance
- Operational Excellence
- Information Security
- Cyber Risk and Security
- Information Security Education
- Information Security Service



### Combined expertise



The first private non academic Italian Business & Management School

THE GROUP

# TAILORED SECURITY APPROACH

Obiectivo develops a strategic and «tailor-made» approach for customers, which includes all the elements relevant to their business. In the absence of this point of view the strategy will be partial and ineffective

## ORGANIZATION & GOVERNANCE

**Governance structures:** to define and control risk levels and to select appropriately trained “talents” and personnel to spread the “risk culture”

## INFRASTRUCTURE

**Security infrastructure:** properly designed, implemented and governed to support information security processes



### Cyber Risk Management Strategy

A “tailored” strategy, which addresses by 360° the management of information/cyber risk, requires a correct address of its fundamental components by a continuous auditing and compliance process

## POLICY, STANDARD & LEGAL

**Security Policies:** to implement the strategy and adapt it to standards/regulations

## PROCEDURE


**Security Procedures:** for the alignment to cybersecurity strategies and policies


# **OBIETTIVO OFFERING**


We have developed a unique value proposition to assist our customers in the most complex transformation process in Information & Cyber Security


**NOT EXHAUSTIVE**


## Information & Cyber Security Pillars

 Cyber Security Advisory & Analysis

 Cyber Security Skills Improvement

 Service +

 Application & Information Security Management

 Legal & Compliance



## Obiettivo Offering

**Assessment & RA,**  
Tech Ass,  
Gap/Risk Analysis BSA,  
BIA  
**Quantitative RA**

**Sicurezza OT/IOT**

**Business Continuity Management**

Awareness, **Cyber Talk**; Coaching, Virtual Education....

DPO as a service/support, CISO as a service/support, Third Party Assessment & Audit, Assessment & Audit as a service, Process Simulations, Crises Event Simulations, Audit Privacy Simulations.

**Secure SW development**

**Secure Architecture**  
Security Infrastructure Architecture  
Supplier Selection

**Compliance Iso/lec 27x;** GDPR; 62443; Nis, 285/BCE, Gefia, Ivass.....

## Offering Dimension

 **Cyber Risk Management Strategy**

Policy, Standards e Legal

Organization e Governance

Procedure


Physical Infrastructure and technology


 **Audit & Compliance**


NOT EXHAUSTIVE


## Information & Cyber Security Pillars

 Cyber Security Advisory & Analysis

 Cyber Security Skills Improvement

 Service +

 Application & Information Security Management

 Legal & Compliance



### Cyber Jumanji\*

Service based on an immersive simulation platform used to test critical procedures and evaluate their applicability. It helps to analyze vulnerabilities and generate remediations plan

### RiskOut\*\*

Platform for the third party management, evaluation and audit. Based on industry standards and regulations it evaluates and assigns a score to suppliers based on the services they are applying for

### IACS Framework\*\*

Risk assessment and management Solution for industrial environments. Analysis of the technological and organizational part that allows to quantify the risk for single item

### Threat Modeling

Threat modelling for new services and innovative products. Through an accurate study we define the most probable risk scenarios and test the vulnerabilities of the solutions

\*Service based on an Obiectivo exclusive licensed platform

\*\* Proprietary framework developed on the basis of international norms and standards

NOT EXHAUSTIVE

## Information & Cyber Security Pillars



Cyber Security Advisory  
& Analysis



Cyber Security Skills  
Improvement



Service +



Application & Information  
Security Management



Legal & Compliance

### Cyber Talk

Short but intense talks held by high-level speakers which aim to rise awareness levels among the organizations top managers, in an engaging TED talk like mode

### Cyber Specialization\*

Training that helps fill the GAP of technical skills and operationally test the knowledge gained in e-lab built on real scenarios

### Cyber Arena\*

Hyperrealistic simulation platform that allows organizations to train teams through computer attack experiments in a simulated, secure and controlled environment

### Cyber Culture

Communication campaigns of high Impact developed with the logic of educating by entertaining in order to stimulate a virtuous attitude of internal staff and stakeholders

\*Platform of virtual learning & e-lab

NOT EXHAUSTIVE

## Information & Cyber Security Pillars



Cyber Security Advisory & Analysis



Cyber Security Skills Improvement



Service +



Application & Information Security Management



Legal & Compliance



### Ciso as a service/support

Not all companies have an internal department for cyber security, which is why we give the opportunity to rely on our structure either for ongoing support or for a full outsourcing of the CISO function

### DPO as a service/support

Not all companies have an internal organization for data privacy, which is why we give the opportunity to rely on our structure for either continuous support or for a full outsourcing of the DPO or the entire management of GDPR compliance

### Third Party Assessment

The verification of third parties is a fundamental aspect in cyber governance, for this reason we have created an assessment / audit as a service



NOT EXHAUSTIVE

## Information & Cyber Security Pillars



Cyber Security Advisory  
& Analysis



Cyber Security Skills  
Improvement



Service +



Application & Information  
Security Management



Legal & Compliance



### Service Design

**Design of services, solutions and architectures**, vendor identification, product selection, solution validation

### Sw Threat Modeling

**Threat modelling of critical or innovative software.**

Through a study we define the most likely and impactful risk scenarios and test the vulnerabilities of the solutions

NOT EXHAUSTIVE

## Information & Cyber Security Pillars



Cyber Security Advisory & Analysis



Cyber Security Skills Improvement



Service +



Application & Information Security Management



Legal & Compliance



### 285/BCE/Gefia (Financial Services)

Gap & maturity analysis, mitigation plan.  
Assessment model, Risk analysis framework\*, audit plans

### IVASS (Insurance)

Gap & maturity analysis, mitigation plan.  
Assessment model, Risk analysis framework\*, audit plans

### 62443\* (Industry)

Gap & maturity analysis, mitigation plan.  
Assessment model, Risk analysis framework\*, audit plans

### NIS (Critical infrastructure)

Gap & maturity analysis, mitigation plan.  
Assessment model, Risk analysis framework\*, audit plans

\* Proprietary framework developed based on international norms and regulations

# CUSTOMIZED APPROACH TO SPECIFIC BUSINESS RISKS

We support your organization with a 4 step approach

## Planning & Setup

Setup a programme to deliver the remediation required and PMO support

- **How to setup the execution structure?**
- **What governance and processes are required?**



4

## Gap Analysis and prioritization

Identification of required remediations and prioritisation of intervention based on agreed criteria.

- **Which are the gaps?**
- **Which are the prioritisation key drivers?**



2



## Initial Diagnostic

Analysis of the possible impact of regulations and standards compared to existing services and planned activities

- **Which services are impacted?**
- **Which are the requirements?**
- **Which are the best practices?**

1

3

## Options assessment and implementation planning

Explore options available (e.g.build/buy/outsource)

- **How to evaluate the options?**
- **What changes are required to the operating model?**





 **ROME | MILAN**

 **+39 06 99704927**

 **info@obietivo.it**