GIR Global Investigations Review

Europe, Middle East and Africa Investigations Review

2026

Europe, Middle East and Africa Investigations Review

2026

The 2026 edition of the Europe, Middle East and Africa Investigations Review contains thought leadership from pre-eminent practitioners from the region, capturing the most substantial recent international investigations developments. The result is an invaluable collection that is part aide-memoire and part horizon-scanning tool for anyone who specialises in investigating and resolving suspected corporate wrongdoing in Europe, the Middle East and Africa.

Generated: April 25, 2026

GIR Global Investigations Review

Explore on **GIR**

Contents

Overviews

Country chapters

The convergence of anti-corruption, counter-fraud and financial integrity in the GCC: what it means for investigations

Ralph Stobwasser and **Tarek Bleik**
Secretariat

Summary

IN SUMMARY

Over the past 12 to 24 months, Gulf Cooperation Council (GCC) jurisdictions have continued shifting from parallel anti-corruption, anti-money laundering (AML), sanctions and transparency reforms towards a more integrated financial integrity model. That shift matters less for legal labels than for its impact on investigative practice. A procurement, bribery or fraud matter that once might have been scoped narrowly, now requires early assessment of beneficial ownership, suspicious transaction reporting, sanctions exposure, governance failures and asset-preservation options. For investigators, the real development is convergence in consequence.

DISCUSSION POINTS

- Why Financial Action Task Force (FATF) and Middle East and North Africa Financial Action Task Force (MENAFATF) effectiveness pressures are pushing GCC authorities towards more visible enforcement outcomes
- How economic diversification, procurement intensity and cross-border capital flows are widening the practical scope of investigations
- Why the United Arab Emirates remains the clearest example of implementation intensity, especially in supervisory action and Designated Non-Financial Businesses and Professions (DNFBP) exposure
- How Saudi Arabia and Qatar illustrate different but related forms of integrity convergence
- Why beneficial ownership, asset tracing and sanctions screening now need to sit nearer the start of an investigation

REFERENCED IN THIS ARTICLE

- Saudi Nazaha materials and relevant Saudi beneficial ownership and counter-fraud guidance
- UAE AML/CFT, targeted financial sanctions and counter-proliferation legislation, executive regulations, supervisory notices and public enforcement announcements
- Qatar integrity, transparency and anti-corruption strategy materials
- Bahrain, Kuwait and Oman mutual evaluation, supervisory and public-sector integrity materials, including rulebooks, follow-up reports, beneficial ownership guidance and audit or disclosure frameworks
- Relevant public enforcement actions, regulatory announcements and case examples referred to in the text
- FATF and MENAFATF materials on effectiveness, mutual evaluation and beneficial ownership transparency

THE END OF SILOED INVESTIGATIONS

For much of the past decade, financial crime risk in the GCC was often analysed along parallel tracks. Anti-corruption was usually treated as a criminal issue. AML obligations were seen as a regulatory matter for banks and certain financial institutions. Corporate transparency sat in a separate governance bucket. Sanctions were often considered only where there was obvious trade or geopolitical exposure. That separation was never complete, but it often shaped how internal teams, advisers and even investigations were organised.

That model is becoming harder to sustain. Across the GCC, authorities are giving more practical effect to the idea that bribery, fraud, money laundering, ownership opacity, sanctions circumvention and weak governance controls are not isolated phenomena. They are often different expressions of the same integrity problem. The shift is not simply conceptual. It affects how a matter is detected, how quickly it escalates and what evidence becomes important early in the process.[1]

For investigators, that means a narrower question now carries broader consequences. A procurement complaint may also raise beneficial ownership questions, suspicious transaction reporting exposure, sanctions screening issues, failures in third-party onboarding and the possibility of earlier asset restraint. A matter that begins as a misconduct review may therefore become, within days rather than months, a multi-regime exercise involving legal, compliance, forensic and regulatory stakeholders.[2]

This is the practical significance of financial-integrity convergence in the GCC. The region is not unique in moving in this direction. Similar themes appear elsewhere, but in the GCC the shift has particular force because of the interaction between state-led economic transformation, high-value procurement, cross-border financial flows, strong reputational incentives linked to international evaluation and the growing visibility of supervisory enforcement. In that setting, the cost of scoping a case too narrowly has increased.

This article focuses on that change. It does not attempt a primer on every anti-corruption or AML rule in the region. Instead, it examines the most significant regional development of the past 12 to 18 months: the increasing tendency to treat anti-corruption, AML, beneficial ownership, sanctions and governance as parts of a single financial-integrity framework. It then considers how that appears in selected GCC jurisdictions and what it means for the practical design of investigations[3].

WHY THE GCC IS MOVING TOWARDS FINANCIAL-INTEGRITY ENFORCEMENT

Three forces are driving this shift. First, international evaluation continues to matter. FATF and MENAFATF assess not only technical compliance, but effectiveness: supervisory activity; use of financial intelligence; confiscation; coordination and credible enforcement. That pushes authorities beyond legal reform towards visible operational outcomes. For investigations, the implication is straightforward: jurisdictions under pressure to show effectiveness have a stronger incentive to connect corruption, money laundering, ownership evidence and asset tracing rather than treat them separately.

Second, economic transformation has increased the scale and complexity of regional risk. Major investment programmes, state-linked procurement, financial-centre growth and cross-border trade create more complex and layered fact patterns. A procurement issue may involve foreign suppliers, local intermediaries, offshore vehicles and high-value assets, making it difficult to assess through a bribery lens alone.

Third, data visibility has improved. Beneficial ownership registers, stronger due diligence, reporting obligations, DNFBPs scrutiny and sanctions controls mean that more integrity-relevant information is now created and expected to be reconciled. That allows investigations to widen faster and inconsistencies to surface earlier.

A simple example shows the change. If a contractor on a public project pays unusual "advisory fees" to a local intermediary, the question is no longer just whether bribery occurred. Investigators may also need to test beneficial ownership, onboarding, reporting obligations, sanctions screening, onward movement of funds and potential asset dissipation from the outset.

That is why the key development is not simply tougher enforcement, but convergence in consequence. The legal regimes remain distinct, but the practical result is increasingly integrated: a single matter can now generate parallel criminal, regulatory and governance exposure much earlier than before.

HOW THE SHIFT IS PLAYING OUT ACROSS THE GCC

United Arab Emirates

The United Arab Emirates is a clear example of implementation intensity in the region. The significance of recent UAE developments lies not only in legislation and guidance, but in the growing visibility of supervisory action and the widening perimeter of sectors expected to maintain effective financial crime controls. For that reason, the United Arab Emirates offers a useful case study of how financial-integrity convergence affects investigations.[4]

First, the United Arab Emirates has moved beyond pure framework-building. Earlier reform phases focused heavily on legislative alignment, institutional architecture and demonstrating commitment to international standards. Those foundations remain important. But the more telling signal in the past 12 to 18 months has been operational. Public enforcement messaging, supervisory action and sustained emphasis on control effectiveness have reinforced the idea that weaknesses in AML systems may themselves become material events, even before any underlying criminal case is fully established.

That matters because many investigations in the United Arab Emirates now touch sectors beyond traditional banking. Real estate intermediaries, precious metals dealers, company-service providers, exchange houses and other higher-risk non-bank actors sit much closer to the centre of the enforcement picture than before. This widens the range of actors whose records, controls and reporting decisions may become relevant in a corruption or fraud investigation.

The second point is beneficial ownership. In UAE-linked matters, ownership analysis is no longer merely a corporate-housekeeping exercise. It is often one of the fastest ways to test the legitimacy of a counterparty relationship, identify undeclared related parties or understand where influence actually sat within a transaction chain. Where free zones, layered holding structures, nominee arrangements or family-linked entities are involved, ownership work can quickly reshape interview strategy, document requests and the assessment of personal exposure.[5]

The third point is sectoral supervision. The United Arab Emirates has increased scrutiny of sectors that historically served as gateways for value transfer, structuring or asset parking. That is especially relevant in real estate and precious metals, where investigators may need to reconcile transactional records, source-of-funds explanations and ownership information

with the primary misconduct narrative. The legal issue may still be bribery or fraud. But the practical work often turns how value moved through sectors that are now more closely supervised for AML purposes.[6]

This has at least three investigative consequences. First, scoping decisions need to include non-bank actors earlier. Second, investigations teams need to assume that control failures may attract supervisory attention even where criminal liability remains uncertain. Third, asset-tracing hypotheses should be formed earlier, especially where funds may have moved into property, commodities or layered corporate structures.

UAE 2025 public enforcement signals

Area	2025 public signal	Why it matters
DNFBP supervision (MOET)	*In July 2025, the Ministry of Economy and Tourism reported that its H1 2025 AML inspections found 1,063 violations and imposed fines exceeding 42 million dirhams across supervised DNFBP sectors, including 495 violations in real estate brokerages (18.5 million dirhams), 473 among precious metals and stones traders (20 million dirhams), and 95 penalties involving corporate service providers and auditors (more than 4 million dirhams).*[7]	*Demonstrates that visible supervisory pressure is now extending well beyond banks and is concentrated in sectors that often sit closest to ownership opacity, funds flows and asset parking.*
Foreign bank branches (CBUAE)	*In May 2025, the Central Bank imposed 18.1 million dirhams in sanctions on two foreign bank branches for AML/CFT failures identified through examinations, followed in July 2025 by a further 5.9 million dirhams sanction on another foreign bank branch.*[8]	*Indicates that enforcement is not limited to local institutions, and that branches of international banks are also being tested on framework effectiveness.*
Exchange houses: high - value sanctions	*Public 2025 CBUAE notices also included very large sanctions on exchange houses, including 200 million dirhams in May 2025 and 100 million dirhams later that month, both linked to significant AML/CFT failures.*[9]	*Reinforces that higher - risk financial gatekeepers remain central to the United Arab Emirates' enforcement model.*
Closures / licence action	*CBUAE revoked the licence of Sundus Exchange in June 2025 and imposed*	*Important because the public enforcement record is not just about fines: in*

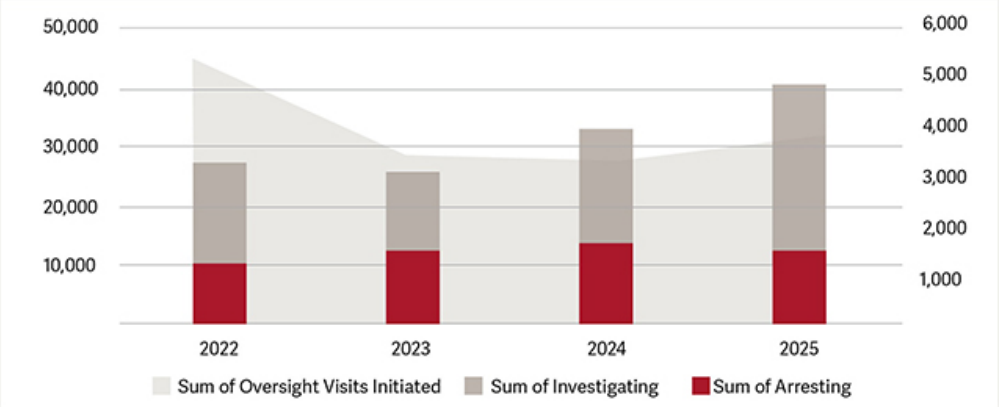
	a 10 - million - dirham sanction; it also revoked the licence of Omda Exchange in December 2025 and imposed a further 10 - million - dirham sanction.[10]	*some cases, it extends to removal from the market.*
Individual liability	*In the May 2025 200 - million - dirham exchange - house case, CBUAE also imposed a 500,000 - dirham sanction on a branch manager and prohibited that individual from holding any position in a licensed financial institution in the UAE.*[11]	*Demonstrates that public enforcement can also reach responsible individuals, not only firms.*
Targeted financial sanctions / CPF	*In December 2025, MOET issued a circular to supervised DNFBPs requiring them to update sanctions screening, re - screen customers and beneficial owners, freeze without delay, and report matches, in connection with the re - imposition of UN sanctions related to Iran.*[12]	*Indicates that sanctions and counter - proliferation controls are being operationalised alongside AML supervision rather than treated as a separate silo.*

Saudi Arabia

Saudi Arabia illustrates the same regional direction, but through a somewhat different emphasis. The clearest recent signal is not a single flagship reform, but the cumulative effect of active anti-corruption enforcement, tighter governance expectations, a new beneficial ownership framework and the practical reality of very large project and procurement environments. In 2025, the Saudi Oversight and Anti-Corruption Authority (Nazaha) reported 32,389 inspection raids, 4,873 criminal and administrative cases and 1,504 arrests. The sectors most frequently appearing in corruption reporting remained Interior, Health, Education and Municipalities & Housing, while Hajj & Umrah emerged as a distinct area of focus, underlining how public-facing, seasonal and procurement-intensive activity can generate concentrated integrity risk.[13]

Sum of Oversight Visits, Investigations and Arrests

	Oversight Visits	Investigations	Arrests
2022	44,871	3,308	1,255
2023	28,933	3,124	1,511
2024	28,430	4,000	1,708
2025	32,389	4,873	1,504
Grand Total	**134,623**	**15,305**	**5,978**



Source: Saudi Oversight and Anti-Corruption Authority "Nazaha" (-https://www.nazaha.gov.saand https://x.com/nazaha_en)

Saudi Arabia's scale matters. In a market shaped by state-led transformation, strategic projects and extensive public-facing procurement, integrity questions are not confined to whether a payment was improper. They often concern who actually stood behind an intermediary, who exercised influence over a supplier relationship, how funds moved after disbursement and whether the relevant institutions had controls capable of identifying warning signs. Nazaha's published case examples show the kinds of fact patterns that continue to shape anti-corruption and counter-fraud risk in Saudi Arabia. The cases are varied, but they point to recurring themes: procurement manipulation, licensing abuse, customs facilitation, unexplained wealth and the misuse of public position to influence commercial outcomes.[14]

- Municipal tender manipulation: Nazaha has also reported cases involving municipal employees receiving payments in exchange for unlawfully awarding public tenders to commercial entities, underlining continuing procurement and contracting risk at local-government level.
- Customs facilitation and import fraud: other cases have involved bribery to facilitate unlawful imports, showing the overlap between corruption, border controls and trade-linked risk.
- Licensing abuse and unexplained wealth: Nazaha has likewise reported cases in which officials used licensing or regulatory authority to benefit commercial entities, with subsequent scrutiny of bank accounts and wealth that could not be legitimately explained.

Taken together, these examples matter less as isolated scandals than as illustrations of a broader investigative reality: in Saudi matters, bribery or abuse-of-authority concerns often sit alongside unexplained funds flows, procurement distortion and wider control failures.

Beneficial ownership also matters in Saudi Arabia. The 2025 UBO framework moved ownership transparency beyond a one-off registry exercise by combining a 25% ownership threshold with a control-rights test, a senior-management fallback, change-notification requirements and penalties of up to SAR 500,000 for non-compliance. In practical terms, that makes ownership mapping more useful not only for registry compliance, but for identifying conflicts, concealed links and potential misuse of corporate vehicles in procurement or related-party arrangements.[15]

Another important Saudi theme is governance. SAMA's counter-fraud framework had already raised expectations around prevention, monitoring and senior ownership of fraud risk, but the April 2025 Counter-Fraud Fundamental Requirements gave that trend more operational force by extending the framework beyond banks to finance companies and payment service providers, requiring board-approved remediation roadmaps and setting a full-compliance date of 13 April 2026. That matters because an investigation into suspected corruption may now also become a test of whether the institution's counter-fraud, escalation and control environment was fit for purpose. In Saudi matters, asset mapping, ownership analysis and control testing should therefore not be treated as downstream tasks. They are part of the narrative from the outset.[16]

The lesson for investigators is straightforward. In Saudi matters, asset mapping and ownership analysis should not be treated as downstream tasks waiting for the factual narrative to be complete. They are part of the narrative. In a large-project environment, they may be the fastest route to understanding whether a concern is isolated misconduct, concealed influence or part of a broader control failure.

Qatar

Qatar offers a different but complementary picture. It reminds us that convergence is not expressed only through highly public enforcement actions. It can also appear through governance strategy, implementation depth and stronger coordination across integrity-related functions.[17]

Qatar's recent trajectory suggests increasing emphasis on institutional maturity rather than constant legislative expansion. The launch of a national integrity strategy provides a clear example of how governance, transparency and corruption prevention are being framed together rather than as isolated policy topics. That does not by itself prove enforcement intensity. But it signals that integrity expectations are being positioned more systemically, with consequences for how public- and private-sector actors are expected to organise controls and respond to risk.[18]

A useful Qatar-specific example is that the 2025–2030 National Strategy to Promote Integrity, Transparency and Corruption Prevention is not framed as a general statement of intent, but as a five-year programme built around 32 strategic objectives, 78 national projects, 16 implementing entities and 35 supporting entities. That degree of implementation planning suggests increasing institutional depth, including for the private sector, legislation and law-enforcement coordination.[19]

For investigations teams, Qatar underlines two points. First, the absence of dramatic publicity should not be mistaken for absence of change. Second, governance and reporting expectations may become as important as the underlying misconduct analysis, especially where state-linked entities, procurement or regulated firms are involved. In that sense, Qatar reflects the same wider regional movement: integrity concerns are becoming more

embedded, and therefore more likely to affect the design and defensibility of internal investigations.

The Wider GCC

Bahrain, Kuwait and Oman each follow their own path, and the practical differences between them still matter. Supervisory maturity, public visibility of enforcement and the pace of institutional change are not identical. That said, the broad direction is similar: greater emphasis on effectiveness, closer attention to beneficial ownership and transparency, and a stronger expectation that AML supervision should produce tangible outcomes rather than remain a paper exercise.

Kuwait is worth watching: it was added to FATF's list of countries under increased monitoring in February 2026 (currently the only GCC country on the "grey list"). At the same time, it has stepped up its beneficial ownership framework, including stricter "actual beneficiary" disclosure requirements. Kuwait's Nazaha also reported 49,564 financial disclosure statements from 21,072 declarants and 1,035 referrals to the Public Prosecution in 2025, while its 2024/2025 reporting also points to a more data-led integrity model, including electronic verification links with 13 government entities.[20]

Bahrain is combining a mature anti-money laundering and counter-terrorist financing (AML/CFT) framework (it launched its National Strategy to Combat Money Laundering, Terrorism Financing and Weapons Proliferation (2025–2027) in September 2025) with stronger beneficial ownership infrastructure, including the Sijilat UBO portal.[21]

Oman likewise reflects the broader trend: public-sector integrity controls remain prominent through the State Financial and Administrative Audit Authority's financial disclosure regime, alongside the authorities' 2023–2025 enhanced AML/CFT national strategy.[22]

The point for readers is not that all GCC states are converging at the same speed. It is that the old assumption of neatly separated anti-corruption, AML and governance risks is becoming less reliable across the region. For businesses operating in several GCC markets at once, that is already a practical reality.

WHAT THIS MEANS FOR INVESTIGATIONS

Broader Triage From Day One

The most immediate consequence of convergence is that intake and triage need to be broader. A case that first appears to be a procurement issue, bribery allegation, sanctions touchpoint or accounting concern may need to be assessed simultaneously under several lenses from the outset. That does not mean every matter becomes a massive multi-jurisdictional exercise. It means the initial questions have changed.

Those questions now often include whether:

- any regulated entity has reporting obligations;
- beneficial ownership information has been verified;
- counterparties or intermediaries raise sanctions concerns;
- value has already moved into recoverable assets; and
- the institution's own governance response could later become part of the exposure.

A useful way to frame triage is to ask not only "what happened?", but also "what additional exposure might this fact pattern generate if it is true?".

A common GCC fact pattern begins with a procurement complaint or whistleblower allegation but quickly widens: the intermediary turns out to have opaque ownership; a relative or nominee sits behind the supplier; payments have already moved into property or other assets; and one or more regulated entities may face reporting or sanctions-screening questions. In those circumstances, triage cannot stop at whether bribery occurred; it must also test ownership, proceeds movement, regulatory exposure and the adequacy of the institution's own response.

Beneficial Ownership As An Investigative Workstream

Beneficial ownership analysis has become one of the most useful early tools in GCC investigations. It can reveal whether a vendor relationship was genuinely arm's length, whether a politically exposed person or relative stands behind a structure, whether undeclared related parties existed or whether payment chains were routed through nominee or opaque entities for concealment purposes.[23]

This workstream should not be reduced to checking a registry extract. In more complex matters, it requires reconciliation of corporate records, onboarding files, transaction evidence, public data, communications and witness accounts. Registry information may identify a declared owner. It may say much less about actual control, influence, family linkage or why a given structure was selected. The most useful investigations therefore treat beneficial ownership as a means to test the factual narrative, not merely document it.

This is also an area where sector and jurisdiction matter. Ownership evidence in a free zone structure, a family office vehicle, a local intermediary or an offshore company will not look the same. That is another reason not to impose a single investigative template on every GCC matter.

A useful public example is the January 2024 arrest of the Royal Commission for AlUla's chief executive, in a case publicly described by Nazaha as involving abuse of authority and money laundering linked to contract awards and concealed ownership interests. Public reporting said that he had represented that he no longer had a relationship with a company that later obtained contracts, but investigators concluded that his exit was only informal in nature, that he remained among the owners and that profits continued to be channelled to him through a relative. That is exactly the kind of matter in which beneficial ownership analysis becomes an investigative workstream rather than a registry check: the key issue was not only who was declared on paper, but who still exercised influence, received value and sat behind the commercial relationship in practice.[24]

Earlier Asset Tracing And Preservation

Asset questions also need to move forward in the sequencing of an investigation. If authorities and regulators are increasingly focused on proceeds, confiscation and control effectiveness, then investigators cannot wait until the end of a case to begin thinking about where value went and what might still be recoverable.[25]

In practical terms, that means examining earlier bank records, payment routing, property acquisitions, commodities exposure, shareholdings, luxury assets and transfers to connected parties. It also means thinking more clearly about the standard and quality of

evidence that might later support freezing, restraint or confiscation applications, whether domestically or through cross-border cooperation.

There is a strategic balance to be struck here. Internal teams may want time to test facts carefully before taking steps that could escalate a matter. But delay can also make recovery harder, especially where assets are mobile or structures are layered. The more effective approach is therefore not to jump immediately to restraint in every case, but to build an early asset hypothesis and test it in parallel with the misconduct narrative.

