EXPOSURE DRAFT

Proposed Criteria for Controls Supporting Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens

June 12, 2025

Comments are requested by August 11, 2025

Prepared by the AICPA Assurance Services Executive Committee

Contents

Explanatory Memorandum

Introduction

As the digital asset space continues to evolve and new types of digital assets are created, it has become apparent that stakeholders, such as investors and regulators, need consistency, transparency, and trust in reports provided by the entities creating and issuing digital assets. Because controls surrounding digital asset operations are an integral part of, and a foundation for, the reliability of information presented by those entities, it is vital that those controls are implemented, operated, and monitored.

One type of digital asset is an asset-backed token. These tokens can be backed by various types of assets, such as fiat currency, commodities, or even other digital assets. Generally, asset-backed tokens include mechanisms designed to minimize price volatility by linking (or pegging) their values to the value of the asset backing them. In the case of a token backed by fiat currency (for example, the U.S. dollar), generally, the value of the token stays consistent with the value of that fiat currency, and therefore, because of the limited changes in value, these types of tokens are typically referred to as "stablecoins."

Once purchased, token holders have the right to redeem their tokens. Tokens are redeemed based on the method and timing established within the token issuer's terms of service, legal terms, user agreements, policies and procedures, and other relevant documents maintained by the token issuer (collectively referred to in this document as the token issuer's "terms"). In accordance with the terms, the token issuer typically holds a certain amount of assets to cover the number of tokens outstanding. Token issuers may be required by regulators to present and disclose information about the redeemable tokens outstanding and the availability of assets for redemption, in addition to designing and establishing suitable and effective controls supporting token operations (for example, token generation and management, redemption asset management, vendor management, and reporting).

Currently, no common framework exists for token issuers to evaluate the suitability of the design and operating effectiveness of controls supporting token operations or for practitioners to perform attestation engagements on this subject matter. This may result in incomplete and inconsistent controls implemented to achieve the control objectives of the token issuer and may lead to risks that all relevant control areas are not covered. In addition, it may create situations in which an attestation engagement performed by practitioners on controls does not cover all necessary control objectives.

A token issuer may face risks that threaten the ability to achieve the token issuer's objectives due to external and internal threats to the achievement of those objectives and the vulnerabilities of its systems, processes, and procedures. These risks are addressed through the implementation of suitably designed controls that, if operating effectively, provide reasonable assurance of achieving the token issuer's objectives.

Therefore, in connection with the *2025 Criteria for Stablecoin Reporting: Specific to Asset-Backed Fiat-Pegged Tokens*, the AICPA has identified a need for criteria to evaluate whether controls are suitably designed and operating effectively to achieve the control objectives of token operations, over a specified period of time. Part II of this document presents those criteria, in the form of control objectives, divided into the following control areas:

- Token generation and management
- Client onboarding and maintenance
- Customer transaction processing
- Key and backup management
- Redemption asset management
- Vendor management
- Reporting
- IT general controls

It is important for token issuers to identify the risks that threaten the achievement of any of the control objectives. These control objectives may inform the token issuer when designing, implementing, operating, and monitoring controls to provide reasonable assurance that those risks would not prevent the control objectives from being achieved. In addition, these control objectives may be used as criteria to evaluate and report on the suitability of the design and operating effectiveness of implemented controls in an attestation engagement.

The AICPA's Assurance Services Executive Committee (ASEC), in establishing and developing these criteria, is following due process procedures, including exposure of the criteria for public comment. BL section 360R, *Implementing Resolutions Under Section 3.6 Committees*,[1] designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA Council or the board of directors. Paragraph .A46 of AT-C section 105, *Concepts Common to All Attestation Engagements,*[2] indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered to be suitable.[3] Accordingly, these criteria are suitable criteria for evaluating the design and operating effectiveness of controls supporting token operations.

In addition to the criteria, accompanying implementation guidance is included and presents factors that may assist both the token issuer and the practitioner when they are evaluating whether controls were suitably designed and operating effectively to achieve the control objectives of token operations. The implementation guidance does not address all possible situations; therefore, users should carefully consider the facts and circumstances of the token issuer and its environment when applying the control objectives as criteria.

1 All BL sections can be found in AICPA *Professional Standards*.
2 All AT-C sections can be found in AICPA *Professional Standards*.
3 These criteria are designed to be used in conjunction with the token issuer's terms (that is, the token issuer's terms of service, legal terms, user agreements, policies and procedures, and any other relevant documents maintained by the token issuer that detail the legal agreement between the token issuer and the entities purchasing the tokens).

Guide for Respondents

Throughout this document, ***boldface italics*** denotes new language, and deleted text is shown in ~~**strikethrough**~~. ASEC is seeking comments specifically on the new language and deleted text within this document, as well as the nature and extent of proposed criteria and related implementation guidance in part II.

Note: ASEC is not seeking comments on the presentation and disclosure criteria in part I, which are included to provide context.

Specifically, please address the following questions:

1. Are any of the criteria or implementation guidance unnecessary or otherwise not relevant? Please provide a list and explain the rationale.
2. Are there any missing criteria or implementation guidance? Please provide a list and explain the rationale.
3. Do you believe these criteria meet the requirements in the attestation standards to be considered suitable?
4. Do you have any concerns about the measurability or level of detail of any of the criteria or implementation guidance? Please provide a list and explain the rationale.
5. Are there any concepts or terms that are provided within the introductory material, criteria, or the implementation guidance that you believe are technically inaccurate or you disagree with?
6. For SC10: *Controls provide reasonable assurance that physical access to computer and other resources relevant to token operations is restricted to authorized and appropriate personnel:*

   Removes Data and Software for Disposal: *Procedures are in place to remove, delete, or otherwise render data and software inaccessible from physical assets and other devices owned by the token issuer, its vendors, and employees when the data and software are no longer required on the asset or the asset will no longer be under the control of the token issuer.*

   - Does this implementation guidance provide relevant information, or does it create confusion?

Comments are most helpful when they refer to specific paragraphs or criterion numbers, include the reasons for the comments, and, when appropriate, make specific suggestions for any proposed changes to wording. If you agree with the proposals in the exposure draft, it will be helpful for the ASEC Stablecoin Controls Workstream to be made aware of this view, as well.

Written comments on the exposure draft should be sent to Di Krupica at StablecoinED@aicpa-cima.com and received by August 11, 2025.

Comment Period

The comment period for this exposure draft ends August 11, 2025.

Assurance Services Executive Committee (2024–2025)

Mary Grace Davenport, *Chair*
Jim Burton, *Immediate Past Chair*
Angela Appleby
Denny Ard
Dora Burzenski
Margaret Christ
Rich Davisson
Werner Erasmus
Bridgett Gyorfi
Khadja Johnson
Tina Kim

ASEC Digital Assets Attestation Subgroup: Stablecoin Controls Workstream

Jeff Trent, Chair
Dan Albanese
Noah Buxton
Michael Gonzales
Sara Krople
Bing Lin
Jeff Maffitt
Shelby Murphy
Jeremy Nau
Kyle Owens
Danh Pham
Virginia Salmuni
Jay Schulman
Kyle Sewell
Rebecca Thomas

AICPA Staff

Ami Beers
Senior Director
Assurance and Advisory Innovation

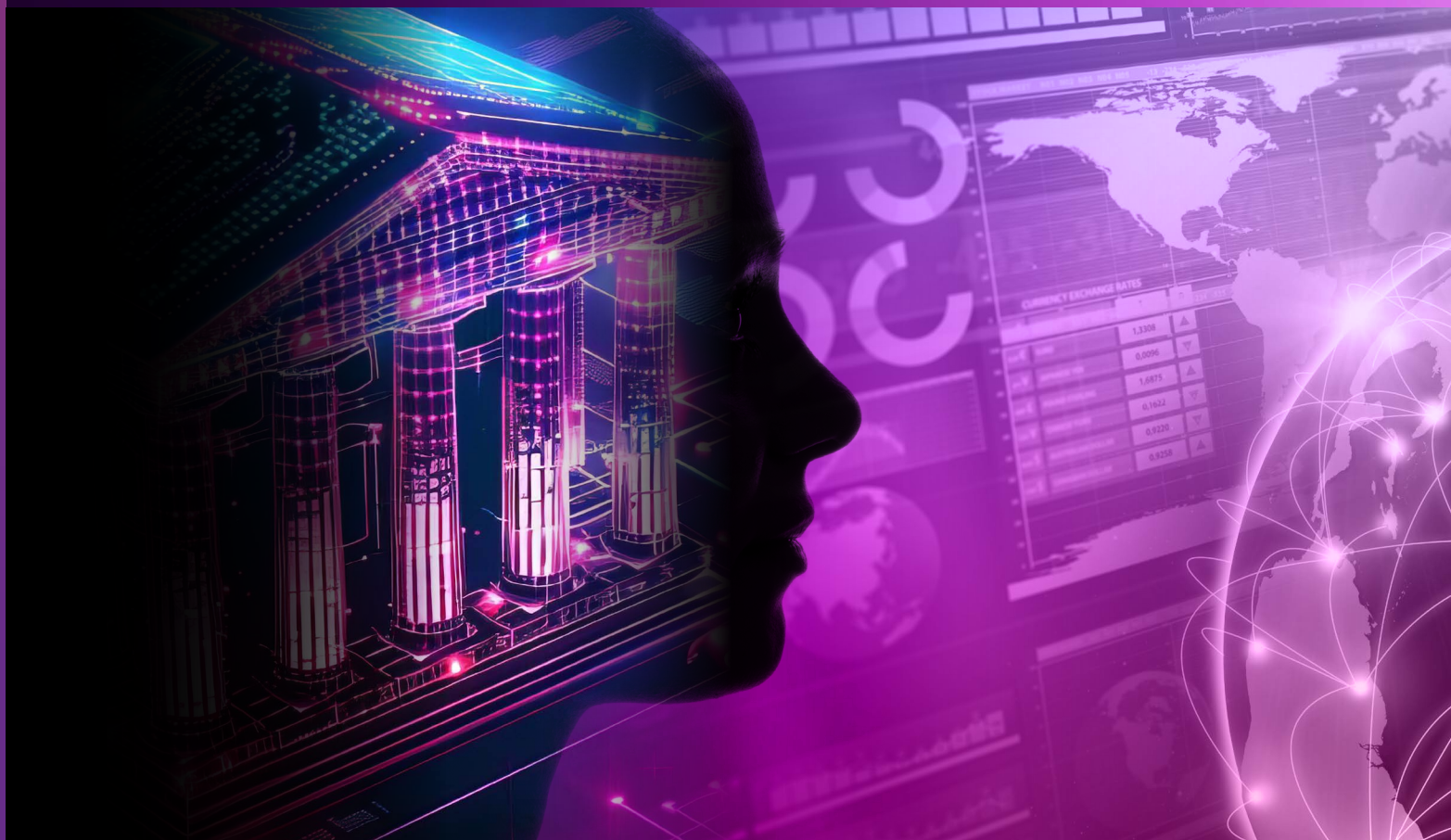
Carrie Kostelec
Senior Manager
Artificial Intelligence
Assurance and Advisory Innovation

Di Krupica
Senior Manager
Digital Assets
Assurance and Advisory Innovation

AICPA

2025 Criteria for Stablecoin Reporting:

Specific to Asset-Backed Fiat-Pegged Tokens



About the AICPA

The American Institute of CPAs® (AICPA®) is the world's largest member association representing the accounting profession, with more than 418,000 members in 143 countries and a 129-year heritage of serving the public interest. AICPA members represent many areas of practice, including business and industry, public practice, government, education and consulting.

