Regulatory disclosure requirements

Capital requirements

		2024	2023
Eligible capital			
Common Equity Tier 1 (CET1) capital	kCHF	57 730	63 056
Tier 1 capital	kCHF	57 730	63 056
Total eligible capital	kCHF	57 730	63 056
Risk-weighted assets (RWA)			
RWA	kCHF	44 218	29 384
Minimum capital requirements	kCHF	3 537	2 351
Capital ratios in % of RWA			
CET1 ratio	%	130.6%	214.6%
Tier 1 ratio	%	130.6%	214.6%
Total eligible capital ratio	%	130.6%	214.6%
Additional CET1 buffer requirements as a percentage of RWA			
Capital conservation buffer requirement according to the Basel minimum standard	%	2.5%	2.5%
Countercyclical buffer requirement (art. 44a Capital Adequacy Ordinance (CAO)) according to the Basel minimum standard	%	0.0%	0.0%
Additional capital buffer for international or national systemic risk	%	0.0%	0.0%
Total of bank CET1 specific buffer requirements	%	2.5%	2.5%
CET1 available to cover buffer requirements according to the Basel minimum standard after meeting the bank's minimum capital requirements according to the Basel minimum standard	%	122.6%	206.6%
Target equity ratios according to appendix 8 of the CAO (in % of RWA)			
Equity buffer according to Appendix 8 CAO	%	2.5%	2.5%
Countercyclical equity buffer (Art. 44 and 44a CAO)	%	0.0%	0.0%
Target ratio in CET1 (in %) according to Appendix 8 of the OFR, plus the countercyclical buffers according to Art. 44 and 44a CAO	%	7.0%	7.0%
Target ratio in Tier 1 (in %) according to Appendix 8 of the OFR, plus the countercyclical buffers according to Art. 44 and 44a CAO	%	8.5%	8.5%
Target ratio in Eligible capital (in %) according to Appendix 8 of the OFR, plus the countercyclical buffers according to Art. 44 and 44a CAO	%	10.5%	10.5%
Basel III leverage ratio			
Total Basel III leverage ratio exposure measure	kCHF	61 985	67 483
Basel III leverage ratio	%	93.1%	93.4%

Overview of RWA

	2024		2023	
	RWA kCHF	Minimum capital requirements kCHF	RWA kCHF	Minimum capital requirements kCHF
Credit risk - standardised approach	14 930	1 194	9 572	766
Market risk - standardised approach	8 838	707	4 288	343
Operational risk - basic indicator approach	20 450	1 636	15 525	1 242
Total	**44 218**	**3 537**	**29 384**	**2 351**

Credit risk - standardised approach

	Risk weighting					
All amounts in kCHF	0%	20%	100%	400%	800%	Total
Sovereigns	46 113					46 113
Banks & Securities dealers		10 977				10 977
Other institutions						
Corporates			1 386			1 386
Retail						
Equity						
Others			2 574	35	1 080	3 689
TOTAL	**46 113**	**10 977**	**3 960**	**35**	**1 080**	**62 165**
TOTAL weighted	**-**	**2 195**	**3 960**	**138**	**8 638**	**14 930**

Liquidity requirements

		2024	2023
Liquidity coverage ratio			
LCR numerator: sum of high-quality liquid assets	kCHF	46 113	56 398
LCR denominator: net cash outflow	kCHF	905	1 006
LCR ratio	%	5095%	5606%
Net stable funding ratio			
Total available stable funding	kCHF	58 438	63 645
Total required stable funding	kCHF	5 979	4 184
NSFR ratio	%	977%	1521%

Credit risk: credit quality of assets

All amounts in kCHF	Default exposures	Non-default exposures	Allowances/ impairments	Net values
Amounts due from customers	-	1 837	(461)	1 376
Debt securities	-	-	-	-
Off-balance sheet exposures	-	10	-	10
Total current year	**-**	**1 846**	**(461)**	**1 386**

Credit risk: overview of credit risk mitigation techniques

	Exposures unsecured	Exposures secured			
	Carrying amount	Carrying amount	By collateral	By financial guarantee	By credit derivatives
Amounts due from customers	1 376	-	-	-	-
Off-balance sheet	10	-	-	-	-
Total current year	**1 386**	**-**	**-**	**-**	**-**
of which, defaulted	-	-	-	-	-

Operational risks

In general

Operational risks are due to the inadequacy of, or failure in procedures, controls, systems, people or result from external events. They can generate financial losses or trigger a discontinuity of the Company's operations or affect its operating conditions. The operational risk is assessed and monitored with Key Risk Indicators for which thresholds have been defined which depict the Company's risk tolerance. Those indicators are monitored by the three independent control functions: Risk management, ICT Security and Compliance. Corrective measures are taken when necessary. Operational losses are systematically logged and analysed in order to find out whether modifications in processes and controls are necessary. The Company applies the basic indicator approach (BIA) for the calculation of required capital.

Regulatory and compliance risks

The Compliance Officer monitors that the Company complies with the legal requirements in place as well as its obligations with regards to the exercise of due diligence applying to financial intermediaries. The Compliance Officer keeps up to date with legal developments coming from the supervisory bodies, the government, the parliament and other organisms. He supervises as well over the updating of the internal directives to take into account new legislative and regulatory requirements.

ICT and cybersecurity risks

Security is a paramount element of the reputation of the Company and must be at the heart of all the main technological choices taken by the Technology unit. The Company appoints a Chief Security Officer ("CSO") who reports to the Executive Committee and has direct access to the Chief Technology Officer ("CTO"). The CSO cannot be the CTO.

The Company implements an ICT security and cyber-risk policy that defines its ICT security and cyber-risk management framework which provides the foundations and organisational arrangements for designing, implementing, monitoring, and continuously improving ICT security and cyber-risk management throughout the Company includes the following items:

- Risk identification: identify cyber-risks related to data and critical ICT infrastructure and applications which are specific to the Company's operating model;
- Protection mechanisms: ensure proper protection against cyber-risks and cyber-attacks in particular in relation to confidentiality, integrity, availability of elements mentioned in the above point;
- Applications & infrastructure monitoring: rapid identification and evaluation of potential cyber-attacks thanks to a systematic surveillance of the application landscape and of the ICT infrastructure;
- Incident management: reaction to incidents, including security incidents thanks to targeted and immediate incident response measures and link with the Company's Business Continuity Management ("BCM") processes;
- Business continuity: ensure, within the targets defined in the BCM policy, an appropriate return to business-as usual mode after an incident.