Observance of CPSS-IOSCO Principles for Financial Market Infrastructures (PFMI) and Cyber Resilience of FMI

Tools and techniques to assess cybersecurity risk

FEBRUARY 1, 2024

RANGACHARY RAVIKUMAR

Oversight vs Supervision

Oversight	Supervision
Less intrusive, ad-hoc, assessment focused	More hands-on and intrusive, continuous, risk based
Often lacking legal powers (e.g. sanctions) and based on moral suasion	Has legal powers and enforcement rights (e.g. sanctions)
Normally desk-based, with limited on-site visits	More on-site inspections
Often lacks right to audit third parties	Normally has right to audit third parties
Often oversight functions have less resources	Normally supervisory authorities have more dedicated and specialized resources
Often lacks regulatory framework and clear requirements	Normally enshrined in regulation and clear requirements
Often relies on FMI self-assessments	Normally will take a risk based approach, gathering substantive and large base of evidence

FMI supervision approaches are changing..

- Cyber Resilience Oversight Expectations – Europe, Canada
- DORA – Europe
- Operational Resilience
- FSMA 2023 – Bank of England
- Regulation and Supervision of Financial Market Infrastructures regulated by RBI

The problems….

Traditionally, oversight of FMIs has been desk-based, not intrusive, and focused on reviewing self-assessments against the Principles of Financial Market Infrastructures;

Continuous oversight often not in place – ad-hoc approach and limited onsite activity

High level principles applied, but without substantive risk assurance work, and without clear expectations, assessment methodology and end-to-end process

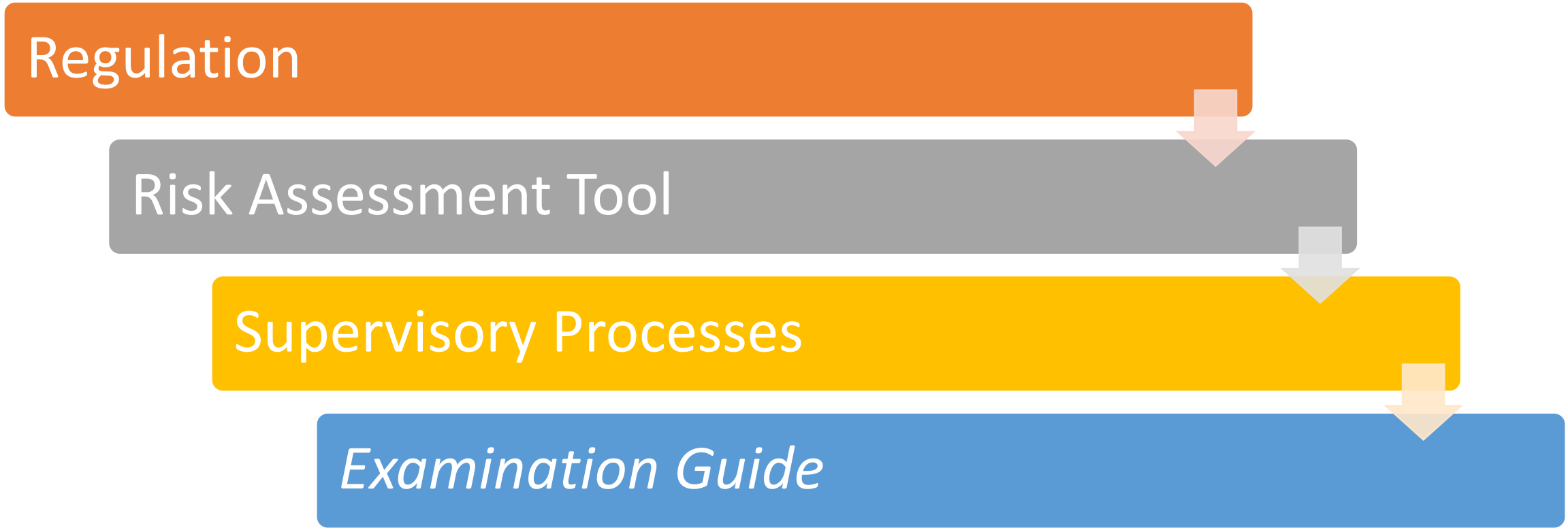
In central banks, oversight of RTGS often lacks sufficient independence and power

Lack of cyber expertise

FMI dependency on third parties is high, but effective oversight of third parties is often lacking and overseers often do not use Annex F effectively

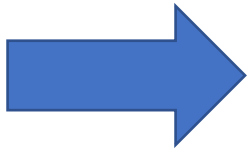
Going forward, oversight needs to adapt to a more supervisory, intrusive and continuous approach

Cyber Risk Supervision Toolkit



Model Regulation => Examination Guide

- D1 - Governance & Oversight
- D2 - Technology and Cyber Risk Management
- D3 - IT Services Management
- D4 - Cyber Security Operations
- D5 - Response & Recovery
- D6 - Scanning, testing, exercising and remediation
- D7 - Independent assurance
- D8 - Outsourcing and technology service provider (TSP) management



A. Examination goals
B. Planning
C. Execution / Assessment
D. Notes

Examination Objectives/Goals

- Decide the examination objectives and goals based on the inputs available.

