primend

CISOaaS - Assessing and developing information security maturity level

CISO-as-a-Service | Assessing and enhancing the organization's information security maturity level

Why many small, medium, and even some larger companies do not have a full-time Chief Information Security Officer (CISO)?

- There isn't enough daily work to justify a full-time position
- Employing such an expert on a full-time basis may not be cost-effective

How Primend's Chief Information Security Officer service can help you?

- Provides advice on protecting the company against various cyber threats
- Assists in adapting to necessary regulations and standards
- Helps the company make strides in ensuring information security.

Primend's CISO-as-a-Service fulfils the role of a missing Chief Information Security Officer in the company or assists the existing person responsible for information security in fulfilling their duties by providing the necessary expertise and experience.

Where to start with information security maturity assessment?

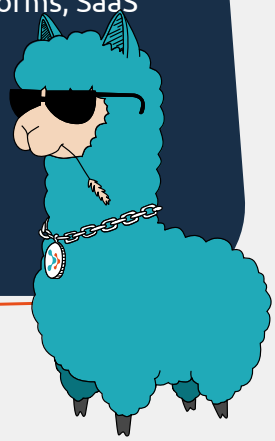
First, it is necessary to gain a comprehensive overview of the various information systems and applications, as well as the roles, processes, and other technologies in use based on the company's business strategy.

As a result of the maturity assessment, a summary will be prepared, describing the next steps and their priorities to bring the greatest benefit to the organization.

Phases of the maturity assessment:

- Interviews with the organization's leadership and key employees
- Interviews with important partners, analysis of IT architecture, and integrations
- Analysis of computer network topology – assessing if networks are adequately protected, segmented, etc.
- General analysis of IT infrastructure
- Analysis of recovery plans and backup policies, assessing business risks regarding RPO/RTO
- Analysis of applications (internal developments, websites, e-commerce platforms, SaaS services)
- Compilation of a summary report along with development proposals.

Depending on the size and complexity of the organization, this process typically takes about 1-3 months and naturally requires good cooperation from the organization.



Based on the information security maturity assessment report, decisions can be made regarding which activities and development proposals are critical to address immediately and which ones can be spread out over a longer period.

Possible next steps:

- Establishing information security strategies, objectives, and metrics based on the company's business strategy
- Conducting risk analyses in the information security domain
- Planning, implementing, and managing necessary information security solutions
- Developing and maintaining information security policies, rules, and guidelines
- Developing and implementing a continuous improvement plan for information security
- Raising awareness among company employees about information security and providing trainings.

The final list of tasks always depends on the specific desires and needs of the company and can be agreed upon during the service ordering process. The Chief Information Security Officer service can be ordered on a project basis or as a monthly service.

Ask for more information

Rene Kaalo | IT Business Consultant

rene.kaalo@primend.com

primend

bm certification ISO 9001 ISO 27001 System certification