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

Response and Recovery, Testing

FEBRUARY 1, 2024

RANGACHARY RAVIKUMAR &

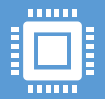
EMRAN ISLAM

CPMI IOSCO Cyber Resilience Guidelines

Cyber: Refers to the interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.

Cyber Risk: The combination of the probability of an event occurring within the realm of an organization's information assets, computer and communication resources and the consequences of that event for an organization.

Cyber Resilience: An FMI's ability to anticipate, withstand, contain and rapidly recover from a cyber attack.



Lexicon Definition: The ability of an organization to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.

… contd

The level of cyber resilience, which contributes to an FMI's operational resilience, can be a decisive factor in the overall resilience of the financial system and the broader economy.

Provides supplemental guidance to the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI), primarily in the context of governance (Principle 2), the framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risk (Principle 17) and FMI links (Principle 20).

Given the extensive interconnections in the financial system, the cyber resilience of an FMI is in part dependent on that of interconnected FMIs, of service providers and of the participants.

CPMI-IOSCO Guidance on Cyber Resilience for FMI – June 2016

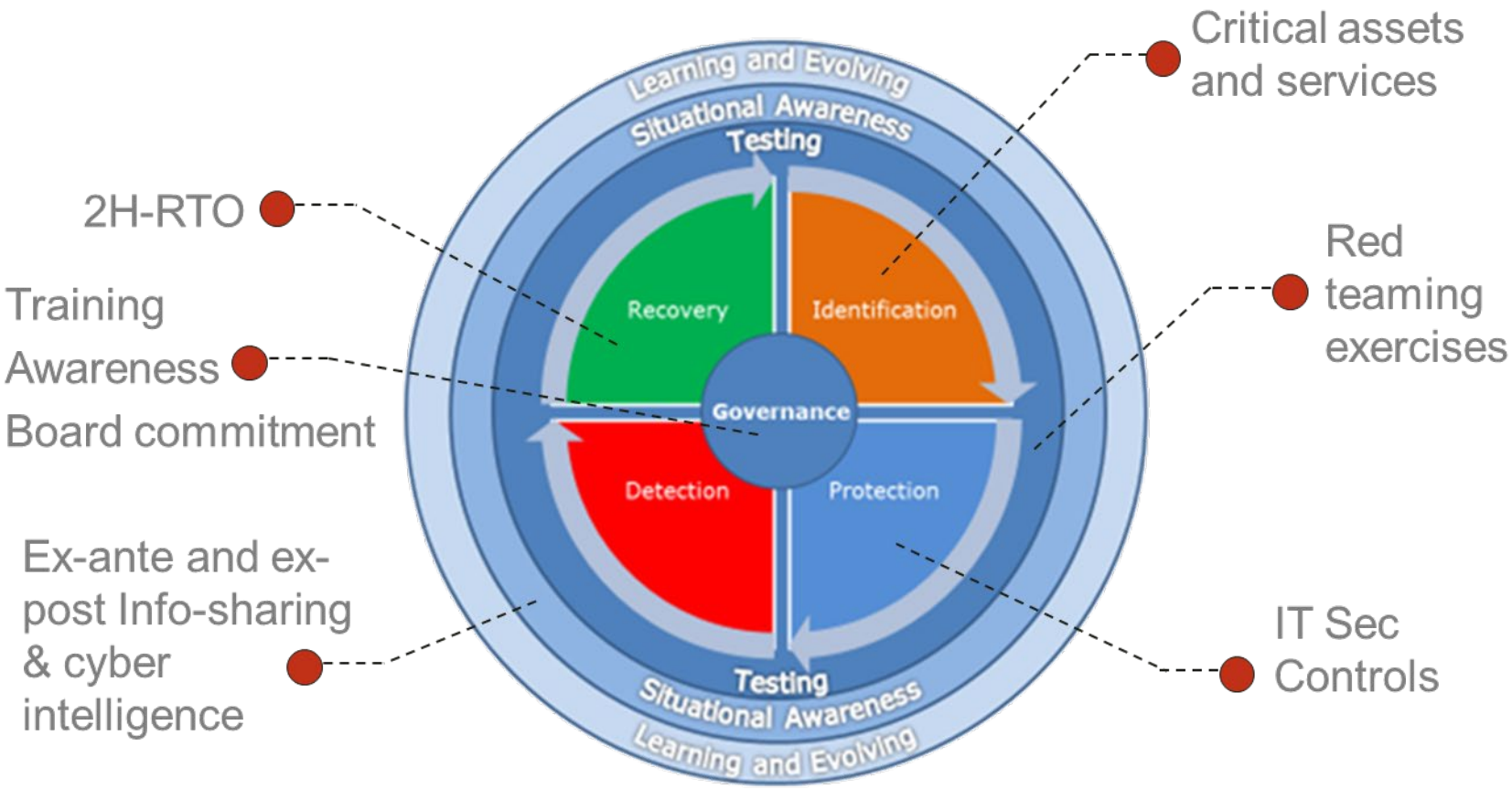
The Guidance is structured in chapters defining five main risk management categories and three general components that should be considered when talking about cyber resilience applied to FMI.

- Risk management categories are:
  i. Governance
  ii. Identification
  iii. Protection
  iv. Detection
  v. Recovery

- General components are:
  i. Test
  ii. Situational awareness
  iii. Learning and Evolution

https://www.bis.org/cpmi/publ/d146.pdf

CPMI-IOSCO Guidance on Cyber Resilience for FMI…key elements



Incident response, resumption and recovery

Incident response planning

- Thorough investigation to determine its nature and extent as well as the damage inflicted
- Immediate actions to contain the situation to prevent further damage and commence recovery efforts

Resumption within two hours

- Design and test its systems and processes to enable the safe resumption of critical operations within two hours
- Complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios
- Exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate

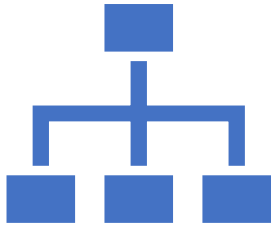
Contingency planning

- Plan for scenarios in which two-hour resumption may not be feasible
- Plan for situations where critical people, processes or systems may be unavailable for significant periods

Planning and preparation

- Develop and test response, resumption and recovery plans.
- Consider cyber threat intelligence, information-sharing and lessons learned from previous events
- Consult and coordinate with relevant internal and external stakeholders

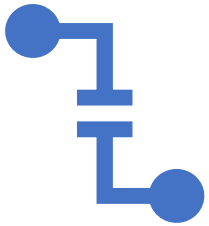
Design elements



Design and business integration

System and process design and controls for critical functions and operations should support incident response activities and to limit the impact of any cyber incident, resume critical operations within two hours of a disruption, complete settlement by day-end and preserve transaction integrity.

Closely integrated with crisis management, BCP/DR



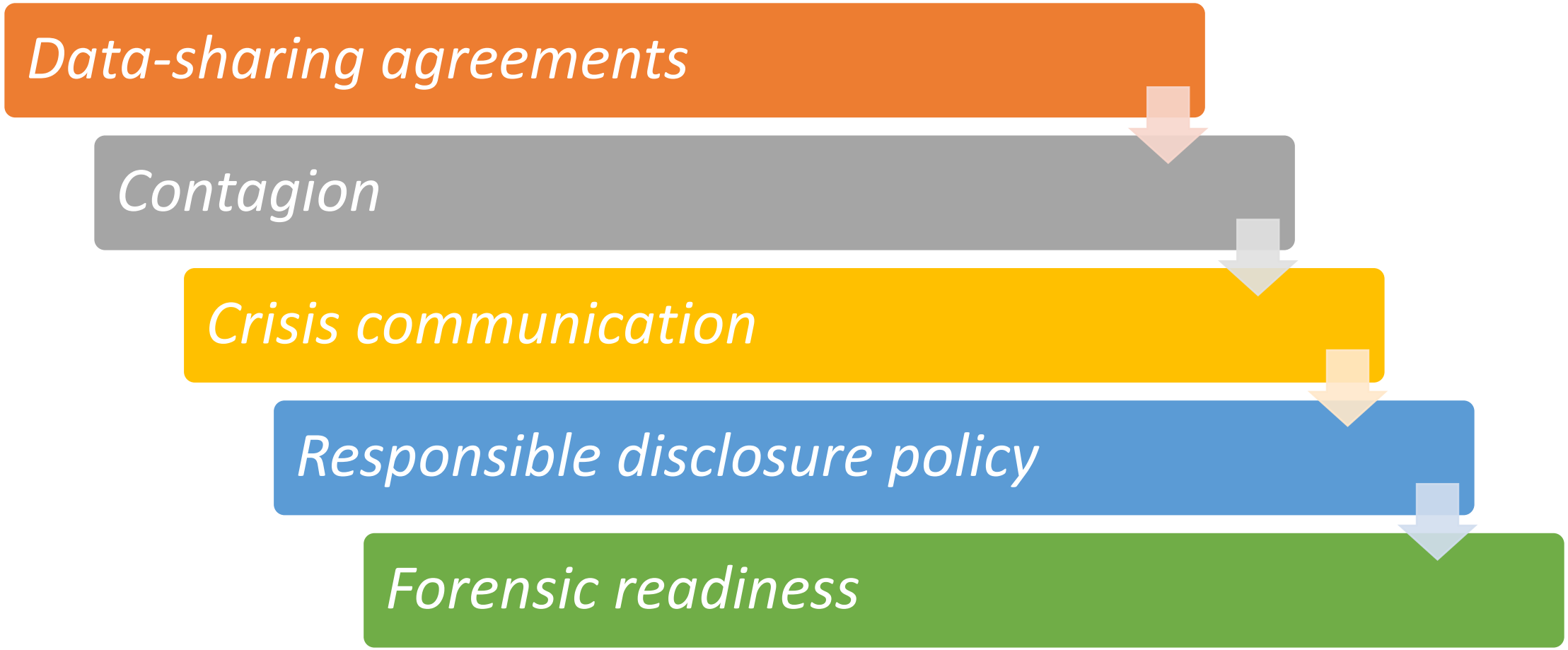
Data integrity.

