



Osmond
RISK MATTERS

Informationssicherheitsgesetz (ISG)

Fact Sheet

Osmond GmbH
+41 56 511 22 90
Rummelmatt 6, CH-5610 Wohlen
info@osmond.ch
www.osmond.ch

28/08/2025

Regulatorische Vorgabe

Das Informationssicherheitsgesetz (ISG) der Schweiz, seit 1. Januar 2024 in Kraft, ist ein entscheidender Schritt zur Stärkung der Cyber-Sicherheit und zum Schutz der Informationen und IT-Ressourcen des Bundes und kritischen Infrastrukturen.

Wer ist vom ISG betroffen?

Das ISG gilt für ein breites Spektrum von öffentlichen und privaten Organisationen sowie für Betreiber kritischer Infrastrukturen und Organisationen, die den Bund bei der Wahrnehmung seiner Aufgaben unterstützen:

Bundesbehörden und Organisationen

(z.B. Bundesamt für Informatik und Telekommunikation)

Kantonale Behörden, die auf Bundesdaten zugreifen, müssen ebenfalls die Sicherheitsvorgaben einhalten

(z.B. Kantonspolizei)

Private Unternehmen, die für den Bund tätig sind

(z.B. IT-Dienstleister für Cloud Services, Datenverarbeiter)

Internationale Partner (z.B. internationale Unternehmen, die mit Schweizer Bundesbehörden zusammenarbeiten)

Betreiber kritischer Infrastrukturen:

- **Energieversorgung:** Strom-, Gas- und Wasserversorgungssysteme (z.B. Axpo)
- **Transport und Verkehr:** Strassen-, Schienen-, Luft- und Wasserverkehrssysteme (z.B. SBB)
- **Informations- und Kommunikationstechnologie:** Telekommunikationsnetze und IT-Systeme (z.B. Swisscom)
- **Gesundheitswesen:** Krankenhäuser, medizinische Versorgung und Notfalldienste (z.B. Universitätsspital Zürich)
- **Finanzdienstleistungen:** Banken, Börsen und Zahlungsverkehrssysteme (z.B. UBS)
- **Lebensmittelversorgung:** Produktion, Verarbeitung und Vertrieb von Lebensmitteln (z.B. Migros)
- **Öffentliche Verwaltung:** Regierungs- und Verwaltungsdienste auf Bundes-, Kantons- und Gemeindeebene (z.B. Bundesamt für Bevölkerungsschutz)



Was ist zu tun?

Meldepflicht für Cyberangriffe an das Bundesamt für Cybersicherheit (BACS) innerhalb von 24 Stunden

Einrichtung eines **Informationssicherheits-Managementsystems (ISMS)** zur Verwaltung und Verbesserung der Informationssicherheit



Vorfallmanagement: Entwicklung von Verfahren zur schnellen Erkennung und Meldung von Cyberangriffen

Schulung und Sensibilisierung: Schulung der Mitarbeiter in den Anforderungen des ISG und der Cybersicherheitsverordnung (CSV)

Was sind die Fristen für die Umsetzung?



- **Informations-Klassifizierungskatalog** bis 31.12.2024
- **Meldepflichtprozess** für Cyber-Angriffe ab 1.4.2025
- Risikoanalyse und **IT-System Klassifizierung / Schutzbedarf** bis 31.12.2025
- **Informationssicherheits-Managementsystem (ISMS)** bis 31.12.2026
- **Technische Sicherheitskonformität** bis 31.12.2027

Osmond bietet umfassende Dienstleistungen und Beratung zur Implementierung der neuen Anforderungen des ISG, um Unternehmen und Organisationen bei der Einhaltung der gesetzlichen Vorgaben zu unterstützen.