The AICPA sets ethical standards for the profession and U.S. auditing standards for audits of private companies, not-for-profit organizations, federal, state and local governments. It develops and grades the Uniform CPA Examination and offers specialty credentials for CPAs who concentrate on personal financial planning; fraud and forensics; business valuation; and information technology. Through a joint venture with The Chartered Institute of Management Accountants (CIMA), it established the Chartered Global Management Accountant (CGMA) designation to elevate management accounting globally. The AICPA maintains offices in New York, Washington, DC, Durham, NC, and Ewing, NJ.

Contents

Notice to Readers

(***Boldface italics*** denotes new language. Deleted text is shown in ~~**strikethrough**~~.)

The* 2025 Criteria for Stablecoin Reporting: Specific to Asset-Backed Fiat-Pegged Tokens *contains the following sets of criteria:

1. **2025 Criteria for the Presentation and Disclosure of Redeemable Tokens Outstanding and the Availability of Redemption Assets: Specific to Asset-Backed Fiat-Pegged Tokens**
2. **Proposed Criteria for Controls Supporting Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens**

2025 Criteria for the Presentation and Disclosure of Redeemable Tokens Outstanding and the Availability of Redemption Assets: Specific to Asset-Backed Fiat-Pegged Tokens

The 2025 Criteria for the Presentation and Disclosure of Redeemable Tokens Outstanding and the Availability of Assets for Redemption: Specific to Asset-Backed Fiat-Pegged Tokens (**~~the criteria~~**) were established by the Assurance Services Executive Committee (ASEC) of the AICPA for use when reporting on the following, at a specific measurement point in time (collectively, the subject matter):

- Presentation and disclosure of the token issuer's redeemable tokens outstanding and related information
- Presentation and disclosure of the redemption assets[1] available for redeemable tokens outstanding and related information
- Presentation and disclosure of the comparison of the redemption assets available for redeemable tokens outstanding and the token issuer's redeemable tokens outstanding, and related information of the comparison

Proposed Criteria for Controls Supporting Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens

The* Proposed Criteria for Controls Supporting Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens *were established by ASEC of the AICPA for use when evaluating the suitability of design and operating effectiveness of controls over token operations (for example, token generation and management, redemption asset management, vendor management, and reporting), over a specified period of time.

Suitable Criteria

ASEC, in establishing and developing these ***sets of*** criteria, followed due process procedures, including exposure of the criteria for public comment. BL section 360R, *Implementing Resolutions Under Section 3.6 Committees,*[2] designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA Council or the board of directors. Paragraph .A46 of AT-C section 105, *Concepts Common to All Attestation Engagements,*[3] indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered to be suitable. Accordingly, these ***sets of*** criteria are suitable criteria for the presentation and disclosure of redeemable tokens outstanding and the availability of assets for redemption, ***and evaluating the suitability of design and operating effectiveness of controls over token operations,*** specific to asset-backed fiat-pegged tokens.

1 Assets held by the token issuer to support redeemability of asset-backed fiat-pegged tokens (such as cash, cash equivalents, or other assets).
2 All BL sections can be found in AICPA *Professional Standards*.
3 All AT-C sections can be found in AICPA *Professional Standards*.

In accordance with AICPA Statements on Standards for Attestation Engagements,[4] criteria are benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter. In an examination or review engagement,[5] criteria to be applied in the preparation and evaluation of the underlying subject matter should be suitable.[6] Attributes of *suitable criteria* are as follows:

a. *Relevance*. Criteria are relevant to the underlying subject matter.

b. *Objectivity*. Criteria are free from bias.

c. *Measurability*. Criteria permit reasonably consistent measurements, qualitative or quantitative, of underlying subject matter.

d. *Completeness*. Criteria are complete when subject matter prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect decisions of the intended users based on that subject matter information.

In addition to being suitable, criteria used in an attestation engagement should be available[7] to intended users. The publication of these ***sets of*** criteria makes the criteria available to users.

The engaging party may specify any criteria for use in the preparation and evaluation of the underlying subject matter, provided that they are suitable, as described in AT-C section 105.[8] Accordingly, there is no requirement that the token issuer use ***these*** ~~**this**~~ set***s*** of criteria when presenting and disclosing redeemable tokens outstanding and the availability of assets for redemption, ***or evaluating the suitability of design and operating effectiveness of controls over token operations,*** specific to asset-backed fiat-pegged tokens.

4 Statements on Standards for Attestation Engagements are commonly known as the *attestation standards.*
5 Examination engagements are performed under AT-C section 205, *Assertion-Based Examination Engagements,* or AT-C section 206, *Direct Examination Engagements,* of the attestation standards. Review engagements are performed under AT-C section 210, *Review Engagements.*
6 Paragraph .27*b* of AT-C section 105, *Concepts Common to All Attestation Engagements.*
7 Paragraph .27*b* of AT-C section 105.
8 Paragraph .A44 of AT-C section 105.

2025 Criteria for Stablecoin Reporting:

Specific to Asset-Backed Fiat-Pegged Tokens

(Boldface italics denotes new language. Deleted text is shown in ~~**strikethrough**~~.)

Introduction

1. Digital assets are digital records that are assets, are created or reside on a distributed ledger based on blockchain or similar technology, and are secured through cryptography. *Asset-backed tokens* are digital assets of which there are many different types, for example, fiat-pegged, commodity-pegged, or crypto-pegged. This document is intended to cover only those asset-backed tokens that are fiat-pegged and is only intended for scenarios addressed herein.

2. When an entity creates an asset-backed token, the entity develops and publishes terms, which may include the token issuer's terms of service, legal terms, user agreements, and any other relevant documents maintained by the token issuer that detail the legal agreement between the token issuer and the entities purchasing the tokens ***(collectively referred to as token issuer's terms)***. The token issuer determines which set of terms is in scope when applying these criteria. These terms generally include stipulations such as the method and timing for issuing and redeeming tokens; the amount of redemption assets[1] for which each token is redeemed; the type of accounts in which the redemption assets are held; and the types of assets that will be held to support the redemption of each token. Because there are no specific requirements to follow when developing terms, they vary by token issuance and may be influenced by a token issuer's applicable regulations (for example, the New York Department of Financial Services "Guidance on the Issuance of U.S. Dollar-Backed Stablecoins").

3. This document covers ~~**only**~~ ***two sets of*** criteria for ~~**presenting and disclosing the availability of cash, cash equivalents, or other assets for redeeming outstanding**~~ asset-backed fiat-pegged tokens, ***as follows:***

    - ***2025 criteria for presenting and disclosing the availability of cash, cash equivalents, or other assets for redeeming outstanding tokens***
    - ***Proposed criteria for evaluating the suitability of design and operating effectiveness of controls over token operations***

    Token issuers will need to evaluate whether ~~**the**~~ ***these sets of*** criteria may be used based on the token issuer's facts and circumstances. Generally, these fiat-pegged tokens include mechanisms designed to minimize price volatility by linking their values to the value of a fiat currency. In this case, typically, each token is pegged on a 1:1 basis to fiat currency (for example, a U.S. dollar for each token) and can be redeemed based on the current effective terms. In order to provide confidence and trust in the redeemability of the tokens, the issuing entity often holds assets (for example, cash, cash equivalents, or other assets), hereafter referred to as *redemption assets,* in an amount equal to or greater than the number of the redeemable tokens outstanding.

4. Varying technical designs exist for the creation (known as *minting*) or destruction (known as *burning*) of fiat-pegged tokens. Prior to minting tokens, the token issuer determines which blockchains the tokens will be minted and circulated on and which smart contracts to use to manage the *token quantity* (that is, *token supply*). These are considered in-scope blockchains and smart contracts, which are defined in the token issuer's terms.

1 Assets held by the token issuer to support redeemability of asset-backed fiat-pegged tokens (such as cash, cash equivalents, or other assets).

5. When a token issuer mints fiat-pegged tokens, the transaction is broadcast and recorded on the nodes of a distributed ledger or blockchain network. The token issuer's terms are expected to clearly outline which tokens are in-scope as well as the processes by which tokens are minted and placed into circulation. Generally, once tokens are minted, they are made available for redemption. However, there may be instances in which a token issuer has *minted tokens* that are *nonredeemable*, based on the token issuer's terms (for example, *pre-minted, test, time-locked for* a specified amount of time, or permanently *access-restricted tokens*). As defined in the token issuer's terms, these tokens may be either temporarily or permanently nonredeemable. Both temporarily and permanently nonredeemable tokens should be clearly defined in the token issuer's terms and disclosed accordingly at the measurement point in time. (Note: The classification of tokens as either temporarily or permanently nonredeemable may change over time; therefore, token issuers would need to update their terms accordingly.)

6. In addition to the requirements for the tokens, the token issuer's terms are expected to specify requirements for the redemption assets. These requirements may include, but are not limited to, the ratio between redemption assets and redeemable tokens (for example, a 1:1 ratio); the composition of redemption assets (for example, cash and cash equivalents, including money market funds, U.S. Treasuries, or repurchase agreements); the timing of redeeming the tokens for fiat currency (for example, withdrawals may take up to two days to complete); and the type of accounts (for example, custodial, noncustodial, omnibus, or individually identified) the redemption assets are held in.

7. Tokens that have been minted on in-scope blockchains, as defined by the token issuer's terms, and have not been *bridged* from other blockchains or networks, are called *natively minted tokens*. There are additional situations in which the issuer's fiat- pegged tokens are wrapped or bridged. A bridging or wrapping service enables the token holder to transfer or transform a token for use across different blockchain networks or protocols. Wrapped tokens are separate and distinct tokenized versions of the fiat-pegged tokens that may be used either on the same blockchain as the original fiat-pegged token or on a different blockchain. Wrapped tokens are often bridged to another blockchain, typically by a party other than the issuer of the fiat-pegged token. If the token issuer is itself bridging or wrapping its tokens, the token issuer's terms should specify which wrapped or bridged tokens are in-scope of the report.

2025 Criteria for the Presentation and Disclosure of Redeemable Tokens Outstanding and the Availability of Redemption Assets: Specific to Asset-Backed Fiat-Pegged Tokens

8. ~~**This**~~ ***Part I of this*** document presents the criteria to use for the following three subject matters, at a specific measurement point in time:

- *Presentation and disclosure of the token issuer's redeemable tokens outstanding and related information*[2]

  This subject matter focuses on the presentation and disclosure of redeemable tokens outstanding (that is, tokens in circulation that have corresponding redemption assets). This includes disclosure of information affecting the reliability of the information obtained from the distributed ledgers or blockchain networks, disclosures of the total natively minted token quantity, and any difference (for example, pre-minted, test, time-locked for a specified amount of time, or permanently access-restricted tokens) from the amount of the redeemable tokens outstanding. In addition, the token issuer's terms define how token redemptions are processed.

- *Presentation and disclosure of the redemption assets available for redeemable tokens outstanding and related information*[3]

  This subject matter focuses on the presentation and disclosure of the redemption assets available for redeemable tokens outstanding based on the token issuer's terms. The disclosures include information such as the type of account in which the assets are held, the composition of those assets, and the nature of the arrangements and rights to the assets, including any other claims, rights, or assessments on the redemption assets.

- *Presentation and disclosure of the comparison of the redemption assets available for redeemable tokens outstanding and the token issuer's redeemable tokens outstanding, and related information of the comparison*[4]

  This subject matter focuses on the comparison of the redemption assets and the redeemable tokens outstanding. In addition, information related to material incidents or events that may affect the amount of redeemable tokens outstanding, the availability of redemption assets, or the redemption asset balance is disclosed.