Design and test their systems and processes to enable recovery of accurate data following a breach. Safeguard data instances.

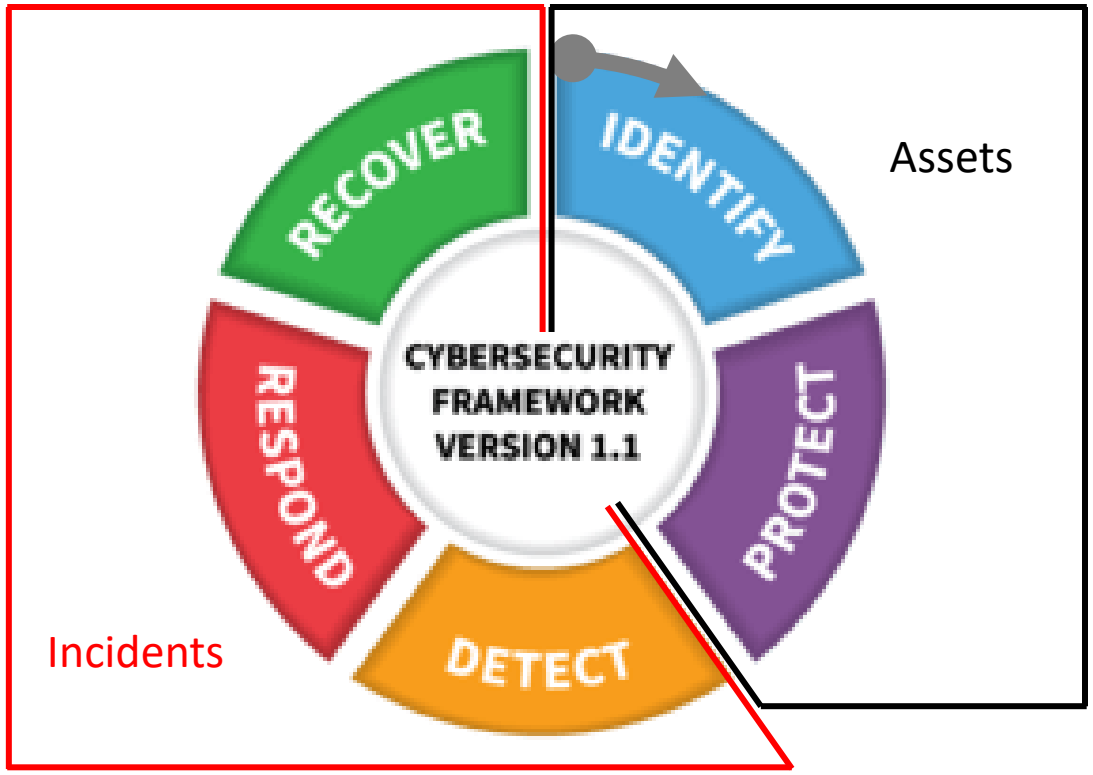
Recovery point objectives consistent with the FMI's resumption time objective for critical operations.

Should consider diverse approaches to achieving these objectives.

Interconnections



Where does incident response and recovery fit?



NIST Cybersecurity Framework

FSB Effective Practices for Cyber Incident Response and Recovery (2020)

Key effective practices

- **Governance** (how do we organize ourselves?)
  - Clearly defined roles and responsibilities
  - Incident coordinator
  - Executive sponsorship and culture
  - Funding and metrics
- **Preparation** (what if things go wrong?)
  - Plans and playbooks
  - Communication strategies, channels and plans
  - Test and exercise
  - Security Operations Centre
  - Log management and forensic capabilities
  - Supply chain management

Key effective practices (cont'd)

- **Analysis** (how did things go wrong?)
  - Transaction and log analysis
  - Trusted information sources
- **Mitigation** (what is our immediate response?)
  - Containment and isolation
  - Plan activation
  - Eradication
- **Recovery** (how do we get back to normal?)
  - Prioritization
  - "Golden copy" of data / last known good state
  - Validation

What should supervisors do?
Examination planning tips: incident response and recovery

Task	Steps, considerations, and tools
Understand IRR governance	Review • Policies and procedures Interview • CIO and CISO • CRO • Incident response coordinators
Assess risks and identify controls	• Are governance structures conducive to fast and effective response? • Is the IRR process / program appropriately funded? • Are there incident coordinators? Are they empowered and capable? • Are metrics used? • Are there regular tests and exercises? • Is there extensive logging and are the logs protected? • Are there log analysis and forensic capabilities available? • Are there known good copies of systems and data? • Is there validation and debrief after recovery?
Test of controls	(out of scope)

