NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: CHE - FINMA Circular 2023/1 - Operational Risks and Resilience - Banks
Focal Document URL: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-che-finma-circ-23-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
I	Subject and scope of application	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
I-1	Subject and scope of application	This Circular relates to the rules on the segregation of duties, risk management and internal controls contained in the Banking Ordinance (Arts. 12 and 14e BO, SR 952.02) and the Financial Institutions Ordinance (Arts. 12 and 68 FinIO; SR 954.11) and sets out the corresponding supervisory practice. It takes account of the Basel Committee's principles for the sound management of operational risk and operational resilience.	Functional	No Relationship	N/A	N/A	N/A	0	
I-2	Subject and scope of application	This Circular applies to banks under Article 1a and persons under Article 1b of the Banking Act (BA; SR 952.0), securities dealers under Article 2 para. 1 let. e and Article 41 of the Financial Institutions Act (FinIA; SR 954.1), and financial groups and financial conglomerates under Article 3c BA and Article 49 FinIA. In the following, banks, persons under Article 1b BA, securities firms, financial groups and financial conglomerates are referred to collectively as "institutions".	Functional	No Relationship	N/A	N/A	N/A	0	
II	Definition of terms	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
II-3	Definition of terms	Operational risk is defined in Article 89 CAO. It refers to the risk of financial loss resulting from inadequate or failed internal processes or systems, inappropriate actions taken by people or mistakes made by them, or from external events. This includes the financial losses that can result from legal or compliance risks. Operational risk management typically also takes other types of damage into account, provided that these can ultimately also result in financial loss. It does not include strategic risk.	Functional	No Relationship	N/A	N/A	N/A	0	
II-4	Definition of terms	Inherent risks are operational risks that the institution is exposed to through its products, activities, processes and systems, without taking control or mitigation measures into account.	Functional	No Relationship	N/A	N/A	N/A	0	
II-5	Definition of terms	Residual risks are operational risks that the institution is exposed to after taking control and mitigation measures into account.	Functional	No Relationship	N/A	N/A	N/A	0	
II-6	Definition of terms	Information and communication technology (ICT) refers to the physical and logical (electronic) architecture of IT and communication systems, the individual hardware and software assets, networks, data and operating environments.	Functional	No Relationship	N/A	N/A	N/A	0	
II-7	Definition of terms	Critical data are data that, in view of the institution's size, complexity, structure, risk profile and business model, are of such crucial significance that they require increased security measures. These are data that are crucial for the successful and sustainable provision of the institution's services or for regulatory purposes. When assessing and determining the criticality of data, the confidentiality as well as the integrity and availability must be taken into account. Each of these three aspects can determine whether data is classified as critical.	Functional	No Relationship	N/A	N/A	N/A	0	
II-8	Definition of terms	Critical processes are processes whose significant disruption endanger the provision of critical functions. They are part of the critical functions.	Functional	No Relationship	N/A	N/A	N/A	0	
II-9	Definition of terms	Business continuity management (BCM) refers to the institution-wide approach for recovering the operation of critical processes in the event of a significant disruption going beyond incident management. It defines the response to significant disruptions. Effective BCM reduces the residual risks in connection with significant disruptions.	Functional	No Relationship	N/A	N/A	N/A	0	
II-10	Definition of terms	The recovery time objective (RTO) is the time within which an application, system and/or process must be recovered. The recovery point objective (RPO) is the maximum tolerable period during which data is lost.	Functional	No Relationship	N/A	N/A	N/A	0	
II-11	Definition of terms	The business continuity plan (BCP) is a forward-looking plan that sets out the necessary procedures, recovery options and alternative resources (the recovery processes) for ensuring continuity and recovering critical processes.	Functional	No Relationship	N/A	N/A	N/A	0	
II-12	Definition of terms	The disaster recovery plan (DRP) defines the recovery processes for achieving the recovery goals in the event of a catastrophic failure or destruction of the ICT and taking into account the possible loss of key personnel.	Functional	No Relationship	N/A	N/A	N/A	0	
II-13	Definition of terms	Crisis situations are exceptional situations that potentially threaten the institution's existence, and that cannot be managed with ordinary measures and decision-making authority. They differ from incidents and significant disruptions that can be overcome with incident management in normal operation or with the defined BCPs and DRPs.	Functional	No Relationship	N/A	N/A	N/A	0	
II-14	Definition of terms	Critical functions include:	Functional	No Relationship	N/A	N/A	N/A	0	
II.a-15	Definition of terms	the activities, processes and services - including the underlying resources necessary for their provision - whose disruption would jeopardise the institution's continuation or its role on the financial market and thus the proper functioning of the financial markets; and	Functional	No Relationship	N/A	N/A	N/A	0	
II.b-16	Definition of terms	the systemically important functions under Article 8 BA.	Functional	No Relationship	N/A	N/A	N/A	0	
II-17	Definition of terms	The tolerance for disruption is the extent (e.g. the duration or expected damage) of the disruption of a critical function that the institution is willing to accept, taking severe but plausible scenarios into account. A tolerance for disruption must be defined for each critical function.	Functional	No Relationship	N/A	N/A	N/A	0	
II-18	Definition of terms	Operational resilience refers to the institution's ability to restore its critical functions in case of a disruption within the tolerance for disruption. That is to say, the institution's ability to identify threats and possible failures, to protect itself from them and to respond to them, to restore normal business operations in the event of disruptions and to learn from them, so as to minimise the impact of disruptions on the provision of critical functions. An operationally resilient institution has designed its operating model in such a way that it is less exposed to the risk of disruptions in relation to its critical functions. Operational resilience thus reduces not only the residual risks of disruptions, but also the inherent risk of disruptions occurring. Effective operational risk management helps strengthen the institution's operational resilience.	Functional	No Relationship	N/A	N/A	N/A	0	
III	Principle of proportionality	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
III-19	Principle of proportionality	This Circular applies to all addressees. However, the requirements are to be implemented on a case-by-case basis, depending on the size, complexity, structure and risk profile of each institution. FINMA can relax or tighten the rules in individual cases.	Functional	No Relationship	N/A	N/A	N/A	0	
III-20	Principle of proportionality	Banks and securities firms in FINMA Categories 4 and 5 are exempt from complying with margin nos. 33-38, 41-46, 48, 51, 57, 73, 74, 76-78, 80, 87, 92, 93, 96, 103, 104 and 110-112.	Functional	No Relationship	N/A	N/A	N/A	0	
III-21	Principle of proportionality	Institutions under Articles 47a-47e CAO, persons under Article 1b BA, and investment firms (non-proprietarian trading) are also exempt from complying with margin nos. 72, 75, 79 and 105-109.	Functional	No Relationship	N/A	N/A	N/A	0	
IV	Operational risk management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
IV.A	Overarching operational risk management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
IV.A-22	Overarching operational risk management	Operational risk management forms part of institution-wide risk management under FINMA Circular 2017/1 "Corporate governance - banks".	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: CHE - FINMA Circular 2023/1 - Operational Risks and Resilience - Banks
Focal Document URL: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-che-finma-circ-23-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IV.A-23	Overarching operational risk management	The board of directors approves the basic principles for the management of operational risks relevant for the institution and monitors their application. Among others, these include the ICT risks, the cyber risks, the risks relating to critical data, the risks resulting from the design and implementation of BCM and, where applicable, the risks from cross-border service business. At least once a year, the board of directors approves the risk tolerance for operational risk in accordance with the risk policy, taking the institution's strategic and financial goals into account. In doing so it considers the results from the risk and control assessments under margin no. 30. It accepts either the extent to which the institution is exposed to operational risk, or decides to adjust the risk tolerance and make the strategic changes necessary for this.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
IV.A-23	Overarching operational risk management	The board of directors approves the basic principles for the management of operational risks relevant for the institution and monitors their application. Among others, these include the ICT risks, the cyber risks, the risks relating to critical data, the risks resulting from the design and implementation of BCM and, where applicable, the risks from cross-border service business. At least once a year, the board of directors approves the risk tolerance for operational risk in accordance with the risk policy, taking the institution's strategic and financial goals into account. In doing so it considers the results from the risk and control assessments under margin no. 30. It accepts either the extent to which the institution is exposed to operational risk, or decides to adjust the risk tolerance and make the strategic changes necessary for this.	Functional	Intersects With	Risk Tolerance	RSK-05.1	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
