# ViveSec

## IT SECURITY MANAGEMENT SYSTEM FOR CRITICAL INFRASTRUCTURE PROVIDERS

## THE CHALLENGE

### Legacy of critical infrastructures

The systems of industrial companies and especially of critical infrastructure providers have traditionally been very vulnerable to cyber-attacks. They are lagging far behind and by their nature are more difficult to protect as they need to be remotely accessible and unobstructed for operational and intervention purposes. These systems have a much longer lifespan and as such they are more outdated and have not been designed with IT security in mind. Due to the specifics of the industry, in many cases, “traditional” IT security solutions cannot be applied as-is.

### In the crossfire of cyber attacks

Critical infrastructure protection is also particularly important as they become increasingly the main target of cyber warfare. Attacks on industrial systems however can be more severe than on an office environment, as physical consequences, equipment failure, personal injury or even environmental pollution could occur.

### Lack of expertise, and regulatory requirements

Critical infrastructure organizations in many cases do not have the necessary cyber defence capacity. However, they are required by law to review their processes, their means of protection and to comply with certain information security standards (e.g., ISO 27001). That's why there may be a great need for an automated service to help utilities manage information security management.

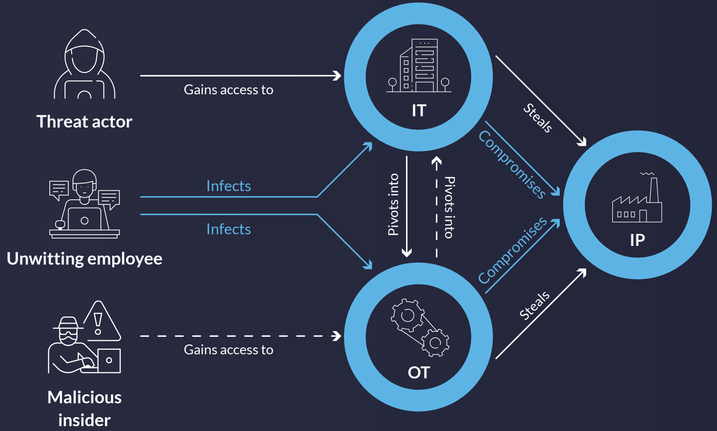


*Figure 1: IT security threats in industrial companies*

www.vivesec.com info@vivetech.com

# THE SOLUTION

## Industry specific safety management system

**ViVeSec is an application platform that, owing to its high level of automation and integration, implements the complete and efficient operation of the information security management system (ISMS) in a single system.**

ViVeSec is a **flexible, easy-to-use platform** that includes all the necessary building blocks to build a software environment that supports an information security management system. By configuring the elements of the platform, IBIR support tailored to the needs of the organization can be developed quickly and risk-free.

One of the cornerstones of its efficiency is a **high degree of automation**: analytical capabilities based on its built-in inventory and workflows actively support decision preparation. In addition to weighted, systematized, interpreted data, **the system assists in decision-making as a digital expert**. Its automatisms and industry-specific templates enable to create a system which can be operated even by a single-member security operation.


*Figure 2: Information security quality management system processes*

# FEATURES

## Information security management system

The platform establishes and operates an information security management framework that includes all related tasks and activities. The elements of the control system are determined by the regulatory requirements but can also be selected by the user. All tasks related to IT security are carried out according to schedule, in cooperation with the relevant responsible persons.

## Inventory and Knowledge Base

Everything in one place: a description of the structure and operation of the given organization, assessment and data recording functionality, operational templates, lists, and other information. An industry-specific collection of predefined templates and workflows reduces the resource requirements for tasks within the IBIR system, including the need for expensive and limited expert capacity.

## Risk management

The workflow-driven risk management module supports the entire risk management process using the templates stored in the Inventory. Based on the Inventory and the built-in logic, it is able to automatically build and simulate the entire chain of threats. This will make risk analyses more accurate and repeatable. Risk management is dynamic and visualizable.

www.vivesec.com info@vivetech.com

## Compliance

ViVeSec is able to create a comprehensive control system with the help of a built-in control list covering compliance requirements, the control levels of which are also influenced by the results of risk analysis.

The key to compliance is a two-tier audit system: "**Compliance audit**" monitors the status of the mapping of external requirements in real-time and is able to dynamically change the reporting system. „**Internal Audit**" compares the information in the mapped policies and applicable unwritten law. The software also effectively supports the plan, execution, and evaluation of the above audit.

## Operations Security Technology Management (OPSEC)

Thanks to its analytics functions, ViVeSec is also capable of managing the different technologies (firewall, IPS, WAF, VM, etc.) and keeping their security level up to date.

## Business continuity

The workflow-driven Business Continuity Module (BCM) allows you to create different emergency management plans and scenarios. This way, the business impact of an unexpected loss or event can be minimized. It provides a high level of support for the testing process, during which individual chains of effects can be simulated. BCM tests can be effectively managed and documented.

## Incident Management

ViVeSec includes an incident management module specifically designed for IT security tasks. In addition to the traditional ticketing functions, it is able to create tasks (IS tasks, risk analysis, BCM tasks, audit, data provision, etc.) from requests and incidents received from users and external systems (SIEM, HD, etc.), along with template processes, and monitor their life cycle. follow and email your results.


*Figure 3: ViVeSec Information security management*

## Why should you choose ViVeSec?

- Contains the expertise required for the implementation and operation of IBIR, eliminates the need for a significant expert presence
- Covers the entire process of information security management, supports all operational activities to be performed
- It also plans and schedules implementation, certification, maintenance, and continuous improvement
- Fully covers the organization's industry and country-specific compliance requirements (ISO 27001, BSI, 2008/114 / EC, GDPR)
- Significantly speeds up audit preparation and reduces costs
- Automatically handles correlations, displays the effect of set changes immediately
- Easy to learn, easy to use, does not require significant expertise
- Highly scalable and customizable software available in the cloud or installed locally

## Who do we recommend it?

- Critical infrastructure companies
- Large industrial companies
- BSI or ISO 27001 compliant organizations

ViVeSec is an expert system that supports the implementation of the organisation's Information Security Management System on a BSI / ISO 27001 basis, regardless of the organisation's IT security level, based on the industry and internal regulatory environment, without the need for significant on-site consulting support and internal expertise, classification, maintenance and enhancement of information security.

# ViVeTech

ViVeTech is a Hungarian-owned IT consulting and development company operating successfully since 2011, which focuses on the interaction between human and technology. In accordance with our mission, aspects of ergonomics also play a prominent role in the novel approach represented by our information security branch, as a guarantee for added business value. The primary goal of our business is to enable our customers to consciously assess and handle their operational risks, and to increase their competitiveness through the measures put in place. We at ViVeTech place great emphasis on research and academic cooperation in each of our fields of expertise, thus in information security as well. We like to think of ourselves as a scientific workshop, where we study different aspects of the human-machine interface.

www.vivesec.com info@vivetech.com