AUSTRIAN
FMA · FINANCIAL MARKET AUTHORITY

ICT SECURITY RE-IMAGINED:
FMA EXPERIENCE IN THE IMPLEMENTATION OF DORA

Peter Braumüller
24 November 2025

MILESTONES & NEXT STEPS

Pre-DORA:
FMA Cybersecurity Toolbox, FMA DORA Gap Analysis,
Dialogues, Q&A

DORA-application:
Start eg of DORA incident reporting and risk-based
resilience testing from 17 January 2025;
DORA Deep Dives

Registers of Information (RoI): First reporting to FMA in 2025

Critical ICT third-party provides (CTPPs):
Designation & initiation of oversight framework by end 2025

Integration of supervisory data on ICT-risk:

New module-based structure

MILESTONES & NEXT STEPS

Pre-DORA:
FMA Cybersecurity Toolbox, FMA DORA Gap Analysis, Dialogues, Q&A

DORA-application:
Start eg of DORA incident reporting and risk-based resilience testing from 17th January 2025;
DORA Deep Dives

Registers of Information (RoI): First reporting to FMA in 2025

Critical ICT third-party provides (CTPPs):
Designation & initiation of oversight framework by end 2025

Integration of supervisory data on ICT-risk:

New module-based structure

DORA PREPARATION- OVERVIEW

FMA Maturity Level Assessments

- FMA Cyber Maturity Level Assessment
- FMA Cloud Maturity Level Assessment
- FMA Blackout Maturity Level Assessment
- FMA Mitigations Assessment
- **FMA DORA Gap Analysis 2024**

FMA Cyber Security Exercise

ICT Service Provider Map of the AT financial market

FMA ICT-related Data Incident Collections

Dialogues & Deep Dives with supervised undertakings

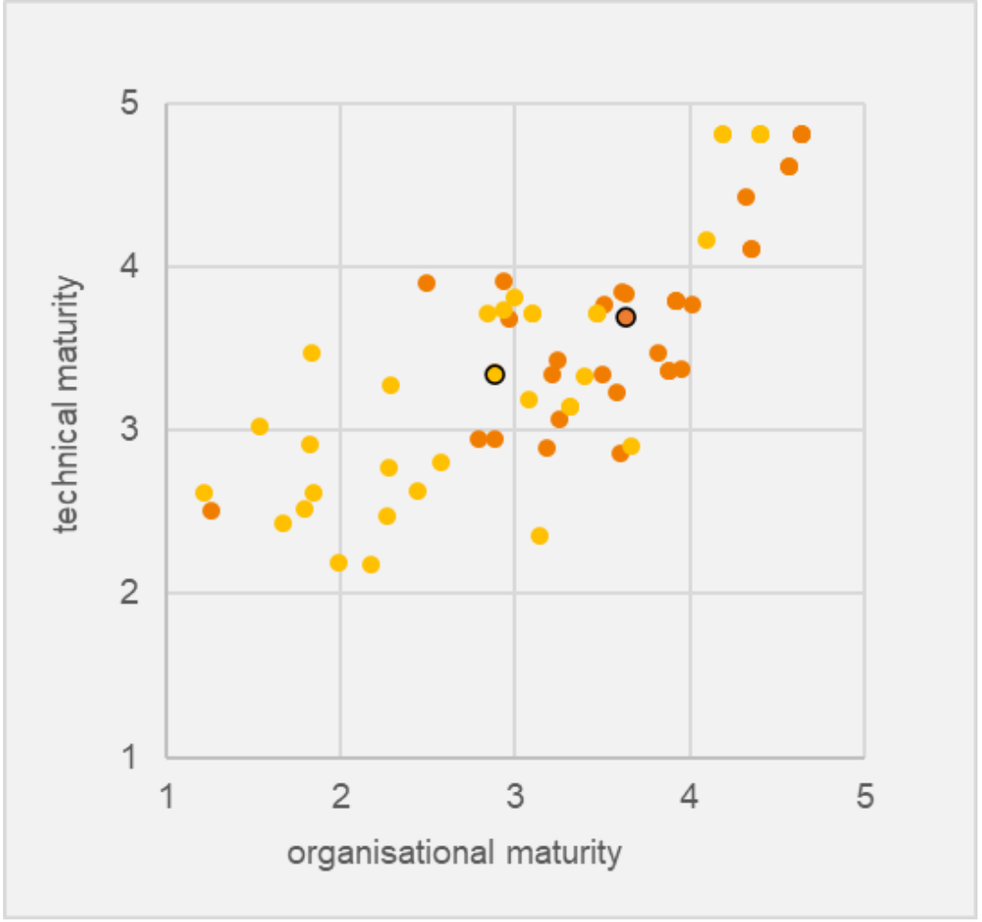
DORA PREPARATION- EXAMPLES OF ACTIVITIES