2 The table of criteria for the presentation and disclosure of the redeemable tokens outstanding, redemption assets, and the comparison of the two is on pages 10–19. See criteria *FP1* and *FP2* related to the redeemable tokens outstanding.

3 The table of criteria for the presentation and disclosure of the redeemable tokens outstanding, redemption assets, and the comparison of the two is on pages 10–19. See criteria *FP3, FP4, FP5,* and *FP6* related to the redemption assets.

4 The table of criteria for the presentation and disclosure of the redeemable tokens outstanding, redemption assets, and the comparison of the two is on pages 10–19. See criteria *FP7* and *FP8* related to the comparison of the redeemable tokens outstanding and redemption assets.

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens

9. ***Part II of this document presents the criteria, in the form of control objectives, to use when evaluating the suitability of design and operating effectiveness of controls to achieve the control objectives over token operations, over a specified period of time, which is divided into eight control areas:***

    - ***Token generation and management***
    - ***Client onboarding and maintenance***
    - ***Customer transaction processing***
    - ***Key and backup management***
    - ***Redemption asset management***
    - ***Vendor management***
    - ***Reporting***
    - ***IT general controls***

Why Are These Presentation and Disclosure Criteria *and Controls Criteria* Needed?

10. No common framework or criteria exist for evaluating the previously mentioned subject matters ***related to presentation and disclosure*** for fiat-pegged tokens. This results in inconsistencies among token issuers in the presentation and disclosure of redeemable tokens outstanding and the redemption assets available that back those tokens. The result is that stakeholders, such as token holders and regulators, do not have transparency regarding the redemption assets available to cover redemption requests. For example, in scenarios in which an issuer does not disclose the regulatory jurisdiction governing the redemption assets (or in the case in which redemption assets are held in more than one jurisdiction, multiple regulatory jurisdictions), the redeemability of those assets by a token holder may be unclear. Because information about the redeemable tokens outstanding and redemption assets is not disclosed in the same manner, there is a lack of comparability and consistency of available information.

11. ~~**These**~~ ***The*** criteria ***in part I*** were developed to provide a common framework to token issuers and other stakeholders for reporting on information about tokens. These criteria are designed to eliminate inconsistencies in presentation and disclosures of redeemable tokens outstanding and the redemption assets available for all stakeholders. Token issuers may leverage these criteria when developing their terms, which would provide transparency to stakeholders regarding the redeemable tokens outstanding as well as the redemption assets available.

12. ***There is also no common framework or criteria for evaluating the previously mentioned subject matter related to controls supporting token operations. This results in inconsistencies among token issuers when identifying controls necessary to support token operations and preparing disclosures related to redeemable tokens outstanding and the redemption assets available that back those tokens. The token issuer may be interested in controls when preparing its disclosures related to redeemable tokens to ensure transparency, as well as completeness and accuracy of information reported. Without complete, accurate, and transparent information, details regarding redeemable tokens, assets available for redemption, or the redeemability of those assets by a token holder may be unclear. Because information about the redeemable tokens outstanding and redemption assets is not disclosed in the same manner, there is a lack of comparability and consistency of available information that may be used when preparing the disclosures related to redeemable tokens outstanding and the redemption assets available that back those tokens.***

13. ***When considering the design of controls that support token operations, the token issuer will first need to identify risks commonly associated with token operations. Once risks have been identified, token issuers can develop policies and procedures, and design and implement relevant controls, to appropriately mitigate such risks. The criteria in part II were developed to provide a common framework for token issuers to identify the risks commonly associated with token operations. The risks are linked to control objectives that are common to token issuer operations and processes. These control objectives may be used by the token issuer when designing, implementing, operating, and monitoring controls to provide reasonable assurance that those risks identified would not prevent the control objectives from being achieved.***

Who Can Use These Presentation and Disclosure Criteria *and Controls Criteria?*

14. ~~**These**~~ ***The*** criteria ***in part I*** can be used to assist token issuers in presenting and disclosing the redeemable tokens outstanding and the redemption assets available specific to asset-backed fiat-pegged tokens. Token issuers may use the criteria to present the redeemable tokens outstanding, redemption assets, and the comparison of the two, based on the token issuer's terms, and disclose relevant information to stakeholders.

15. ***The criteria in part II can be used to assist token issuers when evaluating the suitability of design and operating effectiveness of controls over token operations, over a specified period of time.***

> ***Note: If a token issuer has an existing SOC® 1 report that includes its token operations, the token issuer may not need to obtain a separate report if the existing SOC 1 report adequately addresses all the criteria and control areas outlined in this document.***

16. These ***sets of*** criteria may also be used by a practitioner reporting on management's assertion***(s) related to the subject matters described previously.*** ~~**during an attestation**~~ ***These*** engagement***s are*** performed in accordance with the AICPA Statements on Standards for Attestation Engagements (commonly known as the *attestation standards* and codified in the AT-C sections in AICPA *Professional Standards*) (for example, AT-C section 205, *Assertion-Based Examination Engagements*). In ***each of these*** ~~**such an**~~ engagement***s***, the practitioner uses ~~**these**~~ ***the relevant set of*** criteria when performing procedures and when issuing a report relevant to evaluating management's assertion***(s)***.

17. Throughout the criteria ***in part I***, reference is made to "material" and, where applicable, examples of what may be considered material in the context of the applicable criteria have been provided. However, what is ultimately determined to be material is based on the judgment of the preparer of the presentation and disclosure of redeemable tokens outstanding and the availability of assets for redemption and the applicable facts and circumstances.

18. The provisions of the criteria need not be applied to immaterial items.

***Part I:* 2025 Criteria for the Presentation and Disclosure of Redeemable Tokens Outstanding and the Availability of Assets for Redemption: Specific to Asset-Backed Fiat-Pegged Tokens**

19. The following table presents the criteria for the presentation and disclosure of the redeemable tokens, redemption assets, and the comparison of the two, based on the token issuer's terms,[5] and disclosure of relevant information to stakeholders. It covers three specific subject matters at a specific measurement point in time:

    a. Presentation and disclosure of the token issuer's redeemable tokens outstanding and related information

    b. Presentation and disclosure of the redemption assets available for redeemable tokens outstanding and related information

    c. Presentation and disclosure of the comparison of the redemption assets available for redeemable tokens outstanding and the token issuer's redeemable tokens outstanding, and related information of the comparison

20. The points of focus in the right-hand column represent important characteristics of the presentation and disclosure criteria. These points of focus may assist both the token issuer and the practitioner. In some situations, the token issuer may consider adding additional details to address items not included in the points of focus based on the specific circumstances of the entity (for example, to address specific jurisdictional or regulatory requirements). Use of these criteria does not require an assessment of whether each point of focus is addressed, but rather, requires users of the criteria to understand these points of focus in order to apply the criteria properly. When evaluating the presentation and disclosures of the subject matter using these criteria, users are advised to consider the facts and circumstances of the entity and its environment in actual situations in relation to the entity's objectives.

21. In addition, following the criteria and points of focus, exhibits have been included to provide illustrations of the presentation and disclosures for each aspect of the criteria, based on facts and circumstances, as follows:

    - Exhibit A. An Illustrative Presentation and Disclosure of the Token Issuer's Redeemable Tokens Outstanding and Related Information
    - Exhibit B. An Illustrative Presentation and Disclosure of the Redemption Assets Available for Redeemable Tokens Outstanding and Related Information
    - Exhibit C. An Illustrative Presentation and Disclosure of the Comparison of the Redemption Assets Available for Redeemable Tokens Outstanding and the Token Issuer's Redeemable Tokens Outstanding, and Related Information of the Comparison

5 Token issuer's terms include terms of service, legal terms, user agreements, and any other relevant documents maintained by the token issuer that detail the legal agreement between the token issuer and the entities purchasing the tokens.

Presentation and Disclosure of the Token Issuer's Redeemable Tokens Outstanding and Related Information

Note: Following the criteria and points of focus, exhibit A has been included to illustrate criteria ***FP1, FP2, FP8a, FP8b, FP8c,*** and ***FP8e,*** which relate to the token issuer's redeemable tokens outstanding and related information. The example includes both temporary and permanent nonredeemable reconciling tokens. In addition, example disclosures are included that would be made to comply with the criteria based on facts and circumstances. The example is for illustrative purposes only.

These criteria apply only to asset-backed fiat-pegged tokens and are intended only for the types of asset-backed tokens or scenarios addressed herein.

	Presentation and disclosure criteria	Points of focus
FP1	The redeemable tokens outstanding are disclosed, based on the token issuer's terms.[6]	
	a. Disclosure of the definition of the in-scope[7] total natively minted token quantity would include i. distributed ledgers or blockchain networks. ii. smart contracts.	When defining the total natively minted token quantity, it is important for the definitions and disclosures to be included regarding which tokens are in scope. Tokens with similar names or ticker symbols are often created. Therefore, it is key to clearly define which minted tokens are in scope. Bridged or wrapped tokens may or may not be applicable based on the token issuer's terms. The token issuer's terms specify whether and which bridged or wrapped tokens are in scope to the report. i. Distributed ledgers or blockchain networks. Disclose which distributed ledgers or blockchains, associated with tokens that have been issued, are in scope. ii. Smart contracts. Disclose which specific smart contract or token addresses, associated with tokens that have been issued, are in scope. Generally, a smart contract is used to manage the natively minted token quantity. A smart contract is unique to a specific blockchain. If a token issuer is issuing tokens on multiple blockchains, there will be multiple smart contracts in scope. Therefore, it is important that all smart contracts that have an impact on the overall natively minted token quantity are identified and made available to stakeholders, in the report or by reference.
		Note: The goal of criterion ***FP1a*** is to define the total natively minted token quantity (or starting balance) for all tokens in scope. Criterion *FP1c* incorporates the reconciliation of the total natively minted token quantity, observed on-chain, to the amount of redeemable tokens outstanding. This will enable users of the report to understand the starting amounts and how the amount of redeemable tokens outstanding is derived.

6 Token issuer's terms include terms of service, legal terms, user agreements, and any other relevant documents maintained by the token issuer that detail the legal agreement between the token issuer and the entities purchasing the tokens.

7 Token issuer's terms define which distributed ledgers or blockchain networks and smart contracts are in scope.

Presentation and Disclosure of the Token Issuer's Redeemable Tokens Outstanding and Related Information		
	Presentation and disclosure criteria	**Points of focus**
	b. Amount of redeemable tokens outstanding for in-scope distributed ledgers or blockchain networks, based on the token issuer's terms, is disclosed.	The amount of redeemable tokens outstanding is derived by starting with the total natively minted token quantity and then subtracting any burned tokens and nonredeemable tokens (based on the definitions in the token issuer's terms). Disclosure of the tokens outstanding issued on in-scope distributed ledgers or blockchain networks may be presented individually by network or in the aggregate. The token issuer's terms stipulate what is in scope regarding the token quantity. The total natively minted token quantity incorporates all tokens that are minted on the in-scope distributed ledgers or blockchain networks less any tokens that are burned. However, only the token issuer's terms can specify which tokens minted may not be redeemable, for example, pre-minted, test, time-locked for a specified amount of time, and permanently access-restricted tokens.
	c. Differences between the total in-scope natively minted token quantity and redeemable tokens outstanding are disclosed.	Tokens that are minted, but not redeemable at the measurement point in time, are disclosed to arrive at the appropriate redeemable token outstanding balance. Based on the token issuer's terms, these nonredeemable tokens generally fall into two categories: temporarily or permanently nonredeemable. Neither category is included in the amount of redeemable tokens outstanding.
		Note: Determination of classification of tokens as either temporarily or permanently nonredeemable is based on the token issuer's terms, and such terms or classifications may change over time.

