



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Economic
Affairs, Education and Research EAER
State Secretariat for Economic Affairs SECO

Federal Department of Justice and Police FDJP
Federal Office of Police fedpol
Money Laundering Reporting Office Switzerland MROS

Bern, 19 September 2024

National Risk Assessment (NRA): Proliferation financing

Report of the interdepartmental coordinating
group on combating money laundering and
the financing of terrorism (CGMF)

Inhaltsverzeichnis

- 1. Executive summary 4**
- 2. Glossary 6**
- 3. Introduction 9**
- 4. Methods used to prevent proliferation financing in both international and national contexts 10**
 - 4.1 Definition of the term proliferation financing 10
 - 4.2 International measures to prevent proliferation financing 11
 - 4.2.1 Relevant international treaties and export controls 11
 - 4.2.2 UN Security Council Resolutions 12
 - 4.2.3 Recommendations of the Financial Action Task Force (FATF) 14
 - 4.3 National legislation. 15
 - 4.3.1 Embargo Act (EmbA) and ordinances on targeted measures against Iran and North Korea 15
 - 4.3.2 Legislation on war materiel and goods control 17
 - 4.3.3 AML control system 19
- 5. Objectives, methodology and data used 21**
 - 5.1 Questions raised in the present risk analysis 21
 - 5.2 Methodology 21
 - 5.3 Data and involved parties 23
- 6. Risks associated with proliferation financing 23**
 - 6.1 Global risk landscape 23
 - 6.2 Risks associated with Iran 26
 - 6.3 Risks associated with North Korea 28
- 7. Risks for Switzerland 31**
 - 7.1 Importance and exposure of sectors 31
 - 7.2 Assessment of proliferation financing risks 33
 - 7.2.1 Risks 1 and 2: Intentional or negligent breach of sanctions 33
 - 7.2.2 Risk 3: Failure to identify assets or companies controlled by designated persons 34
 - 7.2.3 Risks 4 and 5: Accepting proceeds from the transfer of goods 34
 - 7.2.4 Risk 6: Accepting proceeds from the transfer of technology 35
 - 7.2.5 Risk 7: Concealment through legal entities (front companies) 35
 - 7.2.6 Risk 8: Concealment through correspondent banking 36
 - 7.2.7 Risk 9: Raising funds from stolen cryptocurrencies 36
 - 7.2.8 Risk 10: Concealment through trade or transport financing 37
 - 7.2.9 Risk 11: Raising funds from commodity trading 37
 - 7.2.10 Risk 12: Raising funds from the sale of refined gold 38
 - 7.2.11 Summary table 40
 - 7.3 Vulnerabilities in proliferation financing countermeasures 40
 - 7.3.1 Due diligence obligations and oversight 41
 - 7.3.2 Information sharing 41
 - 7.3.3 Raising private sector awareness 41
 - 7.3.4 Reporting obligations 42
 - 7.3.5 Comparison of proliferation and terrorist financing bans 42

- 8. Conclusions and recommendations43**
- 9. Literature44**
- 10. Annex 154**
 - 10.1 Data and statistics on Iran.54
 - 10.1.1 Bilateral trade in goods with Iran between 2000-202354
 - 10.1.2 Administrative criminal decisions based on Iran Ordinance55
 - 10.1.3 Rejections of goods based on EmbA, WMA and GCA.56
 - 10.1.4 Financial statistics for Iran58
 - 10.1.5 Statistics on foreign nationals and issuance of visas.59
 - 10.2 Data and statistics on North Korea60
 - 10.2.1 Bilateral trade in goods with North Korea between 2000-2023.60
 - 10.2.2 Administrative criminal decisions based on North Korea Ordinance.60
 - 10.2.3 Rejections of goods based on EmbA, WMA and GCA60
 - 10.2.4 Financial statistics for North Korea61
 - 10.2.5 Statistics on foreign nationals and issuance of visas62
 - 10.3 Other data63
 - 10.3.1 Suspicious activity reports sent to MROS63
 - 10.4 Trade in nuclear materials.65
 - 10.5 Applications for Swiss Export Risk Insurance (SERV)65

1. Executive summary

The proliferation of nuclear,¹ chemical and biological weapons (weapons of mass destruction) and their delivery systems threatens international peace and security. The international Treaty on the Non-Proliferation of Nuclear Weapons (NPT)² contains key elements of the international security architecture that are designed to prevent the proliferation of weapons of mass destruction. In addition, since 2006, the UN Security Council has issued targeted sanctions against Iran and North Korea, which are specifically intended to halt nuclear weapons and delivery system programmes. In 2012, the Financial Action Task Force (FATF) broadened its mandate to include proliferation financing and added a new recommendation to implement UN financial sanctions. Since 2020, all FATF member states, including Switzerland, have committed themselves to **analysing the risk of potential breach, non-implementation or evasion of UN financial sanctions against Iran and North Korea and adopting a risk-based approach aimed at mitigating that risk.**

There is a complex international and national legal framework in place to prevent proliferation financing, which will be presented in this report. Drawing from public sources, the report describes the global risk landscape as well as the specific proliferation financing risks associated with Iran and North Korea. Based on an analysis of how the existing legal framework and risk landscape affects Switzerland as a financial and business centre, 12 risk scenarios are presented to illustrate and assess the various proliferation financing risks (see table).



	Low	Medium	High		
Comparison of proliferation financing risks	Intentional breach of sanctions	Negligent breach of sanctions	Failure to identify assets or companies controlled by designated persons	Concealment through correspondent banking	Concealment through legal entities (front companies)
	Accepting proceeds from the transfer of goods (domestic element)	Accepting proceeds from the transfer of goods (foreign element)	Raising funds from the sale of refined gold	Raising funds from stolen cryptocurrencies	
		Accepting proceeds from the transfer of technology		Raising funds from commodity trading	
		Concealment through trade or transport financing			

1 Also referred to as atomic weapons (synonym)

2 SR 0.515.03 – *Treaty of 1 July 1968 on the Non-Proliferation of Nuclear Weapons*, (NPT, Non-Proliferation Treaty), status as of 15 March 2018.

Given the limited data available, only a qualitative risk analysis is possible. The risk scenarios presented here are hypothetical and not based on specific data or concrete evidence. Risks are only assessed in relation to one another and our analysis does not compare risks in Switzerland with those in other countries. While the report analyses risks for Switzerland, many of the issues identified here are likely to affect other countries as well.

The results of the analysis show that the risk of sanctions being breached intentionally or out of negligence is lower than the risk of failing to identify assets or companies controlled by designated natural persons.

For Switzerland, the proliferation financing risks are deemed to be highest in commodity trading, cryptocurrency trading and correspondent banking. In contrast, the risk that financial intermediaries will receive the proceeds from the illegal transfer of goods or will finance trade in sanctioned goods is deemed lower. However, no industry is immune to circumvention activities, which is why concealment through front companies is considered the highest overriding risk. Additionally, trade-related risks are generally considered higher for Iran, since, unlike North Korea, Iran is not excluded from the value chain. For its part, North Korea poses a higher risk when it comes to cybercrime and the associated use of cryptocurrencies.

A clear understanding of proliferation financing risks allows us to properly assess the respective threats and vulnerabilities and highlight existing risk-mitigating factors. With this in mind, the CGMF recommends that the following four measures be taken to reinforce the control system:

- Expand the CGMF's mandate to include proliferation financing
- Set up a working group for proliferation financing
- Improve datasets
- Raise awareness within the private sector

The CGMF also suggests that consideration be given to the possibility of expanding the scope of the next risk analysis beyond Iran and North Korea to include other countries that have weapons of mass destruction programmes incompatible with the NPT. The report does not contain any recommendations for specific industries or services. However, the private sector is encouraged to conduct its own risk analyses.

2. Glossary

AG	Australia Group
FOCBS	Federal Office for Customs and Border Security
BWC	Biological Weapons Convention – SR 0.515.07
CAD	Computer-aided design; includes all of the electronic data processing tasks involved in the design, construction, planning and improvement of new products.
ChCO	Chemicals Control Ordinance – SR 946.202.21
COTS	Commercial-off-the-shelf refers to mass-produced goods or software that can be used without further modification.
CWC	Chemical Weapons Convention – SR 0.515.08
Dual-use goods	Items that can be used both for civilian and military applications
FDFA	Federal Department of Foreign Affairs
EmbA	Embargo Act – SR 946.231
FATF	Financial Action Task Force
fedpol	Federal Office of Police
Financial intermediaries	Banks, asset managers, insurance companies, VASP, etc. within the meaning of Art. 2 paras 2 and 3 AMLA.
(Financial) services provider	Natural persons and legal entities that provide financial (e.g. certain VASPs) and non-financial services (e.g. trading companies, portfolio manager, lawyers, notaries). While not subject to the Anti-Money Laundering Act (AMLA), financial service providers are subject to the Embargo Act (EmbA).
FINMA	Swiss Financial Market Supervisory Authority
FIU	Financial Intelligence Unit
Targeted sanctions	Sanctions that are directed against natural persons, companies and organisations designated in UN Security Council resolutions or in EU sanction regulations or mentioned in the list of measures annexed to the EmbA, or that restrict trade in certain listed goods. The terms 'targeted sanctions', 'list-based sanctions' or 'smart sanctions' are also used.
GCA	Goods Control Act – SR 946.202
GCO	Goods Control Ordinance – SR 946.202.1
Goods	Merchandise, technologies and software
ML	Money laundering

AMLA	Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act) – SR 955.0
IAEA	International Atomic Energy Agency
JCPOA	Joint Comprehensive Plan of Action. International agreement on the Iranian nuclear programme, from July 2015
NEA	Nuclear Energy Act – SR 732.1
CGMF	Interdepartmental coordinating group on combating money laundering and the financing of terrorism
WMA	War Materiel Act – SR 514.51
Correspondent bank	Bank that processes international wire transfers on behalf of another bank
Weapons of mass destruction	Nuclear, biological or chemical weapons
MTCR	Missile Technology Control Regime
MROS	Money Laundering Reporting Office Switzerland
FIS	Federal Intelligence Service
NPT	Non-Proliferation Treaty (Treaty on the Non-Proliferation of Nuclear Weapons) – SR 0.515.03
NRA	National Risk Assessment
NSG	Nuclear Suppliers Group
OECD	Organization for Economic Co-operation and Development
OPCW	Organisation for the Prohibition of Chemical Weapons
Proliferation	The term is used in technical jargon to refer to the propagation of weapons of mass destruction and their delivery systems.
Red flag indicators	Alerts or indications of potentially suspicious or unusual activity, particularly in the context of financial transactions and money laundering, terrorist financing and proliferation financing
SECO	State Secretariat for Economic Affairs
SERV	Swiss Export Risk Insurance
SRO	Self-regulatory organisation
SIF	State Secretariat for International Finance
SCC	Swiss Criminal Code – SR 311.0
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TF	Terrorist financing

TPNW	Treaty on the Prohibition of Nuclear Weapons
Delivery system	Ballistic missiles, cruise missiles or unmanned aerial vehicles (drones)
UNO	United Nations Organisation
UNSC	United Nations Security Council
VASP / VA	Virtual asset service provider/virtual assets
DDPS	Federal Department of Defence, Civil Protection and Sport

3. Introduction

The proliferation of nuclear,³ chemical and biological weapons (hereinafter: weapons of mass destruction or WMD) and their delivery systems constitutes a threat to international peace and security. International agreements such as the Non-Proliferation Treaty (NPT)⁴ include key elements of the global security architecture that are intended to prevent the proliferation of weapons of mass destruction. The UN Security Council has also issued several binding resolutions to member states in an effort to halt the proliferation of weapons of mass destruction and their delivery systems.

Currently, nine countries possess nuclear weapons: the five recognised as such by the NPT (China, France, Russia, the United Kingdom and the United States) and four non-parties (India, Israel, North Korea and Pakistan). Since nuclear weapons are considered to have a strategic and deterrent value, countries hold on to them or seek to acquire them. If the behaviour of a country threatens international peace and security, the UN Security Council can issue Resolutions against it. Since 2006, targeted UN sanctions have been in effect against Iran and North Korea for the specific purpose of curtailing their nuclear and delivery system programmes.⁵ Targeted sanctions are directed against designated natural persons, companies or organisations or restrict trade in certain goods.

The Financial Action Task Force (FATF) establishes international standards to fight against money laundering and terrorist financing. In 2012, the FATF added combating proliferation financing to its mandate. Following this, the FATF issued Recommendations on implementation of the financial sanctions contained in the UN Resolutions mentioned earlier. In 2020, requirements for a risk-based approach were added to those established for the list-based approach.⁶ Since then, all FATF member countries, including Switzerland, are required to identify, assess and understand the **risk of potential breach, non-implementation or evasion of targeted financial sanctions against Iran and North Korea when conducting their national risk analyses**.⁷ Follow-up measures based on these recommendations should reduce existing proliferation financing risks and preserve the reputation of member countries and their private sector. Implementation of these new FATF Recommendations in Switzerland will be reviewed for the first time during the next FATF evaluation, which will take place sometime between 2026 and 2028.

In 2013, the Federal Council created the interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF).⁸ Acting under the supervision of the State Secretariat for International Finance (SIF),⁹ the CGMF has a mandate to coordinate Swiss AML/CFT policies and assess risks in these areas. In 2021, the CGMF therefore decided to conduct a national risk analysis devoted exclusively to proliferation financing in response to the new FATF Recommendations. It gave a corresponding mandate to the State Secretariat for Economic Affairs (SECO) and to the Money Laundering Reporting Office Switzerland (MROS), which is part of the Federal Office of Police (fedpol).

Proliferation financing concerns several federal offices and falls under various federal acts and goes beyond the control system established to counter money laundering and terrorist financing. This was the reason why the CGMF opted for a separate risk analysis on proliferation financing. The present report presents the results of this analysis.

3 Also referred to as atomic weapons (synonym)

4 SR 0.515.03 – *Treaty of 1 July 1968 on the Non-Proliferation of Nuclear Weapons*, (NPT, Non-Proliferation Treaty), status as of 15 March 2018.

5 UNSC, *Resolution 2231(2015)*, 20 July 2015, S/RES/2231 (IRAN); UNSC, *Resolution 1718 (2006)*, 14 October 2006 (DPRK).

6 Within the context of sanctions, natural persons and legal entities, organisations or countries are placed on a list for the purpose of imposing sanctions against them.

7 Breach and non-implementation correspond to wilful or negligent violations under Swiss law, while evasion refers to a situation in which natural persons on the sanctions list have managed to avoid detection of assets or companies under their control.

8 For the mandate and composition of the CGMF, see State Secretariat for International Finance SIF, *Mandate of the CGMF*, 2021.

9 In addition to running the CGMF, the SIF is also responsible for managing the Swiss delegation at FATF plenary meetings. The SIF also coordinates FATF country reviews.

4. Methods used to prevent proliferation financing in both international and national contexts

At the beginning of this analysis, the term proliferation financing used in this report is defined, taking into account the general understanding and the purpose of this report. The present chapter will then go on to discuss the international and, subsequently, the national legal framework in place to prevent proliferation financing.

4.1 Definition of the term proliferation financing

There is no international definition of proliferation or proliferation financing. However, proliferation is generally understood and defined along the lines of Resolution 1540¹⁰ of the UN Security Council (hereinafter: Resolution 1540): the proliferation of weapons of mass destruction, i.e. nuclear, biological or chemical weapons and their delivery systems.¹¹

In 2010, the FATF adopted a broad working definition¹² of this term based on Resolution 1540. This definition served as a basis for further work on proliferation financing and was helpful as a general aid to understanding the subject.¹³ The current FATF Recommendations relating to proliferation, however, only refer to the implementation of the UN Security Council Resolutions that contain targeted sanctions relating to WMD programmes,¹⁴ in particular sanctions against Iran and North Korea (see Chapter 5.1.).

For this reason, our risk analysis uses the following definition of proliferation financing, with wording taken from Switzerland's Embargo Act (EmbA):

'The direct or indirect provision of financial or economic resources or the provision and receipt of financial services, from or to natural persons, companies and organisations designated in targeted financial sanctions against Iran and North Korea, or for the purpose of carrying out activities prohibited under sanctions measures.'

Under the Embargo Act, the notion of financing in this definition and in the present risk analysis is understood in a broad sense and includes any provision of funds or financial services that are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, storage or use of nuclear, chemical or biological weapons and their means of delivery, as well as related goods,¹⁵ which in turn is consistent with the FATF's understanding.¹⁶

10 UNSC, [Resolution 1540 \(2004\)](#), 28 April 2004, S/RES/1540.

11 Ibid, see OP 3. In social sciences, a distinction is drawn between vertical and horizontal proliferation. Vertical proliferation occurs when countries expand or renew their arsenals. Horizontal proliferation, on the other hand, refers to the transfer of weapons to other countries that do not possess them.

12 The FATF defines proliferation financing as follows: the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nucle-ar, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

13 FATF, [Combating Proliferation Financing. A Status Report on Policy Development and Consultations](#), February 2010. p. 11.

14 Iran: R. 2231 (2015). North Korea: R. 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016) und 2356 (2017). See FATF, [The FATF Recommendations](#), February 2023, Interpretive Note To Recommendation 7, p. 51.

15 Art. 3 para. a of Switzerland's Goods Control Act defines 'goods' as commodities, technologies and software. For this reason, the wording of the FATF definition is not used here.

16 See FATF, [Combating proliferation financing: A status report on policy development and consultation](#), February 2010. p. 11.

4.2 International measures to prevent proliferation financing

At the international level, measures to prevent the proliferation of weapons of mass destruction and proliferation financing are based on three closely related pillars. The first is formed by disarmament and non-proliferation treaties (legally binding under international law) and multilateral regimes aimed at harmonising export controls (politically binding). The second pillar is formed by sanctions adopted by the UN Security Council against Iran and North Korea and Resolution 1540, which Switzerland is required to uphold. Lastly, the third pillar is formed by legally non-binding FATF Standards, which Switzerland adheres to, that are designed to fight money laundering, terrorist financing and proliferation financing.¹⁷ This chapter provides an overview of these measures and how they are interwoven.

4.2.1 Relevant international treaties and export controls

The Non-Proliferation Treaty (NPT)¹⁸ aims to prevent the proliferation of nuclear weapons and ultimately to abolish nuclear weapons while ensuring the peaceful use of nuclear energy. The International Atomic Energy Agency (IAEA) monitors compliance with non-proliferation obligations. The NPT draws a distinction between recognised nuclear-weapon states – China, France, Russia, the United Kingdom and the United States – and non-nuclear-weapon states. States such as India, Israel and Pakistan,¹⁹ which have nuclear weapons and do not want to relinquish them, have not joined the NPT for this reason. North Korea withdrew from the treaty in 2003.²⁰ These countries are unwilling to give up their nuclear weapons because of the strategic importance that these weapons have for military deterrence.²¹ The Treaty on the Prohibition of Nuclear Weapons (TPNW)²² came into effect in 2022 with the aim of accelerating nuclear disarmament nonetheless, with so far, only 69 non-nuclear weapon states have joined the treaty.²³ On the other hand, already in 1925, the Geneva Protocol²⁴ was adopted to prohibit the use in war of asphyxiating, poisonous or other gases as well as bacteriological methods of warfare. In addition to this, the Biological Weapons Convention (BWC)²⁵ and the Chemical Weapons Convention (CWC)²⁶ also prohibit the development, manufacture, stockpiling and transfer of biological and chemical weapons. Compliance with the CWC is verified by the Organisation for the Prohibition of Chemical Weapons (OPCW). The BWC contains confidence-building measures. None of the above treaties explicitly prohibits the funding of nuclear, biological or chemical weapons. However, all of the treaties prohibit assistance, which, in line with the objectives of the treaties, also includes funding.²⁷

17 For more information, see Federal Council's international financial policy strategy for Switzerland. *Leading worldwide, rooted in Switzerland: Policy for a future-proof Swiss financial centre*, Bern, 4 December 2020, p. 7 and 15.

18 SR 0.515.03 – *Treaty of 1 July 1968 on the Non-Proliferation of Nuclear Weapons*, (NPT, Non-Proliferation Treaty), status as of 15 March 2018.

19 SIPRI Yearbook, *Global nuclear arsenals are expected to grow as states continue to modernize*, 4 January 2024.

20 Federation of American Scientists. *North Korea Explains Withdrawal from the NPT*, 22 January 2002, last checked on 5 September 2023.

21 NATO, , 5 July 2023, last checked on 5 September 2023; GOV.UK, *The UK's nuclear deterrent: what you need to know*, 16 March 2023, last checked on 05 September 2023; E-International Relations.

22 Nuclear Weapons Ban Monitor, *The status of the TPNW*, 4 January 2024.

23 Although not a signatory country of the TPNW, Switzerland decided to take part in future intergovernmental conferences as an observer. See also Federal Department of Foreign Affairs (FDFA), *Update on the report of the working group analysing the Treaty on the Prohibition of Nuclear Weapons, 31 January 2024*. More information related to the *Treaty on the Prohibition of Nuclear Weapons (TPNW)* can be found on the website of the Federal Department of Foreign Affairs (FDFA), last checked on 3 April 2024.

24 SR 0.515.105 – *Protocol of 17 June 1925 for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare*, status as of 9 July 2020.

25 SR 0.515.07 – *Convention of 10 April 1972 on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction*, Biological Weapons Convention (BWC), status as of 22 May 2020.

26 SR 0.515.08 – *Convention of 13 January 1993 on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction*, (Chemical Weapons Convention, CWC), status as of 2 July 2020.

27 Non-Proliferation Treaty, NPT, Art. I and Art. II; Chemical Weapons Convention, CWC, Art. I let. d; Biological Weapons Convention, BWC, Art. III. The *International Convention of 13 April 2005 for the Suppression of Acts of Nuclear Terrorism* (ICSANT; SR 0.353.23, status as of 10 September 2020) prohibits the financing of nuclear terrorism, Art. 7. See also Treaty on the Prohibition of Nuclear Weapons, TPNW, Art. I let. e (not ratified by Switzerland, however).

In addition to disarmament and non-proliferation treaties, relevant supplier states have joined together in politically binding export control regimes²⁸ to identify those goods that should be subject to national controls on export, transit or brokering owing to the associated proliferation risk.²⁹ The Nuclear Suppliers Group (NSG)³⁰ lists goods relevant to nuclear weapons programmes and the Australia Group (AG)³¹ lists goods in connection with biological and chemical weapons. The Missile Technology Control Regime (MTCR)³² complements the NSG and AG export controls with a list of delivery systems that are suitable for weapons of mass destruction. A fourth export control regime, the Wassenaar Arrangement (WA),³³ concerns itself with goods used in conventional arms. The lists of goods covered by these four export control regimes include nuclear goods, conventional military goods and goods that can be used for both civilian and military purposes (hereafter: dual-use goods), whereby the term 'goods' includes commodities, tangible and intangible technologies³⁴ as well as software.³⁵ The financing of trade in such goods is not generally included in the information exchanged by the four export control regimes.

4.2.2 UN Security Council Resolutions

On 28 April 2004, the UN Security Council unanimously adopted Resolution 1540³⁶ in accordance with Chapter VII of the United Nations Charter. In this Resolution, it stated that the proliferation of nuclear, chemical and biological weapons and their delivery systems poses a threat to international peace and security. Although terrorism and the acquisition or use of weapons of mass destruction and their delivery systems by non-state proliferation actors were the main reasons this Resolution was adopted, only operative paragraphs 1 and 2 are limited to non-state actors. Operative paragraph 3d establishes the basis for all states worldwide to introduce export and transshipment controls, as Switzerland had already done prior to 2004 (see Chapter 4.2.1.). It also forms the basis of the requirement to control the financing of these trading activities.³⁷

28 The FDFA represents Swiss policy interests in the Nuclear Suppliers Group (NSG), the Australia Group (AG) and the Missile Technology Control Regime (MTCR) and SECO represents Swiss policy interests in the Wassenaar Arrangement (WA). SECO is responsible for negotiating the lists of goods for all four export control regimes in consultation with other federal offices, Swiss companies and technical experts.

29 Swiss Federal Audit Office (SFAO). *Audit des contrôles sur les biens à double usage*, p. 28.

30 NSG. *Nuclear Suppliers Group*, last checked on 5 September 2023.

31 AG. *The Australia Group*, last checked on 5 September 2023.

32 MTCR. *Missile Technology Control Regime*, last checked on 5 September 2023.

33 WA. *The Wassenaar Arrangement*, last checked on 5 September 2023.

34 Technology is defined as specific technical knowledge required for the development, production or use of a product and can be subject to authorisation in terms of technical documentation or technical support. See SR 946.202.1 - *Ordinance of 3 June 2016 on the on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods*, Goods Control Ordinance (GCO), Annex 1, status as of 1 May 2023. Likewise, the Goods Control Act defines technology as information for the development, manufacture or use of goods that is neither generally accessible nor serves the purposes of pure scientific research. See SR 946.202 - *Federal Act of 13 December 1996 on the Control of Dual-Use Goods and of Specific Military Goods*, Goods Control Act (GCA), status as of 1 July 2023.

35 Software is defined as a collection of one or more programs or microprograms stored on any tangible medium (of expression). See SR 946.202.1 - *Ordinance of 3 June 2016 on the on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods*, Goods Control Ordinance (GCO), Annex 1, status as of 1 May 2023.

