




Service brief - CISO as a Service

Entregables
pueden ser
producidos en español 

CISOaaS is a consulting service assuming responsibilities and activities within the following 4 quadrants/categories:

Risk management, Audits and Compliance

Work within frameworks such as NIST, ISO-27k, PCI-DSS ...
BIA / BCP
Risk mgmt, Audits

Technical Security Operations

Vulnerability scanning,
Penetration testing,
Web application security and assessments,
Security practices (Incident Mgmt, Infrastructure and platform Mgmt, Monitoring and event Mgmt, Service continuity Mgmt, Service validation and testing)

Technical Security Architecture

Secure development practices,
Server hardening,
Network and application architectures,
IAM,
Email security,
Ingress and egress security, filtering and monitoring,
Security architectural components (NGFW, IDS, WAF, Secure web gateways...)

Governance, Policies, Awareness

Elaboration of Security policies, guidelines,
staff training and workshops,
support for strategic decisions



Scoping and priorities. From the start we analyze the organization's needs mapped into the 4 quadrants above, and determine where to focus the efforts. The resulting prioritization can be continually reassessed during the engagement

Brought to the table

- Outside-in view on your organization's security posture.
- Scalable consulting service.
- Long and vetted experience from Cyber Security, Software engineering, IT, Team Mgmt. Consulting.
- Bound to code of ethics of **ISACA** and **ISC2**
- Transparency and best practices adherence around customer data retention and confidentiality.
- Flexibility and "Slider adjustment" for focus on Operational VS Governance activities.

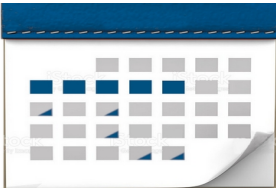


Deliverables (according to agreement)



Hardening of assets and implementation of controls,
 Scanning and assessments of networks and hosts,
 Incident analysis, Proof-Of-Concepts, Feasibility assessments and implementations of strategic products and infrastructure components, Scripting and development, Audit reports, Business Impact analysis, Internal awareness efforts (workshops and training), Governing documents (policies etc), ...

Examples of engagement formats



Continual CISOaaS engagement

Continually assuming responsibilities and work tasks within the 4 quadrants described above. Deliverables as is outlined above and according to agreement.
Monthly 5 x 8 hours full-time scheduled on premise or remote.
Additionally up to 10 hours on-demand availability on monthly basis.



Intermittent / Occasional Workshops

Work sessions with stake-holders within operations and management to outline cyber security risks, debt and objectives. Scoping and prioritization of future work tasks and initiatives. Will be compiled in report with suggestions and scenarios.
2 x 8 hours on premise.

Member of:

