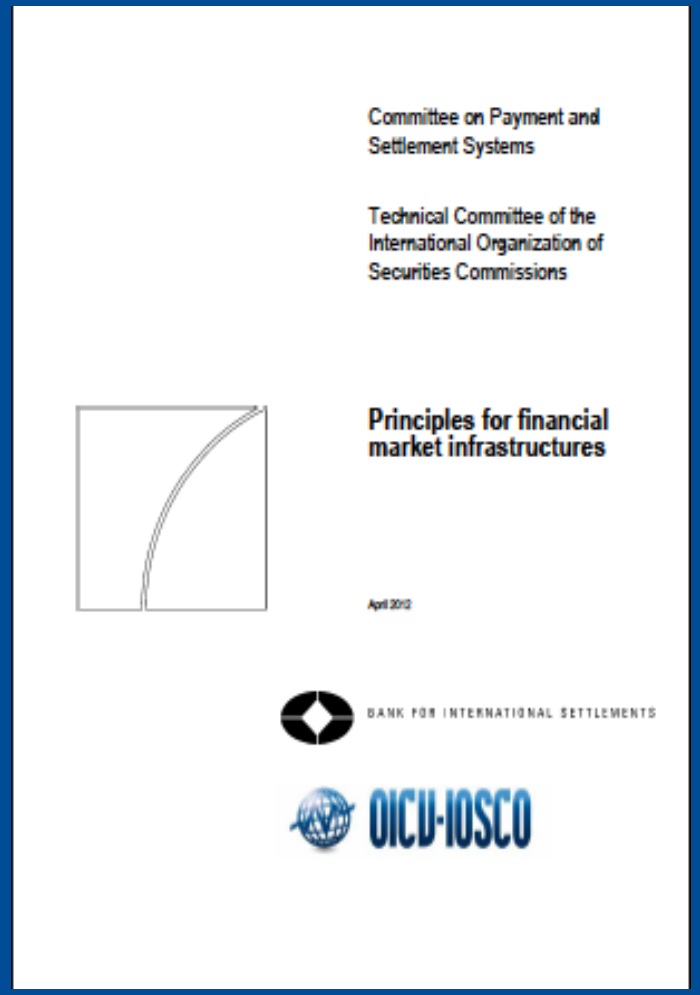


General business and operational risk management | Access | Efficiency

January 2024

Faith Stewart
IMF Short-term Expert

Organization of the principles

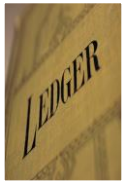
- The principles have been categorized into 9 broad categories that encompass the major elements critical to the safe and efficient design and operation of FMIs

General organization
Principle 1: Legal basis
Principle 2: Governance
Principle 3: Framework for the comprehensive management of risks

Credit and liquidity risk management
Principle 4: Credit risk
Principle 5: Collateral
Principle 6: Margin
Principle 7: Liquidity risk

Settlement
Principle 8: Settlement finality
Principle 9: Money settlements
Principle 10: Physical deliveries

CSDs and exchange-of-value settlement systems
Principle 11: CSDs
Principle 12: Exchange-of-value settlement systems



Default management
Principle 13: Participant-default rules and procedures
Principle 14: Segregation and portability

General business and operational risk management
Principle 15: General business risk
Principle 16: Custody and investment risks
Principle 17: Operational risk

Access
Principle 18: Access and participation requirements
Principle 19: Tiered participation
Principle 20: FMI links

Efficiency
Principle 21: Efficiency and effectiveness
Principle 22: Communication procedures and standards

Transparency
Principle 23: Disclosure of rules, key procedures, and market data
Principle 24: Disclosure of market data by TRs

Principle 15: General business risk

An FMI should identify, monitor and manage its general business risk and hold sufficient liquid net assets funded by equity to cover potential general business losses so that it can **continue operations and services as a going concern** if those losses materialise. Further, liquid net assets should at all times be sufficient to ensure a recovery or orderly wind-down of critical operations and services.

✓ PS	✓ CSD	✓ SSS	✓ CCP	✓ TR

Key requirements

1. Robust risk management and control systems
2. Liquid net assets funded by equity (such as common stock, retainec
3. A viable recovery or orderly wind-down plan
4. High quality and liquid net assets
5. A viable plan for raising additional equity

~ KC 2-5
CB-operated FMIs

Principle 16: Custody and investment risks

An FMI should safeguard its own and its participants' assets and minimise the risk of loss on, and delay in, access to these assets. An FMI's investments should be in instruments with minimal credit, market, and liquidity risks.

