

W H I T E P A P E R

Critical Infrastructure Security Beyond the EU

How Switzerland and the United Kingdom Navigate the NIS 2 Directive

May 2026

Regulatory Affairs & Critical Infrastructure Compliance

About This Paper

This white paper examines how Switzerland and the United Kingdom are responding to the EU's Network and Information Systems Directive 2 (Directive EU 2022/2555, or NIS2), which replaced the original NIS Directive with effect from 18 October 2024. NIS2 is an infrastructure-security directive rather than a product regulation: it imposes cybersecurity risk management, incident reporting, and supply chain security obligations on operators of critical and important services across 18 sectors. It applies not only to entities established in the EU but, through its extraterritorial provisions, to any organisation providing in-scope services to EU customers or operating in the EU market. This paper examines the practical compliance obligations that NIS2 creates for Swiss and UK businesses, the current state of domestic legislation in each jurisdiction, and the degree to which those domestic frameworks align with or diverge from NIS2's requirements.

Executive Summary

The EU's NIS2 Directive is the most consequential overhaul of European critical infrastructure cybersecurity law since 2016. Unlike a product regulation, NIS2 does not attach to specific goods sold in the EU — it attaches to the entities that operate critical services, wherever those entities are established. This gives it a broader and, in some respects, more complex extraterritorial reach than the Cyber Resilience Act or the PPWR: any organisation providing digital services, cloud infrastructure, managed security, or other in-scope services to EU customers is potentially in scope, regardless of whether it has a physical presence in the EU.

Switzerland and the United Kingdom face NIS2's reach through two distinct channels. First, both countries host organisations that provide in-scope services to EU customers directly — cloud providers, managed service providers, DNS operators, and digital infrastructure companies whose services cross borders invisibly. These entities may be required to register with EU member state authorities and comply with NIS2's full suite of obligations. Second, both countries are significant nodes in the supply chains of EU-regulated entities: even Swiss and UK businesses that are not themselves in scope may face NIS2-equivalent obligations imposed contractually by EU partners required to secure their supply chains under Article 21 of the Directive.

Domestically, neither Switzerland nor the UK has enacted a direct equivalent of NIS2, though both have active reform programmes that draw on its architecture. Switzerland's Information Security Act (ISG), in force since January 2024, establishes a critical-infrastructure security baseline, and a new KRITIS-G law — explicitly modelled on NIS2 — is under active development, expected to enter force by 2027. The UK's NIS 2018 Regulations remain in force but are materially narrower than NIS2; the Cyber Security and Resilience Bill, introduced to Parliament in November 2025, updates that framework with clear NIS2 influence while remaining distinctly British in its architecture and scope.

Key Findings

- NIS2 has direct extraterritorial effect on non-EU organisations providing services in the EU. Swiss and UK firms in sectors such as cloud computing, managed services, DNS, digital infrastructure, and trust services may be in scope and face registration, risk management, and incident reporting obligations under national NIS2 implementations.
- Supply chain obligations under NIS2 Article 21 extend NIS2's practical reach further still: EU-regulated entities must assess and manage the cybersecurity of their suppliers, pulling Swiss and UK businesses into NIS2 compliance requirements through contractual pressure even when they fall outside direct scope.
- Switzerland's ISG establishes a risk management and reporting framework for critical infrastructure that parallels NIS2 in structure, and the forthcoming KRITIS-G law is explicitly designed to align with NIS2's architecture. However, the ISG covers fewer sectors and has less prescriptive risk management requirements than NIS2.
- The UK's Cyber Security and Resilience Bill mirrors NIS2 in ambition and shares its incident reporting timelines, but differs in sector coverage (NIS2 is wider), regulatory architecture (the UK relies more on secondary legislation and the NCSC's CAF), and in the novel introduction of 'Designated Critical Suppliers' — a concept that goes further than NIS2 in directly regulating supply chain actors.

- NIS2 compliance does not automatically satisfy domestic Swiss or UK law, and vice versa. Both Switzerland (KRITIS-G from 2027) and the UK (CS&R Bill) maintain independent legal frameworks that companies operating in those markets must comply with separately, in addition to any NIS2 obligations that apply through EU market exposure.
- Both Switzerland and the UK are calibrating their domestic frameworks against NIS2, and convergence is the clear direction of travel — but neither country is moving at EU speed, and mutual recognition of compliance assessments is not currently in place.

