

Digital Trust NewsFlash

August 2025 / No. 10

**PADG No. 14/2025 on
Second Amendment to
PADG No. 17/ 2023
Concerning the
Implementation of BI-
FAST Payment^{P1}**

Key takeaways^{P5}

PADG No. 14/2025 on Second Amendment to PADG No. 17/2023 Concerning the Implementation of Bank Indonesia (BI)-FAST Payment

On 30 June 2025, Bank Indonesia has issued *Peraturan Anggota Dewan Gubernur* (PADG) No. 14/ 2025, the second amendment to PADG No. 17/ 2023 on BI-FAST Implementation. Previously, Bank Indonesia released the first amendment, PADG No. 1/2025, which focused primarily on proactive risk management and fraud management systems. PADG No. 17/ 2023 significantly enhances transaction security and cyber resilience within the BI-FAST ecosystem.

Driven by the increasing volume and complexity of BI-FAST transactions, this amendment reinforces Bank Indonesia's commitment to strengthening security across people, processes and technology for both the BI-FAST Operator (Bank Indonesia) and Participants (e.g. conventional and Islamic commercial banks, foreign bank branches in Indonesia and others) ensuring adherence to the latest risk dynamics, cyber resilience and information system security standards.

Key amendments overview

There are some amendments based on PADG No. 14/ 2025 in several key areas, including:

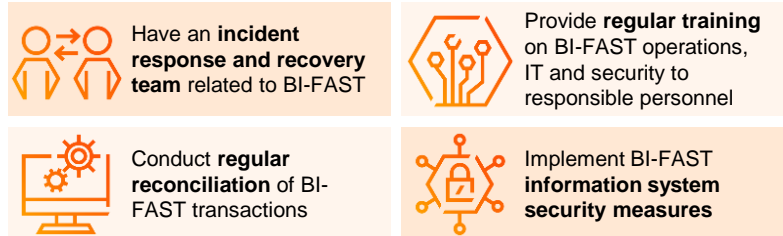
BI-FAST process	Operational processes, handling of invalid transactions, correspondence channels updates.
Policy or procedure	The scope of BI-FAST's internal control policy and information technology-related policies.
Information system audit and security testing	Requirements for information system security testing including the selection of an auditor, frequency, reporting.
Infrastructure	Responsibilities for ensuring the security and smooth operation of BI-FAST, requirements for third parties managing the BI-FAST infrastructure, fraud management.
Incident handling	Roles and responsibilities of the incident response and recovery team, cyber incident handling process.

Detailed key changes

Based on the aforementioned key amendments, the following is a summary of detailed changes:

1. BI-FAST process

- To ensure smooth and secure use of BI-FAST, Participants must:



- BI-FAST transaction reconciliation** is carried out periodically, **once or more per day**, depending on the Participant's risk appetite by comparing the transaction on core banking with the member statement.
- In a case of a change in operational hours by the Operator, Participants should be informed through an administrative message and/or other means.

2. Policy and procedure

- BI-FAST policy and procedure**, which should be developed **no later than six months after the effective date of participation in BI-FAST**, must at the minimum comprise the following:
 - BI-FAST operational organisation, operational provisions and procedures (including information technology, infrastructure, liquidity management and security), and operational supervision.
 - Handling of abnormal and emergency situations and cyber incidents.
 - Customer protection throughout and outside BI-FAST operational hours at the Participant.
- Information technology (IT) policy** must be updated **no later than six months after the change in the information technology policy** and shall at the minimum include:
 - compliance with Bank Indonesia's security and cyber resilience standards.
 - IT governance aligned with global cybersecurity framework guidelines.

3. Information system (IS) audit and security testing

- IS audit and security testing must be carried out **at the minimum once every year**.
- Security testing must be conducted by an **external security auditor** who is **registered with the relevant authority or Self-Regulatory Organisation (SRO)**.
- IS audit and security testing must be submitted to the Operator **no later than the deadline for submitting the compliance assessment report (LHPK)**.
- In a case where there are plans for a new implementation and/or changes within internal IS related to BI-FAST, an IS audit and security testing **must be performed prior to the new implementation and/or changes**. Findings must be "closed" by the auditor before proceeding. The result must be submitted **no later than ten (10) working days after the completion of the IS audit and/or security testing**.

- The IS audit and security testing scope should at the minimum cover:

Material in the minimum technical requirements for BI-FAST information technology infrastructure

- Security of network segmentation and architecture
- Security of remote access and administration
- Configuration of inter-system connections
- Cryptography and key management
- Access control and authentication
- Updates, vulnerabilities and change management
- Logging and log monitoring
- Third-party security
- Physical and environmental security

The scope of the information system audit and security testing in guidelines for preparing written policies and procedures

- Governance (human resources and legal aspects)
- Environment (power supply, air conditioning, etc.)
- System (hardware, software, etc.)
- Fulfilment of Minimum Technical Requirements for BI-FAST Information Technology Infrastructure Protection
- Backup system (availability and function testing)
- Disaster recovery plan
- Data and documentation (data integrity, logbook, etc.)

4. Infrastructure

- Participants must implement BI-FAST information system security.** The implementation should at least cover:

IT infrastructure protection	Establish fraud management	Update and submit BI-FAST infrastructure diagrams to the Operator, including changes
Maintain an anomaly detection system	Monitor BI-FAST operations with an early warning system	Ensure risk management for BI-FAST and third-party connections

The implementation must be fulfilled no later than **1 January 2026**.

