# SoSafe complies with cyber insurance requirements

sosafe

When applying for cyber insurance, risk assessments are conducted varying from the protection of sensitive data, protection against IT business interruptions, maintenance, management of IT, and more. Find out how our solution can help you get cyber insurance!

Crucial requirements	SoSafe Solution
CSAT (Cyber Security Awareness Training)	Low implementation and behavioral science-based continuous awareness training program with a lasting impact.
Reporting Requirements	Audit-ready dashboard makes reporting easy for cyber insurance, ISO 27001, IEC-27001, TISAX, and more.
ISO 27001 framework	Insurance providers assessment approaches are often aligned with ISO 27001 framework. Conveniently, SoSafe is built to align with ISO 27001.
Password management	Robust certification and fast track the right security behaviors with our ‚Password Security' modules.
Data privacy & GDPR	SoSafe is GDPR compliant and follows a privacy-by-design approach.
Security culture - Protection against IT business interruptions	Employees are your greatest asset, with us, employees are continuously trained to protect themselves against cyberattacks.

Other crucial requirements:
Regular backups; Regular patching; Malware protection and antivirus in place and up to date;
Firewall in place and correctly configured; Multi-factor authentication;
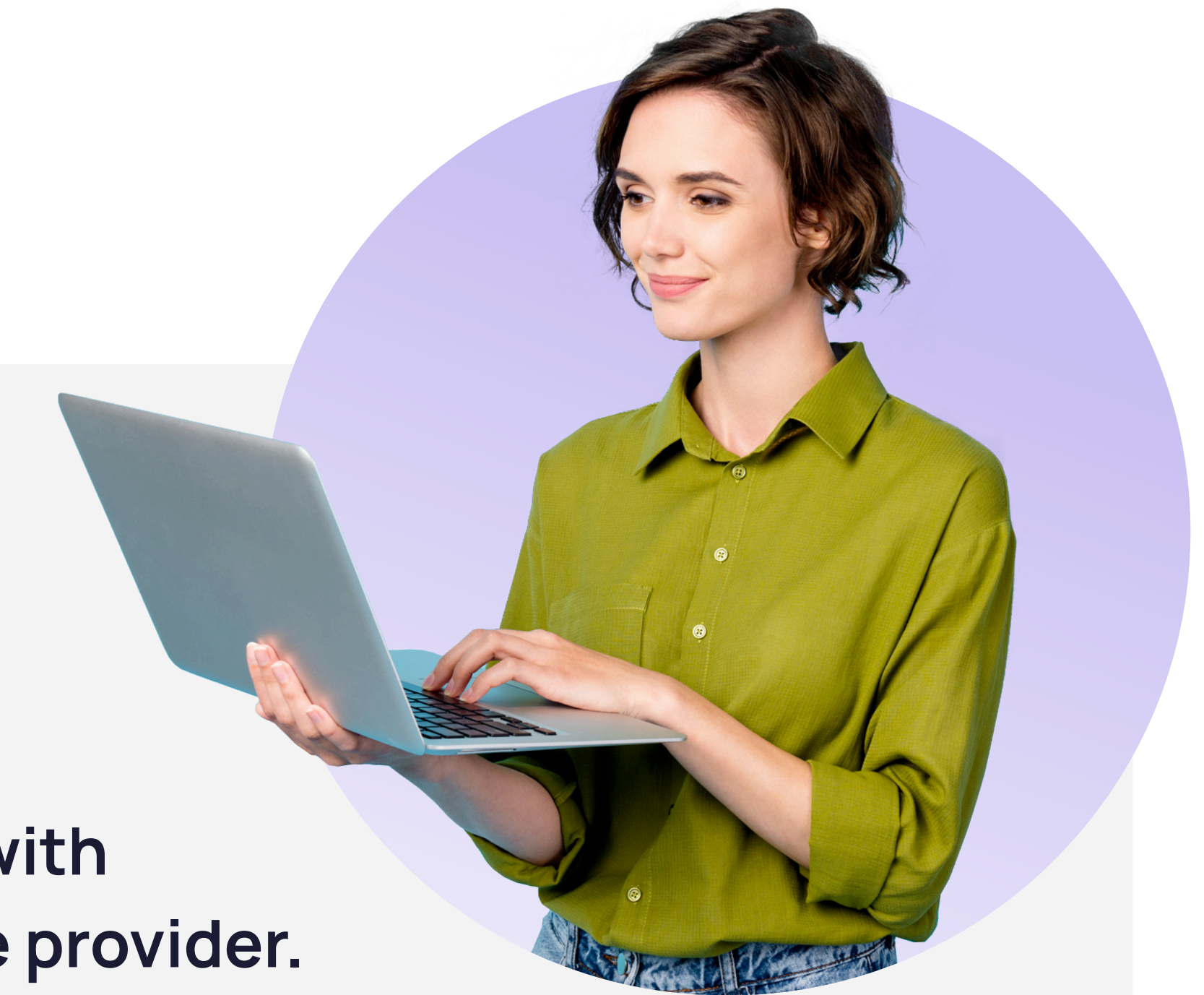
Please check with your insurance provider.

Depending on the size of your company, CSAT may be a mandatory requirement for cyber insurance.
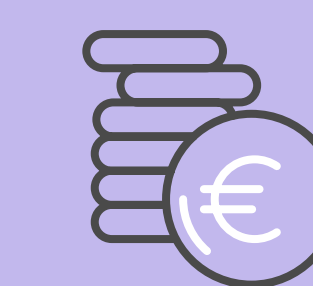
In some cases, CSAT lowers the cost of cyber insurance.

Do you need CSAT set up as soon as possible?

We have a guaranteed implementation time of 20 days.

Request a demo →

sosafe-awareness.com