Testing

- **In Testing, all elements of a cyber resilience framework should be rigorously tested to determine their overall effectiveness before being deployed within a financial institution, and regularly thereafter. Sound testing regimes should produce findings that are used to identify gaps in stated resilience objectives and provide credible and meaningful inputs to the financial institution's cyber risk management process.**

  - Generally, there are four key types of testing:
    - Vulnerability scanning;
    - Penetration testing;
    - Scenario-based testing – market-wide, desktop, simulations and crisis management; and
    - Red team testing.

Exercising

- Conducting market-wide, scenario based testing or exercising is a vital way of improving crisis preparedness, improving the resilience of the financial sector and enhancing co-ordination between all the stakeholders
- These exercises can be market-driven or authority driven
- They provide valuable lessons to all participants
- Are relatively easy to operationalize and cost-effe
- Requires clear scenarios, playbooks, adequate preparation, and clear leadership
- Leads to findings and areas of focus for the entire sector

A working example – UNITAS - market-wide exercise

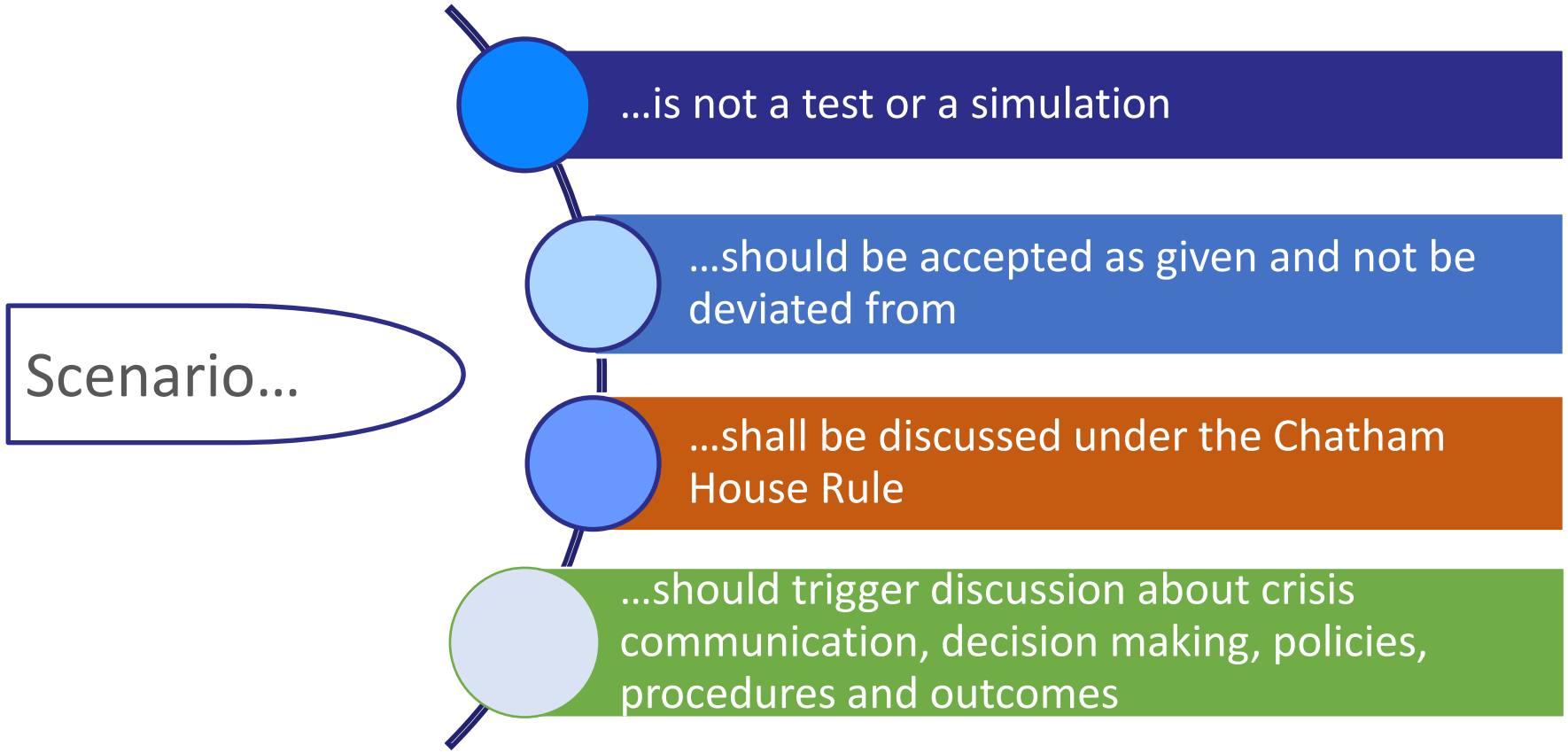
Scenario: cyber attack on financial infrastructures; loss of data integrity and knock-on effect

Observe reactions

Draw conclusions

Provide recommendations

Rules of engagement



Each table **nominates a speaker**, who will present the summarized key findings and conclusions.

