FINCSC – Finnish Cyber Security Certificate

Secure your digital future.

FINCSC®
FINNISH CYBER SECURITY CERTIFICATE

FINCSC.FI

FINCSC – Finnish Cyber Security Certificate

FINCSC is a cost-effective certification mechanism for companies of all sizes to help demonstrate to customers and other stakeholders how a company has taken security into consideration.

FINCSC offers a sound foundation of basic hygiene measures to reduce an organization's vulnerability to cyber security threats. The certification enables an organization to evaluate its information security solutions and data protection principles, in a risk-based manner. The evaluation result serves as an excellent tool for developing an organization's business continuity and situational awareness.

The evaluation is performed three fundamental aspects of information security. The first aspect measures an organization's administrative capabilities to handle information reliably and safely in compliance with the relevant requirements. The second and third aspects assess the physical and technical conditions of the organization to ensure proper data protection when processing data.

The level of data protection is examined through the confidentiality, integrity and availability of information. Special attention is kept in an organization's method of preventing information from unauthorized disclosure, distortion or damage. The examination considers an organization's methods of detecting security breaches and performing corrective actions to minimize damages.

Preventive controls

Controls that are designed to influence the root causes of harmful events

Detective controls

Controls that are used to identify the occurrence of security breaches

Corrective controls

Controls that seek to combat and minimize the damages

How certification benefits my organization

Stand out amongst competitors

With this certificate your organization will be distinguished from other players in the industry sector

Be aware of your cyber security

Certification provides a comprehensive snapshot of your organization's cyber security status

Stay safe even in the future

Certification provides recommendations on the development targets for your organization's cyber security

Certification use cases

FINCSC certification is industry-independent and suitable for use by all types of organizations from private companies to public agencies, institutions and enterprises.

The certification can be used regardless of the extent of an organization's information systems or a number of employees. The certification is automatically scaled according to the nature of the organization to be evaluated.

Certification can be used either to evaluate an organization's own activities or securing its business relations and subcontracting networks. The use of certification helps to create trust in trading and to counter risks associated with business cooperation. Certification ensures the realization of the mutual rights, freedoms and interests of the contracting parties.

Examples of certification use cases are located on the FINCSC website. All organizations that have successfully completed the certification are listed on the above site. The list contains information on the certified organization and the certification level it has passed. The information is stored on the website throughout the validity of the certificate.

What certification can be used for

Review your business activities

Find out your preparedness and resilience against cyber threats

Evaluate the reliability of your business partner

Require certification from your stakeholders to ensure the smoothness of co-operation

Ensure the security of your supply chain

Take care of the continuity of operations by securing the safety of entire supply chain

Certification and authorization services

The FINCSC certification mechanism consists of two certification levels and a separate authorization function for assessment bodies.

Organizations may choose a certification between FINCSC and FINCSC PLUS. Participation in FINCSC PLUS certification requires the organization to have a valid FINCSC certificate when applying for the certification.

FINCSC certification measures the organization's cyber security maturity through a self-assessment questionnaire. The questionnaire is answered electronically through an online web portal. Answering is achieved in one or more parts regardless of the time or place. Questionnaire answers are reviewed by an approved assessment body before the certification decision is made.

FINCSC PLUS certification verifies the accuracy of the FINCSC certification. FINCSC certification results are verified with an external audit by an assessment body. The audit consists of several auditing methods from document reviews to personal interviews, physical observations and security testing. The auditing methods ensure the comprehensiveness and punctuality of the audit results.

FINCSC

Through certification you will personally assess the adequacy of your organization's information security controls and privacy practices

- **self-assessment questionnaire**
- **external evaluation**
- **assessment report**
- **FINCSC certificate**

350 € VAT 0%

FINCSC PLUS

By auditing, you will independently verify your organization's current level of information security and data protection

- **external audit**
- **audit report**
- **FINCSC PLUS certificate**

The price is determined on a tender basis.

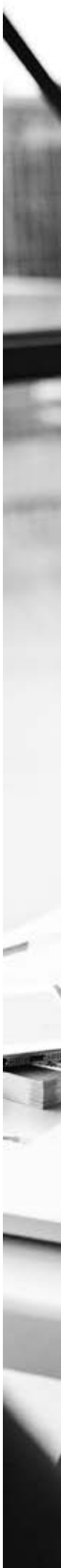
Certification scope

FINCSC certification involves the organization's data processing principles and computing environment.

The certification can cover the whole organization or its subset. The certification may be limited to a particular physical site, operational business unit or a logical part of the network. The certification scope must be clearly defined when applying it to the certification.

The data processing principles include the organization's working methods to handle information and provide adequate guidance on handling the information. In addition, the data processing principles contain the organization's means of ensuring the reliability of persons involved in the handling of information. Determining reliability also applies to third parties with whom the organization cooperates.

For a computing environment, the certification covers the information technology equipment, software and services used to process the data. The computing environment also includes telecommunication between end and intermediary devices. In addition, the computing environment includes the organization's physical facilities and storage units on site.



What is included in the certification?