✓ PS	✓ CSD	✓ SSS	✓ CCP	x TR

Key requirements

1. Hold its own and its participants' assets at supervised and regulated entities
2. Prompt access to its assets and the assets provided by participants, when required
3. Evaluate and understand its exposures to its custodian banks
4. FMI's investment strategy should be consistent with its overall risk-management strategy and fully disclosed to its participants, and investments should be of high-quality

Principle 17: Operational risk

An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption.

✓ PS	✓ CSD	✓ SSS	✓ CCP	✓ TR

What is operational risk?

The risk that deficiencies in **information systems**, **processes** and **personnel [INTERNAL]**, or **disruptions** from **[EXTERNAL]** events will result in the reduction, deterioration, or breakdown of services provided by an FMI

Operational risk management requirements

Key Considerations
1. **Operational risk management framework**. An FMI should establish a **robust operational risk-management framework** with appropriate systems, policies, procedures, and controls to identify, monitor, and manage operational risks .
2. **Roles, responsibilities and testing**. An FMI's board of directors should **clearly define the roles and responsibilities for addressing operational risk** and should endorse the FMI's operational risk-management framework. Systems, operational policies, procedures, and controls should be reviewed, audited, and tested periodically and after significant changes.
3. **Operational reliability**. An FMI should have **clearly defined operational reliability objectives** and should have policies in place that are designed to achieve those objectives.
4. **Scalable capacity**. An FMI should ensure that it has **scalable capacity adequate to handle increasing stress volumes** and to achieve its service-level objectives.
5. **Physical and information security**. An FMI should have **comprehensive physical and information security policies** that address all potential vulnerabilities and threats.
6. **Business continuity**. An FMI should have a **business continuity plan** that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The plan should incorporate the use of a secondary site and should be designed to ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events. The plan should be designed to enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances. The FMI should regularly test these arrangements..
7. **Interdependencies**. An FMI should identify, **monitor, and manage the (interdependency) risks** that key participants, other FMIs, and service and utility providers might pose to its operations. In addition, an FMI should identify, monitor, and manage the risks its operations might pose to other FMIs.

KC1 – Operational risk management framework

KC1 – An FMI should establish a **robust operational risk-management framework** with ***appropriate systems, policies, procedures, and controls*** to identify, monitor, and manage operational risks.

Operational risk management framework....

Key points to consider:

- ❑ Policies typically detail the sources of operational risk and categorise these risks on a more granular basis (e.g. use of Risk Register)
- ❑ ORM typically sits within the wider Enterprise Risk Management framework
- ❑ ORM spread across ***three lines of defense***
- ❑ ***ORMF*** should include formal change management and project management processes (initiate/approve/track/test/implement changes)
- ❑ Use of standards (international, national, industry level)

Personnel practices are key!

- Use employees, not temporary staff as far as possible
- Screen prospective employees
- Change assignments periodically
- Separate duties and have dual control
- Know Your Customers… and employees
- Change passwords, user IDs, often
- Don’t retain staff in sensitive operations jobs who have relatives in other sensitive areas such as programming or computer operations

KC2 – Role of the Board of Directors

KC2 – An *FMI's* ***board of directors*** *should clearly* ***define*** *the roles and responsibilities for addressing operational risk* and should **endorse** the FMI's operational risk-management framework. Systems, *operational policies, procedures, and controls should be reviewed, audited, and tested* periodically and after significant changes.

Key points to consider:

- ❑ Clear governance and approval processes – consistent with P2
- ❑ Buck stops with the Board
- ❑ Policies, procedures, and controls should be reviewed, audited, and tested **periodically** and after significant changes or a major incident
- ❑ Internal and external audit roles
- ❑ Review, audit and testing

KC3 – Operational reliability

KC3 – An FMI should have ***clearly defined operational reliability objectives*** and should have ***policies and procedures in place*** that are designed to achieve those objectives.