- To ensure **IT infrastructure protection**, Participants **should at a minimum cover areas mentioned in PADG No. 14/ 2025**, such as implement network segmentation and architectural security measures, secure access through Privileged Access Management (PAM) or a jump server, configure system connections using Transport Layer Security (TLS) protocols, create a user access matrix, conduct vulnerability scanning and penetration testing, etc.
- Participants **are fully responsible for security and smooth operation if a third party manages their infrastructure**, including:
 - monitor third-party performance
 - implement risk management
 - allow access for Operator inspections.

In addition, Bank Indonesia **may carry out direct inspections** of the third party managing the participant's BI-FAST. Participants **must ensure third parties meet security standards**, including protecting infrastructure, defining responsibilities and segmenting connectors to prevent access by other Participants, etc.
- Fraud Detection System (FDS) - A feature to detect transaction anomalies and mitigate the risk of suspicious financial activities.
 - Participants **must implement FDS at the account and transaction levels for outbound fund transfers** and may also implement for incoming fund transactions.
 - FDS is **rule-based, automatic** and **operates in near real-time or real-time** to identify transaction anomalies or suspicious financial transactions.

- In case a **fraud transaction is identified**, Participants must:

Provide initial information	30 (thirty) minutes after the fraud incident is confirmed by the Participant.
Submit report	No later than three (3) calendar days after the fraud incident is confirmed.
Consequences of failure to meet the obligations	<ul style="list-style-type: none"> • Receive an administrative sanction in the form of a written warning. • A downgrade in participation status (if Participants do not respond to the written warning within 30 (thirty) working days since the written warning is received).





- **If a transaction is deemed unauthorised and/or the customer's account is suspected to be a mule account**, the receiving participant may perform actions in accordance with laws and SRO guidelines such as, freezing or closing the account and/or returning funds to the sender.
- Data used for FDS rules implementation may include whitelist data, blacklist data and other data determined by the Operator.

5. Incident handling

- Incident response and recovery team has the **minimum roles and responsibilities in handling cyber incidents** to:
 - mitigate cyber incidents
 - restore BI-FAST services to normal conditions.
- In a case of a cyber incident,

Participants shall:	Operators shall:
Notify the Operator no later than one (1) hour after the occurrence of the cyber incident	Establish policies and procedures for handling Cyber Incidents , including temporarily suspend the Participant's BI-FAST services.
Have a stop button to halt the BI-FAST services in the event of transaction anomalies, fraud and/or a cyber incident.	Carried out temporary suspension for the Participant affected by the cyber incident and/or for other Participants at risk of experiencing a similar cyber incident.

- Further, BI-FAST services **may be temporarily terminated due to a cyber incident, a regulatory authority's request and/or an Operator's decision**. The Operator will inform Participants of necessary actions to address the incident, suspend BI-FAST operations and notify all Participants through administrative messages or other communication channels.
- To reopen BI-FAST access services, Participants must:

 Submit a request letter signed by a Director or an authorised official	 A declaration confirming completed security risk assessment and accountability for cyber incidents
 Provide assessment results on IT infrastructure compliance	 Obtain clearance confirmation from multitenancy provider and/or other parties managing the BI-FAST infrastructure

Key takeaways

Following the amendments, Participants should note several important updates:

1. Provide **regular training on BI-FAST** and conduct **regular reconciliation of BI-FAST transactions**.
2. **Revise internal policies and procedures** to meet new requirements.
3. **Conduct an information system audit and security testing** at the minimum once per year, ensuring adherence to the specified scope.
4. **Implement comprehensive information system security measures by 1 January 2026**, including IT infrastructure protections, fraud management including FDS, anomaly detection capabilities, etc. Ensure **timely notifications for identified fraudulent transactions**, according to established regulations.
5. **Participants must evaluate the providers who managed the BI-FAST infrastructure on behalf of the Participants** to meet the established security standard.
6. **Establish an incident response and recovery team related to BI-FAST**, tasked with mitigating cyber incidents, restoring services and ensuring timely notification as per regulatory guidelines.

For more information, please reach out to your PwC contacts below:



Subianto

Broader Assurance Services Leader
and Chief Digital and Technology
Officer
subianto.subianto@pwc.com



Melissa Gunarto

IT Audit and Governance Partner
melissa.g.gunarto@pwc.com



Andrew Tirtadjaja

Cybersecurity and Privacy Director
andrew.tirtadjaja@pwc.com



Salman Alfarisy

IT Governance Director
salman.alfarisy@pwc.com



Mila Ichwanto

IT Governance Senior Manager
mila.ichwanto@pwc.com



Ivan Kirsten

Cybersecurity and Privacy Manager
ivan.k.kirsten@pwc.com



Yudhi Ariyanto

Cybersecurity and Privacy Manager
yudhi.ariyanto@pwc.com



Dimas Kusuma

Cybersecurity and Privacy Manager
dimas.kusuma@pwc.com

www.pwc.com/id



PwC Indonesia



@PwC_Indonesia

This publication has been prepared for general guidance on matters of interest only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC Indonesia, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

The documents, or information obtained from PwC, must not be made available or copied, in whole or in part, to any other persons/parties without our prior written permission which we may, at our discretion, grant, withhold or grant subject to conditions (including conditions as to legal responsibility or absence thereof).

PwC Indonesia is comprised of KAP Rintis, Jumadi, Rianto & Rekan, PwC Tax Indonesia, PwC Legal Indonesia, PT Prima Wahana Caraka, PT PricewaterhouseCoopers Indonesia Advisory, and PT PricewaterhouseCoopers Consulting Indonesia, each of which is a separate legal entity and all of which together constitute the Indonesian member firms of the PwC global network, which is collectively referred to as PwC Indonesia.

© 2025 PwC. All rights reserved.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see <http://www.pwc.com/structure> for further details.