Total Information Security Control: all the ICT safety you need

Renowned testing, inspection and certification expert Kiwa introduces Total Information Security Control (TISC), a new integral ICT security tool covering the full spectrum of data and internet of things.

Nowadays society heavily depends on data. Information and communication technology solutions dominate our professional and personal lives and have even found their way to everyday domestic appliances like refrigerators, thermostats and lighting. The internet of things comes with great business opportunities but also involves certain risks. Cyber-attacks or hacking can endanger business continuity with financial hardships and loss of image and goodwill as a consequence. In addition, new data protection legislature rules like the GDPR, that becomes effective Spring 2018, also calls for an integral ICT security approach to continuously map, improve and monitor all aspects of an organisation's ICT. And that's where Total Information Security Control (TISC) by Kiwa comes in.

How safe do you need to be?

When it comes to ICT security, the question should be how safe your organisation actually needs to be rather than how safe it is technically possible to be. Being aware of security risks and being completely in control of the ICT in your business are key if you aim for business continuity and continuous improvement of the security of your processes. Kiwa's TISC proposition does exactly that. This award winning, one of a kind testing, inspection and certification methodology covers international rules and legislation concerning data protection as well as applicable business process standards like ISO27001.

No paper tiger

TISC evolves around determining the level of ICT security and subsequently find a way to match this to your organisation's risk profile. TISC is no paper tiger. It is a pragmatic methodology, focusing on abstraction level and content and connecting to international standards and best practices like ISO, ITIL, Cobit, NIST, IEC, COSO and EN. In TISC Kiwa's security experts have managed to combine all these standards and practices into one integral model, housed in four pillars: Control, People, Process and Technology. In collaboration with several trusted partners Kiwa conceived a generic model around these pillars, consisting of a continuous process of (re-)defining risks and threats, monitoring and improving.

Kiwa N.V.
info@kiwa.nl
+31 (0)88 998 44 00

Circular ecosystem

Kiwa's Total Information Security Control methodology distinguishes four steps that form a circular ecosystem of plan-do-check-act, specially designed for continuous improvement of your organisation's security processes. The four steps of TISC are:

1. Defining the baseline/risk assessment
   The first step to meet the requirements the GDPR and NIS (for providers) is testing the ICT infrastructure and auditing processes and procedures, based on the Open Source Security Testing and Auditing Methodology ICT (OSSTAM). This results in a report incorporating the findings, strengths and vulnerabilities of the four pillars of the security framework: Control, People, Process and Technology.
2. Implementation of the risk treatment plan
   Based on the findings during the information security risk assessment, we will be able to write an information security manual, using ISO27001 as a guideline. This manual provides a package of management measures that emerged from the risk analysis. The design is tailor made and includes elements like policy and scope, employee procedures, physical and technical security, communication and employee awareness, the PDCA cycle and the business continuity plan. This step of TISC reveals the added value of the methodology: three matrices for quality systems, services and components, about which you can read more below.
3. Continuous risk monitoring and reviewing
   At least once a year Kiwa will perform, announced and unannounced, audits on the different aspects of the TISC security framework and even test your resilience with phishing mails and 'friendly hacks'. This enables you to proactively monitor and review the information security of your systems, services and components. It also empowers you to properly trigger the applicable procedures of your management quality system at the time of a risk, calamity or event, putting you completely in control!
4. Maintain and improve
   Risks, threats, technology and legislation and standards are constantly changing. To stay in control constant repetition of steps 1 to 3 is necessary.

TISC matrices

During the second step of TISC, the implementation of the risk treatment plan, the added value of both the model and Kiwa's reputation as a globally reputed testing, inspection & certification organisation becomes clear, as it combines all fields of expertise and knowledge about applicable standards. Kiwa has translated all this into three matrices that enable you to achieve the right measures and test their effect before and during implementation. These three matrices are:

1. Matrix Quality system
   This matrix connects various standards concerning quality management in general and information security and enterprise continuity, like ISO9001, ISO27001 and ISO22301. The insight this matrix provides enables you to gain control over your business.
2. Matrix Services
   This matrix maps the operation and potential risks of all of your organisation's services, i.e. existing networks, storage capacity, ICT services to employees, suppliers etc. The correlation in the matrix maps the overlaps and additional requirements between the different standards and scopes.
3. Matrix Components

Kiwa N.V.
info@kiwa.nl
+31 (0)88 998 44 00

The internet of things is vastly increasing as a growing number of components is connected to the web. Practically all processes in organisations are resourced by combinations of software and hardware and Software as a Service (SAAS) solutions. This matrix maps several applicable national, European and international standards like EN50136 1-2 and EN50131-1 (alarm systems) ISO/IEC29115 (ICT authentication) and NEN7512 (health informatics). The matrix distinguishes four risk grades, giving you the opportunity to choose the safety level that suits you best.

Future proof

An all-encompassing model like Kiwa's TISC security framework asks for a focused project team. Clients who choose to implement TISC can rely on a dedicated project manager who maintains the overall view of the project and manages a team of specialists, ranging from business analyst to 'hacker', from auditor to test engineer and everything in between. TISC is a an ever evolving methodology, anticipating on new developments in technology, standards and legislation. This makes Kiwa's Total Information Security Control a completely future proof information security methodology.

Kiwa N.V.
info@kiwa.nl
+31 (0)88 998 44 00