A practical example is an asset-tracing matter in which early property inquiries showed that a subject had already disposed of 22 Dubai residential units originally acquired for about 126.4 million dirhams, with estimated aggregate proceeds likely exceeding 200 million dirhams, while still retaining a further portfolio of 38 apartments acquired for about 78.2 million dirhams. More detailed tracing then identified a Palm Jumeirah property that appeared to have been bought repeatedly over several years at the same price before being sold to a UAE entity for which little public corporate information was available. In a case like that, waiting until the end of the investigation to ask where value went would be a strategic mistake: the central issues quickly become which assets remain reachable, whether repeated transfers reflect layering or value manipulation and which counterparties, bank accounts and connected entities need to be mapped before recovery options narrow.[26]

Parallel Sanctions, AML And Corruption Analysis

Sanctions and proliferation-related issues are another area where purely sequential analysis has become less defensible. In trade-linked, logistics-heavy or intermediary-driven matters, investigators may increasingly need to consider whether a procurement or corruption fact pattern also raises sanctions-screening, export-control or proliferation-financing concerns.-[27]

This does not mean every GCC corruption case is also a sanctions case. It does mean that in the current environment, a matter involving intermediaries, shipping documents, dual-use goods, third-country payment routes or concealed beneficial ownership should be tested for that possibility earlier. FATF typology work has reinforced how often sanctions evasion and proliferation schemes rely on the same tools seen in corruption-enabled payment structures: shell companies, hidden ownership, falsified documentation and layered transfers.[28]

A useful example is a MENA sanctions-evasion case study in which goods were sourced through Dubai for an Iran-based end user, with the sales routed through another Dubai company to conceal the final destination. In practice, that kind of arrangement forces investigators to test several questions at once whether:

- the distributor is genuine;
- shipping and customs documents accurately describe the transaction;
- the end-user is being concealed; and
- payment routing or ownership structures point to wider AML or corruption risk.[29]

Designing Investigations For Regulatory Visibility

A final implication is procedural. Internal investigations in the GCC increasingly need to be designed on the assumption that they may later be scrutinised by a regulator, supervisor, prosecutor or state stakeholder. That affects how matters are scoped, documented and governed.[30]

In practice, that means maintaining a defensible record of key decisions, keeping a clear audit trail for scoping choices, documenting why certain issues were prioritised or deprioritised, and thinking carefully about interim risk-mitigation steps. It also means ensuring that board, audit-committee or senior-management reporting is properly calibrated. In some matters, the governance response to red flags may become almost as significant as the underlying facts.

This is one reason GIR's audience should care about convergence. It is not simply changing liability theories. It is changing what a credible investigation now looks like. An investigation that ignores ownership, asset location, sanctions touchpoints or reporting consequences until late in the process may not only miss evidence. It may also appear incomplete if later reviewed through a financial-integrity lens.

A TYPICAL MODERN GCC FACT PATTERN

A composite scenario helps illustrate the shift. A state-linked entity awards a subcontract on a major project to a local intermediary said to provide market-entry support. The fees are high, and a whistleblower later alleges that the intermediary is linked to a public official. What begins as a conventional bribery and procurement review soon widens. Interviews suggest the intermediary did little real work; ownership analysis reveals nominee structures and inconsistencies between declared shareholders and actual control; due diligence files show onboarding gaps; and bank records indicate that part of the fees moved rapidly through multiple entities before being used to acquire property and commodities exposure elsewhere.

At that point, the matter is no longer just a bribery case. It also raises books-and-records issues, beneficial ownership and onboarding failures, suspicious transaction reporting questions, possible sanctions or trade-related risk, and the need to consider asset preservation early. The scenario is composite, but it reflects a wider GCC reality: high-value transactions, layered intermediaries, better ownership visibility and stronger supervision mean related integrity issues now surface faster and must be investigated in parallel.

WHAT TO WATCH IN 2026

The most important theme to watch in 2026 is not whether every GCC jurisdiction adopts a dramatic new statute. It is whether authorities continue to favour visible implementation over quiet framework maintenance. Readers should expect continued emphasis on effectiveness: supervision that can be demonstrated publicly, better use of financial intelligence, pressure on higher-risk sectors and continued attention to the traceability of ownership and funds flows.[31]

A second theme is the continued importance of non-financial gatekeepers. Real estate actors, precious metals dealers, corporate-service providers and other DNFBPs are likely to remain central to the region's financial-integrity story because they often sit at the junction between the primary misconduct and the eventual movement or parking of value. For investigators, that means sector knowledge will matter more, not less.

A third theme is governance. Boards, audit committees and senior management are likely to face sharper scrutiny around escalation, control failures and response quality. The issue will not only be whether misconduct occurred. It will also be whether the warning signs were visible, whether ownership and counterparty risks were understood, and whether the institution acted quickly enough once concerns emerged.

Finally, divergence within convergence will remain. The GCC is moving in a broadly similar direction, but not at a uniform speed or with identical tools. Investigators should resist both extremes: assuming complete uniformity across the region, or assuming the differences are so great that no common trend can be identified. The better view is that the common direction is now clear, while local procedure, visibility and sector focus still need to be mapped carefully in each case.

In 2026, real estate and virtual assets may come further into focus in the United Arab Emirates, particularly if follow-up scrutiny places more weight on effectiveness in sectors associated with ownership opacity, asset parking and cross-border funds flows. That would also reflect a wider GCC pattern, as authorities across the region continue to tighten beneficial ownership, DNFBPs and virtual-asset controls. Recent regional conflict may add another layer of pressure by sharpening attention on sanctions-evasion and related typologies, even if the practical response still varies by jurisdiction.

CONCLUSION

The most significant recent development in the GCC is not simply more regulation. It is the narrowing of the distance between anti-corruption, AML, beneficial ownership, sanctions and governance as practical investigative categories. That does not eliminate legal differences between those regimes. It does mean that, in real matters, they increasingly appear together.

For GIR readers, the value of this regional shift is practical rather than theoretical. A bribery or procurement matter in the GCC now needs to be assessed earlier for ownership opacity, reporting obligations, sanctions touchpoints, supervisory consequences and asset-preservation options. The strongest investigations will therefore be those designed from the outset to handle parallel exposure, rather than those that discover it too late.

In the GCC's current enforcement environment, a narrow investigation may still be possible. It is simply becoming harder to defend.

Endnotes

1 Financial Action Task Force (FATF), ***Complex Proliferation Financing and Sanctions Evasion Schemes***, FATF Report, June 2025, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf. ^ Back to section

2 ibid. ^ Back to section

3 See MENAFATF, Evaluation Reports – 2nd round; FATF, Assessments – Global Assessments Calendar, https://www.fatf-gafi.org/en/calendars/assessments.html. ^ Back to section

4 Federal Decree-Law No. (10) of 2025 (UAE), https://uaelegislation.gov.ae/en/legislations/3314/download. ^ Back to section

5 Financial Action Task Force (FATF), ***The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation***, Recommendation 24, "Transparency and beneficial ownership of legal persons," p. 22. ^ Back to section

6 UAE Financial Intelligence Unit, ***Misuse of Precious Metals and Stones in Financial Crime*** (1 September 2025). It is UAE-specific, focused on the precious metals and stones sector, and uses fresh data from July 2021 to June 2025. The UAEFIU says the sector's foreign trade rose from 497 billion dirhams in 2021 to over 959 billion dirhams in 2024, with an 81% increase in registered dealers, and that the report draws on over 1.4 million dealer reports as well as hundreds of STRs/SARs; see also Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing; and, FATF and APG, ***Money Laundering and Terrorist Financing Risks and Vulnerabilities Associated with Gold*** (20 July 2015). ^ Back to section

7 Ministry of Economy and Tourism, "Ministry of Economy and Tourism announces H1 2025 inspection results on private sector compliance with anti-money laundering laws", 24 July 2025. ^ Back to section

8 Central Bank of the UAE, "CBUAE imposes financial sanctions of 18.1 million on two branches of foreign banks operating in the UAE", 28 May 2025; Central Bank of the UAE, "CBUAE imposes a financial sanction of 5.9 million on a branch of foreign bank operating in the UAE", 2 July 2025. ^ Back to section

9 Central Bank of the UAE, "CBUAE Imposes a financial sanction of 200 million on an Exchange House", 20 May 2025; Central Bank of the UAE, "CBUAE Imposes a financial sanction of 100 million on an Exchange House", 29 May 2025. ^ Back to section

10 Central Bank of the UAE, "CBUAE Revokes the Licence of 'Sundus Exchange' and Imposes a Financial Sanction of 10 Million", 17 June 2025; Central Bank of the UAE, "CBUAE Revokes the Licence of 'Omda Exchange' and imposes a financial sanction of 10 million", 23 December 2025. Note that the Omda notice refers to failures and violations of the Central Bank Law and related regulations, rather than expressly to AML/CFT-framework failures. ^ Back to section

11 Central Bank of the UAE, "CBUAE Imposes a financial sanction of 200 million on an Exchange House", 20 May 2025. ^ Back to section

12 Ministry of Economy and Tourism, Circular No. MOET/AML/007/2025, "Regarding the Re-Imposition of United Nations Sanctions Related to Iran", 19 December 2025. The circular requires supervised DNFBPs to update screening systems, re-screen customers, beneficial owners and counterparties, apply freezing measures without delay, and report confirmed and partial matches to the Executive Office through goAML; it also states that it reaffirms, rather than creates, obligations under Cabinet Resolution No. 74 of 2020. ^ Back to section

13 Nazaha 2025 monthly activity updates published on Nazaha's official website and X account, https://www.nazaha.gov.sa/, last accessed on 21 February 2026. ^ Back to section

14 Oversight and Anti-Corruption Authority (Nazaha), "The Oversight and Anti-Corruption Authority initiated several criminal cases", 22 October 2025; Nazaha, "The Oversight and Anti-Corruption Authority initiated several criminal cases", 30 June, see https://www.nazaha.gov.sa. ^ Back to section

15 Ministry of Commerce Clarifies the Key Benefits of the Ultimate Beneficial Owner (UBO) Rules, https://mc.gov.sa/en/mediacenter/News/Pages/09-12-25-01.aspx. ^ Back to section

16 Saudi Central Bank (SAMA), Circular No. 106897184, "Circular Re. Counter-Fraud Fundamental Requirements," 14 April 2025. ^ Back to section

17 Qatar National Strategy to Promote Integrity, Transparency and Corruption Prevention (2025-2030), https://qna.org.qa/en/news/news-details?id=acta-inaugurates-national-strategy-to-promote-integrity-transparency-prevent-corruption-2025-2030&date=8/10/2025; FATF Mutual Evaluation Report of Qatar, https://www.fatf-gafi.org/en/publications/Mutualevaluations/MER-Qatar-20230.html. ^ Back to section

18 Qatar News Agency, "ACTA Inaugurates National Strategy to Promote Integrity, Transparency, Prevent Corruption 2025–2030", Doha, 8 October 2025; FATF Mutual Evaluation Report of Qatar, https://www.fatf-gafi.org/en/publications/Mutualevaluations/MER-Qatar-20230.html. ^ Back to section

19 Qatar News Agency, "Qatar Presents National Strategy to Promote Integrity, Transparency and Corruption Prevention at COSP11", Doha, 17 December 2025. ^ Back to section

20 https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-mon...; https://kuwaittimes.com/article/38147/kuwait/other-news/nazaha-censured-1035-in-2025/; https://www.nazaha.gov.kw/nazaha/wp-content/uploads/2025/08/2024-2025.pdf. ^ Back to section

21 Kingdom of Bahrain, *The Kingdom of Bahrain's National Risk Assessment 2025*, Public Version. ^ Back to section

22 https://www.fatf-gafi.org/en/publications/Mutualevaluations/MER-Oman-2024.html; https://www.imf.org/-/media/files/publications/cr/2025/english/1omnea2025003-print-pdf.pdf. ^ Back to section

23 See Saudi and UAE beneficial ownership disclosure materials, https://rulebook.centralbank.ae /en/rulebook/31-identification-beneficial-owners, https://mc.gov.sa/en/mediacenter/News/Pages/09-12-25-01.aspx; FATF, Guidance on Beneficial Ownership for Legal Persons, https://www.fatf-gafi.org/en/publications /Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html. Back to section

24 Oversight and Anti-Corruption Authority (Nazaha), as reported in ***Al Arabiya English***, "Saudi Arabia arrests CEO of Royal Commission for AlUla for money laundering", 29 January 2024; ***The National***, "AlUla chief executive arrested over corruption allegations", 29 January 2024; ***The National***, "Saudi Arabia's AlUla commission appoints interim boss after chief executive's arrest", 30 January 2024. Back to section

25 FATF, Best Practices on Confiscation Recommendations 4 and 38 and a Framework for Ongoing Work on Asset Recovery, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Bestpracticesonconfiscationrecommendations4and38andaframeworkforongoingworkonassetrecovery.html. Back to section

26 Based on an anonymised asset-tracing investigation involving UAE real estate holdings, repeated property transfers and opaque counterparties. Back to section

27 FATF, Complex Proliferation Financing and Sanctions Evasion Schemes, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf. Back to section

28 ibid. Back to section

29 Global Coalition to Fight Financial Crime MENA Chapter, ***Trade-Based Financial Crime – Middle East and North Africa: A Reference Guide for the Anti-Financial Crime Community***, pp 65–66 (case study on sanctions evasion through destination concealment involving Dubai-based intermediary companies); see also pp 22–23 and 65 on transshipment risk and sanctions exposure associated with routing goods through Iran. Back to section

30 See CBUAE enforcement announcements; SAMA counter-fraud materials; Bahrain financial crime rulebook materials. Back to section

31 See MENAFATF, final statement of the 41st Plenary Meeting (Manama, 13 November 2025), https://www.menafatf.org/information-center/final-statement-41st-plenary-meeting-middle-east-and-north-africa-financial; FATF statements on jurisdictions under increased monitoring (24 October 2025 and 13 February 2026), https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-february-2026.html. Back to section

Secretariat

Ralph Stobwasser rstobwasser@secretariat-intl.com
Tarek Bleik tbleik@secretariat-intl.com

https://secretariat-intl.com/

Germany: headquarter oversight crucial to ensure effective sanctions compliance

Adrian Mom, **Svea Ottenstein** and **Veronica Furtuna**
AlixPartners

Summary

IN SUMMARY

International sanctions regimes and associated restrictive measures, particularly those related to Russia, Venezuela, Iran, China and North Korea, are becoming more complex, requiring companies to implement robust compliance programmes. Effective oversight from headquarters is crucial, especially for decentralised organisations. Additionally, Germany is strengthening sanctions enforcement through the Sanctions Enforcement Acts as part of its strategy to combat financial crime. This sends a clear message to German companies that strong sanctions compliance must be integrated into their financial crime programmes. This article outlines best practices for leading German banks and corporates to strengthen anti-financial crime programmes, focusing on sanctions risk management and oversight at both headquarters and subsidiary levels in an environment shaped by restrictive measures, asset freeze requirements, secondary sanctions risks and expectations around sanctions screening and group-wide oversight.

DISCUSSION POINTS

- Sanctions enforcement trends and regulatory expectations
- Impact of AMLA on sanctions compliance
- Headquarters oversight and group-wide sanctions compliance governance
- Conducting robust sanctions risk assessments
- Developing clear sanctions compliance policies and procedures
- Strengthening sanctions training for employees and relevant stakeholders
- Enhancing screening processes and internal audit functions
- Addressing decentralised compliance structures challenges across subsidiaries
- Examples of best practices for sanctions risk management

REFERENCED IN THIS ARTICLE

- Sanctions Enforcement Acts I and II (Germany)
- EU Council Regulation No. 269/2014
- Directive (EU) 2024/1226
- Regulation (EU) 2024/1624
- Foreign Trade and Payment Act (Außenwirtschaftgesetz – AWG)
- Sanctions and Anti-Money Laundering Act 2018 (United Kingdom)
- Federal Act on the Implementation of International Sanctions (Switzerland)

INTRODUCTION

Leading German banks and multinational companies are increasingly operating in a complex global landscape, where sanctions regimes have become more multifaceted and demanding. The 19 sanctions packages introduced by the Council of the European Union

between February 2022 and 23 October 2025 (the latest package adopted) exemplify the increasing pressure for compliance functions to demonstrate agility and adaptability in response to the complexities of sanctions regimes. Developments in other regions have further escalated the volume and complexity of sanctions to unprecedented levels. Organisations are facing, among other things, significant spikes in alerts generated by screening operations, continuously evolving sanctions circumvention patterns requiring definition of new alerting rules and the need to continuously reassess sanctions risk exposure.

Companies are now not only challenged to navigate these intricate requirements but also face mounting enforcement actions from authorities. In this context, having an effective sanctions compliance programme (SCP) is more critical than ever – particularly for organisations with complex subsidiary networks and international operations or exposure. Effective oversight and accountability from headquarters (HQ) for comprehensive sanctions risk are now paramount to ensuring compliance and mitigating potential risks.

GERMAN COMPANIES HAVE SIGNIFICANT INTERNATIONAL EXPOSURE

The top 10 DAX companies with HQ in Germany account for approximately €1.1 trillion in market capitalisation, or about 58% of the total market capitalisation of the index.[1] Their economic, social and brand awareness footprints extend beyond German borders, carrying considerable economic potential but also exposing them to various risks due to their operations across different geographies.

These top 10 DAX companies have around 2,300 subsidiaries worldwide.[2] Western Europe-[3] hosts 40% of these subsidiaries, which are subject to arguably similar risks, including sanctions risks, regulatory challenges and compliance structures aligned with their German HQ.

Cascading the principles described in the organisation's centralised SCP is not without challenges. However, it is typically facilitated by a common understanding of sanctions risks and the consequences of non-compliance.

The remaining 60% of subsidiaries are located and operate in jurisdictions with differing or contradictory regulatory environments and applicability of sanctions regimes compared to the German HQ.

To uphold good corporate governance and accountability, the HQ compliance function is tasked with designing and rolling out an SCP that effectively mitigates sanctions risks across the organisation and sets the tone for the importance of effective implementation across all geographies. An effective SCP is therefore a component of a holistic anti-financial crime compliance programme serving as a safeguarding mechanism to protect the organisation from financial and reputational losses.

An informal or entirely missing SCP can expose the HQ to considerable regulatory and reputational risk in both home and foreign markets.

An entirely different dimension of sanctions risk exposure is added when SCP implementation lags across subsidiaries. Therefore, oversight at the subsidiary level should be a priority for the HQ compliance function of German companies in their goal to effectively mitigate sanctions risks globally.

GERMANY'S SANCTIONS LANDSCAPE

As a European Union member state, Germany adheres to common sanctions regulations and directives enforced by the European Union. The EU sanctions jurisdiction applies, among other things, to EU entities such as companies and organisations incorporated or constituted under the laws of an EU member state. This creates a fundamental need for EU companies, including German-based multinationals, to exercise thorough oversight of their subsidiary networks.

EU sanctions include measures related to individuals and entities, sectoral sanctions and export controls. Sanctions targeting individuals typically involve asset freezes and travel bans. As of February 2025, EU Council Regulation No. 269/2014,[4] enacted in 2014 following the Russian annexation of Crimea, has sanctioned approximately 1,900 individuals and 700 entities. Regulation No. 269/2014 continues to enforce restrictions and bans introduced through the 19 Russia-related sanctions packages.[5] Sectoral sanctions manifest as restrictions against particular sectors such as energy, defence, aerospace, financial sectors and dual-use goods. Export controls represent prohibitions on selected goods and technologies to prevent military use by sanctioned countries.

In response to growing challenges in ensuring compliance with EU sanctions across industries, the EU launched the EU Sanctions Helpdesk for EU Operators in March 2025. The Helpdesk provides tailored support for sanctions due diligence, primarily targeting small and medium-sized enterprises with balance sheets of up to EUR 43 million, while also assisting larger entities on a case-by-case basis.[6] Alongside these supportive measures, the EU simultaneously strengthened the enforcement framework for sanctions compliance.

In April 2024, the European Council implemented the Directive EU 2024/1226,[7] establishing EU-wide minimum rules for the prosecution of violations or circumvention of EU sanctions within member states. Member states were given 12 months to incorporate these provisions into national legislation.[8] Transposing the requirement into national law has been challenging, since on July 2025, the European Commission opened infringement procedures by sending a letter of formal notice to 18 Member states, including Germany, for failing to notify measures fully transposing the Directive and urging for full implementation and notification within two months.[9]

Further regulatory requirements come into effect across EU member states addressing fragmented national implementation of money laundering and terrorist financing prevention measures prescribed by the EU AML Directives.[10] On 10 July 2027, the EU AML Regulation 2024/1624, as part of the EU AML Regulatory Package, becomes effective. This Regulation becomes directly applicable in all EU member states and aims at achieving a uniform application across the community, among others, on the responsibility of an obliged entity to implement targeted financial sanctions. Thereby, sanctions compliance is positioned as an integral element of anti-money laundering and broader financial crime prevention.

Furthermore, the Regulation stipulates extensive group-wide requirements, where parent undertakings are obliged to establish group-wide strategies, procedures and controls and to carry out group-wide risk assessments even if the subsidiaries are not located in a member state, among other requirements.[11] EU AML Directives introduced the concept of group-wide accountability, yet these extended requirements become directly applicable across all member states once Regulation 2024/1624 comes into effect. On a national level, Germany continues to take concrete steps to enforce sanctions via the German Sanctions Enforcement Acts I and II (SDG I and II).

SDG I took effect in May 2022 and provided the legal basis for investigating and freezing assets. The German cabinet adopted the draft SDG II in October 2022, which was followed by adoption in the German Bundestag in December 2022. The bill, prepared jointly by the Federal Ministry of Finance and the Federal Ministry of Economic Affairs and Climate Action, allowed for structural improvements in the operational enforcement of sanctions and anti-money laundering measures. SDG II marks a strategic shift toward the "follow the money" principle and reinforces Germany's efforts to combat money laundering.[12] As such, sanctions enforcement and anti-money laundering measures are seen as critical pillars for effectively fighting financial crime.

Further Regulatory Implications

One aspect of implementing the follow the money strategy was the creation of the Federal Financial Crime Agency (FFCA) in 2024. The FFCA was expected to begin operations in 2025 and aimed to consolidate key competencies from the Money Laundering Investigative Centre, the Financial Intelligence Unit and the Central Office for Sanctions Enforcement, among others, to address the fragmentation of existing structures.[13] The agency's operational launch has stalled in 2025 while the European Union's Anti-Money Laundering Authority (AMLA) officially started operations on 1 July 2025.

On 1 January 2026, AMLA took over all EU-level anti-money laundering and counter-terrorist financing mandates from the European Banking Authority, marking a key operational milestone.[14] On 4 February 2026, AMLA announced its strategic priorities for 2026–2028, one of which being progressively assuming direct supervisory responsibility over selected high-risk, cross-border financial institutions.[15] It is worthwhile noting that AMLA is to supervise the implementation of targeted financial sanctions on top of its anti-money laundering and anti-terrorist financing duties. On 15 January 2026, the German Bundestag adopted the transportation of the Directive EU 2024/1226 into national law by amending the Foreign Trade and Payments Act, which extends and is applicable for non-financial institutions as well. As a result, key provisions are significantly tightened, and the criminal and administrative fine risks for companies and their management levels have noticeably increased.

Given Germany's substantial global subsidiary presence, EU wide and national regulatory developments, considerable measures must be implemented by the private sector to ensure anti-financial crime compliance on group-wide level.

As a result, effective financial crime programmes, including compliant sanctions and anti-money laundering practices, are essential for German multinationals with extensive subsidiary networks. Addressing existing gaps is of urgent importance at HQ level, communicated through a strong tone from the top that doing the right thing is a core organisational mission.

OVERVIEW OF OTHER KEY SANCTIONS REGIMES ACROSS EUROPE

EU member states generally adhere to common sanctions regulations and directives enforced by the European Union as outlined in the section on Germany's sanctions landscape. Additional local regulations may also apply.

Switzerland, not an EU member state, makes independent decisions on sanctions based on the Federal Act on the Implementation of International Sanctions.[16] In practice, Switzerland typically adopts EU sanctions, but sometimes with delays or modifications. The State

Secretariat for Economic Affairs is responsible for implementing and overseeing the sanctions and ensuring compliance by businesses and financial institutions.

