DIGIFENCE
TECHNOLOGY

27/4 Azatutyan Avenue
Yerevan 0014 Armenia
(374) 11 48 48 48
/digifence.tech
info@digifence.am
www.digifence.tech

Enterprise Cybersecurity Level

▼ FRAMEWORK 01

NIST Cybersecurity Framework

DESCRIPTION

More than ever, organizations must balance a rapidly evolving cyber threat landscape against the need to fulfill business requirements. To help these organizations manage their cybersecurity risk, NIST convened stakeholders to develop a Cybersecurity Framework that addresses threats and supports business. While the primary stakeholders of the Framework are U.S. private-sector owners and operators of critical infrastructure, its user base has grown to include communities and organizations across the globe.

The Framework integrates industry standards and best practices to help organizations manage their cybersecurity risks. It provides a common language that allows staff at all levels within an organization - and at all points in a supply chain - to develop a shared understanding of their cybersecurity risks. NIST worked with private-sector and government experts to create the Framework, which was released in early 2014. The effort went so well that Congress ratified it as a NIST responsibility in the Cybersecurity Enhancement Act of 2014.

The Framework not only helps organizations understand their cybersecurity risks (threats, vulnerabilities and impacts), but how to reduce these risks with customized measures. The Framework also helps them respond to and recover from cybersecurity incidents, prompting them to analyze root causes and consider how they can make improvements. Companies from around the world have embraced the use of the Framework, including JP Morgan Chase, Microsoft, Boeing, Intel, Bank of England, Nippon Telegraph and Telephone Corporation, and the Ontario Energy Board.

NIST continues to promote awareness of the Framework and its implementation in domestic and international markets. NIST also continues to work with industry and other stakeholders to ensure that updates to the Framework maintain its relevance and utility for a broad range of organizations.

▼ FRAMEWORK 02

ISO 27001 Information Security Management System

DESCRIPTION

The ISO/IEC 27000 family of standards helps organizations keep information assets secure.

Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

It can help small, medium and large businesses in any sector keep information assets secure.

Like other ISO management system standards, certification to ISO/IEC 27001 is possible but not obligatory (the Central bank of the Republic of Armenia enforces the compliance to ISO/IEC 27001). Some organizations choose to implement the standard in order to benefit from the best practice it contains while others decide they also want to get certified to reassure customers and clients that its recommendations have been followed.

Many organizations around the world are certified to ISO/IEC 27001.