IV.A-23	Overarching operational risk management	The board of directors approves the basic principles for the management of operational risks relevant for the institution and monitors their application. Among others, these include the ICT risks, the cyber risks, the risks relating to critical data, the risks resulting from the design and implementation of BCM and, where applicable, the risks from cross-border service business. At least once a year, the board of directors approves the risk tolerance for operational risk in accordance with the risk policy, taking the institution's strategic and financial goals into account. In doing so it considers the results from the risk and control assessments under margin no. 30. It accepts either the extent to which the institution is exposed to operational risk, or decides to adjust the risk tolerance and make the strategic changes necessary for this.	Functional	Intersects With	Executive Leadership Approval For Managing Material Risk	RSK-06.1	Mechanisms exist to obtain executive leadership approval for risk management decisions involving material risk.	5	
IV.A-24	Overarching operational risk management	The board of directors regularly approves strategies for dealing with ICT, cyber risks, critical data and BCM, and monitors their application.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
IV.A-24	Overarching operational risk management	The board of directors regularly approves strategies for dealing with ICT, cyber risks, critical data and BCM, and monitors their application.	Functional	Intersects With	Strategic Plan & Objectives	PRM-02	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
IV.A-25	Overarching operational risk management	The executive board ensures in a comprehensible way that the operational risks are identified, assessed, limited and monitored, and that the effectiveness of both the design and also of the implementation of this operational risk management is regularly reviewed. It takes risk-specific supplementary or intensified measures in order to limit the inherent risks deemed to be material as the situation demands.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5	
IV.A-25	Overarching operational risk management	The executive board ensures in a comprehensible way that the operational risks are identified, assessed, limited and monitored, and that the effectiveness of both the design and also of the implementation of this operational risk management is regularly reviewed. It takes risk-specific supplementary or intensified measures in order to limit the inherent risks deemed to be material as the situation demands.	Functional	Intersects With	Risk Remediation	RSK-17	Mechanisms exist to remediate risks to an acceptable level.	5	
IV.A-25	Overarching operational risk management	The executive board ensures in a comprehensible way that the operational risks are identified, assessed, limited and monitored, and that the effectiveness of both the design and also of the implementation of this operational risk management is regularly reviewed. It takes risk-specific supplementary or intensified measures in order to limit the inherent risks deemed to be material as the situation demands.	Functional	Intersects With	Risk Monitoring	RSK-22	Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including: (1) The effectiveness of security, compliance and resilience controls; (2) Changes to the organization's risk profile; and (3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk.	5	
IV.A-26	Overarching operational risk management	To raise awareness among employees for reducing relevant operational risks, particularly ICT risks, cyber risks, risks with regard to critical data and the risks resulting from the design and implementation of BCM, measures are to be implemented and carried out taking into account their tasks, competencies and responsibilities.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
IV.A-26	Overarching operational risk management	To raise awareness among employees for reducing relevant operational risks, particularly ICT risks, cyber risks, risks with regard to critical data and the risks resulting from the design and implementation of BCM, measures are to be implemented and carried out taking into account their tasks, competencies and responsibilities.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
IV.A-27	Overarching operational risk management	If necessary, FINMA will define more stringent requirements for operational risk management for specific topics as part of ongoing supervision. This will be done cautiously and in accordance with the proportionality principle.	Functional	No Relationship	N/A	N/A	N/A	0	
IV.A-28	Overarching operational risk management	The operational risks must be categorised in a uniform manner across the institution and listed in an inventory. The categorisation may be performed based on the categorisation of event types used to calculate the minimum capital requirements for operational risk or based on an internal taxonomy. The categorisation must be applied consistently in all areas of the institution and in all components of operational risk management.	Functional	Intersects With	Risk Catalog	RSK-10	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
IV.A-28	Overarching operational risk management	The operational risks must be categorised in a uniform manner across the institution and listed in an inventory. The categorisation may be performed based on the categorisation of event types used to calculate the minimum capital requirements for operational risk or based on an internal taxonomy. The categorisation must be applied consistently in all areas of the institution and in all components of operational risk management.	Functional	Intersects With	Risk Register	RSK-14	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
IV.A-29	Overarching operational risk management	Internal and external factors shall be taken into account for identifying operational risks. The identified operational risks shall be assessed in a comprehensible way both from the perspective of inherent as well as residual risks.	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	5	
IV.A-29	Overarching operational risk management	Internal and external factors shall be taken into account for identifying operational risks. The identified operational risks shall be assessed in a comprehensible way both from the perspective of inherent as well as residual risks.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
IV.A-30	Overarching operational risk management	The identification and assessment of operational risks shall be based on at least review results and regularly conducted risk and control assessments. The risk and control assessments shall take into account the inherent risks, the effectiveness of the existing control and mitigation measures and the residual risks.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-05.1	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: CHE - FINMA Circular 2023/1 - Operational Risks and Resilience - Banks
Focal Document URL: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-che-finma-circ-23-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IV.A-30	Overarching operational risk management	The identification and assessment of operational risks shall be based on at least review results and regularly conducted risk and control assessments. The risk and control assessments shall take into account the inherent risks, the effectiveness of the existing control and mitigation measures and the residual risks.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
IV.A-31	Overarching operational risk management	To assess the existing control and mitigation measures, in particular a regular assessment of the effectiveness of key controls must be performed and documented by an independent control body (design effectiveness and operating effectiveness testing). Key controls are those control and mitigation measures that minimise the inherent risks deemed to be material. The separation of tasks, competencies and responsibilities to ensure independence and prevent conflicts of interests shall also be regularly assessed.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-05.1	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
IV.A-31	Overarching operational risk management	To assess the existing control and mitigation measures, in particular a regular assessment of the effectiveness of key controls must be performed and documented by an independent control body (design effectiveness and operating effectiveness testing). Key controls are those control and mitigation measures that minimise the inherent risks deemed to be material. The separation of tasks, competencies and responsibilities to ensure independence and prevent conflicts of interests shall also be regularly assessed.	Functional	Intersects With	Independent Assessors	CPL-08	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5	
IV.A-31	Overarching operational risk management	To assess the existing control and mitigation measures, in particular a regular assessment of the effectiveness of key controls must be performed and documented by an independent control body (design effectiveness and operating effectiveness testing). Key controls are those control and mitigation measures that minimise the inherent risks deemed to be material. The separation of tasks, competencies and responsibilities to ensure independence and prevent conflicts of interests shall also be regularly assessed.	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
IV.A-32	Overarching operational risk management	Ad hoc risk and control assessments shall be conducted prior to major changes in products, activities, processes and systems. These shall take into account the operational risks associated with the change process and the operational risks of the target state. If necessary, the risk tolerance should be adjusted and control and mitigation measures implemented.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-06	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
IV.A-32	Overarching operational risk management	Ad hoc risk and control assessments shall be conducted prior to major changes in products, activities, processes and systems. These shall take into account the operational risks associated with the change process and the operational risks of the target state. If necessary, the risk tolerance should be adjusted and control and mitigation measures implemented.	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-13.1	Mechanisms exist to define instances that require a risk assessment to be performed.	8	
IV.A-33	Overarching operational risk management	Depending on the type, scope, complexity and risk of institution-specific products, activities, processes and systems, the following tools and methods shall be applied:	Functional	Intersects With	Risk Assessment Methodology	RSK-12	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	3	
IV.A.a-34	Overarching operational risk management	Systematic collection and analysis of internal loss data and relevant external events associated with operational risk;	Functional	Intersects With	Incident Pattern Analysis	IRO-17.1	Mechanisms exist to analyze historical incidents in aggregate to identify: (1) Patterns; (2) Trends; and (3) Other common root causes in order to address the vulnerability and risk.	3	