The United Kingdom has its own framework for enforcing sanctions under the Sanctions and Anti-Money Laundering Act of 2018 (the SAMLA Act),[17] which includes prohibiting measures such as travel bans, asset freezes and export controls against countries such as Russia, Iran and Myanmar. The enforcement framework strengthening trend is observed in the United Kingdom as well, where on 29 January 2026 the Office of Financial Sanctions Implementation (OFSI) announced five key reforms to its civil enforcement framework.[18] For example, OFSI intends to double its statutory maximum penalties to the higher of £2 million and 100% of the value of the breach.

Other countries in Europe, including those in Central and Eastern Europe, that are not part of the European Union nor members of the European Economic Area, may have their own sanctions regulations, which may align with EU regulations or diverge from them.

CONSIDERATION FOR NON-EUROPEAN SANCTIONS REGIMES

This article primarily focuses on Germany while briefly providing an overview of other key sanctions regimes in Europe. However, Sanctions are a global concept that German companies must navigate, requiring awareness of and compliance with applicable regimes worldwide. Three-quarters of the top 10 DAX subsidiaries are located in regions with complex sanctions regimes, including Western Europe, North America and the Asia-Pacific.[19]Notably, China exemplifies this complexity by enforcing countersanctions against organisations and individuals it perceives as interfering with its interests, including those enforcing sanctions from Western Europe and North America.

The remaining one-fourth[20] of subsidiaries operate in regions that present significant social, political and economic challenges as well. A thorough understanding of each geography's specific sanctions landscape and enforcement trends is good practice for a HQ to follow when developing effective SCPs.

BEST PRACTICES FOR AN EFFECTIVE SCP

The following sections offer best practices for HQ to consider when developing, enhancing or testing centralised SCPs and for overseeing their operational implementation at subsidiaries subject to various complex and challenging sanctions regimes.

Organisations and HQs overseeing less complex subsidiary networks can equally benefit from applying the described best practices in an effort to strengthen their SCPs and mitigate sanctions risks.

Effective SCP oversight starts with a significant commitment to the core pillars of an SCP, which include but are not limited to:

- senior management commitment and governance;
- sanctions risk assessments;
- sanctions policies and procedures;
- training and sanctions knowledge capabilities enhancement;
- sanctions screening technology; and
- controls and internal audit.[21]

Senior Management Commitment And Governance

Formalising the SCP and assigning senior management the role of overseeing its adequacy, implementation, revision and effectiveness can help organisations mitigate sanctions, regulatory and reputational risks.

Senior management's significant commitment to the SCP can be demonstrated in several ways, such as:

- Enabling the sanctions compliance function: empowering the sanctions compliance function with sufficient authority and independence to develop and implement its policies and procedures aimed at mitigating the risks identified through the sanctions risk assessments.
- Establishing transparent reporting lines:creating transparentand documented reporting lines and a schedule of regular interactions with the sanctions compliance function to provide evidence of continuous monitoring of processes.
- Allocating resources proportionate to risk:allocating human and technological resources proportionate to the organisation's size and risk profile, reflecting senior management's awareness of the complexity of screening operations, regulatory environment and sanctions risk profile for its product portfolio.
- Reviewing and approving the SCP:ensuring senior management reviews and approves the SCP, particularly when the revision and approval occur at a determined frequency rather than as a one-off static event that is tardy to changes in regulatory and sanctions risk developments.
- Promoting a zero-tolerance policy for non-compliance:fostering aculture based on values embedded within the organisation, with senior management serving as role models. The tone at the top and the repercussions of sanctions non-compliance for the organisation are thoroughly investigated and clearly communicated by senior management.

Senior management's significant commitment to SCP exercised at HQ is a challenging mission in itself. This commitment gains an additional layer of complexity in the context of a network of subsidiaries subject to contradictory sanctions regimes and geographical, political and supply-chain risks. A series of measures can be applied to align local senior management commitments with the efforts undertaken at HQ:

- Fostering a parent–subsidiary relationship:ensuring SCP principles are continuously transmitted locally in line with the organisation's compliance culture. Enable local senior management to act independently, formalise local specifics to the SCP, coordinate differentiating elements with the HQs where applicable and establish a formal reporting cycle between the subsidiary and the HQ senior management for a comprehensive update on relevant developments, escalations and sanctions screening performance, as it applies.
- Assisting with local sanctions risk assessments: helping develop local sanction risk assessment and sanctions-related policies and procedures to diminish the risk of inadequate, inconsistent or incomplete approaches to assessing and mitigating sanctions risk. Additionally, assistance efforts from HQs targeting the design of sanctions-related policies and procedures can result in more thorough sanctions

compliance assessments conducted by HQs due to enhanced knowledge of local specifics.

- Conducting regular risk-based assessments:performing regular internal and external risk-based assessments at subsidiaries to test compliance with HQ policy and identify shortcomings in sanctions compliance. This can improve both local design and operational effectiveness, as well as signal potential shortcomings in oversight to HQ.

Sanctions Risk Assessments

A core component of an effective SCP is the sanctions risk assessment. Regulatory guidelines and compliance frameworks define "risk assessment" as an evaluation of inherent risks, including those related to product lines, customer base, supply chain, processes, systems and business geographies. The goal is to develop risk-based measures within the SCP to mitigate sanctions risks and monitor residual exposure.

The European Commission's recommendation on internal compliance programmes targeting dual-use trade control mentions that even though the risk assessment might not identify all weak spots and vulnerabilities, it provides organisations with a better base to develop and review their SCPs.[22]

The following non-exhaustive steps can be applied by an organisation in conducting risk assessments that reflect sanctions risks:

- Performing a holistic "top-to-bottom" review of an organisation's:
    - customers, supply chain, intermediaries and counterparties;
    - products and services, including how and where such items fit into other financial or commercial products, services, networks or systems; and
    - geographic locations of the organisation.[23]
- Conducting the risk assessment by:
    - mapping each of the reviewed areas with the associated risks, including whether the reviewed areas have sanctions risk exposure; and
    - allocating a severity and likelihood for the risk's occurrence.
- Developing mitigation strategies proportionate to the severity and likelihood outcome for each reviewed area. These strategies need to be reflected in the organisation's SCP.
- Formalising the risk assessment approach:formalise the approachto conduct the risk assessment as highlighted by regulators (eg, the FCA Handbook), which is a sign of a mature compliance organisation. The sanctions risk assessment can be formalised by integrating it with the organisation's risk assessment or separately. Regardless of the approach, formalising the risk assessment encourages proactive risk management, risk-oriented decision-making and increased consideration for regulatory requirements, reducing legal issues.
- Defining a routine review and update frequency: define a routine review and update frequencyfor the risk assessment that also covers sanctions risk. This demonstrates the organisation's adaptability and recognition of an evolving risk environment. The organisation is therefore aware of the need to review the suitability of its

risk-mitigating approach, including its exposure to sanctions risks. Ensure clear accountability for conducting the risk assessment on schedule and for integrating any updated mitigation measures into the organisation's SCP.

- Develop and conduct advanced sanctions risk assessments: incorporate stress testing mechanisms at HQ and at subsidiary level to evaluate the impact on potential sectoral sanctions implementation or sudden sanctions escalations revealing controls that might fail or entirely missing ones.

An up-to-date risk assessment that considers sanctions risks and has mitigation approaches implemented in HQ SCPs can serve as a blueprint for compliance functions in subsidiaries to conduct a local risk assessment. Conducting such an exercise locally needs to be a priority overseen by local senior management. HQs can support this process to achieve holistic risk management across the organisation:

- Providing technical assistance: offer technical assistance during the risk assessment process, with members of centralised compliance functions participating and guiding local teams.
- Elaborating dedicated training sessions:develop dedicated training sessionsfor relevant personnel locally to implement qualitative and quantitative techniques for an adequate risk assessment.
- Ensuring access to centralised resources:ensure access to centralised resources and tools for conducting the risk assessment and documenting its results in a transparent manner.
- Conducting independent assessments:perform independent assessments (by third parties or led by HQ)on the risk assessments conducted locally to obtain an outside view on the adequacy of the identified risks and mitigation measures developed locally.

Sanctions Policies And Procedures

A key feature of an effective SCP is the creation and implementation of clear, consistent and comprehensive sanctions policies and procedures. These should be specifically tailored to the organisation's unique risks and operational contexts. Below are some best practices for developing sanctions-related policies and procedures:

- Establishing a baseline policy framework:developing a comprehensive set of sanctions policies that outline the organisation's commitment to compliance. This framework should be aligned with international standards and regulatory requirements and be revised under a strictly monitored schedule.
- Tailoring policies to risk profiles: addressing specific risks associated with different regions, industries and business activities. This ensures that policies are relevant and effective in mitigating identified risks. For example, policies should consider the unique sanctions risks in high-risk jurisdictions and sectors.
- Integrating policies with business processes: including sanctions compliance in customer onboarding, transaction monitoring and supply chain management. This integration helps embed compliance into daily operations and decision-making.
-

Disseminating sanctions policies:communicating policies to all employees through clear and accessible channels. Ensure that employees understand their responsibilities and the importance of compliance. This can be achieved through regular training sessions, internal communications and accessible policy documents.

- Elaborating guidelines for complex sanctions-related scenarios: developing guidelines thatshowcase sophisticated circumvention efforts researched by trusted media outlets or observed internally while conducting adverse media screenings (ie, screening against oligarchs affiliated relatives or individuals).

HQs should ensure that subsidiaries implement effective sanctions policies and procedures. Below are a few practices that can support local compliance functions:

- Standardising policy frameworks: adopting the baseline sanctions policies established by HQ, with adjustments to address local regulatory requirements and risk profiles. This ensures consistency across the organisation while allowing for local customisation without a compromise on the update schedule.
- Supporting local customisation efforts:providing guidance and resources to ensure consistency and effectiveness of designed policies.
- Integrating with local processes: ensuring that activities such as customer onboarding, transaction monitoring and supply chain management are governed by documented procedures that align with local specifics and regulatory frameworks.

Training And Sanctions Knowledge Capabilities

One of the hallmarks of a well-designed SCP is appropriately tailored training and communications to ensure the programme is disseminated to, and understood by, employees in practice. Organisations can consider the following best practices when developing sanctions-related training as part of a holistic training approach:

- Determining a baseline standard: establishing a baseline standard for sanctions compliance knowledge that needs to be transmitted annually as part of the general training for employees.
- Developing tailored risk-based training material: creating materials designed for the first line of defence (1LOD), the second and third line of defence (2LOD, 3LOD), and senior management:[24]
    - for example, the 1LOD can be presented with concrete examples for day-to-day operations prone to sanctions risks. Sanctions training should equip the 1LOD with the knowledge to identify, address and escalate sanctions red flags when interacting with clients;
    - for the 2LOD and 3LOD, sanctions training can contain sophisticated patterns for detecting sanctions circumvention, trends in circumvention hubs and case studies of recent regulatory enforcements. Additionally, insights from conducted sanctions look-backs can be incorporated to highlight potential shortcomings in alert clearance processes or the application of the four-eye principle; and
    - senior management training on sanctions should encompass updates on sanctions regimes across various geographies, with a particular focus on

regions where the business operates. This training could also include recent enforcement actions and root causes to illustrate the critical role of a robust SCP throughout the organisation.

- Assessing knowledge post-training: evaluating the knowledge of employees after training completion and monitor mandatory completion with disciplinary measures for non-completion. Such evaluations can take form of tests following the training sessions with a minimum requirement for attestation. Non-compliance disciplinary actions need to be communicated to employees before commencing trainings and can manifest via limited access to systems, the impact on financial incentives and the impact on performance reviews, among other things.
- Following the standard training schedule: ensuring the standard training schedule is mandatory throughout the organisation.
- Developing additional materials: requiring local compliance functions to develop additional sanctions materials for relevant functions in local languages.
- Reporting to HQ: requiring reporting to HQ on the mandatory completion of training locally.
- Validating training quality: validating the quality of locally developed sanctions-related training materials.
- Providing centralised materials: ensuring subsidiaries have access to centralised thematic sanctions training materials to support their local efforts in developing effective training programmes.

Sanctions Screening Operations

The Wolfsberg Group Guidance on Sanctions Screening outlines sanctions screening operations as a mechanism of control, with fundamentals derived from regulatory requirements, expectations and industry good practices.[25]

Sanctions screening operations should be regarded by organisations as a stand-alone component of their SCPs. Organisations should consider the following best practices for effective screening operations:

- Developing a risk-based screening strategy: ensuring an appropriate frequency of customer screenings, integrate relevant sanctions lists into the process and continuously calibrate the screening technology through ongoing testing. Allocate clear ownership for the screening strategy guarded by personnel with sufficient technical capabilities to own the operations at hand.
- Conducting regular screening software calibration:regularly assessing screening software to evaluate the effectiveness and efficiency of implemented rules. Ensuring the effectiveness of screening systems is crucial. Avoid contradictory rules and unjustified alert suppression techniques that could weaken screening efforts. However, in practice, even effective screening can become inefficient. This often results in a high rate of false-positive alerts and prolonged post-screening processes.
- Maintaining robust list management processes: conducting regular checks on the completeness of third-party lists and internal whitelisting and blacklisting applicability.

- Implementing resilient alert clearance and case management: allowing for four-eyes checks and escalation, document the clearance rationale and ensure it can be reviewed by a third party or internal audit. The alert clearance rationale retention policy needs to be aligned with regulatory requirements, where applicable.
- Conducting thematic screening area assessments: performing targeted assessments on trade finance screening software, particularly screening for dual-use goods.
- Conducting regular sanctions lookbacks:performing internal and external sanctions look-backs regardless of whether breaches in screening operations occurred. This is particularly important given the significant changes in sanctions requirements in recent years. Such look-backs can be designed to assess the degree of compliance with particular areas of sanctions regimes. As, for example, the spectrum of measures implemented to comply with export controls, sanctioning of individuals and entities and sectoral sanctions.
- Cautious deployment of modern technical capabilities: oversee the deployment and enhancement of sanctions screening technologies across all subsidiaries to maintain adherence to HQ standards, ensure consistency in methodology and optimise group-wide compliance effectiveness. Mandate HQ coordination for all subsidiary-level sanctions technology initiatives, ensuring that new tools or system upgrades comply with corporate standards, align with group-wide optimisation strategies, and maintain consistent coverage and effectiveness across the organisation.

Even the most calibrated and efficient sanctions screening operations at HQ level are tested for resilience across subsidiary networks. It is not uncommon for subsidiaries to run on different software compared to HQ, struggle with legacy technology and lack the technical understanding of calibration techniques. The following helps HQs to align central requirements with local operations:

- Conducting a technical inventory:identifying deviations from the technical set-ups used at HQs. Subsidiaries may employ differing tools for customer and transaction screenings that do not meet HQ technical standards. Understanding these deviations is crucial for allocating the necessary budgets and resources to roll out unified technical solutions across subsidiaries with higher sanctions risk exposure.
- Offering regular technical assistance: providing support for local calibration efforts post implementation of unified or HQ-friendly solutions. Ensure the same level of documentation standards for calibration efforts as promulgated at HQs. The latter can standardise the formats for calibration reports that can be subject to regular update schedules at subsidiary level and subsequently verified at HQ level. Documentation related to screening calibration efforts can be requested by regulators alongside other SCP documentation.
- Developing locally applicable transliteration and spelling rules:implementing these rules into local screening operations. For example, transliteration best practices for Cyrillic names that can be developed by natives.
- Conducting sanctions look-backs at subsidiary levels: similar to HQ, conducting sanctions look-backs at subsidiary levels. Such look-backs can follow the thematic

assessments applied at HQ level or can be tailored to local specifics based on internal audit findings.

Testing And Internal Audit

An effective and independent auditing function can strengthen the SCP and enhance its robustness. HQ audit functions can adhere to the following best practices related to internal audit:

- Incorporating sanctions into routine audit schedules: using defined, consistent auditing standards that can be replicated at the subsidiary level.
- Defining and conducting risk-oriented audit cycles:focusing on areas of the business with higher exposure to sanctions risk for effectiveness testing.
- Taking immediate action on findings:upon learning of a confirmed negative testing result or sanctions-related audit finding, implementing compensating controls until the root cause of the weakness can be determined and remediated.
- Monitoring time to remediation: delays in implementing remediation actions can indicate additional issues related to the SCP that might have been overlooked. The inability to address high-risk observations in a timely manner poses significant regulatory risks and indicates reduced SCP flexibility.

HQ internal audit functions should ensure that subsidiaries are subject to internal auditing conducted locally or at a regional level. To facilitate effective subsidiary oversight for the audit function that includes sanctions, HQs can adhere to the following best practices:

- Conducting joint sanctions audits: understanding local sanctions challenges, share knowledge and align standards.
- Organising joint workshops and seminars: aligning on internal standards and facilitate continuous access to complex sanctions topics.
- Implementing local metrics for the audit function: monitoring these metrics at the HQ level and track remediation actions for high-risk sanctions findings.
- Leveraging audit technology at subsidiary level: ensuring subsidiaries have access to and utilise audit technology effectively.

CONCLUSION

In conclusion, the increasing complexity of sanctions compliance and broader anti-financial crime regulations, along with Germany's strengthened sanctions enforcement through SDG I and II, require companies to equip their compliance teams with sufficient resources – both human capital and tools. This applies not only to leading German banks and large corporates but also to any company with relevant exposure.

It is crucial to actively monitor regulatory changes and requirements in relevant markets. Additionally, ensuring that all documentation meets the standards set by regulators and other relevant third parties is essential. To maintain a robust SCP, companies must also invest in ongoing employee training, conduct regular risk assessments and establish effective internal controls.

To ensure both effectiveness and efficiency, regular internal assessments and continuous improvements are critical. External, independent expertise can further enhance the programme's resilience.

While this article focuses on sanctions compliance, the principles outlined are equally applicable to other anti-financial crime programmes, such as anti-money laundering, counter-terrorist financing and anti-bribery and corruption. Companies must adopt a proactive, adaptive approach to anti-financial crime compliance, ensuring they are well-prepared for evolving regulatory landscapes.

Endnotes

1 Top 10 DAX companies based on market capitalisation and HQ in Germany: SAP, Siemens, Deutsche Telekom, Allianz, Munich Re, Siemens Healthineers, Mercedes-Benz Group, Infineon, Siemens Energy and BMW. Market capitalisation as of February 2025. Market capitalisation as of February 2025. ^ Back to section

2 Subsidiary information for the top 10 DAX companies extracted by AlixPartners from the Investment Monitor platform, www.investormonitor.ai. ^ Back to section

3 The Investment Monitor platform used for compiling subsidiary information classified the following countries as Western Europe: the United Kingdom, Germany, the Netherlands, France, Spain, Luxembourg, Italy, Ireland, Switzerland and Sweden. ^ Back to section

4 Council Regulation (EU) No. 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. ^ Back to section

5 Timeline - EU sanctions against Russia - Consilium. ^ Back to section

6 Support Service - EU Sanctions Helpdesk - European Union. ^ Back to section

7 Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures and amending Directive (EU) 2018/1673. ^ Back to section

8 EU Council Press Release, Council gives final approval to introduce criminal offences and penalt
ies for EU sanctions' violation - Consilium. ^ Back to section

9 Commission takes action to ensure complete and timely transposition of EU directives. ^ Back to section

10 Refers to the AML Directives 2015/849 (4AMLD) and 2018/843 (5AMLD), while Directive 2018/1673 (6AMLD) remains in force since it defined criminal offences in the area of money laundering, and not preventive compliance framework requirements. ^ Back to section

11 Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Back to section

12 Federal Ministry of Finance, Sanctions Enforcement Act II: making sure sanctions work. Back to section

13 Federal Ministry of Finance, Stepping up the fight against financial crime. Back to section

14 Press Release: EBA and AMLA complete handover of AML/CFT mandates. Back to section

15 AMLA sets strategic priorities with 2026-28 Single Programming Document. Back to section

16 Embargo Act 946.231, 22 March 2002. Back to section

17 Sanctions and Anti-Money Laundering Act 2018. Back to section

18 OFSI's Sanctions Enforcement Overhaul: ofsis-sanctions-enforcement-overhaul-transparency-speed-and-higher-penalties.pdf. Back to section

19 Subsidiary information for the top 10 DAX companies extracted by AlixPartners from the Investment Monitor platform, www.investormonitor.ai. Back to section

20 Subsidiary information for the top 10 DAX companies extracted by AlixPartners from the Investment Monitor platform, www.investormonitor.ai. Back to section

21 SCP core pillars are shaped by: the US Department of Justice, Evaluation of Corporate Compliance Programs (updated in September 2024); the Department of the Treasury, Framework for OFAC Compliance Commitments; and the Wolfsberg Group Guidance on Sanctions Screening. Back to section

22 Commission Recommendation (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009. Back to section

23 A Framework for OFAC Compliance Commitments, ofac.treasury.gov. Back to section

24 Refers to the Three Lines of Defence Model, which divides responsibilities into three layers: operational management (1LoD), risk management and compliance functions (2LoD) and internal audit (3LoD). Back to section

25 Key Themes of the Wolfsberg Group Guidance on Sanctions Screening, www.wolfsberg-group.org. Back to section

AlixPartners

Adrian Mom amom@alixpartners.com
Svea Ottenstein sottenstein@alixpartners.com
Veronica Furtuna vfurtuna@alixpartners.com

United Kingdom

http://www.alixpartners.com

Greece: a regulatory compliance and corporate governance checklist for investors and boards in 2026

Kallia Gavela and **Orestis Omran**

Alvarez & Marsal

DLA Piper

Summary

IN SUMMARY

In recent years, Greece has introduced a series of new laws and regulatory amendments that have, collectively, raised the bar for governance maturity in the country. This has been driven both by domestic priorities and by local implementation of stricter EU-level directives in areas such as anti-bribery and anti-corruption, anti-money laundering (AML) and sanctions. Company boards and investors operating in Greece are now responsible to oversee a wider and more complex range of concerns around compliance, corporate governance and operational resilience.

DISCUSSION POINTS

- Comprehensive changes to Greece's anti-bribery, anti-money laundering and sanctions regimes
- Updates to corporate sustainability, diversity, data and digital finance
- Shift towards more robust oversight and increased scrutiny of board behaviour, internal processes and compliance
- More personal responsibility for board members and senior management, particularly in relation to AML, bribery and sanction failures
- Key developments in these areas and how they are requiring boards to adopt a more active oversight of regulatory and operational risks affecting their businesses

REFERENCED IN THIS ARTICLE

- Directive (EU) 2024/1226
- Law 5232/2025
- Law 5090/2024
- Directive (EU) 2024/1640
- Law 5193/2025
- Regulation (EU) 2022/2554
- Law 5236/2025
- Directive (EU) 2022/2557
- Law 5160/2024
- Law 5164/2024
- Directive (EU) 2024/1760
- Directive (EU) 2022/2464
- Law 4706/2020

Today's corporate boards operate within an unprecedentedly volatile risk and regulatory environment, marked by heightened complexity, accelerated change and expanding

accountability. Geopolitical instability, AI-powered cyber threats, climate change and disrupted and fragile supply chains form just part of a complex web of challenges that organisations must monitor closely to avoid operational disruption and regulatory failures.