36 UNSC, *Resolution 1540 (2004)*, 28 April 2004, S/RES/1540

37 S/RES/1540, OP 3: 'Establish, develop, review and maintain appropriate effective national export and transshipment controls over such items, including appropriate laws and regulations to control export, transit, transshipment and re-export and controls on providing funds and services related to such export and transshipment such as financing, and transporting that would contribute to proliferation, as well as establishing end-user controls; and establishing and enforcing appropriate criminal or civil penalties for violations of such export control laws and regulations.'

The UN Security Council has repeatedly reaffirmed these obligations on several occasions.³⁸ Since goods, natural persons, companies or organisations³⁹ are not designated in Resolution 1540, it is not a sanction resolution in the strictest sense.

The only UN Security Council Resolutions on weapons of mass destruction and their means of delivery relate to Iran and North Korea.⁴⁰ These Resolutions target specific natural persons, companies or organisations or ban certain goods (see Chapter 4.1.). Targeted sanctions are generally directed against natural persons or legal entities close to the regime that are considered a threat to international security. The aim is to prompt these parties to consider the political and economic consequences of their actions and, based on this cost-benefit analysis, to encourage the state to abandon its proliferation efforts.

North Korea withdrew from the NPT in 2003 despite years of diplomatic efforts aimed at achieving denuclearisation of the Korean peninsula. In 2006, the country conducted an underground nuclear weapons test and a series of ballistic missile tests. As a result, the UN Security Council issued nine far-reaching sanctions resolutions against North Korea.⁴¹ These severely restrict the ability of North Korea and its citizens to carry out international activities. The sanctions are intended to encourage North Korea to cease its nuclear activities and missile tests, which are in violation of international law and lead to security concerns, regional tensions and military rearmament. The targeted UN sanctions against North Korea include a goods embargo (e.g. arms, dual-use goods, raw materials, luxury goods), transport embargos, travel bans and financial sanctions. With Resolution 1718, a committee was set up to oversee the relevant sanctions measures relating to the North Korea. Comprised of all 15 members of the UN Security Council, this committee submits annual reports on its activities.⁴² In 2009, the UN Security Council established a panel of independent experts (PoE) to support the work of this sanctions committee.⁴³ Until April 2024,⁴⁴ this PoE would make recommendations on how to improve implementation of sanctions measures and prevent circumvention. The PoE also proposed sanctions lists and published half-yearly reports on implementation of resolutions on North Korea.⁴⁵ Switzerland will continue to chair the Committee on Sanctions against North Korea until the end of 2024.

Iran's nuclear ambitions resulted in the UN Security Council issuing seven Resolutions with targeted sanctions between 2006 and 2015.⁴⁶ In 2016, the UN sanctions were lifted following adoption of the Joint Comprehensive Plan of Action (JCPOA) and were replaced by temporary 'specific restrictions' in the form of bans (*de facto* sanctions) and authorisation requirements under Resolution 2231 (2015). Under the implementation timetable established for this resolution, the ban on delivery systems and the financial sanctions under the JCPOA ceased to apply on 18 October 2023 (Transition Day). After this, the authorisation requirements for nuclear goods will remain in place until 18 October 2025 (Termination Day).

38 UNSC, [Resolution 1673 \(2006\)](#), 27 April 2006, S/RES/1673; [Resolution 1810 \(2008\)](#), 25 April 2008, S/RES/1810; [Resolution 1977 \(2011\)](#), 20 April 2011, S/RES/1977; [Resolution 2325 \(2016\)](#), 15 December 2014, S/RES/2325; [Resolution 2572 \(2021\)](#), 22 April 2022, S/RES/2572; [Resolution 2622 \(2022\)](#), 25 February 2022, S/RES/2622.

39 his report consistently refers to companies and organisations, avoiding the term 'entities' used in the UNSC resolutions. The term 'organisations' includes legal entities such as associations or clubs (e.g. political parties).

40 Other UN Security Council sanctions are not related to nuclear weapons programmes. Previous sanctions against Iraq were aimed at the Iraqi chemical weapons programme. By contrast, despite the confirmed use of chemical weapons in Syria, the UN Security Council has imposed authorisation requirements for chemicals, but has not applied any corresponding sanctions on goods.

41 UNSC, [Resolution 1718 \(2006\)](#), 14 October 2006, S/RES/1718; [Resolution 1874 \(2009\)](#), 12 June 2009, S/RES/1874; [Resolution 2087 \(2013\)](#), 22 January 2013, S/RES/2087; [Resolution 2094 \(2013\)](#), 7 March 2013, S/RES/2094; [Resolution 2270 \(2016\)](#), 2 March 2016, S/RES/2270; [Resolution 2321 \(2016\)](#), 30 November 2016, S/RES/2321; [Resolution 2371 \(2017\)](#), 5 August 2017, S/RES/2371; [Resolution 2375 \(2017\)](#), 11 September 2017, S/RES/2375; [Resolution 2397 \(2017\)](#), 22 December 2017, S/RES/2397.

42 UNSC, [Annual Reports](#), Security Council Committee established pursuant to resolution 1718 (2006), last checked on 2 August 2023.

43 UNSC, [Resolution 1874 \(2009\)](#), 12 June 2009.

44 UN Meetings Coverage and Press Releases, [Security Council Fails to Extend Mandate for Expert Panel Assisting Sanctions Committee on Democratic People's Republic of Korea](#), 28 March 2024, last checked on 7 August 2024; UN News, [Top UN official calls for strict compliance with sanctions on DPR Korea](#), 28 June 2024, last checked on 8 August 2024.

45 UNSC, [Reports](#), Panel of Experts established pursuant to resolution 1718 (2006), last checked on 2 August 2023.

46 UNSC, [Resolution 1737 \(2006\)](#), 23 December 2006, S/RES/1737; [Resolution 1747 \(2007\)](#), 24 March 2007, S/RES/1747; [Resolution 1803 \(2008\)](#), 3 March 2008, S/RES/1803; [Resolution 1835 \(2008\)](#), 27 September 2008, S/RES/1835; [Resolution 1929 \(2010\)](#), 24 March 2007, S/RES/1929; [Resolution 2224 \(2015\)](#), 9 June 2015, S/RES/2224.

All corresponding transfers will still be subject to authorisation by the UN Security Council, assisted by experts from the 2231 Committee and the IAEA. Nevertheless, the United States unilaterally withdrew from the JCPOA in 2018⁴⁷ and reinstated its own sanctions. In response, Iran also ceased to implement its nuclear obligations in February 2021 at the latest and resumed enrichment of uranium to a higher grade.⁴⁸ Iran has also drawn international criticism for its continued delivery of components for ballistic missiles and unmanned aerial vehicles to Russia, in contravention of the JCPOA.⁴⁹ The European Union continued its sanctions against Iran after Transition Day, which in turn gave Switzerland the legal basis to continue its sanctions.⁵⁰ Consequently, Swiss financial intermediaries and (financial) service providers are still required to apply financial sanctions against Iran.

4.2.3 Recommendations of the Financial Action Task Force (FATF)

The FATF is an intergovernmental organisation established by the G7 in July 1989. It is the foremost international body engaged in the fight against money laundering and terrorist financing. It has issued 40 internationally recognised Recommendations⁵¹ and periodically reviews implementation by FATF member countries. The results of these country reviews and the reasons for the respective country ratings are presented and published in a report. The fourth and most recent evaluation of Switzerland was published in December 2016.⁵² Country reviews also assess the effectiveness of implementation of these Recommendations.⁵³

In 2012, the FATF added proliferation financing to its mandate. Recommendation 7 (Targeted financial sanctions related to proliferation) explicitly refers to UN Security Council Resolutions aimed at combating the proliferation and financing of weapons of mass destruction (see Chapter 4.2.2.). Countries are called upon to impose list-based targeted financial sanctions that enable funds and other assets to be frozen and forfeited so as to ensure that no financial resources are directly or indirectly made available to any person or entity designated in the targeted sanctions. The Interpretive Note to Recommendation 7, referencing Resolution 2231 and Resolution 1718 and their follow-up resolutions, clarifies that these are financial sanctions against Iran and North Korea and lists measures to be taken to implement them.⁵⁴ In addition, countries should introduce processes enabling them to propose natural persons, companies or organisations to the UN Security Council for inclusion on the sanctions lists. Assets of designated parties should be frozen and frozen transactions reported. At the same time, a legal basis is needed to remove designated natural persons, companies or organisations from lists (de-listing) and to restore their access to frozen funds.⁵⁵

47 The Trump White House Archives. *President Donald J. Trump is Ending United States Participation in an Unacceptable Iran Deal*, last checked on 5 September 2024.

48 International Atomic Energy Agency (IAEA). *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231*, Board of Governors Report, 28 February 2023, p. 2.

49 UNSC, *Fifteenth six-month report of the Facilitator on the implementation of Security Council resolution 2231*, 30 June 2023, p. 6; UN Press. *Negotiations Stall While Iran's Uranium Stockpiles Increase, Security Council Told, as Additional Allegations Frustrate Return to Joint Nuclear Plan*, 6 July 2023, last checked on 4 September 2023.

50 Although the JCPOA includes a snapback clause enabling UN sanctions to be reintroduced, this clause could not be triggered as this would require significant non-compliance with the JCPOA. See also: Brewer, Jonathan, *Proliferation Financing: The Potential Impact of the Nuclear Agreement with Iran on International Controls*, p. 33, March 2016.

51 FATF, *The FATF Recommendations*, updated November 2023.

52 FATF, *Measures to combat money laundering and the financing of terrorism and proliferation in Switzerland*, December 2016.

53 FATF, *FATF Methodology for Assessing Technical Compliance with the FATF Recommendations*, updated in June 2023.

54 FATF, *The FATF Recommendations*, updated November 2023, Interpretive Note to Recommendation 7, p. 54.

55 FATF, *The FATF Recommendations*, updated November 2023, Interpretive Note to Recommendation 7, p. 55-57.

In 2020,⁵⁶ the list-based approach set out in Recommendation 7 was supplemented with new requirements for a risk-based approach.⁵⁷ Under Recommendation 1 (Assessing risks and applying a risk-based approach) member countries, including Switzerland, are now required to conduct national risk assessments to identify, assess and understand the risk of potential breach, non-implementation or evasion of targeted financial sanctions against Iran and North Korea. The follow-up measures based on this should mitigate existing proliferation financing risks and preserve the reputation of member countries and their private sector. In Switzerland, the CGMF has been tasked with coordinating this risk analysis and any future risk analyses relating to proliferation financing. In addition, member countries are urged to require their financial intermediaries and (financial) service providers to conduct their own risk analyses.⁵⁸

In addition, Recommendation 2 (National cooperation and coordination) also requires each member country to ensure that its government agencies work together to combat proliferation financing. When doing so, each country should designate a competent authority or establish a mechanism to implement guidelines issued in relation to the identified risks.⁵⁹

4.3 National legislation

Switzerland's obligations arising from the international legal framework described above have been implemented through several federal acts and ordinances. In other words, there is no single piece of legislation devoted specifically to proliferation financing, but rather multiple pieces of legislation contain relevant provisions.

4.3.1 Embargo Act (EmbA) and ordinances on targeted measures against Iran and North Korea

Proliferation financing, referring to the breach, non-implementation or evasion of targeted financial sanctions against North Korea and Iran, is regarded as violations of the corresponding ordinances, which the Federal Council has issued on the basis of the Federal Act of 22 March 2002 on the Implementation of International Sanctions (**Embargo Act**, EmbA).⁶⁰ The Ordinance of 11 November 2015 on Measures Against the Islamic Republic of Iran (hereinafter: Iran Ordinance)⁶¹ and the Ordinance of 18 May 2016 on Measures Against the Democratic People's Republic of Korea (hereinafter: North Korea Ordinance)⁶² incorporate the provisions of international law from the relevant UN Security Council Resolutions into the Swiss legal system. Switzerland's sanctions against Iran are also based on EU sanctions. The lists of natural persons, companies and organisations provided by the UN Security Council or the relevant committee of the UN Security Council are automatically adopted.⁶³ SECO usually publishes such amendments to the annexes one working day after publication by the UN and information on current subjects of sanctions can be accessed electronically.⁶⁴ Updates are also conveyed via an email newsletter.

56 Between 2018 and 2019, a working group discussed the possibility of introducing additional measures beyond the ones mentioned in FATF Recommendation 7 'Targeted financial sanctions related to proliferation'. In 2020, the FATF member states decided that the new risk-based approach would not be applied globally, but only in the case of breach, non-implementation or evasion of targeted financial sanctions against Iran and North Korea.

57 FATF, *The FATF Recommendations*, Updated November 2023, R. 1 Para. 2; FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, Para. 1.

58 FATF, *The FATF Recommendations*, Updated November 2023, R. 1 Para 3.

59 FATF, *The FATF Recommendations*, Updated November 2023, R. 2. See also: Royal United Services Institute for Defence and Security Studies, *Countering Proliferation Finance: Implementation Guide and Model Law for Governments*, p. 25-28, 21. July 2017.

60 SR 946.231 – *Federal Act of 22 March 2002 on the Implementation of International Sanctions*, (Embargo Act, EmbA), status as of 1 August 2004.

61 SR 946.231.143.6 – *Ordinance of 11 November 2015 on Measures Against the Islamic Republic of Iran*, (Iran Ordinance), status as of 1 June 2023.

62 SR 946.231.127.6 – *Ordinance of 18 May 2016 on Measures Against the Democratic People's Republic of Korea*, (North Korea Ordinance), status as of 1 June 2023.

63 See Art. 14 of Iran Ordinance; Art. 20 para.1 of North Korea Ordinance

64 To search for subjects of sanctions, see State Secretariat for Economic Affairs (SECO), *Searching for subjects of sanctions (search engine)*

Both the Iran and North Korea Ordinances prohibit funds from being transferred to, or financial or economic resources being made available, directly or indirectly, to designated natural persons, companies and organisations.⁶⁵ Financial and economic resources belonging to or controlled by designated natural persons, companies and organisations must be frozen.⁶⁶ In the case of North Korea, financial and economic resources are also frozen if they are related to the nuclear or delivery system programme or to other activities prohibited in the North Korea Ordinance.⁶⁷ Equally prohibited in these contexts are the provision of financial services (including clearing) or financial or economic resources (including cash and gold).⁶⁸ The North Korea Ordinance also includes a ban on the provision and receipt of financial services and the provision and receipt of funds in connection with the sale, delivery, import, export and transit, transport, procurement, purchase, manufacture, maintenance and use of military goods as well as goods related to weapons of mass destruction and their delivery systems.⁶⁹ The Iran Ordinance also prohibits the sale, delivery, export, transit, development, manufacture and use of delivery systems and military goods, and requires authorisation for services relating to nuclear and dual-use goods.⁷⁰ In addition, there is an authorisation requirement for the purchase of shares or the establishment of joint ventures with Iranian persons in the nuclear field.⁷¹

Both ordinances include a duty to report to SECO. Natural persons, companies or organisations that hold or manage liquidity or are aware of economic resources that fall under the ban must immediately report these to SECO.⁷² Assets may be confiscated if it is not possible to ensure that they will be used legitimately in the future.⁷³ SECO is responsible for enforcing these ordinances and for initiating the relevant administrative criminal proceedings in the event of suspected violations.⁷⁴ Under the EmbA, SECO has the authority to request information and documents and to conduct physical inspections, even without prior notice.⁷⁵ In addition, the Office of the Attorney General of Switzerland (OAG) can open a police investigation upon request if the particular gravity of the offence justifies such action.⁷⁶ In the event of a simultaneous breach of the EmbA or of the legislation discussed in 4.3.2. below, only the criminal provision providing for the most severe penalty shall apply.⁷⁷

As a rule, all financial intermediaries or (financial) service providers must ensure compliance with the obligations arising from the EmbA, where applicable. However, the EmbA does not directly specify an obligation to analyse risks associated with a violation, circumvention or non-implementation of sanctions. As a result, SECO does not take such organisational measures into account in its inspections.⁷⁸ Under the legislative provisions on mutual legal assistance set out in the EmbA, the competent federal authorities as well as cantonal and communal police agencies are authorised to share information with one another as well as with the corresponding oversight bodies if this is necessary in order to implement the relevant legislation.⁷⁹

65 See Art. 7 para. 2 let. a of Iran Ordinance und Art. 10 para. 2 of North Korea Ordinance

66 See Art. 7 para. 1, Annexes 5-7 of Iran Ordinance; Art. 9 para. 1 and 2 of North Korea Ordinance

67 See Art. 9 para. 1 and 2 of North Korea Ordinance

68 See Art. 10 para. 1 of North Korea Ordinance

69 See Art. 5. para. 3 of North Korea Ordinance

70 See Art. 2 para. 2, Art. 4 para. 3 und Art. 3 para. 1 let. b of Iran Ordinance.

71 See Art. 6 para. 1 Iran Ordinance

72 See Art. 8 Iran Ordinance and Art. 18 of North Korea Ordinance

73 See Art. 13 EmbA

74 See Iran Ordinance. Art. 12; North Korea Ordinance, Art. 16 and 17

75 See Art. 3 and 4 EmbA

76 See Art. 14 para. 2 EmbA.

77 See Art. 11 EmbA

78 See Federal Council, *Federal Council Dispatch on Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners*, Bern, 22 May 2024, p. 21

79 See Art. 6-7 EmbA

4.3.2 Legislation on war materiel and goods control

If Switzerland joins international sanctions, the EmbA applies. However, Switzerland's obligations arising from the international treaties mentioned in Chapter 4.2.1. are implemented through several pieces of legislation. For example, the War Materiel Act (WMA) contains its own provision prohibiting proliferation financing. In addition, the the Goods Control Act (GCA) applies.⁸⁰

The *Federal Act of 13 December 1996 on War Materiel (War Materiel Act, WMA)*⁸¹ controls both the production and transfer of war materiel.⁸² Articles 8b and 8c on the financing of prohibited war materiel were added to the WMA in 2013. Article 7 WMA considers nuclear, biological and chemical weapons as well as anti-personnel mines and cluster munitions to be prohibited war materiel.⁸³ Thus, the weapons of mass destruction discussed in this report are covered by this legislation. Delivery systems that were not specifically designed or modified to transport prohibited war materiel (e.g. armed unmanned aerial vehicles or F-35 fighter jets) are non-prohibited war materiel. This is because there are no international conventions prohibiting weapons delivery systems. Accordingly, the prohibition of financing under Art. 8b and 8c does not apply to the aforementioned delivery systems.

The prohibition on financing includes the direct granting of credit, loans and gifts or comparable financial benefits used to pay or pre-pay costs and expenses associated with the development, manufacture or acquisition of prohibited weapons.⁸⁴ In addition, indirect financing (i.e. purchasing shares in companies that develop, manufacture or procure prohibited war materiel or purchasing bonds or other securities issued by such companies) is also prohibited if the aim is to circumvent the prohibition on direct financing.⁸⁵ The prohibition applies if the activity to be financed is incompatible with the NPT (see Chapter 4.2.1.). In principle, SECO is responsible for enforcing the WMA. Other federal agencies, in particular the Federal Department of Foreign Affairs (FDFA) and the Federal Department of Defence, Civil Protection and Sport (DDPS), are involved in the authorisation procedure,⁸⁶ whereas the Federal Council decides on applications that have significant foreign or security policy implications.⁸⁷ Working with police and customs authorities and the Federal Intelligence Service (FIS),⁸⁸ SECO can also conduct inspections and seize incriminating material. This power of inspection is not limited to trading companies and therefore inspections of financial intermediaries or (financial) service providers are also possible.⁸⁹ Unlike the EmbA, however, funds under Art. 8b and c WMA can be neither frozen nor forfeited. However, under Art. 35b WMA, anyone who wilfully violates the financing prohibition is liable to a custodial sentence not exceeding five years or a monetary penalty.⁹⁰ The prosecution of violations of the WMA falls under the jurisdiction of the Federal Criminal Court (FCC).⁹¹ This means that the Office of the Attorney General of Switzerland (OAG) has all the means of ordinary criminal prosecution at its disposal, including the seizure of incriminated assets and ultimately their forfeiture.⁹²

80 The Goods Control Act is only applied directly if the provisions in the EmbA, the WMA or the Nuclear Energy Act of 21 March 2003 (SR 732.1, NEA) also apply.

81 SR 514.51 – *Federal Act of 13 December 1996 on War Materiel*, (War Materiel Act, WMA), status as of 1 July 2023.

82 See Art. 5 WMA. The following are deemed to be war materiel: weapons, weapons systems, munitions and military explosives as well as equipment that has been specifically conceived or modified for use in combat or for the conduct of combat, as well as individual components and assembly packages. The Munitions List established by the Wassenaar Arrangement serves as the frame of reference.

83 See Art. 7-9 WMA. This ensures that the prohibitions set forth in the NPT, BWC, CWC as well as in the Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction (SR 0.515.092) and in the Convention on Cluster Munitions (SR 0.515.093) are implemented.

84 See Art. 8b WMA

85 See Art. 8c WMA

86 See Art. 14 para. 2 WMO

87 See Art. 29 WMA as well as Art. 14 para. 3 WMO

88 *Federal Intelligence Service (FIS)*

89 See Art. 28 para. 1-2 WMA, Art. 19 WMO

90 See Art. 35b WMA

91 See Art. 40 para. 1 WMA

92 So far, there have been no criminal proceedings in connection with Art. 35b WMA.

In Switzerland,⁹³ the export and brokering of nuclear goods, dual-use goods, special military goods and strategic goods are subject to the Federal Act of 13 December 1996 on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods (**Goods Control Act, GCA**).⁹⁴ Annexes 2 and 3 of the Ordinance of 3 June 2016 on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods (Goods Control Ordinance, GCO)⁹⁵ and Annexes 1-3 of the Ordinance of 21 August 2013 on the Control of Chemicals with Civilian and Military Uses (Chemicals Control Ordinance, ChCO)⁹⁶ contain internationally harmonised lists of goods,⁹⁷ which serve as the frame of reference for Swiss export controls for dual-use and specific military goods. SECO updates the lists contained in these Appendices whenever international export control regimes make changes to their lists. The export of designated goods is subject to an authorisation requirement, regardless of the country of destination.⁹⁸ Some of the dual-use goods that are prohibited or subject to authorisation under the Iran and North Korea Ordinances are based on the lists contained in the GCO. The authorisation procedures for dual-use goods are based on the GCA.⁹⁹ Authorisation is given either by SECO or by the Swiss Federal Office of Energy (SFOE).¹⁰⁰ Checks at the border are handled by the customs authorities.¹⁰¹ In addition, the FIS and SECO work to raise awareness within the Swiss business and research community as well as among other relevant federal offices.¹⁰²

Among other things, the control of export, transit and brokering is intended to prevent the procurement of goods that can facilitate the development, manufacture, transfer or use of weapons of mass destruction and their delivery systems.¹⁰³ Even non-designated goods are subject to an authorisation requirement if there is reason to believe that the export or brokering is related to a weapons of mass destruction programme (i.e. catch-all controls).¹⁰⁴ With catch-all controls, new technologies (high-end) can be subject to export controls. However, these controls should also hinder the circumvention of existing controls made possible through the export of standard commercial-off-the-shelf (COTS) goods¹⁰⁵ that do not meet the minimum thresholds (low-end) set out in the lists. Violations of the GCA – including unauthorised exports – must be reported. Felonies, misdemeanours and contraventions are subject to federal criminal jurisdiction and administrative offences fall within the scope of the Administrative Criminal Law Act.¹⁰⁶ SECO examines and approves applications independently or in agreement with other federal agencies, i.e. FDFA, DDPS and DETEC.¹⁰⁷

93 Cross-border movements of goods in the Principality of Liechtenstein are subject to Swiss export controls, See Art. 1 para. 2 GCO

94 SR 946.202 - *Federal Act of 13 December 1996 on the Control of Dual-Use Goods and of Specific Military Goods*, (Goods Control Act, GCA), status as of 1 July 2023

95 SR 946.202.1 – *Ordinance of 3 June 2016 on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods*, (Goods Control Ordinance, GCO), status as of 1 May 2023.

96 SR 946.202.21 - *Ordinance of 21 August 2013 on the Control of Chemicals with Civilian and Military Uses*, (Chemicals Control Ordinance, ChCO) status as of 1 November 2021

97 Lists used by the four export control regimes as well as annexes to the CWC (see 4.2.1. above).

98 See Art. 3 para. 1 GCO

99 See Annex 2 North Korea Ordinance und Annex 1-3 Iran Ordinance

100 See Art. 3 paras 1 and 2 as well as Art. 25 GCO; SECO website: *E-licensing (ELIC)*.

101 See Art. 29 para. 1 WMA and Art. 26 para. 2 GCO; also in Art. 72 para. 5 NEA; Drawing from systematic analysis of customs data, specialised units of the Federal Office for Customs and Border Security (FOCBS) provide operational staff with risk mitigation products that can be used for risk analysis and control decisions.

102 FIS, *Wirtschaftsspionage in der Schweiz*, 6 April 2023, last checked on 3 September 2024, see also FIS brochure for the private sector: *Prophylax*, 2019 and the one for the research community: *Technopol*, 2003; SECO works with relevant Swiss business and research associations (*Swissmem*, *Scienceindustries*, *swiTT*, etc.) and other stakeholders to raise awareness.

103 See Art. 6 para. 1 let. a GCO

104 Export, see Art. 3 para. 4 GCO; Transit See Art. 25 GCO; See also: Schweizerisches Bundesverwaltungsrecht, Band XI, Holzer, Patrick Edgar. Das Güterkontrollgesetz, Rz 130.

105 The term commercial-off-the-shelf (COTS) refers to mass-produced goods or software that can be used without further modification, see Glossary.

106 See Arts 14, 15, 15a and 18 GCA

107 See Art. 26 para. 1 as well as Art. 27 para. 1-3

The SFOE is the licensing authority for nuclear goods.¹⁰⁸ In the case of an individual authorisation,¹⁰⁹ the plausibility of a transfer (e.g. whether the type and number of goods match the available capacities and needs of the recipient country) and the declared intended use are taken into account. The GCA and subordinate ordinances do not contain any provisions on proliferation financing. During review of applications, financing aspects are also not considered. Nevertheless, the applicant is required to provide documents such as company profile, order confirmations, sales contracts, invoices, import certificates and end-use declaration for the review,¹¹⁰ so it is possible that SECO also receives information regarding the financial transactions. As with the EmbA, information can be shared between national and international authorities by virtue of legislative provisions on mutual legal assistance if this is necessary in order to implement the relevant legislation.¹¹¹

4.3.3 AML control system

In Switzerland, efforts to prevent money laundering and terrorist financing are based on the Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA),¹¹² the Swiss Criminal Code (SCC)¹¹³ and relevant supplementary provisions added to other pieces of legislation (see below) for the purpose of implementing international standards. The AMLA applies to all financial intermediaries,¹¹⁴ including virtual asset service providers (VASPs)¹¹⁵ as well as natural persons and legal entities that trade in goods when accepting over CHF 100,000 in cash in a given commercial transaction (dealers).¹¹⁶

The Money Laundering Reporting Office Switzerland (MROS) receives suspicious activity reports (SARs), adds further information and carries out its own analyses. It decides on a case-by-case basis whether the information obtained should be forwarded to a prosecution authority in the form of a report or whether spontaneous information should be given to a national authority or to a partner agency abroad. Financial intermediary compliance with their due diligence obligations is monitored by the Swiss Financial Market Supervisory Authority (FINMA) as well as by other oversight authorities and instances such as the Federal Gaming Board (FGB), the Federal Office for Customs and Border Security (FOCBS) or self-regulatory organisations (SROs) and supervisory organisations (SOs).

The conditions of money laundering are met when an individual takes action that is intended to prevent the identification, tracing or forfeiture of assets, with the knowledge or belief that these assets originate from a crime or qualified tax offence.¹¹⁷ Money laundering thus always requires a predicate offence, which must be a felony within the meaning of Art. 10 SCC, i.e. offences that carry a custodial sentence of more than three years.¹¹⁸ Therefore, violations of proliferation financing provisions contained in the legislation mentioned in 4.3.1. and 4.3.2. above may constitute a predicate offence to money laundering in cases where a felony has been committed.¹¹⁹

108 See Art. 3 para. 2 GCO, as well as Export Control Classification Number (ECCN) 0C001 and 0C002 in Annex 2 der GCO

109 In addition to individual export licences, there are also general export licences based on Arts 12-13 GCO.

110 See Art. 8 GCO

111 See Arts 41-42 WMA und Arts 19-20 GCA; also in Arts 102-103 NEA.

112 SR 955.0 – Federal Act of 10 October 1997 on Combating Money Laundering and Terrorist Financing, (Anti-Money Laundering Act, AMLA), status as of 23 January 2023.

113 SR 311.0 – *Swiss Criminal Code of 21 December 1937*, (Swiss Criminal Code, SCC), status as of 13 December 2022. See Art. 305bis SCC (Money laundering) as well as Art. 260quinquies para. 1 SCC (Financing terrorism)

114 See Art. 2 AMLA

115 For information on virtual asset service providers (VASPs) being subject to the AMLA, see CGMF, *National Risk Assessment (NRA) - Risk of money laundering and the financing of terrorism through crypto assets*, January 2024, p. 27ff. as well as the FINMA *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, February 2018.

116 See Art. 2 para. 1 let. B AMLA and Art. 8a AMLA

117 See Swiss Criminal Code, SCC, Art. 305 bis

118 See Art. 10 para. 2 SCC

119 See Art. 9 para. 2 EmbA, Art. 33 WMA, Art. 14 GCA; also in Art. 89 NEA. This list is not exhaustive. Based on the SCC and other federal legislation, other predicate offences may be considered that are comparable to or could be associated with proliferation financing activities.

If financial intermediaries and other market participants subject to the AMLA have reasonable grounds for suspicion that the assets are related to such a criminal offence, they are legally required to submit an SAR to MROS without delay. MROS will analyse these SARs and, if necessary, will forward them to the prosecution authorities.

Financial intermediaries and dealers falling under the scope of the AMLA are subject to various due diligence and reporting obligations.¹²⁰ Among other things, they must identify their contracting parties and determine the beneficial owners of the assets involved.¹²¹ Business relationships and transactions that carry higher risks must be documented and investigated more closely. In addition, the economic background and purpose must be investigated if a business relationship or a transaction appears unusual or if there are indications that the assets may have been acquired through criminal activity or are intended for terrorist financing.¹²² Financial intermediaries must take the necessary organisational measures to prevent money laundering and terrorist financing.¹²³ These include, in particular, the issuance of in-house guidelines, staff training and conducting audits.

In addition to the due diligence obligations under the AMLA described here, there are a number of organisational requirements under financial market legislation that are intended to ensure that supervised financial institutions adequately identify, limit and monitor all risks, including legal and reputational risks, and establish an effective internal control system.¹²⁴ This includes not only compliance with Swiss sanctions regulations, but also limiting the risks associated with the violation or circumvention of Swiss sanctions. FINMA is responsible for oversight of the organisational provisions under financial market legislation.

The Federal Council Dispatch on the Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners; Legal Entity Transparency Act (LETA) was submitted to the Swiss Parliament on 22 May 2024. Once approved, this legislation will result in these organisational measures being legally anchored in the AMLA. This would explicitly require not only the financial intermediaries subject to the AMLA, but also advisors (who are now also subject to this legislation), to take the necessary organisational measures to prevent violations of coercive measures under the EmbA. Compliance with this obligation would then be monitored by the AMLA supervisory authority.¹²⁵

120 See Art. 3, Art. 8a and Art. 9 AMLA

121 See Art. 3, Art. 4 and Art. 8a AMLA

122 See Art. 6 and Art. 8a AMLA

123 See Art. 8 AMLA

124 See SR 956.1 – [Federal Act of 22 June 2007 on Federal Financial Market Supervision](#), (Financial Market Supervision Act, FINMASA), status as of 1 January 2022; SR 952.0 – [Federal Act of 8 November 1934 on Banks and Savings Banks](#), (Banking Act, BankA), status as of 1 January 2023; SR 941.1 – [Federal Act of 15 June 2018 on Financial Institutions](#), (Financial Institutions Act, FinIA), status as of 1 January 2021; SR 961.01 – [Federal Act of 17 December 2004 on the Oversight of Insurance Companies](#) (Insurance Oversight Act, IOA), status as of 1 January 2023; SR 935.51 – [Federal Act of 29 September 2017 on Gambling](#), (Gambling Act, GambIA), status as of 1 September 2023; SR 941.31 – [Federal Act of 20 June 1933 on the Control of the Trade in Precious Metals and Precious Metal Articles](#) (Precious Metals Control Act, PMCA), status as of 1 June 2023; SR 958.1 – [Federal Act of 19 June 2015 on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading](#) (Financial Market Infrastructure Act, FinMIA), status as of 1 January 2023. SR 951.31 – [Federal Act of 23 June 2006 on Collective Capital Investment Schemes](#) (Collective Investment Schemes Act, CISA), status as of 1 January 2023. We have chosen not to list the ordinances based on these acts.

125 See Federal Council, [Federal Council adopts dispatch on strengthening anti-money laundering framework](#), Press release, 22 May 2024, last checked on 9 August 2024; as well as [Federal Council Dispatch on the Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners](#), paragraph 1.2.2.5, p. 33 and [Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners](#), (Legal Entity Transparency Act, LETA), Art. 8.

5. Objectives, methodology and data used

This chapter explains the objectives and methodology of the present risk analysis and categorises the data and information used.

5.1 Questions raised in the present risk analysis

In line with FATF Recommendation 1, the present national risk analysis is intended to strictly and exclusively assess the risk of proliferation financing in terms of the potential breach, non-implementation or evasion of targeted financial sanctions against Iran and North Korea.¹²⁶ Accordingly, the national risk analysis should answer the following questions:

- What proliferation risks exist for Switzerland, the Swiss financial centre and Swiss companies and private individuals with regard to the violation, non-implementation or circumvention of targeted financial sanctions against Iran and North Korea?
- How likely are these threats?
- Which industries and services are particularly vulnerable in this respect?
- What consequences arise from existing risks?
- Which measures are needed to keep systemic vulnerabilities in check and mitigate the residual risk? Or are existing mitigation measures adequate?

5.2 Methodology

According to international guidelines, risk analyses are iterative processes that entail a continuous review of the risk landscape. By repeating risk analyses and comparing them with prior results and assessments, new insights can be gained and more accurate assessments made. These can then be incorporated into the next analysis. Each repetition can improve the accuracy and relevance of the results.

¹²⁶ FATF, *The FATF Recommendations*, Updated November 2023, Recommendation 1: ‘Countries should also identify, assess, and understand the proliferation financing risks for the country. In the context of Recommendation 1, “proliferation financing risk” refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7.’

The method used in this report to analyse proliferation financing risks is in line with international recommendations on how to conduct national risk analyses in this area.¹²⁷ As with risk analyses for money laundering and terrorist financing, the risk analysis for proliferation financing should focus on identifying threats and vulnerabilities as well as risk-mitigating factors.¹²⁸

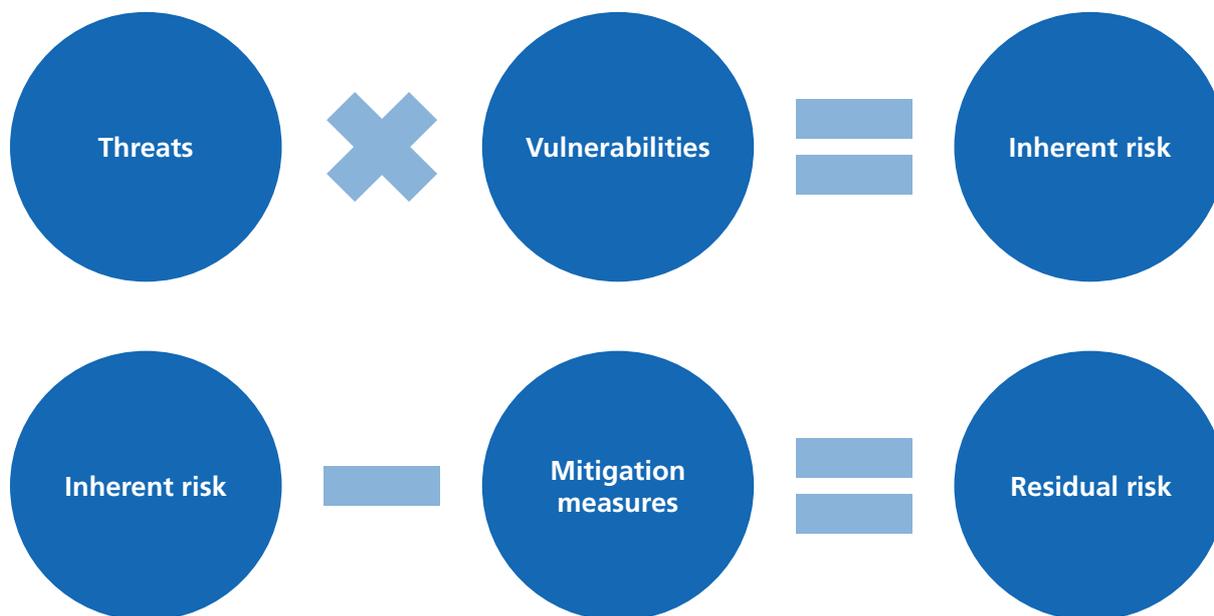


Figure 1: Simplified diagram of methodology to assess proliferation financing risks

Based on this methodology, risk arises from the interplay between three factors: threats, vulnerabilities and consequences. A distinction is drawn between inherent risks, risks prior to the introduction of mitigation measures and residual risk. To ensure a common understanding, these terms are defined in the present risk analysis as follows:

- Inherent risk is the likelihood that threats and present vulnerabilities could facilitate proliferation financing.
- Threats are the intention or ability of natural persons or legal entities to exploit the Swiss financial system in order to violate or circumvent targeted sanctions against Iran and North Korea.
- Vulnerabilities are the sum total of all structural and institutional factors that may contribute to the potential breach, non-implementation or evasion of targeted financial sanctions.
- Residual risk is the amount of risk that remains after the risk mitigation process.
- Consequences are the financing of a weapons of mass destruction programme by natural persons or legal entities based in Switzerland and the associated reputational damage.

127 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021; Royal United Services Institute for Defence and Security Studies, *Guide to Conducting a National Proliferation Financing Risk Assessment*, May 2019.

128 MROS, *Report on the national evaluation of the risks of money laundering and terrorist financing in Switzerland*, June 2015.

5.3 Data and involved parties

The FATF Recommendations provide member countries with non-binding guidelines on how to conduct their risk analyses in the area of proliferation financing. While they do not prescribe a specific risk assessment methodology,¹²⁹ member countries are encouraged to make use financial and intelligence data, law enforcement data and customs clearance documents for such analysis.¹³⁰ Switzerland has data relating to proliferation financing (see Annex 1). However, this data is not telling enough to serve as a basis for quantitative risk analysis.

Consequently, this national risk assessment is mostly limited to a qualitative analysis of proliferation financing risks. In this context, publicly available secondary sources of information on proliferation financing are compared with Switzerland's financial and/or economic situation and applicable legislation as well as with available primary data. Hypothetical risk scenarios are then developed on this basis. This should enable identification of the main inherent risks along with the economic sectors or services that are most exposed to proliferation financing risk in Switzerland. Where possible, the conclusions drawn from our analysis will include suggestions on how best to minimise existing risks.

The CGMF delegated responsibility for this national risk analysis to SECO and MROS. Several federal authorities and agencies, as well as other organisations, were involved or consulted during risk analysis, in particular SIF, FDFA, FOCBS, SFOE, FIS, FINMA, FGB, FOJ and SEM.

6. Risks associated with proliferation financing

6.1 Global risk landscape

Drawing from public sources¹³¹ this chapter will provide an overview of the current state of knowledge on proliferation financing risks. Certain threats and vulnerabilities highlighted here are global and affect all countries equally. Others arise from a specific national or regional context, for example, the exposure of a particular economic sector. This understanding will be used later to identify risks that are relevant to Switzerland (see Chapter 7).

Although this risk analysis based on the FATF Recommendation focuses on Iran and North Korea, it is worth bearing in mind that proliferation actors also use multiple procurement and revenue strategies involving global networks. State and non-state actors alike, knowingly or unknowingly, contribute to such globally active networks that seek to proliferate weapons of mass destruction. Proliferation actors use front companies (also referred to as shell or letterbox companies), joint ventures or complex and opaque ownership structures to conceal their connection to designated natural persons, companies and organisations and to procure goods or financial resources that can advance their proliferation aims. This compounds the difficulty of detecting illicit activities and creates a risk that circumstances will not be properly identified and sanctions will be violated.¹³²

129 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 7, paragraph 17.

130 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 16.

131 This includes reports on implementation of UN Security Council Resolutions, reports by the Financial Action Task Force (FATF), national risk assessments from other countries, academic papers and media reports

132 FATF, *Proliferation Financing Report*, June 2008, p. 3; FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021; Royal United Services Institute for Defence and Security Studies, *AQ Khan is Dead – Long Live the Proliferation Network*, 15 October 2021, last checked on 10 September 2024; HM Treasury, *National risk assessment of proliferation financing*, September 2021, last checked on 3 September 2024, p. 24; Royal United Services Institute for Defence and Security Studies, *Guide to Conduct a National Proliferation Financing Risk Assessment*, May 2019, p. 15. Royal United Services Institute for Defence and Security Studies, *Countering Proliferation Finance: Implementation Guide and Model Law for Governments*, p. 31-38, October 2018.

Procurements relate to listed dual-use goods as well as commercial goods that fall below the threshold values set in the lists of goods of export control regimes (commercial-off-the-shelf or COTS) and to goods from the second-hand market.¹³³ From the export control regimes it is also known that non-proliferation efforts have shifted over the years from the transfer of goods towards the transfer tangible and intangible technologies, especially in the area of science. In this context, universities and research institutes are being made aware of the problem.¹³⁴

As for proliferation financing, several areas have come to light in recent years. For example, proliferation actors generate income from the sale of commodities or arms,¹³⁵ but also from cyberattacks on crypto platforms or the misuse of virtual assets. At the same time, however, the raising of funds does not always involve illicit activities associated with money laundering.¹³⁶ One reason why proliferation actors seek to develop a wide range of sources of revenue is the need to secure financial resources for their nuclear and delivery system programmes.

International finance is particularly exposed to greater risk when conducted with countries known for proliferation or circumvention activities. This includes not just Iran and North Korea but also Pakistan and Syria. In addition, proliferation networks also operate out of neighbouring countries (China, Iraq, Russia, Turkey) or out of financial and trade hubs, especially in Asia¹³⁷ where controls are sometimes inadequate.¹³⁸ The FATF or FATF-like regional bodies in the Global Network¹³⁹ conduct country reviews on proliferation financing and publish their ratings.¹⁴⁰

133 Gouvernement de la République française, *Analyse nationale des risques de financement de la prolifération*, June 2022, last checked on 3 September 2024, p. 27

134 See, for example, for Germany: Bundesamt für Verfassungsschutz, *Proliferation. Wir haben Verantwortung*, July 2018, p. 13f; for France: Direction Générale de la Sécurité Intérieure (DGSI), *Contre prolifération des armes (online)*, last checked on 24 October 2023; for the UK: KCL, *Workshop on the implementation of non-proliferation controls in universities and research institutes*, last checked on 24 October 2023; for Switzerland: FIS, *Bekämpfung von Spionage und Proliferation: akademische Welt im Visier (online)*, last checked on 9 August 2024; FIS, *Akademische Welt im Visier*, last checked on 9 August 2024.

135 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 13-14; HM Treasury, *National risk assessment of proliferation financing*, p. 20

136 FATF, *Proliferation Financing Report*, June 2008, p. 49

137 Brewer Jonathan, *The Financing of WMD Proliferation*, November 2018, p. 16 und Annex 4. Royal United Services Institute for Defence and Security Studies, *Guide to Conduct a National Proliferation Financing Risk Assessment*, May 2019, Annex 4. Australian Government AUSTRAC, *Proliferation Financing in Australia, National Risk Assessment*, 14 December 2022, p. 26. U.S. Department of the Treasury, *National Proliferation Financing Risk Assessment*, February 2022, p. 12-15; U.S. Department of the Treasury, *2024 National Proliferation Financing Risk Assessment*, February 2024, p. 5-6 und p. 14. HM Treasury, *National risk assessment of proliferation financing*, p. 9, p. 17 and p. 22.

138 For example, Hong Kong, Malaysia and UAE in the last country review were rated as compliant; Pakistan, the Philippines, the Russian Federation, Saudi Arabia, Singapore and Turkey (as well as Germany, the United States and the United Kingdom) were rated as mostly compliant; China was rated as partly compliant; and Myanmar, which like Iran and North Korea is on the FATF's blacklist, was rated as non-compliant. FATF, *Consolidated assessment ratings*, 17 July 2024, last checked on 13 August 2024. See assessment rating for Recommendation 7.

139 FATF, *Global Network*, last checked on 7 August 2024.

140 FATF, *Consolidated assessment ratings*, 17 July 2024, last checked on 13. August 2024. See assessment rating for Recommendation 7.

In 2008, the FATF published a report to facilitate identification of potential proliferation financing activities. This report presents case studies to illustrate common techniques.¹⁴¹ The risk indicators (also known as red flag indicators) contained therein show how the international financial system is being exploited to facilitate proliferation. These indicators are very useful in enabling detection of potential proliferation financing activities in various sectors and configurations. In many of the cases presented, traditional trade finance instruments (e.g. letters of credit) were used to facilitate trade in relevant goods. In some cases, simpler methods (e.g. conventional bank transfers or large cash transactions) were used to move proliferation-related funds.¹⁴²

It is interesting to note that, due to the required documents, trade finance is no more susceptible than other financial services. The risks in trade finance arise mainly from the involvement of intermediary or correspondent banks and from forged documents.¹⁴³ In the 2021 FATF Guidance on Proliferation Financing Risks and Mitigation, indicators were broken down according to customer profile, account and type of transaction, the maritime sector and trade finance,¹⁴⁴ whereby some of the indicators could also apply to various money-laundering schemes.¹⁴⁵ The FATF Guidance also states that a single indicator may suggest the likelihood of unusual or suspicious activities. The presence of a single indicator does not necessarily justify suspicion of proliferation financing, but it could prompt further monitoring and examination. Several indicators, on the other hand, could justify a more thorough examination.¹⁴⁶

Identifying these indicators can be challenging for financial intermediaries and (financial) service providers, despite due diligence measures. In some cases, it was only through follow-up investigations that the connection was established.¹⁴⁷ Nevertheless, global examples highlight the importance of this review, as a breach of sanctions can result in serious reputational damage or even liquidation. One example is ABLV Bank, which used to be Latvia's third largest bank. It was classified as non-viable by the European Central Bank (ECB) banking regulator in February 2018 after being accused by the US Financial Crimes Enforcement Network (FinCEN) of knowingly conducting transactions on behalf of sanctioned North Korean clients. The bank was liquidated shortly thereafter.¹⁴⁸ Another notable example is that of the major French bank BNP Paribas, which had to pay a record fine of nearly USD 9 billion in 2014. The bank pleaded guilty in the US to having circumvented sanctions against Sudan, Cuba and Iran.¹⁴⁹ In this context, the Swiss Financial Market Supervisory Authority (FINMA) also conducted enforcement proceedings against BNP Paribas (Suisse) for serious violations of financial supervision legislation. FINMA found that the bank had seriously failed in its duties to identify, limit and monitor the risks involved.¹⁵⁰

141 FATF, *Proliferation Financing Report*, June 2008.

142 FATF, *Proliferation Financing Report*, June 2008, p. 24. For indicators see also: Royal United Services Institute for Defence and Security Studies, RUSI Whitehall Report 3-16, *Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Financing*, Annex 2 June 2016. Brewer, Jonathan, *The financing of nuclear and other weapons of mass destruction proliferation*, January 2018.

143 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 27.

144 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 18-21.

145 One example of this is when orders for goods are placed by companies or individuals from countries other than the country of the stated end user.

146 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 17.

147 FATF, *Proliferation Financing Report*, June 2008, p. 24.

148 European Central Bank Banking Supervision, *ECB determined ABLV Bank was failing or likely to fail*, 24 February 2018, last checked on 7 September 2023. Handelsblatt, *Ehemalige Bank ABLV aus Lettland scheitert mit Klage*, 6 May 2021, last checked on 7 September 2023.

149 Reuters, *BNP Paribas sentenced in \$8.9 billion accord over sanctions violations*, 1 May 2015, last checked on 7 September 2023.

150 FINMA, *Inadequate risk management of US sanctions: FINMA closes proceedings against BNP Paribas (Suisse)*, 1 July 2014, last checked on 3 May 2024.

6.2 Risks associated with Iran

The Iranian nuclear programme, which began in 1950, has repeatedly been the target of sanctions since the outbreak of the Iranian Revolution in 1979 and has been the subject of failed diplomatic efforts.¹⁵¹ Between 2006 and 2015, the UN Security Council passed seven targeted sanctions resolutions to prevent Iran from developing nuclear weapons. These resolutions included extensive financial sanctions.¹⁵² It is known, in particular, that Iran procured relevant goods through sophisticated proliferation networks and also made use of beneficiaries of the well-known and globally active network of A.Q. Khan.¹⁵³ The fact that such networks require access to legitimate financial service providers for their activities is illustrated by the case of the state-owned shipping company Islamic Republic of Iran Shipping Lines (IRISL). A reference to an account at a bank abroad triggered an investigation in 2010 that uncovered a global system of bank accounts that enabled IRISL's activities.¹⁵⁴ IRISL used various concealment tactics, including a network of front companies on several continents, to make it appear that its ships were under different management.¹⁵⁵

In 2016, the JCPOA replaced sanctions with temporary 'specific restrictions' (see Chapter 4.2.2.). The agreement included a procurement channel whereby the export of nuclear goods had to be submitted to the UN Security Council for approval. When the US withdrew from the JCPOA in 2018 and then reinstated sanctions, Iran was once again cut off from the global value chain and Iranian banks were disconnected from the SWIFT system.¹⁵⁶ In February 2020, the FATF once more placed Iran on the list of high-risk countries.¹⁵⁷ The JCPOA Transition Day on 18 October 2023 resulted in the lifting the ban on delivery system and the removal of financial sanctions, which are the subject of the present analysis. In response to Iran's non-compliance with several JCPOA-related obligations, several countries,¹⁵⁸ including Switzerland,¹⁵⁹ retained sanctions. The threat posed by Iran is more significant than that of North Korea because Iran still has a foothold in international finance and maintains established financial ties with other countries.