Key points to consider

- ***Performance objectives*** (availability, i.e. uptime; throughput (rate of message delivery, how many transactions per unit of time); *recovery time objectives; recovery point objectives)*
  - Formally stated in Participant Agreements or System Rules
- **Committed service-level targets**, e.g. processing speed, timing of funds availability
- Policies and procedures to be aligned with objectives
- Monitor **performance and assess** whether the system is meeting its objectives
  - Report performance regularly to senior management, relevant board committees, participants, and authorities
  - Incident management procedures (recording, reporting, analyzing, solving, root cause identification, escalation, etc.)
- Review operational objectives periodically to incorporate new technological and business developments

KC 4 – Scalable capacity

KC4 - An FMI should ensure that it has ***scalable capacity adequate to handle increasing stress volumes*** **and to achieve its service-level objectives.**

Key points to consider:

- ❑ Capacity constraints should not compromise achievement of service-level objectives (e.g. processing speed)
- ❑ Forecast demand based on plausible changes in business volumes (may be due to new participants, increased activity levels) or technical requirements
- ❑ Stress volumes (market stress, new services); impact on processing times
- ❑ Monitor, review, and test actual capacity and performance on an ongoing basis
- ❑ Evaluate off-the-shelf solutions [role of the vendor, SLA, regular upgrades?]
- ❑ How quickly and cost effectively can upgrades be implemented?
- ❑ Scalability - not a major issue for most modern systems built with open architectures and significant levels of redundancy

KC 5 – Physical and information security

KC5 – An FMI should have ***comprehensive physical and information security policies*** that address all potential ***vulnerabilities and threats***.

Physical and information security

Physical security

- Comprehensive policies to address vulnerabilities and threats
- Assess and mitigate vulnerabilities on physical sites from (terror) attacks, intrusions, natural disasters
- Limit access to sensitive locations, systems and data (e.g. through access controls, device locks, system time-out for inactivity)
  - Access should be limited to authorized personnel only
  - Employees should wear picture badge at all times
  - Visitors should wear guest passes and be accompanied by an employee escort at all times
- Safe and secure storage

Physical and information security

Information security

- Protect data from loss, leakage, unauthorized access, fraud
- Avoid data corruption – file accountability, file balancing
  - Maintain duplicate (back-up) records
  - Maintain audit trails of transaction life cycle, change to data
  - Encryption, authentication
- IS objectives and policies should conform to commercially reasonable standards for confidentiality, authentication, integrity, authorization, non-repudiation, availability and auditability

Simple security precautions

- Maintain FMI on separate, dedicated network (VPN)
- Intrusion and malware monitoring; should include linked (feeder) systems such as Central Bank's GL or CBS
- Control use of Central Bank email
- Close off USB ports on machines connected to the FMIs
- Use secure methods for updating anti-virus software; do regular updates
- Control access to locations where FMIs are run (operations, administration and technology)
- Screen staff who have access, and segregate admin, security and payment users
- Remove root passwords (applicable to databases and operating systems)and enforce password policy
- Configure (and periodically re-set) security settings on databases and operating software
- Do daily backups and maintain backups and archived data securely

KC 6 – Business continuity management

KC6 – An FMI should have a ***business continuity plan*** that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The plan should ***incorporate the use of a secondary site and should be designed to ensure that critical information technology (IT) systems can resume operations within 2 hours following disruptive events***. The plan should be designed to enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances. The FMI should regularly test these arrangements.

- What are the BCP arrangements for the FMI?
- How were they assessed to ensure that they fully cover the key activities?
  - How long do they take to invoke?
  - How was the timing assessed? Does it cover the needs of the market, RTO?
  - How do you address communication requirements, internal and external?
  - What about testing, including with participants? CSPs?
  - Does the vendor play a role? Is this addressed in the SLA?

Business continuity management

BCP should have clearly stated **objectives**, **policies** and **procedures** for the rapid recovery and timely resumption of critical operations following a disruption

Both internal and external threats should be considered in a BCP

BCP to identify and address events that pose a significant risk of disrupting operations and ensure that the FMI continues to meet agreed service levels:

- Resume operations within two hours following disruptive events;, backup systems ideally should commence processing immediately
- The plan should enable the FMI to complete settlement by the end of the day even in extreme circumstances
- Contingency plans should ensure that the status of all transactions at the time of the disruption can be identified with certainty in a timely manner

Responsibility for BCP should be clearly assigned and adequate resources should be dedicated.