IV.A.b-35	Overarching operational risk management	Risk and control indicators for monitoring operational risk and identifying relevant risk increases in a timely manner;	Functional	Intersects With	Key Risk Indicators (KRIs)	GOV-12.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring, trend analysis, and possible control redesign or replacement for the Security, Compliance & Resilience Program (SCRP).	8	
IV.A.b-35	Overarching operational risk management	Risk and control indicators for monitoring operational risk and identifying relevant risk increases in a timely manner;	Functional	Intersects With	Risk Monitoring	RSK-22	Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including: (1) The effectiveness of security, compliance and resilience controls; (2) Changes to the organization's risk profile; and (3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk.	5	
IV.A.c-36	Overarching operational risk management	Scenario analyses and/or estimates of the loss potential in view of or in comparison with the minimum capital requirements for operational risk;	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3	
IV.A.d-37	Overarching operational risk management	Comparative analyses (read-across), for example, analyses of the relevance of review results for other areas of the institution or comparisons between the results of the risk and control assessments for various areas.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3	
IV.A-38	Overarching operational risk management	The risk tolerance for operational risk takes account of both the tolerance in relation to inherent as well as residual operational risk and is monitored using risk or control indicators.	Functional	Intersects With	Key Risk Indicators (KRIs)	GOV-12.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring, trend analysis, and possible control redesign or replacement for the Security, Compliance & Resilience Program (SCRP).	5	
IV.A-38	Overarching operational risk management	The risk tolerance for operational risk takes account of both the tolerance in relation to inherent as well as residual operational risk and is monitored using risk or control indicators.	Functional	Intersects With	Risk Tolerance	RSK-05.1	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	8	
IV.A-39	Overarching operational risk management	The risk control function reports to the board of directors at least annually and to the executive board at least every six months in accordance with margin nos. 75-76 of FINMA Circ. 17/1 on the operational risks at the top level of the categorisation defined in accordance with margin no. 28, on their comparison with the defined risk tolerance, and on details of material internal losses.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	8	
IV.A-40	Overarching operational risk management	In relation to the relevant ICT and cyber risks, the report for the executive board produced at least annually shall also contain information on the development of these risks, on the effectiveness of the corresponding key controls, and on material internal and external events in connection with these risks.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
IV.A-41	Overarching operational risk management	The internal reporting in accordance with margin no. 39 shall contain in addition the following information:	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	3	
IV.A-42	Overarching operational risk management	relevant, external factors in accordance with footnote 9,	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
IV.A-42	Overarching operational risk management	relevant, external factors in accordance with footnote 9,	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	3	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: CHE - FINMA Circular 2023/1 - Operational Risks and Resilience - Banks
Focal Document URL: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-che-finma-circ-23-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IV.A-43	Overarching operational risk management	summary overview of the effectiveness of the key controls in accordance with margin no. 31,	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-05.1	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	3	
IV.A-43	Overarching operational risk management	summary overview of the effectiveness of the key controls in accordance with margin no. 31,	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
IV.A-44	Overarching operational risk management	emerging operational risks;	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
IV.A-44	Overarching operational risk management	emerging operational risks;	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	3	
IV.A-45	Overarching operational risk management	results from the application of additional tools and methods in accordance with margin no. 33.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
IV.A-46	Overarching operational risk management	In accordance with the principle of proportionality, for systemically important banks, regular reporting on operational risks shall also be conducted at the level of the business or organisational areas that are exposed to relevant or material operational risks.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
IV.B	ICT risk management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
IV.B.a	ICT strategy and governance	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
IV.B.a-47	ICT strategy and governance	The basic expectations for the strategy, governance and raising of awareness in relation to ICT are set out in margin nos. 23-26 and 40.	Functional	No Relationship	N/A	N/A	N/A	0	
IV.B.a-48	ICT strategy and governance	ICT risk management shall take into account relevant internationally recognised standards and practices as well as the influence of new technological developments on the ICT risks.	Functional	Intersects With	Secure Practices Alignment Justification	GOV-03.1	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and (2) Provide defensible justification for secure practices.	5	
IV.B.a-48	ICT strategy and governance	ICT risk management shall take into account relevant internationally recognised standards and practices as well as the influence of new technological developments on the ICT risks.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5	
IV.B.a-49	ICT strategy and governance	The executive board shall ensure that procedures, processes and controls as well as tasks, competencies and responsibilities are implemented and documented both for change management and for ICT operations (run, maintenance). These shall be adequately resourced with qualified staff.	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	5	
IV.B.a-49	ICT strategy and governance	The executive board shall ensure that procedures, processes and controls as well as tasks, competencies and responsibilities are implemented and documented both for change management and for ICT operations (run, maintenance). These shall be adequately resourced with qualified staff.	Functional	Intersects With	Operations Security	OPS-02	Mechanisms exist to facilitate the implementation of operational security controls.	5	
IV.B.a-49	ICT strategy and governance	The executive board shall ensure that procedures, processes and controls as well as tasks, competencies and responsibilities are implemented and documented both for change management and for ICT operations (run, maintenance). These shall be adequately resourced with qualified staff.	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	3	
IV.B.b	Change management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
IV.B.b-50	Change management	Change management shall define the procedures, processes and controls for all phases in the development or procurement of ICT. In each of these phases it shall consider the impact of the change on the ICT risks. It shall focus in particular on the requirements with regard to confidentiality, integrity and availability.	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	8	
IV.B.b-50	Change management	Change management shall define the procedures, processes and controls for all phases in the development or procurement of ICT. In each of these phases it shall consider the impact of the change on the ICT risks. It shall focus in particular on the requirements with regard to confidentiality, integrity and availability.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-06	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
IV.B.b-50	Change management	Change management shall define the procedures, processes and controls for all phases in the development or procurement of ICT. In each of these phases it shall consider the impact of the change on the ICT risks. It shall focus in particular on the requirements with regard to confidentiality, integrity and availability.	Functional	Intersects With	Technology Development & Acquisition	TDA-02	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
IV.B.b-51	Change management	It must be ensured that the development or test environments are separate from the ICT production environment. This also involves the clear allocation of tasks, competencies and responsibilities and laying down rules for the associated access rights.	Functional	Intersects With	Access Restriction For Change	CHG-04.1	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	5	
IV.B.b-51	Change management	It must be ensured that the development or test environments are separate from the ICT production environment. This also involves the clear allocation of tasks, competencies and responsibilities and laying down rules for the associated access rights.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-15.1	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	8	
IV.B.b-52	Change management	When developing and procuring ICT, functional and non-functional requirements shall be clearly defined and approved; they shall be tested and validated based on their criticality.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-09	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	5	
IV.B.b-52	Change management	When developing and procuring ICT, functional and non-functional requirements shall be clearly defined and approved; they shall be tested and validated based on their criticality.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5	
IV.B.c	ICT operations (run, maintenance)	N/A	Functional	No Relationship	N/A	N/A	N/A	0	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: CHE - FINMA Circular 2023/1 - Operational Risks and Resilience - Banks
Focal Document URL: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-che-finma-circ-23-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IV.B.c-53	ICT operations (run, maintenance)	The institution shall keep one or more inventories of the ICT assets. The inventory shall include hardware and software assets as well as the storage locations of critical data. Both dependencies within the institution as well as interfaces to significant external service providers should be taken into account.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