The main sectors of the Iranian economy, such as banking, energy, transport and telecommunications, as well as parts of its industrial base, are under state control or are close to the regime. The reintroduction of US sanctions has prompted the Iranian government to reduce the country's dependence on the West. Subsequently, Iran has also banned the import of more than 1,300 goods¹⁶⁰ and is increasingly focusing on self-sufficiency – including with regard to nuclear technology. Iran nevertheless continues to depend on foreign products and intermediate goods. The preferential treatment given to Iranian companies and the promotion of Iranian products and the associated legal uncertainties pose major challenges for companies operating in the Iranian market.

151 NTI, *Iran Nuclear Overview*, last checked on 10 September 2024.

152 UNSC, *Resolution 1737 (2006)*, 23 December 2006, S/RES/1737; *Resolution 1747 (2007)*, 24 March 2007, S/RES/1747; *Resolution 1803 (2008)*, 3 March 2008, S/RES/1803; *Resolution 1835 (2008)*, 27 September 2008, S/RES/1835; *Resolution 1929 (2010)*, 24 March 2010, S/RES/1929; *Resolution 2224 (2015)*, 9 June 2015, S/RES/2224.

153 SWP-Studie. *Das A Q-Khan-Netzwerk*, May 2008, last checked on 31 August 2023.

154 RUSI Journal, *Money Talks: The Surging Revolution in Counterproliferation Strategy*, December 2011, last checked on 31 August 2023.

155 IRAM Center for Iranian Studies, *Evading Sanctions via IRISL, Iran's Shipping Company - IRAM Center | Center for Iranian Studies in Ankara*, 21 April 2021, last checked on 31 August 2023.

156 The Swiss Humanitarian Trade Agreement (SHTA) was developed by Switzerland in close cooperation with the relevant authorities in the US and Iran, as well as with selected Swiss banks for the purpose of facilitating the delivery of humanitarian goods to Iran. In effect since 27 February 2020, the SHTA has provided Swiss-based exporters and trading companies in the food, pharmaceutical and medical sectors with a secure payment channel through a Swiss bank, thereby facilitating the delivery of humanitarian goods. Moreover, the agricultural sector has not been affected by sanctions and thus trade in this sector is generally possible. So far, only four transactions totalling around CHF 4.5 million have been processed through the SHTA.

157 FATF, *High-Risk Jurisdictions subject to a Call for Action*, updated in June 2023, last checked on 07 September 2023.

158 For example, all EU member states as well as Japan, Canada, South Korea, the United States and the United Kingdom.

159 SECO, *Switzerland retains measures linked to Iran's nuclear programme*, 5 January 2024

160 Switzerland Global Enterprise, *Iran bans the import of more than 1,300 products*, last checked on 28 August 2023.

Complex ownership structures make it difficult to determine which natural persons, companies and organisations are involved in any given transaction. For example, the Iranian Islamic Revolutionary Guard Corps, is de facto active in all Iranian economic sectors, also in the key oil and gas sector.¹⁶¹

Iran has achieved greater independence from the West by developing economic (and strategic) ties with Russia and China. Iran's main sources of income are the export of crude oil and natural gas (with Iran holding 10-20% of global reserves) and petrochemical products. Iran predominantly exports to China, with which it signed a comprehensive cooperation agreement in March 2021, followed by exports to neighbouring Turkey and Iraq. Although Russian and Iranian oil and gas fields compete with one another, Iran and Russia have expressed an interest in strategic cooperation. This is partly explained by the fact that Russian oil production companies operate Iranian oil fields and oil-gas exchange arrangements are in place.¹⁶² Since the start of the war in Ukraine, Russia and Iran have also joined forces in the grain trade. In addition, a free trade agreement between the Eurasian Economic Union (EAEU)¹⁶³ and Iran will soon come into force.¹⁶⁴ Proceeds from these trade activities may be used for Iran's proliferation financing efforts. It should also be mentioned that in February 2023, Iran and Russia agreed to link their national systems for electronic interbank transactions in order to bypass the US-controlled SWIFT network and sanctions.¹⁶⁵

In order to gain access to the global market and circumvent economic sanctions, cryptocurrency mining is also used in Iran. The cryptocurrencies mined in Iran are transferred to accounts held with the Central Bank of Iran and are used to finance both legal and illegal imports.¹⁶⁶ Although no specific cases of Iranian use of cryptocurrencies for proliferation purposes are known, it is possible that cryptocurrencies could be used in this manner.

The importance of crude oil and natural gas for Iran also means that trade in commodities can be misused to raise funds that are then channelled to finance Iran's nuclear and delivery system programmes. In order to circumvent sanctions and maintain its oil exports, Iran maintains a shadow fleet of oil tankers owned by front companies to transport oil under false flags.¹⁶⁷ Consequently, there is a risk in the shipping industry that designated natural persons, companies and organisations will circumvent the sanctions by using front companies or falsifying their names and documents. Here too, there are reputational risks and a risk of secondary sanctions, as illustrated by the example of Naftiran Intertrade Co. (NICO) Sàrl, an Iranian subsidiary of the Iranian state-owned oil company in the canton of Vaud, which is involved in oil and gas trading.¹⁶⁸

161 Wehrey, Frederic, et al. *Economic Expansion: The IRGC's Business Conglomerate and Public Works*. The Rise of the Pasdaran: Assessing the Domestic Roles of Iran's Islamic Revolutionary Guards Corps, RAND Corporation, 2009, p. 55–76. JSTOR, last checked on 18 July 2023. See also Khalaji, Mehdi. *Iran's Revolutionary Guards Corps, Inc. Brief Analysis*, The Washington Institute, 17 August 2007, last checked on 18 July 2023. Reuters. *U.S. blacklist oil shipping network allegedly run by Iran Revolutionary Guards*, 4 September 2019, last checked on 18 July 2023.

162 Zeit Online, *Treffen in Teheran: Russland, die Türkei und der Iran wollen in Syrien zusammenarbeiten*, 19 July 2022, last checked on 28 August 2023; IRAM Center for Iranian Studies. *New Details of Iran-Russia Energy Agreement and the Predictions*, 29 August 2022, last checked on 28 August 2023. The Central Asia-Caucasus Analyst. *Iran and Russia: from 'Oil-for-Goods Swap' to 'Oil-Gas Swap'*, 17 January 2023, last checked on 28 August 2023.

163 EAEU. *Eurasian Economic Union*, last checked on 12 September 2023. The EAEU is comprised of five member states: Armenia, Belarus, Kazakhstan, Kyrgyzstan and Russia.

164 EURACTIV, *Russia to attach Iran to its Eurasian Economic Union* 19 June 2023, last checked on 28. August 2023.

165 Russia Briefing. *Russia and Iran Connect Financial Payment Systems*, 30 January 2023, last checked on 28 August 2023.

166 Elliptic, *How Iran Uses Bitcoin Mining to Evade Sanctions and 'Export' Millions of Barrels of Oil*, May 2021, last checked on 27 November 2023. Arab News, *How Iran is cashing in on cryptocurrencies to evade US sanctions*, November 2022, last checked on 27 November 2023.

167 Financial Times, *Iran's 'ghost fleet' switches into Russian oil*, February 2023, last checked on 27 November 2023.

168 U.S. Department of the Treasury, *OFAC Identifies Entities Owned or Controlled by the Government of Iran*, 26 November 2008, there are also several media reports, e.g. NZZ. *Handel mit iranischem Erdöl*, 17 September 2012, last checked on 18 July 2023.

The UN Secretary-General's reports on implementation of the JCPOA contain information on reported violations.¹⁶⁹ Recent reports concerned violations related to Iran's deliveries of unmanned aerial vehicles to Russia.¹⁷⁰ In 2021, asset freeze violations were reported in connection with two Iranian companies, one of which was involved in international trade and the other in the provision of services related to the manufacture, installation, commissioning, repair and maintenance of machinery, tools and industrial equipment.¹⁷¹

As a result of US sanctions and strict government control of the export and transit of goods, as well as the countries desire to reduce its dependence on the West, Iran has increased its procurement of nuclear expertise. With the help of selected students and scientists, Iran has managed to secure access to nuclear-relevant knowledge at international technical universities, which has provided it with insights needed to advance its own nuclear research. Information on how such technology transfers are financed is largely unavailable. Nevertheless, individual cases are known where Iranian individuals and other nationals have been paid to transfer specific technical knowledge¹⁷², also with large sums of cash.¹⁷³ In so doing, they became guilty of proliferation financing.

Iran continues to pursue weapons of mass destruction and now has the potential for a nuclear weapons breakout, characterised by the enrichment of weapons-grade uranium, together with and significant ballistic missile capabilities.

6.3 Risks associated with North Korea

Comprehensive sanctions have severed North Korea's ties to world trade and financial markets. It has responded by engaging in a wide range of illegal activities to maintain and finance its nuclear weapons and delivery system programme. This includes the theft of cryptocurrencies, money laundering of crypto and fiat currencies, hacking, extortion, insurance fraud, trade in narcotics, wild animals and weapons, smuggling and forced labour. In addition, there are commercial activities that would be legitimate in the absence of sanctions, first and foremost the sale of mineral raw materials (e.g. coal, sand or gold) or commercial fishing.¹⁷⁴ North Korea also uses foreign investment and companies run by North Korean nationals abroad to generate income. For these and other reasons, North Korea is on the FATF's list of high-risk countries.¹⁷⁵

As described in Chapter 6.1, North Korea also maintains a global network of front companies with complex structures to conceal the North Korean origin of companies or goods.¹⁷⁶ Revenues from these transactions are highly likely to flow to Central Committee Bureau 39 (Bureau 39), which raises funds on behalf of Kim Jong Un for use in the North Korean nuclear weapons and delivery system programmes.¹⁷⁷

169 UN documents on Iran: *Secretary-General's Reports*.

170 Security Council Report, *S/2022/912*, p. 5, last checked on 28 August 2023. Security Council Report, *S/2023/473*, p. 5-6, last checked on 3 May 2024. Conflict Armament Research, *Dissecting Iranian drones employed by Russia in Ukraine*, November 2022, last checked on 3 May 2024. Yermak-McFaul, International Working Group on Russian Sanctions & KSE Institute, *Foreign Components in Russian Military Drones*, 23 August 2023, last checked on 3 May 2024. U.S. Intelligence Agency, *Iranian UAVs in Ukraine: A Visual Comparison*, August 2023, last checked on 3 May 2024.

171 Security Council Report, *S/2021/995*, p. 6, last checked on 28 August 2023.

172 The specific technical expertise required for the development, manufacture and use of a product can be transferred in the form of technical documentation (e.g. plans, diagrams) or technical support (e.g. instruction, imparting skills).

173 Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB), Secrétariat général de la défense et de la sécurité nationale (SGDSN). *Analyse nationale des risques de financement de la prolifération (ANR-FP)*, 2022, p. 29.

174 RUSI. *Guide to conducting a national proliferation financing risk assessment*, May 2019, last checked on 3 September 2024, p. 14, p. 17-18.

175 FATF, *High-Risk Jurisdictions subject to a Call for Action*, updated in June 2023, last checked on 7 September 2023. North Korean origin of companies or goods

176 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 15. Stewart, Shannon R., DPRK Overseas Financial Networks, June 2021, p. 121.

177 Radio Free Asia. *North Korean bandits steal 200 kilos of gold bars worth US \$12 million*, 22 December 2022, last checked on 4 September 2023; Financial Times. *North Korea: The secrets of Office 39*, 24 June 2015, last checked on 5 September 2024; Reuters. *Factbox. North Korea's shady 'Office 39'*, World News, 19 November 2010, last checked on 5 September 2024; Time. *Kim Yo-Jong's Links to North Korea's Secretive Office 39*, 29 April 2020, last checked on 5 September 2024.

All financial intermediaries and (financial) service providers, including VASPs,¹⁷⁸ which we will cover in the following chapter, run the risk of establishing a business relationship with one of these front companies. For example, insurance companies controlled by North Korea can submit false claims for compensation in order to collect large sums of money from reinsurance companies.¹⁷⁹

North Korea also uses cyberattacks on traditional financial service providers and VASPs to raise foreign funds. North Korean state-sponsored hacking groups have been behind high-profile cyberattacks such as the 2016 attack on Bangladesh's central bank,¹⁸⁰ as well as the WannaCry ransomware attack in 2017, Axie Infinity's Ronin Bridge exploit in 2022 and other hacks against financial service providers.¹⁸¹ North Korea's cyber capabilities are said to be concentrated in the Reconnaissance General Bureau (RGB), which is the country's premiere military intelligence service.¹⁸² Large-scale attacks on VASPs could earn North Korea significant sums in cryptocurrencies, which, unlike traditional currencies or bank accounts, are difficult to freeze or confiscate. Protection against third-party access, the ability to conceal payments, and the speed of transactions makes cryptocurrencies particularly appealing to North Korea as a means of storing assets for future use.¹⁸³ In 2022 alone, North Korean hacker groups are said to have stolen cryptocurrencies valued at over USD 1.7 billion – nearly half of all cryptocurrencies stolen that year.¹⁸⁴ From January to September 2023, over USD 340 million in losses were reported, which corresponds to roughly 30% of all crypto thefts during this period.¹⁸⁵

In addition to hacking crypto platforms to steal cryptocurrencies, North Korean cyber actors also misuse these platforms to exchange the stolen cryptocurrencies online into fiat currency or other cryptocurrencies. By using anonymous cryptocurrencies (e.g. Monero) and cryptocurrency mixers (e.g. Tornado Cash), North Korea can hide the origin and destination of its cryptocurrency transactions, i.e. launder funds used to support the North Korean weapons programme. In doing so, it appears to deliberately select financial service providers in jurisdictions with weak or non-existent AML control systems when converting crypto to fiat currency. North Korea is also involved in cryptocurrency mining and cryptojacking operations: It is suspected that North Korea has used electricity and computer resources stolen through cryptojacking¹⁸⁶ to mine Bitcoin and other cryptocurrencies, which it has then been able to sell at a profit on the global market.¹⁸⁷

178 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 27-28

179 HM Treasury, *National risk assessment of proliferation financing*, p. 15; The Guardian. *UK freezes assets of North Korean company based in south London*, 23 April 2017, last checked on 3 September 2024.

180 BBC News, *The Lazarus heist: How North Korea almost pulled off a billion-dollar hack*, 21 June 2021, last checked on 3 September 2024.

181 Panel of Experts. *Midterm Report of the Panel of Experts of the 1718 DPRK Sanctions Committee*, 30 August 2019, last checked on 27 March 2023.

182 Panel of Experts. Final Report of the Panel of Experts of the 1718 DPRK Sanctions Committee, 4 March 2021, p. 306, last checked on 27 March 2023. Office of the US Secretary of Defense. *Military and Security Developments Involving the Democratic People's Republic of Korea*, 15 December 2017, last checked on 27 March 2023

183 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 28. Chainalysis. The Chainalysis 2023 Crypto Crime Report, February 2023, last checked on 27 March 2023. The Diplomat. *How the North Korean Government Is Squeezing Foreign Currency Out of Its People*, 13 August 2022, last checked on 12 September 2023.

184 The total value of all cryptocurrencies stolen in 2022 amounts to USD 3.8 billion. See Chainalysis, The 2023 Crypto Crime Report, February 2023, p. 56-60, last checked on 27 March 2023.

185 See Chainalysis, *Russian and North Korean Cyberattack Infrastructure Converge: New Hacking Data Raises National Security Concerns*, last checked on 25 October 2023.

186 Cryptojacking refers to the unauthorised use of devices (computers, smartphones, tablets or even servers) by cybercriminals for the purpose of mining cryptocurrencies. Mining cryptocurrencies requires a significant amount of computing power and electricity, which can be very expensive. Cryptojacking allows hackers to mine cryptocurrencies without having to bear these costs themselves, by hijacking computing resources from their victims' devices.

187 Panel of Experts. *Midterm Report of the Panel of Experts of the 1718 DPRK Sanctions Committee*, 28 August 2020, last checked on 27 March 2023. FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 28.

North Korean arms production and related exports also serve as a source of funding for its nuclear weapons and delivery system programmes. Arms, in particular missiles, but also nuclear technology, are supplied to the Middle East (e.g. to Iran, Syria or Egypt) as well as to non-state actors.¹⁸⁸ Other sources claim that several countries on the African continent and in Southeast Asia are the destination countries for these exports.¹⁸⁹ Current discussions revolve around the delivery of arms to Russia¹⁹⁰ in exchange for the delivery of Russian crude oil to North Korea.¹⁹¹

North Korea has mining resources such as gold, silver, iron ore, coal and another 200 minerals, which are estimated to be worth seven trillion dollars. Sanctions prevent these resources from being mined by foreign companies or exported by North Korea.¹⁹² Despite this, reports from public sources indicate that coal is being smuggled to China, Russia and other recipient countries.¹⁹³ There are also reports of sand being sold to China.¹⁹⁴ North Korea is further suspected of using the gold trade to circumvent sanctions, although the country is said to produce only two tonnes of gold annually.¹⁹⁵ In 2014, during an investigation of gold from the Democratic Republic of the Congo, it was discovered by chance that dozens of multinational companies were using North Korean gold in their electrical products.¹⁹⁶ It is suspected that this gold, like other minerals, is smuggled via China.¹⁹⁷

North Korean diplomats are also involved in the smuggling business. For example, diplomats have been accused of illegally trading in rhino horn and ivory.¹⁹⁸ Likewise, impounded diplomatic bags destined for North Korea were found to contain large amounts of cash, gold, other valuables and luxury goods, including watches¹⁹⁹ as well as alcohol, tobacco and drugs.²⁰⁰ In order to generate additional state revenue, North Korea also uses forced labourers abroad who receive only a portion of their wages to cover their living expenses.

188 YaleGlobal Online, *North Korea's Missile Trade Helps Fund Its Nuclear Program*, 5 May 2003, last checked on 5 September 2024; Middle East Eye, *North Korea's enigmatic role in the Middle East arms market*, 20 January 2023, last checked on 5 September 2024; 38 North, *The North Korean-Syrian Partnership: Bright Prospects Ahead*, 21 March 2021, last checked on 5 September 2024.

189 Royal United Services Institute for Defence and Security Studies. *Target Markets: North Korea's Military Customers in the Sanctions Era*, 8 December 2015, last checked on 5 September 2024.

190 The New York Times, *Kim Jong-un and Putin Plan to Meet in Russia to Discuss Weapons*, 4 September 2023, last checked on 5 September 2024; SRF, *Treffen zwischen Putin und Kim - So realistisch sind nordkoreanische Waffenlieferungen an Russland*, 6 September 2023, last checked on 5 September 2024. Conflict Armament Research, *Documenting a North Korean missile in Ukraine*, January 2024, last checked on 5 September 2024.

191 Radio Free Asia. *Russia resumed shipments of oil to North Korea in December, UN data shows*, 6 June 2023, last checked on 7 September 2023; Reuters, *Russia resumes oil exports to North Korea after long pause*, 14 June 2023, last checked on 7 September 2023.

192 Stimson. *North Korea's Komdok Mining Region: Empty Promises?*, 17 August 2022, last checked on 5 September 2024. WirtschaftsWoche, *Bodenschätze im Wert von sieben Billionen US-Dollar*, last checked on 5 September 2024.

193 Radio Free Asia. *North Korean Traders Smuggle Coal to Power-Short China*, 11 October 2021, last checked on 5 September 2024; Indo-Pacific Defense. *Countering North Korean Sanctions Evasion*, 3 August 2020, last checked on 5 September 2024; Korea Economic Institute of America. *North Korean Sanctions Evasion: The UN Panel of Experts Report*, 1 June 2021, last checked on 5 September 2024.

194 CNN Business. *North Korea is making millions selling sand*, 10 June 2020, last checked on 5 September 2024.

195 CEIC. *North Korea Gold Production, 1990 – 2022*, last checked on 18 August 2024. Reuters. *The Cold Frontier: Dreams of Gold*, 12 April 2018, last checked on 5 September 2024.

196 Supply Chain 24/7. *Dozens of Companies Report North Korea Gold Used In Their Supply Chain*, 4 June 2014, last checked on 7 September 2023; The New Yorker, *The Puzzle Over North Korean Gold*, 4 August 2014, last checked on 7 September 2023.

197 Radio Free Asia. *To make extra money, North Koreans pay big bribes for gold refinery jobs*, 22 August 2023, last checked on 7 September 2023

198 National Geographic. *North Korean Diplomats Accused of Smuggling Ivory and Rhino Horn*, 16 October 2017, last checked on 7 September 2023.

199 Wilson Center. North Korea, the Smuggler State, last checked on 7 September 2023. FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 25.

200 Wilson Center. North Korea, the Smuggler State, last checked on 7 September 2023. FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 25.

Such forced labourers are primarily employed in Russia and China, but can also be found on the African continent and in Europe, for example in Poland and the Czech Republic.²⁰¹ They are active in a range of sectors, and are also prominent in China's textile industry²⁰² or build prestigious structures such as museums or monuments in Africa.²⁰³ This is despite the fact that the granting of work permits is prohibited under UN Security Council Resolutions and North Korean workers abroad should have been returned to their home country by 22 December 2019.²⁰⁴ North Korea has always operated hotels, youth hostels, casinos, travel agencies, restaurants and bars to generate income.²⁰⁵ In 2015, the country was represented at Bern's holiday fair.²⁰⁶ The majority of North Korean restaurants are located in China and other Asian countries, but they can also be found in Europe, where the presence of North Korean citizens in the country increases²⁰⁷ the risk that the system will be used for smuggling purposes or that state revenue will be misused.²⁰⁸

7. Risks for Switzerland

This chapter elaborates on the proliferation risks posed by Iran and North Korea, which were presented in Chapter 6, placing them in the context of Swiss financial and economic activities. The following is an overview of the most important and most exposed sectors for this analysis. Ten inherent risks were identified and are described using hypothetical scenarios. These scenarios then serve as the basis for assessment of proliferation risks for Switzerland.

7.1 Importance and exposure of sectors

Switzerland is one of the global financial centres. Around a quarter of the world's cross-border assets are managed in Switzerland.²⁰⁹ This makes Switzerland a global leader in offshore wealth management.²¹⁰ The Swiss financial centre is also an important location for trade finance and one of the world's most important locations for insurance and reinsurance.²¹¹ The level of vulnerability of the Swiss financial centre increases due to the broad range of financial products offered in Switzerland. Proliferation financing risks can arise for the Swiss financial centre through the direct or indirect provision of financial or economic resources and through the provision and use of financial services (see definition in Chapter 4.1.).

201 Arterburn, Jason. *Dispatched: Mapping Overseas Forced Labor in North Korea's Proliferation Finance System*. C4ADS Report. 2018, p. 13-14; Breuker. *People For Profit*, 2018

202 Reuters. *North Korea factories humming with 'Made in China' clothes, traders say*, Business News, 13 August 2017, last checked on 5 September 2024.

203 RUSI. *Guide to conducting a national proliferation financing risk assessment*, p. 19. Die Weltwoche. *Nordkorea in Afrika*, 15 January 2023, last checked on 17 July 2023; Vice. *Warum Nordkorea in Afrika riesige Denkmäler für Diktatoren baut*, 6 February 2018, last checked on 17 July 2023; Panel of Experts. *Final Report of the Panel of Experts of the 1718 DPRK Sanctions Committee*, 4 March 2021, last checked on 27 March 2023.

204 Implemented in SR 946.231.127.6 – *Ordinance of 18 May 2016 on Measures Against the Democratic People's Republic of Korea*, (North Korea Ordinance), status as of 1 June 2023, Art. 2a.

205 NK News. *North Korean spy ran hotels, casinos and travel agency in Cambodia: UN report*, 15 February 2022, last checked on 27 March 2023, DW. *Umstrittenes Berliner Hostel endgültig dicht?*, 28 March 2020, last checked on 4 September 2023

206 Berner Zeitung, *Nordkorea an der Berner Ferienmesse*, 6 January 2015, last checked on 7 September 2023.

207 To cite one example, in 2021 Swiss financial intermediaries reported a client who had been known for his smuggling activities in connection with North Korea since the 1990s

208 RUSI. *Guide to conducting a national proliferation financing risk assessment*, p. 19.

209 Federal Department of Foreign Affairs (FDFA), Swiss financial centre, last checked on 27 November 2023.

210 SWI swissinfo.ch, *Switzerland's global wealth crown up for grabs*, 7 August 2023, last checked on 12 September 2023.

211 SIF, *Swiss financial centre, Key figures April 2023*, last checked on 27 November 2023. S-GE: *Switzerland is the world's third-largest reinsurance location*, 13 February 2023, last checked on 12 September 2023. Federal Department of Foreign Affairs (FDFA), Swiss financial centre, last checked on 27 November 2023.