Presentation and Disclosure of the Token Issuer's Redeemable Tokens Outstanding and Related Information		
	Presentation and disclosure criteria	**Points of focus**
		The tokens that are categorized as temporarily nonredeemable based on the token issuer's terms may not be redeemable at a specific point in time; however, they may become redeemable at some point in the future and therefore have associated redemption assets. Examples of these include (as defined by the token issuer's terms) the following types of tokens: • Time-locked (for a specified amount of time) • Pre-minted • Temporarily access-restricted The tokens that are categorized as permanently nonredeemable based on the token issuer's terms will never be redeemable in the future and therefore may not be required to have associated redemption assets. Examples of these include (as defined by the token issuer's terms) the following types of tokens: • Permanently access-restricted • *Test tokens* Disclosure of the reconciling components from the total natively minted token quantity to the redeemable tokens outstanding may be incorporated into a table that illustrates the balances for each in-scope distributed ledger or blockchain network. Adjustments made to reflect the number of redeemable tokens may require commensurate adjustments to the redemption asset balances, based on the token issuer's terms.

Presentation and Disclosure of the Token Issuer's Redeemable Tokens Outstanding and Related Information		
	Presentation and disclosure criteria	**Points of focus**
	d. Disclosure is made of any known unresolved events or occurrences that have materially affected the natively minted token quantity or redeemable tokens outstanding related to: i. the distributed ledgers or blockchain networks (including the consensus and security mechanisms). ii. smart contracts used to issue and manage token operations (that is, in-scope smart contracts).	Disclosures include unresolved events or occurrences related to the distributed ledger or blockchain networks that tokens are issued on, and any smart contracts that are used to issue and manage token operations, that materially affected the number of redeemable tokens outstanding at a specific measurement point in time. Known unresolved events or occurrences that have affected the mechanics, security, maturity, and maintenance of the distributed ledger or blockchain networks need to be disclosed when they have materially affected the number or redeemability of tokens. Considerations when evaluating these types of known events or occurrences may include, but are not limited to, the following: i. Unreliable consensus and security mechanisms • Lack of reliability of the consensus mechanism because of design vulnerabilities – Accepting invalid transactions as valid, resulting in material inaccurate or invalid transaction detail and balances – High level of risk associated with the type of consensus mechanism used • Lack of method for handling unconfirmed transactions or validating and recording confirmed transactions • Lack of sufficient number of validators or miners securing the network • Failure to disseminate the same information to all nodes • Lack of hash power or "at-risk" stake securing the network • Lack of verifiability of current and previous ledger states • Low confidence in the final state of the ledger • Lack of process for resolving forks ii. Lack of maturity and maintenance of network • Recent launch date of protocol or network • Lack of developer activity • Lack of availability of software (for example, open sourced or closed sourced) • Material recent forks or network upgrades Smart contracts are used to issue as well as manage the token quantity (that is, the minting and burning of tokens). When evaluating whether there has been an event or occurrence that has had a material impact on the tokens, considerations may include identification of the following: • Lack of third-party smart contract code assessments • Lack of appropriate accounting for tokens that are categorized as temporary or permanent nonredeemable based on token issuer's terms • Lack of security for the keys controlling the in-scope smart contracts during some or all the key life cycle (key generation, backup, key recovery seeds, continued key security, encryption, distribution, destruction)

Presentation and Disclosure of the Token Issuer's Redeemable Tokens Outstanding and Related Information		
	Presentation and disclosure criteria	**Points of focus**
FP2	Token issuer's terms for purchases and redemptions are made available to authorized token holders and include the following:	
	a. Established terms for token purchases and redemptions b. Definition of purchase and redemption rights (including which holders have such rights)	Token issuers establish terms for purchases and redemptions, which are made available to authorized token holders (for example, posted on the token issuer's website). These terms may consider any regulatory requirements that have been identified. Example types of token purchase and redemption terms may include the following: • Whether purchases and redemptions must be processed within a specific timeframe • Whether purchases and redemptions are always at par • Whether purchases and redemptions are to be made through the delivery of cash, cash equivalents, or other forms of consideration Example definitions of purchase and redemption rights may include the following: • What conditions need to be met for a holder of the token to have a direct right to purchase and redeem (rather than merely an ability to exchange) • What conditions could cause a purchase and redemption right to be revoked temporarily or permanently

Presentation and Disclosure of the Redemption Assets Available for Redeemable Tokens Outstanding and Related Information

Note: Following the criteria and points of focus, exhibit B has been included to illustrate criteria ***FP3, FP4, FP5, FP6,*** and ***FP8d,*** which relate to redemption assets available for redeemable tokens outstanding and related information. The example is based on specific facts and circumstances and is for illustrative purposes only.

These criteria apply only to asset-backed fiat-pegged tokens and are intended only for the types of asset-backed tokens or scenarios addressed herein.

	Presentation and disclosure criteria	Points of focus
FP3	Disclosures related to the counterparties holding redemption assets include the following:	
	a. Type of counterparty b. The jurisdiction (regulatory or geographic) of the counterparty c. Related party, as applicable	Counterparties can be in various forms, such as an FDIC-insured bank, trust company, escrow agent, or otherwise qualified custodian. The jurisdiction of the counterparty is important to understand with respect to the regulations within that jurisdiction. Disclosures would include any related party transactions or arrangements or other contractual provisions that may affect the timely redemption of tokens, including, but not limited to, a regulators ability to restrict redemptions in case of receivership.
FP4	Disclosures and measurement of the redemption assets include the following:	
	a. Description of the composition of redemption assets by asset type (such as cash and cash equivalents [including U.S. Treasuries], money market funds, repurchase agreements, and other investments), including, as applicable i. geographic location, ii. amount/value, and iii. terms (for example, maturity dates)	Requirements for the composition of the redemption assets are detailed in the token issuer's terms. When disclosing maturity dates, consideration may include the timing of liquidation. In addition, disclosure of the industry, geographic location, credit rating of investments, and CUSIP numbers (as applicable) may be considered. Generally, geographic classification is based on the concentration of the risk and economic exposure (where the principal business actually takes place).
		Note: Redemption asset composition disclosures may be made in a tabular form.
	b. Description of the method used to measure the value of redemption assets by asset type, based on the issuer's terms, including: i. cash and cash equivalents, ii. money market funds, iii. repurchase agreements, and iv. other assets	The method used to measure the valuation of redemption assets is based on facts and circumstances along with token issuer's terms. For each of the asset types, example disclosures may include the following: i. Cash and cash equivalents. Disclosed at par ii. Money market funds. Disclosed at net asset value iii. Repurchase agreements. Disclose the term, collateral, any relevant risks, and valuation in accordance with applicable standards iv. Other assets. Disclosed at fair value in accordance with the applicable standards

Presentation and Disclosure of the Redemption Assets Available for Redeemable Tokens Outstanding and Related Information		
	Presentation and disclosure criteria	**Points of focus**
FP5	Disclosures regarding the redemption asset arrangements include:	
	a. the nature of the arrangement between the token issuer and the counterparty (such as the token issuer's rights to the redemption assets), b. the value of the redemption assets subject to each type of arrangement, and c. any restrictions on the use of the redemption assets	In order to adequately disclose the nature of the arrangements between the token issuer and the counterparty, consider the type of account, as well as the rights the token issuer has to the redemption assets. Examples of account types include the following: • Custodial (omnibus or individually identified) • Noncustodial (omnibus or individually identified) • Assets held in an account "for the benefit of" token holders • Assets held in a separate bankruptcy remote trust Examples of the token issuer's rights to the redemption assets by the counterparty, based on the agreement, include the following: • Rights to transfer assets • Rights to sell assets • Rights to loan • Rights to rehypothecate In addition, there may be restrictions placed on the token issuer's use of redemption assets (for example, the redemption assets are able to be used by the token issuer, only to redeem in-scope redeemable tokens outstanding).
FP6	Disclosures regarding whether the token issuer has direct contractual mechanisms to mitigate risk of loss of redemption assets, and if so, describe the nature and extent of such mechanisms.	When disclosing whether or not the token issuer has mechanisms to mitigate risk of loss of redemption assets, including bankruptcy, consideration may include sufficient detail to adequately explain the extent to which the risk of loss has been mitigated. For example, if deposit insurance does not pass through to the token holder, the token issuer would make an explicit statement to that effect. Depending on the type of counterparty and the nature of the arrangement with the counterparty, the token issuer discloses the mechanisms to mitigate the risk related to the redemption assets. The redemption assets may be insured only up to certain amounts, and the token issuer may have to implement other mechanisms to mitigate the reserve risk. For example, if the redemption assets are held in an FDIC-insured bank, the amount above the insured amount would be at risk. Risk mitigation strategies might include entering into credit default swaps; interest rate hedges; deposit sweep network; and purchase of private insurance.

Presentation and Disclosure of the Comparison of the Redemption Assets Available for Redeemable Tokens Outstanding and the Token Issuer's Redeemable Tokens Outstanding, and Related Information of the Comparison

Note: Following the criteria and points of focus, exhibit C has been included to illustrate criterion *FP7,* which relates to the comparison of the redemption assets available for redeemable tokens outstanding and the token issuer's redeemable tokens outstanding, and related information of the comparison. This comparison includes timing and temporary differences as well as examples of disclosures that would be made to comply with the criteria based on facts and circumstances. The example is for illustrative purposes only.

These criteria apply only to asset-backed fiat-pegged tokens and are intended only for the types of asset-backed tokens or scenarios addressed herein.

	Presentation and disclosure criteria	Points of focus
FP7	Disclosures of the comparison of available redemption assets to redeemable tokens outstanding include the following:	
	a. Disclosures of the value of available redemption assets and the redeemable tokens outstanding, including any surplus or deficit, and differences between the total redemption assets and total redeemable tokens outstanding	This disclosure includes the appropriately defined and measured amounts from *FP1* and *FP4*, representing redeemable tokens outstanding and the value of available redemption assets, respectively. Differences may include the following: • Purchases to be minted • *Burns* to be redeemed, including – timing differences (that is, cut-off issues) – missing or inaccurate data (that is, bad token issuer or authorized token holder data)
		Note: The reconciliation of redeemable tokens outstanding to the total redemption assets held includes reconciling items for temporary and permanent differences (for example, timing of cash settlement and tokens associated with access-restricted addresses).
	b. Disclosures of redemption assets include whether the asset-backing level is based on the token issuer's terms	This compares the ratio of redemption assets and redeemable tokens outstanding to the token issuer's terms. The redemption asset requirements refer to the concept of the asset-backing level (for example, 1:1 ratio). Token issuers may have a formal asset-backing level per the terms that is other than 1:1 (for example, 50% redemption assets to total tokens outstanding).
	c. Disclosures of the amounts of unprocessed purchase and redemption requests	A token issuer establishes processes to ensure that any outstanding purchases and redemptions are handled based on the token issuer's terms; that is, there are justified reasons why the purchase or redemption remains outstanding (for example, timing differences due to the processing of redemption and purchase requests; incorrect bank account information). Disclosure includes the amount of unprocessed purchase and redemption requests and whether any unprocessed purchases and redemptions, at the measurement point in time, have exceeded the time period pursuant to the token issuer's terms for the delivery of tokens and redemption assets. These amounts may include timing or temporary differences between tokens outstanding and available assets.