IV.B.c-53	ICT operations (run, maintenance)	The institution shall keep one or more inventories of the ICT assets. The inventory shall include hardware and software assets as well as the storage locations of critical data. Both dependencies within the institution as well as interfaces to significant external service providers should be taken into account.	Functional	Intersects With	Asset-Service Dependencies	AST-06	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
IV.B.c-54	ICT operations (run, maintenance)	The inventory is available in real time and shall be reviewed and updated regularly with regard to its completeness and accuracy.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
IV.B.c-54	ICT operations (run, maintenance)	The inventory is available in real time and shall be reviewed and updated regularly with regard to its completeness and accuracy.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-08.1	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	8	
IV.B.c-55	ICT operations (run, maintenance)	The institution shall have procedures, processes and controls in place that ensure the confidentiality, integrity and availability of the ICT production environment, taking into account the respective risk tolerance.	Functional	Intersects With	Operations Security	OPS-02	Mechanisms exist to facilitate the implementation of operational security controls.	5	
IV.B.c-55	ICT operations (run, maintenance)	The institution shall have procedures, processes and controls in place that ensure the confidentiality, integrity and availability of the ICT production environment, taking into account the respective risk tolerance.	Functional	Intersects With	Secure Engineering Principles	SEA-05	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
IV.B.c-56	ICT operations (run, maintenance)	The institution shall ensure that it can transition smoothly to its BCP and DRP processes in the event of significant disruptions to its ICT operations. It shall implement adequate back-up processes and recovery processes that are tested and validated regularly.	Functional	Intersects With	Coordinate with Related Plans	BCD-07.3	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5	
IV.B.c-56	ICT operations (run, maintenance)	The institution shall ensure that it can transition smoothly to its BCP and DRP processes in the event of significant disruptions to its ICT operations. It shall implement adequate back-up processes and recovery processes that are tested and validated regularly.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
IV.B.c-56	ICT operations (run, maintenance)	The institution shall ensure that it can transition smoothly to its BCP and DRP processes in the event of significant disruptions to its ICT operations. It shall implement adequate back-up processes and recovery processes that are tested and validated regularly.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	5	
IV.B.c-57	ICT operations (run, maintenance)	The institution shall have procedures, processes and controls in place to ensure that ICT that its nearing the end of its operational life or whose planned decommissioning date has passed is dealt with in a risk-oriented way.	Functional	Intersects With	Technology Lifecycle Management	AST-37	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5	
IV.B.c-57	ICT operations (run, maintenance)	The institution shall have procedures, processes and controls in place to ensure that ICT that its nearing the end of its operational life or whose planned decommissioning date has passed is dealt with in a risk-oriented way.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5	
IV.B.d	Incident management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
IV.B.d-58	Incident management	The institution shall have procedures, processes and controls in place for dealing with significant ICT incidents, including those resulting from dependencies on external service providers and outsourcing operations within the group. In this regard, the full life-cycle of significant ICT incidents must be taken into account and tasks, competencies and responsibilities for dealing with these incidents must be defined.	Functional	Intersects With	Incident Response Operations	IRO-02	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
IV.B.d-58	Incident management	The institution shall have procedures, processes and controls in place for dealing with significant ICT incidents, including those resulting from dependencies on external service providers and outsourcing operations within the group. In this regard, the full life-cycle of significant ICT incidents must be taken into account and tasks, competencies and responsibilities for dealing with these incidents must be defined.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
IV.B.d-58	Incident management	The institution shall have procedures, processes and controls in place for dealing with significant ICT incidents, including those resulting from dependencies on external service providers and outsourcing operations within the group. In this regard, the full life-cycle of significant ICT incidents must be taken into account and tasks, competencies and responsibilities for dealing with these incidents must be defined.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-21	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	3	
IV.B.d-59	Incident management	Dealing with significant ICT incidents must be coordinated and linked with the processes for BCM and the DRP.	Functional	Intersects With	Coordinate with Related Plans	BCD-07.3	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5	
IV.B.d-59	Incident management	Dealing with significant ICT incidents must be coordinated and linked with the processes for BCM and the DRP.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	3	
IV.B.d-60	Incident management	ICT incidents that are regarded by the institution as a significant disruption in the provision of its critical processes and are of material significance for supervision must be reported to FINMA without delay.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: CHE - FINMA Circular 2023/1 - Operational Risks and Resilience - Banks
Focal Document URL: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-che-finma-circ-23-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IV.B.d-60	Incident management	ICT incidents that are regarded by the institution as a significant disruption in the provision of its critical processes and are of material significance for supervision must be reported to FINMA without delay.	Functional	Intersects With	Serious Incident Reporting	IRO-16.3	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	8	
IV.C	Cyber risk management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
IV.C-61	Cyber risk management	The basic expectations for the strategy, governance and raising of awareness in relation to cyber risks are set out in margin nos. 23-26 and 40.	Functional	No Relationship	N/A	N/A	N/A	0	
IV.C-62	Cyber risk management	The institution shall define clear tasks, competencies and responsibilities. It must cover at least the following aspects in accordance with internationally recognised standards and practices, and ensure their effective implementation through appropriate procedures, processes and controls and continuously develop and improve them:	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
IV.C-62	Cyber risk management	The institution shall define clear tasks, competencies and responsibilities. It must cover at least the following aspects in accordance with internationally recognised standards and practices, and ensure their effective implementation through appropriate procedures, processes and controls and continuously develop and improve them:	Functional	Intersects With	Commitment To Continual Improvements	PRM-05.1	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	5	
IV.C.a-63	Cyber risk management	Identification of the institution-specific threat landscape from cyber attacks and assessment of the possible impacts of exploiting vulnerabilities with regard to the inventoried ICT assets and the electronic critical data (in accordance with margin nos. 53, 54 and 7);	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
IV.C.a-63	Cyber risk management	Identification of the institution-specific threat landscape from cyber attacks and assessment of the possible impacts of exploiting vulnerabilities with regard to the inventoried ICT assets and the electronic critical data (in accordance with margin nos. 53, 54 and 7);	Functional	Intersects With	Threat Analysis	THR-08	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5	
IV.C.b-64	Cyber risk management	Protection of the inventoried ICT assets and the electronic critical data from cyber attacks by implementing appropriate protective measures, particularly with regard to the confidentiality, integrity and availability;	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-07	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
IV.C.b-64	Cyber risk management	Protection of the inventoried ICT assets and the electronic critical data from cyber attacks by implementing appropriate protective measures, particularly with regard to the confidentiality, integrity and availability;	Functional	Intersects With	Operations Security	OPS-02	Mechanisms exist to facilitate the implementation of operational security controls.	5	
IV.C.c-65	Cyber risk management	Timely logging and detection of cyber attacks on the basis of a process for the systematic and consistent monitoring of the inventoried ICT assets and the electronic critical data;	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	8	
IV.C.c-65	Cyber risk management	Timely logging and detection of cyber attacks on the basis of a process for the systematic and consistent monitoring of the inventoried ICT assets and the electronic critical data;	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5	
IV.C.d-66	Cyber risk management	Response to identified vulnerabilities and cyber attacks by developing and implementing appropriate processes for taking rapid containment and remediation measures; and	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
IV.C.d-66	Cyber risk management	Response to identified vulnerabilities and cyber attacks by developing and implementing appropriate processes for taking rapid containment and remediation measures; and	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
IV.C.e-67	Cyber risk management	Ensuring the prompt recovery of normal business operations after a cyber attack through appropriate measures.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-18	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
IV.C.e-67	Cyber risk management	Ensuring the prompt recovery of normal business operations after a cyber attack through appropriate measures.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