FMA Cyber Maturity Level Assessments

- Conducted 2019-2022, covering insurers and pension funds
- Broad assessment, about 60 questions on ICT-security measures
- Thematically very similar to new DORA requirements on ICT-RM
- Improvements between surveys noted and confirmed by on-sites

FMA Cyber Security Exercise

- Two runs with 6 undertakings in total conducted in 2022/23
- Tabletop exercise conducted in realtime with insurer‘s crisis team
- Focus on realism: real-life attack scenario, incomplete information for participants, time-pressure for their reactions



Graph: Cyber Maturity Level Assessment
Results of individual insurance undertakings
2019 (yellow) vs 2021 (orange)

MILESTONES & NEXT STEPS

Pre-DORA:
FMA Cybersecurity Toolbox, FMA DORA Gap Analysis,
Dialogues, Q&A

DORA-application:
Start eg of DORA incident reporting and risk-based resilience testing from 17th January 2025;
DORA Deep Dives

Registers of Information (RoI): First reporting to FMA in 2025

Critical ICT third-party provides (CTPPs):
Designation & initiation of oversight framework by end 2025

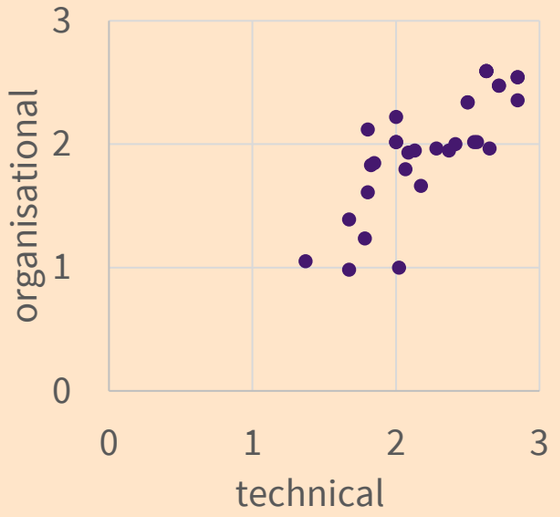
Integration of supervisory data on ICT-risk:

New module-based structure

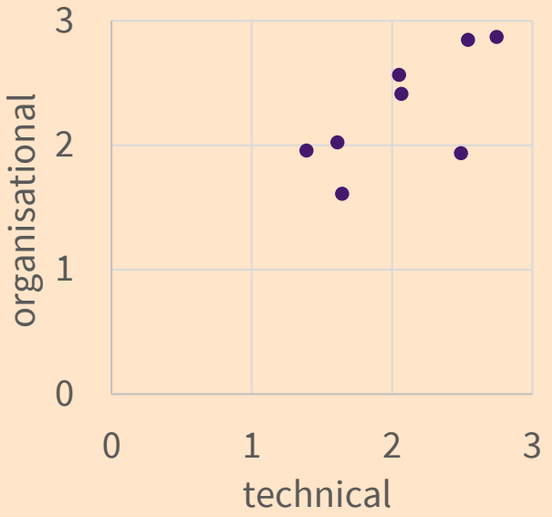
FMA DORA GAP ANALYSIS 2024 & SUBSEQUENT DEEP DIVES

