S&P Global
Ratings

Research

Analytical Approach: Vault Risk Assessments

October 4, 2026

This report does not constitute a rating action.

Primary Contacts

Andrew O'Neill, CFA
London
44-20-7176-3578
andrew.oneill
@spglobal.com

Lisa R Schroeer
Charlottesville
434-529-2862
lisa.schroeer
@spglobal.com

Anton Rassadkin
New York
1-332-297-3260
anton.rassadkin
@spglobal.com

Miguel de la Mata
New York
1-3037214478
miguel.de.la.mata
@spglobal.com

See complete contact list at end of article.

Overview And Scope

This article describes S&P Global Ratings' analytical approach for assessing risk in lending vaults. A lending vault is a smart contract that pools and allocates digital assets to provide liquidity to blockchain-based lending markets collateralized by crypto or tokenized real-world assets. Such vaults support secured and unsecured lending and can operate in environments that are permissioned, where access is restricted to verified and approved users; or permissionless, which are open to anyone with a digital wallet.

We use the term "vault" throughout this article in reference to the overall risk profile that a vault investor is exposed to, including intermediary dependencies and other smart contracts a vault may interact with, rather than a narrow reference to the vault smart contract itself.

Our Vault Risk Assessment (VRA) is a forward-looking and relative opinion about the overall risk of impairment to an investor's position in a lending vault. It indicates credit risks inherent in a vault's underlying assets and lending markets, while accounting for protocol and blockchain risks and the curator's ability and willingness to maintain the vault's risk profile. The VRA is applicable across lending-vault structures and strategies and is identified by the suffix 'v', for example 'AAA(v)', which indicates the lowest risk.

A VRA is not a credit rating or a commentary on yield levels. Unlike traditional credit ratings, a VRA does not address a vault's ability to meet payment obligations in full. A VRA is not intended as a guarantee of a vault's credit quality or an exact measure of its risk profile.

As new types of vaults emerge, our VRAs will use the key risk concepts in this document. The vault segment is nascent and evolving rapidly. We may use our analytical approach for existing vault types as a starting point for assessing novel vault characteristics and structures.

We will monitor our VRAs and update them periodically to reflect changes in our view of the relative risk associated with a particular vault. VRA updates could be triggered by, among other things, changes to assets that can be allocated to or from the vault, the risk profile of any assets, the smart contract's features, or the liquidity mismatch profile.

We may place a VRA under review. This may happen when material events or new information could reasonably result in a change to our VRA, or when we believe the existing VRA no longer accurately reflects the vault's current risk profile.

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

How lending vaults operate

Generally, lending vaults can invest in a defined list of eligible markets. Eligibility is governed by the vault's smart contract: A vault can only invest deposits in lending markets that are made eligible in its smart contract.

Each market comprises an asset pair: a lending asset (a deposit the vault receives and invests in lending markets) and a collateral asset (which secures lending). Generally, a vault's eligible asset pairs include a single lending asset and multiple collateral assets.

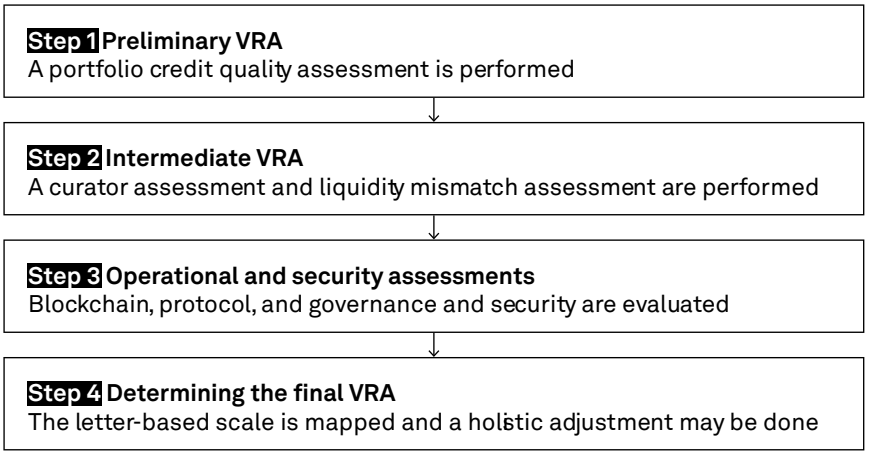
Lending in these markets is subject to liquidation loan-to-value (LTV) triggers: If a loan's LTV ratio exceeds its liquidation LTV threshold--either because the market value of the collateral asset has decreased, or interest has accrued on the loan balance--the collateral asset is liquidated to repay the loan.

The key risk for vaults lending in these markets is bad debt exposure. This is when liquidation proceeds are insufficient to fully repay loans that breach their liquidation LTV trigger, resulting in a loss to lenders in the market.

Summary Of Our VRA Analytical Approach

We determine a VRA in four steps (see chart).

Steps to a VRA



Source: S&P Global Ratings.
© 2026 Standard & Poor's Financial Services LLC.

Step 1: Establish a preliminary VRA by evaluating credit risks inherent in the assets and markets that a vault can allocate to. The result is a score on a scale of 1 to 6, with 1 denoting the lowest risk and 6 the highest risk.