Example - Agenda

09:00	Welcome and introductory remarks		
09:05	Phase 1	10:20	Presentations & collective discussion
10:50	Coffee break		
11:00	Phase 2	12:50	Presentations & collective discussion
13:20	Wrap-up and conclusion on the key lessons, outcome & follow-ups		
13:30	Lunch		

Scenario Phase 1, Stage 1
Exercise time 12.30pm, date: 28 June 2021

A staff member of your institution received a phone call during the lunch hour, by an individual referring to himself as 'Underground Rising'. The individual announced an attack on the institution within the next 90 minutes. The individual informed the staff member of his precise username and password, and information about an email he sent 32 minutes ago. The individual warned that the public will know about the attack. Given the very confidential nature of information related to the staff member, he is concerned that the threat is very plausible.

❑ *For the purposes of this exercise, assume Underground Rising is a highly renowned hacktivist group.*

Question for FMIs/MIs/SPs/CCPs/CSDs:

1. How would your institution respond to this situation?

Questions for Overseers:

1. Do you have any arrangements in place to be informed by your overseen institutions about such imminent threats?
2. Assuming you have been informed by your respective institution of the imminent threat, how would you respond to this situation?

Scenario Phase 1, Stage 2
Exercise time 14.00, date: 28 June 2021

The hacktivist group ('Underground Rising') has hacked your institution's website and made a public announcement on it, stating that the institution has been hacked and that its data integrity has been compromised. The "national cybersecurity agency" (or the equivalent) in one jurisdiction has confirmed increased activity on the dark web with regards to the hacktivist group and has informed the institution in that jurisdiction that a number of other institutions (FMIs, MIs and SPs) also appear to have been targeted

❑ *For the purposes of this exercise, assume that you are the institution that has been informed by the national cyber security agency (or equivalent).*

Questions for FMIs/MIs/SPs/CCPs/CSDs:

1. How would your institution respond to this situation?
2. More specifically, participants should structure their thinking around the following questions:
   - Do you have policies and procedures in place to validate whether your data integrity has been compromised? If so, what are they?
   - Do you have a relationship with your national cybersecurity agency (or equivalent) and clear communication protocols in place? If so, what are they?
   - What are your communication protocols with other FMIs, MIs and your service providers and what other information sharing arrangements are you a part of (international, cross-border)? At what point in time would you make use of these protocols?
   - How would you respond, in terms of public communications, to the public announcement made by the hacktivist group? What kind of message would you release and when?

Questions for Overseers:

1. What is the role of the overseer in this situation?
2. Do you have any arrangements in place to be informed by your overseen institutions about the materialization of a threat?
3. If yes and you are informed by your respective institution of the situation, how would you respond?

Scenario Phase 2
Exercise time 15.30, date: 28 June 2021

Several participants have noted discrepancies during their reconciliation processes and have asked the institutions (FMIs and T2S) to confirm their flow of transactions and balances. Following internal investigations, some institutions (FMIs and T2S) discover that their data integrity has been compromised.

- *For the purposes of this exercise, assume the data integrity of your institution has been compromised.*
- *For the purpose of this phase, please use the following definition when giving due consideration to the core themes and questions: **"Compromised data integrity"** is the compromise of security that leads to accidental or unlawful creation, destruction, loss, or alteration to data transmitted, stored, or otherwise processed".*

Questions for FMIs/MIs/SPs/CCPs/CSDs:

1. Based on the definition of 'compromised data integrity', what are the different possible data integrity scenarios which your institution may be subject to and what are their implications on your institution and the ecosystem? These data integrity scenarios should consider the plausibility of creation, destruction, loss or alteration to data transmitted, stored, or otherwise processed.
2. Do you have operational policies and procedures in place to address the different types of data integrity scenarios from question 1? In such scenarios what are the possible implications in terms of settlement finality?

