



Make the world a safer place

AI Cyber Resilience Management

March 2025



Agenda

- | | |
|-----|--|
| I | Regulations on Digital Operational Resilience for the Financial Sector |
| II | The Agnostic Cyber Resilience Management Module |
| III | Benefits |



Requirements for Financial Institutions on Digital Operational Resilience and Cyber Risk Management

The Digital Operational Resilience Act (DORA) as well as FINMA Circular 2023/1 Operational risks and resilience set more restrictive and uniform requirements for financial institutions as well as for critical third parties

- for the security of network and information systems
- to define an internal governance and control framework for an effective and prudent management of ICT risks, including policies and tools for identifying, monitoring, testing and communicating about assets and detecting vulnerabilities
- to manage operational risks, particularly in connection with ICT, and handle critical data and cyber risks

Specific Resilience and Cyber Risk Management Requirements by DORA & FINMA

DORA Art. 8 §2

- On a continuous basis, identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess **cyber threats** and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets.
- Review on a regular basis, and at least yearly, the risk scenarios impacting them.

DORA Art. 17 §2:

- Record all ICT-related incidents and significant cyber threats.
- Establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents.

DORA Art. 18 §2:

- Classify cyber threats as significant based on the criticality of the services at risk, including the transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk.

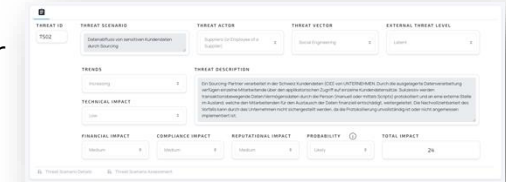
FINMA Circular 2023/1 Operational risks and resilience – C. Cyber Risk Management

- 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

Cyber Resilience Management Module

Threat Scenario Assessment

Define, describe, and evaluate cyber threats and define the potential impact to your organization with a structured process regularly.



Threat Scenario Mapping

Map cyber threat scenarios to your internal controls and derive a control priority based on the threat impact.

Threat Scenario Mapping - Mapping RK 22-12-23

CONTROL POSITION	CONTROL ID	FUNCTION	CONTROL	THREAT SCENARIOS	CONTROL STATUS	CONTROL PRIORITY
1	0001-1	Security	Organizational cybersecurity policy is established and communicated	1000, 1001	OK	✓
2	0001-2	Security	Information security and organizational security are coordinated and aligned with organizational and management objectives	1000, 1001	OK	✓
3	0001-3	Security	Information security and organizational security are coordinated and aligned with organizational and management objectives	1000	OK	✓
4	0001-4	Security	Information security and organizational security are coordinated and aligned with organizational and management objectives	1000, 1001, 1002	OK	✓

Cyber Resilience Report



Cyber Resilience Assessment & Reporting

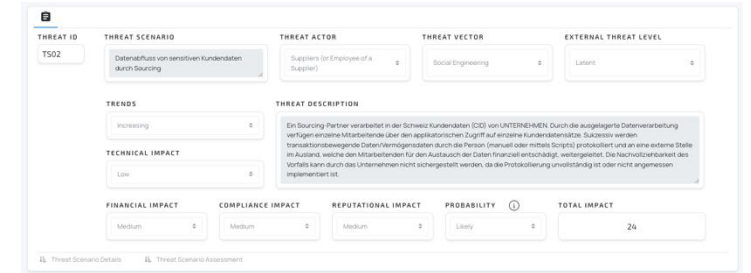
Evaluate the maturity of your internal ICT and cyber controls and automatically assess gaps against required maturity. Present the results of the whole process in a management-friendly way directly via the platform



Elements of the Cyber Resilience Module

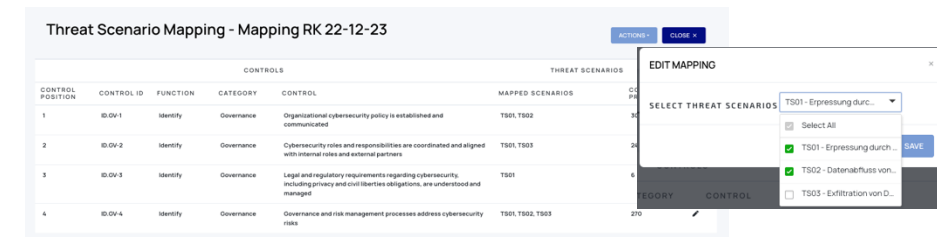
Threat Scenario Assessment

- Identify and define current **Cyber Threat Scenarios**
- Evaluate the Cyber Threat Scenarios based on a **structured risk methodology**.
- Derive the potential total impact to your organization regularly.