Business continuity management

Alternate (secondary) site

Requires sufficient (technical) resources, capabilities, and functionalities

Requires adequate staffing

Secondary site must be equipped to take over operations with minimal delay

- secondary site should provide the level of critical services necessary to perform the functions consistent with the **recovery time objective**
- should be located at a geographical distance from the primary site that gives it a distinct risk profile
- the need for a third site should be assessed
- alternative arrangements should be considered (for example, manual paper-based procedures) to allow for the processing of time-critical transactions in extreme circumstances

Business continuity management

Components

- Clearly defined procedures for crisis and event management
- Rapid deployment of a multi-skilled crisis and event-management team
- Procedures to consult and inform stakeholders quickly
- Communication with regulators, supervisors, and overseers
- Communication with local civil authorities (for physical attacks or natural disasters) or computer experts (for software malfunctions or cyber-attacks) or vendor (SLA)
- FMI with global importance or critical linkages to one or more interdependent FMIs, should set up, test, and review appropriate cross-system or cross-border crisis-management arrangements

Business continuity management

Testing

BCP should be subject to periodic review and testing

Tests should address various scenarios that simulate wide-scale disasters and inter-site switchovers

FMI's employees should be thoroughly trained to execute the BCP

Participants, critical service providers, and linked FMIs should be regularly involved in the testing of the BCP as appropriate

FMI should also consider the need to participate in industry-wide tests

An FMI should make appropriate adjustments to its BCP based on the results of the testing exercises

May commission penetration tests

Recovery and resumption objectives

Principle 17 versus Sound Practices

Requirement	Principle 17	Sound Practices
*Resumption of **FMI operations***		
Target	**2 hours** *An FMI should aim to be able to resume operations within two hours following disruptive events*	**2 hours** *…overall goal of achieving recovery and resumption [of clearing and settlement activities] within two hours after an event*
Requirement	**End of day** *The [business continuity] plan should enable the FMI to complete settlement by the end of the day even in case of extreme circumstances*	**Within business day** *…recover and resume clearing and settlement activities within the business day on which the disruption occurs*
*Recovery of **participant operations***		
Target	**No requirement** *Critical participants may need to meet some of the same operational risk-management requirements as the FMI itself*	**4 hours** *Firms that play significant roles … should strive to achieve a four-hour recovery time capability for clearing and settlement activities*
Requirement	**No requirement** *To manage operational risks associated with participants, an FMI should consider establishing minimum operational requirements for its participants*	**Within business day** *… firms that play significant roles in critical financial markets should plan to recovery clearing and settlement activities … within the business day on which a disruption occurs*

KC 7 - Interdependencies

KC7 – An FMI should ***identify, monitor, and manage*** the ***risks that key participants, other FMIs, and service and utility providers might pose to its operations***. In addition, an FMI should identify, monitor, and manage the risks ***its operations might pose to other FMIs***.

Key points:

- ❑ Risks to the FMI's own operations (from key participants, other FMIs, and service and utility providers)
- ❑ Outsourcing arrangements and critical service providers (see Annex F); the outsourcing provider should be held to the same standards
- ❑ Risks posed to other FMIs (BCP coordination with other interdependent FMIs)

Interdependencies

Systems, service providers, utility providers, critical participants

Where FMI is connected to other FMIs

- identify the effects on its ability to operate and to manage risks that stem from external operational failures of connected entities (including participants that may participate in other FMIs)
- identify, monitor, and manage the risks it faces from and poses to other FMIs
- to the extent possible, interdependent FMIs should coordinate business continuity arrangements and tests
- consider risks associated with service and utility providers

Establish minimum operational requirements for participants

- define operational and business continuity requirements for participants
- identify critical participants
- determine criteria critical participants must meet to ensure their operational risks are managed appropriately

Requirements for Critical Service Providers

What is a CSP? A service provider that has a ***direct contractual arrangement*** with an FMI to provide, on a ***continuous basis***, services to that FMI (and potentially its participants) which are ***essential for ensuring information confidentiality, integrity and service availability***, as well as the **smooth functioning of its core operations**

- Outsourced services may include data centers, financial messaging/network services, payment processing services, settlement functionality, or other business applications related to payment/clearing/settlement services
- Services should meet the same requirements as if provided internally
- Robust arrangements should be in place for the **selection**, **use** and **substitution** of CSPs and formal agreements should be instituted (FMI/CSP)

FMI should **disclose** the nature and scope of this dependency to participants

Direct/Indirect oversight: Overseer may have either a direct relationship with CSP or require FMI to obtain confirmation of adherence

