BASE4 SECURITY

We help building a

more secure digital ecosystem!

Security Risk and Compliance

DATA SHEET

General aspects of the area

We work in the area in an integrated and systemic way to address governance, risk and compliance (GRC) of Information Security.

BASE4 Security's services seek to ensure ethically correct actions in accordance with the level of risk acceptable to the organization (risk appetite), taking into account its internal policies, external regulations and compliance frameworks taken as a reference.

This is achieved through an alignment of corporate and cybersecurity strategy, processes, technology and people.

GRC Principles

- Achievement of business objectives through the joint work of all those involved.
- Timely, reliable and useful information for those responsible for execution on risks, incentives and responsibilities.
- Improving organizational culture by promoting accountability, integrity, reliability and communication.
- Increased stakeholder confidence.
- Organization prepared to manage risk.
- Detection, prevention and reduction of adverse situations or weaknesses.

- Motivation and inspiration to encourage desired behavior, especially in the face of new challenges.
- Permanent state of alert for new opportunities.
- Improved response and efficiency as a competitive advantage.
- Maximization of economic return and value generation.

Cybersecurity Governance comprises the framework, principles, structures, processes and best practices that establish the direction, monitoring and performance of Information Security.

Governance and management

- Virtual CISO (VCISO)
- Advice for the preparation of a Cybersecurity Master Plan (IS Strategy).
- GAP analysis (Information Security Maturity Level Determination)
- Preparation of a “Road Map” (corrective actions and opportunities for improvement in the short, medium and long term).
- Documentation and review of IS policies and procedures (controls by opposition).
- IS strategic management tools (Annual Operating Plan, metrics and indicators).
- Alignment to compliance frameworks, international standards and IS best practices (ISO, CIS, PCI, SOX, COBIT, BCRA, NIST, others).
- Information Security Management System (ISO 27001).
- Business Continuity Management System (ISO 22301).
- Cyber Resilience: Contingency Plan / BCP (Business Continuity Plan) / DRP (Disaster Recovery Plan).
- Advice for the implementation of Digital Signature.
- Industrial Safety - OT
- Preparation of executive reports for management.
- Information Security Awareness and Training.

Risk Assessment and Management is the process by which the probability of occurrence of a situation and its possible consequences are analyzed. In addition, appropriate decisions are made to reduce the risk to an acceptable level (risk appetite).

Risk

- Evaluation, management and treatment of operational and IT risks (ISO 27005 / ISO 31001 / COBIT 5 / Magerit / COSO / BCRA / Others).
- Preparation of Risk Matrix associated with projects.
- Inventory of Information Assets (CMDB).
- Information asset classification and labeling methodologies (ISO 27002)
- (Bussiness Impact Analysis).
- BIA Analysis uditorías de cumplimiento.
- Design of IS controls (Annex A - ISO 27001 / CIS Critical Security Controls).
- Risk metrics and indicators.
- Preparation of executive reports for management.
- Risk-based thinking (ISO 9001), corrective actions and opportunity for improvement.

Compliance is an independent function that identifies, advises, alerts, monitors and reports compliance risks in organizations, i.e. the risk of being penalized for legal or regulatory non-compliance, suffering financial loss or reputational damage due to failure to comply with applicable laws, regulations, codes of conduct and standards of good practice.

Compliance

- GAP ISO.
- Compliance audits: ISO, SWIFT, PCI, SOX, BCRA.
- First (internal) and second party (stakeholder) audits. According to ISO 19011 guidelines.
- Legal framework: personal data law, privacy, digital signature,

computer crimes.

- Audit report with findings and opinion on the reasonableness of compliance with the framework requirements.

Services

Creation of policy

Preparation and review of Information Security policies and procedures, taking into account documentary requirements established by international standards.

GAP Regulatory analysis

Preparation and review of Information Security policies and procedures, taking into account documentary requirements established by international standards.

Information Security Master Plan

Advice for the preparation of a Cybersecurity Master Plan (IS Strategy). Elaboration of a “Road Map” (corrective actions and opportunities for improvement in the short, medium and long term).

vCISO

It is a consulting service that helps executives, IT and Information Security teams to protect information assets, while supporting their operations without having to focus on the core business. BASE4 Security helps to design the best Information Security strategy, taking into account the particular characteristics of your organization.

Risk Management

Identification, assessment, management and treatment of operational and IT risks and opportunities (ISO 27005 / ISO 31001 / COBIT 5 / Magerit / COSO / BCRA / Other)

BASE4
SECURITY

www.base4sec.com