RSECURE

CISO as a Service

Take control of your IT security with the help of our cyber security experts!

MADE IN LUXEMBOURG

The role of the CISO (Chief Information Security Officer) is crucial in ensuring that the company's sensitive information is protected against potential threats, such as cyber attacks, data breaches and other IT security risks.

The main responsibilities of a CISO include defining and implementing information security strategy, risk management, compliance with standards and regulations, overseeing security operations, incident management, raising staff awareness, technology watch, and working with other departments to ensure a holistic approach to security within the organisation.

THE CISO'S MISSIONS

◆ Writing and implementing security policies

◆ Phishing tests

◆ Security awareness training

◆ Security risk management and analysis

◆ Advice on regulatory compliance

◆ Management of security tools

◆ Audit

◆ Implementation of international standards such as ISO 27001 - ISO27005 - DORA - NIS 2 - CSSF - …

◆ and many more!

WHO SHOULD USE THIS SERVICE ?

CISO services are aimed at all companies that are unable to appoint a security manager internally for various reasons, or to support the internal CISO .

Depending on the size of the company, hiring a CISO would not necessarily make sense because the workload would not be sufficient, or because the costs of a full-time contract would be too high!

But doing without a CISO is dangerous! Rsecure will analyse the risks, maintain the registers and advise you on all aspects of cybersecurity.

OUR PACKAGES

	1 to 15	15 to 50	51 to 100
Number of employee			
Number of CISO days/month	1,5 D/M	2 D/M	3 D/M

Human

Employee awareness

	1 to 15	15 to 50	51 to 100
Awareness training	☑		
New employee onboarding	☐	Online platform (Additional cost)	
Phishing report functionalities	☐		
Phishing campaign	2/year	3/year	4/year
Annual board training	☑	☑	☑

Tools

Monitoring & KPI'S (Monthly)

	1 to 15	15 to 50	51 to 100
M365	☑	☑	☑
Security tools (Antivirus, Endpoint management, Firewall,…)	☑	☑	☑
Help on yearly access review	☑	☑	☑
Technology and regulatory watch	☑	☑	☑

Digital operational Testing

	1 to 15	15 to 50	51 to 100
Physical security reviews (1/year)	☑	☑	☑
Yearly BCP and DRP testing	☑	☑	☑
(Vulnerability assessment)	☑	☑	☑

Process

Risk management

	1 to 15	15 to 50	51 to 100
Identify assets and Business process	☑	☑	☑
Create & Maintain asset register	☑	☑	☑
Create & Maintain Risk register	☑	☑	☑

Supplier management

	1 to 15	15 to 50	51 to 100
Assess new supplier	1/year*	2 /year	3/year*
Maintain supplier register, due diligence, exit strategies,…	☑	☑	☑
Notify regulatory authorities	☑	☑	☑

Incident and resilience management

	1 to 15	15 to 50	51 to 100
Maintain incident register and document incident	☑	☑	☑
Review BIA and *update* BCP/DRP policies	☑	☑	☑
Notify competent authorities	☑	☑	☑

Other GRC subject

	1 to 15	15 to 50	51 to 100
Yearly GAP analysis and report	☑	☑	☑
Annual review of policies	☑	☑	☑
Help with audit and client due diligence	2/year*	4/year*	5/year*
Writing policies and procedures	Additional project required		
Put the regulatory framework in place			

Security meetings

	1 to 15	15 to 50	51 to 100
Monthly security meeting with point of contact	☑	☑	☑
Quarterly Board meeting		☑	☑
Yearly Security summary meeting	☑	☑	☑

*number per year, additional may lead to aditional costs