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Step 2: Derive an intermediate VRA. This builds on the preliminary VRA with two additional assessments, which may cap the preliminary VRA:

- A curator assessment, reflecting our view of how a curator designs, manages, and controls the strategy of its vaults; and
- A liquidity mismatch assessment, reflecting our view on the extent to which a vault can reliably meet investors' withdrawal demands in a timely and value-preserving manner.

The intermediate VRA is expressed as a score on a scale of 1 to 6, with 1 denoting the lowest risk and 6 the highest risk. The intermediate VRA cannot be more than 2 points better than the curator risk score or the liquidity mismatch risk score.

Step 3: Operational and security assessments. These evaluate three critical dimensions of a vault's operational infrastructure and security:

- The blockchain, to assess the infrastructure's resilience, adoption, and technological maturity;
- Protocol risk, to assess the protocol's design, smart-contract integrity, and transparency; and
- Governance and security, to assess vault-level operational controls, security, and transparency measures.

Each of these assessments is expressed as a score on a scale of 1 to 6, with 1 denoting the lowest risk and 6 the highest risk.

This step caps the intermediate VRA at the highest risk score among the three operational and security assessments. This aims to ensure the most significant vulnerabilities are reflected.

Step 4: The final VRA. The intermediate VRA score, after any adjustments from step 3, is translated into a corresponding letter-based outcome. We may then adjust the outcome further to reflect factors not fully captured in our preliminary or intermediate analysis. For example, we may adjust the outcome if we see security or liquidity risks separate from those captured in steps 1 to 3. We may also adjust based on a comparable assessment analysis, in which we evaluate a vault's characteristics with those of other vaults with a similar portfolio strategy and composition. The result is the final VRA (see table 1).

Table 1

Vault Risk Assessment (VRA)*

VRA scale	Definition
AAA(v)	The vault's portfolio exhibits extremely low credit risk, with an extremely low likelihood of impairment of an investor's position, even under stressed market conditions.
AA(v)	The vault's portfolio exhibits very low credit risk, with a very low likelihood of impairment of an investor's position. Stressed conditions are very unlikely to materially affect an investor's position.
A(v)	The vault's portfolio exhibits low credit risk, with a low likelihood of impairment of an investor's position. Adverse conditions are unlikely to materially affect an investor's position.
BBB(v)	The vault's portfolio exhibits moderate credit risk. The likelihood of investor impairment is moderate, particularly during periods of market stress.
BB(v)	The vault's portfolio exhibits moderately high credit risk, with an elevated likelihood of impairment of an investor's position under reasonably foreseeable stressed market conditions.
B(v)	The vault's portfolio exhibits high credit risk, with a high likelihood of impairment of an investor's position under reasonably foreseeable stressed market conditions.
CCC(v)§	Assets within the vault have been impaired, but a credible remediation mechanism is expected to restore a material portion of the vault's assets within a reasonable time frame.

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Vault Risk Assessment (VRA)*

VRA scale	Definition
CC(v)§	Assets within the vault have been materially impaired, and recovery of a material portion of the vault's assets depends on uncertain and potentially legal insolvency, or other asset recovery proceedings or mechanisms.
D(v)§	Assets within the vault have been effectively and permanently impaired, with no credible path to meaningful recovery.

*A VRA expresses a forward-looking and relative opinion about the overall risk of impairment to an investor's position in a lending vault, from strongest to weakest, within our VRA scale. The VRA does not have +/- modifiers. §For vaults where loss has already crystallized. Source: S&P Global Ratings.

Vault Risk Assessment: Step By Step

Here we detail each of the four steps in determining a VRA.

Step 1: Preliminary VRA

The preliminary VRA is based on a portfolio credit quality assessment, which is intended to reflect the structural market risk of a vault's strategy rather than the vault's point-in-time composition. This assessment has two components:

- A market risk analysis, and
- Infrastructure risk analysis.

We assess the risk of each asset pair that a vault can allocate to on a scale of 1 (lowest risk) to 6 (highest risk). This asset-pair assessment covers both market risk factors and infrastructure risk factors that can contribute to the risk of bad debt exposure.

We then calculate a weighted average of these asset-pair assessments to determine the overall portfolio credit quality assessment. Since this calculation is not based on point-in-time allocation, we weight asset pairs using an assumption that a portfolio's composition may migrate toward its riskier eligible assets (see "Determining the stressed portfolio allocation" below).

The outcome of this step is the preliminary VRA, expressed as a score on a scale of 1 to 6, with 1 denoting the lowest risk, and 6 the highest risk. The preliminary VRA is generally equal to the weighted average portfolio credit quality assessment, rounded to the nearest integer.

We may adjust the preliminary VRA, in specific cases, to reflect risks not already captured in the asset-pair assessment. Examples of such risks include an illiquid lending asset, correlation effects between collateral assets, or correlation between a vault's collateral and lending assets, to the extent we view such risks as insufficiently reflected in the asset-pair assessment scores.