Technology

End devices

Intermediary devices

Storage devices

Software and applications

Facilities

Premises

Storage units

Data erasure solutions

Personnel

Users

Admin users

Processes

Policies and practices

Work instructions

Outside the scope of the certification

Internet

Service providers

Public services

FINCSC certification process

Fill in the online application form

Certification begins by filling in the online application form at www.fincsc.fi

Login to the FINCSC portal

After the application has been accepted, the organization receives login credentials in the portal

Answering to self-assessment

Certification is performed by answering the electronic self-assessment questionnaire in the portal

Completion of the self-assessment

Completed self-assessment questionnaire is submitted to the assessment body for an external evaluation

Certification decision

After passing the certification, the organization receives the certificate for a one-year period of time

FINCSC PLUS certification process

Call for submission

Certification is attended by submitting a call for tenders through the FINCSC portal

Acceptance of tenders

After the end of the offer period, the organization processes the received offers and places an order

Collection of audit evidence

The organization compiles the audit evidence for the requirement verification

Audit

The organization participates in the external audit organized by the assessment body

Certification decision

After passing the certification, the organization receives the certificate for a three-year period of time

Development background

The FINCSC certification mechanism has been developed together with both public and private sector actors.

Actors from Finland and the United Kingdom have participated in the development work, which is influenced by the British Cyber Essentials Scheme. FINCSC, like the British national program, aims to help organizations in the fight against cybercrimes.

The status of the FINCSC certification mechanism reflects its membership in the implementation of the Finnish National Cyber Security Strategy. It has been defined as one of the key measures of the Finnish National Cyber Security Strategy Implementation Program for the years 2017 – 2020. FINCSC is also listed as one of the European cyber security assessment models by the European Cyber Security Organization ECSO.

The strategic objective of the FINCSC certification mechanism is to improve the cyber knowledge and perception of actors in society. To meet the strategic objectives, FINCSC creates the common criteria for the organizations to meet cyber security requirements. FINCSC offers organizations a basic starting point to implement cyber security and data protection, as well as securing continuity of business operations during cyber security incidents.

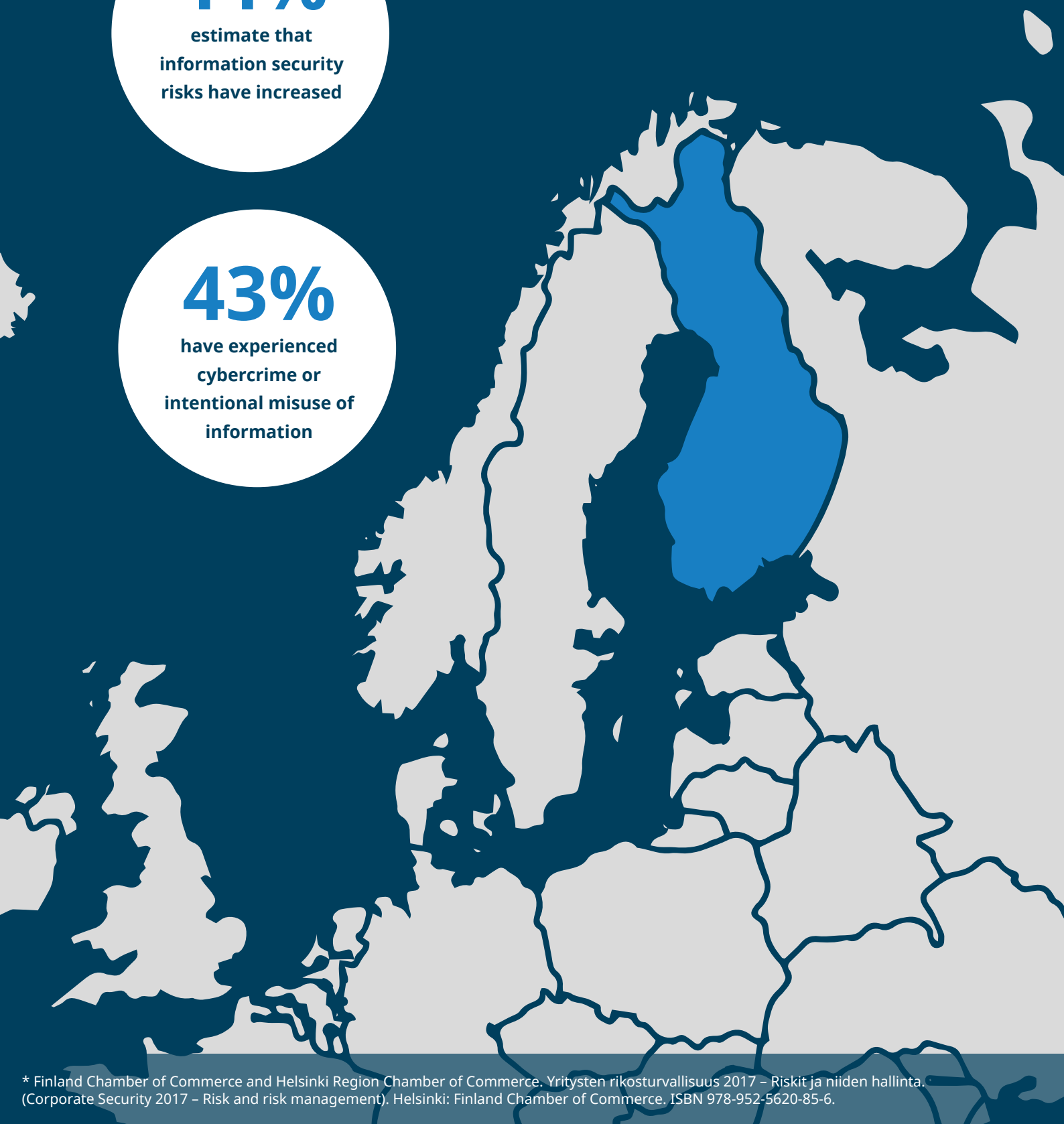
According to a survey* from Finnish companies