In principle, services such as trade financing, open account transactions,²¹² correspondent banking and virtual asset transactions can be misused for proliferation financing purposes.²¹³ In addition to traditional banking, this may also include offshore wealth management and reinsurance. Furthermore, the parabanking sector (e.g. portfolio manager, lawyers or notaries who carry out financial transactions) may be exposed to this risk they are not subject to AMLA provisions (as natural persons or legal entities) when facilitating financial transactions.²¹⁴ Similarly, the 200+ financial intermediaries in Switzerland engaging in VASP activities are exposed to the risk of misuse.²¹⁵

Furthermore, with 900 companies, Switzerland is one of the largest commodity trading centres in the world. It is a significant trading centres for crude oil, metals, minerals and agricultural products. In 2016, the trading volume of the five largest trading companies in Switzerland amounted to 18 million barrels of crude oil per day, which corresponds to around 20% of global demand. The most commonly traded commodities in Switzerland are energy commodities (crude oil, diesel, natural gas, coal, etc.), metals (iron, copper, gold, etc.) and agricultural commodities (coffee, cocoa, grain, etc.). A large portion – between one-third and two-thirds – of global trade in these goods is handled by companies in Switzerland.²¹⁶ A highly innovative country,²¹⁷ Switzerland is also a key trading partner and major research location for dual-use goods, particularly with regard to their components and technologies. The industries most affected by sanctions and export controls are the machinery, electrical engineering and metals (MEM) industries, whose exports in 2022 totalled CHF 72.3 billion,²¹⁸ as well as the pharmaceutical industry, which has an export turnover of CHF 134.5 billion.²¹⁹ The direct added value generated by the manufacturers of dual-use goods is CHF 829 million.²²⁰ Proliferation financing risks arise in trade finance, in commodity trading and trading in dual-use goods. Switzerland is also one of the major gold refining centres. Five of the world's top nine industrial leaders conduct a large part of their business in Switzerland. Swiss refineries account for roughly 70% of total global capacity. Refineries transform raw or recycled gold into gold products.²²¹ The origin of gold imported into Switzerland is also relevant in the context of proliferation.

212 An open account transaction in international trade is a sale where goods are produced, shipped and delivered by an exporter to an importer before payment is due. Such transactions are arranged directly between the seller and buyer without the involvement of intermediary banks and without the risk-mitigating effect of documentary protection such as a letter of credit or bank guarantee.

213 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, p. 27-28. See also: Royal United Services Institute for Defence and Security Studies, RUSI Guidance Paper, *Countering Proliferation Finance: An Introductory Guide for Financial Institutions*, April 2017, p. 12. Brewer, Jonathan, *Basic Principles for Conducting Financing-of-Proliferation Risk Assessments*, Center for a New American Security, p. 9, 1. November 2018

214 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021, *ibid.*

215 In January 2024, the CGMF published a specific risk analysis of money laundering and terrorist financing involving virtual assets (VAs) and virtual asset service providers (VASPs). The conclusions drawn in this report are also largely applicable to proliferation financing risks. See: Federal Office of Police fedpol, *National Risk Assessment (NRA) - Risk of money laundering and the financing of terrorism through crypto assets*, January 2024.

216 Federal Council, *Rohstoffsektor Schweiz: Standortbestimmung und Perspektiven*, November 2018, p. 12-13.

217 WIPO, *Global Innovation Index 2023: Switzerland, Sweden and the U.S. lead the Global Innovation Ranking; Innovation Robust but Startup Funding Increasingly Uncertain*, 27 September 2023, last checked on 5 January 2024

218 Swissmem. *Kennzahlen 2022 - Panorama*, last checked on 8 September 2023; Federal Office for Customs and Border Security (FOCBS). *Anteil der MEM-Exporte im Aussenhandel innert 25 Jahren deutlich gesunken*, 6 July 2023, last checked on 5 September 2024.

219 Scienceindustries. *Swiss foreign trade: Chemistry pharma life sciences are export champions*, 24 January 2023, last checked on 8 September 2023.

220 BAK, *Die volkswirtschaftliche Bedeutung der Schweizer Rüstungs- und der Dual-Use Industrie*, 17 February 2023, last checked on 5 January 2024.

221 See Federal Council Report in fulfilment of Recordon Postulate 15.3877, Goldhandel und Verletzung der Menschenrechte, 21 September 2015, last checked on 3 May 2024. See also SRF. *Goldhandel im Zwielicht - Die Schweiz tut sich schwer mit Gesetzesverschärfungen zum Gold*, last checked on 8 September 2023; Swissgoldsafe, *Edelmetall-Raffinerien in der Schweiz und weltweit*, updated 6 June 2024, last checked on 8 August 2024.

7.2 Assessment of proliferation financing risks

Based on Chapter 6 and 7.1. above, the CGMF's risk analysis²²² subgroup identified the following 12 hypothetical risk scenarios affecting sectors and services that are both important in Switzerland and possibly exposed to proliferation financing risk relating to Iran or North Korea:

1. Intentional breach of sanctions
2. Negligent breach of sanctions
3. Failure to identify assets or companies controlled by designated persons
4. Accepting proceeds from the transfer of goods (domestic element)
5. Accepting proceeds from the transfer of goods (foreign element)
6. Accepting proceeds from the transfer of technology
7. Concealment through legal entities (front companies)
8. Concealment through correspondent banking
9. Raising funds from stolen cryptocurrencies
10. Concealment through trade or transport financing
11. Raising funds from commodity trading
12. Raising funds from the sale of refined gold

Given the limited data available, only a qualitative risk analysis is possible. The risk scenarios presented here are hypothetical and not based on specific data or concrete evidence. Risks are only assessed in relation to one another and our analysis does not compare risks in Switzerland with those in other countries.

7.2.1 Risks 1 and 2: Intentional or negligent breach of sanctions

A natural person, company or organisation that has been added to the UN Security Council's sanctions list holds financial or economic resources in Switzerland. The financial intermediary does not freeze the funds in a timely fashion and these funds are used for the Iranian or North Korean missile or nuclear weapons programme.

A natural person, company or organisation that is added to the UN Security Council sanctions list has a strong incentive to withdraw financial or economic resources from Switzerland before they are frozen. Therefore, the threat is that financial intermediaries may violate Swiss sanctions. The vulnerability is due to Switzerland's exposure in the international financial markets and its role in global wealth management. Sanctions against Iran and North Korea have been in place for many years, and Swiss financial intermediaries and (financial) service providers are aware of their obligations arising from the Embargo Act. In Switzerland, there are no known cases to date where financial or economic resources have not been frozen or were frozen too late in relation to Iran or North Korea. The fact that the AML control system includes due diligence obligations and organisational measures is a risk-mitigating factor that also helps in the fight against proliferation financing. Responsibilities are laid out in company policies, and regular sanctions screening is carried out to prevent violations of the law and minimise reputational risk. Although the authorities have not specifically raised awareness of proliferation financing issues, since February 2022, awareness was raised in the context of the sanctions against Russia, and warnings have been given regarding the possible consequences of non-compliance in general. Finally, risk is mitigated even further by the fact that lists issued or updated by the UN Security Council regarding natural persons, companies and organisations are automatically applied. There is therefore no time lag between the inclusion of a natural person, company or organisation on the UN Security Council's sanctions list and the resulting legally effective obligation to freeze assets in Switzerland. While a residual risk cannot be ruled out, the risk of a negligent breach (e.g. due to organisational failings, human or technical errors) is deemed greater than the risk of an intentional breach.

222 SIF, *Mandate of the CGMF*, last checked on 8 September 2023.

7.2.2 Risk 3: Failure to identify assets or companies controlled by designated persons

A natural person, company or organisation that has been added to the UN Security Council's sanctions list indirectly holds financial or economic resources in Switzerland. Despite correct implementation of AMLA due diligence obligations and other clarifications, forged documents prevent the financial intermediary from recognising that its contracting party is controlled by a person on the UN Security Council's sanctions list. The financial intermediary fails to freeze the funds and allows them to be transferred for use in the Iranian or North Korean missile or nuclear weapons programme.

The threat remains that natural persons, companies or organisations indirectly hold financial or economic resources in Switzerland that have not been identified or frozen. Here too, the vulnerability is due to Switzerland's prominent position on international financial markets and the Swiss financial sector's dominance in global wealth management. Indicators for proliferation financing do not necessarily differ from those of other suspected cases of money laundering. The use of front companies and possibly forged documents make identification more difficult. In addition, the actual origin of a customer can be concealed when a business relationship is established by using what are known as 'golden passports'.²²³ In addition, financial agents, known as 'money mules', can receive illicitly obtained money in their account and transfer it abroad. Irrespective of Iran and North Korea, there have been cases in which financial intermediaries were unable to properly identify the beneficial owners of business relationships as a result of false statements and forged documents. However, existing legal measures that can be applied in the event of violations are risk-mitigating factor. The associated consequences set out in Swiss financial market oversight legislation and in the Swiss Criminal Code encourage correct implementation of the existing legal framework. However, a residual risk remains that correct identification does not take place and sanctions are violated. In the context of this risk analysis, this risk is considered greater than the aforementioned risk of violation of sanctions in cases where designated natural persons, companies or organisations hold funds directly in Switzerland (see Chapter 7.3.1).

7.2.3 Risks 4 and 5: Accepting proceeds from the transfer of goods

A Swiss financial intermediary receives a payment into the account of a Swiss or foreign company that manufactures dual-use goods and knowingly or unknowingly sells them to North Korea or Iran, or its intermediaries.

Iran and North Korea still rely on goods from abroad for their nuclear and delivery system programmes. Applications for export licences to Iran that were approved or rejected by SECO or withdrawn by customers (see Annex 1) suggest that Iran intends to continue to procure goods from Switzerland. The threat here is that Swiss financial intermediaries and (financial) service providers accept proceeds from trade activities that are either prohibited or for which no export licence has been obtained. The goods may originate from Switzerland or abroad. Vulnerabilities arise when front companies, proliferation networks and forged documents are used to facilitate procurement and payment through multiple intermediaries. Assessment is complicated by the fact that, outside the scope of sanctions, trade in dual-use goods is legal and only requires that an export licence be obtained. The existing AML control system also acts as a risk-mitigating factor here. A financial intermediary is required by law to know its domestic and foreign customers and should therefore at least be aware of whether the customer manufactures or trades in dual-use goods. Export and customs controls also apply to exports from Switzerland and thus represent a first line of defence. Consequently, the residual risk for financial intermediaries working with a Swiss customer is relatively small. The same assessment applies if the export is carried out from another country that conscientiously implements export controls. That said, dual-use goods are also manufactured in, exported from or transshipped through countries that do not sufficiently implement transshipment controls. The residual risk is therefore considered higher for a transaction with a foreign element than for one involving Swiss companies only. Since Switzerland has closer economic ties with Iran than with North Korea, the risk of accepting proceeds in connection with the export of dual-use goods is correspondingly higher in the case of Iran.

²²³ See OCCRP, *Dominica: Passports of the Caribbean*, last checked on 25.10.2023; OCCRP, *Spain's 'La Liga' Soccer League Received Iranian Money Through Shell Company Set Up With Purchased Dominican Passport*, last checked on 25 October 2023.

7.2.4 Risk 6: Accepting proceeds from the transfer of technology

A Swiss financial intermediary accepts funds from a resident of Switzerland that are intended as payment for the transfer of intangible technologies that benefit the Iranian or North Korean nuclear or delivery system programme.

A further threat is that a natural person residing in Switzerland transfers intangible technologies, i.e. technical knowledge acquired through work or study in Switzerland, to designated natural persons, companies or organisations and receives payment for this in a personal account in Switzerland. This could also be an involuntary technology transfer, e.g. through extortion. Although the intangible transfer of listed dual-use technology would require authorisation, verifying this is a challenge in practice. Furthermore, little is known about the financing of such technology transfer. There is a vulnerability due to Swiss innovation capacity and because Swiss industry and universities have an exceptionally high level of technology. In addition, numerous Iranian citizens have settled in Switzerland and become naturalised in recent years.²²⁴ In contrast, there are only a few North Korean citizens in Switzerland, and there have been hardly any naturalisations (see Annex 1). It is also possible that other natural persons who have access to dual-use technologies – regardless of their nationality – may be paid for such technology transfers. The fact that Swiss authorities are raising awareness of this issue among affected companies and universities is a risk-mitigating factor. In order to prevent such knowledge from being transferred from Switzerland, the purpose of stay is reviewed, among other things, when issuing visas to Iranian and North Korean nationals who enter to work or study in Switzerland.²²⁵ The residual risk that proceeds from the transfer of intangible technology will be paid into Swiss accounts is considered to be as high as that associated with the transfer of goods abroad. This is because no border controls can be carried out and because it is almost impossible for a financial intermediary to identify the economic background of the transfer. Due to the higher number of Iranian students at technical research institutes, this population group poses a higher risk of transfer of nuclear-related knowledge than North Korean nationals.

7.2.5 Risk 7: Concealment through legal entities (front companies)

Legal entities, in Switzerland or abroad, are misused by designated natural persons, companies or organisations to dissimulate their activities. These may include, for example, portfolio manager, real estate agencies, insurance or reinsurance companies (e.g. in maritime transport). The proceeds benefit the Iranian or North Korean missile programme.

Since designated natural persons, companies or organisations cannot enter into business relationships under their own name, there is a threat that front companies may be hiding complex legal constructs designed to enable proliferation financing. The use of front companies and concealment by means of forged documents is not specific to proliferation financing, but it is a well-known method in financial crime. For example, a front company may be used to open a business relationship with a financial intermediary in Switzerland or abroad, it may be an operational element of the legal construct, or its shares may be transferred without it ever becoming active. Since it is relatively easy to set up a company in Switzerland, vulnerability here is higher. Some Swiss companies explicitly offer company formation services, including the establishment of offshore companies.²²⁶ Such advisory services are not currently regulated by the AML control system. The EmbA applies in the event of a reference to sanctions. One risk-mitigating factor – irrespective of proliferation financing – would be to address legislative gaps relating to legal entities. This action item has already been recognised in Switzerland. On 22 May 2024, the Federal Council adopted a corresponding dispatch to Parliament.²²⁷

224 There are currently over 5,000 Iranian citizens living in Switzerland. Around 150 Iranian citizens are naturalised each year. (See Annex 1)

225 In 2022, a total of 2,639 visa applications were rejected, one-fifth of them because the purpose of the stay or the conditions were not credible. (See Annex 1)

226 An offshore company is a legal entity that operates in a jurisdiction other than where the owner is domiciled.

227 Federal Council. *Federal Council adopts dispatch on strengthening anti-money laundering framework*, 22 May 2024, last checked on 7 August 2024

Regardless of the outcome of the proposed legislative revision, greater vigilance is required of all service providers to mitigate risks. The CGMF is currently preparing a national risk analysis focusing specifically on risks associated with the use of legal entities for money laundering and terrorist financing purposes. Publication of the report is planned for 2025 and the findings will most likely also be applicable to proliferation financing. Since the use of legal entities to mask financial crime is a well-known risk that stands out prominently among the various inherent risks identified in this risk analysis, the residual risk should be deemed greater than any of the other risks considered individually.

7.2.6 Risk 8: Concealment through correspondent banking

A Swiss financial intermediary providing correspondent banking services to a foreign bank attempts to mitigate risk by seeking additional clarification required by law. However, it is unable to determine the economic background and intended use of the funds to be transferred.

In the case of correspondent banking services, there is a threat that a financial intermediary checking a given transaction may obtain the necessary clarifications of the counterparty and also take appropriate risk-mitigating measures, but may not recognise the designated natural persons, companies or organisations because of the use of a front company for concealment purposes. The challenges in terms of transparency in correspondent banking in the fight against money laundering and terrorist financing are well known. Switzerland's vulnerability arises from the fact that Swiss financial intermediaries provide correspondent banking services to foreign banks. Compared to the control system in place to counter money laundering and terrorist financing, the control system used to prevent proliferation financing is even more complex. A risk-mitigating factor here is again existing AML control system, which requires financial intermediaries, depending on the circumstances, to seek additional clarifications regarding the counterparty and consider whether adequate AML/CFT supervision and regulation measures have been applied. Despite this, the residual risk of Swiss financial intermediaries becoming involved in proliferation financing via correspondent banking is considered higher than in wealth management, for example.

7.2.7 Risk 9: Raising funds from stolen cryptocurrencies

A Swiss financial intermediary with VASP activities is improperly used to launder stolen cryptocurrencies from a cyberattack on a foreign crypto exchange. The cyberattack is carried out by the North Korean state and the laundered money benefits its nuclear and delivery system programmes.

The threat in the area of cryptocurrencies (virtual assets, VA) is, for example, that a financial intermediary engaged in VA activities (i.e. virtual asset service provider or VASP) may be used as a conduit to convert stolen cryptocurrencies into another cryptocurrency or into fiat currency following a cyberattack. These cyberattacks are not specifically aimed at proliferation financing, but they may be proliferation financing if the attack – through corresponding blockchain analysis – can be attributed to a hacker group with close ties to the North Korean regime and the funds obtained benefit the North Korean state. Iran and North Korea are increasingly engaged in cybercrime, which heightens this threat. The vulnerability arises from the fact that Switzerland is a significant location for VAs. However, the detection of money laundering and terrorist financing through VAs in Switzerland still depends heavily on the reporting behaviour of financial intermediaries with VA activities. Available figures suggest that the latter still submit SARs significantly less often than financial intermediaries *not* engaged in VA activities. One risk-mitigating factor is that the rules on payment transactions also apply to VAs. In addition, when exchanging cryptocurrencies for fiat currencies (and vice versa), financial intermediaries are legally required to identify the customer if the amount exceeds CHF 1,000 per month. Because large sums of money are needed to develop and maintain nuclear and missile programmes, this can be relevant for proliferation financing. Significant volumes would also be reported in all likelihood. In January 2024, the CGMF published a National Risk Assessment on the risks of money laundering and the financing of terrorism through crypto assets.²²⁸ This report points out that virtual assets are increasingly being used for criminal purposes.

228 CGMF, *National Risk Assessment (NRA) - Risk of money laundering and the financing of terrorism through crypto assets*, January 2024.

This assertion, along with other findings presented in the report apply equally well to proliferation financing. Residual risk of proliferation financing through the misuse of a VASP domiciled in Switzerland are estimated to be comparable to the risk of misuse of correspondent banking services. In addition, the risks of cyberattacks from North Korea are considered to be higher than those coming from Iran.

7.2.8 Risk 10: Concealment through trade or transport financing

A Swiss financial intermediary provides direct (letter of credit) or indirect (open credit) trade credit services to a company based in Switzerland or abroad in order to finance the import or transfer of goods. The fact that the goods originate from North Korea or Iran is concealed by front companies. An effort may also be made to disguise the fact that a trade credit is intended to facilitate the export or transport of sanctioned goods to North Korea or Iran or that a designated natural person, company or organisation is behind the trade or transport transaction.

There is a threat that Swiss financial intermediaries will be misused to finance the cross-border trade or transport of goods that otherwise are prohibited from such trade or transport.²²⁹ International findings show that this is a real threat (see also Chapter 6.1.). Trade and transport financing (relating to import and export), or rather the misuse of such financing through concealment, is a classic circumvention practice. The vulnerability for Switzerland and its financial centre arises from its leading role in trade finance. The fact that funds are not of illicit origin makes it more difficult to detect misuse. However, the EmbA and the sanctions regulations do apply. A risk-mitigating factor is that trade and transport financing instruments ensure greater transparency with regard to the counterparties and other parties involved in the transaction. Reputational risks and the possibility of secondary sanctions could help to ensure that financial intermediaries take their risk management obligations seriously. In contrast, the risk is estimated to be slightly higher when settling the trade via open accounts, as the documentation requirements are not considered to be as stringent. Taking into account the risk countermeasures presented here, the residual risk for financial intermediaries in trade and transport financing is estimated to be lower than for correspondent banking, for example. This assessment does not apply to direct funding by commodity dealers (see Chapter 7.2.9. below).

7.2.9 Risk 11: Raising funds from commodity trading

A Swiss commodity dealer buys coal from an intermediary. In some circumstances, the commodity dealer finances the transaction directly, as it has easy access to financial markets. However, the coal traded comes from North Korea. An analogous example would be possible with oil and gas from Iran.

The threat is that funds raised from the sale of commodities could potentially be used for proliferation purposes. Based on international reports (see Chapter 6), the sale of commodities is one of the most frequently used means of funding proliferation-related activities. The risks come from both Iran (e.g. oil and gas) and North Korea (e.g. coal, gold) as both countries have major raw material deposits. Since there are no UN sanctions against Iran with regard to its trade in commodities, Iranian commodities are bought and sold legally on the world market. Consequently, the threat that Swiss commodity dealers might finance Iranian proliferation is greater than in the case of North Korea, which is subject to a strict UN sanctions regime in this area. However, North Korean commodities also find their way to the world market through smuggling. Commodity trade activities are usually carried out with the involvement of intermediary companies and financial intermediaries from different countries. This increases the potential for abuse, e.g. through the use of front companies. The misuse of commodity trade insurance also cannot be ruled out. The vulnerability arises from the fact that Switzerland is an important commodity trading hub.²³⁰ In the case of trade finance through a financial intermediary, AMLA due diligence and reporting obligations apply. Supervision is handled by FINMA or by a FINMA-recognised SRO.

229 FATF, *Typologies Report on Proliferation Financing*, June 2008. FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021.

230 Around 900 Swiss companies are involved in commodity trading. See Federal Council. *Stand der Umsetzung der Empfehlungen aus dem Bericht 'Rohstoffsektor Schweiz: Standortbestimmung und Perspektiven'*, 21 April 2021, p. 1.

Commodity dealers that carry out transactions on behalf of third parties must join an SRO. However, if a commodity dealer finances the trade using its own resources, the AML control system does not apply directly. SECO is responsible for monitoring compliance with sanctions regulations. In contrast to traditional trade finance, this heterogeneous mechanism means that commodity trade finance is subject to different risk management requirements, and the quality of supervision is also different. So far, there have been no criminal proceedings relating to Iran and North Korea in this area (see Annex 1). It should also be emphasised that most commodities (except gold) are not imported or exported in Switzerland. As a result, no customs controls are applied. There is thus no first physical line of defence in the actual trade in commodities. In February 2020, the Federal Council stated that commodity trade risks are particularly associated with complex financial structures, large trade volumes, the different transparency measures for commodity dealers and the separation of control and lending activities.²³¹ These risks are, of course, also relevant in the context of proliferation financing. The current legal framework offers various risk-mitigating factors that help to prevent proliferation financing through commodity trade finance.²³² The compliance measures of commodity dealers have been tightened in recent years, particularly in the wake of several corruption and money laundering cases.²³³ The industry's risk appetite is further reduced by the risk of secondary sanctions for non-compliance with foreign sanctions, which is particularly relevant in the case of Iran. However, since trade in commodities is not always subject to AMLA due diligence obligations, the residual risk is substantially greater than for trade finance.

7.2.10 Risk 12: Raising funds from the sale of refined gold

A Swiss refinery takes delivery of raw gold from a supplier. This raw gold is then refined in Switzerland and sold as monetary gold, for example. However, the raw gold originated from North Korea and the payment in turn benefits the country's nuclear and delivery system programmes.

The threat is that designated natural persons, companies or organisations may circumvent sanctions by selling gold in Switzerland, or use the proceeds from the sale of the gold to fund sanctioned activities. A vulnerability exists because Switzerland is home to four of the world's largest gold refineries. It is known that sanctions have been circumvented in the past through gold trade. Both North Korea and Iran have gold mines. It is also possible that the North Korean or Iranian governments own gold mines located in other countries. Before the gold trade was restricted by sanctions, gold was the main item imported from Iran. Gold is refined in Switzerland to different levels of purity, then either refined further or used for further processing. Through refining and/or melting, gold loses its original characteristics such as shape and composition, which can intentionally or unintentionally obscure its origin. The importing of mined gold (raw gold) is not directly subject to the AMLA; however, all refineries (trade assayers²³⁴) are subject to the AMLA. From a technical point of view, only companies licensed by the Central Office for Precious Metals Control are in a position to transform raw gold or other gold into banking precious metals (fine gold) or other tradable forms (e.g. alloys or semi-finished products).

231 Federal Council. *Aufsicht über die Rohstoffhandelstätigkeiten unter dem Blickwinkel der Geldwäscherei*, 26 February 2020, p. 14-16.

232 Money laundering under the Swiss Criminal Code and sanctions violations under the Embargo Act (Emba).

233 Federal Council. *Aufsicht über die Rohstoffhandelstätigkeiten unter dem Blickwinkel der Geldwäscherei*, 26 February 2020, p. 17

234 Trade assayers under Art. 41 des *Federal Act of 20 June 1933 on the Control of the Trade in Precious Metals and Precious Metal Articles* (Precious Metals Control Act, PMCA). They often have a melter's licence under Art. 24 PMCA. Most also have an additional licence for trading in banking precious metals within the meaning of Art. 42bis PMCA, and are therefore considered to be financial intermediaries within the meaning of Art. 2 para. 2 let. g AMLA and are subject to supervision by the Central Office for Precious Metals Control by virtue of Art. 42ter PMCA.