Planning

- Information gathering*(strategy, org. structure, internal policies, internal audit reports, incident reports, any other relevant reports(ISO27001, PCI DSS). CVs of IT and cybersecuirty key staff etc)*

Execution/ Assessment

- Interview results, test results*(evidence)* etc.

Reporting

- Summary of all finding and/or non-compliance issues
- Detailed information for every single findings and/or non-compliance issues

Follow Up

- Follow Up report to show progress of the findings and/or non-compliance issues

Risk Assessment Tool

Assessment methodology (Word/PDF File)

User Guide (Word/PDF File)

Assessment Tool (Excel File)

MANAGING TECHNOLOGY RISK, CYBER RESILIENCE, AND BUSINESS CONTINUITY IN REGULATED ENTITIES	Score	Rating_Calc
D4 - Cyber Security Operations	**Moderate**	**2.63**
Cyber Threat Intelligence and Information Sharing	**Moderate**	3.25
There is established process to collect, process and analyse cyber-related information (for its relevance and potential impact to the FI's business and IT environment) which include cyber events, cyber threat intelligence and information on system vulnerabilities.	Strongly disagree	4
The collected information includes voluntary and collaborate industry or national networks, where such networks exist.	Somewhat disagree	3
FI procures cyber intelligence monitoring services.	Somewhat agree	2
FI participates in cyber threat information-sharing arrangements with trusted parties (to share and receive timely and actionable cyber threat information).	Strongly disagree	4
Cyber Event Monitoring and Detection	**Minimal**	2.00
Cyber Incident Response, Management, and Reporting	**Moderate**	3.25
Incident Reporting	**Minimal**	2.00

Risk Assessment Tool – Methodology

The basic assessment approach:

Available: Control design is correct.

Adequate: – Controls are satisfactory to mitigate risks.

Implemented: Controls are operational.

Effective: Controls are capable of mitigating risks.

Risk Assessment Tool – Methodology

The basic assessment approach:

Assessment of controls with reference to the strategies, policies, standards, and procedures for each element under each domain	Control(risk) rating
Available, adequate, implemented, and effective	4
Available, adequate, and implemented, but mostly not effective	3
Available and adequate, but mostly not implemented	2
Not available, or available but inadequate	1

Supervisory Process - Preparatory Work

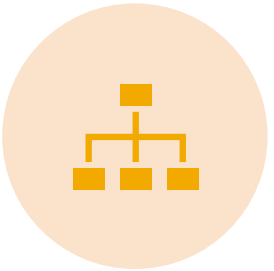
A.	Standing committee for cyber preparedness
B.	Cyber risk management regulation or guidelines
C.	Cyber risk supervisory unit (CRSU)
D.	Cyber risk examination guide (CREG) or cyber risk supervision manual (CRSM)
E.	Pilot examinations
F.	Expected maturity levels

Core Supervisory Processes

G. OFFSITE SUPERVISION

H. ONSITE SUPERVISION (EXAMINATION)

I. OVERSIGHT OF CYBERSECURITY TESTING



J. INTERRELATIONSHIPS BETWEEN CORE SUPERVISORY PROCESSES

Support processes

K.	Process regulatory returns and incident reporting
L.	Quality assurance
M.	Training
N.	Industry consultation
O.	Support sectoral information sharing
P.	Public outreach and education
Q.	Cooperation with government agencies
R.	International cooperation
S.	Supervisory framework improvement

Advanced topics

T. Integrated cyber risk supervision
U. Financial computer emergency response team (FinCERT)
V. Supervisory technologies (SupTech)
W. Promoting research

Supervisory Assessment - coverage

- IT / Cyber governance practices;
- Effectiveness of Board/management engagement;
- Cyber security policies and procedures;
- Risk Management practices;
- Characteristics and effectiveness of firm’s monitoring, testing and internal/systems auditing practices;
- Data integrity and security controls;
- Incident management, recovery and reporting;
- Information sharing within the industry; and
- Independent validation of threats, vulnerabilities, cyber security gap analyses and action plans for mitigations.

Off-site supervision

Continuity to the supervisory/oversight efforts by collecting, analyzing and monitoring cyber risk data / indicators at more frequent intervals and in-between on-site inspections

Contributing to the on-site work to make it more focused and efficient

Policy inputs and exception handling

Coordination with various stakeholders / market intelligence

Cyber Exercises

Helping build cyber awareness

Risk Profile

Technology landscape

Digital products

Inter-connections – between entities and market infrastructure, between market infrastructures

KRIs

Third Party Dependency Registry

Dashboard

Baseline expectations – Gap assessment

Either mandated or voluntary;

Drawn from international standards;

Level of preparedness of supervised/overseen entities a key input;

Gaps need to be monitored and closed;

Informs supervisors/overseers about challenges in implementing certain expectations;

Enables monitoring of progress at institutional level as well as the system as a whole

