/ 2021

wisesecurity
GLOBAL

CISOaaS

wisesecurity
GLOBAL

CISOaaS

SECURITY OFFICE – GENERAL VIEW

INTERNAL & EXTERNAL COMMUNICATION PLAN (EMPOWERED BY BOARD)

CYBERSECURITY PLAN

DIAGNOSIS	STRATEGY FORMULATION	ROADMAP
RISK ANALYSIS Y THREATS OF CYBERSECURITY	GOALS, LINES, INITIATIVES	INITIATIVES PRIORIZATION
SWOT	PRIORIZATION COST/PROFIT	CONTROL PANEL FOLLOW UP

PLAN&BUILD

RUN

CISOaaS

Initiatives to protect the Organization's assets:

- Critical Information Systems
- Cross Information Systems
- People
- Cybersecurity culture
- Compliance

PROPOSED SOLUTION

CISOaaS

Wise Security Global has designed a model based on the figure of **CISO as a Service** **adaptable to any risk scenario in the company**. This is a service specially designed for companies that **need a figure that manages their cybersecurity but do not need a full-time CISO or can not afford it**.

We plan and build while we run the correct actions in order to implement the Cybersecurity function of our customers.

- Continuous expert support in cybersecurity technology: organizational, legal/normative, procedural and technological environment.
- Support during the definition process, selection and training for the future CISO
- Coordination during the security labors, from governance to the technical part.
- Report and continuous coordination with C-Level.
- Contact with internal & external stakeholders to ensure the implementation of the best practices.
- Analysis and treatment of the identified risks.
- Collectives identification and definition of an awareness plan on cybersecurity addressed and adapted to each of them.
- Policies and documents of security documentation (information classification, devices security configuration, technical procedures…).

PROPOSED SOLUTION

PLAN & BUILD: CYBERSECURITY PLAN

We get a global view of the company by working on a **Cybersecurity Plan** in order to create a solid structure of cybersecurity inside the organization by aligning the cybersecurity objectives with the own of the organization.

Wise Security Global has designed a methodology based on the identification of the organization main risks and weakness in order to, subsequently, be able to define a strategy in a period, adapted to the own needs and in line with the objectives of the business.

- Diagnosis of the current cybersecurity situation.
- Interviews with relevant members.
- Review of existent and valid cybersecurity documentation.
- Risk determination and elaboration of the correspondent SWOT.
- Formulation of the strategy to follow (goals, axis and initiatives for next years)
- Validation sessions with responsibles.
- Priorization of cost vs benefit and scheduling of initiatives.
- Final customed-tailored cybersecurity roadmap.

CISOaaS

PLAN & BUILD: CYBERSECURITY PLAN

DIAGNOSIS (RA & SWOT) / **STRATEGIC FORMULATION** / **STRATEGY DEPLOYMENT PLANIFICATION**

PHASE 1: Diagnosis

01/ Internal Analysis

Internal analysis of the current situation of the cybersecurity function

02/ External Analysis

External analysis with the perspective of the environment, trends and innovations at a national and international level

03/ SWOT Analysis (Includes AR)

Evaluation of the current situation of the field with a SWOT and AR cyber approach.

PHASE 2: Strategy formulation

04/ Strategic Aspiration

Strategic reflection and construccion of the strategic aspiration and strategic map

05/ Definition of the objectives and strategic lines, and associated initiatives

Definition of the main actions to be implemented for each of the objectives and/ or strategic lines.

06/ Definition of detailed initiative files

Detail in files of the prioritized initiatives to implement.

07/ Initiative/ program prioritization

Prioritization of the initiatives to be implemented (Cost-benefit matrix)

PHASE 3: Planning the deployment of the strategy (Master Plan)

08/ Definition of the Implementation Plan

Define the Implementation Plan of the defined initiatives.

09/ Definition of the Plan Monitoring Scorecard

Definition of the Scorecard to evaluate the degree of implementation of the Master Plan.

CISOaaS

SECURITY OFFICE: CISOAAS SERVICE

We plan and build while we run the correct actions in order to implement the Cybersecurity function of our customers. Our working method is based on protecting the main organization's assets: Critical Information Systems, Cross Information Systems, people of the organization, Cybersecurity culture level and compliance.

- Diagnosis of the current cybersecurity situation.
- Interviews with relevant members.
- Review of existent and valid cybersecurity documentation.
- Risk determination and elaboration of the correspondent SWOT.
- Formulation of the strategy to follow (goals, axis and initiatives for next years)
- Validation sessions with responsibles.
- Priorization of cost vs benefit and scheduling of initiatives.
- Final customed-tailored cybersecurity roadmap.

Phase 1

Context understanding

- Industry type
- Main necessities

Identification

- Organization processes
- Management areas
- Interlocutors

Execution planification

- Information recopilation method
- Necessary efforts estimation

Phase 2

Information recopilation

- Interviews with interlocutors
- Documented information existent identification
- General infraestructura identification
- Evidence capture

Analysis

- Identified information registration and clasification
- Analysis model application
- Results obtention

Phase 3

Results report creation

- Current compliance level
- Desired compliance level
- Correlation of findings

Results report delivery

- General report of delivery
- Identified strenghts and weaknesses
- Recommendations and comments

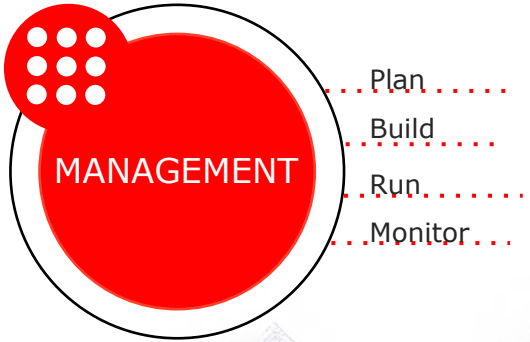
*Standardization methodology phases

PROPOSED SOLUTION

SECURITY OFFICE: CISOAAS SERVICE

METHODOLOGY AND FRAME OF REFERENCE APPLIED TO THE CISOaaS SERVICE

**Methodology detail*



Operation: CISOaaS

- Corporative strategy of Information Security
- Normative Compliance
- Risk analysis
- Action Plans of Security Incidents
- Risk Management of Supplier Security
- Awareness and Training
- Business Continuity
- Identity management, authentication and access control
- Petitions approval and Security exceptions

EMAIL
sales@wsg127.com

WEB
www.wsg127.com

wisesecurity
GLOBAL

THANK YOU!