Additional risk-mitigating factors would include sector-specific due diligence obligations,²³⁵ the guarantee of proper business conduct in accordance with precious metal legislation,²³⁶ and enactment of the Ordinance of 3 December 2021 on Due Diligence and Transparency in relation to Minerals and Metals from Conflict-Affected Areas and Child Labour (DDTrO),²³⁷ which is applicable to gold. The Ordinance also brings greater transparency to the gold trade, as it contains requirements and obligations that companies must meet in terms of their supply chain policy and traceability. Direct imports of gold from Iran and North Korea can therefore be ruled out, while indirect imports via other countries, e.g. their neighbouring countries or the UAE, remain a realistic scenario. On importation to Switzerland, mined gold is subject to risk-based controls and a plausibility analysis at customs. Trade auditors perform more comprehensive, risk-based audits of imported and processed mined gold during periodic supervision pursuant to the PMCA and AMLA. Consequently, most of the large quantities of gold which is refined in Switzerland or imported in interbank trading is subject to due diligence obligations according to the AMLA and/or PMCA. The control system for the import and processing of raw gold can therefore be considered comprehensive due to statutory due diligence obligations and existing customs controls. Risk is therefore considered to be lower than for commodity trade finance. In addition to the efforts²³⁸ to reduce residual risk by subjecting precious metals dealers (e.g. intermediaries) not previously subject to the AMLA, the ongoing revision of customs legislation aims to further tighten the due diligence obligations set out in the PMCA.²³⁹

235 What is meant here is the requirement of the Responsible Gold Guidance and Member Certification and Chain of Custody Certification (CoC) of the Responsible Jewellery Council. See Federal Council Report in fulfilment of Recordon Postulate 15.3877, Goldhandel und Verletzung der Menschenrechte, Para 3.5, p. 8, 21 September 2015, last checked on 3 May 2024.

236 See SR 941.31 - *Federal Act of 20 June 1933 on the Control of the Trade in Precious Metals and Precious Metal Articles* (Precious Metals Control Act, PMCA). SR 941.311 – *Ordinance of 8 May 1934 on the Control of the Trade in Precious Metals and Precious Metal Articles* (Precious Metals Control Ordinance, PMCO)

237 SR 221.433, *Ordinance of 3 December 2021 on Due Diligence and Transparency in relation to Minerals and Metals from Conflict-Affected Areas and Child Labour* (DDTrO), status as of 1 January 2024.

238 This would be changed with the Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners (LETA), because, among other amendments, it is proposed that a new Art. 8a para. 2bis AMLA be introduced covering persons who trade in gold, silver, platinum and palladium in the form of semi-finished products, melt material and melt products.

239 See *Curia Vista, Geschäft des Bundesrates 22.058 Totalrevision Zollgesetz*. With the total revision of the Customs Act, proposed changes will be made to ensure that only trade assayers will be permitted to import non-tradable melt products (e.g. mine gold), and that these assayers must perform due diligence in compliance with recognised international standards as a mandatory minimum requirement.

7.2.11 Summary table

Given that the consequences of proliferation financing are difficult to quantify, the 12 selected risk scenarios are compared only with each other.



Comparison of proliferation financing risks	Intentional breach of sanctions	Negligent breach of sanctions	Failure to identify assets or companies controlled by designated persons	Concealment through correspondent banking	Concealment through legal entities (front companies)
	Accepting proceeds from the transfer of goods (domestic element)	Accepting proceeds from the transfer of goods (foreign element)	Raising funds from the sale of refined gold	Raising funds from stolen cryptocurrencies	
		Accepting proceeds from the transfer of technology		Raising funds from commodity trading	
		Concealment through trade or transport financing			

The results of the analysis show that the risk of sanctions being breached either with intent or out of negligence is less than the risk of failing to identify assets or companies controlled by designated natural person. For Switzerland, proliferation financing risks are the highest in cryptocurrency trade and correspondent banking. The risk of accepting proceeds from the illegal transfer of goods or risk of financing trade in sanctioned goods are considered to be low. However, no economic sector is immune to circumvention activities, which is why concealment through front companies is considered the highest overriding risk. Furthermore, trade-related risks in relation to Iran are generally considered higher because, unlike North Korea, Iran is not excluded from the value chain. North Korea, on the other hand, poses a higher risk in the area of cybercrime.

7.3 Vulnerabilities in proliferation financing countermeasures

The Swiss legal framework for the prevention of proliferation financing is an interplay of complementary legal provisions. In principle, they substantively cover Switzerland’s international commitments, which was also recognised in the last FATF evaluation report on Switzerland.²⁴⁰ This chapter takes a closer look at where the vulnerabilities of the existing control system lie.

240 FATF, *Measures to combat money laundering and the financing of terrorism and proliferation in Switzerland*, Mutual Evaluation Report, Paris, December 2016. Switzerland received a rating of ‘compliant’ for Recommendation 7 and achieved a ‘substantial’ (highest rating) level of effectiveness for Immediate Outcome 11.

7.3.1 Due diligence obligations and oversight

Implementation of the EmbA-based Iran Ordinance and North Korea Ordinance is binding on all natural persons and legal entities. However, the EmbA does not directly require financial intermediaries or (financial) service providers to analyse their risk of potential breach, non-implementation or evasion of sanctions. The EmbA also does not specify how a financial intermediary or (financial) service provider must be organised. As a result, SECO does not monitor organisational measures. FINMA checks whether the financial intermediaries under its supervision comply with their due diligence obligations. Under the EmbA, SECO is responsible for prosecuting sanction violations. In 2022 and 2024, for example, FINMA and SECO carried out several on-site inspections relating to sanctions.²⁴¹ As part of its review of organisational measures and the EmbA, the Federal Council is now proposing in the draft of LETA that Art. 8 AMLA be clarified.²⁴² The scope of application of the EmbA also applies to all natural and legal persons and not just to financial intermediaries. Currently, most VA services are subject to AMLA provisions.²⁴³ The AMLA now applies to a sizeable portion of the gold trade but only part of commodity trading. This means that due diligence obligations and/or compliance monitoring are partly non-existent or covered by other legislation.

7.3.2 Information sharing

Information sharing relating to proliferation financing or sanctions violations is today possible thanks to a legislative provision on mutual legal assistance (Art. 6 EmbA) that may be invoked if necessary to implement the Federal Act and sanction ordinances. However, if MROS determines in the course of its investigations that the SAR relates not to a predicate offence to money laundering but rather to a breach of the EmbA or WMA (which is not reportable under AMLA), then there is currently no legal basis enabling MROS to forward this information to SECO. If the LETA enters into force in its current form, MROS and SECO would be authorised to exchange all information and documents they need in order to implement the AMLA and EmbA.²⁴⁴ Information from foreign Financial Intelligence Units (FIUs)²⁴⁵ could also be brought to SECO's attention. Improved information sharing with other federal agencies would also enable SECO to detect and punish proliferation financing violations more effectively. Information sharing is an essential means of preventing proliferation financing, irrespective of which specific sanctions violations occur.

7.3.3 Raising private sector awareness

For several years, the FIS²⁴⁶ and SECO have been working to raise awareness of proliferation issues and export controls among trading companies and universities. However, this work has not yet been extended to the financial sector or other service providers. The work for this risk analysis in particular has brought the complexity of proliferation financing to the fore and the analysis itself can lead to a better understanding of this complex issue. Raising awareness in the sectors concerned would be advisable.

241 These on-site inspections were mainly carried out to verify implementation of the [Ordinance of 4 March 2022 on Measures Relating to the Situation in Ukraine](#) (SR 946.231.176.72)

242 This should establish the legal basis for clearly requiring legal entities to analyse their risk with regard to proliferation financing. A portion of the FATF recommendation would thus be implemented. See [Federal Council adopts dispatch on strengthening anti-money laundering framework](#), 22 May 2024, last checked on 9 August 2024; as well as [Federal Council Dispatch on Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners](#) and [Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners \(LETA\)](#)

243 In Switzerland, expanding the definition of financial intermediation to include virtual asset service provision has helped to ensure that a wider range of players fall within the scope of AMLA. See [National Risk Assessment \(NRA\) - Risk of money laundering and the financing of terrorism through crypto assets](#), January 2024, p. 27ff

244 See [Federal Council adopts dispatch on strengthening anti-money laundering framework](#), 22 May 2024, last checked on 9 August 2024; as well as [Federal Council Dispatch on Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners](#) and [Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners \(LETA\)](#)

245 MROS is the financial intelligence unit (FIU) for Switzerland. The [Egmont Group](#) could facilitate international exchange with other financial intelligence units on proliferation financing.

246 The FIS runs an awareness programme called Prophylax to prevent industrial espionage and proliferation in companies. A specific programme called Technopol focuses on higher education institutions. FIS, [Wirtschaftsspionage](#), last checked on 30 April 2024.

7.3.4 Reporting obligations

A duty to report to SECO is set out in both the Iran Ordinance and North Korea Ordinance²⁴⁷ whenever financial and economic resources are frozen on the basis of these ordinances.²⁴⁸ This would be the case if there is a suspicion that funds are intended for natural persons, companies or organisations listed in the Annexes of these Ordinances. The EmbA does not provide for any other obligation to report suspicions of proliferation financing to SECO. Similarly, the WMA, which prohibits proliferation financing, does not contain any corresponding reporting obligations. For its part, the AMLA provides for a duty to report suspected cases of money laundering, their predicate offence, organised crime and terrorist financing. A suspicion of proliferation financing must only be reported under the AMLA if there is also a suspicion that a predicate offence to money laundering (i.e. a felony) has been committed.²⁴⁹ No conclusive picture of proliferation financing can be drawn on the basis of available MROS data. The data show that a small number of financial intermediaries have submitted SARs relating to possible proliferation financing transactions to MROS. However, the lack of further reports could be an indication that these financial intermediaries have not encountered any suspicious circumstances of this nature. It is also possible that reports were sent both to SECO and MROS. More extensive data collection through expanded reporting obligations would provide a clearer picture and allow for a quantitative risk analysis in the area of proliferation financing.

7.3.5 Comparison of proliferation and terrorist financing bans

The FATF has issued two Recommendations and corresponding Interpretative Notes concerning terrorist financing.²⁵⁰ The first of these is Recommendation 6, which, like Recommendation 7 on proliferation financing, contains provisions for the implementation of the UN's targeted financial sanctions. The second is Recommendation 5, which stipulates that countries should also have the legal means to prosecute and punish those who finance terrorism. In Switzerland, a corresponding ban on terrorist financing has been in force since March 2003 in the form of Art. 260quinquies para. 1 SCC.²⁵¹ In contrast, proliferation financing, i.e. the direct or indirect funding of nuclear, biological and chemical weapons, is prohibited by the WMA. However, this ban does not cover all delivery systems for weapons of mass destruction (see Chapter 4.3.2.).

Despite the discrepancies between the ban set out in the SCC and in relevant federal acts, both terrorist and proliferation financing can carry a custodial sentence of over three years (felony).²⁵² The jurisdiction is not necessarily the same, however, because violations of the EmbA are usually prosecuted under administrative criminal law, because the Office of the Attorney General of Switzerland (OAG) can only open a police investigation at the request of SECO and only if the particular seriousness of the offence justifies such action.²⁵³ Under WMA provisions, on the other hand, the Federal Criminal Court has jurisdiction.²⁵⁴

247 In the case of North Korea, since 2007, banks must also report if they hold accounts for diplomatic and consular missions of the Democratic People's Republic of Korea or their employees. See Art. 18 para. 1bis North Korea Ordinance

248 See Art. 8 Iran Ordinance; Art. 18. North Korea Ordinance

249 For example, Art. 9 para. 2 EmbA, Art. 33 para. 2 WMA, Art. 14 para. 2 GCA

250 FATF, *The FATF Recommendations*, Updated November 2023.

251 This criminal provision was enacted in order to implement the International Convention for the Suppression of the Financing of Terrorism and 11 other UN conventions. See: BBI 2002 5390 *Federal Council Dispatch of 26 June 2022 on the International Convention for the Suppression of the Financing of Terrorism and on the International Convention for the Suppression of Terrorist Bombings as well as on Amendment of the Swiss Criminal Code*, 26 June 2022; *Federal Act on Amendment of the Swiss Criminal Code and the Federal Act on the Surveillance of Post and Telecommunications (Financing of Terrorism)*, 21 March 2003; SR 0.353.22 *International Convention for the Suppression of the Financing of Terrorism*, Status as of 11 September 2020.

252 See Art. 9 para. 2 EmbA, Art. 33 WMA, and Art. 260quinquies para. 1 SCC

253 See Art. 14 para. 2 EmbA

254 See Art. 40 para. 1 WMA

8. Conclusions and recommendations

Switzerland is well positioned to counter proliferation financing in terms of substantive law. Several industries and services are still at risk: first and foremost trade in commodities, the exchange of cryptocurrencies, and transactions involving correspondent banks. The risk of receiving proceeds from the illegal transfer of goods or financing trade in sanctioned goods is lower. The greatest risk is concealment through front companies, which affects all sectors. Moreover, the risk of failing to identify assets or companies controlled by designated natural persons is relatively higher than the risk of sanctions being violated with intent or out of negligence.

The analysis of the risk scenarios covered in this report provides an overview of the respective threats and vulnerabilities and identifies existing risk-mitigating factors. In order to further improve and reinforce this control system, CGMF proposes the following four action steps:

- **Expanding the CGMF mandate to include proliferation financing**
The CGMF serves as a platform for coordinating all issues related to anti-money laundering and terrorist financing policy and risk assessment in this area. Extending the CGMF's mandate to include proliferation financing is in line with developments in international standards and helps to ensure a Swiss policy coherence. In addition, given SECO's thematic expertise and responsibilities, consideration should be given to admitting SECO as a permanent member of the CGMF.
- **Creation of a working group devoted to proliferation financing**
The working group's remit would be to facilitate regular discussion and develop sufficient expertise and to monitor the development of proliferation financing risks. The working group would evaluate legal provisions and recommend amendments as need to reinforce the control system, in particular with regard to proliferation financing prohibition and information sharing. The working group could be set up as a specialised sub-group of CGMF.
- **Improvement of information base**
In order to collect adequate data on proliferation financing and improve the quality of the information available to the authorities, a review of the existing reporting system should be carried out.
- **Raise private sector awareness**
Suitable awareness-raising measures should be taken to ensure that financial intermediaries and (financial) service providers possess sufficient expertise in the area of proliferation financing, regardless of whether they are subject to the AMLA or not. Awareness-raising should focus on the sectors that are exposed to a greater risk and should involve the relevant umbrella organisations (associations, SROs, etc.).

The scope of this national risk analysis was limited to proliferation financing risks relating to Iran and North Korea pursuant to FATF guidance. The working group to be set up to continue monitoring proliferation financing risks will also examine whether developments warrant further sectoral analyses or an analysis which goes beyond those countries specified by the FATF (Iran and North Korea).

Due to the often overarching risks, this report does not contain any recommendations for specific economic sectors or services. **The private sector is, however, encouraged to carry out its own risk analyses.**

9. Literature

38 North, *The North Korean-Syrian Partnership: Bright Prospects Ahead*, Foreign Affairs, 23 March 2021.

AG. *The Australia Group*, last checked on 5 September 2024.

Arab News, *How Iran is cashing in on cryptocurrencies to evade US sanctions*, November 2022.

AS 2003 3043 – *Federal Act on Amendment of the Swiss Criminal Code and the Federal Act on the Surveillance of Post and Telecommunications (Financing of Terrorism)*, 21 March 2003.

Australian Government (AUSTRAC), *Proliferation Financing in Australia, National Risk Assessment*, 14 December 2022.

Conflict Armament Research, *Documenting a North Korean missile in Ukraine*, January 2024.

Arterburn, Jason. *Dispatched: Mapping Overseas Forced Labor in North Korea's Proliferation Finance System*. C4ADS Report. 2018.

BBC News. *The Lazarus heist: How North Korea almost pulled off a billion-dollar hack*, 21 June 2021.

BBI 2002 5390 - *Federal Council Dispatch of 26 June 2022 on the International Convention for the Suppression of the Financing of Terrorism and on the International Convention for the Suppression of Terrorist Bombings as well as on Amendment of the Swiss Criminal Code*.

Berner Zeitung, *Nordkorea an der Berner Ferienmesse*, 6 January 2015.

Breuker, *People For Profit*, 2018.

Brewer, Jonathan, *The financing of nuclear and other weapons of mass destruction proliferation*, January 2018.

Brewer, Jonathan, *Basic Principles for Conducting Financing-of-Proliferation Risk Assessments*, Center for a New American Security, 1 November 2018

Brewer, Jonathan, *The Financing of WMD Proliferation*, Center for a New American Security, November 2018.

Brewer, Jonathan, *Proliferation Financing: The Potential Impact of the Nuclear Agreement with Iran on International Controls*, March 2016.

Federal Office for Customs and Border Security (FOCBS), *Foreign trade statistics*, last checked on 2 August 2023.

Bundesamt für Verfassungsschutz (BfV), Germany, *Proliferation. Wir haben Verantwortung*, July 2018.

Federal Office for Customs and Border Security (FOCBS). *Anteil der MEM-Exporte im Aussenhandel innert 25 Jahren deutlich gesunken*, 6 July 2023.

Federal Council, in fulfilment of the Recordon Postulate 15.3877, *Goldhandel und Verletzung der Menschenrechte*, 21 September 2015.

Federal Council, *Rohstoffsektor Schweiz: Standortbestimmung und Perspektiven*, Bern, November 2018.

Federal Council. *Aufsicht über die Rohstoffhandelstätigkeiten unter dem Blickwinkel der Geldwäscherei*, 26 February 2020.

Federal Council, *Weltweit führend, verankert in der Schweiz: Politik für einen zukunftsfähigen Finanzplatz Schweiz*, Bern, 4 December 2020.

Federal Council, *Stand der Umsetzung der Empfehlungen aus dem Bericht «Rohstoffsektor Schweiz: Standortbestimmung und Perspektiven»*, Bern, 21 April 2021.

Federal Council, *Federal Council Dispatch on the Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners*, Bern, 22 May 2024.

Federal Council, *Federal Council adopts dispatch on strengthening anti-money laundering framework*, press release, Bern, 22 May 2024.

CEIC. North Korea Gold Production, 1990 – 2022, last checked on 5 September 2024.

Chainalysis, *The 2023 Crypto Crime Report*, February 2023.

Chainalysis, *Russian and North Korean Cyberattack Infrastructure Converge: New Hacking Data Raises National Security Concerns*, 14 September 2023.

CNN Business. *North Korea is making millions selling sand*, 10 June 2020.

Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB), Secrétariat général de la défense et de la sécurité nationale (SGDSN), France. *Analyse nationale des risques de financement de la prolifération (ANR-FP)*. 2022.

Deutscher Übersetzungsdienst der Vereinten Nationen, *Demokratische Volksrepublik Korea*, last checked on 3 May 2024.

Deutscher Übersetzungsdienst der Vereinten Nationen, *Iran*, last checked on 03 May 2024.

Direction Générale de la Sécurité Intérieure (DGSI), France, *Contre prolifération des armes (online)*, last checked on 24 October 2023

Die Weltwoche. *Nordkorea in Afrika*, 15 January 2023.

DW. *Umstrittenes Berliner Hostel endgültig dicht?*, 28 March 2020.

EAEU. Eurasian Economic Union, last checked on 12 September 2023. Currently, the EAEU is comprised of five member states: Armenia, Belarus, Kazakhstan, Kyrgyzstan and Russia.

Swiss Federal Audit Office (SFAO), *Audit of controls on dual-use goods*, 22 May 2023, last checked on 3 September 2024.

Federal Department of Foreign Affairs (FDFA), *Swiss Financial Centre*, last checked on 27 November 2023.

Federal Department of Foreign Affairs (FDFA), Treaty on the Prohibition of Nuclear Weapons (TPNW), last checked on 5 September 2024.

Federal Department of Foreign Affairs (FDFA), Update on the report of the working group analysing the Treaty on the Prohibition of Nuclear Weapons, 31 January 2024, last checked on 3 September 2023.

Elliptic, *How Iran Uses Bitcoin Mining to Evade Sanctions and 'Export' Millions of Barrels of Oil*, May 2021, last checked on 27 November 2023.

EURACTIV, *Russia to attach Iran to its Eurasian Economic Union*, 19 June 2023, last checked on 5 September 2024.

European Central Bank Banking Supervision, *ECB determined ABLV Bank was failing or likely to fail*, 24 February 2018.

FATF, *Typologies Report on Proliferation Financing*, June 2008.

FATF, *Proliferation Financing Report*, June 2008.

FATF, *Combating Proliferation Financing. A Status Report on Policy Development and Consultations*, February 2010.

FATF, *Measures to combat money laundering and the financing of terrorism and proliferation in Switzerland*, Mutual Evaluation Report, Paris, December 2016.

FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021.

FATF, *The FATF Recommendations*, updated February 2023.

FATF, *FATF Methodology for Assessing Technical Compliance with the FATF Recommendations*, updated June 2023.

FATF, *High-Risk Jurisdictions subject to a Call for Action*, updated in June 2023.

FATF, *Global Network*, last checked on 07 August 2024.

FATF, *Consolidated assessment ratings*, 17 July 2024.

Federation of American Scientists. *North Korea Explains Withdrawal from the NPT*, 22 January 2002.

Financial Times. *North Korea: The secrets of Office 39*, 24 June 2015.

Financial Times, *Iran's 'ghost fleet' switches into Russian oil*, February 2023.

FINMA, *Inadequate risk management of US sanctions: FINMA closes proceedings against BNP Paribas (Suisse)*, 1 July 2014.

Government of the French Republic, *Analyse nationale des risques de financement de la prolifération*, June 2022.

Handelsblatt. *Ehemalige Bank ABLV aus Lettland scheitert mit Klage*, 6 May 2021.

Handelszeitung. *Nordkorea: Schweizer Geschäfte mit dem «geliebten Führer»*, 2 December 2010.

HM Treasury, *National risk assessment of proliferation financing*, September 2021.

Indo-Pacific Defense. *Countering North Korean Sanctions Evasion*, 3 August 2020.

International Atomic Energy Agency (IAEA). *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231*, Board of Governors Report, 28 February 2023.

IRAM Center for Iranian Studies. *New Details of Iran-Russia Energy Agreement and the Predictions*, 29 August 2022.

IRAM Center for Iranian Studies, *Evading Sanctions via IRISL, Iran's Shipping Company - IRAM Center | Center for Iranian Studies in Ankara*, 21 April 2021.

KCL. *Workshop on the implementation of non-proliferation controls in universities and research institutes*, last checked on 5 September 2024.

CGMF, *Report on the national assessment of the risks of money laundering and terrorist financing in Switzerland*, October 2021.

CGMF, *National Risk Assessment (NRA) - Risk of money laundering and the financing of terrorism through crypto assets*, January 2024.

Khalaji, Mehdi. [Iran's Revolutionary Guards Corps, Inc. Brief Analysis](#), The Washington Institute, 17 August 2007.

Korea Economic Institute of America. [North Korean Sanctions Evasion: The UN Panel of Experts Report](#), 1 June 2021.

Middle East Eye, [North Korea's enigmatic role in the Middle East arms market](#), 20 January 2023.

MROS, [Report on the national evaluation of the risks of money laundering and terrorist financing in Switzerland](#), June 2015.

MTCR. [Missile Technology Control Regime](#), last checked on 5 September 2024.

Federal Intelligence Service (FIS), [PROPHYLAX. Prävention- und Sensibilisierungsprogramm des Nachrichtendienstes des Bundes](#). Published by: Federal Department of Defence, Civil Protection and Sport (DDPS), 2019.

Federal Intelligence Service (FIS), [Bekämpfung von Spionage und Proliferation: akademische Welt im Visier](#), press release, last checked on 9 August 2024

Federal Intelligence Service (FIS), [Akademische Welt im Visier](#), last checked on 9 August 2024.

Federal Intelligence Service (FIS), [Wirtschaftsspionage in der Schweiz](#), 6 April 2023, last checked on 3 September 2024.

National Geographic. [North Korean Diplomats Accused of Smuggling Ivory and Rhino Horn](#), 16 October 2017.

NATO, [NATO's nuclear deterrence policy and forces](#), 5 July 2023.

NK News. [North Korean spy ran hotels, casinos and travel agency in Cambodia: UN report](#), 15 February 2022.
NSG. [Nuclear Suppliers Group](#), last checked on 5 September 2023.

NTI, [Iran Nuclear Overview](#), last checked on 10 September 2024.

Nuclear Weapons Ban Monitor, [The status of the TPNW](#), 4 January 2024.

NZZ. [Handel mit iranischem Erdöl](#), 17 September 2012.

Office of the US Secretary of Defense. [Military and Security Developments Involving the Democratic People's Republic of Korea](#), 15 December 2017.

Panel of Experts. [Final Report of the Panel of Experts of the 1718 DPRK Sanctions Committee](#), 4 March 2021, S/2021/211.

Panel of Experts. [Midterm Report of the Panel of Experts of the 1718 DPRK Sanctions Committee](#), 30 August 2019, S/2019/261.

Panel of Experts. [Midterm Report of the Panel of Experts of the 1718 DPRK Sanctions Committee](#), 28 August 2020, S/2020/840.

Radio Free Asia. [North Korean bandits steal 200 kilos of gold bars worth US \\$12 million](#), 22 December 2022.

Radio Free Asia. [Russia resumed shipments of oil to North Korea in December, UN data shows](#), 6 June 2023.

Radio Free Asia. [North Korean Traders Smuggle Coal to Power-Short China](#), 11 October 2021.

Radio Free Asia. [To make extra money, North Koreans pay big bribes for gold refinery jobs](#), 22 August 2023.