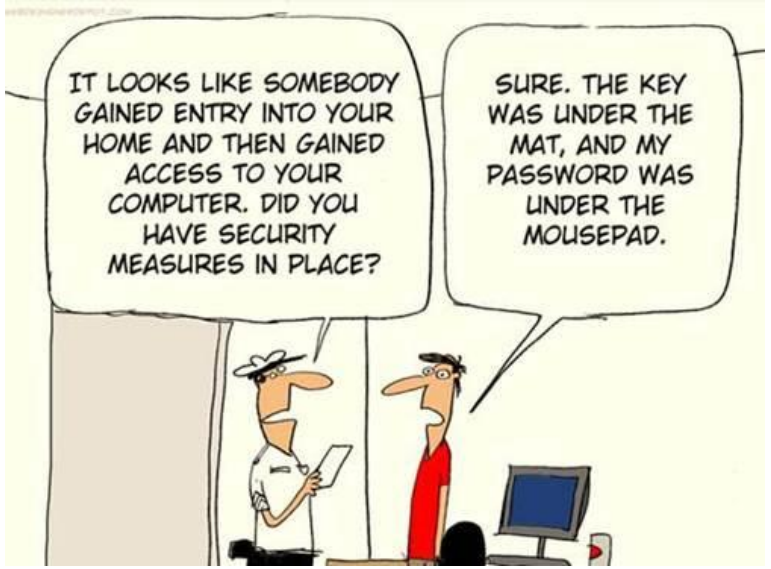
Oversight Expectations for Critical Service Providers – Annex F

Authorities may establish expectations specifically targeted at critical service providers, such as:

- Have effective processes and systems for identifying and managing risks
- Have a robust information security framework that manages information security risks
- Have robust, reliable, and resilient operations that meet or exceed the needs of the FMI
- Have effective technology planning that minimizes overall operational risk and enhances operational performance
- Be transparent to users and provide sufficient information to enable them to have a clear understanding of their risks

To conclude….

- …….Managing risk means knowing what the risks are and making a determined effort to reduce risks you can control and manage risks you can't ….
- Much is common sense, but often the urgent crowds out the important and gaps remain



Questions to consider

- Is the two-hour recovery window a “hard” or “soft” requirement?
- What type of “alternative arrangements” should an FMI consider to process time-critical transactions in extreme but plausible market conditions? (3.17.15)
- Are FMIs expected to maintain a third site?
- Why is the location of the secondary site of importance?

Further reading on operational risk

Operational Resilience in Digital Payments: Experiences and Issues (imf.org)