IV.C-68	Cyber risk management	Cyber risk management must ensure that a successful or partially successful cyber attack is analysed based on its materiality for critical inventoried ICT assets or electronic critical data and critical processes (including outsourced services and functions) and that the reporting obligation under the FINMASA is met. After an initial assessment and preliminary notification to the body responsible at FINMA within 24 hours, the report in accordance with the catalogue of requirements on the EHP survey and application platform (mandatory fields) must be submitted to FINMA within 72 hours. Once the institution has finished processing the case, a conclusive root cause analysis corresponding to the degree of severity must be submitted to the body responsible at FINMA.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
IV.C-68	Cyber risk management	Cyber risk management must ensure that a successful or partially successful cyber attack is analysed based on its materiality for critical inventoried ICT assets or electronic critical data and critical processes (including outsourced services and functions) and that the reporting obligation under the FINMASA is met. After an initial assessment and preliminary notification to the body responsible at FINMA within 24 hours, the report in accordance with the catalogue of requirements on the EHP survey and application platform (mandatory fields) must be submitted to FINMA within 72 hours. Once the institution has finished processing the case, a conclusive root cause analysis corresponding to the degree of severity must be submitted to the body responsible at FINMA.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
IV.C-68	Cyber risk management	Cyber risk management must ensure that a successful or partially successful cyber attack is analysed based on its materiality for critical inventoried ICT assets or electronic critical data and critical processes (including outsourced services and functions) and that the reporting obligation under the FINMASA is met. After an initial assessment and preliminary notification to the body responsible at FINMA within 24 hours, the report in accordance with the catalogue of requirements on the EHP survey and application platform (mandatory fields) must be submitted to FINMA within 72 hours. Once the institution has finished processing the case, a conclusive root cause analysis corresponding to the degree of severity must be submitted to the body responsible at FINMA.	Functional	Intersects With	Serious Incident Reporting	IRO-16.3	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: CHE - FINMA Circular 2023/1 - Operational Risks and Resilience - Banks
Focal Document URL: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-che-finma-circ-23-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IV.C-69	Cyber risk management	The executive board shall arrange for vulnerability assessments and penetration tests to be conducted regularly. These must be performed by qualified staff with adequate resources. All inventoried ICT assets that are accessible over the internet must be taken into account. In addition, inventoried ICT assets that are not accessible over the internet, but that are necessary for the provision of critical processes, or that contain electronic critical data, must be included as well.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
IV.C-69	Cyber risk management	The executive board shall arrange for vulnerability assessments and penetration tests to be conducted regularly. These must be performed by qualified staff with adequate resources. All inventoried ICT assets that are accessible over the internet must be taken into account. In addition, inventoried ICT assets that are not accessible over the internet, but that are necessary for the provision of critical processes, or that contain electronic critical data, must be included as well.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
IV.C-70	Cyber risk management	Risk-based, threat intelligence-related scenario cyber exercises must be conducted on the basis of the institution-specific threat landscape. The result of the exercises must be documented and reported in an appropriate form.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	3	
IV.C-70	Cyber risk management	Risk-based, threat intelligence-related scenario cyber exercises must be conducted on the basis of the institution-specific threat landscape. The result of the exercises must be documented and reported in an appropriate form.	Functional	Intersects With	Red Team Exercises	VPM-21	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	5	
IV.D	Critical data risk management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
IV.D-71	Critical data risk management	The basic expectations for the strategy, governance and raising of awareness in relation to the risks of critical data are set out in margin nos. 23-26.	Functional	No Relationship	N/A	N/A	N/A	0	
IV.D-72	Critical data risk management	The executive board shall define appropriate processes, procedures and controls as well as clear tasks, competencies and responsibilities for dealing with the data identified as critical by the institution. Furthermore, the executive board shall appoint a unit to establish the framework for ensuring the confidentiality, integrity and availability of critical data and to monitor its observance.	Functional	Intersects With	Sensitive / Regulated Data Governance	DCH-03	Mechanisms exist to facilitate data governance so that sensitive and/or regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	8	
IV.D-72	Critical data risk management	The executive board shall define appropriate processes, procedures and controls as well as clear tasks, competencies and responsibilities for dealing with the data identified as critical by the institution. Furthermore, the executive board shall appoint a unit to establish the framework for ensuring the confidentiality, integrity and availability of critical data and to monitor its observance.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
IV.D-73	Critical data risk management	The institution shall identify its critical data in a systematic and comprehensive way, categorise it on the basis of its criticality and define clear responsibilities.	Functional	Intersects With	Data Catalog	DCH-03.1	Mechanisms exist to identify and catalog the organization's data holdings in a structured format to document each sensitive and/or regulated data asset.	5	
IV.D-73	Critical data risk management	The institution shall identify its critical data in a systematic and comprehensive way, categorise it on the basis of its criticality and define clear responsibilities.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	8	
IV.D-74	Critical data risk management	The critical data defined by the institution must be managed throughout its entire life-cycle.	Functional	Intersects With	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	5	
IV.D-74	Critical data risk management	The critical data defined by the institution must be managed throughout its entire life-cycle.	Functional	Intersects With	Sensitive / Regulated Data Governance	DCH-03	Mechanisms exist to facilitate data governance so that sensitive and/or regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5	
IV.D-75	Critical data risk management	In the management of critical data, in particular the confidentiality, integrity and availability of the critical data must be ensured through appropriate processes, procedures and controls.	Functional	Intersects With	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	5	
IV.D-75	Critical data risk management	In the management of critical data, in particular the confidentiality, integrity and availability of the critical data must be ensured through appropriate processes, procedures and controls.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-07	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	8	
IV.D-76	Critical data risk management	Critical data must be adequately protected from being accessed and used by unauthorised persons during operations and during the development, change and migration of ICT. This also applies to critical data in test environments.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-07	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
IV.D-76	Critical data risk management	Critical data must be adequately protected from being accessed and used by unauthorised persons during operations and during the development, change and migration of ICT. This also applies to critical data in test environments.	Functional	Intersects With	Secure Migration Practices	TDA-15.2	Mechanisms exist to ensure secure migration practices purge Technology Assets, Applications and/or Services (TAAS) of test/development/staging data and accounts before it is migrated into a production environment.	5	
IV.D-76	Critical data risk management	Critical data must be adequately protected from being accessed and used by unauthorised persons during operations and during the development, change and migration of ICT. This also applies to critical data in test environments.	Functional	Intersects With	Use of Live Data	TDA-18	Mechanisms exist to approve, document and control the use of live data in development and test environments.	5	
IV.D-77	Critical data risk management	The ICT assets that store or process critical data must be afforded particular protection. Access to these data must be regulated systematically and monitored continuously.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-06.1	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and/or physical access to sensitive and/or regulated data.	5	
IV.D-77	Critical data risk management	The ICT assets that store or process critical data must be afforded particular protection. Access to these data must be regulated systematically and monitored continuously.	Functional	Intersects With	High Value Assets (HVAs)	GOV-08	Mechanisms exist to identify and catalog the organization's High Value Assets (HVAs) (e.g., crown jewels), including defining: (1) Criteria for high-value Intellectual Property (IP) to be categorized as a HVA; (2) Criteria for Technology Assets, Applications and Services (TAAS) to be categorized as a HVA based on business process criticality or dependency relationships; (3) Location of HVA Technology Assets, Applications, Services and/or Data (TAASD); (4) Assigned owners; (5) Minimum protection mechanisms that must be implemented; and (6) Assurance requirements.	5	
IV.D-77	Critical data risk management	The ICT assets that store or process critical data must be afforded particular protection. Access to these data must be regulated systematically and monitored continuously.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3	