Organisational & technical implementation levels

Insurance undertakings



Pensionskassen



3 - requirement fully met

2 –minor adjustments required

1 –major adjustments required

Key findings

- ICT risk management:
  Review of the ICT risk management framework partially undeveloped, ICT risk control function not fully in place
- Digital resilience testing:
  Vulnerability & network scans & penetration tests already in use pre-DORA
- ICT third-party risk management:
  Intensive effort to set up registers of information
- DORA incident management & reporting:
  Development of processes & structures

⇨ Deep Dives

DORA THREAT-LED PENETRATION TESTS (TLPTS)

Risk-based
testing programs

Threat Led Penetration
Testing

TLPT preparations

- Identification of supervised entities required to perform TLPTs:
  Information of respective undertakings
- FMA-preparation for test manager-role:
  Performed together with OeNB
- Generic threat-landscape:
  Input for undertaking-specific threat scenarios
- Preparation of processes with OeNB:
  OeNB provides expert opinions &
  FMA issues certificates

MILESTONES & NEXT STEPS

Pre-DORA:
FMA Cybersecurity Toolbox, FMA DORA Gap Analysis, Dialogues, Q&A

DORA-application:
Start eg of DORA incident reporting and risk-based resilience testing from 17th January 2025;
DORA Deep Dives

Registers of Information: First reporting to FMA in 2025

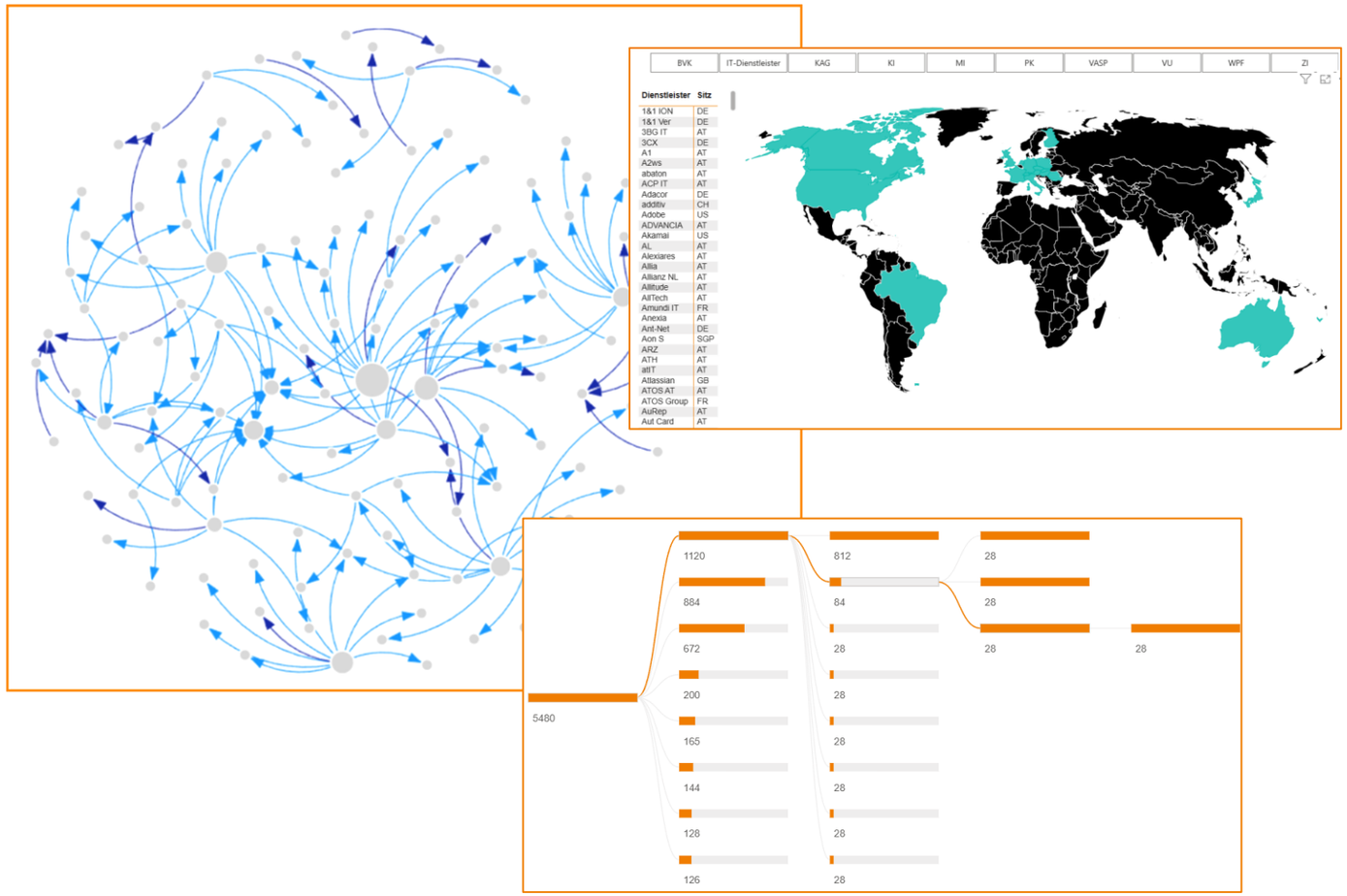
Critical ICT third-party provides (CTPPs): Designation & initiation of oversight framework by end 2025