Presentation and Disclosure of the Comparison of the Redemption Assets Available for Redeemable Tokens Outstanding and the Token Issuer's Redeemable Tokens Outstanding, and Related Information of the Comparison		
	Presentation and disclosure criteria	**Points of focus**
FP8	Disclosures regarding redeemable tokens outstanding, their redeemability, or available redemption assets include the following:	
	a. Disclosures of events or transactions materially affecting the redeemable tokens outstanding or available redemption assets occurring after the measurement point in time and up to the date of the token issuer's report	These types of events or occurrences are similar to subsequent events. Examples include the following: • Forks • Compromised security of the blockchain underlying the redeemable tokens • Inability to access redemption assets in the normal course of business • Compromise of or other issue related to the governing smart contracts Example 1: On X date, the ABC blockchain experienced a hard fork, splitting the ABC blockchain into two versions. Redemptions will be honored on version 1, which inherits the total circulating supply of tokens and the ledger history prior to the hard fork at block height XXX. Redemptions will not be supported for tokens issued on version 2. Tokens issued on version 2 are considered out of scope and will not contribute to the total redeemable token balance. Example 2: On X date, state regulators filed a petition for receivership on ABC Bank, which custodies the redemption asset on behalf of the token issuer. The impact on the valuation and availability of redemption assets is not yet fully known.
	b. Disclosures related to litigation, claims, and assessments that may have a material impact on the redeemable tokens outstanding or the available redemption assets	The token issuer may have pending legal matters that may place additional claims upon the assets pledged to redeem outstanding tokens. Examples include the following: • Outstanding litigation or claims between the token issuer and the custodian that may result in the token issuer not being able to redeem its tokens • Outstanding litigation or claims between the token issuer and other institutions (for example, the SEC or other regulators) that may result in the token issuer not being able to redeem its tokens • Outstanding claims, rights, or assessments on the available redemption assets

Presentation and Disclosure of the Comparison of the Redemption Assets Available for Redeemable Tokens Outstanding and the Token Issuer's Redeemable Tokens Outstanding, and Related Information of the Comparison		
	Presentation and disclosure criteria	**Points of focus**
	c. Disclosures of market, operational, technological, regulatory, or other events that may materially affect the token issuer's ability to perform token redemption based on token issuer terms	Certain events may affect the token issuer's ability to perform token redemptions based on the token issuer's terms. Examples include the following: • Tokens. Service providers' (for example, exchanges or custodians) terms or matters that may result in delays in redeeming, or the inability to redeem, tokens on demand • Redemption assets. Geopolitical events that may disrupt or freeze the redemption assets involved in the redemption process • Events after report date. Disclosure of token issuer's events that occur after the report has been issued, such as updating the report or issuing additional information to support the report, as necessary
	d. Disclosures of the existence and nature of any commitments that may materially affect the available redemption assets	Examples include the following: • Liens, security interests or encumbrances, or other arrangements in which available redemption assets have been pledged as security for a borrowing arrangement
	e. Disclosures of token issuer's regulatory jurisdiction	Examples include the following: • Regulatory jurisdiction. Where not otherwise disclosed, any information regarding the regulatory jurisdiction that would affect the redemption process

Effective date

22. The criteria may be used upon issuance.

Part II: Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens

23. The following table includes control objectives that address the risks commonly associated with token issuers' operations. Each control area and all criteria within the control areas relevant to token operations are expected to be addressed. However, in limited circumstances, a particular control area and corresponding criterion may not be relevant, and consequently, are not applicable. For example, when a token issuer does not outsource any aspect of the token operations to a vendor or business partner, the vendor management control area may not be relevant.

> ***Note: Due to the evolving nature of the digital asset space, there may be situations in which other control objectives may be required that are not outlined in these criteria. Token issuers will need to evaluate their specific risks based on individual facts and circumstances.***

24. The implementation guidance in the right-hand column presents factors that may assist both the token issuer and the practitioner when they are evaluating whether controls were suitably designed and operating effectively to achieve the control objectives of token operations. The implementation guidance does not address all possible situations; therefore, users should carefully consider the facts and circumstances of the token issuer and its environment when applying the control objectives as criteria.

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens

Note: Due to the evolving nature of the digital asset space, there may be situations in which other control objectives may be required that are not outlined in these criteria. Token issuers will need to evaluate their specific risks based on individual facts and circumstances.

These criteria apply only to asset-backed fiat-pegged tokens and are intended only for the types of asset-backed tokens or scenarios addressed herein.

Token Generation and Management		
	Control objectives	*Implementation guidance*
SC1	*Controls provide reasonable assurance that tokens are minted and burned in a complete, accurate, and secure manner based on authorized requests and in accordance with the token issuer's terms.*	*Identifies Technical Components: A process is in place to identify technical components supporting token operations (for example, wallets, cryptographic keys, blockchains, smart contracts, and bridges).* *Assesses Relevance and Reliability of Technical Components: A process is in place to assess the relevance and reliability of technical components supporting token operations prior to the initial token launch and on a periodic or ongoing basis thereafter, as appropriate.* *Assesses Blockchain Information: A process is in place to assess information obtained from the blockchain(s) for accuracy and completeness.*[8] *Establishes, Implements, and Maintains Policies for Minting and Burning Activities: A process is in place to establish, implement, and maintain policies with respect to minting and burning activities (for example, minting approval or thresholds, fiat currency disbursement approvals or thresholds, automated minting, or burning) in accordance with token issuer's terms and relevant regulatory requirements.* *Codifies Smart Contract and/or Token Functions: A process is in place to codify, test, and approve functionality of smart contracts and/or the token functionality and configurations, enabling the token issuer to operate in accordance with the token issuer's terms and relevant regulatory requirements, prior to the initial token launch and on an ongoing basis.* *Performs Security Assessments: A process is in place to perform security assessments to identify potential security concerns or vulnerabilities and implement remedial actions, as necessary, to address identified concerns prior to the token launch and routinely thereafter, as well as during system modifications.* *Conducts Minting and Burning Activities Securely: A process is in place to securely execute authorized minting and burning activities.*

8 For additional information on relevance and reliability of information obtained from a blockchain, see AU chapter 5, "Considerations for existence, rights, and obligations of digital assets," in the practice aid Accounting for and Auditing of Digital Assets.

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
Token Generation and Management (continued)		
	Control objectives	Implementation guidance
SC2	Controls provide reasonable assurance that token quantity is completely and accurately recorded in the token issuer's books and records.	Records Activities Affecting Token Quantity: A process is in place to record all activities that increase or decrease the token quantity (for example, mints and burns) in the books and records. Determines Status and Records Nonredeemable Tokens: A process is in place to determine the status of nonredeemable tokens (that is, temporarily versus permanently nonredeemable), in accordance with the token issuer's terms and record them in the books and records. Compares On-Chain Token Quantity to Internal Records: A process is in place to compare on-chain token quantity to the token issuer's books and records. Identifies and Monitors Events and Occurrences: A process is in place to identify and monitor events or occurrences that may affect the token quantity or redeemable tokens outstanding (for example, unreliable consensus and security mechanisms). Note: In the event that the token issuer has outsourced controls related to this criterion to a service organization, it is critical that the token issuer designs and operates sufficient controls to demonstrate that they maintain the completeness and accuracy of the token issuer's books and records.

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
	Client Onboarding and Maintenance	
	Control objectives	*Implementation guidance*
SC3	*Controls provide reasonable assurance that new accounts and account modifications are authorized and processed in a complete and accurate manner, in accordance with client agreements.*	*Establishes Client Account Information: A process is in place to record client account information in accordance with client agreements prior to executing the initial transaction.* *Client account information may include the following:* • *Proof of client identity (for example, driver's license, government-issued ID)* • *Identification number (for example, Social Security number, taxpayer identification number)* • *Personal information (for example, phone number, email address, financial institutions, wallet addresses)* • *Other client information as required by token issuer policies (for example, information needed to meet regulatory requirements), as applicable* *Updates Client Account Information for Changes: A process is in place to record client account modifications in accordance with client agreements. Changes may be initiated by the token issuer (for example, if it is determined that a client's tokens are required to be time-locked, or a client's wallet address is required to be access-restricted). Other changes may be initiated by the client (for example, changes to financial institutions where funds will be deposited upon redemption of tokens).*

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
Client Transaction Processing		
	Control objectives	Implementation guidance
SC4	Controls provide reasonable assurance that cash receipts and disbursements from token purchases and redemptions are authorized and recorded completely, accurately, and timely in accordance with the token issuer's terms.	Establishes, Implements, and Maintains Token Issuer Purchase/ Redemption Policy and Procedures: Policies and procedures are defined, implemented, and maintained such that (1) users are informed of the token issuer's terms for purchases and redemptions, (2) requests for purchases and redemptions are fulfilled in a manner consistent with the token issuer's terms, and (3) updates to the token issuer's terms are communicated to clients. Processes Client Transactions: A process is in place to receive authorized requests for purchases and redemptions and process related cash receipts and disbursements from/to the established client account. Note: See SC3, "Controls provide reasonable assurance that new accounts and account modifications are authorized and processed in a complete and accurate manner, in accordance with client agreements," for controls over the corresponding account setup and modification activities that make sure new accounts and account modifications are completely and accurately processed in accordance with client agreements. Records Processed Transactions: A process is in place to record transactions on the blockchain and in the token issuer's books and records to the appropriate client account in accordance with the token issuer's terms and relevant regulatory requirements as applicable. Note: See SC1, "Controls provide reasonable assurance that tokens are minted and burned in a complete, accurate, and secure manner based on authorized requests and in accordance with the token issuer's terms," for controls over the corresponding minting and burning activities that make sure the transactions (between fiat currency and tokens) are completely and accurately processed in accordance with the token issuer's terms. Compares Purchases and Redemptions: A process is in place to compare the token issuer's books and records related to purchases and redemptions to corresponding bank activity. For example: • Receipts: Cash receipts (and the minted and/or issued tokens) to corresponding bank activity • Redemptions: Cash disbursements (and the redeemed tokens) to corresponding bank activity

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
Key and Backup Management		
	Control objectives	Implementation guidance
SC5	Controls provide reasonable assurance that cryptographic key material is generated, distributed, stored, used, rotated, retired or destroyed (as applicable), and backed up in a secure and confidential manner.	Establishes, Implements, and Maintains Policies and Procedures for Cryptographic Keys: Policies and procedures are defined, implemented, and maintained related to the key management life cycle. The policies and procedures may consider the following: • How risks related to key generation are identified and mitigated. This includes consideration of how the location of the key generation is secured (for example, physical and logical access to where key generation ceremony occurs), ensuring keys are generated with sufficient entropy, criteria for aborting the key generation, and a process for documenting new keys. • How keys are tracked and distributed (for example, physical and logical access, location). • How keys are protected from unauthorized disclosure or discovery throughout the generation and initial storage processes. • Hardware and software to be used. • How keys are securely stored. • When keys are used and how their use is authorized. • How and when keys are rotated. • Timing and method of key retirement or destruction as applicable. • Security and confidentiality of key backups. • Timing of use of backup key rather than generating a new key. • How segregation of duties is addressed throughout each stage of the key management life cycle. • Protocols for responding to key compromises in order to protect the integrity and security of the tokens in a timely manner. Monitors Key Management Life Cycle Activities: A process is in place to monitor the key management life cycle activities, for example: • Chain of custody of hardware and software used for key storage • Maintenance of keys in accordance with the token issuer's policy, including rotation of keys within specified time frame • Key storage locations, environments, and authorized access • Authorization requirements for key use • Key usage and triggers for retirement or destruction as applicable • Material on which the backup keys are stored and the time frame to regenerate backup keys on the current material • Review of wallet systems and configurations • External factors that may drive the need for key rotation events