Questions for overseers:

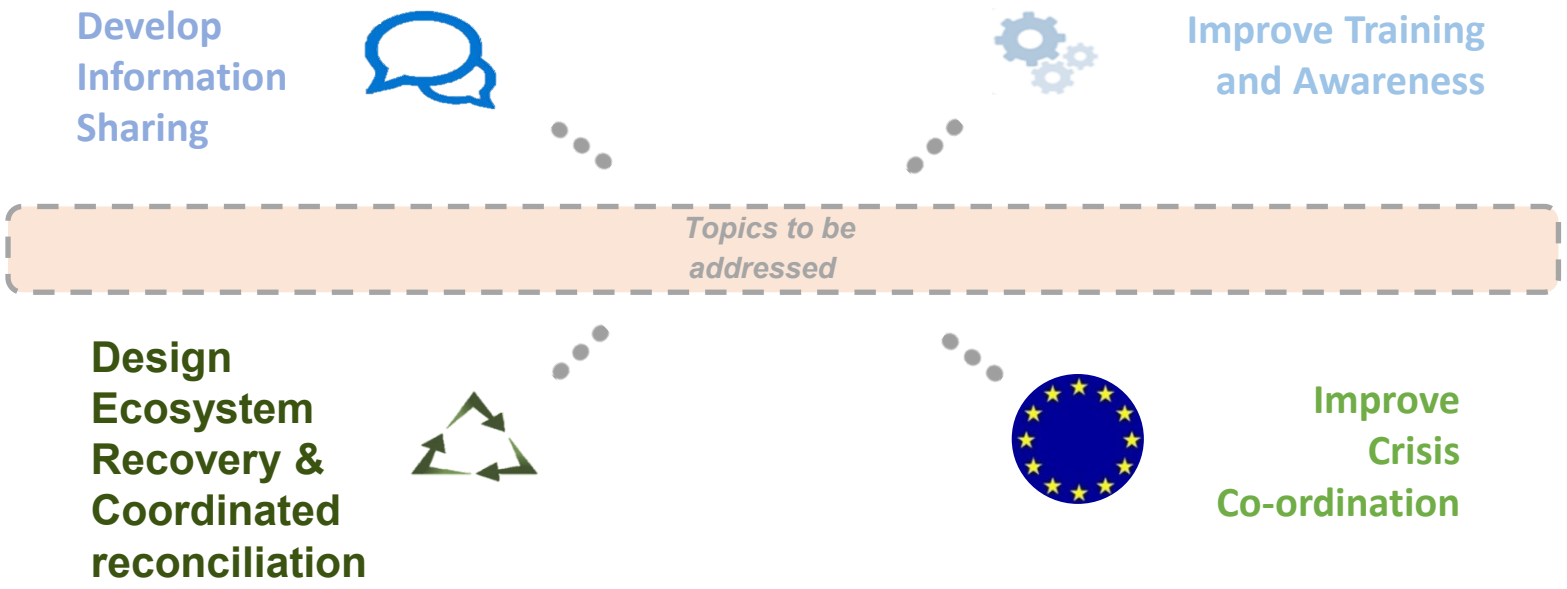
1. How has the role of the overseer changed due to the fact that multiple institutions are affected?
2. Do you have communication protocols and channels in place to liaise with all the relevant regulators (at a European and International level), including banking supervisors, law enforcement agencies, etc?

Wrap-up and conclusion on the key lessons, outcome & follow-ups

Questions:

1. In all the phases outlined above, how can we work collectively together to address the scenarios?
2. Are there are any gaps that we have identified, which we should address collectively?