IV.D-78	Critical data risk management	Access to critical data and processing functionalities shall be restricted to persons who require this to carry out their tasks. The institution must have an authorisation system in place. Access to this authorisation system must be afforded particular protection and reviewed on a regular basis. The authorisations included in the authorisation system must be reviewed on a regular basis.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
IV.D-78	Critical data risk management	Access to critical data and processing functionalities shall be restricted to persons who require this to carry out their tasks. The institution must have an authorisation system in place. Access to this authorisation system must be afforded particular protection and reviewed on a regular basis. The authorisations included in the authorisation system must be reviewed on a regular basis.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	8	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: CHE - FINMA Circular 2023/1 - Operational Risks and Resilience - Banks
Focal Document URL: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-che-finma-circ-23-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IV.D-78	Critical data risk management	Access to critical data and processing functionalities shall be restricted to persons who require this to carry out their tasks. The institution must have an authorisation system in place. Access to this authorisation system must be afforded particular protection and reviewed on a regular basis. The authorisations included in the authorisation system must be reviewed on a regular basis.	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
IV.D-79	Critical data risk management	If critical data is stored outside of Switzerland or if it can be accessed from abroad, increased risks associated with this must be adequately mitigated and monitored via suitable means and the data afforded particular protection.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-07	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	3	
IV.D-79	Critical data risk management	If critical data is stored outside of Switzerland or if it can be accessed from abroad, increased risks associated with this must be adequately mitigated and monitored via suitable means and the data afforded particular protection.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	
IV.D-80	Critical data risk management	Both internal and external persons who can access critical data or who can change these must be selected carefully. These persons must be monitored with the help of appropriate measures and given regular training in the handling of these data. Increased security requirements shall apply to persons with increased privileges. In addition, a list of all persons with privileged access rights must be kept and updated on a regular basis.	Functional	Intersects With	Roles With Special Protection Measures	HRS-05.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
IV.D-80	Critical data risk management	Both internal and external persons who can access critical data or who can change these must be selected carefully. These persons must be monitored with the help of appropriate measures and given regular training in the handling of these data. Increased security requirements shall apply to persons with increased privileges. In addition, a list of all persons with privileged access rights must be kept and updated on a regular basis.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
IV.D-80	Critical data risk management	Both internal and external persons who can access critical data or who can change these must be selected carefully. These persons must be monitored with the help of appropriate measures and given regular training in the handling of these data. Increased security requirements shall apply to persons with increased privileges. In addition, a list of all persons with privileged access rights must be kept and updated on a regular basis.	Functional	Intersects With	Privileged User Training	SAT-05.2	Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities.	5	
IV.D-81	Critical data risk management	Incidents that substantially impair the confidentiality, integrity or availability of critical data must be reported to FINMA without delay.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-16.2	Mechanisms exist to report sensitive and/or regulated data incidents in a timely manner.	5	
IV.D-81	Critical data risk management	Incidents that substantially impair the confidentiality, integrity or availability of critical data must be reported to FINMA without delay.	Functional	Intersects With	Serious Incident Reporting	IRO-16.3	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	
IV.D-82	Critical data risk management	When selecting service providers that can process or view critical data, due diligence must be particularly thorough. Clear criteria for assessing how service providers handle critical data must be defined and checked before entering into a contractual agreement. The service providers must be monitored and checked periodically as part of the institution's internal control system.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	8	
IV.D-82	Critical data risk management	When selecting service providers that can process or view critical data, due diligence must be particularly thorough. Clear criteria for assessing how service providers handle critical data must be defined and checked before entering into a contractual agreement. The service providers must be monitored and checked periodically as part of the institution's internal control system.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
IV.E	Business continuity management (BCM)	N/A	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	10	
IV.E-83	Business continuity management (BCM)	The basic expectations for the strategy, governance and raising of awareness in relation to risks resulting from the design and implementation of BCM are set out in margin nos. 23-26.	Functional	No Relationship	N/A	N/A	N/A	0	
IV.E-84	Business continuity management (BCM)	Every relevant business and organisational area must identify its critical processes and the resources required for these in a business impact analysis (BIA).	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
IV.E-84	Business continuity management (BCM)	Every relevant business and organisational area must identify its critical processes and the resources required for these in a business impact analysis (BIA).	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	8	
IV.E-85	Business continuity management (BCM)	The institution shall define the RTO and RPO for the critical processes in accordance with margin no. 10. These shall be coordinated with the necessary service providers and adherence to the RTO and RPO shall be regulated by service level agreements or contracts or by other appropriate procedures, processes and controls.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	
IV.E-85	Business continuity management (BCM)	The institution shall define the RTO and RPO for the critical processes in accordance with margin no. 10. These shall be coordinated with the necessary service providers and adherence to the RTO and RPO shall be regulated by service level agreements or contracts or by other appropriate procedures, processes and controls.	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	5	
IV.E-86	Business continuity management (BCM)	The institution shall define at least one BCP in accordance with margin no. 11 that also describes the conditions triggering the plan and the decision-making processes, and takes into account the loss of resources in accordance with margin no. 84. The acceptance of residual risks must be adequately documented.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	8	
IV.E-86	Business continuity management (BCM)	The institution shall define at least one BCP in accordance with margin no. 11 that also describes the conditions triggering the plan and the decision-making processes, and takes into account the loss of resources in accordance with margin no. 84. The acceptance of residual risks must be adequately documented.	Functional	Intersects With	Recovery Operations Criteria	BCD-05	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recovery (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
IV.E-87	Business continuity management (BCM)	The BIA and BCP shall be prepared and documented in a consistent manner following institution-wide guidelines. They must be reviewed and updated annually and on an ad hoc basis in the event of significant changes to the business operations (reorganisations, development of a new business segment etc.).	Functional	Intersects With	Ongoing Contingency Planning	BCD-07	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services); (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing activities.	8	
IV.E-87	Business continuity management (BCM)	The BIA and BCP shall be prepared and documented in a consistent manner following institution-wide guidelines. They must be reviewed and updated annually and on an ad hoc basis in the event of significant changes to the business operations (reorganisations, development of a new business segment etc.).	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	3	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: CHE - FINMA Circular 2023/1 - Operational Risks and Resilience - Banks
Focal Document URL: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-che-finma-circ-23-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IV.E-88	Business continuity management (BCM)	The institution shall define at least one DRP as part of the BCP. If critical processes or parts thereof are outsourced, the DRP shall take into account the external dependencies and contractual provisions as well as alternative solutions. The DRP must be reviewed and updated on an ad hoc basis in the event of significant changes and at least annually.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	8	
IV.E-88	Business continuity management (BCM)	The institution shall define at least one DRP as part of the BCP. If critical processes or parts thereof are outsourced, the DRP shall take into account the external dependencies and contractual provisions as well as alternative solutions. The DRP must be reviewed and updated on an ad hoc basis in the event of significant changes and at least annually.	Functional	Intersects With	Ongoing Contingency Planning	BCD-07	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services); (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing activities.	3	
IV.E-88	Business continuity management (BCM)	The institution shall define at least one DRP as part of the BCP. If critical processes or parts thereof are outsourced, the DRP shall take into account the external dependencies and contractual provisions as well as alternative solutions. The DRP must be reviewed and updated on an ad hoc basis in the event of significant changes and at least annually.	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	5	