A recent World Economic Forum survey illustrates this unease, with half of global executives expecting stormy conditions over the next two years. Emerging threats like AI misuse and cyber insecurity are seen as likely triggers of a global crisis in the near term.[1]

Meanwhile, regulation is reaching further and intensifying the pressure on compliance functions while elevating the board's responsibility for effective oversight.

Against this backdrop, the spotlight on boards to manage compliance, risk and organisational resilience has tightened. Directors are expected to ensure that governance frameworks, internal controls and reporting mechanisms are sufficiently robust to withstand regulatory and investor scrutiny. The traditional oversight model, where directors reviewed reports, approved policies and intervened only when issues arose, is giving way to a more proactive approach. Increasingly, boards are engaging in shaping enterprise resilience strategies, ensuring that new risks are integrated at a strategic level and working in closer partnership with the leadership.

This evolution is also visible in Greece, where a series of new amendments have expanded firms' obligations and heightened expectations of boards.

The following sections explore these developments in detail and provide a roadmap for boards looking to adopt a more active oversight of regulatory and operational risks affecting their businesses.

SANCTION COMPLIANCE

The European Union operates under three distinct sanction regimes. First, sanctions adopted by the United Nations Security Council (UNSC), which the European Union is required to transpose into EU law. Second, the European Union may reinforce the UNSC's sanctions by adopting additional stricter measures, that is, the mixed sanctions. Third, the European Union can impose sanctions autonomously without a UN mandate. At present, the European Union maintains more than 40 EU autonomous sanction regimes the majority of which are geographically focused (eg, Syria, Iran, North Korea and Russia). Others are horizontal in scope targeting threats such as terrorism, cybersecurity, the use of chemical weapons and serious human rights violations.

While EU sanctions are directly applicable in all EU member states, their enforcement is governed at national level. To ensure more consistent and effective sanction enforcement across member states, the European Union adopted Directive (EU) 2024/1226,[2] which imposes minimum harmonisation regarding the definition of criminal conduct in case of sanction violations and the penalties applicable to them.

In September 2025, Greece enacted Law 5232/2025, which transposed Directive (EU) 2024/1226 into national law. Law 5232/2025 introduced increased penalties for sanction violations, including prison sentences on natural persons of up to 10 years. In case of aggravating circumstances, the minimum term of imprisonment is increased by an additional year. A particularly aggravating circumstance arises when the violation concerns the import, export, sale, purchase, etc of dual-use items under Regulation (EU) 2021/821[3] or items listed in the EU Common Military List. Under Law 5232/2025, legal entities can be held liable to pay fines of up to 5% of the legal entity's concerned annual global turnover

or €40 million. Legal entities may also face exclusion from access to public funding and participation in public tender procedures.

Following the adoption of Law 5232/2025, enforcement activity in Greece is expected to increase. To avoid the risk of committing a sanction violation, businesses established in Greece and those doing business in the country should ensure transparent ownership and control structures, maintain robust contractual safeguards and implement continuous monitoring measures.

ANTI-BRIBERY, AML AND CORRUPTION

Alongside significant changes to its sanction regime, Greece has recently overhauled its anti-bribery and AML framework as it continues to converge with evolving EU norms.

Law 5090/2024 introduced, for the first time, a comprehensive system of corporate criminal liability for corruption offences, filling a long-standing gap in Greek legislation. Under article 1, a legal entity may be held liable for bribery offences committed for its benefit or on its behalf by persons who exercise management or control, represent the entity or are authorised to make decisions. Article 2 further extends liability to situations where inadequate supervision or control enables bribery to be committed by lower-level officials.

Liability as a general term may refer to individuals and entities alike and may be criminal or civil. Regarding criminal liability, in principle, it applies to individuals. However, there are special provisions for entities' liability within the context of criminal proceedings in relation to corruption offences. An entity that has been involved in corruption acts and has benefited or gained from these acts may be the subject of criminal proceedings. The entity becomes party to the proceedings (pre-trial and trial) and may face penalties such as fines, suspension of operations, licensing termination and so on. Regarding civil liability, individuals and entities may be held liable during civil proceedings. Individuals and entities may also be held liable during independent proceedings conducted by other regulatory bodies (eg, the Capital Market Commission, the Competition Commission, the Central Bank of Greece, etc).

The penalties stipulated by Law 5090/2024 for bribery offences committed by legal entities include fines, potential prohibition of business operations and the temporary or permanent suspension of the company's operating licence. Specifically, bribery may result in fines between €50,000 and €10 million, which may reach up to double the pre-tax annual net profits of the legal entity, if the entity's annual net profit before tax exceeds the €10 million cap. Other penalties may include the permanent suspension or temporary suspension of business for a period of one month to two years, as well as the revocation of the operating licence.

In addition, lack of monitoring and control may lead to a fine of €10,000 to €5 million, which may reach up to double the pre-tax annual net profits of the legal entity, if the entity's annual net profit before tax exceeds the €5 million cap. Other penalties may include the permanent or temporary, for a period of up to one year, revocation or suspension of the operating licence or prohibition of doing business activity.

AML

Concerning AML, Greek companies will need to adjust their internal controls and practices to the new EU-wide AML framework (Directive 2024/1640), including the new EU AML authority (AMLA) and its broad mandate including power to investigate and penalise breaches.[4] Greece is expected to implement the Directive in its national legislation by July 2027.

The Directive imposes several new obligations on EU member states, making the overall AML framework more stringent. The regime on Ultimate Beneficial Owners (UBOs) registers is expanded, with enhanced requirements on transparency. It also expands the obligation to maintain centralised automated mechanisms (registers or data retrieval systems) so that persons holding or controlling bank accounts can be identified in a timely manner to securities accounts and crypto-asset accounts.

Another novelty concerns Financial Intelligence Units (FIUs). These units will be required to designate a Fundamental Rights Officer, which will monitor the FIU's compliance on fundamental rights and will inform the unit head on possible violations of fundamental rights.

AMLA[5] will play a central role in the correct implementation of the Directive, as it is the new EU authority tasked with overseeing AML supervision in the European Union. AMLA has several supervisory responsibilities on FIUs, such as contributing to cooperation and facilitating joint analyses for relevant cross-border cases. The AMLA is also responsible for directly supervising selected obliged entities and for facilitating the functioning of supervisory colleges, contributing to the conveyance of supervisory practices and taking appropriate measures when intervention is required.

Prior to becoming fully operational in 2028, AMLA is currently developing the methodology that will define which institutions will fall under its direct supervision. It has also launched a public consultation on three draft regulatory technical standards (RTS) that will clarify elements of the new regime, such as criteria for business relationships and customer due diligence rules.[6]

These reforms on the anti-bribery and AML frameworks mark a significant shift in Greece's approach to corporate misconduct. The introduction of corporate criminal liability demonstrates the country's willingness to align with general EU practice and pursue legal entities directly. Boards, compliance functions and senior management bodies are expected to demonstrate active oversight and effective monitoring systems, while companies should see increased scrutiny of internal controls and supervisory processes, especially given the law's emphasis on failures of oversight.

Collectively, these reforms signal a decisive move toward a governance environment grounded in prevention, transparency and accountability.

New EU Criminal Rules Against Corruption

Furthermore, Greece is preparing to align with the first EU-wide criminal law rules against corruption, which will set common anti-corruption regulations across the European Union and strengthen enforcement cooperation across borders.

The European Commission submitted a proposal for a Directive[7] on combating corruption, aiming to:

- harmonise definitions for offences such as bribery, misappropriation of funds and obstruction of justice;
- introduce common rules on corruption offences; and
- establish a common level for maximum prison sentences across the European Union.

As part of a December 2025 provisional agreement, the European Parliament ensured that EU-wide corruption data will be published annually in accessible formats, improving

transparency. This approach will reinforce cooperation among national authorities and EU bodies including the European Anti-Fraud Office (OLAF), the European Public Prosecutor's Office, Europol and Eurojust, towards combatting cross-border corruption.

This is a highly significant development for Greece, as companies will be required to adopt more stringent preventative compliance frameworks. Particularly, companies engaging in cross-border activities will face heightened scrutiny from national authorities, but also from coordinated EU authorities.

LISTED COMPANIES AND CORPORATE GOVERNANCE RULES

Listed companies in Greece have already been subject to stronger corporate governance mechanisms through Law 4706/2020. This legislation introduced several provisions strengthening corporate governance requirements within companies, increasing transparency and accountability, improving investor protection and aligning with EU rules to create a safer investment environment.

More specifically, Law 4706/2020 introduces the obligation on the board of a company to adopt a fit and proper policy setting the eligibility criteria for the appointment of the board of directors' members, such as knowledge, skills, experience, independent judgment, character and integrity.[8] In addition to the fit and proper framework, Law 4706/2020 expands the responsibilities of the board by requiring the effective operation of internal audit, risk management and regulatory compliance mechanisms, reinforcing internal control structures.

With regards to gender representation and diversity, an important development was Law 5178/2025, which transposed Directive (EU) 2022/2381, the Women on Boards Directive. Under the provisions of new article 3A, the gender board quota for listed companies in Greece has been increased to 33% from 25%.[9]

ELEVATED CORPORATE GOVERNANCE RESPONSIBILITIES ON BOARDS OF FINANCIAL INSTITUTIONS

In July 2025, the Bank of Greece established additional standards of internal governance applicable to financial institutions, by issuing Act No. 243/2/07.07.2025. The Act clarifies the role, structure and responsibilities of the board of directors, including the need to distinguish clearly between supervisory and executive functions. It calls for the implementation of a forward-looking business plan (covering at least three years) that takes into account all relevant risks, including money laundering threats and ESG-related risks.

The Act also strengthens the governance framework for board committees, particularly by clarifying the different functions of the risk management committee and the internal audit committee.

In terms of risk management, the Act promotes the establishment of a robust risk culture. Institutions must be able to make timely and well-informed decisions aimed at reducing their exposure, both individually and at group level. Boards are responsible for setting and enforcing high ethical and professional standards, ensuring that internal policies remain neutral and non-discriminatory. Moreover, the Act enhances the internal control and regulatory compliance framework by requiring institutions to adopt a holistic approach to risk and internal controls. This includes implementing an integrated risk management system covering all business areas, applying strict procedures for approving

new or significantly altered products or services and ensuring the independence of risk management, compliance and internal audit functions.

The strengthened governance framework requires boards of financial institutions to exercise far more active and informed oversight, ensuring that strategy, risk management and internal control systems are not merely formalities but functioning, forward-looking mechanisms.

DIGITAL RESILIENCE IN FOCUS

Digital resilience has moved to the forefront of businesses' risk agendas as rapid technological innovation has introduced threats of unprecedented scale and complexity.

As an illustration, in the fraud space, AI technology is making scams more sophisticated and harder to detect. Generative AI and large language models (LLMs) are enabling hyper-personalised phishing and lifelike deepfakes that can bypass traditional identity verification methods. In the financial sector, underground banking networks are leveraging technology to facilitate illicit financial flows.[10]

Recent Greek reforms in 2025 have significantly strengthened the national regulatory framework on digital resilience and cybersecurity. Law 5193/2025 established the national framework necessary to supplement the EU Digital Operational Resilience Act (DORA),[11] which introduces a harmonised EU framework directly (ie, with no need for transposition on a national level) applicable to all member states. DORA aims to improve the security and resilience of the financial sector against the increased threats and the digital fluctuations. DORA's scope covers, among others, credit institutions, payment institutions, trading venues, investment firms and electronic money institutions.[12]

DORA introduces an obligation on financial entities to have an Information and Telecommunications Technology (ICT) risk management framework as part of their overall risk management system that is sound, comprehensive and well-documented. Such frameworks will include strategies, policies and tools to minimise the exposure to and impact of ICT risk.[13] Entities must also have in place a reporting system to notify ICT-related incidents and notify clients when appropriate.[14]

According to article 149 of Law 5193/2025, the competent authorities for supervising the correct implementation of DORA in Greece are the Greek National Bank and the Hellenic Capital Markets Commission (HCMC).

Similarly, Law 5236/2025 brought into national law Directive (EU) 2022/2557[15] on the resilience of entities providing essential services. Law 5236/2025 coordinates with Greece's NIS2 regime (Law 5160/2024), aligning physical and organisational resilience requirements with cybersecurity rules.[16] The new framework aims to strengthen the resilience of critical entities against physical and technological risks as well as to ensure the smooth operation of critical services essential for public security, economy and society. The law is applicable to critical entities in the sectors of energy, transport, banking and financial markets, health, drinking water and wastewater, digital infrastructure, public administration, space and production, processing and distribution of food.[17]

The 2025 digital resilience reforms mark a significant shift in Greece's governance architecture for managing technological and operational risk. By embedding DORA into the national supervisory framework, Greece has moved toward a governance model in which digital resilience is treated as an integral component of institutional oversight. Supervisory bodies, the Bank of Greece and the HCMC, are now expected to apply consistent,

EU-harmonised standards when assessing the adequacy of ICT governance structures, risk management committees and escalation procedures. This strengthens the overall system of institutional accountability and positions digital resilience as a core pillar of financial-sector governance.

At the same time, the implementation of the Critical Entities Resilience Directive through Law 5236/2025 extends this governance evolution beyond the financial sector to essential services more broadly. The new classification of "critical entities" introduces governance obligations centred on risk identification, continuity planning and cross-sector coordination. National authorities, including the General Secretariat for the Security of Critical Entities, will need to adopt more integrated supervisory and monitoring practices, ensuring alignment between physical resilience, organisational preparedness and cybersecurity rules under NIS2.

SUSTAINABILITY REQUIREMENTS IN FLUX

Amid a broader policy debate over how to balance sustainability ambitions with the practicalities of corporate compliance, the European Union has put forward a series of amendments to streamline its major sustainability regimes and boost competitiveness through significantly reducing the sustainability reporting and due diligence requirements for entities that are currently within the scope of the CSRD, the EU Taxonomy (EUT)[18] and Directive (EU) 2024/1760[19] on corporate sustainability due diligence (CSDDD). In addition to higher applicability thresholds, the Omnibus text introduces significant relief regarding both reporting and due diligence requirements. For example, it removed the CSDDD's obligation for companies to prepare climate transition plans and lowered the maximum fine for pecuniary penalties to 3% of global revenues. A provisional agreement reached in December 2025 extended the deadlines for the CSDDD to be transposed into national law (to July 2028) and increased thresholds for coverage (effectively scaling back reporting obligations for companies of a certain size). If this agreement is finally approved by the Council and the European Parliament, significant amendments to Law 5164/2024 will be introduced.

Despite what can be seen as an overarching trend toward simplification, sustainability considerations remain embedded directors' duties under Greek corporate law. Through their duties of care, loyalty and diligence, directors are required to identify, assess and manage material risks affecting the company, including climate-related and environmental risks where these may have financial or operational impact. Failure to manage foreseeable climate-related risks or ignorance of material nature-loss risks may constitute a breach of directors' duties and may give rise to civil liability towards the company.[20]

THIRD-PARTY RISK MANAGEMENT

Regulatory expectations around third-party risk management continue to intensify, posing an additional challenge for businesses and their boards.

While companies are generally able to control their own activities to ensure compliance with regulations, keeping the same level of oversight over their third parties is far more challenging, particularly for those firms operating across dispersed and globalised value chains.

Any misconduct, weakness or failure by a third party acting on behalf of a company can lead to severe penalties, reputational damage and operational disruptions for that company. Vendors are now identified as a key access point for ransomware attacks and data breaches;

88% of companies surveyed in a 2024 report cited a compromise in their vendor supply chain as the cause of their breach, up from 77% in 2023.[21] Recent high-profile incidents where third-party failures led to severe business disruption highlight this has become a boardroom issue.

Regulators are increasingly scrutinising companies' outsourced activities and oversight of business relations, and organisations are no longer exposed only to internal operational risks but also to vulnerabilities embedded within their supply chains. This reflects a core regulatory principle: operational functions can be outsourced, but accountability cannot. To achieve this goal and hold organisations accountable, regulators impose fines or remedial orders for failures committed by third parties in their value chain.

For example, the EU NIS2 Directive, effective since 2024, requires firms to conduct ongoing risk assessments of third-party IT services to ensure adherence to robust standards. Third-party risk management is also one of the core pillars of DORA, with financial firms expected to monitor digital risks across their extended ICT supply chain, a monumental task that can involve the review and updating of hundreds of contracts.[22]

The EU AI Act requires organisations to implement robust third-party risk management frameworks, especially for high-risk AI systems. This includes conducting thorough due diligence across their vendor ecosystem, integrating AI-specific compliance into contracts and the continuous monitoring of third-party AI usage and data protection practices.

The expansion of EU-level rules on third-party due diligence reflects a shift in the legal framework for corporate accountability from an organisation-centric model toward a model in which governance bodies must account for risks generated outside their own structures and into the wider value chain.

In managing risks, companies are expected to work directly with business partners, as well as with affected stakeholders or representatives. However, if this does not lead to successfully managing the risks, the company may, as a last resort, choose to temporarily suspend the business relationship until the risk is resolved, or refrain from entering into new or existing relations with the relevant partner, if it has been determined that the situation will not be further affected.[23]

RECOMMENDATIONS FOR BOARDS AND INVESTORS CONDUCTING DUE DILIGENCE ON GREEK ASSETS

The evolving Greek regulatory landscape is raising the level of scrutiny and expectations placed on boards and investors during due diligence. Boards have a duty to ensure effective compliance through stronger governance standards across Greek corporate structures, including whistleblowing procedures, internal investigations and third-party management. Due diligence is no longer limited to financial soundness or contractual review; it must include a comprehensive assessment of governance structures and internal controls.

We recommend that boards:

- Embed risk and compliance into strategy: ensure that regulatory, digital resilience, sustainability and third-party risks are treated as core strategic considerations. Compliance and resilience objectives should be reflected in business planning, investment decisions and performance metrics.
-

Strengthen governance structures and accountability: given the growing personal and corporate liability exposure, boards should review whether their governance arrangements remain fit for purpose. This includes clarifying oversight responsibilities, enhancing the mandates of audit and risk committees, and ensuring that risks are embedded within governance frameworks.

- Conduct regular, enterprise-wide gap analyses:boards should require management to periodically assess existing policies, procedures and controls against evolving EU and national requirements. Identified weaknesses should be addressed through structured remediation plans with clear timelines and ownership.
- Invest in integrated, data-driven risk management frameworks:boards should promote the development of holistic risk management frameworks that link regulatory compliance, operational resilience, sustainability and third-party oversight. These frameworks should be supported by reliable data, digital monitoring tools and clear escalation mechanisms.
- Enhance oversight of third parties and transactions: with regulatory expectations extending across value chains, boards should ensure that robust due diligence processes are applied to customers, suppliers, partners and acquisition targets. This includes risk-based assessments, contractual safeguards, audit rights and ongoing monitoring. M&A and major outsourcing arrangements should receive heightened board-level scrutiny.
- Embed a strong culture of integrity and sustainability: sustainable compliance depends on organisational culture. Boards must set the tone from the top by promoting ethical conduct, transparency and long-term value creation. Incentive structures, performance evaluations and leadership messaging should reinforce responsible behaviour and respect for regulatory obligations.
- Strengthen skills, training and awareness:directors and employees alike must remain informed about regulatory developments and emerging risks. Boards should support continuous training programmes and ensure that they themselves receive regular briefings on legal, technological and sustainability trends affecting the business.

Endnotes

1 https://www.weforum.org/publications/global-risks-report-2026/digest/. ^ Back to section

2 Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 ^ Back to section

3 Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), OJ L 206, 11 June 2021. ^ Back to section

4 Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by member states for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849, OJ L,19 June 2024. Back to section

5 Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, OJ L, 10 June 2024. Back to section

6 https://www.amla.europa.eu/amla-consults-key-mandates-private-sector-and-harmonized-supervision_en. Back to section

7 2023/0135(COD). Back to section

8 Law 4706/2020, article 3. Back to section

9 https://faolex.fao.org/docs/pdf/gre232870.pdf. Back to section

10 https://www.acams.org/en/opinion/how-ai-and-fraud-are-reshaping-afc-inside-acams-global-threats-report-2026. Back to section

11 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) No. 2016/1011. OJ L 333/1, 27 December 2022. Back to section

12 ibid., article 2. Back to section

13 ibid., article 6. Back to section

14 ibid., article 17. Back to section

15 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333/164, 27 December 2022. Back to section

16 https://www.zeya.com/newsletters/greece-transposes-directive-eu-2022557-resilience-critical-entities. Back to section

17 Law 5236/2025, article 3(1). Back to section

18 Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088, OJ L 198, 22 June 2020. Back to section

19 Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859, OJ L, 2024/1760, 5 July 2024. ^ Back to section

20 https://climate-governance.org/cza-content/Greece-Directors-Duties-Navigator-2026.pdf. ^ Back to section

21 https://6236605.fs1.hubspotusercontent-na1.net/hubfs/6236605 /Marketing%20Collateral/2024-TPRM-Report.pdf. ^ Back to section

22 https://www.fsisac.com/hubfs/Knowledge/DORA/FSISAC_DORA-Implementation Guidance.pdf. ^ Back to section

23 ibid., article 11. ^ Back to section

Kallia Gavela kgavela@alvarezandmarsal.com

http://www.alvarezandmarsal.com

Orestis Omran orestis.omran@dlapiper.com

http://www.dlapiper.com

Italy: corporate criminal liability and how the system works

Roberto Pisano
Studio Legale Pisano

Summary

IN SUMMARY

Legislative Decree No. 231/2001 on corporate criminal liability significantly affected the practice of criminal lawyers in advising corporate entities and their strategy for criminal investigations and prosecutions. Companies can be considered liable in respect of a wide range of criminal offences committed by their managers or employees in the interest or for the benefit of the company. A company will be deemed liable for having committed an administrative offence if it has not implemented an adequate compliance programme that is able to prevent the commission of the criminal offence by its managers or employees. If the criminal offence is committed by senior managers, corporate liability can theoretically be avoided; however, the standard of proof is extremely high and almost unreachable in practice.

DISCUSSION POINTS

- Nature and requirements of corporate liability
- Applicable procedure
- Conditions to exclude or mitigate corporate liability
- Applicable sanctions

REFERENCED IN THIS ARTICLE

- Legislative Decree No. 231/2001
- Court of Cassation, United Sections, 24 April 2014, Case No. 38343
- Court of Cassation, Section VI, 11 November 2021, Case No. 23401
- Code of Criminal Procedure
- *Impregilo*
- *Siemens AG*

FUNDAMENTAL PRINCIPLES OF CORPORATE CRIMINAL LIABILITY

As of 2001, companies can be considered criminally liable with regard to a list of criminal offences committed by their managers or employees in the interest or for the benefit of the company (Legislative Decree No. 231/2001 (Law 231)).

The list of predicate offences is constantly updated and broadened. It currently covers a wide range of business crimes, such as corruption, tax fraud and fraud against the state, market manipulation and insider trading, false accounting, money laundering, handling of stolen goods, health and safety crimes, intellectual property crimes, infringement of trademarks, environmental crimes and, as of 2026, violation of EU sanctions and restrictive measures.

A company's liability is qualified by the law as an "administrative offence" that comprises not having implemented an adequate compliance programme or internal control system that is able to prevent the commission of the criminal offence by its managers or employees; however, the competence for the investigation and prosecution of a company's offences lies with the usual prosecuting authorities, in accordance with the rules regarding criminal

procedures and in the frame of criminal proceedings subject to the jurisdiction of criminal courts, which are usually joined with the criminal proceedings against the managers or employees who committed the predicate offence.