44%

estimate that information security risks have increased

43%

have experienced cybercrime or intentional misuse of information



* Finland Chamber of Commerce and Helsinki Region Chamber of Commerce. Yritysten rikosturvallisuus 2017 – Riskit ja niiden hallinta. (Corporate Security 2017 – Risk and risk management). Helsinki: Finland Chamber of Commerce. ISBN 978-952-5620-85-6.

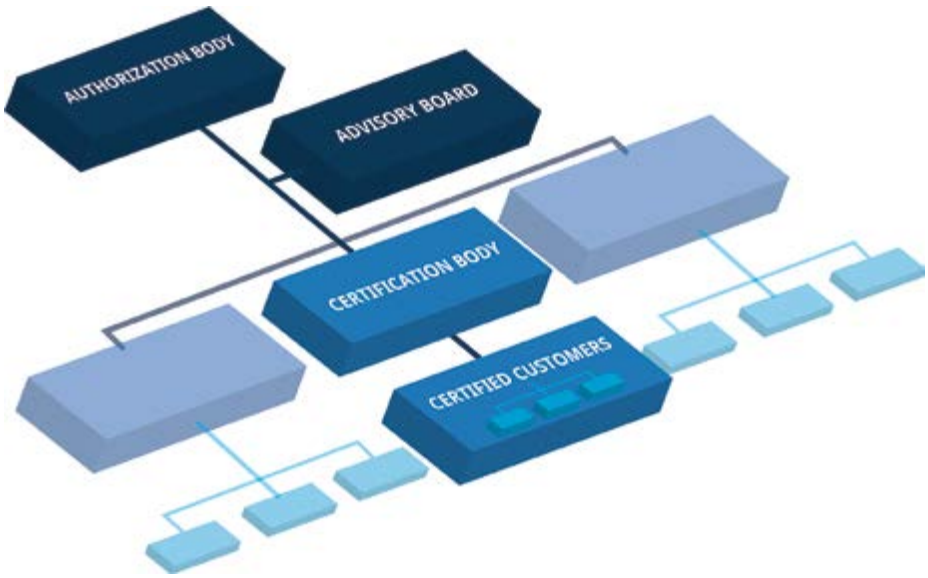
The maintenance of the certification mechanism

FINCSC certification mechanism is maintained with the principle of continuous improvement.

JYVSECTEC develops the certification mechanism alongside the FINCSC advisory board. The advisory board is represented by a wide range of business and public sector actors from Finland.

The advisory board works to promote the dissemination and deployment of the certification mechanism as a part of the systematic work toward corporate security. The advisory board is responsible for the independence and impartiality of certifications. The activities of the advisory board are governed by its operating rules.

The advisory board consists of representatives from customer organizations and authorized certification bodies. In addition, the advisory board has a member from the civil administration. The members of the advisory board work as a multi-professional team bringing the latest view of their respective fields.



“Trust is one of the most valuable assets of a company – no matter what is the size or business branch of your company. In current environment it is important to have suitable and scalable tools assuring your business is worth it.”

Mika Susi
Chairman of the FINCSC Advisory board
Confederation of Finnish Industries

“FINCSC certificate is an easy to use tool for SME companies when evaluating and enhancing their cyber security resilience against threats.”

Jarno Lötjönen
Service Manager
JYVSECTEC, JAMK University of Applied Sciences

FINCSC®
FINNISH CYBER SECURITY CERTIFICATE

Contact us:

In case you have any questions, feel free to contact us
fincsc@jamk.fi

JAMK University of Applied Sciences
Institute of Information Technology
Piippukatu 2, 40100 Jyväskylä, Finland

Follow us:
@FINCSC_fi

JYVSECTEC is JAMK University of Applied Sciences IT Institute-based cyber security research, development and training center. It maintains and develops **FINCSC** certification mechanism in cooperation with the advisory board.

jamk.fi Institute of Information Technology

JYVSECTEC Jyväskylä Security Technology

Confederation of Finnish Industries

Yrittäjät THE FEDERATION OF FINNISH ENTERPRISES

Keski-Suomen liitto Regional Council of Central Finland

Telia

Helsinki Region Chamber of Commerce

Viestintävirasto Finnish Communications Regulatory Authority