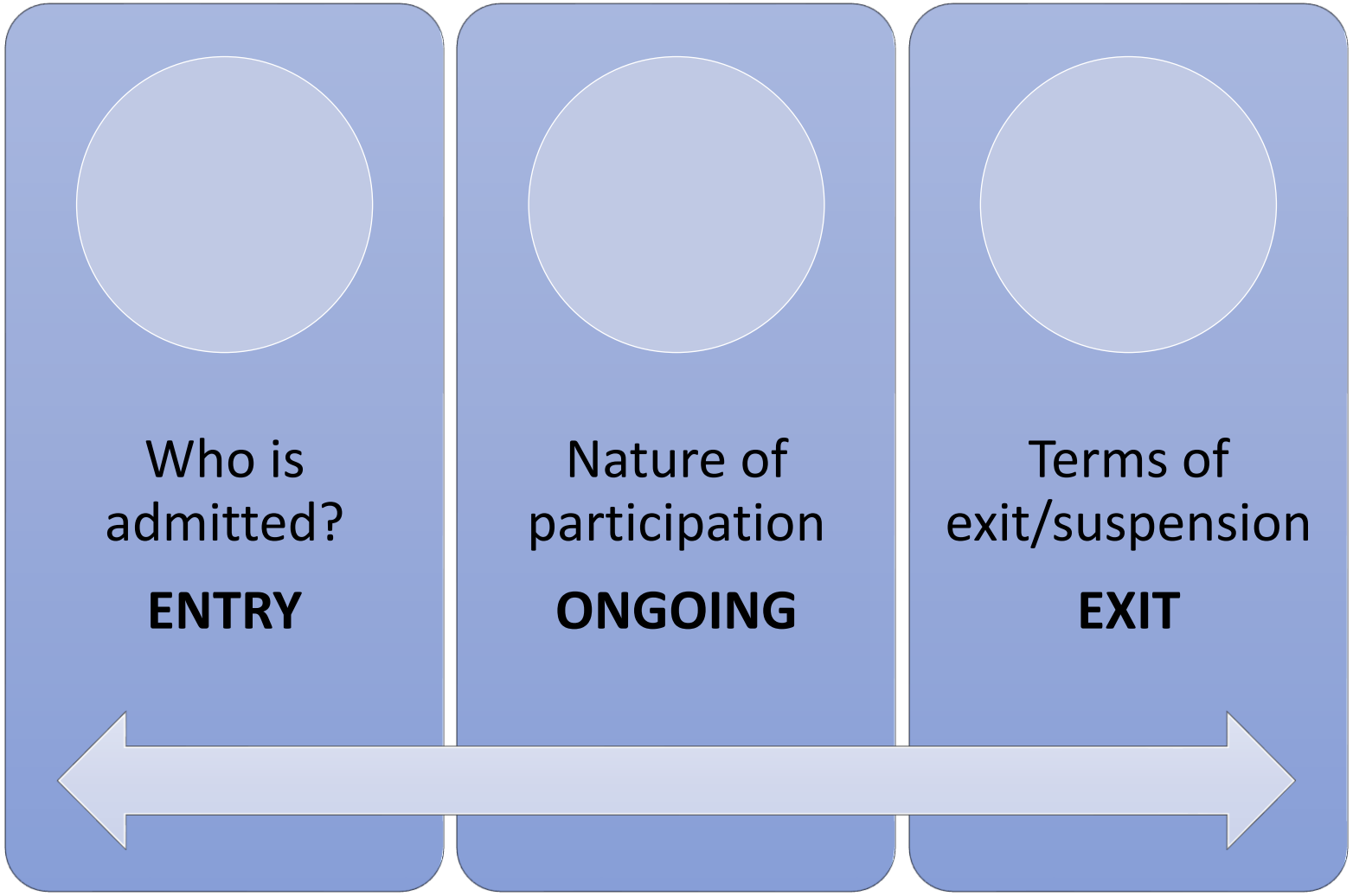
Principles for operational resilience (bis.org)

Principle 18: Access and participation

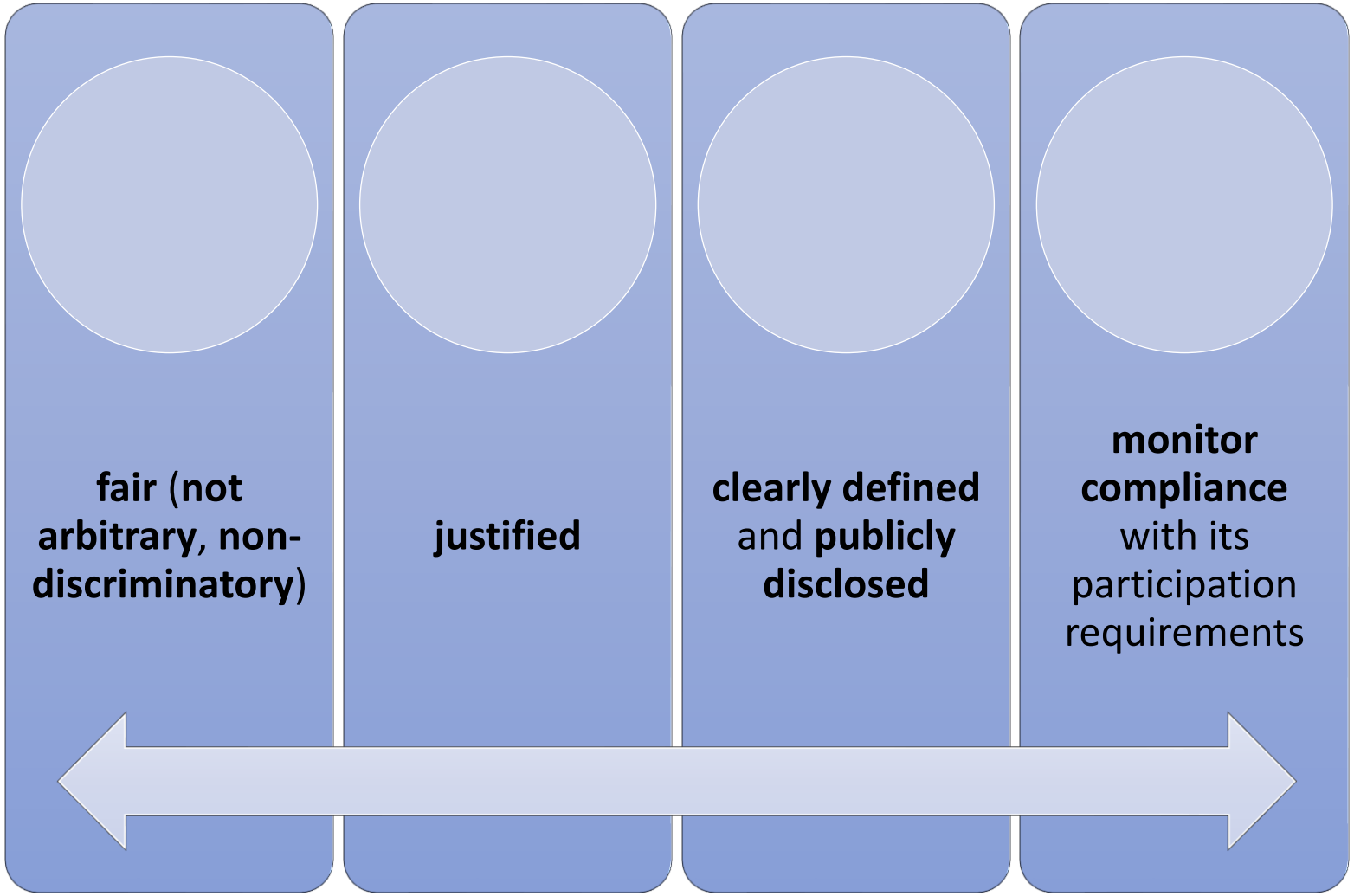
An FMI should have objective, risk-based, and publicly disclosed criteria for participation, which permit **fair** and **open access**.