Cyber mapping

IMF paper on Cyber Risk Supervision

Cyber Mapping is useful

Entities to be encouraged to commence such exercises

Collecting such mapping would play a role in motivating

Useful in identifying key gaps / vulnerabilities

Key Risk Indicators

- Indicators provide insights into cyber preparedness
- To cover identify, protect, detect, respond and recover functions
- Aggregated score can provide useful metric to assess cyber security posture
- Provides a comparability with other entities
- Enables monitoring progress over a period
- Useful in understanding the areas that require supervisor’s/overseer’s attention
- Summary level cyber incident data

Concentration

Major technologies adopted in critical applications

Implementation challenges; migration issues;

Data on concentrations

Vendor

Product

Third party services

Cloud service providers

Other critical service providers

Information sharing

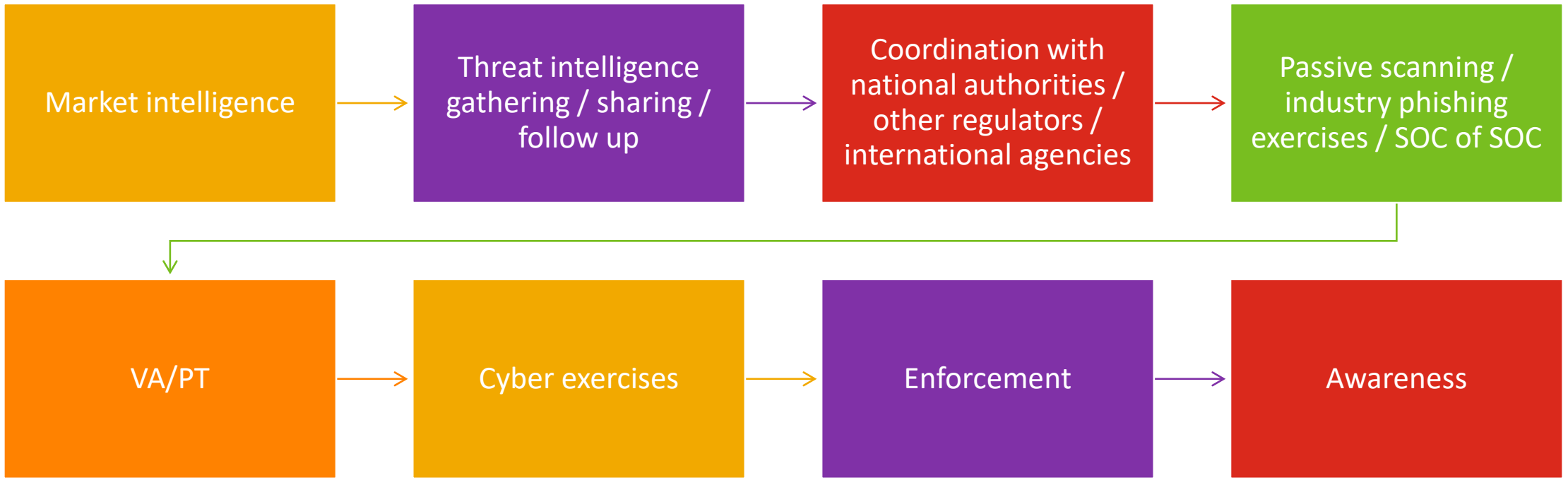
MECHANISM TO COLLECT INFORMATION

ARRANGEMENTS TO RESPOND TO REPORTED INCIDENTS

DISSEMINATING THE LEARNINGS

GAPS IN REPORTING, INCORRECT REPORTING, NON-REPORTING

Other functions



Process

Planning / Scanning / Scoping

- Based on resources, what, when and how; Environment
- Off-site inputs; Key risk register
- Resource identification

Pre-Inspection

- Carefully seek data/info
- Ask for presentations
- Identify weak spots
- Discuss / Research

On-site

- Allocate work areas;
- Take periodic feedback;
- Soft skills / inquisitive
- Collect evidence

Report Preparation

- Concise – to the point
- Based on evidence
- Progressive
- Not a fault finding mission

Quality Assurance

- Rating approval;
- Consistency of findings
- Objectives met
- Presentation to Committee with Team

Exit meeting

- Verify facts;
- Discuss material findings;
- Agree on remediation timings;

Post Inspection

- Brief your management;
- Feed back to off-site team
- Feedback to regulators

Tools / Techniques

Data / verifying records	Presentations by relevant teams	Step-by-step walk through of different processes	Interviews – with key stakeholders
Board Agenda / minutes	Discussions with top management	Market intelligence	Key Risk Register / Off-site inputs / Incident inputs / Frauds / Customer complaints
Use of independent external auditors and testers	Thematic reviews and deep dives on specific topics	Onsite inspections	Self-assessments, surveys and questionnaires to build evidence-base

Conclusion

- FMIs play an important role
- Traditionally, the oversight has been light touch
- Considering the critical role, interconnections and interdependencies there is a need to strengthen oversight further.
- Changes to supervisory approaches visible
- Oversight need to be elevated to supervision, on assessing cyber risk.

Thank you!