IV.E-89	Business continuity management (BCM)	In crisis situations, a crisis unit shall take on the task of crisis management until order is restored. The conditions triggering a crisis and the tasks, competencies and responsibilities of the crisis unit must be regulated in advance and the crisis organisation aligned to the business activities and geographical structure of the institution. The availability of responsible persons in crisis situations must be ensured.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	5	
IV.E-89	Business continuity management (BCM)	In crisis situations, a crisis unit shall take on the task of crisis management until order is restored. The conditions triggering a crisis and the tasks, competencies and responsibilities of the crisis unit must be regulated in advance and the crisis organisation aligned to the business activities and geographical structure of the institution. The availability of responsible persons in crisis situations must be ensured.	Functional	Intersects With	Recovery Operations Criteria	BCD-05	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recovery (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
IV.E-90	Business continuity management (BCM)	The institution shall define a communication strategy for internal and external communication in crisis situations.	Functional	Intersects With	Recovery Operations Communications	BCD-06	Mechanisms exist to communicate the status of recovery activities and progress in restoring operational capabilities to designated internal and external stakeholders.	8	
IV.E-90	Business continuity management (BCM)	The institution shall define a communication strategy for internal and external communication in crisis situations.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	3	
IV.E-91	Business continuity management (BCM)	The implementation of the BCP and DRP as well as the functioning of the crisis organisation must be regularly evaluated through tests. Systematic plans shall be drawn up for this, which ensure regular coverage. Various means of testing of varying intensity and effectiveness can be selected including, for example, tabletop exercises.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	8	
IV.E-92	Business continuity management (BCM)	The most important measures according to the BCP and DRP and the crisis organisation must be tested at least once a year.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	8	
IV.E-93	Business continuity management (BCM)	Relevant stakeholder groups, including those in specialist and IT functions, shall take part in the tests in order to familiarise themselves with the recovery processes.	Functional	Intersects With	Contingency Training	BCD-09	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	5	
IV.E-93	Business continuity management (BCM)	Relevant stakeholder groups, including those in specialist and IT functions, shall take part in the tests in order to familiarise themselves with the recovery processes.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
IV.E-94	Business continuity management (BCM)	The tests shall encompass various severe but plausible scenarios and take into account recovery dependencies, including those that exist with internal or external third parties.	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	3	
IV.E-94	Business continuity management (BCM)	The tests shall encompass various severe but plausible scenarios and take into account recovery dependencies, including those that exist with internal or external third parties.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
IV.E-95	Business continuity management (BCM)	Regular reporting to the board of directors and the executive board shall include information about the testing and review activities carried out and their results. It shall clearly show prioritisations made (e.g. prioritisation of the critical processes necessary for the provision of the critical functions in accordance with margin no. 14) and recognised gaps in the coverage of other critical processes.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-11	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	3	
IV.E-95	Business continuity management (BCM)	Regular reporting to the board of directors and the executive board shall include information about the testing and review activities carried out and their results. It shall clearly show prioritisations made (e.g. prioritisation of the critical processes necessary for the provision of the critical functions in accordance with margin no. 14) and recognised gaps in the coverage of other critical processes.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
IV.E-96	Business continuity management (BCM)	The employees and members of the crisis organisation shall be adequately trained in their tasks, competencies and responsibilities resulting from the various BCM activities, both when new employees join the institution and as part of regular training.	Functional	Intersects With	Contingency Training	BCD-09	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	8	
IV.E-96	Business continuity management (BCM)	The employees and members of the crisis organisation shall be adequately trained in their tasks, competencies and responsibilities resulting from the various BCM activities, both when new employees join the institution and as part of regular training.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	3	
IV.F	Management of risks from cross-border service business	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
IV.F-97	Management of risks from cross-border service business	If institutions or their group companies provide services or distribute financial products cross-border, then the risks resulting from the application of foreign legislation (tax, criminal, anti-money laundering legislation etc.) must also be adequately identified, limited and controlled.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
IV.F-97	Management of risks from cross-border service business	If institutions or their group companies provide services or distribute financial products cross-border, then the risks resulting from the application of foreign legislation (tax, criminal, anti-money laundering legislation etc.) must also be adequately identified, limited and controlled.	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	3	
IV.F-98	Management of risks from cross-border service business	The institutions shall conduct a thorough analysis of their cross-border service business and cross-border distribution of financial products, examining the legal framework and associated risks. Based on this analysis, the institutions shall take the necessary strategic and organisational measures to eliminate and minimise risk, and continuously adapt these to changing conditions. In particular, they shall have the necessary country-specific specialist knowledge, define specific service models for the countries served, train employees and ensure compliance with the guidelines through appropriate organisational measures, directives, remuneration and sanctions models.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: CHE - FINMA Circular 2023/1 - Operational Risks and Resilience - Banks
Focal Document URL: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-che-finma-circ-23-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IV.F-98	Management of risks from cross-border service business	The institutions shall conduct a thorough analysis of their cross-border service business and cross-border distribution of financial products, examining the legal framework and associated risks. Based on this analysis, the institutions shall take the necessary strategic and organisational measures to eliminate and minimise risk, and continuously adapt these to changing conditions. In particular, they shall have the necessary country-specific specialist knowledge, define specific service models for the countries served, train employees and ensure compliance with the guidelines through appropriate organisational measures, directives, remuneration and sanctions models.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
IV.F-98	Management of risks from cross-border service business	The institutions shall conduct a thorough analysis of their cross-border service business and cross-border distribution of financial products, examining the legal framework and associated risks. Based on this analysis, the institutions shall take the necessary strategic and organisational measures to eliminate and minimise risk, and continuously adapt these to changing conditions. In particular, they shall have the necessary country-specific specialist knowledge, define specific service models for the countries served, train employees and ensure compliance with the guidelines through appropriate organisational measures, directives, remuneration and sanctions models.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	3	
IV.F-99	Management of risks from cross-border service business	The risks generated by external asset managers, intermediaries and other service providers must also be taken into account. Accordingly, a diligent approach must be adopted in selecting and instructing these partners.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3	
IV.F-99	Management of risks from cross-border service business	The risks generated by external asset managers, intermediaries and other service providers must also be taken into account. Accordingly, a diligent approach must be adopted in selecting and instructing these partners.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
IV.F-100	Management of risks from cross-border service business	This basic approach also covers situations where a foreign-based subsidiary, branch or similar serves clients of a Swiss financial institution cross-border.	Functional	Intersects With	Compliance Scope	CPL-03	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	3	
V	Ensuring operational resilience	N/A	Functional	Intersects With	Operational Resilience Capabilities	BCD-03	Mechanisms exist to ensure capabilities are implemented to provide operational resilience to: (1) Unintentional errors; and (2) Intentional attack or circumvention.	5	
V-101	Ensuring operational resilience	The institution shall identify its critical functions and their tolerances for disruption. These must be approved by the board of directors. The board of directors must also regularly approve and monitor the approach for ensuring operational resilience.	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
V-101	Ensuring operational resilience	The institution shall identify its critical functions and their tolerances for disruption. These must be approved by the board of directors. The board of directors must also regularly approve and monitor the approach for ensuring operational resilience.	Functional	Intersects With	Defined Operational Resilience Requirements	BCD-02.1	Mechanisms exist to define operational resilience requirements for Technology Assets, Applications, Services and/or Data (TAASD) to operate in a controlled and acceptable manner during: (1) Routine operations; and (2) Adverse conditions.	5	