✓PS	✓CSD	✓SSS	✓CCP	✓TR

What does ‘participation’ entail?



Governance arrangements should provide for fair, open, risk-based access



Risk-based criteria include…

- Operational capacity, e.g. IT capability
- Risk management expertise/competence
- Financial resources, e.g. risk-related capital requirements, contributions to prefunded default arrangements, and appropriate indicators of creditworthiness
- Legal powers/authorisations
    - Legal or policy constraints (e.g. RTGS access may be constrained by law, requiring the inclusion/exclusion of certain financial institutions)
    - Conflict-of-laws issues if participant is a foreign entity

Expand access through graduated requirements

To reduce concentration risk

Direct (full)

Direct (partial)

Indirect

Monitoring

- FMI should monitor compliance with its participation requirements on an ongoing basis

Key points to consider:

- ❑ Need for timely and accurate information
- ❑ Participants should be **obligated** to provide this information
- ❑ FMI must take action if participant is deemed to pose heightened risk
- ❑ Additional reporting requirements for non-regulated institutions
- ❑ Monitoring may also extend to indirect participants…

Questions to ponder

- **Should non-bank PSPs have access to central bank settlement accounts?**

Does this require:

- A lowering of standards? or
- Increasing standards by making a money transmitter or other PSP subject to prudential supervision and banking rules?

What are the benefits of expanded access?

Principle 19: Tiered participation

An FMI should **identify**, **monitor**, and **manage** the material risks to the FMI arising from tiered participation arrangements.

✓PS	✓CSD	✓SSS	✓CCP	✓TR

Principle 19 – Tiered participation

Key points to consider:

- ❑ Tiered participation arrangements create credit and liquidity exposures between direct and indirect participants and can concentrate risk
- ❑ DP, **not FMI** is required to manage these risks
- ❑ These risk concentrations may also affect the FMI
- ❑ FMI requires information that allows it to identify and monitor (if necessary) IPs responsible for a significant %age of FMI's transactions
- ❑ Establish objective thresholds above which direct participation (of the IP) would be encouraged/required
- ❑ FMI must ensure the participation rules are supportive of the risk management requirements

Principle 20: FMI Links

An FMI that establishes a link with one or more FMIs should identify, monitor, and manage link-related risks.

x PS	✓ CSD	✓ SSS	✓ CCP	✓ TR

A link is a set of contractual and operational arrangements between two or more FMIs that connect the FMIs directly or through an intermediary. An FMI may establish a link with a similar type of FMI for the primary purpose of expanding its services to additional financial instruments, markets, or institutions

This principle covers links between CSDs, CCPs, and TRs, as well as CSD-CCP links and links between TRs and other FMIs

Links to payment systems are addressed in P9 – Money settlements

Principle 21: Efficiency

An FMI should be **efficient** and **effective** in meeting the requirements of its participants and the markets it serves..