Reuters. *Factbox. North Korea's shady 'Office 39'*, World News, 19 November 2010.

Reuters, *BNP Paribas sentenced in \$8.9 billion accord over sanctions violations*, 1 May 2015.

Reuters. *The Cold Frontier: Dreams of Gold*, 12 April 2018.

Reuters. *North Korea factories humming with 'Made in China' clothes, traders say*, Business News, 13 August 2017.

Reuters. *U.S. blacklists oil shipping network allegedly run by Iran Revolutionary Guards*, Oil report, 4 September 2019.

Reuters. *North Korea factories humming with 'Made in China' clothes, traders say*, Business News, 13 August 2017.

Reuters, *Russia resumes oil exports to North Korea after long pause*, 14 June 2023.

Royal United Services Institute for Defence and Security Studies, The RUSI Journal, *Money Talks: The Surging Revolution in Counterproliferation Strategy*, December 2011.

Royal United Services Institute for Defence and Security Studies, RUSI Whitehall Paper, *Target Markets: North Korea's Military Customers in the Sanctions Era* by Andrea Berger, RUSI, 8 December 2015

Royal United Services Institute for Defence and Security Studies, RUSI Whitehall Report 3-16, *Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance* by Emil Dall, Tom Keatinge and Andrea Berger, June 2016.

Royal United Services Institute for Defence and Security Studies, RUSI Guidance Paper, *Countering Proliferation Finance: An Introductory Guide for Financial Institutions* by Emil Dall, Tom Keatinge and Andrea Berger, April 2017.

Royal United Services Institute for Defence and Security Studies, *Countering Proliferation Finance: Implementation Guide and Model Law for Governments* by Andrea Berger and Anagha Joshi, 21 July 2017.

Royal United Services Institute for Defence and Security Studies, *Countering Proliferation Finance: Implementation Guide and Model Law for Governments* by Anagha Joshi, Second Edition, October 2018.

Royal United Services Institute for Defence and Security Studies, *Guide to Conducting a National Proliferation Financing Risk Assessment* by Anagha Joshi, Emil Dall and Darya Dolzikova, May 2019.

Royal United Services Institute for Defence and Security Studies, *AQ Khan is Dead – Long Live the Proliferation Network* von Aaron Arnold and Darya Dolzikova, 15 October 2021.

Russia Briefing. *Russia and Iran Connect Financial Payment Systems*, 30 January 2023, last checked on 28 August 2023.

Scienceindustries. *Schweizer Aussenhandel: Chemie Pharma Life Sciences sind Exportmeister*, 24 January 2023.

Swiss National Bank (SNB), *Supplementary data on foreign trade*, Iran, last checked on 24 June 2024.

Swiss National Bank (SNB), *Supplementary data on banking statistics*, Iran, last checked on 24 June 2024.

Swiss National Bank (SNB), *Supplementary data on foreign trade*, North Korea, last checked on 24 June 2024.

Swiss National Bank (SNB), *Supplementary data on banking statistics*, North Korea, last checked on 24 June 2024.

Swiss National Bank (SNB), *Number of banks for all bank categories*, last checked on 5 September 2024.

S-GE: *Switzerland is the world's third largest reinsurance location*, 13 February 2023.

SIPRI Yearbook, *Global nuclear arsenals are expected to grow as states continue to modernize*, 4 January 2024.

SR 0.353.23 – *International Convention of 13 April 2005 for the Suppression of Acts of Nuclear Terrorism* (ICSANT), status as of 10 September 2020.

SR 0.515.03 – *Treaty of 1 July 1968 on the Non-Proliferation of Nuclear Weapons*, (NPT, Non-Proliferation Treaty), status as of 15 March 2018.

SR 0.515.07 – *Convention of 10 April 1972 on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction*, Biological Weapons Convention (BWC), status as of 22 May 2020.

SR 0.515.08 – *Convention of 13 January 1993 on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction*; , (Chemical Weapons Convention, CWC), status as of 2 July 2020.

SR 0.515.092 – *Convention of 18 September 1997 on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction*, status as of 31 May 2013.

SR 0.515.093 – *Convention of 30 May 2008 on Cluster Munitions*, status as of 25 February 2021.

SR 0.515.105 – *Protocol of 17 June 1925 for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare*, status as of 9 July 2020.

SR 221.433, *Ordinance of 3 December 2021 on Due Diligence and Transparency in relation to Minerals and Metals from Conflict-Affected Areas and Child Labour* (DDTrO), status as of 1 January 2024.

SR 311.0 – *Swiss Criminal Code of 21 December 1937*, (Swiss Criminal Code, SCC), status as of 13 December 2022.

SR 514.51 – *Federal Act of 13 December 1996 on War Materiel*, (War Materiel Act, WMA), status as of 1 July 2023.

SR 732.1 – *Nuclear Energy Act of 21 March 2003*, (NEA), status as of 1 July 2023.

SR 935.51 - *Federal Act of 29 September 2017 on Gambling* (Gambling Act, GambIA), status as of 1 September 2023

SR 941.1 – *Federal Act of 15 June 2018 on Financial Institutions*, (Financial Institutions Act, FINIG), status as of 1 January 2021.

SR 941.31 - *Federal Act of 20 June 1933 on the Control of the Trade in Precious Metals and Precious Metal Articles* (Precious Metals Control Act, PMCA), status as of 1 June 2023

SR 941.311 – *Ordinance of 8 May 1934 on the Control of the Trade in Precious Metals and Precious Metal Articles* (Precious Metals Control Ordinance, PMCO)

SR 946.202 – *Federal Act of 13 December 1996 on the Control of Dual-Use Goods and of Specific Military Goods*, (Goods Control Act, GCA), status as of 1 July 2023

SR 946.202.1 – *Ordinance of 3 June 2016 on the on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods*, (Goods Control Ordinance, GCO), status as of 1 May 2023.

SR 946.202.21 - *Ordinance of 21 August 2013 on the Control of Chemicals with Civilian and Military Uses*, (Chemicals Control Ordinance, ChCO) status as of 1 November 2021

SR 946.231 – *Federal Act of 22 March 2002 on the Implementation of International Sanctions*, (Embargo Act, EmbA), status as of 1 August 2004.

SR 946.231.143.6 – *Ordinance of 11 November 2015 on Measures Against the Islamic Republic of Iran*, (Iran Ordinance), status as of 1 June 2023.

SR 946.231.127.6 – *Ordinance of 18 May 2016 on Measures Against the Democratic People’s Republic of Korea*, (North Korea Ordinance), status as of 1 June 2023.

SR 946.231.176.72 – *Ordinance of 4 March 2022 on Measures Relating to the Situation in Ukraine* , status as of 1 September 2024.

SR 951.31 - *Federal Act of 23 June 2006 on Collective Capital Investment Schemes* (Collective Investment Schemes Act, CISA), status as of 1 January 2023.

SR 952.0 – *Federal Act of 8 November 1934 on Banks and Savings Banks*, (Banking Act, BankA), status as of 1 January 2023.

SR 955.0 – *Federal Act of 10 October 1997 on Combating Money Laundering and Terrorist Financing*, (Anti-Money Laundering Act, AMLA), status as of 23 January 2023.

SR 956.1 – *Federal Act of 22 June 2007 on Federal Financial Market Supervision*, (Financial Market Supervision Act, FINMASA), status as of 1 January 2022.

SR 958.1 – *Federal Act of 19 June 2015 on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading*, (Financial Market Infrastructure Act, FinMIA), status as of 1 January 2023.

SR 961.01 – *Federal Act of 17 December 2004 on the Oversight of Insurance Companies*, (Insurance Oversight Act, IOA), status as of 1 January 2023

SRF, *Treffen zwischen Putin und Kim - So realistisch sind nordkoreanische Waffenlieferungen an Russland*, 6 September 2023.

SRF, *Goldhandel im Zwielficht - Die Schweiz tut sich schwer mit Gesetzesverschärfungen zum Gold*, last checked on 5 September 2024.

State Secretariat for International Finance (SIF), *Payment mechanism for humanitarian supplies to Iran in effect*, 27 February 2020.

State Secretariat for International Finance (SIF), *Mandate of the interdepartmental coordinating group on combating money laundering and the financing of terrorism*, approved by the Federal Council Decree of 17 November 2021.

State Secretariat for International Finance (SIF), *Mandate of the CGMF*, 2021.

State Secretariat for International Finance (SIF), *Swiss financial centre, key figures April 2023*, last checked on 27 November 2023.

State Secretariat for Economic Affairs (SECO), Export controls on military goods, *Zahlen und Statistiken*, last checked on 5 September 2024.

State Secretariat for Economic Affairs (SECO), *Massnahmen gegenüber der Demokratischen Volksrepublik Korea (Nordkorea)*, status as of 16 April 2024, last checked on 9 August 2024.

State Secretariat for Economic Affairs (SECO), *Massnahmen gegenüber der Islamischen Republik Iran*, status as of 15 August 2024.

SECO, Military supplies, [Zahlen und Statistiken](#)

State Secretariat for Economic Affairs (SECO), Dual-use and specific military goods, [Zahlen und Statistiken/ ab 2015](#)

State Secretariat for Economic Affairs (SECO), [Switzerland retains measures linked to Iran's nuclear programme](#), 5 January 2024.

State Secretariat for Economic Affairs (SECO), [Bericht zur Aussenwirtschaftspolitik 2022 einschliesslich Botschaften zu Wirtschaftsvereinbarungen sowie Bericht über zolltarifarisches Massnahmen im Jahr 2022](#), 11 January 2023.

State Secretariat for Economic Affairs (SECO), [Die volkswirtschaftliche Bedeutung der Schweizer Rüstungs- und der Dual-Use Industrie](#), 17 February 2023.

Stewart, Shannon R., [DPRK Overseas Financial Networks](#), June 2021.

Stimson. [North Korea's Komdok Mining Region: Empty Promises?](#), 17 August 2022.

Supply Chain 24/7. [Dozens of Companies Report North Korea Gold Used In Their Supply Chain](#), 4 June 2014.

SWI swissinfo.ch, [Switzerland's global wealth crown up for grabs](#), 7 August 2023.

Swissgoldsafe, Edelmetall-Raffinerien in der Schweiz und weltweit, updated 6 June 2024.

Swissmem. [Kennzahlen 2022 - Panorama](#), last checked on 5 September 2024.

Switzerland Global Enterprise, [Iran bans the import of more than 1,300 products](#), 30 August 2023.

SWP study. [Das A Q-Khan-Netzwerk](#), May 2008.

The Central Asia-Caucasus Analyst. [Iran and Russia: from "Oil-for-Goods Swap" to "Oil-Gas Swap"](#) , 17 January 2023.

The Diplomat. [How the North Korean Government Is Squeezing Foreign Currency Out of Its People](#), 13 August 2022.

The Guardian. [UK freezes assets of North Korean company based in south London](#), 23 April 2017.

The New Yorker, [The Puzzle Over North Korean Gold](#), 4 August 2014.

The New York Times, [Kim Jong-un and Putin Plan to Meet in Russia to Discuss Weapons](#), 4 September 2023.

The Trump White House. [President Donald J. Trump is Ending United States Participation in an Unacceptable Iran Deal](#), Archive, 8. May 2018.

Time. [Kim Yo-Jong's Links to North Korea's Secretive Office 39](#), 29 April 2020.

GOV.UK, [The UK's nuclear deterrent: what you need to know](#), 16 March 2023.

UN Meetings Coverage and Press Releases, [Security Council Fails to Extend Mandate for Expert Panel Assisting Sanctions Committee on Democratic People's Republic of Korea](#), 28 March 2024.

UN News, [Top UN official calls for strict compliance with sanctions on DPR Korea](#), 28 June 2024.

UN Press. [Negotiations Stall While Iran's Uranium Stockpiles Increase, Security Council Told, as Additional Allegations Frustrate Return to Joint Nuclear Plan](#), 6 July 2023.

UNSC, [Annual Reports](#), Security Council Committee established pursuant to resolution 1718 (2006).

UNSC, [Reports](#), Panel of Experts established pursuant to resolution 1718 (2006).

UNSC, [Fifteenth six-month report of the Facilitator on the implementation of Security Council resolution 2231](#), 30 June 2023.

UNSC, [Resolution 1540 \(2004\)](#), 28 April 2004, S/RES/1540.

UNSC, [Resolution 1673 \(2006\)](#), 27 April 2006, S/RES/1673.

UNSC, [Resolution 1718 \(2006\)](#), 14 October 2006, S/RES/1718.

UNSC, [Resolution 1737 \(2006\)](#), 23 December 2006, S/RES/1737.

UNSC, [Resolution 1747 \(2007\)](#), 24 March 2007, S/RES/1747.

UNSC, [Resolution 1803 \(2008\)](#), 3 March 2008, S/RES/1803.

UNSC, [Resolution 1810 \(2008\)](#), 25 April 2008, S/RES/1810.

UNSC, [Resolution 1835 \(2008\)](#), 27 September 2008, S/RES/1835.

UNSC, [Resolution 1874 \(2009\)](#), 12 June 2009, S/RES/1874.

UNSC, [Resolution 1929 \(2010\)](#), 24 March 2007, S/RES/1929.

UNSC, [Resolution 1977 \(2011\)](#), 20 April 2011, S/RES/1977.

UNSC, [Resolution 1874 \(2009\)](#), 12 June 2009, S/RES/1874.

UNSC, [Resolution 2087 \(2013\)](#), 22 January 2013, S/RES/2087.

UNSC, [Resolution 2094 \(2013\)](#), 7 March 2013, S/RES/2094.

UNSC, [Resolution 2224 \(2015\)](#), 9 June 2015, S/RES/2224.

UNSC, [Resolution 2231 \(2015\)](#), 20 July 2015, S/RES/2231.

UNSC, [Resolution 2270 \(2016\)](#), 2 March 2016, S/RES/2270.

UNSC, [Resolution 2321 \(2016\)](#), 30. November 2016, S/RES/2321.

UNSC, [Resolution 2325 \(2016\)](#), 15 December 2014, S/RES/2325.

UNSC, [Resolution 2356 \(2017\)](#), 2 June 2017, S/RES/2356

UNSC, [Resolution 2371 \(2017\)](#), 5 August 2017, S/RES/2371.

UNSC, [Resolution 2375 \(2017\)](#), 11 September 2017, S/RES/2375.

UNSC, [Resolution 2397 \(2017\)](#), 22 December 2017, S/RES/2397.

UNSC, [Resolution 2572 \(2021\)](#), 22 April 2022, S/RES/2572.

UNSC, [Resolution 2622 \(2022\)](#), 25 February 2022, S/RES/2622.

U.S. Department of the Treasury, [National Proliferation Financing Risk Assessment](#), February 2022.

U.S. Department of the Treasury, [OFAC Identifies Entities Owned or Controlled by the Government of Iran](#), 26 November 2018.

U.S. Department of the Treasury, *2024 National Proliferation Financing Risk Assessment*, February 2024.

Vice. *Warum Nordkorea in Afrika riesige Denkmäler für Diktatoren baut*, 6 February 2018.

WA. *The Wassenaar Arrangement*, last checked on 5 September 2024.

Wehrey, Frederic, et al. *Economic Expansion: The IRGC's Business Conglomerate and Public Works*. The Rise of the Pasdaran: Assessing the Domestic Roles of Iran's Islamic Revolutionary Guards Corps, RAND Corporation, 2009, JSTOR.

Wilson Center. *North Korea, the Smuggler State*, 18 September 2017.

WIPO, *Global Innovation Index 2023: Switzerland, Sweden and the U.S. lead the Global Innovation Ranking; Innovation Robust but Startup Funding Increasingly Uncertain*, 27 September 2023.

WirtschaftsWoche, *Bodenschätze im Wert von sieben Billionen US-Dollar*, last checked on 5 September 2024.
YaleGlobal Online, *North Korea's Missile Trade Helps Fund Its Nuclear Program*, 5 May 2003.

Zeit Online, *Treffen in Teheran: Russland, die Türkei und der Iran wollen in Syrien zusammenarbeiten*, 19 July 2022.

10. Annex 1

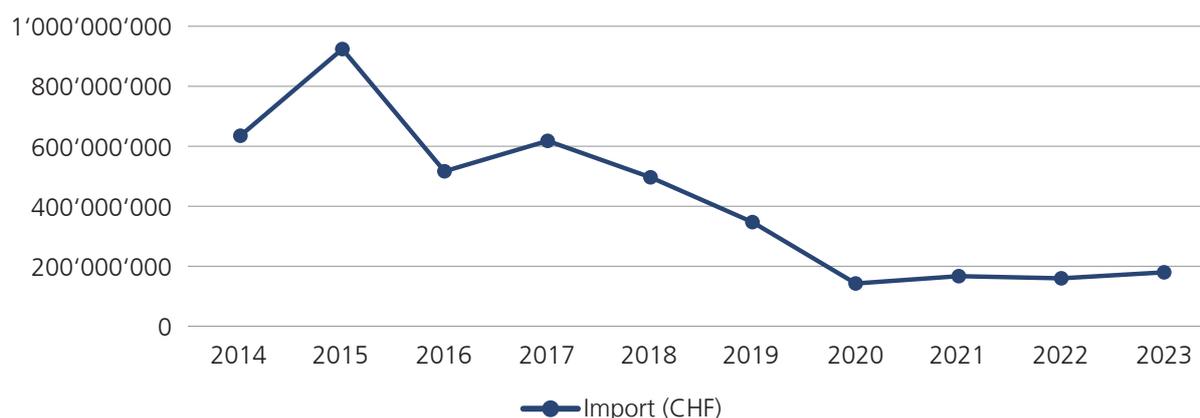
10.1 Data and statistics on Iran

10.1.1 Bilateral trade in goods with Iran between 2000-2023²⁵⁵

Since 2019, bilateral trade in goods between Switzerland and Iran has remained at a comparatively low level, partly due to the reintroduction of US sanctions. In 2023, it amounted to CHF 183 million.²⁵⁶ It should be emphasised that Swiss exports are significantly higher than imports, which are subject to sanctions for the most part. Imports to Switzerland mainly consisted of Persian rugs, food (e.g. spices such as saffron and Govinda barberry) and clothing. Importing companies in Switzerland include furniture retailers and companies engaged in the food industry. Consignments from Iran are subject to risk-based inspection by the FOCBS. The range of exported goods includes mostly machinery (electrical and non-electrical), pharmaceuticals, chemicals, precision instruments and plastics. Exports were undertaken by companies engaged in the tool and fastening systems sector or in the food industry. These shipments involved non-listed goods that do not require an export licence from SECO or the SFOE. These exports are in turn monitored by the FOCBS on a risk-oriented basis. Between 2014 and 2023, the most frequently exported goods to Iran were drawing parts and fasteners (4,478x), perfume mixtures (2,232x) and food flavouring samples (1,432x). The exporters from Switzerland were companies engaged in the tooling and fastening technology or in the food industry. The three most frequent recipients of these goods were Iranian partner companies of the exporting Swiss companies. In some cases, the exporting Swiss company had its own representative office in Iran with its own staff.

Before Switzerland adopted sanctions against Iran in 2007, bilateral trade in goods with Iran rose gradually between 2000 and 2005 from CHF 577 million to CHF 804 million. Between 2006 and 2018, it then developed unevenly, fluctuating between CHF 363 million and CHF 925 million each year. Since 2019, trade between Switzerland and Iran has been at a comparatively lower level. Specifically, trade amounted to CHF 350 million in 2019, CHF 147 million in 2020, CHF 170 million in 2021, CHF 163 million in 2022 and CHF 183 million in 2023 (see graph on imports and exports in CHF).

Cumulative imports and exports between Switzerland and Iran (in CHF)

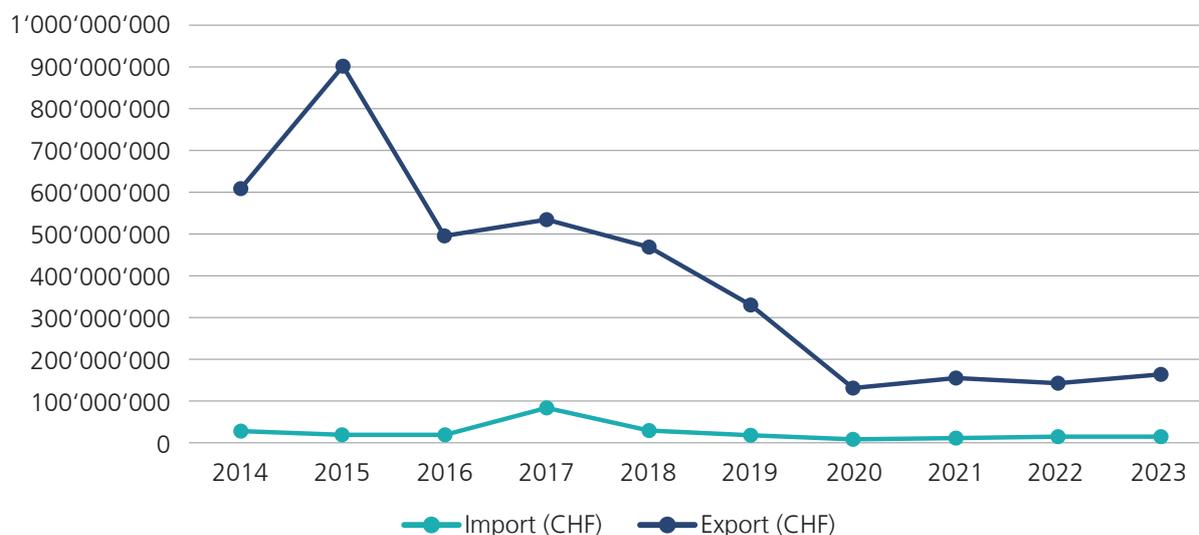


²⁵⁵ Federal Office for Customs and Border Security (FOCBS), *Foreign trade statistics*, last checked on 13 July 2023.

²⁵⁶ In comparison: Trade between Switzerland and the EU in 2023 amounted to CHF 296 billion

Generally speaking, Switzerland has always had a large trade surplus with Iran, as Swiss exports are significantly higher than imports (see graph on imports and exports in CHF).

Imports and exports in CHF



10.1.2 Administrative criminal decisions based on Iran Ordinance

Based on the Ordinance of 11 November 2015 on Measures Against the Islamic Republic of Iran, there have been a total of 14 legally binding administrative criminal decisions (penalty notices and discontinuation orders) since 2013. In none of these cases was there any recognisable direct or indirect link to proliferation or proliferation financing. However, such a link cannot be completely ruled out in most of the cases.

	Breach	Legal categorisation	Decision date	Proliferation, incl. proliferation financing
1)	Duty to report and authorisation requirement (Art. 12)	Contravention/misdemeanour	27 January 2014	Cannot be ruled out
2)	Duty to report (Art. 12)	Contravention	29 January 2014	No
3)	Duty to report and authorisation requirement (Art. 12)	Contravention/misdemeanour	10 February 2014	No
4)	Duty to report and authorisation requirement (Art. 12)	Contravention/misdemeanour	12 February 2014	Cannot be ruled out
5)	Duty to report (Art. 6a) and authorisation requirement (Art. 12)	Contravention/misdemeanour	17 July 2014	Cannot be ruled out
6)	Duty to report (Art. 6a) and authorisation requirement (Art. 12)	Contravention/misdemeanour	30 January 2015	Cannot be ruled out

7)	Duty to report (Art. 11)	Contravention	17 August 2015	Cannot be ruled out
8)	Duty to report (Art. 12)	Contravention	21 September 2015	Cannot be ruled out
9)	Duty to report (Art. 12)	Contravention	14 April 2016	No
10)	Provisioning ban (Art. 10) and duty to report (Art. 11)	Contravention/misdemeanour	14 December 2016	Cannot be ruled out
11)	Authorisation requirement (Art. 3)	Misdemeanour	27 May 2019	Cannot be ruled out
12)	Authorisation requirement (Art. 3)	Misdemeanour	17 June 2019	Cannot be ruled out

Failure to comply with the duty to report (see table, cases 1-10) usually occurs when persons or institutions subject to reporting obligations fail to report frozen funds or economic resources to SECO, or fail to report them in a timely fashion. In the case of a failure to comply with authorisation requirements, a corresponding request for authorisation is also not made or is not made in a timely manner. Failure to comply with the duty to report is legally qualified as a contravention, while failure to comply with authorisation requirements usually constitutes a misdemeanour. In the case of an export of goods, for example, it may well be that if the sale and delivery as well as the export and transit are prohibited, proceedings may have to be initiated against more than one party in individual cases. For example, in cases 11 and 12, proceedings were initiated against both the importer or exporter and the freight forwarder. Of the administrative criminal proceedings listed, two were discontinued (see table, cases 3 and 12). In one of the cases, the proceedings were discontinued because there was neither intent nor negligence (subjective evidence). In the second case, it turned out that the main offence had been committed out of negligence, for which aiding and abetting is neither possible nor punishable.

Since 17 January 2016, there has no longer been any requirement to report or approve transfers of funds to or from Iran under the Ordinance of 11 November 2015 on Measures Against the Islamic Republic of Iran.

10.1.3 Rejections of goods based on EmbA, WMA and GCA

SECO publishes annual statistics on the export of war materiel²⁵⁷ as well as quarterly statistics on individual export licences for dual-use goods and specific military goods.²⁵⁸ Exports subject to the GCA are also included in the foreign economic policy report.²⁵⁹ Export licences are applied for via the electronic licensing platform ELIC.²⁶⁰

257 SECO, Military supplies, *Zahlen und Statistiken*, last checked on 10 September 2024.

258 SECO, Dual-Use and specific military goods, *Zahlen und Statistiken/ab 2015*, last checked on 10 September 2024.

259 SECO, *Bericht zur Aussenwirtschaftspolitik 2022 einschliesslich Botschaften zu Wirtschaftsvereinbarungen sowie Bericht über zolltarifische Massnahmen im Jahr 2022*, 11 January 2023, last checked on 27 July 2023.

260 SECO, *E-Licensing ELIC*

A total of 124 applications for Iran were rejected between 1991 and 2023 under EmbA and GCA provisions. Between 2001 and 2011, a total of 77 applications for Iran were rejected, whereas in the period 2014-2023, only 7 applications were officially rejected (for 17 items). In the same period, 50 applications (for 53 items) for the export of GCO-listed goods and sanctioned goods were withdrawn by the customers themselves. Most of the goods rejected under Art. 6 GCA were dual-use goods, such as machine tools or corresponding software. The application relating to nuclear goods was for a service.

Applications for an export licence from 2014 to 2023 (Number of items)	Total number	Dual-use goods listed in Annexes 1,2 GCO	Annex 3 GCO (special military goods)	Nationally controlled goods listed in Annex 5 GCO	Nuclear goods	Sanctioned goods listed in Ordinance SR 946.231.143.6
Applications relating to listed goods²⁶¹	748	118 (62 AG, 44 WA, 3 MTCR, 9 NSG)	1	44	7	578
Applications withdrawn by customer	53	27	0	8	1	10
Applications rejected	17	11	1	2	1	2

No licences for the export of war materiel were issued between 2014 and 2023. Two applications for an annex to the Ordinance of 21 August 2013 on the Control of Chemicals with Civilian and Military Uses were also submitted during this period, with one application being approved and one being withdrawn by the customer. A single application for an item with catch-all relevance to weapons of mass destruction was approved for a measuring device.

In the period from 2014 to 2023, SECO also issued 163 export licences for sanctioned goods to be sent to Iran. In this period, SECO also received around 2,600 requests for confirmation that the goods to be exported to Iran were not covered by the annexes to the GCO or were subject to sanctions.

261 Goods listed in Annexes 1, 2, 3 and 5 of the GCO, and sanctioned goods as per Ordinance SR 946.231.143.6

10.1.4 Financial statistics for Iran

Between 2014 and 2020, the balance of payments and international investment position in relation to Iran fluctuated between CHF 0 and 1 million. By the end of 2021, the figure had risen to CHF 9 million, after which it fell again to CHF 2 million by the end of 2023.²⁶²

Banking statistics^{263, 264} for Iran are as follows:

	End of 2023 (CHF)	Between 2014-2023 ²⁶⁵
Liquid assets	0	0
Amounts due from customers	77,000	This value fell sharply from 2014 onwards and fluctuated between CHF 746,000 and CHF 32,000 from the end of 2017 to 2023.
Trading portfolio assets	0	This value was CHF 820,000 in 2018 and CHF 986,000 in 2019, in all other years it is CHF 0.
Total assets	90,000	As of the end of 2017, this value fluctuated between approximately CHF 9.7 million and CHF 75,000.
Amounts due in respect of customer deposits	87,854,000	This value fell from around CHF 643.6 million at the end of 2014 to CHF 87.85 million.
Amounts due to banks	139,269,000	This value increased to around CHF 1.63 billion by 2017 and has since then steadily dwindled to CHF 139.27 million.
Total liabilities	227,149,000	This value steadily decreased from CHF 1.86 billion in 2017 to CHF 227.15 million in 2023.
Fiduciary assets and liabilities	2,326,000	The value of fiduciary liabilities amounted to CHF 3.6 million at the end of 2017, CHF 0 for the period 2018 to 2021, CHF 4.9 million for 2022 and CHF 2.3 million for 2023. The value of fiduciary assets remained at CHF 0 for the entire period.

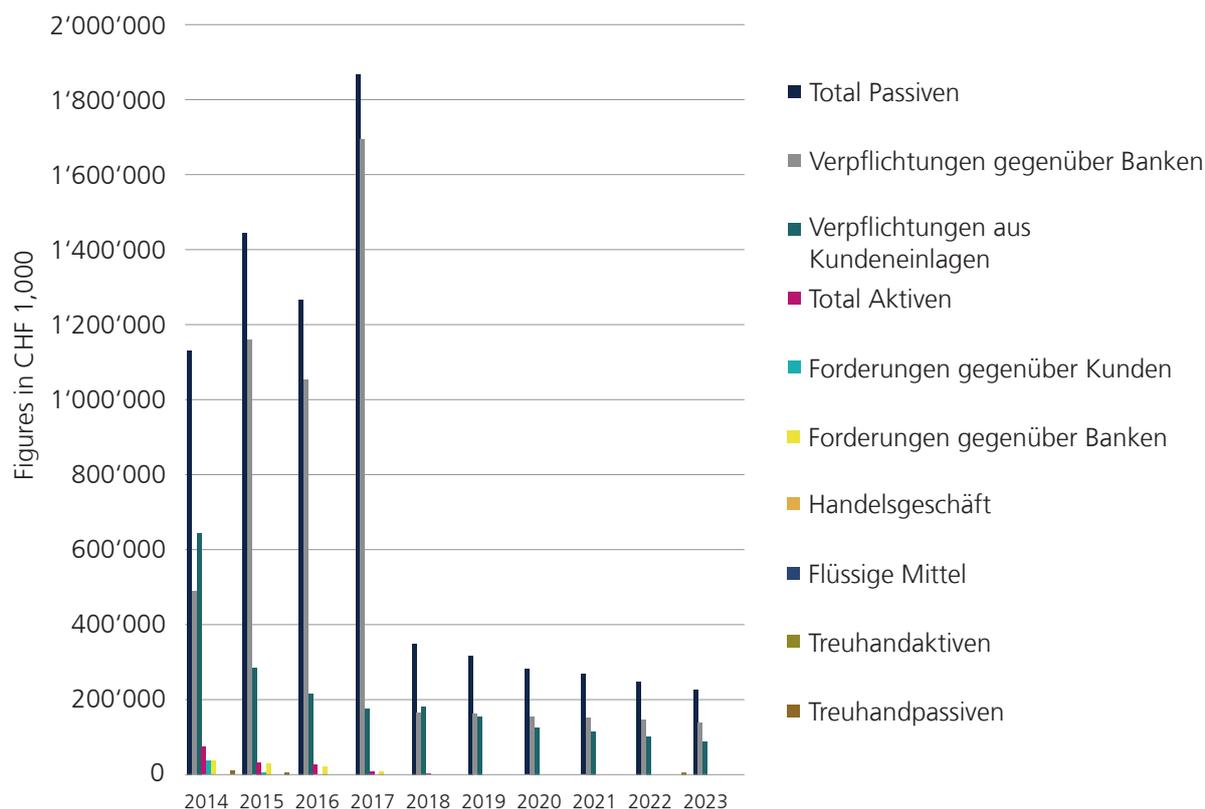
262 Source: Swiss National Bank (SNB), *Swiss balance of payments and international investment position*, Iran, last checked on 24 June 2024.

263 Source: Swiss National Bank (SNB), *Supplementary data on banking statistics*, Iran, last checked on 24 June 2024.

264 The volumes in banking statistics are aggregated balance sheet items (e.g. liabilities from customer deposits) or fiduciary transactions reported by banks in Switzerland at the end of the year. Allocation to North Korea or Iran is based on the domicile of the counterparty. The underlying transactions were carried out either at business premises in Switzerland or at branches abroad. In the case of customer deposits, for example, this means that the Swiss bank may have accepted the deposits via a branch abroad.

265 Unless otherwise noted, these figures have remained stable.

Banking statistics for Iran 2014-2023



Financial flows between Switzerland and Iran since 27 January 2020 are partly related to the Swiss Humanitarian Trade Agreement (SHTA).²⁶⁶ This payment mechanism enables trade finance to be provided to Swiss companies and trading companies engaged in the food, pharmaceutical and medical sectors for the delivery of humanitarian goods. Because of the heightened due diligence requirements, this mechanism is also compatible with US sanctions against Iran. By the end of August 2022, a total of four transactions worth around EUR 4.5 million had been processed through the SHTA for cancer and transplant drugs, accessory medical devices and dental hygiene products.

Based on these banking statistics, both domestic and foreign, Iran accounts for no more than 0.009% of the total assets held for the various individual financial activities.

10.1.5 Statistics on foreign nationals and issuance of visas

At the end of 2023, there were 5,521 Iranian nationals legally residing in Switzerland. This figure has been rising steadily since 2014, when the figures stood at 3,624 Iranian nationals. Most of these individuals hold a regular type B residence permit (66.7%) or a type C settlement permit (32.1%), with the remainder holding a short-term type L residence permit (1.2%). In addition to this, there are around 50 to 70 Iranian nationals who visit Switzerland each year for short stays without a residence permit. And finally, a total of 159 Iranian nationals acquired Swiss citizenship through naturalisation in 2023. In 2022, the figure stood at 180 people. This was the highest number since 2013, although it consistently exceeded 100 people annually. Since 2014, between 1,000 and 1,750 asylum proceedings involving Iranian nationals remain pending each year, with an average of 450 new asylum applications being submitted annually.

In addition, 11,519 visas were issued to Iranian citizens and 1,148 visa applications were rejected (10%) in 2023. In the three previous years, the number of visas granted was lower, but this was mainly due to the entry restrictions imposed as a result of the COVID-19 pandemic. In 2022, the visa rejection rate was 29.6%. It is not possible to determine whether these visa applications were rejected out of proliferation concerns.

²⁶⁶ SIF, *Payment mechanism for humanitarian supplies to Iran in effect*, 27 February 2020, last checked on 28. August 2023.

10.2 Data and statistics on North Korea

10.2.1 Bilateral trade in goods with North Korea between 2000-2023²⁶⁷

Bilateral trade in goods between Switzerland and North Korea is also almost non-existent due to the sanctions and poses no proliferation financing risks: three Swiss companies delivered dairy products to the UN World Food Programme (WFP) and the UN Children's Fund (UNICEF) in North Korea between 2000 and 2023. The export of milk powder, medical goods and other humanitarian goods is not prohibited and is organised and carried out by international organisations. In addition, a small number of watches and watch accessories were delivered, although these were not models subject to the ban on luxury goods.²⁶⁸ And finally, FIFA sends documents from Switzerland to the North Korean football association.

Since 18 May 2016, all exports and transits to North Korea require a written declaration to SECO at least five days before the planned export.²⁶⁹ SECO forwards these documents to the relevant customs office for review. Since February 2017, the FOCBS has inspected every import and transit shipment from North Korea and every export to North Korea. Between 2011 and 2014, bilateral trade in goods between Switzerland and North Korea was extremely low. Based on figures up to 2017, imports related mainly to textile and clothing goods, which are nevertheless also prohibited at the present time. No imports from North Korea have been reported since 2018, apart from documents or diplomatic bags.

10.2.2 Administrative criminal decisions based on North Korea Ordinance

All in all, there have been three judgments in administrative criminal proceedings relating to the Ordinance of 18 May 2016 on Measures Against the Democratic People's Republic of Korea. The outcome was either a penalty notice or a discontinuation order.

	Breach	Legal categorisation	Date of judgment	Proliferation, incl. proliferation financing
1)	Obligation to provide information (Art. 3)	Contravention	20 January 2020	Cannot be ruled out
2)	Joint venture ban (Art. 8a), Ban on the provision of financial services and money transfers (Art. 10) and Control of import, export and transit (Art. 17)	Contravention/ misdemeanour	29 November 2021	Cannot be ruled out
3)	Control of import, export and transit (Art. 17)	Contravention	29 November 2021	Cannot be ruled out

Case 1 was dropped because the accused complied with his duty to provide information in accordance with Art. 3 EmbA during ongoing proceedings, and thus objectively no longer violated this provision.

10.2.3 Rejections of goods based on EmbA, WMA and GCA

SECO publishes annual statistics on the export of war materiel²⁷⁰ as well as quarterly statistics on individual export licences for dual-use goods and specific military goods.²⁷¹ Exports subject to the GCA are also included in the foreign economic policy report.²⁷²

²⁶⁷ Federal Office for Customs and Border Security (FOCBS), *Foreign trade statistics*, last checked on 13 July 2023.

²⁶⁸ See North Korea Ordinance, Annex 5, status as of 1.06.2023.

²⁶⁹ See North Korea Ordinance, Art. 17 paras 2 and 3, status as of 1.06.2023.

²⁷⁰ SECO, *Zahlen und Statistiken*, last checked on 28 July 2023.

²⁷¹ SECO, *Zahlen und Statistiken/ab 2015*, last checked on 28 July 2023

²⁷² SECO, *Bericht zur Aussenwirtschaftspolitik 2022 einschliesslich Botschaften zu Wirtschaftsvereinbarungen sowie Bericht über zolltarifische Massnahmen im Jahr 2022*, 11 January 2023, last checked on 27 July 2023.

Only one application for North Korea was rejected in the period from 1991 to 2023 under GCA provisions. The application in question was submitted in 2005 and related to a vacuum pump. Two applications were withdrawn in the period 2012-2023.

10.2.4 Financial statistics for North Korea

At the end of 2023, the balance of payments and the international investment position in relation to North Korea amounted to CHF 10,000. This number remained stable at CHF 0 from the end of 2014 to the end of 2023.²⁷³

Banking statistics²⁷⁴ for North Korea are as follows:

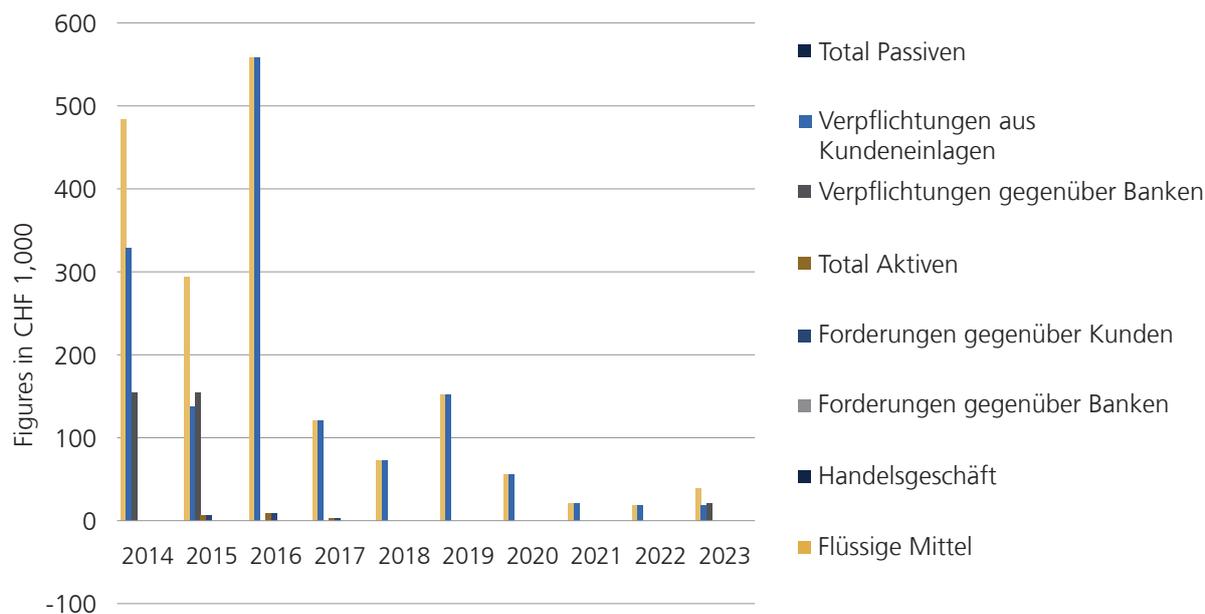
	End of 2023 (CHF)	Between 2014-2023 ²⁷⁵
Liquid assets	0	0
Amounts due from customers	0	The value rose to CHF 9,000 in 2016 and fell to CHF 0 in the following two years. It has remained stable at CHF 0 since 2019.
Trading portfolio assets	0	0
Total assets	0	The value rose to CHF 9,000 in 2016 and fell to CHF 0 in the following two years. It has remained stable at CHF 0 since 2019.
Amounts due in respect of customer deposits	Rounded to 19,000	This value fluctuated at around CHF 559,000 at the end of 2014 and has now been rounded to CHF 19,000.
Amounts due to banks	Rounded to 21,000	This value was just under CHF 156,000 in 2014 and 2015 and remained at CHF 0 between 2016 and 2022.
Total liabilities	Rounded to 39,000	This value fell from CHF 485,000 at the end of 2014 (with a peak of CHF 559,000 in 2016) and was rounded to CHF 39,000 in 2023.
Fiduciary assets and liabilities	0	0

²⁷³ Source: Swiss National Bank (SNB), *Swiss balance of payments and international investment position*, North Korea, last checked on 24 June 2024.

²⁷⁴ Source: Swiss National Bank (SNB), *Supplementary data on banking statistics*, North Korea, last checked on 24 June 2024.

²⁷⁵ Unless otherwise noted, these figures have remained stable.

Banking statistics for North Korea 2014-2023



Based on these banking statistics, which include both domestic and foreign assets, the individual business relationships linked to North Korea account for no more than 0.009% of the total assets held for the various individual financial activities.

10.2.5 Statistics on foreign nationals and issuance of visas

In line with the relevant resolutions adopted by the UN Security Council, Switzerland does not grant work permits to North Korean citizens, and North Korean workers in Switzerland have left the country.

Looking at the usual resident population of Switzerland, we find a total of eight North Korean nationals legally residing in Switzerland at the end of 2023. This constitutes a steady decline since 2014, when there were sixteen residents. Three of these individuals hold a settlement permit (type C permit), the remainder hold regular residence permits (type B permit). There are no North Koreans residing in Switzerland who do not hold a residence permit. Moreover, the last time a North Korean national obtained Swiss citizenship through naturalisation was in 2013. No visa applications were rejected.

In addition, 41 North Korean nationals work in Switzerland (at the North Korean embassy in Bern, at the Permanent Mission of North Korea to the United Nations in Geneva, or at an international organisation) or accompany such a person (family).²⁷⁶

Since 2014, no more than two asylum proceedings per year have related to North Korea, and no new asylum application has been filed since 2018.

276 Status as of October 2023

10.3 Other data

10.3.1 Suspicious activity reports sent to MROS

When submitting an SAR, reporting financial intermediaries describe in writing the circumstances surrounding the suspicious transactions and explain their reasons for filing an SAR.

Between 2012 and 2023, a total of 83,493 business relationships were reported to MROS.²⁷⁷ It is interesting to note that the word ‘proliferation financing’ was mentioned in the circumstances described in only ten business relationships (0.01% of the total), all of which were in the years 2022 to 2023. The word ‘proliferation’ (without ‘proliferation financing’) was mentioned in 35 business relationships (0.04% of the total). The 35 business relationships were reported to MROS by only three different banks.²⁷⁸ The word ‘Iran’ was mentioned in 800 business relationships (0.96% of the total), while ‘North Korea’ was only mentioned in 119 business relationships (0.14% of the total).²⁷⁹

Furthermore, between 2012 and 2023, only 173 reported business relationships related to Iranian nationals who were either contracting parties²⁸⁰ or beneficial owners²⁸¹ (0.21% of all reported business relationships). Only seven reported business relationships related to legal entities domiciled in Iran (0.01% of all reported business relationships). During the same period, MROS reported that there were no business relationships involving natural persons of North Korean origin or legal entities domiciled in North Korea.

277 The term ‘business relationship’ refers to the contractual or commercial relationship between a financial intermediary and a specific client. A business relationship can include several accounts (e.g. a current account, a savings account and a brokerage account). The introduction of the goAML system has changed the way MROS counts the number of SARs it receives: since 1 January 2020, MROS has been counting the number of SARs and not, as previously, the number of reported business relationships. Since a single SAR may include multiple business relationships maintained by the reporting FI, it is therefore difficult to make precise comparisons with the figures from previous years, when MROS was reporting on the number of business relationships. In 2019, each SAR that MROS received from Swiss financial intermediaries related to an average of 1.8 business relationships. This average was used to enable comparisons between the years following the transition to goAML and the years prior to this transition. Since the ‘reports’ examined in the present analysis were mostly submitted before 1 January 2020, MROS decided to include the number of business relationships in the present calculations.

278 To put this in perspective, according to MROS there were a total of 239 banks in Switzerland in the 2021 financial year, whereas the total number of financial intermediaries subject to reporting obligations in Switzerland is estimated to be in the low four digits. See statistics of the Swiss National Bank (SNB), *Number of banks for all bank categories*, last checked on 24 June 2022.

279 All keywords were used in different languages (German, Italian, French, English) and possible spellings for the text search.

280 Clients of Swiss financial intermediaries

281 The actual owners of the assets held in the reported accounts

2012 – 2023	Reported business relationships
Total volume	83,493 (100%)
PF-relevant predicate offences ²⁸²	197 (0.28%)
Reporting financial intermediary mentioned the keyword 'proliferation financing' when describing the facts in the SAR	10 (0.005%)
Reporting financial intermediary mentioned the keyword 'proliferation' when describing the facts in the SAR	35 (0.04%)
Reporting financial intermediary mentioned the keyword 'Iran' when describing the facts in the SAR	800 (0.96%)
Reporting financial intermediary mentioned the keyword 'North Korea' when describing the facts in the SAR	119 (0.14%)
Reported business relationships with contracting parties and/or beneficial owners from Iran (natural persons or legal entities)	180 (0.22%)
Reported business relationships with contracting parties and/or beneficial owners from North Korea (natural persons or legal entities)	0 (0%)

Between 2012 and 2023, MROS received a total of 10,253 information requests²⁸³ from foreign FIUs. These requests were analysed using various methods²⁸⁴ to detect possible links to proliferation financing. For the period in question, only four information requests could be identified (0.04% of all requests) whose facts were linked to proliferation at the time when MROS carried out its analysis. However, none of the cases was explicitly linked to financing.

Between the end of November 2019 and the end of 2023, MROS received a total of 3,127 information requests from foreign FIUs, including eleven information requests (0.35% of all information requests received during this period) relating to a PF-relevant predicate offence²⁸⁵ to money laundering. For the present risk analysis, we took a second look at these requests to ascertain whether there were any links to proliferation financing. We found that only one of these eleven information requests had a confirmed link to proliferation financing.

282 PF-relevant predicate offences: Misuse of explosives and toxic gases with criminal intent (Art 224 para. 1 SCC); Manufacture, concealment and transport of explosives and toxic gases (Art. 226 SCC); Causing danger by means of nuclear energy, radioactivity or ionising radiation (Art. 226bis SCC); Causing danger by means of genetically modified or pathogenic organisms (Art. 230bis para. 1 SCC); Prohibited methods of warfare (Art. 264g SCC), Use of prohibited weapons (Art. 264h SCC); Unlawful activities on behalf of a foreign state (Art. 271 No 1 para. 4, No 2 and No. 3 SCC); Felonies and misdemeanours (Art. 14 para. 2 GCA); Failure to observe safety and security measures (Art. 88 para. 2 NEA), Offences involving nuclear goods and radioactive waste (Art. 89 para. 2 NEA); Offences against licensing and reporting obligations (Art. 33 para. 2 WMA); Offences against the prohibition of nuclear, biological and chemical weapons (Art. 34 para. 1 WMA); Offences against the prohibition of anti-personnel mines (Art. 35 WMA); Offences against the prohibition of cluster munition (Art. 35a para. 1 WMA); Offences against the prohibition of financing (Art. 35b para. 1 WMA); Felonies and misdemeanours (Art. 49 ChemA); Felonies and misdemeanours (Art. 9 para. 2 EmbA); Felonies and misdemeanours (Art. 33 para. 3 WG)

283 A single information request can contain requests regarding multiple subjects (natural persons or legal entities) as well as multiple accounts or business relationships (with different financial intermediaries).

284 Following the introduction of the goAML system, information requests from foreign FIUs are entered into the system in various forms, determined by when MROS received them. Different indicators can be evaluated depending on when the request is received. For this reason, we cannot exclude the possibility that a small number of information requests were not taken into account in the figures provided.

285 PF-relevant predicate offences: See footnote 282

10.4 Trade in nuclear materials

Several companies in Switzerland are involved in brokering nuclear materials. The Swiss Federal Office of Energy (SFOE) requires quarterly reporting, with specific mention of trading partners and quantities, as a requisite to obtain a licence to handle and trade nuclear materials within the meaning of Art. 13 let. a of the Nuclear Energy Ordinance.

Between 2014 and 2023, eight companies were granted such a licence or had their licence renewed. A total of 81 licences were issued. Each licence is currently valid for a period of 12 months.

10.5 Applications for Swiss Export Risk Insurance (SERV)

SERV has not accepted any insurance applications for exports to North Korea in the last 10 years due to the proliferation risk.

In Iran, SERV has mainly provided insurance coverage for the delivery of medicines and, to a lesser extent, trade in the areas of mechanical engineering and electronics, none of which involved proliferation-sensitive goods. It has had no outstanding insurance policies in Iran since 2020.