

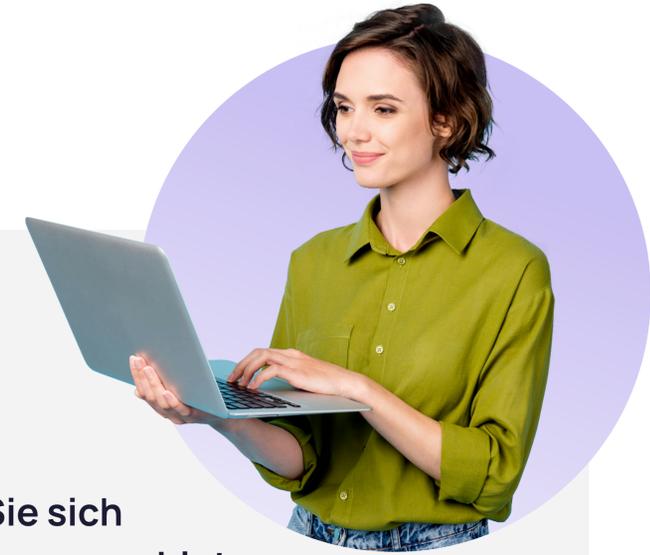
# SoSafe erfüllt die Anforderungen der Cyberversicherung



Bei der Beantragung einer Cyberversicherung werden Risikobewertungen durchgeführt, die sich auf den Schutz sensibler Daten, den Schutz vor IT-Betriebsunterbrechungen, die Wartung und Verwaltung der IT sowie vieles mehr beziehen. Finden Sie heraus, wie unsere Lösung Ihnen helfen kann eine Cyberversicherung abzuschließen.

Maßgebliche Anforderungen	SoSafe Lösung
CSAT (Cyber Security Awareness Training)	Geringer Implementierungsaufwand und ein verhaltenswissenschaftlich fundiertes Awareness-Training für eine nachhaltige Sensibilisierung.
Meldepflicht	Auditfähiges Dashboard für ein einfaches Reporting für Cyberversicherungen, ISO 27001, IEC-27001, TISAX, und mehr.
ISO 27001 Rahmenbedingungen	Die Bewertungsansätze von Versicherungsanbietern sind oft an den ISO 27001-Rahmen angepasst. Praktischerweise ist SoSafe so aufgebaut, dass es mit ISO 27001 übereinstimmt.
Password management	Robuste Zertifizierung und schnelles Erlernen des richtigen Verhaltens bei Sicherheitsvorfällen mit unseren Modulen zum Thema "Passwortsicherheit".
Datenschutz & DSGVO	SoSafe ist DSGVO-konform und folgt einem Privacy-by-Design-Ansatz.
Sicherheitskultur – Schutz vor Ausfällen der IT	Ihre Mitarbeitenden sind Ihr größtes Kapital. Bei uns werden Ihre Mitarbeitenden kontinuierlich geschult, um sich vor Angriffen zu schützen.

**Andere wichtige Anforderungen:** Regelmäßige Backups; Regelmäßiges Patching; Malware- und Antivirenschutz; Firewall mit korrekter Konfigurierung; Multi-Faktor-Authentifizierung;



## Bitte erkundigen Sie sich bei Ihrem Versicherungsanbieter

Je nach Größe Ihrer Organisation kann CSAT eine zwingende Voraussetzung für die Cyberversicherung sein.



In einigen Fällen verringert CSAT die Kosten einer Cyberversicherung.

## Brauchen Sie CSAT so schnell wie möglich?

Wir haben eine garantierte Implementierungszeit von nur 20 Tagen.

Jetzt Demo anfragen →

[sosafe-awareness.com/de](https://sosafe-awareness.com/de)