SandaS GRC

Manage your organization's risks and legal and security requirements efficiently and in a unified way

SandaS GRC helps organizations support their business strategy, improve their operational performance, reduce operational risks and ensure regulatory compliance, by integrating their key processes around three strategic domains: Corporate Governance, Risk Management and Regulatory Compliance. SandaS GRC is the perfect complement to create an effective program for the governance, risk management and compliance of your organization's information security.

Corporate Governance

It provides information that helps you with the decision-making to ensure that information security is aligned with your organization's aims and targets.

Risk Management

It allows security risk identification, evaluation, analysis and processing at a technical and compliance level, minimizing their impact on your business.

Regulatory Compliance

It helps to implement the best international practices on management systems and the compliance with the legal and contractual requirements in order to develop you business with the highest guarantees.

Benefits

- It helps to develop and prove compliance with legislation (DPL "Data Protection Law", ENS "Esquema Nacional de Seguridad", critical infrastructures...), international standards (ISO 27001, ISO 27002, ISO 22301, PCI DSS...) and corporate policies in an efficient and centralized way.
- Full and unified view of the risk helping to manage the key risks and normative and regulatory compliance problems in the organization, minimizing their impact on the business.
- It allows to conduct a strategic assignment of resources and to ensure the appropriate controls for an integral security plan.

Target Group

- Public and private bodies that need to ensure their security and properly manage risks.
- Organizations that need to meet obligation and internal policies imposed by legislators, regulators and clients.
- Companies that need to shield and protect information in order to maintain the confidentiality, availability and integrity of it.
- Organizations that need to have a comprehensive and unified view of their security, covering both operational and business aspects.

Technical Features

- Risk identification and management based on ISO 31000 with full support to frameworks such as ISO 27005, NIST SP 800-30 or COBIT 5 for Risk.
- Specific module for MAGERIT with support to the National Security Framework (ENS, "Esquema Nacional de Seguridad") and legislation on Critical Infrastructures based on the Logical IT Processing for Risk Analysis (PILAR, "Procedimiento Informático Lógico para el Análisis de Riesgos").
- Modeling of your organization's assets according to the TOGAF9.1 and Archimate reference standards.
- First international implementation of the measurement standard of Information Security ISO 27004:2009.
- Check of the security of IoT deployments according to GSMA IoT Security Guidelines & Assessment.