Case law on this is consolidated in the sense that the corporate liability has the nature of criminal liability, with the consequence that all related principles and guarantees provided for by criminal law (ie, personality of criminal liability) must be applied.[1]

FUNDAMENTAL PRINCIPLES OF CRIMINAL PROCEDURE

In the Italian legal system, public prosecutors are responsible for the investigation and prosecution of all criminal offences, including business crimes, of both individuals and companies. They are assisted by the police.

Public prosecutors are not part of the government but are professional magistrates, such as court judges, and their decision to bring criminal prosecutions is compulsory not discretionary. This means that when they acquire or receive a "notice of crime" – a notice regarding specific facts potentially constituting a crime – they have a duty to open formal criminal proceedings (by immediately registering the notice in a special register) and start an investigation. Subsequently, if they assess that an offence was committed by certain individuals or companies, they have a duty to bring a criminal prosecution by requesting the committal for trial of the targets.

The investigation does not start if the event to which the notice refers is clearly unable to constitute a criminal offence (including a company's offence). In any case, where public prosecutors assess that the notice of crime is ungrounded, they have the power to directly dismiss the case with regard to companies, although with regard to individuals they must request the dismissal to the competent judge (the judge for preliminary investigations).

The notice of crime can be generated from multiple sources, such as criminal complaints filed by injured parties; reports made by the police, other public officials or the relevant enforcement agencies (eg, tax authorities or the authority regulating the financial market, Consob); or other channels, such as press articles.

The acts of investigation carried out by the public prosecutors with the assistance of police officers are, with some exceptions, covered by judicial secrecy until the conclusion of the preliminary investigations. The time limit for carrying out and concluding the preliminary investigation is one year, extendable up to a maximum of two years (and even longer if new suspects are added to the original investigation).

Once the individuals and companies under investigation receive a notice of conclusion of the investigations, they are entitled to obtain a copy of all the acts of investigation,[2] and in the subsequent 20-day period, they have the right to request to be interviewed by the public prosecutor and to file written submissions to convince the prosecutor's office not to request the committal for trial.

The existence of a criminal investigation is usually publicly acknowledged before the conclusion of the investigation, especially when significant acts of investigation are carried out, such as the execution of search and seizure or the issuance of arrest warrants. Individuals or companies that are potential targets of a criminal investigation have the right to file a formal application to the public prosecutor to be informed about their status as persons under investigation. Under specific requirements, the public prosecutor can deny disclosure for a limited period.

CONDITIONS FOR EXCLUDING CORPORATE CRIMINAL LIABILITY

Under article 5 of Law 231, companies can be considered criminally liable for not implementing an adequate compliance programme or internal control system that is effectively able to prevent criminal offences by their managers or employees that are committed in the interest or for the benefit of the company.

If the predicate criminal offence is committed by an employee, the company can avoid liability by proving that it has implemented an adequate compliance programme that is properly designed to effectively prevent the commission of that type of offence;[3] however, if the offence is committed by senior managers, the liability of the company can be avoided only by proving that:

- the company has implemented an adequate and effective compliance programme;
- there was sufficient surveillance by the supervisory board (ODV); and
- the senior manager committed the offence by "fraudulently circumventing" those corporate internal controls.[4]

In this scenario, a crucial role is performed by the ODV, which is responsible for monitoring and continuously supervising the effectiveness and adequacy of the compliance programme or internal control system for the purpose of excluding or mitigating corporate criminal liability. In particular, to exclude liability, the ODV must be composed of qualified professionals and have, and effectively exercise, autonomous powers of action that are independent from those of the management (and other corporate bodies).

In practice, case law indicates that if the predicate criminal offence was committed by a senior manager, the standard to prove that the compliance programme in place and the surveillance by the ODV were totally adequate and effective, and that the perpetrator acted by fraudulently circumventing those internal controls, is extremely high and almost unreachable.

A violation by a senior manager of the principles, policies and procedures imposed by the compliance programme is not sufficient to obtain an acquittal: the company has the burden of proving that the senior manager fraudulently circumvented the internal control system and was effectively able to mislead the other officers and bodies of the company in such a way as to prevent a perfect internal control system from detecting and impeding the violation.[5]

In practice, the above standard is extremely difficult to meet and almost unreachable. There have been several requests and proposals for change by scholars and the business community.

SANCTIONS

Sanctions applicable to companies under Law 231 include fines, disqualifications and confiscation of the proceeds of crime.[6]

Fines always apply in the event of a company's conviction. Their financial impact does not usually exceed €3 million (but it can reach €40 million for the violation of EU sanctions), and it is often lower depending on several factors, such as the type and seriousness of the offence, the degree of liability of the company, the activity carried out by the company to eliminate or reduce the consequences of the offence and prevent the commission of further offences, and the economic and patrimonial conditions of the company.[7]

Disqualifications can include:

- suspension or revocation of government authorisations, licences or concessions;
- debarment (prohibition of entering into contracts with the public administration);
- exclusion from or revocation of government financing, contributions or subsidies; and
- prohibition from carrying on business activity.

Disqualifications compulsorily apply in the event of conviction of the company, where the following requirements are met:

- the criminal offence was committed by a senior manager or by employees and, in the latter case, the commission of the offence was a result of serious organisational deficiencies; and
- the company has obtained "significant profits" as a result of the crime committed by its managers or employees.[8]

Disqualifications compulsorily apply if there is a repeat of the company's offence. A repeat offence is deemed to have occurred if the company commits an offence in the five-year period subsequent to its *res judicata* conviction for a previous and different offence.[9]

Disqualifications can be particularly damaging. This is amplified by the fact that they can also be applied at a pretrial stage, during the investigations, as interim coercive measures.[10]

The application of interim coercive measures, such as disqualifications, is ordered by the judge for preliminary investigations on request of the public prosecutor, if the following requirements are met:

- there is serious evidence of a company's commission of an offence;
- there is a concrete risk of further offences being committed (of the same type as the ones under investigation); and
- the company has obtained significant profits as a result of the crime committed by its managers or employees.

An advisable strategy to reduce the risk of a company being subject to interim coercive measures is to eliminate the risk of commission of further offences. If there appears to be *prima facie* grounds for a criminal investigation, it is advisable to react to the knowledge of those grounds by immediately adopting appropriate and effective reaction measures, such as:

- suspending working relations with and revoking the powers of the managers or employees who are alleged to have had a key role in the criminal activity;
- entrusting a qualified forensic firm to carry out an in-depth assessment of the allegations and the effectiveness of the company's internal control system, with the task of identifying any possible gaps and advising on improvements; and
- presenting to the prosecuting and judicial authorities an effective remedial plan to be promptly implemented.

LENIENCY AND COOPERATION WITH THE AUTHORITIES

There is no formal mechanism by which companies can cooperate with the investigation or disclose violations in exchange for immunity or lesser penalties (with the exception of plea bargaining); however, a certain degree of cooperation with the prosecuting authorities during the investigations and before trial can have a significant impact on reducing the pretrial and final sanctions imposed on the company.

In particular, applicable fines can be reduced by up to two-thirds, and disqualifications can be excluded if the following conditions are fulfilled before the opening of the trial of first instance is declared:

- the company has entirely compensated the damage and eliminated the damaging consequences of the crime, or has taken effective actions in that respect;
- the company has eliminated the organisational deficiencies that gave rise to the crime by adopting and implementing an adequate compliance programme that is able to prevent the commission of offences of the same type as those under investigation; and
- the company has made the profits obtained from the crime available to the authorities for confiscation.[11]

To benefit from leniency, it is generally advisable that the company adopt appropriate and effective reaction measures as soon as it becomes aware of the investigation and ensure that those measures are fully executed before the deadline provided for by the law (ie, the declaration of the opening of the trial of first instance).

Under certain conditions, plea bargaining with the prosecuting authorities is recognised by Italian law, both for individuals and for companies.

With regard to individuals, the plea bargaining must be approved by the competent judge. The punishment agreed with the prosecution's office cannot be more than five years' imprisonment, and it is considered equivalent to a conviction (with certain exceptions) by an express law provision.[12] The adoption of a plea bargaining entitles the offender to up to a one-third reduction of the punishment.

With regard to companies, a similar mechanism of plea bargaining is available in relation to less serious offences and to predicate criminal offences for which the managers or employees under investigation are entitled to a plea bargaining.[13] The reduction of the sanctions by up to one-third owing to a plea bargaining also applies, and the reduction operates on the amount of the fine and the length of the relevant measure of disqualification.

Even if the plea bargaining is considered equivalent to a conviction by an express law provision, an admission of wrongdoing is not required. In particular, according to case law, a plea bargaining cannot be considered an admission of wrongdoing but rather as an incomplete assessment of liability deriving from the decision of the defendant to renounce its challenge of the charges.

In the related civil, tax and ethical litigations, the plea bargaining cannot be used as evidence.-[14]

A conviction of the company for offences under Law 231 – and, under certain conditions, a plea bargaining – may remove the ability of the company to take part in public tenders.

JURISDICTION OF ITALIAN COURTS AND LIABILITY UNDER LAW 231

The main governing principle of the jurisdiction of Italian courts, in respect of both individuals and companies, is territoriality, according to which Italian courts have jurisdiction on all offences considered to be or to have been committed within Italian territory. This principle is subject to derogation in favour of extraterritorial jurisdiction only to a very limited extent and under stringent requirements.

The principle of territoriality is interpreted in a broad sense with a wide reach since it is sufficient that only a portion of the prohibited conduct took place in Italy for it to be under Italian jurisdiction; therefore, foreign companies that have their registered seat and main place of business abroad can be subject to Law 231 and be prosecuted in Italy if at least a portion of the criminal offence committed by their managers or employees took place in Italy and all the other requirements for the company's liability are fulfilled.

In essence, the predicate offence must have been committed in the interest or for the benefit of the foreign company by its managers or employees, and the foreign company should have failed to implement an adequate and effective compliance programme to prevent the commission of the offence.

The principle of the liability of foreign companies under the strict terms mentioned above (with a corresponding burden to adopt a compliance programme in accordance with the principles of Law 231, if the companies are conducting part of their business in Italy) is consolidated in Italian case law, ever since the landmark decision *Siemens AG*.[15]

In respect of companies that have their main seat (registered office or main place of business) in Italy, including Italian subsidiaries of multinational groups, the jurisdiction of the Italian courts applies not only to offences committed in Italy but also to offences committed abroad, under stringent conditions (including the fact that the offence is not prosecuted in the foreign state of commission);[16] therefore, in that limited respect, the principle of territoriality is subject to derogation in favour of extraterritorial jurisdiction.

Law 231 does not provide for any express provision to regulate corporate liability in a group of companies. The most significant issue, in particular, is whether a parent company can be held responsible under Law 231 in relation to a criminal offence committed in the immediate interest or for the benefit of its subsidiary.

According to the prevailing case law, the answer is negative: a holding or parent company can be responsible under Law 231, but only if the relevant law requirements are satisfied. In particular, a manager or employee of the parent company must be involved in the commission of the predicate criminal offence, and the predicate criminal offence must have been committed in the specific interest or for the specific benefit of the parent company. In other words, it is not admissible to infer an interest or benefit for the parent company only on the basis of the group relation, because this conflicts with the fundamental principle of personality of criminal liability.[17]

Endnotes

1 Court of Cassation, United Sections, 24 April 2014, Case No. 38343. ^ Back to section

2 Code of Criminal Procedure (CCP), articles 329 and 415-bis. ^ Back to section

3 Legislative Decree No. 231/2001 (Law 231), article 7. Back to section

4 Law 231, article 6. Back to section

5 Court of Cassation, Section V, 18 December 2013, Case No. 4677, ***Impregilo***; Court of Cassation, Section VI, 11 November 2021, Case No. 2340, ***Impregilo***. Back to section

6 Law 231, article 9. Back to section

7 Law 231, articles 10 to 11. Back to section

8 Law 231, article 13. Back to section

9 Law 231, article 20. Back to section

10 Law 231, article 45. Back to section

11 Law 231, article 17. Back to section

12 CCP, article 445. Back to section

13 Law 231, article 63. Back to section

14 CCP, article 445, paragraph 1-bis. Back to section

15 Milan Judge for Preliminary Investigations, 28 April 2004; subsequently confirmed by the Court of Milan, 28 October 2004. Back to section

16 Law 231, article 4. Back to section

17 Court of Cassation, Section IV, 18 January 2011, Case No. 24583; Court of Cassation, Section II, 27 September 2016, Case No. 52316; and, in a contrary and broader sense, Court of Cassation, Section III, 11 January 2018, Case No. 28725. Back to section

Studio Legale Pisano

Roberto Pisano robertopisano@pisanolaw.com

http://www.pisanolaw.com/

Netherlands: Export control developments in the Netherlands in 2026

Sebastiaan Bennink
Bennink Dunin-Wasowicz

Summary

IN SUMMARY

This article surveys recent developments in Dutch export controls, focusing on the evolving legal and regulatory landscape for dual-use and military items. It outlines the interplay between national and EU measures, including the introduction and subsequent partial repeal of national controls on advanced semiconductors, and examines the impact of recent court decisions halting F-35 exports to Israel. The article further discusses the ***Nexperia*** case, heightened scrutiny of exports to Israel and enhanced due diligence obligations for cyber-surveillance items, providing a comprehensive overview of current policy trends.

DISCUSSION POINTS

- In 2025, the Dutch government invoked the Goods Availability Act for the first time since 1952 to intervene in the ***Nexperia*** case, underscoring a willingness to use exceptional corporate law tools to address national security risks where standard export controls and FDI screening are insufficient.
- Recent amendments to Dutch general export and transit licences have resulted in Israel's exclusion from several authorisations, reflecting a significant shift towards stricter scrutiny and restrictive policy for sensitive exports to Israel.
- The Dutch Supreme Court and Court of Appeals decisions led to the suspension of F-35 component exports to Israel, prompting immediate changes to existing general licences and marking a high-profile judicial intervention in export policy.
- In 2024, Dutch authorities granted 99.5% of 1,500 military export licence applications, with more than half the total value linked to deliveries to Ukraine, demonstrating the Netherlands' active role in supporting European security priorities.

REFERENCES IN THIS ARTICLE

- The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies
- Treaty on the Functioning of the European Union (TFEU)
- The Council Common Position 2008/944/CFSP defining common rules governing control of exports of military technology and equipment (the EU Council Common Position)
- The Common Military List of the European Union (equipment covered by the Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment) (the EU Common Military List)
- Regulation (EU) 2021/821 setting up a Union regime for control of exports, brokering and technical assistance, transit and transfer of dual-use items (the Dual-Use Regulation)
- Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community (Directive 2009/43)
- Defence Readiness Omnibus

- The Strategic Goods Act
- The Strategic Services Act
- The Regulation on Additional Control Measures to the Dual-use Regulation
- The Dutch Advanced Semiconductor Manufacturing Equipment Decree
- the Central Import and Export Office

INTRODUCTION

The Netherlands has held a long reputation as a trading nation, with Dutch enterprises frequently emerging as leading actors in the global marketplace. Major sectors such as high-tech manufacturing (ASML, Philips), chemical production (DSM, AkzoNobel) and maritime logistics (Royal Vopak, Boskalis, Port of Rotterdam) exemplify the country's central role in international commerce. Facilitating Dutch business and supporting its integration into global value chains has consistently been a key priority for the Dutch government.

Yet, as global trade expands and geopolitical uncertainties intensify, export controls have become increasingly prominent as tools for safeguarding national security and advancing foreign policy objectives. Their significance is particularly acute for Dutch companies operating at the forefront of sensitive technology development and production. ASML's advanced semiconductor equipment and Philips's medical devices are prime examples. These sectors face growing scrutiny as governments seek to prevent the unauthorised transfer of dual-use and advanced technology items.

Dutch export control policy is therefore crafted to enhance international security while minimising unnecessary obstacles for Dutch industry and its global operations. The challenge for policymakers is to strike a careful balance: implementing robust export controls for security purposes, while ensuring that Dutch companies remain competitive against non-EU rivals who may face less stringent restrictions. In the sections that follow, we outline the legal framework governing Dutch export controls and examine recent developments that reflect the government's complex balancing act — navigating between security imperatives and the need to preserve the global standing of Dutch business.

EXPORT CONTROLS

Export controls are implemented to restrict both the physical and intangible transfer of sensitive goods, technology and software, with the primary aim of safeguarding national and international security interests. These controls also serve to prevent human rights abuses, combat terrorism and address the risks associated with the proliferation of weapons of mass destruction.

Export controls principally target two categories of items and technologies:

- military technologies and equipment — a reasonably self-explanatory category that includes, among others, war vessels, missiles, chemical agents and other equipment and technology specially designed or modified for military use; and
- dual-use items — goods, including software and technology, which can be used for both civil and military purposes, such as lasers, electronic components or nuclear technologies.

LEGAL FRAMEWORK

As a member state of the European Union, the Netherlands applies comprehensive export control regimes regulating the export, brokering, technical assistance, transit and transfer of both military items and dual-use items. Owing to the specific characteristics of these items and the allocation of competences between the European Union and its member states, the relevant legal frameworks differ.

Military Items

The export of military items from the Netherlands is primarily regulated by Dutch national law, specifically the Strategic Goods Act. This framework transposes EU Common Position 2008/944/CFSP (the EU Common Position), which sets out common rules among member states for controlling exports of military technology and equipment. Licensing and enforcement are carried out by the Central Import and Export Office (CDIU), which assesses applications against national policy criteria as well as the EU Common Position.

The regulation of exports of military items remains primarily within member states' jurisdiction: both the establishment of control measures and the licensing procedures are determined by national law. Nevertheless, the EU Common Position provides a non-binding but widely recognised framework, serving as a basis for harmonising national approaches in this area. The Dutch control list is a direct transposition of the EU Common Military List, which forms part of the EU Common Position.

This retained jurisdiction for member states is principally founded on article 346 of the Treaty on the Functioning of the European Union (TFEU), which provides that

> the provisions of the Treaties shall not preclude the application of the following rule: […] any Member State may take such measures as it considers necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms, munitions and war material.

Although export controls on military items remain a national competence, close coordination with the European Union and other member states is essential. The Netherlands participates in regular exchanges of information on licensing decisions, denials and sensitive transactions to ensure a harmonised approach — thereby preventing "licence shopping" and maintaining consistency with EU-wide embargoes. The Dutch government also communicates relevant national measures, embargoes and policy shifts to the European Council and other member states, supporting transparency and the effective application of common security and foreign policy objectives.

In addition, the intra-EU transfer of defence-related products is harmonised by EU Directive 2009/43/EC (Directive 2009/43), which simplifies the terms and conditions of trade in items listed in the EU Common Military List between member states.

Dual-use Items

Whereas article 346 TFEU enables member states to retain jurisdiction over military equipment, it does not apply to dual-use items. As such, dual-use items fall within the common commercial policy under article 207 TFEU and are therefore subject to EU competence. [1]

Export controls on dual-use items within the European Union are primarily governed by Regulation (EU) 2021/821 (the Dual-Use Regulation). This Regulation is directly applicable in the Netherlands and does not require further national implementing legislation for its core provisions.

The Dual-Use Regulation establishes a common Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. Specifically, it requires an authorisation for the export of dual-use items listed in Annex I to destinations outside the European Union. For intra-Union transfers, an authorisation is also required for items listed in Annex IV, which covers the most sensitive dual-use items, such as certain nuclear materials and technologies.

The EU dual-use control list in Annex I is based on commitments under major international non-proliferation and export control regimes, including the Wassenaar Arrangement, the Nuclear Suppliers Group (NSG), the Australia Group and the Missile Technology Control Regime (MTCR). The Regulation thereby ensures that EU controls are aligned with multilateral standards and obligations.

While the regulation of dual-use exports is a Union competence, the Dual-Use Regulation grants member states significant discretion. The CDIU retains broad latitude in shaping its licensing policies and decision-making processes, and member states are expressly empowered to adopt additional national control measures — including national control lists and catch-all controls — to address specific security or human rights concerns. The CDIU exercised this competence by adopting national controls on semiconductor manufacturing equipment.

The Netherlands' export control policy for strategic goods is founded on the following principles:

- the Netherlands does not contribute to the development and proliferation of weapons of mass destruction or their delivery systems;
- the Netherlands does not issue licences for the export of military or dual-use goods where they would contribute to human rights violations, internal repression, international aggression or instability;
- in deciding whether to issue a licence, security interests take precedence over economic interests;
- the Netherlands aims to reduce unnecessary administrative burdens on companies and is committed to ensuring an international level playing field for Dutch companies; and
- export controls take place prior to an export.

STRATEGIC SERVICES

In addition to the export controls applicable to military and dual-use items, the provision of certain services, such as technical assistance and brokering, is also subject to regulatory controls. In the Netherlands, alongside the requirements set out in the Dual-Use Regulation where applicable, the provision of these strategic services is regulated by the Strategic Services Act.

RECENT DEVELOPMENTS

Developments On National Control Measures

As noted above, EU export controls on dual-use items originate from multilateral regimes. Annex I of the Dual-Use Regulation, which lists items under export control, was for a long time a direct copy of the lists adopted under those regimes, particularly the Wassenaar Arrangement. However, decisions under the Wassenaar Arrangement require consensus, effectively granting any member a veto right. Russia made extensive use of this in recent years to block updates to the control lists, which in turn prevented Annex I of the Dual-Use Regulation from keeping pace with the latest developments in advanced technology industries, including the semiconductor sector.[2]

To address this, a number of member states established national control measures pursuant to article 9 of the Dual-Use Regulation. The Netherlands did so through two instruments:

- the Regulation on Additional Control Measures to the Dual-Use Regulation, adopted on 1 December 2024; and
- the Dutch Advanced Semiconductor Manufacturing Equipment, adopted on 23 June 2023, subsequently expanded on 7 September 2024 to cover deep ultraviolet lithography equipment and technology, and further extended on 1 April 2025 to a range of technologies used in other stages of the advanced semiconductor manufacturing process.

On 8 September 2025, however, the Commission adopted a delegated regulation to update Annex I of the Dual-Use Regulation independently of the amendment process under the Wassenaar Arrangement. This empowerment of the Commission is based on a literal reading of article 17(1)(a) of the Dual-Use Regulation, which provides:

> The list of dual-use items set out in Annex I shall be amended [by the Commission] in conformity with the relevant obligations and commitments, and any amendment thereof, that Member States and, where applicable, the Union have accepted as members of the international non-proliferation regimes and export control arrangements, or by ratification of relevant international treaties.

While this provision was initially interpreted as requiring a formal decision from those regimes, the Commission's position is that EU member states and the EU itself having voted in favour of an amendment is sufficient to enable the Commission to implement it in the Dual-Use Regulation.

On 24 November 2025, to reflect these changes and to address the partial overlap between Dutch national control measures and EU export controls as updated by the amended Annex I:

- the Regulation on Additional Control Measures to the Dual-Use Regulation was repealed; and
- the Dutch Advanced Semiconductor Manufacturing Equipment Decree was amended to list only items not covered by EU export controls.[3]

Developments On F-35 Export Licence

The Netherlands participates in the F-35 programme. Dutch industry produces components of the fighter jet, and the regional warehouse for F-35 parts is located at Woensdrecht. This gives rise to exports of military items from Dutch territory to various destinations, including Israel, which has purchased 50 F-35I aircraft — a specific variant of the F-35A incorporating Israeli equipment and weapons.