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
Redemption Asset Management		
	Control objectives	Implementation guidance
SC6	Controls provide reasonable assurance that redemption assets are maintained in accordance with the token issuer's terms.	Establishes, Implements, and Maintains Investment Policies: Investment policies are established, implemented, and maintained with respect to the permitted (that is, in accordance with token issuer's terms and relevant regulatory requirements) composition of redemption assets (for example, cash and cash equivalents [including U.S. Treasuries], money market funds, repurchase agreements, and other investments) and asset valuation methodology (for example, fair value, net asset value, par). Establishes and Maintains Counterparty Risk Management Processes: A process is in place to establish and maintain processes to manage risk related to counterparties who hold redemption assets or manage redemption asset accounts. For example, establishing counterparty selection criteria and counterparty agreements (including account type and ownership/beneficiary structure), evaluating the financial health and solvency of the counterparty, and identifying counterparty concentrations. (See the vendor management control area for application of these processes.) Segregates Redemption Assets: A process is in place to segregate redemption assets from the token issuer's assets based on account type (that is, custodial or noncustodial) and identify restrictions placed on their use (for example, right to transfer, sell, loan, or rehypothecate assets). Records Redemption Assets: A process is in place to record redemption assets on the token issuer's books and records. Compares Custodian Holdings to Books and Records: A process is in place to compare redemption asset holdings by the custodian with the token issuer's books and records. Values Redemption Assets: A process is in place to value redemption assets in accordance with the token issuer's terms. Manages Redemption Assets: A process is in place to manage compliance with asset-backing thresholds (for example, stress-testing and scenario analysis, daily or real-time reconciliation of token supply to reserve asset balances) and investment types in accordance with the token issuer's terms and relevant regulatory requirements as applicable. Mitigates Risk of Loss: A process is in place to manage mechanisms, if any, to mitigate risk of loss of redemption assets (for example, insurance, account segregation, trust structures, credit default swaps). Establishes Authorization Requirements Over Use of Redemption Assets: A process is in place to establish authorization requirements over the use of redemption assets (for example, segregation of duties or other elements of authorization and access to the redemption assets). Monitors Redemption Assets and Custodians: A process is in place to monitor redemption assets and custodians to identify threats to asset redeemability (for example, declining asset quality or financial instability of asset custodians).

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
	Vendor Management	
	Control objectives	***Implementation guidance***
SC7	***Controls provide reasonable assurance that risks associated with vendors and business partners relevant to the token operations are identified, assessed, and managed by the token issuer.***	***Establishes Requirements for Vendor and Business Partner Engagements: A process is in place to establish specific requirements for vendor and business partner engagements and changes to these engagements, including (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.*** ***Identifies and Evaluates Vulnerabilities: A process is in place to identify and evaluate vulnerabilities arising from vendor and business partner relationships and changes to these relationships, including third-party access to the token issuer's IT systems and connections with third-party networks.*** ***Assesses Vendor and Business Partner Risks: A process is in place to assess risks arising from relationships with vendors and business partners (and those entities' vendors and business partners, as applicable) and to inventory, tier, and assess the vulnerability of the token issuer's objectives to those risks. Examples of risks arising from relationships with vendors and business partners include those arising from their (1) financial failure; (2) security vulnerabilities, including those related to cryptographic key management; (3) operational disruption; and (4) failure to meet business or regulatory requirements.*** ***Assigns Responsibility and Accountability for Managing Vendors and Business Partners: A process is in place to assign one or more individuals responsibility and accountability for the management of risks and changes to services associated with vendors and business partners.*** ***Establishes Communication Protocols for Vendors and Business Partners: A process is in place to establish communication and resolution protocols for service or product issues related to vendors and business partners.*** ***Establishes Exception Handling Procedures for Vendors and Business Partners: A process is in place to establish exception handling procedures for service or product issues related to vendors and business partners.*** ***Assesses Vendor and Business Partner Performance: A process is in place to assess the performance of vendors and business partners as frequently as warranted, based on the risk associated with the vendor or business partner.*** ***Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments: A process is in place to implement procedures for addressing issues identified with vendor and business partner relationships.*** ***Implements Procedures for Terminating Vendor and Business Partner Relationships: A process is in place to implement procedures for terminating vendor and business partner relationships based on predefined considerations. Those procedures may include safe return of data and its removal from the vendor or business partner system.*** ***Note: Certain implementation guidance presented in this control area has been aligned to the points of focus in CC9.2 in the "Risk Mitigation" section of the* 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022) *(trust services criteria).***

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
	Reporting	
	Control objectives	*Implementation guidance*
SC8	*Controls provide reasonable assurance that token quantity, redemption asset information, and related disclosures used to support reporting by the token issuer are complete and accurate.*	*Discloses Redeemable Tokens Outstanding: A process is in place to accurately and completely disclose the amount of redeemable tokens outstanding, including:* • *Identification of the in-scope total natively minted token quantity that reflects how the token quantity is measured and includes disclosure of the distributed ledger or blockchain networks and smart contracts* • *The amount of redeemable tokens outstanding in both in-scope distributed ledgers and blockchain networks* • *Differences between total in-scope natively minted token quantity and redeemable tokens outstanding (for example, temporarily time-locked or permanently access-restricted)* *Discloses Available Redemption Asset Details: A process is in place to completely and accurately disclose the composition of available redemption assets by asset type, including geographic location, amount or value, maturity dates, and terms (for example, limitations on redemptions).* *Discloses Comparison of Available Redemption Assets to Redeemable Tokens Outstanding: A process is in place to disclose the comparison of available redemption assets to the redeemable tokens outstanding, including the following:* • *The value of available redemption assets and the redeemable tokens outstanding, including any surplus or deficit as reflected in supporting records* • *The redemption asset requirements for the asset-backing level reflected in established agreements and regulatory requirements, if applicable* • *The amount of cash receipts for unprocessed purchase requests or the amount of expected cash disbursements for unprocessed redemption requests reflected in supporting records*

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
	Reporting (continued)	
	Control objectives	***Implementation guidance***
		Identifies and Discloses Other Information: A process is in place to identify and disclose other information that may affect the amount of redeemable tokens outstanding or amount of redemption assets, for example: • ***Any known unresolved events or occurrences that have materially affected the natively minted token quantity or redeemable tokens outstanding*** • ***Descriptions of the methods used to measure the value of redemption assets by asset type*** • ***Type of counterparties holding redemption assets (for example, FDIC-insured bank) and the jurisdiction (regulatory or geographic) of the counterparty and related parties, as applicable*** • ***Redemption asset arrangements, including the nature of the arrangement between the token issuer and the counterparty, the value of the redemption assets subject to each type of arrangement, and any restriction on the use of the redemption assets*** • ***Whether the token issuer has direct contractual mechanisms to mitigate risk of loss of redemption assets, and if so, a description of the nature and extent of such mechanisms*** • ***Events or transactions that have a material effect occurring after the measurement point in time and up to the date of the token issuer's report*** • ***Litigation, claims, and assessments that may have a material impact*** • ***Market, operational, technological, and regulatory events that may materially affect the token issuer's ability to perform token redemptions based on token issuers terms*** • ***Existence and nature of any commitments that may materially affect the available redemption assets*** • ***Token issuer's regulatory jurisdiction***

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
IT General Controls		
Information Security		
	Control objectives	Implementation guidance
SC9	Controls provide reasonable assurance that logical access to programs, data, and computer resources relevant to token operations is restricted to authorized and appropriate users and that such users are restricted to performing authorized and appropriate actions.	Identifies and Authenticates Users: The token issuer identifies and authenticates persons, infrastructure, and software prior to accessing information assets, whether locally or remotely. The token issuer uses more complex or advanced user authentication techniques (for example, phishing-resistant multifactor authentication) when such protections are deemed appropriate based on its risk-mitigation strategy. Creates Access Credentials to Protect Information Assets: Credentials for accessing protected information assets are created based on an authorization from the system's asset owner or authorized custodian. Authorization is required for the creation of all types of credentials of individuals (for example, employees, contractors, vendors, and business partner personnel), systems, and software. Reviews Validity of Access Credentials: Access credentials are reviewed on a periodic basis for validity (for example, employees, contractors, vendors, and business partner personnel) and inappropriate system or service accounts. Prevents the Use of Credentials When No Longer Valid: Processes are in place to timely disable, destroy, or otherwise prevent the use of access credentials when no longer valid. Reviews Access Roles and Rules: The appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals (for example, employees, contractors, vendors, business partner personnel) and inappropriate system or service accounts. Access roles and rules are modified as appropriate. Uses Access Control Structures: Access control structures (for example, role-based access controls) are used to restrict access to protected information assets, limit privileges, and support segregation of incompatible functions. Uses Encryption to Protect Data: The token issuer uses encryption with appropriate strength to protect data (at rest, during processing or in transmission) when such protections are deemed appropriate based on the entity's risk mitigation strategy. Note: Certain implementation guidance presented in this control area has been aligned to the points of focus in CC6.1, CC6.2, and CC6.3 in the "Logical and Physical Access Controls" section of the trust services criteria.

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
IT General Controls		
Information Security (continued)		
	Control objectives	Implementation guidance
SC10	Controls provide reasonable assurance that physical access to computer and other resources relevant to token operations is restricted to authorized and appropriate personnel.	Creates or Modifies Physical Access: A process is in place to create or modify physical access by employees, contractors, vendors, and business partner personnel to facilities (for example, cryptographic key storage locations, data centers, office spaces, and work areas), based on appropriate authorization. Removes Physical Access: Processes are in place to remove physical access to facilities and protect information assets when an employee, contractor, vendor, or business partner no longer requires access. Recovers Physical Devices: Processes are in place to recover devices (for example, smart cards, badges, laptops, and mobile devices) when an employee, contractor, vendor, or business partner no longer requires access. Reviews Physical Access: Processes are in place to periodically review physical access to help ensure consistency with job responsibilities. Removes Data and Software for Disposal: Procedures are in place to remove, delete, or otherwise render data and software inaccessible from physical assets and other devices owned by the token issuer, its vendors, and employees when the data and software are no longer required on the asset or when the asset will no longer be under the control of the token issuer. Note: Certain implementation guidance presented in this control area has been aligned to the points of focus in CC6.4 and CC6.5 in the "Logical and Physical Access Controls" section of the trust services criteria.

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
IT General Controls		
Change Management		
	Control objectives	Implementation guidance
SC11	Controls provide reasonable assurance that development of and changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete and accurate processing and reporting of transactions and balances relevant to token operations.	Manages Changes Throughout the System Life Cycle: A process for managing system changes throughout the life cycle of the system and its components (data, software, and manual and automated procedures) is used to support the achievement of token issuer objectives. Authorizes Changes: A process is in place to authorize system and architecture changes prior to design, development, or acquisition and configuration. Designs and Develops Changes: A process is in place to design and develop system changes in a secure manner to support the achievement of token issuer objectives. Documents Changes: A process is in place to document system changes to support ongoing maintenance of the system and to support internal and external users in performing their responsibilities. Tracks System Changes: A process is in place to track system changes prior to implementation. Configures Software: A process is in place to select, implement, maintain, and monitor configuration parameters used to control the functionality of developed and acquired software. Tests System Changes: A process is in place to test internally developed and acquired system changes prior to implementation into the production environment. Examples of testing may include unit, integration, regression, static and dynamic application source code, quality assurance, or automated testing (whether point-in-time or continuous). Approves System Changes: A process is in place to approve system changes prior to implementation. Deploys System Changes: A process is in place to implement system changes with consideration of segregation of responsibilities (for example, restricting unilateral code development or testing and implementation by a single user, ensuring that only authorized changes are moved to production) to prevent or detect unauthorized changes. Identifies and Evaluates System Changes: Objectives affected by system changes are identified, and the ability of the modified system to support the achievement of the objectives is evaluated throughout the system development life cycle. Identifies Changes in Data, Software, and Procedures Required to Remediate Incidents: Changes in data, software, and procedures required to remediate incidents are identified, and the change process is initiated upon identification.