V-101	Ensuring operational resilience	The institution shall identify its critical functions and their tolerances for disruption. These must be approved by the board of directors. The board of directors must also regularly approve and monitor the approach for ensuring operational resilience.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	3	
V-101	Ensuring operational resilience	The institution shall identify its critical functions and their tolerances for disruption. These must be approved by the board of directors. The board of directors must also regularly approve and monitor the approach for ensuring operational resilience.	Functional	Intersects With	Risk Tolerance	RSK-05.1	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
V-102	Ensuring operational resilience	The institution shall take measures to ensure operational resilience, taking into account severe but plausible scenarios.	Functional	Intersects With	Operational Resilience Capabilities	BCD-03	Mechanisms exist to ensure capabilities are implemented to provide operational resilience to: (1) Unintentional errors; and (2) Intentional attack or circumvention.	8	
V-102	Ensuring operational resilience	The institution shall take measures to ensure operational resilience, taking into account severe but plausible scenarios.	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-08.1	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration of primary processing and/or storage sites	3	
V-102	Ensuring operational resilience	The institution shall take measures to ensure operational resilience, taking into account severe but plausible scenarios.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	5	
V-103	Ensuring operational resilience	The critical functions and the associated tolerances for disruption according to margin no. 14 must be approved at least annually by the board of directors.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
V-103	Ensuring operational resilience	The critical functions and the associated tolerances for disruption according to margin no. 14 must be approved at least annually by the board of directors.	Functional	Intersects With	Risk Tolerance	RSK-05.1	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	3	
V-104	Ensuring operational resilience	The institution shall coordinate the relevant components of a comprehensive risk management framework, such as operational risk management, including ICT and cyber risk management, business continuity management, outsourcing management (cf. FINMA Circular 2018/3 "Outsourcing"), and emergency planning (Chapter VI.) such that these contribute to strengthening the institution's operational resilience. This includes an appropriate exchange of relevant information between these various areas.	Functional	Intersects With	Coordinate with Related Plans	BCD-07.3	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5	
V-104	Ensuring operational resilience	The institution shall coordinate the relevant components of a comprehensive risk management framework, such as operational risk management, including ICT and cyber risk management, business continuity management, outsourcing management (cf. FINMA Circular 2018/3 "Outsourcing"), and emergency planning (Chapter VI.) such that these contribute to strengthening the institution's operational resilience. This includes an appropriate exchange of relevant information between these various areas.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5	
V-105	Ensuring operational resilience	Reporting to the board of directors and the executive board must take place annually and in the event of significant control weaknesses or incidents that jeopardise operational resilience.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	8	
V-106	Ensuring operational resilience	Internal and external threats and the corresponding exploitation of vulnerabilities shall be identified and assessed for the critical functions. The resulting operational risks shall be identified, assessed, limited and monitored as part of operational risk management.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
V-106	Ensuring operational resilience	Internal and external threats and the corresponding exploitation of vulnerabilities shall be identified and assessed for the critical functions. The resulting operational risks shall be identified, assessed, limited and monitored as part of operational risk management.	Functional	Intersects With	Threat Analysis	THR-08	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: CHE - FINMA Circular 2023/1 - Operational Risks and Resilience - Banks
Focal Document URL: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-che-finma-circ-23-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
V-107	Ensuring operational resilience	The institution shall keep an inventory of its critical functions, which is reviewed and updated at least annually. This inventory shall contain the tolerances for disruption of the critical functions, as well as connections and dependencies between the necessary critical processes and their resources for providing the critical functions.	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
V-107	Ensuring operational resilience	The institution shall keep an inventory of its critical functions, which is reviewed and updated at least annually. This inventory shall contain the tolerances for disruption of the critical functions, as well as connections and dependencies between the necessary critical processes and their resources for providing the critical functions.	Functional	Intersects With	Asset-Service Dependencies	AST-06	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
V-108	Ensuring operational resilience	As a minimum, the significant operational risks and the key controls must be documented for the critical functions.	Functional	Intersects With	Risk Register	RSK-14	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
V-109	Ensuring operational resilience	The critical functions and the critical processes and resources required for these shall be covered by BCPs pursuant to Chapter IV./E.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	8	
V-109	Ensuring operational resilience	The critical functions and the critical processes and resources required for these shall be covered by BCPs pursuant to Chapter IV./E.	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-08.1	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration of primary processing and/or storage sites is performed.	5	
V-110	Ensuring operational resilience	The ability to provide critical functions within their tolerance for disruption in severe but plausible scenarios shall be tested or exercised regularly. These also include scenarios that differ from shorter and more limited interruptions and that are characterised by a longer duration (e.g. over several months) and a lack of basic resources. The tests or exercises must be designed in such a way that they do not fundamentally endanger the institution.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	8	
V-111	Ensuring operational resilience	For systemically important banks, the BCP, DRP and the crisis organisation in accordance with Chapter IV./E. that are relevant for the continuation of the critical functions in accordance with margin no. 14 must be coordinated with the emergency planning in accordance with Chapter VI.	Functional	Intersects With	Coordinate with Related Plans	BCD-07.3	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5	
VI	Continuation of critical services during the resolution and recovery of systemically important banks	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
VI-112	Continuation of critical services during the resolution and recovery of systemically important banks	As part of their emergency planning, systemically important banks shall take the necessary measures for the uninterrupted continuation of systemically important functions (Art. 9 para. 2 let. d BA in conjunction with Art. 60 ff. BO). They shall identify the services necessary to continue the systemically important functions in the event of resolution, recovery or restructuring ("critical services") and take the measures necessary for their continuation. In doing so they shall take into account the requirements issued by international standard setters in this context.	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
VI-112	Continuation of critical services during the resolution and recovery of systemically important banks	As part of their emergency planning, systemically important banks shall take the necessary measures for the uninterrupted continuation of systemically important functions (Art. 9 para. 2 let. d BA in conjunction with Art. 60 ff. BO). They shall identify the services necessary to continue the systemically important functions in the event of resolution, recovery or restructuring ("critical services") and take the measures necessary for their continuation. In doing so they shall take into account the requirements issued by international standard setters in this context.	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-08.1	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration of primary processing and/or storage sites is performed.	5	
VII	Transitional provisions	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
VII.A	Concerning ensuring operational resilience	N/A	Functional	Intersects With	Operational Resilience Capabilities	BCD-03	Mechanisms exist to ensure capabilities are implemented to provide operational resilience to: (1) Unintentional errors; and (2) Intentional attack or circumvention.	5	
VII.A-113	Concerning ensuring operational resilience	The identification of critical functions, the definition of tolerances for disruption and initial approvals in accordance with margin nos. 101 and 103, as well as initial reporting in accordance with margin no. 105, will be expected following the Circular's entry into force. A transitional period of one year from the entry into force shall apply for fulfilling the requirements in accordance with margin nos. 106-109 and the first tests in accordance with margin no. 110. It is expected that operational resilience will be ensured in accordance with margin no. 102 and the requirements met in accordance with margin nos. 104 and 111 within a transitional period of two years.	Functional	No Relationship	N/A	N/A	N/A	0	
VII.B	Concerning the capital requirements for operational risk	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
VII.B-114	Concerning the capital requirements for operational risk	The capital requirements for operational risk in accordance with Article 89 ff. CAO shall be based on margin nos. 3-116 of FINMA Circular 2008/21 "Operational risk - banks" until the entry into force of the CAO revised as part of the final Basel III revision package and the implementing FINMA ordinance.	Functional	No Relationship	N/A	N/A	N/A	0	