To facilitate the export of F-35 parts to purchasing countries, including Israel, general licence NL009 was established in 2016. However, following a legal challenge brought by three non-governmental organisations (NGOs), on 12 February 2024, the Court of Appeals in The Hague ordered the Dutch government to halt exports of F-35 fighter jet components to Israel owing to concerns about violations of international humanitarian law.[4] The Dutch Supreme Court upheld that decision, ordering the Dutch government to reassess the general licence; exports of F-35 components remained prohibited in the interim.

Following the Court of Appeals' ruling, the Minister amended the licence to exclude exports of F-35 parts to Israel. That licence, in its amended form, remains in force.

Further Developments Related To Exports To Israel

Following the Court of Appeals' decision, and in light of the prevailing security situation in Israel, the Palestinian territories and the broader region, the Netherlands also amended the Strategic Goods Decree to introduce further restrictions, particularly concerning exports of certain sensitive products to Israel. As set out in a letter to the House of Representatives of 7 April 2025 from Minister for Foreign Trade and Development Reinette Klever and Minister of Foreign Affairs Caspar Veldkamp, the amendments mark a shift towards significantly stricter scrutiny of all exports and transits through the Netherlands of military and dual-use goods.[5]

The following amendments took effect on 8 April 2025:

- National General Export Licence NL002, which previously permitted — subject to certain conditions — the export to all destinations except 11 countries of items covered by 39 entries of Annex I of the Dual-Use Regulation (categories 1, 2, 3 and 4), was amended to add Israel to the list of excluded destinations.[6]
- National General Export Licence NL010, which permits the export of certain information security items to all destinations except those on an extensive exclusion list, was amended to include Israel in that list. Israel therefore no longer benefits from that authorisation as of 8 April 2025.[7]
- National General Transit Licence NL007, which permits the transit of certain items listed in the EU Common Military List originating from EU or NATO countries, and their close partners, namely Australia, Japan, New Zealand and Switzerland, destined for certain countries, was amended to exclude Israel as of 8 April 2025.[8]

As a result, transactions previously covered by these general licences now require either a global or individual licence. While they remain permissible, these amendments, together with the Ministers' letter, signal a more restrictive licensing policy for such transactions going forward.

ONGOING WORK ON THE RECAST OF THE DIRECTIVE ON INTRA-EU TRANSFERS OF DEFENCE-RELATED PRODUCTS

Seventeen years after the adoption of Directive 2009/43, the European Union is undertaking a recast of the instrument.

On 17 June 2025, as part of the Defence Readiness Omnibus, a legislative proposal was published with the objective of simplifying and harmonising regulatory frameworks to foster a more favourable environment for defence industries. The proposal aims to facilitate the operation, innovation and production of capabilities necessary to strengthen European security and defence readiness, in the context of renewed large-scale conflict in Europe.

The legislative proposal to amend Directive 2009/43 notably provides for:

- an extension of cases in which member states may exempt transfers of defence-related products from prior authorisation, including for EU-funded defence projects, structured cross-border industrial partnerships, transfers to EU institutions and the European Defence Agency and emergency situations arising from crises;
- an expansion of general transfer licences to cover transfers by certified entities, not only certified European defence undertakings; and
- the introduction of general transfer licences for EU defence industrial projects (such as the European Defence Fund), covering all necessary defence-related products and transfers required for project implementation.[9]

On 22 December 2025, the relevant committees of the European Parliament proposed to go further by recommending the following amendments:

- Member states should exempt transfers of defence-related products from prior authorisation where:
    - the supplier or recipient is a governmental body, armed forces or national security authority;
    - the transfer occurs under a European strategic cross-border partnership; or
    - the transfer is required urgently due to a crisis or following activation of the European Union's mutual assistance clause under article 42(7) TFEU.
- Member states should publish general transfer licences for transfers necessary to European strategic cross-border partnerships.[10]

By letter addressed to Maroš Šefčovič, European Commissioner for Trade and Economic Security, the Dutch Senate — in particular members of the Volt Group in the Committee on Foreign Affairs, Defence and Development Aid — expressed support for the Commission's efforts in this regard.

The Dutch Senate took the view that the directive falls within the scope of internal market legislation and may therefore be adopted by a qualified majority. It did, however, express concern about the possibility of member states invoking article 346 TFEU, and queried why it had not been considered necessary to amend the Dual-Use Regulation in parallel.[11]

The directive recast, together with the broader Defence Readiness Omnibus, is currently subject to interinstitutional negotiations between the co-legislators.

THE NEXPERIA INVESTIGATION

The year 2025 marked a turning point in Dutch and European export control policy. The ***Nexperia*** case highlighted the evolving legal landscape for safeguarding national security

in the semiconductor sector and illustrated how foreign direct investment (FDI) controls are increasingly being used alongside, and as a complement to, traditional export controls.

Nexperia BV, a major Dutch chipmaker acquired by China's Wingtech in 2019, became a focal point for concerns over technology transfer and compliance with international sanctions. These concerns, initially rooted in the absence of Dutch FDI screening at the time of acquisition, intensified as geopolitical tensions rose and the risk of circumvention of EU and US export controls became more apparent.

By 2023, Dutch and international media reported that Nexperia chips had been found in Russian military equipment, raising questions about the effectiveness of existing export control mechanisms under Regulation 833/2014 and the Dual-Use Regulation. The situation escalated further in 2024 and 2025, when the US Bureau of Industry and Security (BIS) added Wingtech to the US Entity List, triggering the "50% rule" and the Affiliates Rule. As a majority-owned subsidiary, Nexperia was accordingly at risk of becoming subject to US export controls, which would severely restrict its access to critical technology and international markets.

In response, and given that traditional FDI screening and direct export control measures were unavailable or insufficient, the Dutch government took unprecedented action. On 30 September 2025, the Minister of Economic Affairs invoked the Goods Availability Act for the first time since its enactment in 1952. This emergency measure was justified by two principal concerns: the conduct of Nexperia's CEO and indirect shareholder, Zhang Xuezheng, and the risk that Nexperia's semiconductor products could become unavailable to the Netherlands and the wider European market. The government described the intervention as "highly exceptional" and aimed at ensuring the continued availability of critical goods and safeguarding national interests.

The legal process moved swiftly. On 1 October 2025, three Nexperia board members filed an emergency petition with the Enterprise Chamber of the Amsterdam Court of Appeal, seeking a corporate investigation and provisional measures. Following an ex parte hearing, the Chamber provisionally suspended the CEO and transferred control of Nexperia's shares from Wingtech to an independent administrator. This effectively severed Nexperia's ties with its Chinese parent and, crucially, led the US BIS to exempt Nexperia from the 50% rule as of 21 October 2025. The Chamber's decision was later upheld following a full hearing in February 2026, with an order for a thorough investigation into Nexperia's policies and operations.

The ***Nexperia*** case is significant for several reasons. First, it demonstrates the willingness of Dutch authorities to deploy emergency corporate law measures to achieve national security objectives when traditional export control and FDI tools are unavailable or insufficient. This represents a novel use of domestic law as a de facto export control mechanism, enabling the government to rapidly reassert control over a strategic company and mitigate the risk of circumvention or diversion of sensitive technology. Second, it underscores the growing interplay between national corporate governance and international sanctions regimes, including those under Regulation 833/2014, which prohibit the export of dual-use goods and technology to Russia and other designated entities.

For companies and practitioners, the ***Nexperia*** case signals that compliance risks in strategic sectors now extend beyond formal EU sanctions and dual-use controls to encompass the possibility of emergency interventions under national law. It also underscores the importance of robust internal governance and risk management, as board members and

other stakeholders may invoke national measures to protect corporate and national interests under geopolitical pressure.

As the divide between the West and China deepens, the ***Nexperia*** case serves as a warning to foreign investors in sensitive sectors: the Dutch government is prepared to deploy innovative legal mechanisms, including corporate law, to address export control and national security risks.

BROCHURE ON EXPORTS OF CYBER-SURVEILLANCE ITEMS

With the 2021 recast of the Dual-Use Regulation, specific provisions addressing cyber-surveillance items were introduced, reflecting growing concerns about their potential misuse in human rights abuses.

Cyber-surveillance items are defined by article 2(20) of the Dual-Use Regulation as "dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems".

In addition to the existing export controls applicable to cyber-surveillance items listed in Annex I, a specific catch-all clause was introduced by article 5 of the Dual-Use Regulation, covering situations where such items may be used in connection with internal repression or the commission of serious violations of human rights and international humanitarian law.

Following similar guidance published by the Commission in 2024, the CDIU published a brochure providing an accessible and user-friendly explanation of the notification requirement under article 5(2) of the Dual-Use Regulation.

DUTCH EXPORT CONTROL REPORT

In July 2025, Dutch authorities published their export control report for 2024.

Military Items

In 2024, the Netherlands received 1,500 licence applications for the export of military goods, a decrease of 184 applications compared to 2023. Of these, 1,491 licences were granted, reflecting an approval rate of 99.5%. The majority of approved licences — 979 out of 1,491 — were for NATO and EU member states, or equivalent countries (the "NATO+ countries", comprising Australia, Japan, New Zealand and Switzerland).

The total value of licences granted for military items in 2024 was approximately €1.87 billion, up from €1.78 billion in 2023 and €928 million in 2022. This growth is primarily attributable to substantial military deliveries to Ukraine, which alone accounted for €1.09 billion, representing more than 58% of the total value of approved licences.

In terms of regional distribution, other European countries (principally Ukraine) received the largest share, followed by EU/NATO+ states and Germany. By product category, aircraft and parts accounted for approximately one-third of the total value, and vehicles and parts for approximately one quarter.

Only nine applications were refused in 2024 (including export, transit and preliminary sondage applications), a slight increase from five refusals in 2023. Refusals represented less than 1% of all applications. Reasons for refusal were primarily related to risks identified under EU Common Position criteria, such as concerns over end-use or the risk of human rights violations.

Dual-use Items

For dual-use items, 855 licence applications were processed in 2024, a decrease from 898 in 2023. Despite the reduction in application numbers, the total value of licences granted rose sharply, from nearly €21 billion in 2023 to €34 billion in 2024.

Of the licences granted:

- 611 individual licences were issued, with a total value of €352 million;
- 186 global licences were issued, with a total value of €32.8 billion;
- 53 intra-EU licences were issued, with a total value of €1.1 billion; and
- 5 catch-all licences were issued, with a total value of €7 million.

Thirteen applications were refused in 2024, compared to 14 in 2023, with a total refused value of €14 million.

Recent Dutch export control developments demonstrate a clear shift towards stricter and more agile measures, including the use of exceptional national tools such as the Goods Availability Act and heightened scrutiny of exports to sensitive destinations like Israel. The interplay between national and EU-level regulation, as well as the convergence of export controls, FDI screening and corporate governance, highlights the increasing complexity and strategic importance of compliance in this area. Companies must now anticipate not only formal licensing requirements but also the possibility of emergency interventions and evolving policy priorities in response to geopolitical risks.

The author would like to thank Lucas Laurent and Sanne Spelbos for their contributions to this article.

Endnotes

1 ECJ, 8 April 2008, ***Commission against Italy*** (C-337/05). ^ Back to section

2 Sebastian Bennink et al, Europe, 58 ABA/ILS YIR (forthcoming June 2024). CSIS "Wa, Wa, Wassenaar!" retrieved on 26 March 2024, https://www.csis.org/analysis/wa-wa-wassenaar. ^ Back to section

3 Regeling van de Staatssecretaris van Buitenlandse Zaken van 20 november 2025, No. BZ2520952, houdende intrekking van de Regeling aanvullende controlemaatregelen op de Verordening producten voor tweeërlei gebruik en de wijziging van de Regeling geavanceerde productieapparatuur voor halfgeleiders (https://zoek.officielebekendmakingen.nl/stcrt-2025-38653.html). ^ Back to section

4 Gerechtshof Den Haag, 12 February 2024, (ECLI:NL:GHDHA:2024:191) https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHDHA:2024:191. ^ Back to section

5 Beslisnota bij Kamerbrief Exportcontrole – intrekking algemene vergunning NL002 en aanpassing algemene vergunningen NL007 NL010 door Israël uit te sluiten als land van eindbestemming. ^ Back to section

6 Nationale Algemene Uitvoervergunning NL 002. ^ Back to section

7 Nationale Algemene Uitvoervergunning NL 010 (items voor informatiebeveiliging). ^ Back to section

8 Regeling algemene doorvoervergunning NL007. ^ Back to section

9 EU Commission, Proposal for a Directive of the European Parliament and Of The Council amending Directives 2009/43/EC and 2009/81/EC, as regards the simplification of intraEU transfers of defence-related products and the simplification of security and defence Procurement (2025/0177 (COD)) https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2025/0823/COM_COM(2025)0823_EN.pdf. ^ Back to section

10 EU Parliament, REPORT on the proposal for a Directive of the European Parliament and of the Council amending Directives 2009/43/EC and 2009/81/EC, as regards the simplification of intra-EU transfers of defence-related products and the simplification of security and defence procurement (COM(2025)0823) https://www.europarl. europa.eu/doceo/document/A-10-2025-0275_EN.html. ^ Back to section

11 Eerste Kamer der Staten-Generaal, Questions regarding the Omnibus Package proposals for Defence Readiness 2030 in the context of the political Dialogue, 3 October 2025 (178288). ^ Back to section

Sebastiaan Bennink sb@benninkdunin.com

https://www.benninkdunin.com/

Read more from this firm on GIR

Saudi Arabia: Fresh transactions framework opens the door to foreign investment

Fahad AlDehais AlMalki, **Hamad AlBazai** and **Talal AlOtaibi**
Suhail Partners LLP

Summary

IN SUMMARY

Saudi Arabia's new Civil Transactions Law (CTL) of 2023 is a game changer offering a clear framework for commercial and civil transactions. The CTL incorporates the General Rules (GR), principles derived from principles and doctrines of Islamic law (sharia), to address situations not covered by specific legal provisions. Understanding these GR is crucial for legal professionals and anyone involved in Saudi business or legal matters.

DISCUSSION POINTS

- Introduction of the CTL
- Explanation of GR and their sources and importance
- Real-life examples demonstrating GR application
- Conclusion highlighting the value of GR for legal professionals

REFERENCED IN THIS ARTICLE

- Case No. 7103/3/1436 AH, The collection of commercial rulings and principles issued by the Court of Grievances, published in 1436 AH
- Case No. 773/3/1432 AH, The collection of commercial rulings and principles issued by the Court of Grievances, published in 1436 AH
- Case No. 3196/2/1433, The collection of commercial rulings and principles issued by the Court of Grievances, published in 1438 AH

INTRODUCTION

Since the launch of Saudi Vision 2030 on 25 April 2016,[1] the legislative and legal landscape in Saudi Arabia has undergone significant and visible developments. These include the development of legal legislation, the review and development of judicial systems and the digital transformation of the judicial sector through the launch of the Ministry of Justice's online platform (Najiz – "Accomplished"), which relieved stakeholders from the need to visit judicial locations and has successfully digitised over 200 judicial and legal services.[2]

In this context, it is worth highlighting that some legal aspects have been identified as barriers to some foreign investors, so Saudi Arabia's authorities revamped key laws such as the Investment Law, Companies Law and Bankruptcy Law for clarity and ease of use as a means to avoid this issue and overcome the difficulties facing foreign investment, which will subsequently contribute to improving the business environment and boosting foreign investments.

Focusing on the legislative aspect, the Civil Transactions Law (CTL), issued by Royal Decree No. M/191 in November 2023, is the latest law to be issued in Saudi Arabia. This comprehensive legislation serves as the primary reference for all commercial and civil transactions as well as disputes not covered by other existing laws and regulations. The CTL represents a landmark advancement in the specialised legal framework. It leverages the latest developments in international legal thoughts and incorporates best practices from

global judiciaries, all while remaining firmly grounded in the principles and doctrines of Islamic law (sharia).[3]

Prior to the CTL, the legal system, in some respects, heavily relied on the interpretations of the principles and doctrines of Islamic law (sharia) by different scholars from different schools of thought and approaches. This approach presented significant challenges for judges, parties to disputes and their lawyers. The enactment of the CTL has revolutionised the legal system by codifying the principles and doctrines of Islamic law (sharia) into clear, written articles. This codification provides judges with a readily accessible reference, facilitates legal representation for lawyers and enhances transparency for both citizens and foreign investors. Among the aspects that were subject to codification in the CTL were the GR, which play an important role in the field of litigation.

WHEN IS IT APPROPRIATE TO RELY ON GENERAL PRINCIPLES IN THE CTL?

Article 1 of the CTL outlines a clear structure for addressing legal disputes:

> 1. The provisions of this Law shall apply to all matters addressed thereby in letter and spirit. In cases where none of the provisions of this Law can be applied, the General Rules provided for in the Concluding Provisions shall apply, and in the absence of a relevant general rule, the provisions derived from Sharia that are most consistent with this Law shall apply 2. The application of the provisions of this Law shall not prejudice any specific legal provision.

With no prejudice against any specific legal provisions mentioned in other laws, the CTL prioritises its own provisions to maintain and ensure consistency. If no explicit provisions directly address the issue at hand, the CTL directs courts to follow the GR. In the absence of both explicit provisions and the GR, the CTL authorises courts to consider principles drawn from Islamic law (sharia) that are most in line with the spirit of the CTL.

The Concluding Provisions (Chapter No. 1 of the CTL) list 41 of these GR. However, it is crucial to bear in mind that these GR apply only if they do not contradict the specific provisions of the CTL. The nature, conditions and exceptions of each GR should also be considered. In addition to that, it is important to clarify that mentioning only 41 GR in the CTL does not invalidate other general rules. After all, general rules are ultimately derived from religious texts and Islamic principles. So, if a rule aligns with the spirit of the CTL, it can still be relied upon, even if it is not explicitly listed.

Definition Of The GR

The concept and specific applications of the GR warrant further exploration. This article will delve deeper into the origin and meaning of these GR, analyse a selection of them and explore how they have been applied by Saudi court cases.

The GR outlined in the CTL are rooted in the established body of principles and doctrines of Islamic law (sharia). Consequently, the established definition of principles and doctrines of Islamic law (sharia) applies comprehensively to the GR as incorporated within the CTL framework. In his book, *The Concise Elucidation of General Jurisprudential Principles*-, Muhammad Sidqi Al-Borno defines the Islamic jurisprudential rules as "general principles and fundamentals formulated in concise texts that include general legislative rulings on the incidents that fall under their subject matter".[4]

Sources Of The GR

Centuries of scholarly effort by Islamic scholars have resulted in the current form of the GR. These scholars meticulously extracted, formulated and categorised these rules from religious texts. The three main sources of the GR are as follows:

- The Holy Qur'an: the Holy Quran stands as the cornerstone for Islamic scholars in formulating the GR. By examining its core principles, scholars were able to extract and establish these general rules. This process not only provided the foundation for the GR but also offered insight into the underlying objectives and purposes of Islamic legal rulings. For instance, the verse "except it be a trade amongst you, by mutual consent" exemplifies this approach. This verse establishes the principle of mutual consent in contracts and transactions, emphasising the importance of individual will. This very principle later evolved into a rule within the CTL, specifically article 15, which states: "Consent is attained when the mutual intent of two or more parties who have the legal capacity to conclude contracts is expressed by any means indicating such intent."
- Prophetic tradition (Sunna): the Prophet Muhammad (PBUH) played a crucial role in shaping the GR. His concise yet profound sayings, characterised by their brevity and comprehensiveness, served as important guiding principles. A prime example is his saying "Muslims are bound by their conditions", which underscores the importance of honouring commitments and fulfilling obligations. This very principle evolved into the established rule that "contracts and conditions shall be presumed valid and binding", which was specifically chosen for inclusion within the CTL, highlighting its significance in Islamic legal principles.
- The principles and doctrines of Islamic law (sharia): Islamic scholars have dedicated themselves to understanding the principles and doctrines of sharia. By doing so, scholars were able to derive comprehensive rules from them. For example, the rule that "matters shall be determined according to intentions" was derived from the deep analysis of PBUH's sayings, such as: "Actions are only by intentions."[5]

Importance Of The GR

The importance of the GR lies in their role as a foundational framework for understanding Islamic law (sharia) and boundaries of conflicted interpretation. They provide stability through a systematic methodology for interpreting legal texts, deriving legal rulings and resolving new issues that may arise in accordance with the principles of Islamic jurisprudence. Al-Qarafi, a prominent Islamic scholar in the thirteenth century, in his book ***al-Furuq*** (***Distinctions***) emphasises the importance of the GR in Islamic jurisprudence. He argues that mastering them allows the scholar to make sound rulings, achieve a deeper understanding of Islamic law and attain a higher level of scholarly distinction:

> These rules are important in Islamic jurisprudence, of great benefit, and the more one grasps them, the greater the status of the jurist becomes, and he becomes honored, and the beauty of jurisprudence becomes apparent and known. Whoever deduces rulings based on specific analogies without the general rules, his rulings will contradict and differ, and he will need to memorize the endless particulars. But whoever masters jurisprudence through its rules will be able to dispense with memorizing most of the particulars, since they are

included in the general rules, and what is contradictory for others will become unified for him, and he will understand the coherence of the rulings.[6]

Benefits Of The GR

The study of the GR has many benefits. However, we will focus on three benefits that relate to the article topic:

- The GR provide non-specialist legislators with the opportunity to understand the spirit, content, bases, and principles and doctrines of Islamic law (sharia). They also assist them in deriving rulings from them and considering rights and obligations within them.[7]
- General rules provide a framework for judges to analyse legal issues and arrive at well-reasoned decisions, even in situations where a specific legal text is absent.[8]
- The GR provide stability in civil and commercial transactions, having established the boundaries of interpreting the principles and doctrines of Islamic law (sharia), and contain conflicted interactions into a governing law.

Types And Ranks Of The GR

Major fundamental rules serve as keys to understanding the principles and doctrines of Islamic law (sharia), as they are used to interpret religious texts and derive new rulings through analogy. These rules are listed below:

- The Rule of Intention: "Matters shall be determined according to intentions."
- The Rule of Certainty: "Certainty may not be dispelled by doubt."
- The Rule of Harm: "Harm shall be removed."
- The Rule of Hardship: "Hardship shall beget facility."
- The Rule of Custom: "Custom shall have legal effect."
- The Rule of Presumed Meaning in Legal Interpretation: "Words shall be presumed to have meaning and shall not be disregarded."
- General principles are rules that are universally accepted within Islamic scholars across different schools of thought (*madh'hab*) but they are considered to be less extensive in their scope and application compared with the major fundamental rules mentioned above. An example of these rules is "The person warranting a thing shall retain its yields."
- Thought-specific rules are rules that are unique to a particular school of thought (-*madh'hab*), such as "He who rushes a thing before its time is punished by being deprived of it."[9]

Examples Of The Application Of The GR

As stated previously, the recent issuance of the CLT complicates the search for court decisions that relied on the GR. The subsequent instances of judicial decisions serve to exemplify the way in which these GR have been implemented.

"FREEDOM FROM LIABILITY SHALL BE PRESUMED"

Meaning Of The Rule

The rule was derived from the major fundamental rule: "Certainty may not be dispelled by doubt." It holds that the default state for individuals is freedom from any obligations, liabilities or burdens until proven otherwise by valid legal evidence. In essence, it asserts that people are born with a clean slate, and any claims against them require proof based on established legal principles.