Interesting conclusions from this exercise…



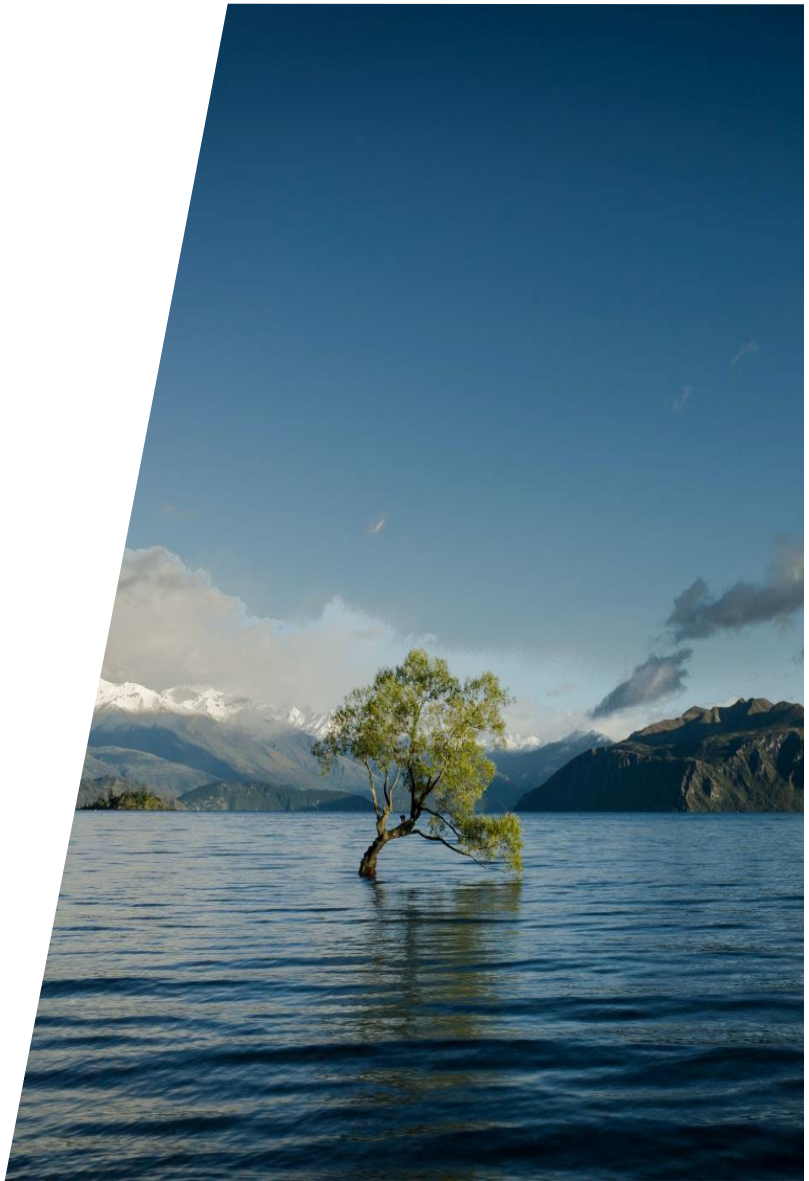
Red team testing or TLPT

Threat Intelligence led Red teaming or penetration testing shows if the threat actor, that is likely to target you, **can**

- **bypass your defensive measures**
- and if so **will they be detected by you?**
- and **what is your response** to this**?**

Why?

- (Financial) organizations struggle to become cyber resilient.
- Cyber threat landscape is evolving, organizations need to evolve accordingly.
- Preferably get ‘ahead of the curve’.
- Organizations need to be tested, matching the threats they actually face.
- Multi-national organizations operate in different jurisdictions and fall under different authorities.



The stakeholders

The Referees:

The authorities/supervisors/regulators

The TI and RT providers who do the reconnaissance and execute the attack

The people in the entity being attacked and responsible for reacting to the attack. They don't know that it is a CEBST/TIBER/CORIE test

The team that know it is a test and are responsible for managing the process and ensure a safe and controlled test. They liaise with the providers and the 'referees'

The Kill Chain...an example of an attack process

Reconnaissance is focused on collecting as much information as possible about the target. Reconnaissance is one of the most critical steps, and it is usually possible to learn a great deal about the target's people, technology, surroundings and environment. This step may also involve building or acquiring specific tools for the engagement.

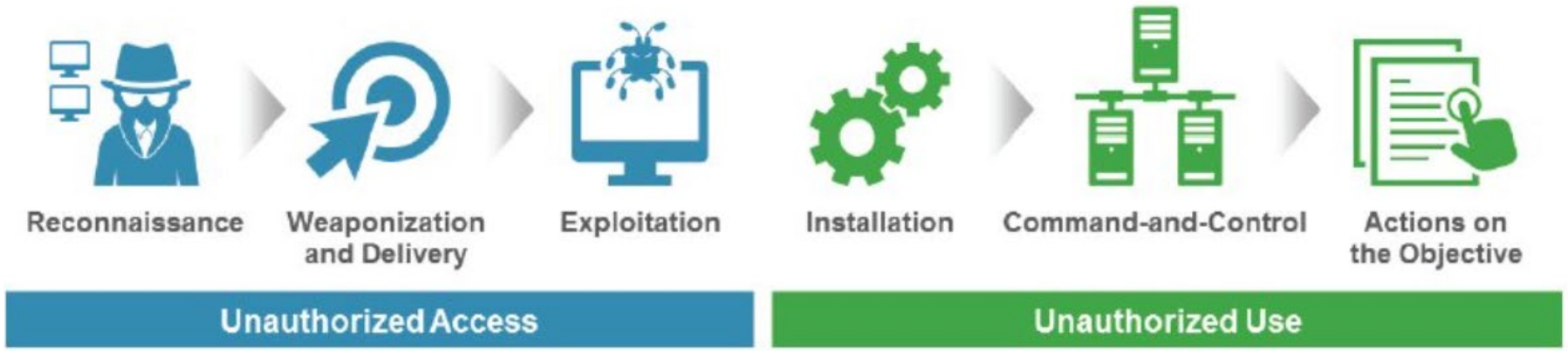
These phases involve analysing the information gathered about the infrastructure, facilities and employees. Attacker begins to form a picture of the target and its primary operations. Effective **weaponisation** involves preparation for the operations specific to the targets. **Delivery** marks the active launch of the full operation. The attacker begins to carry out the actions on the target(s) intended to reach the targets, such as social engineering, analysing cyber vulnerabilities, planting hardware trojans for remote network persistence, etc. One of the most important objectives is to identify the best opportunities for exploitation.

During **exploitation**, the attacker's goal is to "break in", i.e. to compromise servers/apps/networks and exploit target staff through social engineering. The exploitation stage paves the way for the installation and control & movement phase.