Integration of supervisory data on ICT-risk:

New module-based structure

ICT-SERVICE PROVIDER LANDSCAPE

Dashboard:



FMA DORA preparation work

- Key IT areas in finance were outsourced to specialized service providers since the 2010s
- Outsourcing increased, especially with cloud services
- ICT providers now face even more cyberattacks and major service risks
- Now, majority of incidents at insurers propagate through ICT provider

FMA ICT service provider landscape

- Created in 2021 based on dedicated survey, partially updated until 2023
- Covers critical providers
- Data now supplemented by RoI (but RoI data still incomplete regarding groups)

REGISTERS OF INFORMATION (ROI): FIRST REPORTINGS 2025

RoI-reportings to FMA & ESAs

- Reporting time frame:
  April / May 2025
- Communication with supervised entities:
  eg via letters, web conferences, mail
- Multi step approach:
  - Upload of xlsx-template to FMA
  - Automatic quality checks
  - Transmission to EBA
  - Corrections and resubmissions as needed
- Data quality:
  Good AT data quality acc. to ESAs feedback
- FMA-RoI-dashboard:
  PowerBI analyses

⇨ High overall effort required

RoI Use Cases

- Input for supervisory activities:
  eg on-site inspections
- Identification of DORA-incident impact:
  Usage of respective ICT-third party provider
- Analysis of concentration risk:
  Identification of non-critical ICT-third party provider concentrations
- Identification of critical third-party providers (CTPPs):
  Designation of CTPPs and start of new oversight framework by end 2026

MILESTONES & NEXT STEPS

Pre-DORA:
FMA Cybersecurity Toolbox, FMA DORA Gap Analysis,
Dialogues, Q&A

DORA-application:
Start eg of DORA incident reporting and risk-based
resilience testing from 17th January 2025;
DORA Deep Dives