Legal Applications Of The Rule

In Case No. 3196/2/1433, the plaintiff claimed the return of shipping containers and payment of late fees. The defendant denies any dealings with the plaintiff and receiving the containers. Because the plaintiff did not present any evidence to prove the defendant's receipt of the containers, the court presumed that the defendant was innocent of any dealings with the plaintiff. On that basis, the court dismissed the case, building its decision upon the solid ground of certainty, not the shifting sands of doubt.[10]

"AN ATTACHMENT SHALL FOLLOW THE PRINCIPAL"

Meaning Of The Rule

Anything that is subordinate to something else, whether de facto or de jure, is considered a part of its principal. Therefore, the rulings of the principal apply to the subordinate and cannot be separated.

Legal Applications Of The Rule

In Case No. 7103/3/1436 AH, the plaintiff bought goods consisting of electrical appliances and contracted with the defendant to ship the goods to Riyadh city. The goods did not reach the plaintiff. The plaintiff claimed that the defendant caused the loss of the goods due to its negligence. The defendant argued that the worker who was supposed to deliver the goods caused the loss of the goods. The defendant's attorney submitted a memorandum stating that there was an agreement between the parties to insure the shipment for an amount of 100,000 Saudi riyals. The court rejected the defendant's defence of the existence of an agreement on a maximum compensation limit, reasoning that that should have been accepted in cases where there was no negligence from its side, ordering the defendant to pay the value of the lost goods.[11]

"THE ONE WHO IS NEGLIGENT IS MORE DESERVING OF COMPENSATION"

Meaning Of The Rule

This rule applies to anyone who has a responsibility, such as trustees, guardians, agents and tenants. The meaning is simply that whoever exceeds the limits of their responsibility or neglects it will bear the consequences. However, this does not mean that the person responsible for something is obligated to protect it no matter what happens; it means that they are prohibited from acting wrongly or neglecting their duties. If a mistake or negligence occurs, the person responsible is considered the "guarantor", meaning that they bear the consequences. The rule focuses on determining what constitutes exceeding one's authority, as not every mistake is a betrayal of trust.

Legal Applications Of The Rule

In Case No. 773/3/1432 AH, the plaintiff filed her claim, demanding that the defendant be held liable for the rental fee of the tankers for storing petroleum products under the contract

authenticated by mutual seal and signatures. The defendant acknowledged the validity of the contract, arguing that he had not benefited from the leased tank since receiving it from the Customs Administration, as it was seized due to his possession of prohibited oils. The plaintiff responded to the defendant's argument that he did not benefit from the tankers due to their seizure by the Customs Administration by asserting that the reason for the seizure was the defendant's possession of prohibited oils. After analysing the facts of the case, the court concluded that the defendant took possession of the tankers under a valid contract but failed to utilise them for a cause that happened by his side, and since the contract is binding and requires good faith execution, the defendant is responsible for this missed benefit. There were no exceptional circumstances justifying contract termination. On that ground, the court ordered the defendant to pay the agreed rental fee for the tankers.[12]

CONCLUSION

The CTL represents a significant step forward in Saudi Arabia's legal landscape. It introduces a comprehensive framework for commercial and civil transactions, addressing disputes not covered by other existing laws. A key feature of the CTL is its incorporation of the GR, which are principles derived from principles and doctrines of Islamic law (sharia).

The GR play a crucial role in filling gaps in the legal code and providing guidance to judges in reaching sound decisions. These rules encompass various aspects, including intention, certainty, harm, hardship, custom and interpretation. Understanding the origin, meaning and application of these rules is essential for legal professionals and anyone involved in commercial or civil matters in Saudi Arabia.

This article has explored the concept of the GR, their sources and their importance within the Saudi legal system. It has also provided examples of how these rules are applied in real-world cases. By delving deeper into the GR, legal professionals can gain a more nuanced understanding of Saudi law and effectively navigate the complexities of commercial and civil transactions in Saudi Arabia.

Endnotes

1 For more information, see https://www.vision2030.gov.sa/en/progress/environment-nature/. ^ Back to section

2 Najiz platform website: https://najiz.sa/. ^ Back to section

3 The Civil Transactions Law (CTL), issued by Royal Decree No. M/191 in November 2023, https://laws.moj.gov.sa/legislations-regulations?pageNumber=1&term=civil &sortingBy=7&type=1&pageSize=16. ^ Back to section

4 The Concise Elucidation of General Jurisprudential Principles, Muhammad Sidqi Al-Borno, available at https://shamela.ws/book/8379/6#p1. ^ Back to section

5 The Rules of Jurisprudence and Their Applications in the Four Schools of Thought, Muhammad Mustafa al-Zuhayli, available at https://shamela.ws/book/21786/25#p1. ^ Back to section

6 Available at https://shamela.ws/book/2215/2#p1. ^ Back to section

7 The Rules of Jurisprudence and Their Applications in the Four Schools of Thought, Muhammad Mustafa al-Zuhayli, available at https://shamela.ws/book/21786/25#p1. ^ Back to section

8 The Role of Islamic Jurisprudence in Judicial Reasoning, Abdul Aziz Al-Hamad, available at https://qadha.org.sa. ^ Back to section

9 The Rules of Jurisprudence and Their Applications in the Four Schools of Thought, Muhammad Mustafa al-Zuhayli, available at https://shamela.ws/book/21786/25#p1. See also The Concise Elucidation of General Jurisprudential Principles, Muhammad Sidqi Al-Borno, available at https://shamela.ws/book/8379/16#p1. ^ Back to section

10 The collection of commercial rulings and principles issued by the Court of Grievances, published in 1436 AH, available at https://www.bog.gov.sa/ScientificContent/JudicialBlogs/1436/Pages/default.aspx. ^ Back to section

11 The collection of commercial rulings and principles issued by the Court of Grievances, published in 1436 AH, is available at https://www.bog.gov.sa/ScientificContent/JudicialBlogs/1436/Pages/default.aspx. ^ Back to section

12 Available at https://www.bog.gov.sa/ScientificContent/JudicialBlogs/1436/Pages/default.aspx. ^ Back to section

SUHAILPARTNERS
شركاء سهيل محامون ومستشارون
INSIGHT DEDICATION IMPACT RESOLUTION

Fahad AlDehais AlMalki fahadaldehais@suhailpartners.sa
Hamad AlBazai hamadalbazai@suhailpartners.sa
Talal AlOtaibi talalalotaibi@suhailpartners.sa

https://suhailpartners.sa/

Switzerland: seizure and forfeiture of Russian assets as legal basis called into question

Pascal de Preux
Resolution Legal Partners

Summary

IN SUMMARY

Following the war initiated by Russia against Ukraine in 2022, the Swiss government decided to adopt the EU sanctions against Russia to strengthen their impact. This article explores the development in Switzerland of the freezing and forfeiture of assets and economic resources of sanctioned persons, companies and organisations. The legal basis of the forfeiture is in question, especially since the European Union adopted several Directives on this issue.

DISCUSSION POINTS

- Freezing of assets and economic resources amounts to 7.4 billion Swiss francs, plus 14 properties, sports and luxury cars, works of art, furniture and instruments
- Such freezing does not remove property rights from the sanctioned persons, companies and organisations
- The Embargo Act is not a sufficient legal basis for forfeiting assets
- The Swiss government considers that Swiss law does not have a legal basis to forfeit Russian assets to compensate Ukraine
- Switzerland is not legally bound by the EU Directive on violation of EU restrictive measures
- The forfeiture of assets will raise different legal issues, and the owner of these assets will have the right to have their case heard by a judicial authority

REFERENCED IN THIS ARTICLE

- Embargo Act of 2002
- Ordinance on measures in relation to the situation in Ukraine
- State Secretariat for Economic Affairs
- Swiss Criminal Code
- Decision of the Swiss Supreme Court regarding Abacha
- Swiss Parliament
- Directive (EU) 2024/1260 on asset recovery and confiscation
- Directive (EU) 2024/1226 on the definition of criminal offences and penalties for violation of EU restrictive measures

BRIEF INTRODUCTION

The notions of asset freezing and asset forfeiture are often confusing. However, it is essential to understand these two concepts, which have completely different legal consequences. Freezing is a provisory measure, preventing the owner of the assets from accessing, transferring or converting them. Freezing also covers the revenues of assets. Forfeiture or confiscation implies a change of ownership. The right of the person or company to the assets is lost without any compensation.

FREEZING OF ASSETS AND ECONOMIC RESOURCES

According to the Federal Act on the Implementation of International sanctions (the Embargo Act of 2002),[1] the Swiss Confederation may enact compulsory measures to implement sanctions that have been ordered by the United Nations, by the Organization for Security and Co-operation in Europe or by Switzerland's most significant trading partners, and that serve to secure compliance with international law and, in particular, the respect of human rights. Article 2 of the Embargo Act gives the Swiss government the authority to enact compulsory measures in the form of ordinances.

Following the war in Ukraine, the Swiss government decided on 28 February 2022 to adopt the European Union's sanctions against Russia to strengthen their impact. This decision concerns only the restrictive measures per se but not the EU Directive on restrictive measures and the EU Directive on asset recovery. The ordinance of 2 March 2022 on measures in relation to the situation in Ukraine contains the Swiss measures and is legally binding. This text includes several types of measures, in particular the freezing of assets and economic resources, a reporting obligation concerning the freezing of assets and economic resources, and prohibitions concerning securities and money market instruments.

Assets and economic resources include values of any kind, whether tangible or intangible, movable or immovable. For example, real estate, luxury goods and works of art are also considered economic resources and are therefore subject to freezing. Valuables stored in free ports are also subject to this regime.[2]

Article 15, paragraph 1 of the ordinance provides, in particular, that assets and economic resources can be frozen if owned or controlled, directly or indirectly by:

1. natural persons, companies and organisations listed in appendix 8;
2. natural persons, companies and organisations acting on behalf of or at the direction of natural persons, companies and organisations referred to in point 1; or
3. companies and organisations owned or controlled by natural persons, companies and organisations referred to in point 1 or point 2.

Switzerland is free to decide the extent to which it adopts EU sanctions and does not do so automatically. As a member of the United Nations, Switzerland is legally bound to apply the sanctions decided by the United Nations Security Council. On the other hand, the Swiss government decides on a case-by-case basis whether to adopt (in full or in part) the sanctions decided by the European Union. It weighs up the interests involved, taking into account legal considerations, foreign policy and foreign economic policy criteria.[3]

Article 16 of the ordinance contains a mandatory declaration concerning the freezing of assets and economic resources. Persons and institutions that hold or manage assets or have knowledge of economic resources that are deemed to fall within the scope of the assets to be frozen, provided for in article 15, paragraph 1 of the ordinance, must report this to the State Secretariat for Economic Affairs without delay. Persons and institutions holding or managing assets or with knowledge of economic resources belonging to or controlled by natural persons, companies and organisations listed in appendix 8 must report to the State Secretariat for Economic Affairs without delay all transactions carried out in the two weeks preceding the inclusion of such persons, companies and organisations listed in appendix 8.

As at 31 March 2025, the financial assets frozen in Switzerland amounted to 7.4 billion Swiss francs, plus 14 real estate assets in Switzerland. The total amount of reserves and assets of the Central Bank of Russia held in Switzerland is approximately 7.4 billion Swiss francs.[4] The website of the State Secretariat for Economic Affairs has a page that allows persons, companies and organisations subject to sanctions to be searched for.[5] However, appendix 8 (which contains the list of persons, companies and organisations subject to sanctions) is not published in the official or systemic collection of federal laws.

Unlike forfeiture, the freezing of assets and economic resources does not remove property rights from the sanctioned person, company or organisation (rule of law). The real estate, automobiles or other similar assets of a person or company on a sanctions list are also frozen, but they are not taken away. In practice, this means a ban on trading them. For example, a sanctioned person may continue to live in a house they own but is not allowed to sell or rent it.[6]

FORFEITURE OF ASSETS UNDER THE EMBARGO ACT AND ITS ORDINANCE

As far as international sanctions are concerned, if the legal basis for freezing is quite clear, the question of the forfeiture of Russian assets is not, as far as Swiss law is concerned.

The situation is different in the European Union. On 4 April 2024, the European Union adopted Directive 2024/1260 on asset recovery and confiscation and Directive 2024/1226 on the definition of criminal offences and penalties for violation of EU restrictive measures. These two texts are linked as they specify that the forfeiture of assets derived from the violation of EU sanctions is carried out in accordance with the provisions of the asset recovery Directive.

Article 10, paragraph 2 states that:

> Member States shall take the necessary measures to enable the freezing and confiscation of funds or economic resources subject to Union restrictive measures in respect of which the designated natural person, or the representative of a designated entity or body, commits, or participates in, an offence covered by Article 3(1), point (h)(i) or (ii). Member States shall take those necessary measures in accordance with Directive 2014/42/EU.

These Directives have been presented in the context of Russia's military aggression against Ukraine as a means of combating the circumvention of restrictive measures and facilitating the forfeiture of Russian assets. The purpose of the Directives is to create a minimum, uniform legal standard within the European Union that member states cannot evade, but that they can nevertheless surpass.

In Switzerland, the Embargo Act has a provision regarding forfeiture of property and assets. Article 13, paragraph 1 of the Embargo Act states that property and assets that are subject to compulsory measures shall be forfeited irrespective of the criminal liability of any particular person if their continued lawful use is not guaranteed. According to the State Secretariat for Economic Affairs, this provision does not provide a sufficient legal basis for confiscating the assets of sanctioned persons, companies and organisations. As long as assets are seized by sanctions, they are used in accordance with the law. A criminal offence is therefore missing. For this reason, the conditions for forfeiture within the meaning of article 13 of the Embargo Act are not met in the case of frozen assets. In its report on the EU Directive on the definition of criminal offences and penalties for the violation of EU restrictive measures and

the difference with Swiss law dated 27 November 2024, the Swiss government mentioned that there is no legal basis for forfeiture in the case of restrictive measures, as the assets or economic resources have not been obtained through an offence and are therefore, until proven otherwise, not considered illicit.[7]

The forfeiture of assets is not foreseen in the ordinance on measures in relation to the situation in Ukraine. Therefore, currently, there is no legal basis for the forfeiture of Russian assets under Swiss sanctions law.

Three years ago, forfeiture of assets of a sanctioned person was not even a question for the Swiss government.

On 11 May 2022, a member of the Swiss Parliament called for the creation of a legal basis for using frozen assets to rebuild Ukraine. The aim was that the frozen assets of oligarchs close to President Putin could be used for international efforts to rebuild Ukraine.[8] The Swiss government responded to the Swiss Parliament member as follows:

> No state has yet confiscated assets solely because a natural or legal person was on a sanctions list. Confiscating assets solely on the basis of the presence of a natural or legal person on a sanctions list or deemed to be close to the Russian state, and then using them for the reconstruction of Ukraine, as envisaged in the motion, is not currently an option.

The three main reasons are, first, that the forfeiture of assets, in comparison with their freezing, represents a massive infringement of the constitutionally guaranteed property rights and the fundamental rights of the individuals concerned. Forfeiture of assets presupposes a criminal offence confirmed by a court of law, which is not the case with the freezing of assets. The freezing of assets does not imply that they have been acquired illicitly. Second, the question of immunities in the case of a state's financial assets also arises. Indeed, the 7.4 billion Swiss francs belonging to the Central Bank of Russia that are currently frozen are protected by the immunity from execution of the state's assets. It is therefore not certain that the forfeiture of such assets would be compatible with the state's immunity from jurisdiction and execution under international law. Third, the confiscation of assets would produce the opposite effect from that intended by sanctions, which are, above all, temporary coercive measures designated to induce a state to return to behaviour that complies with international law.[9]

To date, the elaboration of a legal basis to allow the forfeiture of assets to compensate Ukraine for damages is not in the Swiss government's agenda.

FORFEITURE OF ASSETS UNDER SWISS CRIMINAL LAW

As forfeiture of assets in Swiss sanctions is not possible, the only alternative is to look at the possibilities existing in Swiss criminal law.

The forfeiture of assets is in the Swiss Criminal Code. Article 70, paragraph 1 states that the judge orders the confiscation of assets that are the result of a crime or that were intended to decide or reward the perpetrator of a crime, if they are not to be returned to the injured party in restoration of their rights. Confiscation is not a sanction but a measure that must be ordered when the legal conditions are met. It presupposes the existence of an unlawful act combining both the objective and the subjective elements of an offence. Assets derived

from an objectively legal act cannot be confiscated. There must be a connection between the criminal offence committed, on the one hand, and the seized assets, on the other hand. Therefore, without a criminal offence, forfeiture per se is not possible. Moreover, the forfeiture supposes that a criminal investigation is opened. As a result, the mere fact that a person is sanctioned under the Embargo Act and its ordinance is not sufficient to consider the application of the forfeiture based on the Criminal Code. The conditions of forfeiture are strict because forfeiture is a serious infringement of the guarantee of private property mentioned in article 26 of the Swiss Constitution. The forfeiture must be pronounced in accordance with the procedural guarantees provided by the Swiss Constitution and the European Convention of Human Rights. Therefore, there needs to be a criminal offence and, subsequently, a confiscation can be ordered. However, in international sanctions, the reason for forfeiture is not the offence but the violation of international law as mentioned in article 1 of the Embargo Act.

As those violations do not constitute criminal offences, it is not possible to forfeit Russian assets of sanctioned persons, companies and organisations based on article 70 of the Swiss Criminal Code.

Another possibility is the forfeiture of Russian assets based on article 72 of the Swiss Criminal Code, which provides for the forfeiture of assets of criminal or terrorist organisations. This provision states that in the case of assets of a person who participates in or supports such an organisation (article 260-ter of the Swiss Criminal Code), it is presumed that the assets are subject to the power of disposal of the organisation until the contrary is proven. The legal presumption arising from this provision assumes that the owner of the assets to be confiscated is punishable under article 260-ter. This sentence contains a reversal of the burden of proof. Such forfeiture presupposes that the person whose assets are forfeited belongs to a criminal or terrorist organisation. The central element of this provision is the existence of a criminal or terrorist organisation within the meaning of article 260-ter of the Swiss Criminal Code. To determine whether an organisation is considered to be terrorist or criminal, the courts that have jurisdiction in the matter must proceed on a case-by-case basis. The case law of the Swiss Supreme Court suggests that classifying a government as a criminal organisation within the meaning of article 260-ter of the Swiss Criminal Code would inevitably give rise to difficulties, particularly with regard to defining the objectives of this organisation or, in this case, the government and administration of evidence.[10] Consequently, it seems unlikely that the Swiss courts would qualify President Putin's government as a terrorist or criminal organisation.

However, the Swiss Supreme Court used article 72 of the Swiss Criminal Code to confiscate the money stolen from Nigeria by the former head of state, Sani Abacha, who was accused of setting up a criminal organisation to loot the country. Abacha had indeed established a criminal regime. This provision was also used to freeze assets belonging to relatives of former President of Egypt Hosni Mubarak, considering that it was plausible that the relatives were linked to the Mubarak regime, that the system set up by this regime could be described as a criminal organisation and, consequently, that the frozen funds could have been used to support this organisation.[11] The Mubarak decision was used by the Swiss Federal Criminal Court to freeze assets belonging to relatives of former President of Libya Mouammar Gaddafi.[12]

According to the criminal law Professor Mark Pieth, it is conceivable to classify President Putin and his inner circle as a criminal organisation, and the oligarchs who are filling the war chest could be accomplices in a similar way to the henchmen of mafia.[13]

Even if the possibility of using article 72 of the Swiss Criminal Code was recognised, no criminal prosecution has been initiated against President Putin and his inner circle in Switzerland. Most probably, this provision will not be used as long as President Putin remains the head of the Russian state.

FORFEITURE OF ASSETS: WHAT NEXT?

As explained, there is no legal basis in Switzerland for confiscation on the basis of a restrictive measure, and assets or economic resources that have not been obtained through an offence are therefore not considered illicit until proven otherwise. Forfeiting assets of a person not convicted of a criminal offence but only because they are mentioned on a list seems doubtful. The purpose of the Embargo Act is clearly not to foresee such an option. On 15 February 2023, the working group led by the Federal Office of Justice of the Swiss government concluded that the confiscation of private Russian assets would undermine the Federal Constitution and the prevailing legal order.[14] Therefore, the expropriation of private assets of lawful origin without compensation is not permissible under Swiss law. The right of private property is indeed a fundamental right. Moreover, the general rules of procedure must be respected, as must the right to be heard and the right to have a case determined by a judicial authority. As the forfeiture has an impact on the civil rights of the owner, the guarantees of the European Convention on Human rights are also applicable.

We also consider that the principle of non-retroactivity of the law is at stake. The Swiss Constitution guarantees the principle of legality and the principle of predictability and legal certainty of the law. Passing a law that allows the forfeiture of assets for facts that happened before the law's entry into force will also raise many legal issues.

The forfeiture of Central Bank of Russia assets raised additional concerns, in particular a state's immunity from jurisdiction and execution under international law.

Endnotes

1 https://www.fedlex.admin.ch/eli/cc/2002/564/en. ^ Back to section

2 See website of the State Secretariat for Economic Affairs, https://www.seco.admin.ch/seco/fr/home/ Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/ Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos/ sanktionsmassnahmen/ faq_russland_ukraine.html. ^ Back to section

3 See website of the State Secretariat for Economic Affairs, https://www.seco.admin.ch/seco/fr/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/ Wirtschaftsbeziehungen/ exportkontrollen-und-sanktionen/ sanktionen-embargos/sanktionsmassnahmen/faq_russland_ukraine.html. ^ Back to section

4 Press release of the Swiss government, dated 1 April 2025, https://www.news.admin.ch/fr/nsb?id=104687. Back to section

5 See website of the State Secretariat for Economic Affairs, https://www.seco.admin.ch/seco/en/home/ Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/ Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos/ sanktionsmassnahmen/suche_sanktionsadressaten.html. Back to section

6 See website of the State Secretariat for Economic Affairs, https://www.seco.admin.ch/seco/fr/home/ Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/ Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/ sanktionen-embargos/ sanktionsmassnahmen/faq_russland_ukraine.html. Back to section

7 See website of the State Secretariat for Economic Affairs, https://www.seco.admin.ch/seco/en/home.html. Back to section

8 See website of the Swiss Parliament, https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20223455. Back to section

9 See website of the Swiss Parliament, https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20223455. Back to section

10 ATF 145 IV 470 of November 8, 2019, recital 4.8, see website of the Swiss Parliament, https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20233270. Back to section

11 Decision of the Swiss Supreme Court, dated 5 September 2012, https://www.bger.ch/ext/eurospider/ live/de/php/aza/ http/index.php?highlight_docid=aza%3A%2F%2F05-09-2012-1B_175-2012&lang=de&type=show_document&zoom=YES&. Back to section

12 Decision of the Federal Criminal Court, dated 20 December 2012, https://entscheide.weblaw.ch/cache.php?link=20.12.2012_BB.2012.71. Back to section

13 https://www.swissinfo.ch/ger/wirtschaft/die-schweiz-hat-bereits-eine-rechtsgrundlage-um-russische-gelder-fuer-die-ukraine-zu-verwenden/48227654. Back to section

14 Press release of the Federal Office of Justice, dated 15 February 2023, https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-93089.html. Back to section

Pascal de Preux depreux@resolution-lp.ch

Avenue de l'Avant-Poste 4, Case postale 1255, 1001 Lausanne, Switzerland

https://resolution-lp.ch/

Switzerland: strategy and defence in corporate criminal liability

Andrea Taormina and **Nadine Wantz**
Taormina law AG

Summary

IN SUMMARY

Switzerland introduced criminal liability of companies on 1 October 2003, which is rather late compared with other countries. There are only a few court rulings on this topic. Currently, there has been only one ruling by the Federal Supreme Court regarding the Swiss Post, which resulted in the company being acquitted. The former private bank Falcon was the first bank ever to be convicted pursuant to article 102, paragraph 2 of the Swiss Criminal Code. In the appeal procedure, the bank was acquitted in June 2023.

