POLICY

Governance, Risk Management, Compliance (standard ISO 37301 and ISO 31000)

Dear Customer,
Dear Collaborator,
Dear Supplier,
Dear Business Partner,
Dear Consortium Member,

We built our success by managing in an integrated way all aspects of governance, risk management and compliance related to our innovative business model. This has allowed us to maintain and develop our reputation as a recognized and reliable competence center, able to meet the different needs of our customers.

Our business context

We are a joint stock cooperative consortium (our business name). Our consortium members (shareholders) are represented by micro and small medium enterprises, each of which represents a Subject Matter Expert.
We hold minority interests in other associated companies.
Due to our business name we are subject to auditing both by a ministerial auditor and by a statutory auditor.
Our mission is to provide professional services to businesses (consultancy, training, audit and business assurance). We support our customers in the delicate task of ensuring compliance of their business with mandatory and regulatory, technical, contractual and internal requirements.
We operate in different industries, in different geographical areas and with different types of customers. We must ensure to our customers and in general to our stakeholders adequate levels of governance, risk management and compliance in the performance of our processes, in the management of our resources and in the provision of our services.

Our commitment for Governance, Risk Management, Compliance Management

By this policy we are committed to adopting and incorporating the following principles for governance, risk management and compliance into our business model, processes and services provided by us:

1. Management of governance by assigning roles, responsibilities and authorities at the level of the governing body, of the management, of the organizational area, of the single process and of the single project;
2. Risk management at company, business area, organizational area, process and service level;
3. Management of compliance with legal and regulatory, contractual, technical and internal requirements (policies and ethical codes);

We adopt a policy for Governance, Risk Management and Compliance. This policy is communicated to all our stakeholders and is available on our website www.minervagroupservice.com

Our Governance, Risk Management, Compliance Management Objectives

Our commitment

We are committed to pursuing governance, risk management and compliance objectives in a systematic and planned manner and to integrating them into more general strategic and operational objectives.

Picture 1 strategic objectives, GRC objectives and operational objectives

Strategic objectives

GRC objectives support the pursuit of our strategic objectives. Strategic objectives include:

1. economic and financial objectives;
2. competitive objectives, related to our positioning on the market;
3. stakeholder satisfaction objectives;

GRC objectives

The objectives of the Integrated Management System support the pursuit of our GRC objectives. GRC goals include:

1. Governance objectives. These objectives are related to the objectives of identifying and managing the stakeholders, to the objectives of correct assignment of roles, responsibilities and authorities at the various levels of the organization (including processes and projects), to the objectives of planning processes and related deliverables, to objectives of provision and development of resources (financial, physical infrastructures, IT infrastructures and Services, human resources and their skills, documented information), control and review objectives, objectives of continuous improvement;
2. Risk Management objectives. These objectives are related to risk assessment objectives and risk treatment objectives through the identification and application of operational controls (control objectives).
3. compliance management objectives. These objectives are related to objectives for monitoring and assessing compliance with the legal and regulatory, contractual, technical and internal policy requirements applicable to the business context and to the services provided to our customers.

In particular, we have defined the following criteria for risk evaluation and related acceptability:

1. Risks of loss of compliance: all risks of compliance with legal, regulatory, contractual and technical requirements are unacceptable to us. These risks must be reduced to the reasonably lowest possible level ("alarp"). Even if these risks are already assessed at a low level, further operational controls for the treatment must be prudently applicable.
2. Reputational risk: all reputational risk is unacceptable to us. These risks must be reduced to the reasonably lowest possible level ("alarp"). Even if these risks are already assessed at a low level, further operational controls for the treatment must be prudently applicable.
3. Risks of loss of transparency and ethics: all risks of loss of transparency and ethics are unacceptable to us. These risks must be reduced to the reasonably lowest possible level ("alarp"). Even if these risks are already assessed at a low level, further operational controls for the treatment must be prudently applicable.
4. Risks of loss of fundamental rights and freedoms: all risks of loss of fundamental rights and freedoms (including risks related to occupational health and safety, the processing of personal data, discrimination) are unacceptable to us. These risks must be reduced to the reasonably lowest possible level ("alarp"). Even if these risks are already assessed at a low level, further operational controls for the treatment must be prudently applicable.
5. Risks of loss of innovation opportunities: all risks of loss of significant innovation opportunities are unacceptable. All innovation opportunities must be identified and assessed.

Integrate Management System objectives

The objectives of the Integrated Management System include the objectives applicable to the following organization models and management systems:

1. crimes prevention objectives referred to in Italian Legislative Decree 231/01 (corporate criminal liability) as described into our code of ethics available on our website www.minervagroupservice.com);
2. Transparency, integrity and antibribery Objectives (ISO 37001 standard) as described into our anti-bribery policy available on our website www.minervagroupservice.com;
3. Quality objectives (ISO 9001 standard) for the conformity of our services provided and the satisfaction of our customers as described into our quality policy available on our website www.minervagroupservice.com);
4. Innovation objectives (ISO 56002 standard), as described into our innovation policy available on our website www.minervagroupservice.com);
5. Business Continuity objectives (ISO 22301 standard), as described into our business continuity policy available on our website www.minervagroupservice.com);
6. Information security objectives (ISO 27001 and ISO 27701 standards), as described into our information security policy available on our website www.minervagroupservice.com);
7. Personal data protection objectives (GDPR) and related information for data subjects, as described into our data protection policy available on our website www.minervagroupservice.com ;

Our Integrated GRC Management System

In order to pursue our GRC objectives in a systematic and integrated way, we have adopted an integrated management system that includes governance and internal control system aspects, risk management aspects (with reference to the guidelines of the ISO 31000 standard) and aspects of Compliance (with reference to the ISO 37301 standard).

The GRC Integrated Management System includes different organization models and management systems that address different management areas: Ethical Code of Legislative Decree 231/01, ISO 9001 Quality, Data Protection GDPR, Information Security ISO 27001 and ISO 27701, Business Continuity ISO 22301, Innovation ISO 56002.

We have appointed a manager of the integrated management system (ISO System Manager) with the task of planning, implementing, controlling and improving our integrated management system. We have also set up a Project Management Office (PMO) to uniformly address the management of all our projects (internal projects and projects related to the services provided to our customers) with reference to the guidelines of the ISO 21500 standard (project management).

We are committed to continually adapt and improve our GRC Integrated Management System and to make aware and train our stakeholders on its correct application.

Our contact channels

For any report of vulnerabilities, threats, opportunities for improvement, non-compliance you can contact our ISO System Manager at the following email address: PMO@minervagroupservice.it

Minerva Group Service