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
IT General Controls		
Change Management (continued)		
	Control objectives	Implementation guidance
		Creates Baseline Configuration of IT Technology: A baseline configuration of IT and control systems is created and maintained. *Provides for Changes Necessary in Emergency Situations: A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent time frame).* *Manages Patch Changes: A process is in place to identify, evaluate, test, approve, and implement patches on software in a timely manner.* *Monitors Proposed Blockchain Changes: A process is in place to identify planned blockchain changes that could affect token functionality or result in the need to modify internal systems or processes.* *Note: Certain implementation guidance presented in this control area has been aligned to the points of focus in CC8.1 in the "Change Management" section of the trust services criteria.*
SC12	*Controls provide reasonable assurance that network infrastructure is configured as authorized to* (a) *support the effective functioning of application controls to result in valid, complete, and accurate processing and reporting of transactions and balances relevant to token operations and* (b) *protect data relevant to token operations from unauthorized changes.*	*Manages Changes Throughout the System Life Cycle: A process for managing system changes throughout the life cycle of the system and its infrastructure is used to support the achievement of token issuer objectives.* *Identifies Changes in Infrastructure Required to Remediate Incidents: Changes in infrastructure required to remediate incidents are identified, and the change process is initiated upon identification.* *Creates Baseline Configuration of IT Technology: A baseline configuration of IT and control systems is created and maintained.* *Manages Patch Changes: A process is in place to identify, evaluate, test, approve, and implement patches on infrastructure in a timely manner.* *Protects Data: The ability to modify data is restricted to only authorized personnel, and data modifications are approved.* *Note: Certain implementation guidance presented in this control area has been aligned to the points of focus in CC8.1 in the "Change Management" section of the trust services criteria.*

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
IT General Controls		
Computer Operations		
	Control objectives	Implementation guidance
SC13	Controls provide reasonable assurance that application and system processing relevant to token operations are authorized and executed in a complete and accurate manner, and deviations, problems, and errors that may affect token operations are identified, tracked, recorded, and resolved in accordance with the token issuer's terms.	Approves Changes to Production Processor Scheduler/Orchestration Tool: Appropriate documented approvals are required before modifications are made to the job scheduler tool or the schedule, for example, a change ticket that includes relevant information such as the following: • Install date and time • Description of the job • System affected • Instructions for executing the change Approves Changes to Schedule: Additions and changes to scheduled production jobs and scheduling definitions are requested and approved before being made (for example, through formal ticket initiation and/or management tool). Testing is performed to assess the impact to the permanent job schedule and jobs with dependencies before additions and changes are approved. Approves Nonscheduled Changes to Production Processing: Changes related to production processing specifications (for example, ad hoc or one-time code changes to production batch jobs) are approved prior to production implementation. Evidence of the change and approval is fully documented. Identifies Production Incidents: The production environment is monitored for incidents. The incidents are identified, researched, and resolved in a timely manner. Monitors Uptime and Security Status: A process is in place to monitor uptime and security status of technical components, including during minting and burning activities.

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
IT General Controls		
Computer Operations (continued)		
	Control objectives	Implementation guidance
SC14	Controls provide reasonable assurance that data transmissions between the token issuer and its clients and other outside entities that affect token operations are from authorized sources and are complete, accurate, and secure.	Restricts the Ability to Perform Transmission: Data-loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement, and removal of information (for example, mint and burn requests, on-chain transactions, monthly statements, transactions and balances, or private key materials are not extractable). Uses Encryption Technologies or Secure Communication Channels to Protect Data: Encryption technologies with appropriate strength or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points. Supports Data Transmissions: A process is in place to support the completeness and accuracy of data transmissions (for example, data validity checks, the use of digital signatures, monitoring procedures, or reconciliation controls). Protects Removable Media: Encryption technologies with appropriate strength and physical asset protections are used for removable media (for example, USB drives and backup tapes) as appropriate. Protects Endpoint Devices: Processes and controls are in place to protect endpoint devices (for example, mobile devices, laptops, desktops, and sensors). Note: Certain implementation guidance presented in this control area has been aligned to the points of focus in CC6.7 in the "Logical and Physical Access Controls" section of the trust services criteria.

Proposed Criteria for Controls Over Token Operations: Specific to Asset-Backed Fiat-Pegged Tokens		
IT General Controls		
Computer Operations (continued)		
	Control objectives	Implementation guidance
SC15	Controls provide reasonable assurance that data relevant to token operations is backed up regularly and is available for restoration in the event of processing errors or unexpected processing interruptions.	Considers System Resilience: System resilience is considered in the design of systems, and resilience is tested during development to help make sure the token issuer has the ability to respond to, recover from, and resume operations through significant disruptions. Determines Data Requiring Backup: Data is evaluated to determine whether backup is required. Performs Data Backup: Procedures are in place for backing up data, monitoring to detect backup failures, and initiating corrective action when such failures occur. Addresses Offsite Storage: Backup data is stored in a location at a distance from its principal storage location sufficient so that the likelihood of a security or environmental threat event affecting both sets of data are reduced to an appropriate level. Implements Alternate Processing Infrastructure: Measures are implemented for migrating token operations to alternate infrastructure in the event that normal processing infrastructure becomes unavailable. Measures may include geographic separation, redundancy, and failover capabilities for components. Considers Data Recoverability: Threats to data recoverability (for example, ransomware attacks) that could impair the availability of the token operations and related data are identified and mitigation procedures are implemented. Tests Integrity and Completeness of Backup Data: The integrity and completeness of backup information is tested on a periodic basis. See SC1, "Controls provide reasonable assurance that tokens are minted and burned in a complete, accurate, and secure manner based on authorized requests and in accordance with the token issuer's terms," for controls related to evaluating the reliability of blockchains, smart contracts, bridges, and technical components, and monitoring the uptime of those components, which are an integral part of controls related to system resilience. See SC5, "Controls provide reasonable assurance that cryptographic key material is generated, distributed, stored, used, rotated, retired or destroyed (as applicable), and backed up in a secure and confidential manner," for controls related to cryptographic key backups that are an integral part of controls over the availability of data relevant to token operations. Note: Certain implementation guidance presented in this control area has been aligned to the points of focus in CC8.1 in the "Change Management" section and A1.2 and A1.3 in the "Availability" section of the trust services criteria.

Effective date

25. The criteria may be used upon issuance.

Exhibit A:

An Illustrative Presentation and Disclosure of the Token Issuer's Redeemable Tokens Outstanding and Related Information

The following disclosure [*FP1*, *FP2*, *FP8a*, *FP8b*, *FP8c* and *FP8e*] is for illustrative purposes only and includes the following types of tokens as defined by the token issuer's terms. Disclosure of the tokens outstanding issued on in-scope distributed ledgers or blockchain networks may be presented individually by network, or in the aggregate.

- Temporary nonredeemable tokens include the following:
  - Temporarily access-restricted
  - Time-locked (become unlocked on XX/XX/XXXX)
- Permanent nonredeemable tokens include the following:
  - Permanently access-restricted

If facts and circumstances differ, modify this table as appropriate.

	Blockchain ABC[6, 7]	Blockchain DEF[8, 9, 10]	Blockchain GHI[11,12]	Total
Total natively minted tokens quantity [*FP1a*]	XXX,XXX,XXX	XXX,XXX,XXX	XXX,XXX,XXX	XXX,XXX,XXX
Less temporary nonredeemable tokens:[1] [*FP1c*]				
Temporarily access-restricted[2]	(XXX,XXX)		(XXX,XXX)	(XXX,XXX)
Time-locked[3]	(XXX,XXX)			(XXX,XXX)
Less permanent nonredeemable tokens:[4] [*FP1c*]				
Permanently access-restricted	(XXX,XXX)			(XXX,XXX)
Total nonredeemable tokens	(XXX,XXX)		(XXX,XXX)	(XXX,XXX)
Total redeemable tokens outstanding[5, 9] [*FP1b*]	XXX,XXX,XXX	XXX,XXX,XXX	XXX,XXX,XXX	XXX,XXX,XXX

[1] Consistent with the definition in the token issuer's terms, temporary nonredeemable tokens are currently not redeemable; however, they may become redeemable at a future point in time and therefore have corresponding redemption assets. (See exhibit C for the comparison between the redemption assets and the redeemable tokens outstanding, which includes a reconciliation for the temporary nonredeemable tokens.) [*FP1c*]

[2] Tokens are associated to addresses that are restricted due to a review of [*Description of item reviewed*]. The restriction may be removed pending results of such review. [*FP1c*].

[3] Time-locked tokens become unlocked on XX/XX/XXXX. [*FP1c*]

[4] Consistent with the definition in the token issuer's terms, permanently nonredeemable tokens will never become redeemable and therefore do not have corresponding redemption assets. [*FP1c*]

[5] The token issuer is in [*Description of regulatory jurisdiction*], which has affected the redemption process by [*Description of impact*]. [*FP8e*]

[6] Blockchain ABC refers to the smart contract running on ABC at 0x0000000000. [*FP1a*]

[7] On XX/XX/XXXX, the ABC blockchain experienced a hard fork, splitting the ABC blockchain into two versions. Redemptions will be honored on version 1, which inherits the total circulating supply of tokens and the ledger history prior to the hard fork at block height XXX. Redemptions will not be supported for tokens issued on version 2. Tokens issued on version 2 are considered out of scope and will not contribute to the total redeemable token balance. [*FP8a*]

[8] Blockchain DEF refers to the smart contract running on DEF at 0x00000000. [*FP1a*]

[9] As of the report date, the token issuer had outstanding litigation with a custodian that resulted in the token issuer not being able to redeem X amount of tokens. [*FP8b*]

[10] On XX/XX/XXXX [*Description of event*] occurred on DEF blockchain that involved [*Name of service provider*] that resulted in the inability to redeem XX tokens on demand, which affected the token issuer's ability to perform token redemption in accordance with its terms. [*FP8c*].

[11] Blockchain GHI refers to the smart contract running on GHI at 0x0000000. [*FP1a*]

[12] On XX/XX/XXXX this blockchain [*Description of event*] and [*Details of impact on report*]. [*FP1d*]

Note: Policies and procedures are defined, implemented, and maintained such that authorized token holders are informed of the token issuer's terms for purchases and redemptions. [*FP2*]

Exhibit B:

An Illustrative Presentation and Disclosure of the Redemption Assets Available for Redeemable Tokens Outstanding and Related Information

The following disclosure is for illustrative purposes only. If facts and circumstances differ, modify these tables as appropriate.