DISCUSSION POINTS

- The origin and development of criminal liability of companies in Switzerland
- Facts and figures on criminal liability of companies in Switzerland
- Case law on criminal liability of companies
- Arguments of the defence in the ***Falcon*** case

REFERENCED IN THIS ARTICLE

- Decision of the Federal Supreme Court on the ***Rhine pollution*** case (BGE 113 Ib 60)
- Decision of the Federal Supreme Court on the ***Swiss Post*** case (BGE 142 IV 333)
- Decision of the Criminal Chamber of the Federal Criminal Court on the ***Credit Suisse-/Banev*** case (BStGer SK.2020.21, 15 December 2021)
- Decision of the Appeals Chamber of the Federal Criminal Court on the ***Credit Suisse-/Banev*** case (BStGer CA.2023.20, 26 November 2024)
- Conclusions of the Decision of the Appeals Chamber of the Federal Criminal Court on the ***Credit Suisse/Banev*** case (BStGer CA.2025.17, 3 March 2026)
- Decision of the Appeals Chamber of the Federal Criminal Court on the ***Falcon*** case (BStGer CA.2022.12, 30 June 2023)
- Article 102 of the Swiss Criminal Code
- Police crime statistics of the Swiss Federal Statistical Office

INTRODUCTION

In this article we discuss the introduction of criminal liability of companies in Switzerland and court decisions that have resulted from these criminal law provisions.

HOW CRIMINAL LIABILITY OF COMPANIES EMERGED IN SWITZERLAND

Unlike other countries, Switzerland had no criminal liability of companies for a long time. It was only on 1 October 2003 that the article on criminal liability of companies was implemented in the Swiss Criminal Code (SCC).[1] Until then, the principle of ***societas delinquere non potest***, according to which companies could not be held criminally liable, prevailed.

The trigger for the introduction of the article for criminal liability of companies was an incident in 1986 involving a fire in a chemical warehouse in Basel.[2] Toxic gases were released, and toxic fire-fighting water was poured into the river, causing severe pollution of the river from Basel to Rotterdam. It was not possible for the authorities to deal with what had happened by applying the traditional means of individual criminal law. At the time, only the firefighters could be held accountable, not the responsible managers of the chemical company.[3] In addition to this incident, another reason for the introduction of criminal liability of companies was the fear of organised crime. The Federal Council came under pressure, which set legislation on criminal liability of companies in motion.[4]

What Are The Regulations Governing Criminal Liability Of Companies In Switzerland?

The criminal liability of companies is governed by article 102 of the SCC. The law makes a distinction depending on the offence committed within the company. According to article 102, paragraph 1 SCC, the company is only subsidiarily liable for ordinary criminal offences (eg, traffic offences with company cars, fraud and personal injury). This means that the company is liable only if the offence cannot be attributed to a specific individual person due to the lack of organisation of the company.

Only seven specific offences, the catalogue offences, may constitute the basis of a cumulative criminal liability of a company that competes with the criminal liability of an individual person who committed a crime. All of these offences are white-collar or macro-crime offences in the areas of organised crime, money laundering, corruption or the financing of terrorism. This cumulative criminal liability is governed by article 102, paragraph 2 SCC.

In both paragraphs of article 102 SCC, the requirements of a liability are that a criminal offence has been committed in a company in the course of business activities within the scope of the company's purpose.

EMPIRICAL DATA ON CRIMINAL LIABILITY OF COMPANIES

In Switzerland, there are no official empirical statistics on the number of convictions of companies under article 102 SCC. This is due to the way in which data is collected by the Swiss Federal Statistical Office (FSO). The FSO's conviction statistics are based on the convictions of individuals that result in an entry in the register of convictions. As companies are not entered in the register of convictions, the convicted companies do not appear in the conviction statistics.[5] This is one of the reasons why it is argued that companies should also be entered in the register of convictions.[6]

However, there are statistics on the number of companies that have been accused of an offence. The data is collected by the cantonal police authorities (not legal experts) as part of the police crime statistics.[7] The legal classification of criminal offences may therefore not always be correct, and it is not possible to infer from this data the number of convictions. Nevertheless, certain trends can be deduced from the statistics. The latest figures available are those for 2024, published by the FSO on 24 March 2025.

The number of companies that are listed as defendants has increased slightly in recent years but is still very low in absolute numbers. In 2019, a total of 247 companies were registered in Switzerland. In 2020, the number rose drastically to 548, probably due to the coronavirus pandemic, as 395 of the 548 cases registered in 2020 alone were fraud offences, presumably relating to government loans granted to companies during the pandemic. In

2021, the numbers dropped to 512, in 2022 to 388 and in 2023 to 179 registered defendant companies. In 2024, the number rose to 300 companies, almost doubling compared to the previous year.[8]

As already mentioned, these numbers do not show the convicted companies. Since the liability of the company is subsidiary under article 102, paragraph 1 SCC, it is often the case that companies were recorded by the police as a defendant at the beginning of the investigation. However, as soon as an individual person has been identified, this person is subject to criminal liability and not the company. Only in the case of the catalogue offences listed under article 102, paragraph 2 SCC (money laundering and financing of terrorism, etc) is it possible for the company to be prosecuted, if the offence can be attributed to a specific individual person.

The police crime statistics show that the cases in which companies were registered as defendants are hardly ever cases of the seven catalogue offences listed in article 102, paragraph 2 SCC. The only catalogue offence that occurs relatively frequently is money laundering. In 2020, 208 companies were registered as defendants in criminal proceedings; in 2021, 88 companies; in 2022, 42 companies; in 2023, 10 companies; and, in 2024, 26 companies. For other catalogue offences (eg, criminal organisation (article 260-ter SCC)), no companies were registered as defendants at all between 2020 and 2024, while there were only a few cases of corruption (eg, one case of private bribery (article 322-octies SCC) in 2021).[9] This is also reflected in the case law. To date, convictions under article 102, paragraph 2 SCC have mainly been in connection with money laundering and less frequently with corruption.

SWISS CASE LAW ON CRIMINAL LIABILITY OF COMPANIES

As there have been no court decisions of subsidiary criminal liability within the meaning of article 102, paragraph 1 SCC in practice (apart from one case of a traffic offence involving a company car, which was settled by a summary penalty order),[10] the following explanations are limited to cases of cumulative criminal liability under article 102, paragraph 2 SCC. It is not entirely clear why there are no cases under paragraph 1, even though companies repeatedly appear in the police crime statistics as accused persons even outside the catalogue of offences under paragraph 2. It must be assumed either that the cases were abandoned or that an individual person was convicted.

Settlement By Summary Penalty Order

Although there are some criminal cases in which companies are accused persons (at least initially), these cases hardly ever reach the courts. There is very little case law on criminal liability of companies. However, the lack of court rulings does not mean that there have been no convictions. The majority of convictions occurred by virtue of issuing a summary penalty order. Summary penalty orders are issued not by the court but directly by the public prosecutor's office. This fast-track procedure is in the interest of the state, as the matter is settled quickly and often results in large payments to the state. In many cases, a summary penalty order is also in the interest of the accused company as a result of the fact that summary penalty orders attract much less public attention than court decisions and, to a certain extent, are open to negotiation.

To give just a few examples, the cases settled by summary penalty order include the conviction in 2011 of the Swiss subsidiary of the French Alstom Group, which was fined 2.5 million Swiss francs and ordered to pay an equivalent claim[11] of over 36 million Swiss

francs. The company had failed to take the necessary precautions against the bribery of foreign public officials in Latvia, Tunisia and Malaysia.[12] In addition, a summary penalty order was issued against the Brazilian construction group Odebrecht (currently the highest fine of 4.5 million Swiss francs).[13] In a recent summary penalty order dated 22 August 2025, the Office of the Attorney General of Switzerland (OAG) ordered Banque J Safra Sarasin SA to pay a fine of 3.5 million Swiss francs for failing to take all reasonable and necessary organisational measures to prevent the commission or attempted commission of aggravated money laundering acts. Since Safra also paid a settlement amount of 16 million Swiss francs to the private claimant in the proceedings, the OAG has not ordered a compensatory claim.[14]

Selected Court Rulings

The Post Ruling

There are very few cases of criminal liability of a company that have resulted in court proceedings. One of these cases is the ***SwissPost*** ruling.[15] In Switzerland, this is the only case of criminal liability under article 102, paragraph 2 SCC that was decided by the Federal Supreme Court, the highest national court. In December 2004, a Swiss public limited company was granted a licence to act as a financial intermediary. The company had two executive bodies, A and B. Just two months later, on 10 February 2005, 5 million Swiss francs were transferred to an account held in the name of the limited company. The very next day, A withdrew 4.6 million Swiss francs in cash from this account at a post office counter, allegedly for the purchase of a precious gemstone. B allegedly took this money to Rome, where she handed it over to an unknown person. The money has since disappeared. Following lengthy proceedings, the two company executives were convicted of commercial fraud, money laundering and qualified embezzlement by the Federal Supreme Court in 2014.[16]

The public prosecutor charged Swiss Post as a company with money laundering because it did not carry out prior checks on the origin and use of the money withdrawn and because this was not required by the company's internal regulations. In the first instance, Swiss Post was found guilty of money laundering under article 305-bis SCC.[17] Both the indictment and the first instance verdict for money laundering were wrong in principle. The offences listed in article 102, paragraph 2 SCC, which also include money laundering, are only the underlying offences that are committed by an individual person in the company. The company itself cannot be convicted of these offences itself (ie, it cannot be convicted of money laundering). A company may be convicted under article 102, paragraph 2 SCC only for the organisational deficiency in the company that made the underlying offence possible. It must therefore first be proven that a person in the company has committed one of the catalogue offences under article 102, paragraph 2 SCC; otherwise, the company is not liable to prosecution. Article 102, paragraph 2 SCC does not establish a strict liability on the part of the company.

In the ***Swiss Post*** case, no individual person within Swiss Post was identified as having committed money laundering. Due to the lack of an underlying offence, the Federal Supreme Court ultimately acquitted Swiss Post.[18]

Credit Suisse Ruling

For a long time, there were no cases in which banks were prosecuted on the basis of article 102, paragraph 2 SCC. Then, in 2021, two cases became public in which banks were defendants. Although the Federal Supreme Court has not yet ruled on these cases, the Federal Criminal Court has already issued rulings.

One of these was the ***Banev*** case against the former Swiss bank Credit Suisse, which merged with UBS Switzerland AG on 1 July 2024.[19] Evelin Banev was the head of an alleged Bulgarian drug gang. The OAG accused the bank of enabling Banev's drug gang to launder 55 million Swiss francs between 2004 and 2007. In June 2022, the Federal Criminal Court issued its first instance judgment. The Court convicted a Credit Suisse employee of qualified money laundering. Concerning Credit Suisse, the Court found that, during the period in question, there were deficiencies within the bank with regard to both the management of the client relationship with the criminal organisation and the monitoring of the implementation of the anti-money laundering rules. The court sentenced Credit Suisse to a fine of 2 million Swiss francs for violating article 102, paragraph 2 SCC and an equivalent claim of more than 19 million Swiss francs. The Court held that the amount of the equivalent claim corresponded to the assets that could not be confiscated due to internal deficiencies at Credit Suisse, which had facilitated the money laundering.[20] In second instance, UBS, which inherited the ***Banev*** case as a result of the merger, was acquitted. The decision is not final yet.[21]

Falcon Ruling

The other case against a bank in which the Federal Criminal Court has already issued its second decision (by the Appeals Chamber) is the case against Falcon. Taormina law defended Falcon, and a few arguments of the defence will be discussed below.

The case involved the bank and its former CEO, A, as well as an investment company that was the ultimate mother company of the bank. The investment company wanted to increase its stake in the Italian financial institution UniCredit and acquired a €62 million share package in 2012. The transaction was accompanied by Falcon. According to the indictment, there was an alleged concentration of power since the seller of the shares, B, was the chair of the board of directors of the investment company as well as the former chair of the board of directors of Falcon. As a result of this, he was qualified by the OAG as a de facto "executive body" of Falcon. In the view of the OAG, a massively inflated price was paid for the stake in UniCredit. Separate proceedings were brought against the seller for mismanagement but were suspended and no conviction has yet been obtained. Although there was no conviction in the Swiss proceedings, the first instance of the Federal Criminal Court found that B had committed qualified criminal mismanagement by selling Falcon his privately held shares worth €61.7 million as well as worthless additional rights ("certain rights") for a total price of €210 million. This was the alleged predicate offence for the subsequent money laundering, which allegedly took place as follows.

After the sale, proceeds totalling €194 million were received into accounts of B at Falcon for the alleged unlawful enrichment of B. At the request of B, CEO A subsequently helped to ensure that various complex transactions were carried out via Falcon, according to the indictment, to thwart the confiscation of these proceeds of crime. The OAG charged the CEO of Falcon with money laundering and the bank itself with criminal liability under article 102, paragraph 2 SCC.

The Federal Criminal Court ruled differently. It found that CEO A neither knew nor must have known that the funds in question were the proceeds of a crime, and therefore acquitted him of the charge of money laundering. However, in the court's view, B had committed the offence of money laundering and was a responsible individual within the meaning of article 102, paragraph 2 SCC due to his position as a de facto executive body. It found that the execution of the money transactions without due consideration was facilitated by

organisational deficiencies at Falcon. On 15 December 2021, Falcon became the first bank in Swiss history to be held accountable under article 102, paragraph 2 SCC. Falcon was ordered to pay a fine of 3.5 million Swiss francs and an equivalent claim of 7.2 million Swiss francs.[22]

However, this judgment did not become final. Falcon appealed, and in its judgment of 30 June 2023,[23] the Appeals Chamber of the Federal Criminal Court confirmed the acquittal of the CEO and this time also acquitted Falcon.[24]

ARGUMENTS OF THE DEFENCE IN THE FALCON CASE

The OAG intended to conclude the proceedings with a summary penalty order. The decision to ask for ordinary proceedings and not to accept a summary penalty order was of strategic importance. This decision was taken in view of the risk of a negative judgment, which ultimately always exists in court proceedings, and despite the publicity surrounding it. The view prevailed that the bank should not be criminally convicted based on the facts of the case.

According to the indictment, the bank should have been convicted based on article 102, paragraph 2 SCC in conjunction with article 305-bis SCC as the underlying offence for criminal liability of companies. For the defence of the bank, various points were addressed. Two were of particular importance. First, there was the absence of a predicate offence as required by article 305-bis SCC. If it can be established that there is no predicate offence to money laundering, the company is ultimately not liable to prosecution: no money laundering without a predicate offence, hence no underlying offence for criminal liability of the company without money laundering. Second, there was the lack of causality between the organisational deficiencies and the alleged money laundering.

According to the prosecution, the predicate offence required by article 305-bis SCC had been mismanagement. The existence of such an offence was questioned based on the files. It was then shown that, even if money laundering were to be affirmed and subsequently considered as an underlying offence for criminal liability, the money laundering was not committed within the company; the act of money laundering was attributed to a person whom the prosecution qualified as a de facto executive body. However, it is highly questionable whether the legal concept of the de facto executive body, which originated in civil law, fulfils the requirement of article 102, paragraph 2 SCC (ie, that the offence must be committed within the company). Finally, it was shown that the requirement that the offence be committed "in the course of business" was clearly not met.

Article 102 SCC requires a lack of organisation to be the cause of the offence committed. The defence pointed out that even if all the alleged organisational deficiencies had been absent, the transactions in question – qualified as money laundering by the OAG – would still have taken place; it was simply not obvious to those involved that the transactions in question could be illegal. They would therefore not have been prevented even if appropriate organisational measures had been taken.

* *The authors would like to thank Leonie Monstein and Katarina Balac for their help drafting this article.*

** *This article was accurate as at 11 March 2026.*

Endnotes

1 See article 102 of the Swiss Criminal Code (https://www.fedlex.admin.ch/eli/cc/54/757_781_799/en#book_1/part_1/tit_7) (last visited 10 March 2026). Back to section

2 https://relevancy.bger.ch/php/clir/ http/index.php?highlight_docid=atf%3A%2F%2F113-IB-60%3Ade& lang=de& type=show_document#page62 (last visited 10 March 2026). Back to section

3 Mark Pieth, Die Reform der Strafrechtlichen Unternehmenshaftung in der Schweiz, in: Unternehmensstrafrecht (ed. Lehmkuhl & Wohlers, 2020), at 283; Botschaft [Federal Council Dispatch] zur Änderung des Schweizerischen Strafgesetzbuches (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) und des Militärstrafgesetzes sowie zu einem Bundesgesetz über das Jugendstrafrecht, 21 September 1998, BBl 1999 II 1979, at 2140. Back to section

4 Marcel Alexander Niggli and Diego R Gfeller, in: Basler Kommentar (4th ed. 2018 Niggli/Wiprächtiger), at Art. 102 N 14. Back to section

5 For the methodology of the criminal conviction statistics, see FSO, fact sheet, https://www.bfs.admin.ch/bfs/de/home/statistiken /kriminalitaet-strafrecht/erhebungen/sus.assetdetail.35957057.html (last visited 10 March 2026). Back to section

6 For example, Nora Markwalder, Warum braucht es ein Strafregister für Unternehmen?, in: Empreinte d'une pionnière sur le droit pénal Mélanges en l'honneur sur d'Ursula Cassani (ed. Jeanneret & Sträuli, 2021), at 257–267. Back to section

7 FSO, Police Crime Statistics (PCS), Swiss Criminal Code (SCC): Criminal offenses and accused persons, 2024, published on 24 March 2025, at https://www.bfs.admin.ch/bfs/en/home/statistics/crime-criminal-justice/police/offences.assetdetail .34387367.html (last visited 10 March 2026). Back to section

8 FSO, Police Crime Statistics (PCS), Swiss Criminal Code (SCC): Criminal offenses and accused persons, 2024, published on 24 March 2025, at https://www.bfs.admin.ch/bfs/en/home/statistics/crime-criminal-justice/police/offences.assetdetail .34387367.htm (last visited 10 March 2026); on this topic, see Nora Markwalder, Die Sanktionierung von Unternehmen gemäss Art. 102 StGB in Theorie und Praxis – Part 2, ZStrR 140/2022, at 273–301. Back to section

9 See footnote 7. The numbers of companies listed as defendants regarding article 322-octies SCC in 2022 and 2023 and article 260-quinquies SCC in 2023 has not been published due to data protection reasons. Back to section

10 Summary penalty order issued by the Freiburg public prosecutor's office on 5 January 2005, published in Freiburger Zeitschrift für Rechtsprechung, FZR 2005, at 60. Back to section

11 If the assets subject to forfeiture are no longer available, the court may uphold a claim for compensation by the state in respect of a sum of equivalent value (article 71 SCC). ^ Back to section

12 Press release from the Office of the Attorney General of Switzerland dated 22 November 2011 (https://www.news.admin.ch/de/nsb?id=42300) (last visited 10 March 2026). ^ Back to section

13 Press release from the Office of the Attorney General of Switzerland dated 21 December 2016 (https://www.admin.ch/gov/de/ start/dokumentation/ medienmitteilungen.msg-id-65077.html) (last visited 10 March 2026). ^ Back to section

14 Press release from the Office of the Attorney General of Switzerland dated 22 August 2025 (https://www.bundesanwaltschaft.ch/en/newnsb/2y8oBsJ36EJLYA723v50c-) (last visited 10 March 2026). ^ Back to section

15 https://search.bger.ch/ext/eurospider/live/de/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F142-IV-333%3Ade&lang=de&zoom =& ;type=show_document (last visited 10 March 2026). ^ Back to section

16 See decision of the Federal Supreme Court of 18 July 2014, BGer 6B_1198/2013 (https://www.bger.ch/ext/eurospider/live/de/php/aza/http/index.php?highlight_docid=aza%3A%2F%2F18-07-2014-6B_1198-2013&lang=de&type=show _document&zoom=YES&) (last visited 10 March 2026). ^ Back to section

17 See decision of the District Court Solothurn-Lebern of 19 April 2011, AGer Nr. SLSPR.2010.00109-ASL. ^ Back to section

18 See decision of the Federal Supreme Court of 11 October 2016, BGer 6B_124/2016, published in BGE 142 IV 333 (https://www.bger.ch/ ext/eurospider/live/de/php/clir/http/ index.php?highlight_docid=atf%3A%2F%2F142-IV-333%3Ade& lang=de& zoom=& type=show_document) (last visited 10 March 2026). ^ Back to section

19 Press release from UBS dated 1 July 2024 (https://www.ubs.com/global/de/media/display-page-ndp/de-20240701-sbm.html) (last visited 10 March 2026). ^ Back to section

20 See decision of the Criminal Chamber of the Federal Criminal Court of 27 June 2022, SK.2020.62 (https://bstger.weblaw.ch/cache/450ca3ef-a347-340b-a55a-a1181b7b985d?q=SK.2020.62&sort-field=relevance&sort-direction=relevance) (last visited 10 March 2026). ^ Back to section

21 Decision of the Appeals Chamber of the Federal Criminal Court of 26 November 2024, CA.2023.20 (https://bstger.weblaw.ch/cache/4e028a33-b68a-34c9-aa7c-389021d76a46?q=%20CA.2023.20&sort-field=relevance&sort-direction=relevance) (last visited 10 March 2026); Conclusions of the Decision of the Appeals Chamber of the Federal Criminal Court dated 3 March 2026 , CA.2025.17 (https://www.bstger.ch/uploads/2026-03-04_20260303_Dispo_CA_2025_17.pdf) (last visited 10 March 2026); press release of the Appeals Chamber of the Federal Criminal Court dated 4 March 2026 (https://bstger.ch/de/media/comunicati-stampa/2026/2026-03-04/1543.html) (last visited 10 March 2026). ^ Back to section

22 Decision of the Criminal Chamber of the Federal Criminal Court of 15 December 2021, SK.2020.21 (https://bstger.weblaw.ch/cache/3db6611a-6606-39bf-918d-470eb44e12b9?q=SK.2020.21&sort-field=relevance&sort-direction=relevance)% 20(last%20visited%2010%20March%202026) (last visited 10 March 2026). ^ Back to section

23 https://www.bstger.ch/de/media/comunicati-stampa/2023/2023-07-03/1351.html (last visited 10 March 2026). ^ Back to section

24 Decision of the Appeals Chamber of the Federal Criminal Court of 30 June 2023, CA.2022.12 (https://bstger.weblaw.ch/cache/8117d30a-cf1c-39db-a9d3-de7b2f4ef458) (last visited 10 March 2026). ^ Back to section

taormina

Andrea Taormina taormina@taormina-law.ch
Nadine Wantz wantz@taormina-law.ch

https://www.taormina-law.ch/