Registers of Information (RoI): First reporting to FMA in 2025

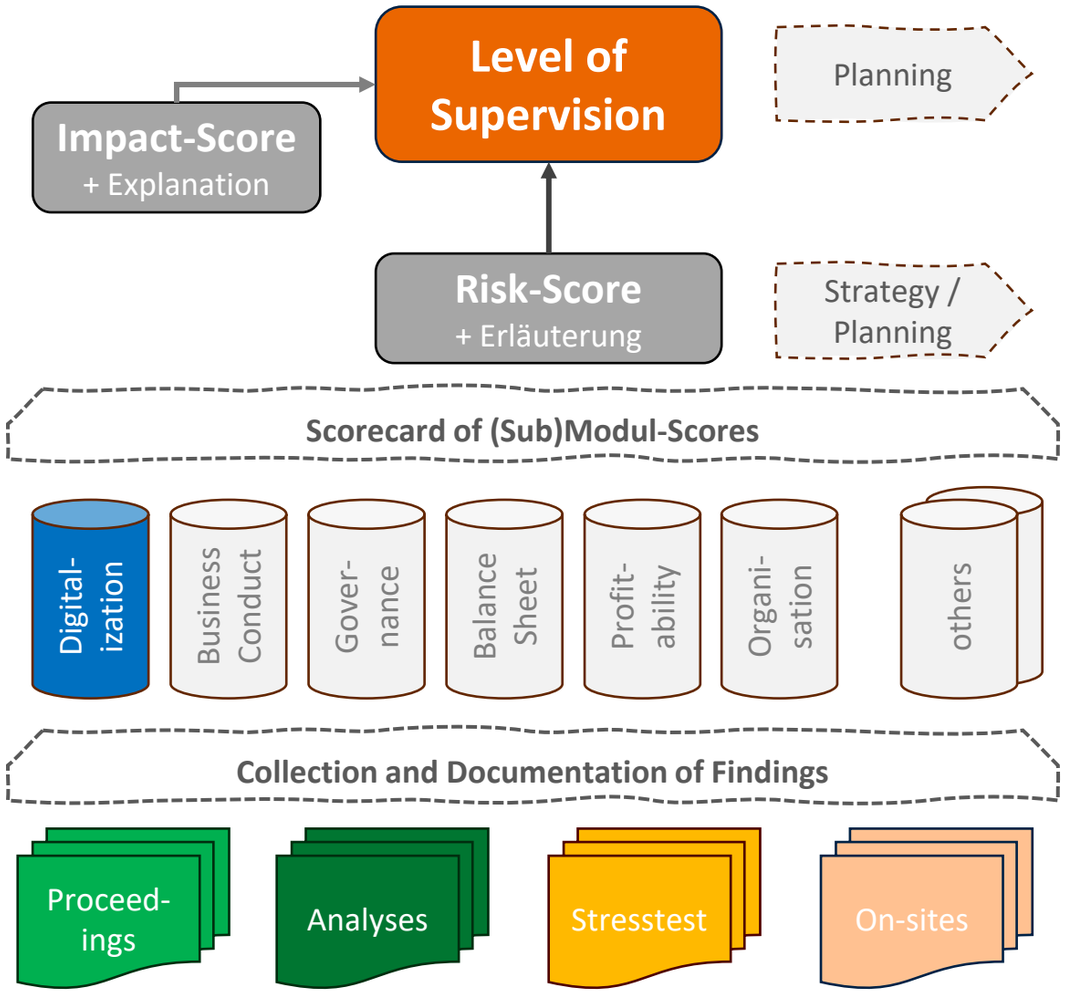
Critical ICT third-party provides (CTPPs):
Designation & initiation of oversight framework by end 2025

Integration of supervisory data on ICT-risk:

New module-based structure

RISK MAP – INCLUDING RISK MODULE ON DIGITALIZATION

Interface with overall supervisory framework



Level of Supervision

- Defining **Level of Supervision** as low / medium / high / very high

Impact-Scoring

- Depends on financial footprint of the undertaking on the market

Risk-Scoring

- Aggregated from the scores of the individual modules

Supervisory (Sub)modules

- Structured scoring of a supervisory topic, based on its sub-topics

Supervisory instruments and activities

- Make structured and pre-analysed information on supervised undertakings available