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Determining the stressed portfolio allocation

We consider the curator's track record of revising allocation targets through periods of significant inflows to and outflows from the vault. If target allocations are not provided, representative portfolio weights are inferred from disclosed allocation ranges or maximum allocation limits.

Where a range of portfolio compositions is allowed, we estimate a representative allocation that reflects the intended implementation rather than apply a hypothetical highest-risk allocation scenario. In forming this estimate, we consider the relative breadth of allocation limits, the vault's stated strategy, and any other information provided by the curator regarding the vault portfolio's composition.

Where there is insufficient information to estimate representative allocations with reasonable confidence, we align the preliminary VRA with the highest risk score among the vault's eligible assets.

A. Market risk analysis

For each eligible asset pair, we assess market risks that affect collateral liquidation, the timeliness of deleveraging, expected slippage, and loss realization during adverse market conditions.

Our analysis diverges for permissioned and permissionless liquidation mechanisms due to their differing risk factors:

- In permissionless environments, the focus is on the market's depth, economic incentives that support participation in the liquidation process, the liquidation mechanism's track record through times of stress, and investor-concentration risks.
- In permissioned environments, the focus is on the counterparties supporting the liquidation mechanism, their creditworthiness, and the sufficiency and strength of their contractual commitment to participate in liquidations.

1. Permissionless liquidation mechanisms: We first set an initial asset-pair assessment--the market risk anchor--on a scale of 1 to 6 (see table 2) to reflect our view of the market risk associated with a vault's asset pairs.

Table 2

Market risk anchor*

Risk score	Principles for asset categorization
1	Native gas tokens to the relevant layer 1 blockchain with broad reserve/collateral status and adoption, such as WETH (wrapped ether, the native gas token to the Ethereum blockchain)
2	The most liquid assets within the category of liquid staking tokens, such as the Lido protocol's wstETH token The most liquid assets within the category of wrapped bitcoin tokens, such as cbBTC (Coinbase wrapped bitcoin)
3	Less liquid assets within the categories of liquid staking tokens or wrapped bitcoin tokens
4	Crypto assets other than those listed above, with an established operational track record of trading on decentralized exchanges (DEX) and centralized exchanges (CEX)
5	Lower liquidity crypto assets without a track record of CEX and DEX trading
6	Assets that we consider represent higher risk than those described above, such as those with limited liquidity

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Market risk anchor*

Risk score	Principles for asset categorization

*On a scale of 1 to 6, with 1 denoting the lowest risk and 6 the highest risk, based on the asset-pair assessment. wstETh--Wrapped staked ETH. Source: S&P Global Ratings.

Exposure to other vaults: The VRA analytical approach does not apply to vaults whose investment strategy is primarily to invest in other vaults. If a vault's asset portfolio has a minority exposure to other vaults, we assign a market risk anchor to that exposure by considering its underlying assets and applying the principles in the table above.

Stablecoins as collateral assets: If a vault includes stablecoins as collateral assets, in determining the market risk anchor, we consider the stablecoins' liquidity across centralized (CEX) and decentralized (DEX) cryptocurrency markets, as well the risk of depegging from the target fiat currency (e.g. U.S. dollar). This is because depegging causes such stablecoins to lose their intended value, which may significantly reduce the vault's ability to liquidate them.

Our assessment of depegging risk is informed by our Stablecoin Stability Assessment, where available. If we have not assigned a Stablecoin Stability Assessment to a stablecoin used as collateral in a vault, we will assess depegging risk according to the principles of that analytical approach. We set the market risk anchor for stablecoins used as collateral as follows:

- For stablecoins without a track record of high liquidity across CEX and DEX markets, the market risk anchor is 5 on the 1-6 scale (where 1 denotes the lowest risk);
- For stablecoins with a track record of high liquidity across CEX and DEX markets, the market risk anchor depends on our assessment of depegging risks. If we assess depegging risk as:
- Commensurate with a Stablecoin Stability Assessment of 4 or 5, the market risk anchor is 5.
- Commensurate with a Stablecoin Stability Assessment of 1, the market risk anchor is 3.
- Otherwise, the market risk anchor is 4.

Liquidation loan to value and depositor concentration risk: If liquidation LTVs significantly exceed market benchmarks for that asset pair, we generally add one point to the market risk anchor. If a single depositor exceeds 20% of a vault's deposit supply, the outcome of the market risk analysis is no better than 3.

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Considerations for real-world assets (RWAs)

Because the RWA vault market is nascent, there is typically little to no secondary market for tokenized RWAs. This means our market risk anchor for an RWA vault backed by a permissionless liquidation mechanism is likely to be at the weaker end of the 1 to 6 scale initially, although this may evolve over time.

RWA vaults may be more likely to use permissioned liquidation mechanisms, however.

For vaults that invest a portion of their assets in tokenized RWAs (as opposed to lending against them), our market risk anchor considers the vault curator's specific ability to convert these assets into cash. In the absence of a liquid secondary market, this may--for example--require the ability to redeem directly with the asset issuer.

2. Permissioned liquidation mechanisms: Strong features of a liquidation mechanism include contractual commitments from participating entities to purchase collateral on loans where liquidation has been triggered, and for the size of this commitment to cover all liquidations that may be needed throughout the life of the vault.

