CORA
CYBERSEC

CyberSec. Information security Management system.

CORA CyberSec is part of the **GRC CORA** solution, a multi-compliance software platform that allows you to manage, in a single synergistic system, more regulations, binding and non-binding, optimizing the time of implementation and management. The modules can be activated independently. Upon activation, the new module will inherit the information it has in common with the other elements already operational. **GRC CORA** is available in **SaaS** and **OnPremise** mode to better accommodate the needs of each customer.

The regulatory environment

The new challenges in **cybersecurity** require that each organization must define and apply an appropriate and unique risk assessment process that can:

- **Establish** and **maintain** safety risk criteria including both criteria for risk acceptance and criteria for risk assessment;
- **Ensure** that recurrence of risk assessment results are consistent, valid and comparable;
- **Identify** security risks through an assessment process that identifies all critical factors associated with the loss of confidentiality, integrity and availability of information and data;
- To **analyse** safety risks by comparing the results of the analyses carried out with the risk criteria defined above and by setting priorities for action in order to produce an appropriate treatment plan.

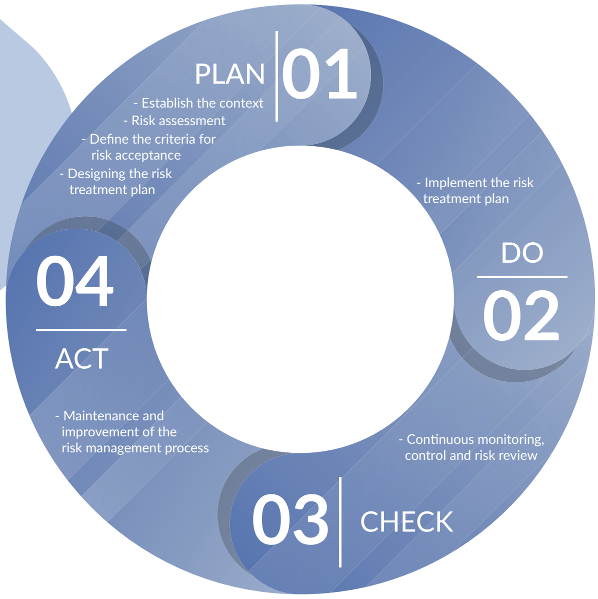
The treatment plan can be carried out by applying appropriate countermeasures or controls, drawing from the following best practices: **Annex A “Control objectives and controls”** of **ISO 27001**, Cloud Controls Matrix (**CCM**) of **CSA Star**, **CIS Controls**, **NIST Controls List**, **Minimum Security Measures Agid for the PA**, etc...

The solution

The adoption of **CORA CyberSec** allows to:

- Provide operational support both during the risk assessment process and in the subsequent maintenance phases;
- To guide the operation of the different actors within the activities of detection and measurement;
- Manage interactivity between the different actors involved;
- Structure and host, in your repository, the set of information and documents to support the entire process ensuring:

✓ Correctness and uniqueness of data and documents;
✓ Correct distribution of information within the corporate structure;
✓ Confidentiality of data and documents;
✓ Information stored on a historical basis.


PLAN 01
- Establish the context
- Risk assessment
- Define the criteria for risk acceptance
- Designing the risk treatment plan
- Implement the risk treatment plan
DO 02
- Continuous monitoring, control and risk review
03 CHECK
- Maintenance and improvement of the risk management process
04 ACT

CORA
CYBERSEC

CyberSec.
Information security Management system.

The main features

- Register of processes and services;
- BIA (Business Impact Analysis);
- SRA (Security Impact Analysis);
- SOA (Declaration of applicability under ISO 27001);
- Audit and non-conformity.

In short

INFRASTRUCTURE

Risk management and calculation on business infrastructure

REGISTER OF PROCESSES AND SERVICES

Census of processes and services to be monitored in the field of safety

RISK ANALYSIS

BIA
(Business Impact Analysis)
SRA
(Security Impact Analysis)

SOA

Creazione della Dichiarazione di applicabilità in caso di adozione dello standard ISO 27001

AUDIT AND NON-CONFORMITY

Audit plans and programmes;
Identification of non-conformities;
Application of corrective actions

A simple, complete, scalable compliance suite.

GRC CORA

CORA CYBERSEC is part of the GRC CORA solution.

GRC CORA is a customizable and modular solution according to the specific needs of each reality.

AGID | Cloud Marketplace

You can find us on Marketplace AgID
Cloud Services Catalog for Qualified PA