1. NIS2: What It Requires and How It Reaches Beyond EU Borders

Directive (EU) 2022/2555 was adopted on 14 December 2022, published on 27 December 2022, and entered into force on 16 January 2023. EU member states were required to transpose it into national law by 17 October 2024 — a deadline met in full by only a minority of member states, prompting the European Commission to open infringement proceedings against 23 member states in November 2024 and send reasoned opinions to 19 in May 2025. As of mid-2026, approximately 20 of 27 member states have completed transposition. For non-EU businesses, the practical implication is that NIS2's obligations are being activated on a rolling basis as national implementations come into force, and the country-by-country picture varies.

NIS2 replaces the original NIS Directive (Directive 2016/1148) and dramatically expands its scope. Where NIS1 applied to operators of essential services in seven sectors, NIS2 covers 18 sectors split into 'essential' and 'important' entities. Essential entities include operators in energy, transport, banking and financial market infrastructure, health, drinking water, wastewater, digital infrastructure, ICT service management (managed service providers), public administration, and space. The transport sector under NIS2 Annex I is defined broadly: it covers air transport (airlines, airports, air traffic management operators), rail transport (infrastructure managers and railway undertakings), water transport (maritime and inland waterway carriers, port authorities, vessel traffic management services), and road transport (road authorities responsible for traffic management, operators of intelligent transport systems). Logistics operators and supply chain service providers — including warehouse operators, distribution centres, freight forwarders, and port and airport logistics operators — fall within the transport and, in some cases, postal and courier categories depending on their specific function and size. Companies primarily moving freight digitally (route optimisation, fleet management, digital freight platforms) may also be captured as digital providers. Important entities add postal and courier services, waste management, chemicals, food, manufacturing (of medical devices, electronics, machinery, motor vehicles), and digital providers. On postal and courier services: the Annex II category covers national postal operators and large private courier companies. Pure logistics — warehousing, distribution, freight forwarding — does not automatically fall under the postal and courier category; it is more likely captured under transport (Annex I) if the company operates transport infrastructure, or under manufacturing or digital providers if its primary activity is elsewhere. A logistics company that also provides last-mile delivery parcels, however, may fall within postal and courier scope depending on how the relevant member state has transposed the directive. Size thresholds apply: organisations with more than 250 employees and €50 million turnover, or more than €43 million in balance sheet total, are subject to the full regime; smaller organisations may be captured where they operate in critical sub-sectors.

The core obligations under Article 21 require all in-scope entities to implement appropriate and proportionate technical, operational, and organisational cybersecurity risk management measures. These must address: risk analysis and information security policies; incident

handling; business continuity and crisis management; supply chain security; procurement, development and maintenance of network and systems; cybersecurity hygiene and training; cryptography and encryption policies; human resources security; access control; and multi-factor authentication. Article 23 requires incident reporting in three stages — an early warning within 24 hours of becoming aware of a significant incident, a full notification within 72 hours, and a final report within one month. Fines under NIS2 can reach €10 million or 2% of global annual turnover for essential entities, and €7 million or 1.4% for important entities.

THE EXTRATERRITORIAL MECHANISM

Unlike the CRA — which applies to products placed on the EU market — NIS2 applies to entities that provide services in the EU. Article 26 of the Directive requires non-EU entities that provide in-scope services in the EU to designate a representative in one of the member states where they provide services. That member state becomes the jurisdiction responsible for supervising that entity's NIS2 compliance. The practical effect is that a Swiss managed service provider with German or French customers, or a UK cloud infrastructure operator with Belgian or Dutch clients, may be fully subject to NIS2's obligations — including registration, Article 21 risk management, and Article 23 incident reporting — regardless of Brexit or Switzerland's bilateral arrangements.