Threat Scenario Mapping

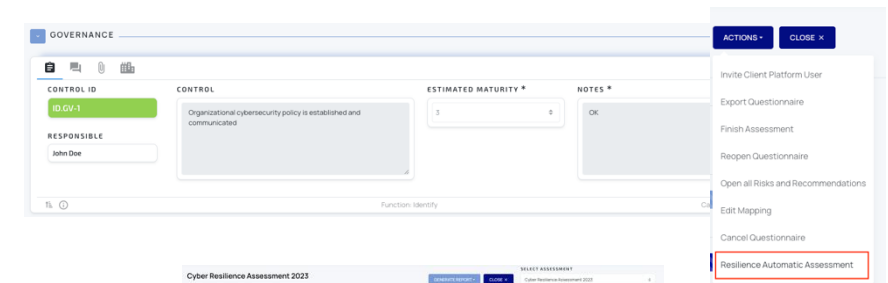
- Map **Cyber Threat Scenarios** to (NIST) Cyber Security Framework and controls
- Derive control priority based on the threat impact.



CONTROL POSITION	CONTROL ID	FUNCTION	CATEGORY	CONTROL	MAPPED SCENARIOS
1	ID.OV-1	Identify	Governance	Organizational cybersecurity policy is established and communicated	TS01, TS02
2	ID.OV-2	Identify	Governance	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	TS01, TS03
3	ID.OV-3	Identify	Governance	Legal and regulatory requirements regarding cybersecurity, including privacy and confidentiality obligations, are understood and managed	TS01
4	ID.OV-4	Identify	Governance	Governance and risk management processes address cybersecurity risks	TS01, TS02, TS03

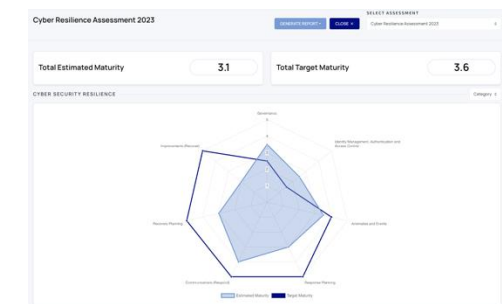
Cyber Resilience Assessment

- Evaluate and assess your **Cyber Resilience Status** (Maturity) based on the (NIST) Cyber Security Framework.
- Automatically** assess gaps against required maturity
- Derive recommendations for improving a (NIST) Subcategory / Control.



Resilience Management Reporting and Manage Improvements

- Summarize a **recommendation catalogue** to the CISO and the Security Board for improving Cyber Resiliency
- Present the results of the full assessment process in a **management-friendly** way
- Define and **track** improvement **actions** on the platform



Views Cyber Resilience Module

The collage displays several key views of the Views Cyber Resilience Module:

- Steps to a successful cyber resilience assessment:** A process flow diagram showing the stages: Unassigned, Invited, In Progress, Submitted, Review, Assessed, and Accepted.
- Mapping Overview:** A dashboard showing mapping progress for different templates, including Threat Scenario Assessment (TSA) and Cyber Resilience Questionnaire (CRA).
- Threat Scenario Mapping - Mapping RK 22-12-23:** A detailed view of a threat scenario mapping, including fields for Threat ID, Threat Scenario, Threat Actor, Threat Vector, and External Threat Level.
- Resilience Management Reports:** A section showing various reports, including a Cyber Resilience Report and a Threat Scenario Assessment Report, with metrics like Total Estimated Maturity and Total Target Maturity.
- Automatic Assessment Completed:** A notification pop-up indicating that the automatic assessment is complete, showing 4 total controls, 0 not assessed, and 4 fully assessed.



Benefits

The Agnostic TPRM platform and its Cyber Resilience Management Module supports financial institutions to comply with DORA and FINMA Circular 2023/1 Operational risks and resilience regulations.

- Identify, document and evaluate your institution-specific threat landscape.
- Assess cyber threats relevant to ICT supported business functions, information assets and ICT assets.
- Review on a regular basis, and at least yearly, the risk scenarios and assess the possible impacts.
- Establish an internal governance and control framework for an effective and prudent management of ICT risks, including policies and tools.
- Be **compliant** with regulatory requirements and **improve** your Cyber Resilience!



Contact Us



Gotthardstrasse 26
CH – 6300 Zug
Switzerland



+41 44 520 33 00



info@agnostic-intelligence.com



<https://www.agnostic-intelligence.com>

Dirk Fisseler, CEO



+41 (0)79 608 95 90



fisselerd@agnostic-intelligence.com

Rolf Kralisch, Head of Platform



+41 (0)76 331 11 60



kralischr@agnostic-intelligence.com

Raphael Jakob, Head of Products and Customer Services



+41 (0)79 850 03 88



jakobr@agnostic-intelligence.com