The following table summarizes redemption assets by asset type [*FP3*, *FP4*, *FP5*, *FP6*, and *FP8d*]:

	As of [Month, day, year]
Cash and cash equivalents, at par	$X,XXX[1]
Money market funds, at net asset value	X,XXX
Repurchase agreements, at fair value	X,XXX
Obligations of U.S. Treasury, at fair value	X,XXX
Total	**$X,XXX**

[1] As of the date of this report, $XXX,XXX of redemption assets have been pledged as security for a borrowing arrangement based on the token issuer's terms. [*FP8d*]

Cash and cash equivalents at par [*FP4b*]. Cash and cash equivalents consist of cash on hand and investments with maturities of three months or less from the date of purchase. The majority of the Company's cash is held at major commercial banks [*FP3*], which at times may exceed the Federal Deposit Insurance Corporation (FDIC) limit of $250,000 [*FP6*]. As of [*Date*], uninsured FDIC demand deposits at major commercial banks totaled $X,XXX. The Company has obtained private uninsured deposit insurance with a(n) [[A++ A.M. Best][AAA Moody's][AAA Standard & Poor's][AAA Fitch]] rated provider of insurance services with a nationwide presence in the amount of $X,XXX [*FP6*]. The following table summarizes cash and cash equivalents by type of account, regulatory agency, and geographic location:

Cash and cash equivalents

Type of account [*FP5*]	Regulatory agency	Geographic location [*FP4a*]	Amount [*FP4a*]
Demand deposit	Regulatory Agency 1 (for example, federally chartered bank)	United States	$X,XXX
For the benefit of authorized token holders	Regulatory Agency 2	United States	X,XXX
Trust account	Regulatory Agency 3	United States	X,XXX
Total			**$X,XXX** (should agree to the redemption assets by type table)

- *Money market funds at net asset value* [*FP4b*]. Money market funds hold investments in cash, cash equivalents, and short-term debt securities. The following table summarizes money market funds by fund, at net asset value:

Money market funds

CUSIP [*FP4a*]	Maturity date [*FP4a*]	Net asset value [*FP4a*]
123456XX7	XX/XX/XX	$X,XXX
234567XX8	XX/XX/XX	X,XXX
Total		**$X,XXX** (should agree to the redemption assets by type table)

Repurchase agreements at fair value [*FP4b*]. Repurchase agreements are agreements with selected commercial banks and broker-dealers [*FP3*], under which the Company acquires securities as collateral (debt obligation) subject to an obligation of the counterparty to repurchase and the Company to resell the securities (obligation) at an agreed-upon time and price. The Company, through a custodian or a sub-custodian, receives delivery of the underlying securities collateralizing repurchase agreements. The following table summarizes the remaining contractual maturity of the agreements by counterparty at fair value:

Repurchase agreements						
Counterparty [*FP3*]	Collateral[1]	Coupon rate	Purchase date	Maturity date [*FP4a*]	Par	At fair value [*FP4a*]
Counterparty ABC	[*Description of collateral, for example, "Obligations of U.S. Treasury and federal agencies"*]	X.XX%	XX/XX/XX	XX/XX/XX	$XX,XXX	$XX,XXX
Counterparty DEF	[*Description of collateral*]	X.XX%	XX/XX/XX	XX/XX/XX	XX,XXX	XX,XXX
Total repurchase agreements						**$XX,XXX** (should agree to the redemption assets by type table)

Obligations of U.S. Treasury, at fair value [*FP4b*]. Obligations of U.S. Treasury are held by a qualified custodian and are in the amount of $X,XXX.

Obligations of U.S. treasury

The fair value of obligations of the U.S. Treasury are $X,XXX with a 91–180 day contractual maturity, and $X,XXX with a 181-day to 1-year contractual maturity. Expected maturities may differ from contractual maturities if borrowers have the right to call or prepay obligations with or without call or prepayment penalties [*FP4a*].

[1] Fair value of collateral may be disclosed if relevant to the report.

Exhibit C:

An Illustrative Presentation and Disclosure of the Comparison of the Redemption Assets Available for Redeemable Tokens Outstanding and the Token Issuer's Redeemable Tokens Outstanding, and Related Information of the Comparison

The following report [*FP7*] is for illustrative purposes only and includes the following types of tokens as defined in the token issuer's terms:

- For each redeemable token outstanding there is $1 (or an equivalent of U.S. denominated amounts) available for redemption
- Timing differences, which include the following:
  - — Tokens purchased but not yet minted
  - — Tokens redeemed but not yet paid
- Temporary differences, which include the following:
  - — Access-restricted tokens
  - — Time-locked tokens (become unlocked on XX/XX/XXXX)

If facts and circumstances differ, modify this report as appropriate.

Note: [*The terms as of XX/XX/XXXX or Version X of the terms*] were used to prepare the following comparison.

	Total
Redemption assets [*FP7a*]	**$XXX,XXX,XXX**
Less: Amount of redeemable tokens outstanding[1] [*FP7a*]	XXX,XXX,XXX
Subtotal prior to timing difference	**$XXX,XXX**
Timing differences: [*FP7c*]	
Tokens purchased but not yet minted	$(XX,XXX)
Tokens redeemed but not yet paid[2]	$(XX,XXX)
Subtotal prior to temporary difference	**$XXX,XXX**
Temporary differences:[3]	
Access-restricted tokens[4]	(XX,XXX)
Time-locked tokens[5]	(XX,XXX)
Surplus (Deficit)[6] [*FP7a*]	**$X,XXX**

[1] The amount of redeemable tokens outstanding includes requests for purchases and redemptions that have not yet been processed due to timing differences. [*FP7c*]

[2] None of the unprocessed redemptions have exceeded the period pursuant to the token issuer's terms for the delivery of redemption assets. [*FP7c*]

[3] Consistent with the token issuer's terms, temporary differences relate to tokens that are not redeemable at the measurement point in time but may be redeemable in the future and have redemption assets backing them. These tokens are not included in the redeemable token outstanding balance. (See exhibit A). [*FP1c*]

[4] Tokens are associated to addresses that are restricted due to a review of [*Description of item reviewed*]. The restriction may be removed pending results of such review. [*FP1c*]

[5] Time-locked tokens become unlocked on XX/XX/XXXX. [*FP1c*]

[6] The token issuer's terms stipulate that for each redeemable token outstanding there is $1 available (or an equivalent of U.S. denominated amounts) for redemption. This surplus indicates that asset-backing levels are in accordance with token issuer's terms. [*FP7b*]

Glossary

Note: ~~**These t**~~ ***T***erms ***in this glossary encompass applicable terms from both*** ~~**are included in**~~ the *Blockchain Universal Glossary* ***and the*** **2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)** ~~**along with additional terms related to blockchain and digital assets**~~.

access-restricted tokens. Tokens associated with wallet addresses that may be temporarily or permanently restricted from redemption with the token issuer.

architecture. The design of the structure of a system, including logical components, and the logical interrelationships of computers, operating systems, networks, or other elements, whether internally or externally hosted.

asset-backed tokens. Digital assets whose redemption is supported by other assets (for example, fiat currency, commodities, or other digital assets).

authentication. The process of verifying the identity or other attributes claimed by or assumed of a token issuer (user, process, or device) or to verify the source and integrity of data.

authorization. The process of granting access privileges to a user, program, or process by a person who has the authority to grant such access.

bridged tokens. The application of wrapping a token for use on blockchains for which the tokens were not natively minted by the issuer.

burned tokens (burning). Tokens destroyed by the issuer, typically in conjunction with redemption.

business partner. An individual or business (and its employees), other than a vendor, that has some degree of involvement with the token issuer's business dealings or agrees to cooperate, to any degree, with the token issuer.

client. An individual or entity who has signed a client agreement with the token issuer.

controls. Policies and procedures that are part of the token issuer's system of internal control. The objective of a token issuer's system of internal control is to provide reasonable assurance that principal system objectives are achieved.

criteria. The benchmarks used to measure or evaluate the subject matter (for example, suitability of design and operating effectiveness of internal controls supporting token operations).

design. As used in the COSO definition of internal control, the internal control system design is intended to provide reasonable assurance of the achievement of a token issuer's objectives.

disclosure. The provision of access to or the release, transfer, or divulging in any other manner of information outside the token issuer holding the information. Disclosure is often used interchangeably with the terms sharing and onward transfer.

disposal. A phase of the data life cycle that pertains to how a token issuer removes or destroys data, information, or equipment/devices storing such data and information.

endpoint devices. Connected hardware or virtual devices that communicate across a network (for example, mobile devices, laptops, desktops, and sensors).

environmental. Of or having to do with the matters that can damage the physical elements of information systems (for example, fire, flood, wind, earthquake, power surges, or power outages). A token issuer implements controls and other activities to detect, prevent, and manage the risk of casualty damage to the physical elements of the information system from environmental elements.

external users. Users, other than token issuer personnel, who are authorized by token issuer management, customers, or other authorized persons to interact with the token issuer's information system.

fiat-pegged token. A common type of asset-backed token, which is pegged to the value of fiat currency (for example, the U.S. dollar). Also may be referred to as a stablecoin. See asset-backed tokens; stablecoins.

information assets. Data and the associated software and infrastructure used to authorize, process, transmit, and store information.

infrastructure. The collection of physical or virtual resources that supports an overall IT environment, including the server, storage, network elements, and endpoint devices.

issuing tokens. The process of sending minted tokens to a token purchaser and placing them in circulation.

measurement point in time. The date and time at which the subject matter is being measured or determined.

minted tokens (minting). Tokens created by the issuer that reside on a distributed ledger or blockchain network.

natively minted tokens. Tokens that have been minted on blockchains and that have not been bridged from other blockchains or networks.

nonredeemable tokens. Tokens that cannot be redeemed with the token issuer at the measurement point in time or that are otherwise encumbered and not valid for redemption. Nonredeemable tokens may include, but are not limited to, time-locked tokens; pre-minted tokens; test tokens; bridged or wrapped tokens; and tokens that have been access-restricted. Tokens can be either temporarily or permanently nonredeemable. See measurement point in time; token issuer; pre-minted tokens; test tokens; bridged tokens; wrapped tokens; access-restricted tokens.

personal information. Information that is about, or can be related to, an identifiable individual.

policies. Management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures.

pre-minted tokens. Tokens that have been minted by a token issuer but not yet issued and are considered nonredeemable. See nonredeemable tokens.

redeemable tokens outstanding. The total of natively minted tokens less nonredeemable tokens. Also known as issued tokens that are in circulation. See natively minted tokens; nonredeemable tokens.

risk. The possibility that an event will occur and adversely affect the achievement of objectives.

service provider. A vendor (such as a service organization) engaged to provide services to the entity. Service providers include outsourced service providers as well as vendors that provide services not associated with business functions, such as janitorial, legal, and audit services.

software. A collection of instructions that tell a computer how to operate. Software may be both internally developed and purchased from vendors and can include both application software (for example, user applications and database management systems) and system software (for example, operating systems, drivers, utilities, programming software, and interfaces).

system. Refers to the infrastructure, software, procedures, and data that are designed, implemented, and operated by people to achieve one or more of the token issuer's specific business objectives in accordance with management-specified requirements.

test tokens. Minted tokens for which there are no associated redemption assets. These are used for the sole purpose of performing entity-related testing of the system for functionality and are considered nonredeemable. See nonredeemable tokens.

threat. Any circumstance or event arising from human actions or natural events that could potentially impair (a) the achievement of a token issuer's objectives, its assets, or activities of its personnel, or (b) other entities through unauthorized access, destruction, disclosure, modification of data, or denial of service.

time-locked tokens (locked tokens). Tokens that are subject to a restriction mechanism that locks the use of the token for a set time limit. Depending on the use, these tokens may or may not be redeemable.

token issuer. An entity managing token and redemption operations, such as minting, burning, issuing, and redeeming.

token quantity (token supply). The number of tokens that have been natively minted on a particular blockchain. See natively minted tokens.

vendor. An individual or business (and its employees) that is engaged to provide goods or services to the token issuer. Depending on the services provided (for example, if the vendor operates certain controls on behalf of the token issuer that are necessary to achieve the token issuer's objectives), it also might be a service provider.

vulnerability. Weakness in a component of a system, particularly information assets, system security procedures, internal controls, or implementation that could be exploited or triggered by human action or natural events.

wrapped tokens. Tokens that are separate and distinct tokenized versions of another digital asset. These may be used either on the same blockchain as the original digital asset or on a different blockchain.

aicpa-cima.com

Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe.