Regulatory disclosure requirements

Capital requirements

		2022	2021
Eligible capital			
Common Equity Tier 1 (CET1) capital	kCHF	12 441	13 665
Tier 1 capital	kCHF	12 441	13 665
Total eligible capital	kCHF	12 441	13 665
Risk-weighted assets (RWA)			
RWA	kCHF	20 196	23 450
Minimum capital requirements	kCHF	1 616	1 875
Capital ratios in % of RWA			
CET1 ratio	%	61,6%	58,3%
Tier 1 ratio	%	61,6%	58,3%
Total eligible capital ratio	%	61,6%	58,3%
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	%	-	-
Additional capital buffer for international or national systemic risk	%	-	-
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	%	53,6%	50,3%
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)	%	-	-
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	13 957	16 057
Basel III leverage ratio	%	89,1%	85,1%

Overview of RWA

	2022		2021	
	RWA kCHF	Minimum capital requirements kCHF	RWA kCHF	Minimum capital requirements kCHF
Credit risk - standardised approach	5 646	452	13 831	1 106
Market risk - standardised approach	4 275	342	2 966	237
Operational risk - basic indicator approach	10 275	822	6 658	532
Total	**20 196**	**1 616**	**23 450**	**1 875**

Credit risk - standardised approach

	Risk weighting				
All amounts in kCHF	0%	20%	100%	800%	Total
Sovereigns	3 667				
Banks & Securities dealers		8 785			
Other institutions					
Corporates			545		
Retail					
Equity					
Others			619	341	
TOTAL	**3 667**	**8 785**	**1 163**	**341**	**13 957**
TOTAL weighted	**0**	**1 756**	**1 163**	**2 727**	**5 646**

Liquidity requirements

		2022	2021
Liquidity coverage ratio			
LCR numerator: sum of high-quality liquid assets	kCHF	3 667	N/A(*)
LCR denominator: net cash outflow	kCHF	379	N/A(*)
LCR ratio	%	968%	N/A(*)
Net stable funding ratio			
Total available stable funding	kCHF	12 577	14 206
Total required stable funding	kCHF	2 535	4 102
NSFR ratio	%	496%	346%

(*) FINMA has granted the Company a waiver of the liquidity requirements until 31 December 2021, until the Company has an account with the Swiss National Bank.

Credit risk: credit quality of assets

All amounts in kCHF	Defaulted exposures	Non-defaulted exposures	Allowances/ Impairments	Net values
Amounts due from customers	-	706	(161)	545
Debt securities	-	-	-	-
Off-balance sheet exposures	-	2	-	2
Total current year	**-**	**708**	**(161)**	**547**

Credit risk: overview of credit risk mitigation techniques

All amounts in kCHF	Exposures unsecured	Exposures secured			
	Carrying amount	Carrying amount	By collateral	By financial guarantees	By credit derivatives
Amounts due from customers	545	-	-	-	-
Off-balance sheet	2	-	-	-	-
Total current year	**547**	**-**	**-**	**-**	**-**
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, IT 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 Company 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 Company's internal directives to take into account new legislative and regulatory requirements.

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

- Risk identification: identify cyber-risks related to data and critical IT 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 IT 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.