✓PS	✓CSD	✓SSS	✓CCP	✓ TR

- "***Efficiency***" refers generally to the resources required by the FMI to perform its functions (what the FMI does, how it does it), while "***effectiveness***" refers to whether the FMI is meeting its intended goals and objectives.
- **Efficiency is determined by:**
  - Clearing and settlement arrangements:
    - gross, net, or hybrid settlement;
    - real time or batch processing;
  - Use of technology and procedures (for example, communication procedures and standards)
  - Cost to participants and customers
  - Flexibility to respond to changing demand and new technologies
  - Flexibility to integrate with new (and other) technologies

Key highlights in efficiency

- Consider practicality and costs for users and customers
  - An FMI's efficiency will ultimately affect the use of the FMI by its participants and their customers as well as these entities' ability to conduct robust risk management, which may affect the broader efficiency of financial markets
- Efficiency also involves cost control (direct, e.g. transaction processing; and indirect, e.g. administrative)
  - A review of an FMI's efficiency or cost-effectiveness could include an evaluation of both the productivity of operational processes and the relative benefits of the processing method given the corresponding costs.*
- FMI should review its efficiency regularly, including cost and pricing structure
- Competition – an important mechanism for promoting efficiency
- Where economies of scale and scope impede competition, relevant authorities may have a responsibility to review the costs imposed on the FMI's participants and the markets it serves
- Both private and central bank operators of FMIs should make use of market disciplines, as appropriate, to promote efficiency in the FMI's operations.
  - For example, an FMI could use competitive tendering to select service providers

Key highlights in effectiveness

- An FMI's effectiveness may also involve meeting service and security requirements.
- To facilitate assessments of effectiveness, an FMI should have clearly defined goals and objectives that are **measurable** and **achievable**. E.g.
  - Minimum service-level targets (such as the time it takes to process a transaction)
  - Risk-management expectations (such as the level of financial resources it should hold), and
  - Business priorities (such as the development of new services).
- An FMI should establish mechanisms for the regular review of its effectiveness, such as periodic measurement of its progress against its goals and objectives
  - One mechanism an FMI might use to gauge its success in meeting the needs of its participants and the markets it serves are periodic satisfaction surveys of its participants and other relevant institutions in the market

Questions to consider

- How can the FMI determine whether the safety and efficiency objectives are being achieved?

- In what circumstances would the authorities have a role in reviewing the FMI's pricing structure for its services?

- Is an analysis of the number of transactions that could be processed in a given period or measuring the processing cost per transaction part of an efficiency review?

Principle 22 Communication procedures and standards

An FMI should use, or at a minimum accommodate, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, settlement, and recording.

✓PS	✓CSD	✓SSS	✓CCP	✓TR

- **Purpose:** An FMI's adoption of internationally accepted communication procedures and standards for its core functions can facilitate the elimination of manual intervention in clearing and settlement processing, reduce risks and transaction costs, improve efficiency, and reduce barriers to entry into a market.

- **Point to note:**
  - An FMI is encouraged but not required to use or accommodate internationally accepted communication procedures and standards for purely domestic transactions.

Principle 22: Communication procedures and standards

- **Key requirements:**
  - Standardized communication procedures (or protocols) provide a common set of rules across systems for exchanging messages. They can:
    - Reduce the need for intervention and technical complexity when processing transactions can help to reduce the number of errors, avoid information losses, and ultimately reduce the resources needed for data processing by the FMI, its participants, and markets generally
    - Facilitate interoperability between the information systems or operating platforms of FMIs in different jurisdictions, which allows market participants to obtain access to multiple FMIs without facing technical hurdles (such as having to implement or support multiple local networks with different characteristics)
  - Standardized messaging formats and reference data standards for identifying financial instruments and counterparties will generally improve the quality and efficiency of the clearing and settlement of financial transactions.
    - Alternatively use or accommodate systems that translate or convert data from international standards into the domestic equivalent and vice versa

Questions to consider

- Is an FMI that operates solely in the domestic market required to use internationally accepted communication standards?
- What are the alternatives to a domestic FMI using internationally accepted communication standards?
- How does the use of these standards enhance FMI efficiency?

Questions and discussion?

Thanks!