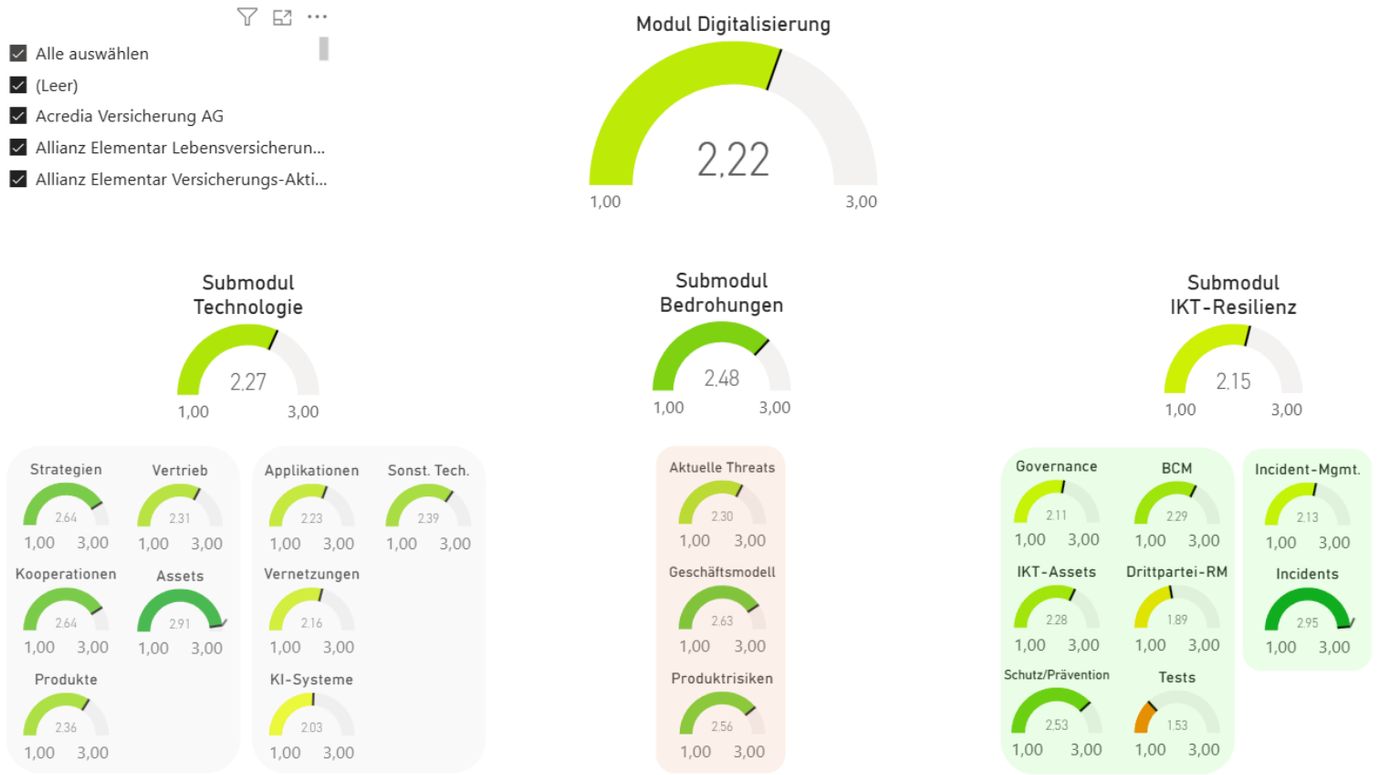
RISK MODULE DIGITALIZATION

Goals

- The FMA Cyber Toolbox has been integrated with the Risk Scoring since its inception
- he module approach can facilitate:
  - Documentation and transparency
  - Continuously checking/adapting the weights given to various subtopics
  - Priorisation of future focus topics
  - Communication and knowledge sharing

´Implementation

- Predetermined weights determine score aggregation
- Current scores reflect past focus topics and aggregated supervisory information
- Final scores not calculated purely automated - expert judgement included to validate and enrich the final result



Picture: Screenshot from Digitalisation Module Dashboard

AUSTRIAN FINANCIAL MARKET AUTHORITY

Competence Control Consistency