We assess dependency on the entities participating in the liquidation mechanism, as well as the strength and scale of these entities' commitment to participate.

We also consider the vault's exposure to the creditworthiness of these entities, which could affect their ability to meet their obligations and therefore support the liquidation mechanism.

B. Infrastructure risk analysis

Once we determine the market risk anchor, we assess--for each asset pair--whether any aspect of the market's infrastructure materially increases the overall risk exposure beyond what is implied by the market characteristics alone.

The infrastructure risk assessment is holistic, with risk dimensions considered collectively to determine whether the infrastructure's characteristics materially increase the overall risk for an asset pair. We consider the following:

- **Custody/wrapper risk.** The risk that the asset's value or accessibility depends on a third party or a technical wrapper, a smart contract acting as a bridge, rather than on direct ownership of the underlying asset.
- **Oracle risk.** The risk that an oracle, which provides external, real-world data to blockchain-based smart contracts, could relay inaccurate, delayed, or manipulated data that could adversely affect the asset or protocol.
- **Operational security risk.** The risk of losses arising from weaknesses in security structures, including multichain and smart-contract risk.

The infrastructure risk analysis has four possible outcomes (see table 3). This is applied to the market risk anchor that resulted from the market risk analysis to derive the preliminary VRA.

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Table 3

Infrastructure risk analysis outcomes

	Impact on the market risk anchor
Neutral	No impact
Moderately negative	Increases by 1 point
Negative	Increases by 2 points
Strongly negative	Increases by 3 points and the asset-pair assessment is no better than 5

Source: S&P Global Ratings.

Step 2: Intermediate VRA

Once the preliminary VRA has been determined, we derive an intermediate VRA, which reflects two additional risk assessments:

- **Curator assessment**, which reflects our view of how a curator designs, manages, and controls the strategy of its vaults; and
- **Liquidity mismatch assessment**, which evaluates the risk associated with a vault's ability to meet redemption requests.

Each of these assessments results in a score on a scale of 1 to 6, with 1 denoting the lowest risk, and 6 the highest risk.

The intermediate VRA cannot be more than two points better than the worse of the curator assessment or liquidity mismatch assessment.

For example, if the preliminary VRA is '2', the curator assessment is '4', and the liquidity mismatch assessment is '5', the intermediate VRA would be '3' (two points better than the liquidity mismatch assessment).

A. Curator assessment

The curator assessment covers the curator's strategic approach; operational robustness, including emergency preparedness; and the strength of its oversight framework. We assess the curator's:

- Management and organization,
- Risk management and compliance, and
- Investment culture and research.

We review various characteristics that fall under these three factors. The individual components may or may not be equally weighted. We consider them on a case-by-case basis, reflecting the extent to which we believe they may enhance, or detract from, a vault's credit risk or security.

We determine the overall curator risk score on the 1 to 6 scale using a holistic approach (see table 4), based on our assessment of each factor as strong, adequate, or constrained (see tables 5, 6, and 7).

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Table 4

Curator assessment

Risk score*	Principles determining the score
1	The curator demonstrates strengths across all elements of our analysis, with no material constraints.
2	Strengths clearly outweigh constraints.
3	Strengths and constraints are balanced.
4	Constraints clearly outweigh strengths.
5	The curator demonstrates constraints across all elements of our analysis, with no material strengths.
6	The curator has experienced meaningful operational or security failures.

*On a scale of 1 to 6, with 1 denoting the lowest risk and 6 the highest. Source: S&P Global Ratings.

1. Management and organization

This assessment evaluates the curator's operational capacity to manage a vault's assets safely and consistently. We analyze the curator's ability to maintain stable operations and execute critical functions during periods of market and technical stress. We assess three components (see table 5):

- Governance and reporting frameworks,
- Domain expertise and implementation track record, and
- Operational resilience and business continuity.

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Table 5

Management and organization assessment

	--Principles determining the assessment--	
Components	**Examples of stronger features**	**Examples of weaker features**
Governance and reporting frameworks	There is a clear, distinct, and professional governance and reporting structure, commensurate with the vault's TVL and complexity. There is a rigorous separation between the strategy-selection function and the risk-monitoring/compliance function that maintains effective checks and balances.	Insufficiently clear or distinct reporting structures. There is an ineffective method to ensure checks and balances between strategy implementation and risk management. The structure appears prone to conflicts of interest or lacks the necessary oversight to ensure the curator is operating within the vault's mandate.
Domain expertise and implementation track record	The curation team has deep, multi-disciplinary expertise spanning decentralized finance (DeFi) activities, tokens, smart-contract logic, and traditional portfolio management. There is a track record of successful strategy implementation across different market cycles. The team's ability to translate high-level strategy into precise on-chain execution is well proven.	The curation team has limited experience in DeFi, tokens, or portfolio management. There is little to no demonstrable track record of successful strategy implementation, or the team lacks the technical depth required to manage the specific complexities of the vault's underlying assets.
Operational resilience and business continuity	The curator demonstrates superior operational resilience. Governance is decentralized or highly redundant (e.g. due to multi-signature signers in different geographic locations). There is a robust, tested response plan for technical failures or security breaches. Business continuity is ensured through clear, documented roles for key decision-makers and automated fail-safes.	Governance is overly centralized (e.g., a single signer or highly concentrated keys), creating significant keyman or single-point-of-failure risk. Insufficient operational resilience. Incident response is ad hoc or non-existent. A disruption of key personnel or technical infrastructure would likely impair the vault's operations.

TVL--Total value locked. Source: S&P Global Ratings.

2. Risk management and compliance

This assessment evaluates the curator's effectiveness in identifying, monitoring, and mitigating risks in its vaults. It focuses on the robustness of the curator's risk management framework rather than the inherent riskiness of the vault's underlying strategies or protocols. We assess the following components (see table 6):

- Standards and policies, and
- Monitoring.

We consider on-chain monitoring tools, the approach to regulatory compliance, automated risk triggers, and governance participation as primary components of a curator's risk management toolkit. We do not assess the creditworthiness of the underlying assets, but rather the curator's ability to respond to changes in the risk profile of those assets.

Table 6

Risk management and compliance assessment

	--Principles determining the assessment--	
Components	**Examples of stronger features**	**Examples of weaker features**
Standards and policies	There is a sophisticated risk culture, demonstrated by a dedicated risk function	Lack of adequate risk-management capabilities, resources, or culture. Risk

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Risk management and compliance assessment

	--Principles determining the assessment--	
Components	**Examples of stronger features**	**Examples of weaker features**
	(human or automated) that is clearly separated from the strategy-selection function; a proven track record of effective challenge (e.g., proactively exiting a protocol due to a known vulnerability or before a liquidity event). Policies for risk escalation (e.g., automated circuit breakers or emergency pause functions) are documented, tested, and reviewed regularly. Procedures for protocol vetting and exit strategies are comprehensive and driven by real-time market/protocol events.	management functions are insufficient relative to the complexity of the DeFi strategies being curated. There is no clear separation between those selecting strategies and those monitoring risk. There is inadequate documentation regarding how risks are identified or how to exit positions. Suitable stress testing (e.g., liquidity/exit simulations) is not performed, or management repeatedly fails to act upon identified risk thresholds.
Monitoring	There are robust, real-time portfolio monitoring tools (e.g., indexers, custom bots, or specialized DeFi risk dashboards) to track relevant risk factors. A strong pre-trade and post-trade compliance framework is in place (if applicable), with smart contract constraints or automated guardrails to ensure all selections and exits adhere to the vault's mandate and risk limits. There are multiple layers of risk oversight, including real-time on-chain monitoring and controls to manage available liquidity to specified and transparent targets.	There are substandard or manual monitoring capabilities that are insufficient to track the rapid nature of DeFi risks. There is a lack of automated or systematic tools to examine and monitor risk factors, leading to delayed responses to protocol or market changes.

DeFi primitives--Fundamental system protocols. RWA--Real-world assets. DEX--Decentralized exchange. TVL--Total value locked.

3. Investment culture and research

This assessment evaluates the extent that a curator develops and applies rigorous systematic frameworks for selecting and monitoring strategies, protocols, or assets for inclusion in a vault. We assess two components (see table 7) the:

- Selection methodology, since a robust curation process ensures that the selection of borrower markets (for lending vaults) or liquidity pools (specific smart contracts) is not arbitrary but driven by documented, repeatable methodologies; and
- Transparency, meaning the curator's transparency and the adequacy of its disclosures to vault participants.

Table 7

Investment culture and research assessment

	--Principles determining the assessment--	
Components	**Examples of stronger**	**Examples of weaker features**
Selection methodology	There's a comprehensive, documented framework for vetting strategies/protocols. This includes multi-layered due diligence (e.g., smart contract audits, economic stress testing, and liquidity depth analysis). Selection criteria are consistently applied and reviewed periodically to account for evolving DeFi activities. Incentives for curators are strictly aligned with the long-term solvency and risk-adjusted returns of the vault.	Minimal or no documented processes for selecting strategies or protocols. Selection appears ad hoc or driven by yields, without regard to underlying risk profiles. There is no formal procedure to update selection criteria or exit underperforming/risky strategies; or curator incentives are misaligned with vault safety (e.g., high-yield bias). There is a lack of alignment between the curator's selections and the vault's stated risk appetite. The curator may include high-risk

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Investment culture and research assessment

	--Principles determining the assessment--	
Components	**Examples of stronger**	**Examples of weaker features**
	The selection process is strictly calibrated to the vault's specific risk mandate. The curator demonstrates a proactive ability to rotate out of protocols showing signs of increased risk (e.g., declining TVL, oracle latency, or governance shifts).	protocols in a conservative vault or fail to manage concentration risk in specific borrow markets. Frequent or unmanaged deviations from the strategy lead to unintended risk profiles or deterioration of vault quality.
Transparency		Disclosures are opaque or infrequent.
	Reporting to vault participants is transparent, frequent, and uses reliable on-chain data and/or professional reporting tools.	

Source: S&P Global Ratings.

B. Liquidity mismatch assessment

This assessment evaluates the alignment between a vault's assets and its redemption schedule. Liquidity mismatch risk is expressed as a score on a scale of 1 to 6, with 1 denoting the lowest risk and 6 the highest risk.

The intermediate VRA cannot be more than 2 points better than the liquidity mismatch risk score.

Determining liquidity mismatch risk

For instant withdrawal from crypto-backed lending vaults, liquidity mismatch risk is determined by the percentage of the vault held in highly liquid markets and the concentration of its depositors. We calculate this in two steps, resulting in a score on a scale of 1 to 6, with 1 denoting the lowest risk and 6 the highest risk.

1. We calculate the vault's risk-adjusted available liquidity (see table 8). This calculation uses our stressed portfolio allocation (see the portfolio credit risk assessment section). We calculate adjusted available liquidity by weighting the assumed allocations based on the applicable asset-pair assessment.

Table 8

Calculating risk-adjusted available liquidity

Asset pair risk score	Weighting in risk-adjusted available liquidity calculation (%)
1	100
2	66.7
3	33.3
4, 5, and 6	0

Source: S&P Global Ratings.

If our stressed portfolio allocation includes an allocation to idle liquidity held by the vault (in the vault's lending asset), that is available to withdraw, we would apply a 100% weighting to this allocation in calculating adjusted available liquidity.

2. To derive the liquidity mismatch risk score, we compare the risk-adjusted available liquidity result against two sets of thresholds (see table 9):

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

- Thresholds based on a percentage of total deposits, which measure a vault's ability to meet large or concentrated withdrawal requests; and
- Thresholds based on largest depositor concentration.

The table below shows the thresholds commensurate with each assessment level, for vaults with an expectation of instant withdrawals. If a vault has an expectation of instant withdrawals, the best achievable risk score is '3'. Stronger scores of '1' or '2' are achievable only if a vault's asset maturity and deposit redemption profiles match, and there's a framework that limits depositor concentration risk.

Table 9

Vault liquidity mismatch risk assessment

	--Risk-adjusted available liquidity (as % of total vault deposits) compared to the higher of:--	
Risk scores	**Thresholds based on total vault deposits (%)**	**Thresholds based on largest depositor concentration (%)**
1 and 2	Achievable only if asset and liability profiles are matched and depositor concentration risk is addressed	Achievable only if asset and liability profiles are matched and depositor concentration risk is addressed
3	>50	>3 largest depositors
4	30-50	>2 largest depositors
5	10-30	> largest depositor
6	<10	< largest depositor

Source: S&P Global Ratings.

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Measuring depositor concentration risk

We measure depositor concentration risk based on depositor wallet addresses. This is an imperfect measure because it may not be apparent that multiple addresses are controlled by closely related parties, who are likely to withdraw at the same time. As part of our curator review, we assess to what extent risks related to the vault's largest depositors are monitored.

Using depositor wallet addresses can also overstate concentration risk, for example, when a large balance is deposited by a single wallet address that corresponds to a DeFi protocol and actually reflects a more granular, dispersed underlying deposit base. In such cases, we may assign a better liquidity risk score than the depositor concentration metric suggests. We could do this if we see a very low likelihood of the whole balance being withdrawn at once as if it were a single deposit, considering for example the levels at which a decision could be made to execute such withdrawals.

If a depositor wallet is the smart contract address of a DeFi protocol that aggregates the deposits of thousands of users, we may still view this as a single depositor concentration if that protocol's governance actors have the ability to withdraw the whole amount from the vault at once.

Bridge liquidity risk modifier: We may worsen the vault liquidity mismatch risk score by adding one point if a vault uses multiple blockchains and we assess that the use of bridges, which allow transfers between blockchains, may delay liquidity to meet withdrawals.

Step 3: Operational And Security Assessments

Once we have derived the intermediate VRA, we undertake supplemental risk assessments. We evaluate the following factors to determine whether they mitigate or contribute to risks associated with the vault:

- Blockchain;
- Protocol; and
- Governance and security.

A. Blockchain assessment

This assessment evaluates the infrastructure's resilience, alongside broader adoption and maturity. We assess multiple factors (see table 10) and rank each as low risk, medium risk, or high risk. Where neither weak nor strong features dominate, we assess the factor as medium risk.

Table 10

Blockchain assessment

Factors	Examples of weaker features	Examples of stronger features
Finality type*	Instant, or qualitatively judged finality	Deterministic or economic finality
Consensus actors	Few or unknown number of validators Geographic concentration in validator pool	A substantial number of validators Validators have geographic diversity
Economic security	Low cost to compromise network Lack of penalty mechanisms	Capital required to attack is economically unviable
Block production actors	Permissioned chains	Chain is public and permissionless

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Blockchain assessment

Factors	Examples of weaker features	Examples of stronger features
	Private chains	
Testnet availability	Lack of public permissionless testnets Testnets do not provide a reasonable testing window for third-party developers before changes are implemented	There are public, permissionless testnets for purposes such as applications, validators, and protocol operations
Consensus and execution client diversity	One client or multiple forks of the same client	Separate consensus and execution client software Diverse clients and programming languages
Blockchain age	Short operational tenures	Operational history spans long time periods and market cycles/events
Uptime performance and exploit (attack) history	History of recorded interruptions Unaddressed interruption causes History of unmitigated exploits	Little to no recorded interruptions Little to no material exploits.
Monitoring and tooling	Limited wallet infrastructure Lack of tools found in stronger features	Availability of explorers and testing tools Standardized code libraries Smart-contract frameworks
Economic activity	Low TVL Low quarterly DEX activity	TVL and DEX indicate a sufficiently capitalized ecosystem
Upgradeability and governance	Private roadmap No or little pre-implementation comment period A single entity can upgrade the blockchain at anytime	Public roadmap Historical adherence to public roadmap No entity can unilaterally implement changes

*Finality--The point at which a transaction is permanently written on the blockchain's ledger. TVL--Total value locked. DEX--Decentralized exchange. Source: S&P Global Ratings.

We use a holistic ranking approach rather than focus on a single factor. The result is a blockchain risk score on a scale of 1 to 6 (see table 11). This score acts as a cap on the intermediate VRA, limiting it to no better than the blockchain risk score.

Table 11

Blockchain assessment

Risk score*	Principles determining the score
1	The blockchain demonstrates strengths across all assessment factors, with no material weaknesses
2	Strengths clearly outweigh weaknesses
3	Strengths and weaknesses are balanced
4	Weaknesses clearly outweigh strengths
5	The blockchain demonstrates weaknesses across all assessment factors, with no material strengths
6	The blockchain exhibits severe weaknesses.

*On a scale of 1 to 6, where 1 denotes the lowest risk, and 6 the highest risk. Source: S&P Global Ratings.

B. Protocol assessment

We assess the protocol's design and transparency (see table 12), as well as the resilience of the operating framework. Collectively, these factors indicate how effectively the protocol's design

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

identifies and manages governance, security, and operational risks over time. We rank each risk factor as low risk, medium risk, or high risk. Where neither weak nor strong features dominate, we assess the factor as medium risk.

Table 12

Protocol design and transparency assessment

Factors	Examples of weaker features	Examples of strong features
Immutability	Instant and unrestricted upgradeability	Certainty of immutability
Governance	Highly concentrated voting power Absence of mandatory timelocks Weak quorum requirements	Distributed voting power Extended timelocks High quorum requirements
Risk-management tools	Stagnant or negative TVL performance compared to peers' History of unmitigated exploits	Stronger performance track record Proven performance through high volatility and liquidation events
Quality of technical documentation	Technical documentation not released publicly or not reflective of the latest update Lack of complete function references	Accessible, updated technical documentation with version labeling Key protocol concepts are explained All contract addresses provided for production and test networks
Smart-contract audits	Poor bug-bounty payout reputation One or zero audits from reputable auditors Unmitigated or not satisfactorily acknowledged findings	Several third-party audits from reputable auditors Appropriately funded and ongoing bug bounty programs
UI/UX quality	Stagnant or negative TVL performance compared to peers History of unmitigated exploits	Stronger performance track record Proven performance through high volatility and liquidation events

UI/UX--User interface/user experience. TVL--Total value locked. Bug bounty--Payment for discovering/reporting bugs. Source: S&P Global Ratings.

We use a holistic approach to rank the design and transparency features to reflect the protocol's overall risk profile, resulting in a risk score on a scale of 1 to 6 (see table 13). This assessment acts as a cap on the intermediate VRA, limiting it to no better than the protocol assessment risk score.

Table 13

Protocol assessment

Risk score*	Principles determining the score
1	The protocol demonstrates strengths across all design and transparency features, with no material weaknesses
2	Strengths clearly outweigh weaknesses
3	Strengths and weaknesses are balanced
4	Weaknesses clearly outweigh strengths
5	The protocol demonstrates weaknesses across all design and transparency features, with no material strengths
6	The protocol demonstrates severe weaknesses

*On a scale of 1 to 6, where 1 denotes the lowest risk, and 6 the highest risk. Source: S&P Global Ratings.

C. Governance and security assessment

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

We consider the vault's operational controls, multi-signature protocols, and transparency measures to evaluate the robustness of its internal controls and the clarity of its operational framework.

We assess and rank multiple governance and security factors (see table 14) as low risk, medium risk, or high risk. Where neither weak nor strong features dominate, we assess the factor as medium risk.

Table 14

Governance and security assessment

Factors	Examples of weaker features	Examples of stronger features
Segregation of duties	Lack of consideration of the geographic location/time zone of signers for round-the-clock coverage	Purposeful and strict separation of duties, with clear and distinct duties/powers for each role
Multi-signature operational security	No multi-signature requirements or use of a single signature for each role (curator/owner)	High-threshold multi-signature structures, requiring a majority (more than 50%) of signers to be compromised to take control
Timelocks for allocation	No or insufficient timelocks	Sufficient timelocks for adding assets, increasing relative/absolute asset caps, and setting/changing management, performance, or other vault fees.
Bridge usage	Use of bridges	No bridges used
Transparency	Insufficient or unclear disclosures regarding fees, yield, or risk exposures	Disclosure of fees, detailed yield attribution, and market/asset exposure within the vault

Bridge--Tool/protocol that facilitates transfers between blockchains. Source: S&P Global Ratings.

