cyberunity

the who, what, when, and why: Federal Act on Information Security in the Confederation (FAISC)

who (will the FAISC impact)?

Switzerland's new Federal Act on Information Security in the Confederation (FAISC) will primarily impact **federal authorities**, **offices**, and **organisations** in the context of their data processing activities. Beyond these bodies, it will also have implications for the information security practices of **cantonal authorities**, **critical infrastructure operators (OT)**, any **third-party contractors**, **service providers** or **business partners** who process federal data or interact with federal IT resources, and **international partners** collaborating with Swiss federal entities.

what (is the FAISC)?

The FAISC establishes an overarching legal framework upon which more detailed ordinances and directives then set out **legal provisions**, **best practices**, and **minimum requirements** related to secure information processing in the federal context (the processing of information by authorities and/or the use of Federal IT resources for information processing by third parties).

It introduces three new ordinances that flesh out its provisions:

- the Information Security Ordinance (ISV) addresses minimum requirements for information security management, the handling of classified information, IT- and physical-security (e.g., ISMS, contractual obligations, third party collaborations, risk management, awareness campaigns, audits, incident management, and reporting obligations).

- The ordinance on Personnel Security Checks (VPSP) deals with risk management in the individual context i.e. ensuring that background checks are conducted for staff tasked with security-sensitive-work. It sets out benchmarks for the kinds of data that may be processed for this purpose and the ways in which said data may be processed

- The ordinance on Operational Security Procedure (VBSV) replaces the previous Ordinance on the Protection of Secrecy, which was limited to classified military contracts, and aims to prevent companies controlled by foreign intelligence services from gaining access to highly classified information or to critical federal IT systems. It sets procedures for security-sensitive contracts granted to companies by the federal administration including background checks on said companies (which are conducted in cooperation with the Federal Intelligence Service), unannounced spot checks, as well as inspections and audits

when (is the deadline for FAISC implementation)?

The FAISC and its ordinances came into effect on January 1, 2024. The following transition deadlines have been announced for the implementation of its provisions:

- Classification Catalogue: Entities in scope need to establish a robust information classification in line with the new regulations by **December 31, 2024**.

- Risk Analysis and IT Classification: Risk analyses must be conducted, and IT systems classified according to the FAISC and its ordinances by **December 31, 2025**.

- Information Security Management Systems (ISMS): Entities in scope will be required to set up an ISMS by **December 31, 2026**.

- Technical Security Compliance: All IT resources must comply with the FAISC's new technical security regulations by **December 31, 2029**.

why (does the FAISC matter)?

The FAISC represents an important milestone in Switzerland's commitment to bolstering information security across federal and cantonal entities. By establishing a comprehensive legal framework, introducing detailed ordinances, and paying special attention to the security of critical infrastructures it will

help standardise best practices for secure information processing in an ever more precarious information landscape.

Its phased implementation deadlines emphasize the urgency of aligning organizational practices with its provisions and the broad scope of stakeholders to which it applies will help bring uniformity to information security practices across Switzerland.

With implications extending to federal authorities, critical infrastructure operators, and international partners, the FAISC will play a crucial role in fortifying Switzerland's digital infrastructure, enhancing cybersecurity resilience, and safeguarding sensitive data.

find out more:

- New Swiss information security law with implications for private companies working for the federal government (ethics-compliance.ch)
- ISG – Bundesrat schickt Verordnungen in Vernehmlassung (admin.ch)
- Erläutender Bericht zum ISG (admin.ch)

interested in what FAISC means for your business?

Joshua Bucheli (cyberunity AG) and John Corona (Osmond GmbH) look forward to hearing from you!

Stay tuned for more - look out for our next **cyberbyte** on the EU AI Acts