Beyond direct scope, the supply chain provisions of NIS2 have a second-order reach that extends significantly further. Article 21(2)(d) requires in-scope entities to adopt policies on supply chain security covering their relationships with direct suppliers and service providers. Member state authorities have begun issuing guidance that explicitly requires NIS2-regulated entities to conduct security assessments of their suppliers, impose contractual cybersecurity requirements on them, and in some cases arrange audits. A Swiss IT provider or a UK software firm that is not itself in NIS2's scope may nonetheless find that its EU customers are required to impose NIS2-equivalent security obligations on it as a condition of their own compliance. In practice, this makes NIS2 a supply chain standard as much as a direct regulatory requirement. A note on Germany and the KRITIS framework: Germany's implementation of NIS2 illustrates how national transposition layers on top of — and sometimes significantly extends — the EU baseline. Germany enacted its NIS2 Implementation Act (NIS2UmsuCG) in December 2025, bringing approximately 30,000 organisations into scope — up from around 4,700 under the previous KRITIS and NIS1 framework. Alongside this, Germany enacted the KRITIS-DachG (the KRITIS Umbrella Act), which came into force on 17 March 2026. These two laws are complementary but distinct: the NIS2 Implementation Act governs cybersecurity obligations — IT risk management, incident reporting, and technical security measures — and is Germany's transposition of NIS2. The KRITIS-DachG implements a separate EU instrument, the Critical Entities Resilience (CER) Directive, and governs physical resilience: protection against natural disasters, sabotage, and physical infrastructure outages. Operators of critical facilities in Germany must comply with both laws simultaneously — the NIS2 Act for their digital security posture, and the KRITIS-DachG for their physical resilience. The two instruments are not redundant; they cover different risk dimensions of the same critical infrastructure. For Swiss and UK companies with German operations or German customers, both layers are relevant: NIS2 compliance (through the NIS2 Implementation Act) is the

cybersecurity floor, while physical resilience under the KRITIS-DachG adds a further layer of obligation for entities operating critical physical facilities in Germany.

2. Switzerland: Parallel Architecture, Narrower Scope

2.1 Direct NIS2 Exposure for Swiss Organisations

Swiss companies are not EU member states and are not obliged to transpose NIS2. But the extraterritorial provision in Article 26 means that Swiss organisations operating in classified sectors and providing services to EU customers may be directly subject to NIS2's requirements through the national law of whichever EU member state they designate as their representative jurisdiction. This is not a theoretical risk. Switzerland's technology sector — cloud service providers, managed security operators, colocation data centres, trust service providers, and DNS operators — has deep commercial ties with EU clients.

Determining whether a Swiss organisation is in scope requires a two-step analysis: first, whether the organisation's activities fall within one of NIS2's 18 covered sectors; and second, whether the organisation meets the size thresholds or falls within a sub-category exempt from those thresholds. For Swiss companies already undertaking this analysis in connection with the GDPR or other EU regulations, the exercise is familiar in structure — but NIS2's sector classifications and the specific definitions of 'essential' and 'important' entities require careful review against the national implementing law of the relevant EU member state, since transposition is not fully uniform.

A further complexity for Swiss multinationals is that EU subsidiaries — branches or affiliated entities established in EU member states and operating above the relevant thresholds — are directly subject to NIS2 through those entities' national law, regardless of where the parent company is headquartered. For Swiss-headquartered groups with EU operations, NIS2 compliance is not optional — it is a live obligation for the EU parts of the business.

SUPPLY CHAIN PRESSURE: THE INVISIBLE COMPLIANCE OBLIGATION

Even Swiss companies that are not directly in scope face NIS2 indirectly. A Swiss pharmaceutical packaging supplier to a German hospital group, or a Swiss IT services firm supporting a French energy operator, may be required by its EU customer to demonstrate NIS2-aligned security practices, provide audit access, sign specific contractual security terms, and report incidents within NIS2 timelines — all as a condition of the EU entity's own regulatory compliance. This supply chain pull is already being felt in Swiss export sectors and is likely to intensify as EU member states publish more detailed guidance on supply chain obligations.

2.2 The Swiss Information Security Act (ISG) and KRITIS-G

Switzerland has been developing its own critical infrastructure cybersecurity framework independently of the EU, though with clear awareness of NIS2's direction. The Information Security Act (Informationssicherheitsgesetz, ISG) entered into force on 1 January 2024 and establishes the core framework for information security in Swiss federal authorities, cantonal and communal bodies, and private organisations that process data or provide IT services on

their behalf. It sets out obligations around risk management, security classification, incident management, and auditing.

The ISG was extended in 2024–2025 through a key amendment: from 1 April 2025, operators of critical infrastructure in Switzerland are required to report significant cyberattacks to the National Cyber Security Centre (NCSC) within 24 hours of becoming aware of them. This reporting obligation extends across the federal and cantonal public sector and to a defined list of private critical infrastructure operators, including those in energy, transport, water, finance, and health. In structure — a 24-hour initial notification to a central national authority — this closely mirrors NIS2's Article 23 early-warning obligation, representing a deliberate convergence with EU standards on the most operationally critical element of the regime.

The ISG alone, however, covers a narrower range of sectors than NIS2 and does not yet impose the full suite of Article 21 risk management measures or the supply chain security obligations that NIS2 requires. Recognising this gap, the Swiss government is developing new critical infrastructure protection legislation — commonly referred to as KRITIS-G — alongside amendments to the ISG, collectively described in some commentaries as the 'Swiss Cyber Act'. The legislation is structured around three instruments: the KRITIS-G law establishing sectoral coverage, risk management duties, and incident reporting; a revised ISG aligning public administration cybersecurity with EU standards; and a KRITIS-V ordinance defining compliance thresholds and sector-specific rules.

Alignment with NIS2

The KRITIS-G architecture mirrors NIS2's design in several respects: sectoral scope, a tiered entity classification, risk management obligations, incident reporting, and enforcement through the NCSC with audit powers and binding orders. The legislation is expected to be ready for parliamentary process by 2027, with the Federal Council having explicitly cited NIS2 as a reference standard in framing the bill's mandate. Key points of divergence from NIS2 are likely to include the following.

- Sector coverage: KRITIS-G is expected to cover Switzerland's critical infrastructure sectors — energy, water, transport, finance, health — but the full 18-sector scope of NIS2, including food, space, waste management, and manufacturing, has not been confirmed for the initial Swiss legislation.
- Size thresholds: Switzerland's critical infrastructure community is smaller than the EU's. The legislation is likely to apply sector-specific thresholds rather than the NIS2 turnover and headcount criteria, which were calibrated for the EU's much larger single-market economy.
- Management liability: NIS2 introduces explicit personal accountability provisions for management bodies of in-scope entities. Whether KRITIS-G replicates this is not yet confirmed; Swiss corporate governance traditions have historically resisted director-level regulatory liability in non-financial sectors.
- Mutual recognition: Switzerland and the EU have not established a mechanism for mutual recognition of NIS2 compliance assessments. A Swiss entity compliant with KRITIS-G will not automatically be considered NIS2-compliant by EU member state authorities, and vice versa.

The practical position for Swiss organisations is that they face a period of dual-track compliance: NIS2 obligations for EU-market and EU-service activities on one track, and the

emerging KRITIS-G framework for domestic operations on the other. The two tracks are moving toward the same destination but are not yet synchronised, and the gap between them creates both compliance complexity and, for some organisations, a temptation to treat the domestic Swiss obligations as the governing standard — an approach that underestimates the reach of NIS2 through the Article 26 and Article 21 supply chain mechanisms.

3. The United Kingdom: Reforming Independently with NIS2 in Sight

3.1 NIS2's Direct Reach into UK Organisations

The UK departed from the EU before NIS2 was adopted and is under no obligation to transpose it. The NIS 2018 Regulations, which implemented the original NIS Directive, remain the domestic UK framework for network and information systems security. However, like Switzerland, the UK faces NIS2's extraterritorial reach through the Article 26 mechanism. UK companies that provide in-scope services to EU customers — cloud computing, managed security services, online marketplaces, DNS services, trust services — may be directly subject to NIS2 through the national law of their designated EU member state.

The scale of UK exposure here is arguably larger than Switzerland's, given the size and depth of the UK's digital services sector and its historic integration with European markets. UK-headquartered cloud providers, managed service providers, and digital infrastructure operators with significant EU customer bases have been assessing their NIS2 status since 2023. For those that determine they are in scope, the obligations are substantive: registration with an EU national authority, appointment of an EU representative, full Article 21 risk management implementation, and Article 23 incident reporting — all governed by the national law of the member state where they register, which may contain additional requirements beyond the NIS2 minimum.

UK businesses with EU subsidiaries are in the same position as their Swiss counterparts: the EU entities are directly subject to national NIS2 implementations, regardless of where the group's parent is headquartered. For large UK-based multinationals with operations across the EU, NIS2 is already an operational reality — not a future horizon.

3.2 The UK NIS 2018 Regulations: A Framework That Has Aged

Before Brexit, the UK implemented the original NIS Directive through the Network and Information Systems Regulations 2018. Those regulations remain in force and cover operators of essential services in seven sectors — transport, energy, health, drinking water, digital infrastructure — and three categories of digital service providers: online marketplaces, online search engines, and cloud computing services. They impose risk management and incident reporting obligations backed by penalties of up to £17 million.

Against NIS2, the NIS 2018 Regulations show their age in several respects. The sector coverage is substantially narrower: NIS2's 18 sectors include managed service providers, data centres, waste management, space, food, chemicals, postal services, and manufacturing — none of which are captured by the UK 2018 framework. The incident reporting timeline under the 2018 regulations is 72 hours — matching NIS2's second-stage notification but lacking the 24-hour early-warning requirement. Supply chain security obligations are less prescriptive. There is no equivalent to NIS2's management liability provisions. And the 2018 framework predates the managed-service-provider threat landscape that has become central to European cyber policy since then.

The NCSC's Cyber Assessment Framework (CAF) provides detailed implementation guidance for the 2018 regulations and is widely used by UK operators. The CAF is broadly aligned with international standards including ISO 27001 and NIST, and much of its substantive content would satisfy NIS2's Article 21 requirements. However, CAF compliance under the 2018 regulations has been a matter of regulatory expectation rather than strictly enforced legal obligation, and the framework's elevation to legally binding status is one of the core changes introduced by the Cyber Security and Resilience Bill.

3.3 The Cyber Security and Resilience Bill: NIS2 Influence, British Architecture

The UK Government introduced the Cyber Security and Resilience (Network and Information Systems) Bill to Parliament on 12 November 2025. It is the most significant overhaul of UK cyber legislation since 2018 and is explicitly framed as a response both to the evolving threat landscape — accelerated by high-profile attacks on Marks and Spencer, Jaguar Land Rover, and the NHS in 2025 — and to the widening gap between the UK's 2018 framework and EU NIS2.

The Bill proposes to amend the NIS 2018 Regulations materially. It expands the scope of regulated entities to include managed service providers (MSPs) and data centres — two categories not currently covered that are central to NIS2's 'important entities' category. It introduces the concept of Designated Critical Suppliers (DCS): a power for regulators to designate specific supply chain providers as falling within the regulatory scope directly, bringing them under cybersecurity obligations and incident reporting duties. The DCS concept is presented by the UK government as a supply chain risk measure, and it does extend direct legal obligations to suppliers who would not otherwise be in scope. Whether this meaningfully “goes beyond” NIS2 is debatable: NIS2 Article 21(2)(d) requires regulated entities to manage supply chain security and imposes contractual pull-through obligations on suppliers in practice. The DCS mechanism formalises this differently — placing obligations directly on designated suppliers by regulatory order rather than through contractual cascade — but the practical security outcome is not obviously superior. The UK government's own policy statement notes that DCS obligations will not be more stringent than those for operators of essential services, limiting how far the designation extends the substance of obligations. It is more accurate to describe DCS as a structural innovation in regulatory architecture than as a substantive expansion of security requirements beyond NIS2. The Bill also elevates the NCSC's CAF to legally binding status, tightens incident reporting timelines, and introduces a two-tier penalty regime with fines up to £17 million for essential services and proportionate penalties for other regulated entities.

As of May 2026, the Bill has completed its committee stage in the House of Commons and is approaching the Report Stage. Royal Assent is expected in late 2026, with phased implementation through secondary legislation running to approximately 2028.

Comparison with NIS2: Alignment and Divergence

- Incident reporting timelines are aligned: the Bill introduces 24-hour and 72-hour notification obligations that match NIS2's Article 23 structure — a deliberate convergence that eases dual-compliance for businesses operating in both jurisdictions.

- Sector scope remains narrower: NIS2 covers 18 sectors including space, food, chemicals, manufacturing, and public administration at all levels. The Bill's expansion focuses on MSPs and data centres, and does not bring the full NIS2 sector list into scope. Public administration outside central government, the food sector, and manufacturing remain outside the UK framework.
- The DCS regime introduces a structural difference in how supply chain obligations are enforced: rather than relying solely on contractual cascade from regulated entities, regulators can designate specific suppliers directly. Whether this represents a substantive improvement over NIS2's approach or simply a different architectural choice is genuinely contested. The UK government's own documentation confirms that DCS obligations will not exceed those of operators of essential services — so the ceiling is the same; the delivery mechanism differs.
- No customer notification requirement: NIS2 obliges in-scope entities, in certain circumstances, to notify customers affected by significant incidents. The Bill does not include an equivalent provision.
- Management liability: NIS2 explicitly holds management bodies accountable for approving cybersecurity risk management measures and makes members personally liable for infringements. The Bill introduces greater board accountability, but the regime for personal liability is less explicit than under NIS2.
- Reliance on secondary legislation: the Bill establishes a framework, with detailed security requirements to be specified through secondary legislation and NCSC guidance. This gives the UK greater flexibility to update its framework quickly but creates more uncertainty for businesses trying to plan long-term compliance programmes.

A STRUCTURAL DIFFERENCE WORTH NOTING

NIS2 is a directive, meaning it requires transposition into national law by each member state, which also permits member states to impose stricter requirements if they choose. Germany's transposition, for instance, captures approximately 30,000 entities and introduces sector-specific thresholds not in the EU text itself. The UK Bill amends existing UK secondary legislation and is itself a primary Act — a single national instrument rather than 27 national implementations of a common baseline. This means the UK framework is more uniform across its jurisdiction than NIS2 is across the EU (where transposition varies significantly), but it also means the UK lacks the cross-border supervisory cooperation and information-sharing architecture that NIS2 builds into the EU system. Neither approach is inherently superior; they reflect different regulatory traditions and institutional contexts.

4. Comparative Overview

The table below presents the regulatory position across the three relevant jurisdictions (EU NIS2, Switzerland, and Great Britain) as of May 2026. The KRITIS-G law is expected but not yet enacted; the CS&R Bill is in its final parliamentary stages. Both the Swiss and UK columns therefore reflect a current/anticipated composite position.

Obligation	EU NIS2	Switzerland (ISG/KRITIS)	Great Britain (CS&R Bill)
Legally binding	Yes (via transposition)	ISG in force; KRITIS-G bill by 2027	CS&R Bill — Royal Assent 2026
Sectors covered	18 critical sectors	Critical infra + public admin	~same as NIS 2018 + MSPs/data centres
Risk mgmt measures	Art. 21 — 10 mandatory measures	ISG Art. 6–23 (aligned)	CAF (NCSC) elevated to binding
Incident reporting	24h / 72h / 1-month	24h to NCSC (from Apr 2025)	24h / 72h (aligned with NIS2)
Supply chain security	Mandatory due diligence	Vendor-risk frameworks required	DCS regime (new)
Management liability	Yes — personal accountability	Not yet explicit	Being introduced via Bill
Registration of entities	National authority registers	NCSC/sector registration	Enhanced registration required
Fines	€10M or 2% global turnover	TBD under KRITIS-G	Up to £17M or 10% turnover
Non-EU entity scope	Yes — services provided in EU	EU subsidiaries in scope	Domestic only

The table reveals an important asymmetry: in both Switzerland and the UK, domestic legislation is catching up to NIS2 in intent but is currently less comprehensive in scope, less prescriptive in risk management detail, and — for Switzerland — still partially unlegislated. Organisations that benchmark themselves against NIS2 for EU compliance purposes will, in most respects, be exceeding the current domestic requirements in both countries. This does not mean NIS2 compliance is sufficient to satisfy domestic obligations; it means the domestic obligations are currently a lower bar. As KRITIS-G and the CS&R Bill come into force, the gap will narrow — but the administrative separation of distinct national regimes will remain.

5. Practical Implications for Businesses

5.1 Swiss Organisations

Swiss organisations face NIS2 obligations through three distinct channels, each requiring a different response. The first is direct scope: organisations in covered sectors providing services to EU customers should conduct a formal NIS2 scoping analysis, identify the relevant member state(s) for registration, appoint an EU representative under Article 26, and implement Article 21 risk management measures. This is a compliance programme of similar scale to GDPR implementation.

The second channel is through EU subsidiaries, which are directly subject to national NIS2 implementations as domestic law. Group cybersecurity programmes should encompass EU entities' NIS2 obligations as a matter of priority, rather than treating them as a localised compliance matter for in-country teams to handle in isolation.

The third channel is supply chain pressure: even where a Swiss organisation is not itself in scope, its EU customers may be required to impose NIS2-aligned security requirements contractually. Establishing a credible security posture — documented against a recognised framework such as ISO 27001, aligned with the ISG's requirements, and able to respond to EU customer audit requests within NIS2-consistent timelines — is the most efficient way to address this channel. Companies that wait for contractual demands to arrive before building their security programmes will find themselves responding reactively to multiple simultaneous customers with overlapping but not identical requirements.

5.2 UK Organisations

UK businesses with EU operations or EU-service exposure are in a broadly similar position to Swiss organisations: direct NIS2 obligations through Article 26 for those providing in-scope services in the EU, group-level obligations for UK parents with EU subsidiaries, and supply chain pressure across all sectors. The same three-channel framework applies.

For UK businesses operating purely domestically, the CS&R Bill introduces materially expanded obligations — particularly for MSPs, data centres, and any organisations that become Designated Critical Suppliers. Compliance planning should begin now, notwithstanding that Royal Assent and secondary legislation are still to come. The incident reporting timelines in the Bill (24h/72h) will align with NIS2, meaning that businesses compliant with the Bill's reporting obligations will also satisfy NIS2's in that specific respect. The broader risk management obligations, however, may require additional work for organisations whose current posture was calibrated against the NIS 2018 framework.

5.3 Does NIS2 Compliance Cover Domestic UK and Swiss Obligations?

The central question for any Swiss or UK organisation operating in or providing services to the EU is: if we comply fully with NIS2, does that also satisfy our domestic legal obligations in

Switzerland or the UK? The answer is no — not automatically, and not in full. NIS2 creates obligations for organisations in scope in the EU. Domestic Swiss and UK law creates separate, parallel obligations for the same or similar entities operating in those markets. The two frameworks must both be satisfied; one does not substitute for the other.

For Switzerland: as of May 2026, there is no directly applicable domestic infrastructure cybersecurity law equivalent to NIS2 — the ISG covers the public sector and critical infrastructure incident reporting, but the full KRITIS-G framework is not yet in force. Companies meeting NIS2 obligations for EU-facing services will typically exceed what Swiss domestic law currently requires. Once KRITIS-G enters force (expected 2027), it will introduce distinct obligations — registration with Swiss authorities, risk management to Swiss standards, reporting to the Swiss NCSC — that sit alongside NIS2 obligations even where the substantive requirements overlap. There is no mutual recognition arrangement: NIS2 compliance does not discharge KRITIS-G obligations, and vice versa.

For the UK: NIS2 and the CS&R Bill are entirely separate legal instruments. A UK organisation providing services in France under NIS2 must register with the French national authority (ANSSI), implement Article 21 risk management, and report to ANSSI and the French CSIRT. The same organisation providing UK-domestic services as an MSP or data centre must, once the CS&R Bill is in force, register with the relevant UK regulator, implement CAF-compliant risk management, and report to the NCSC under the UK 24h/72h regime. The two reporting obligations go to different authorities on different national portals. Incident reporting timelines are aligned (both 24h/72h), which eases dual compliance on that specific element, but registration, supervisory relationships, and sector classifications are handled independently in each jurisdiction.

The practical implication is that an organisation operating across all three jurisdictions — EU, Switzerland, and the UK — faces three overlapping but legally distinct compliance programmes. The most efficient approach is to build security programmes to the NIS2 standard (which is currently the most comprehensive), document compliance in a way that maps to all three frameworks, and manage the jurisdiction-specific administrative steps — registration, authority contacts, national reporting portals — as distinct but parallel workstreams. On 20 January 2026, the European Commission proposed targeted amendments to NIS2 aimed at simplifying compliance for smaller entities, a signal that the framework is entering a maturation phase. That simplification should reduce, not increase, the gap between NIS2 and domestic frameworks over time — but it will not eliminate the need for jurisdiction-specific compliance steps in Switzerland and the UK.

6. Conclusions

NIS2 represents a fundamentally different kind of regulatory reach from product regulations like the CRA or PPWR. It does not attach to goods or packaging — it attaches to the organisations that operate critical services and digital infrastructure. Through the Article 26 extraterritorial mechanism and the Article 21 supply chain obligations, it reaches deep into the Swiss and UK economies without requiring either country to transpose the Directive or surrender any regulatory sovereignty. The result is a compliance landscape of considerable complexity for organisations with EU market exposure.

Switzerland enters this landscape with a domestic framework that is structurally compatible with NIS2 but not yet equivalent. The ISG's incident reporting obligation for critical infrastructure, in force from April 2025, is the most concrete domestic convergence point. KRITIS-G, when enacted, will provide a more complete alignment — but it will arrive after many Swiss organisations have already had to engage with NIS2 directly through EU market obligations. The window between now and 2027 is one in which Swiss organisations face a genuine dual-regime compliance burden, with no mutual recognition arrangement to ease it.

The United Kingdom's trajectory is more advanced. The CS&R Bill is close to enactment, its incident reporting timelines deliberately mirror NIS2, and the NCSC's CAF — when elevated to binding status — will provide a substantive risk management framework broadly consistent with NIS2's Article 21 requirements. The gaps in sector scope and management liability are real, but they reflect deliberate UK policy choices rather than inadvertent divergence. For UK businesses, the immediate priority is less about closing an awareness gap and more about operationalising compliance: building the governance structures, security programmes, and incident response capabilities that both the CS&R Bill and NIS2 require. UK businesses operating cross-border services that touch both UK-domestic and EU markets must manage both the CS&R Bill (domestic) and NIS2 (EU-facing) as distinct regulatory obligations.

For all organisations in both countries, the overarching message is that NIS2 is already an operational reality — through EU subsidiaries, through EU customers' supply chain requirements, and through the Article 26 extraterritorial mechanism. The question is no longer whether to engage with it but how to do so efficiently, in a way that supports rather than duplicates emerging domestic compliance obligations in Switzerland and the UK. To be clear: NIS2 is organisational and infrastructure law — it governs how entities operate their systems. This is distinct from the CRA, which governs the cybersecurity properties of products. A company may face obligations under both, but they address different dimensions: NIS2 asks “how secure are your operations?”; the CRA asks “how secure is your product?” There is no redundancy between the two.

References and Further Reading

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Official Journal of the EU, 27 December 2022.

European Commission, NIS2 Transposition Tracker and Infringement Proceedings, digital-strategy.ec.europa.eu, November 2024 — May 2025.

European Commission, Proposed Amendments to NIS2 Directive (Cybersecurity Package), 20 January 2026.

Swiss Federal Act on Information Security (ISG / Informationssicherheitsgesetz), in force 1 January 2024; incident reporting amendment in force 1 April 2025.

Swiss Federal Council — Mandate to Develop KRITIS-G Critical Infrastructure Protection Legislation, August 2025.

UK Network and Information Systems Regulations 2018 (SI 2018/506), implementing Directive (EU) 2016/1148.

UK Cyber Security and Resilience (Network and Information Systems) Bill, introduced to Parliament 12 November 2025. Committee Stage completed February 2026.

UK Government, Cyber Security and Resilience Bill: Policy Statement, Department for Science, Innovation and Technology, November 2025.

Mayer Brown LLP, United Kingdom Proposes Changes in the Cyber Security and Resilience Bill — Key Differences to NIS2, March 2026.

VISCHER AG, Scaling the Swiss Information Security Act — Its New Amendment and Implications for Financial Institutions, March 2025.

Wavestone, NIS2 Directive: Transposition Status Across Europe, updated January 2026.

OpenKRITIS, NIS2 Implementation in Germany (BSIG / NIS2UmsuCG), updated 2026. Noerr LLP, Cybersecurity Briefing Q4 2025 — NIS2 Implementation and KRITIS-DachG in Germany, December 2025.