Attacker **installs** malware weapon to open an access point (e.g., "backdoor") which is usable for effective intrusion.

Once a successful compromise has been performed, attempts to move from initial compromised systems to further vulnerable or high value systems will be made. For example, this may consist of "hopping" between internal systems, continually reusing any increased access obtained in order to eventually compromise agreed target systems.

This entails gaining further access to compromised systems and acquiring access to target information and data. At this point, the attacker takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.



Simplified TIBER/CBEST/CORIE process

01

Generic threat landscape

Generic threat landscape is created and provided to the institutions. Foundational intelligence report for the entire sector and each test.

02

Scoping & Procurement

Critical functions are defined and approved by the board. Institution selects a threat intelligence and red teaming provider to execute the attack simulation.

03

Threat Intelligence & Red Teaming

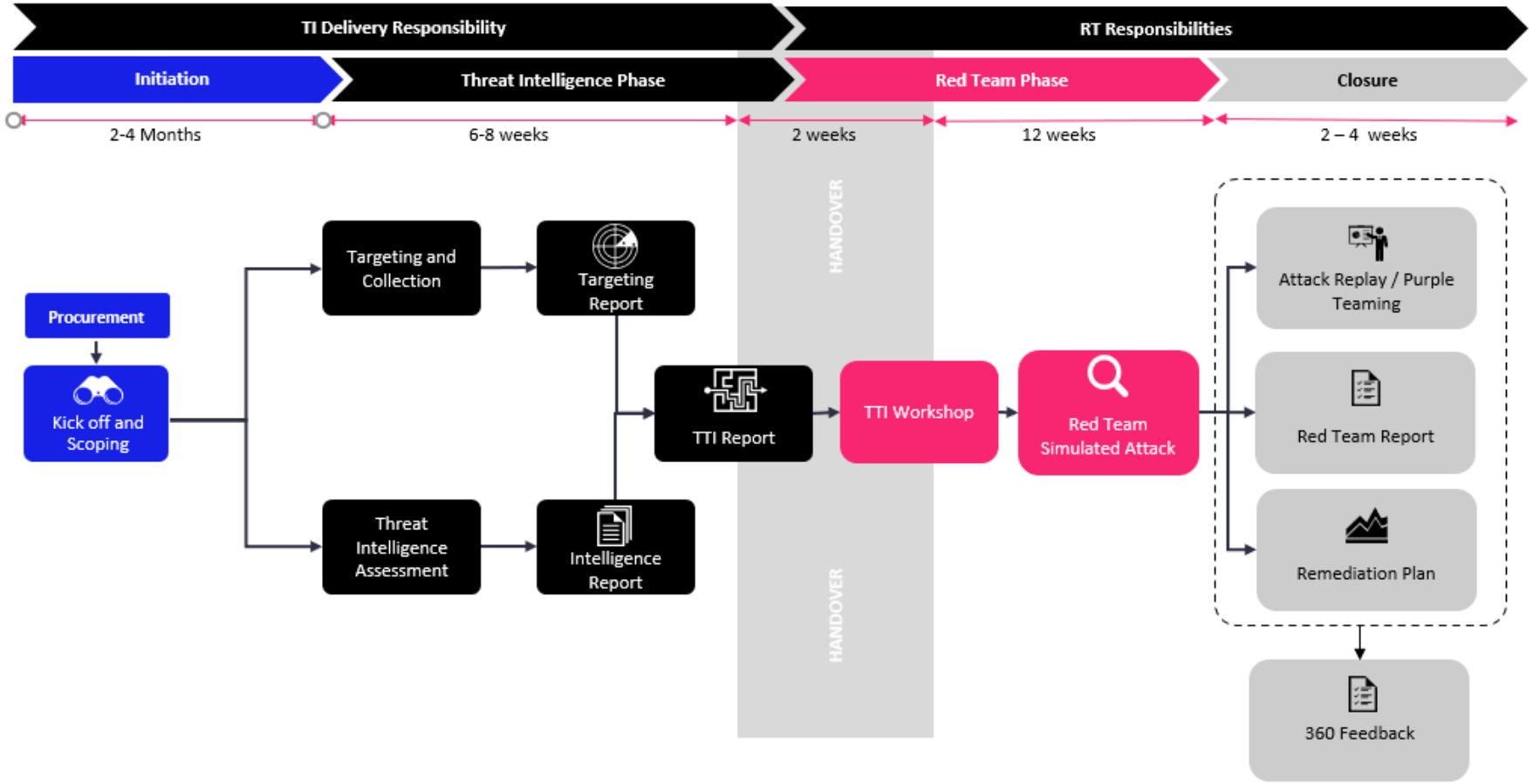
Execution is broken down into targeted threat intelligence and red teaming phases.

04

Purple Teaming & Remediation

Results are shared in multiple ways to different stakeholders: reporting and debrief and purple teaming sessions. Remediation plan is the final deliverable.

TIBER Approach Overview



Thank you!