

Why us?

- We reduce time and costs
- We use a flexible approach
- We bring measurable planned business results
- We guarantee fast and transparent cost calculation
- We have many years of experience



🌐 www.aktiv.consulting

✉ info@aktiv.consulting

☎ +7 (495) 925-77-90

Try our services for free

To get a degustation consultation please contact:
Oleg Simakov, Head of Customer Relations
simakov@aktiv.consulting

AKTIV.
CONSULTING

Information security consulting

Solutions for:

- Business and corporations
- Government organizations and agencies
- IT and cybersecurity companies

Cybersecurity function management

Statement of the function and processes of information security

Preparation of the concept and roadmap for the allocation and implementation of the information security function in accordance with the compliance and business goals of the company

Development of a strategy and programs for the development of the cybersecurity function

Creation of a roadmap for the transformation of the information security function in the medium and long term

Cyber-risks governance

Setting up cyber-risks management processes

Designing cyber-risk management processes and a roadmap for their implementation in risk management processes

Development of a methodology for assessing cyber-risks

Creation of a methodology for assessing cyber-risks adapted to the needs of the customer, including the development of a mathematical model

Compliance

Implementation of cybersecurity standards requirements

Assessment of compliance with the requirements and development of a roadmap for their implementation

Development of cybersecurity standards and requirements

Preparation of information security requirements at the level of the state, industry or individual company

Creation of information security requirements for exported digital products

Definition of a scope of requirements for creating and launching a digital product on the market and developing a roadmap for its implementation

Secure software development lifecycle

Implementing SSDLC processes

Designing a SSDLC process in accordance with cybersecurity requirements, taking into account the existing development life cycle and product features

Development of cybersecurity requirements for information systems

Preparation of terms of reference for cybersecurity and consulting in the process of its implementation

Vulnerability Analysis

Conducting Static and Dynamic Application Security Testing (SAST and DAST) for applications and information systems in order to identify vulnerabilities



Experts with experience in various industries



25 years in the information security market



Hundreds of implemented projects in ICT, financial and public sectors

Protection of information systems and infrastructure

Conducting security analysis

Analysis of the security of the organization's infrastructure and identification of vulnerabilities

Conducting penetration tests

Simulation of an attack by an intruder in order to assess the possibility of its successful implementation

Designing a cybersecurity module for automating business processes

Development of cybersecurity requirements for an automated enterprise management systems (aEMS) and a roadmap for their implementation

Provision of the information confidentiality

Establishment of processes for the protection of confidential information

Designing processes for the protection of confidential information, including trade secrets, protection of intellectual property and know-how

Setting up processes for personal data management

Designing processes for working with personal data in accordance with cybersecurity requirements (including CCPA, GDPR) and a roadmap for their implementation.

Protection of automated process control system

Cyber security processes for industrial control systems (ICS)

Development of the configuration of information security processes for an organization with automated process control systems (SCADA, HMI, PLC)

Assessment of compliance with cybersecurity requirements in industrial control systems (IEC 62443xx, IEC 62859, IEC 62645, IEC 63096)

Assessment of the organization's compliance with cybersecurity requirements and development of a roadmap for their implementation