We use a holistic approach to rank the features, resulting in a risk score on a scale of 1 to 6 (see table 15). This assessment acts as a cap on the intermediate VRA, such that it cannot be better than the governance and security assessment risk score.

Table 15

Governance and security assessment

Risk score*	Principles determining the score
1	The vault demonstrates strengths across all governance and security features, with no material weaknesses.
2	Strengths clearly outweigh weaknesses.
3	Neither strengths nor weaknesses outweigh each other.
4	Weaknesses clearly outweigh strengths.
5	The vault's governance and security demonstrate weaknesses across all elements of our analysis, with no material strengths.
6	The vault's governance and security demonstrate severe weaknesses.

*On a scale of 1 to 6, where 1 denotes the lowest risk, and 6 the highest risk. Source: S&P Global Ratings.

Step 4: Determining The Final VRA

After all adjustments have been made to the intermediate VRA, the resulting risk score is translated into a letter-based assessment ranging from AAA(v), denoting the lowest risk, to 'B(v)', denoting the highest risk (see table 16).

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

For vaults that have experienced actual impairment, meaning that loss has already crystallized, we assign VRAs of CCC(v), CC(v), or D(v). These reflect increasing levels of actual impairment and decreasing likelihood and timeliness of recovery. As such, we expect VRAs on such vaults to arise primarily through ongoing monitoring/surveillance, rather than during the initial assessment.

After mapping to the letter-based scale, we may further adjust the VRA to reflect factors not fully captured in our preliminary or intermediate analysis. This approach allows for a holistic view of overall vault risk. For example, we may adjust the VRA if we see security or liquidity risks apart from those captured in our four-step VRA process.

We may also adjust based on a comparable assessment. In this analysis, we compare the vault we have assessed with other vaults that have a similar portfolio strategy and composition.

Table 16

VRA Mapping Table

Final VRA score	Vault Risk Assessment (VRA)
1	AAA(v)
2	AA(v)
3	A(v)
4	BBB(v)
5	BB(v)
6	B(v)
--	CCC(v)*
--	CC(v)*
--	D(v)*

*This reflects actual impairment of an investor's position, differentiated by the expected extent and timing of recovery, whether through vault earnings, protocol remediation, legal proceedings, or other mechanisms. Source: S&P Global Ratings.

VRA Under Review

An "under review" designation indicates that we are reviewing the VRA in light of new or updated information or developments we believe may be material to our overall opinion.

Examples of events that may trigger an under review designation include:

- Evidence of an active or suspected exploit affecting the vault or a critical dependency.
- Material changes to the portfolio's composition, allocation strategy, or risk-management parameters.
- Deployment of a new smart-contract version, or significant protocol or blockchain upgrade.
- Changes to governance, the curator structure, or key operational controls.

We expect to resolve VARs under review as soon as practicable. Some may be resolved within a few business days, but complex or evolving situations may require additional time. Upon

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

resolution, the under review designation will be removed and the VRA will be confirmed or revised as appropriate.

Glossary

- Bridging--The process of transferring assets or data between blockchain networks.
- cbBTC--A tokenized representation of bitcoin issued by Coinbase that is backed 1:1 by bitcoin held in custody and designed for use on supported blockchain networks.
- CEX--Centralized exchange, which is managed by a single corporate entity.
- Curator--An entity responsible for selecting and managing the strategies, parameters, and risk settings of a vault on behalf of depositors.
- DeFi--Decentralized finance.
- DEX--Decentralized exchange, where users trade digital assets directly from their own wallets using smart contracts, without a central company in control.
- Native gas token--The native cryptocurrency of a blockchain that is used to pay transaction fees and, in some cases, participate in consensus or governance.
- Protocol--A set of rules and standards, usually implemented as smart contracts, that enables decentralized financial services and interactions on the blockchain.
- RWA--Real-world asset, meaning a traditional financial or physical asset represented on a blockchain through tokenization.
- Smart contract--A self-executing program on the blockchain that automatically enforces the terms and conditions of a financial agreement without the need for intermediaries.
- Staking--The process of locking assets to support the operation and security of a proof-of-stake blockchain in exchange for potential rewards.
- TVL--Total value locked. This is the total value of assets deposited in a DeFi protocol or smart contract, typically expressed in U.S. dollars for market comparison purposes.
- Validator--A participant that verifies transactions and helps secure a proof-of-stake blockchain by proposing and validating new blocks.
- Wrapping--The process of creating on a blockchain a representation of an asset that exists natively on a different blockchain (its native chain). Wrapped assets are generally designed to track the value of the underlying asset, usually by allowing holders to redeem the wrapped asset for the underlying asset on its native chain. Wrapped assets introduce incremental risks to the risk of the underlying asset: the smart contract risk of the wrapping contract; the operational security risk of the custodian holding the underlying asset; any exposure to the credit risk of that custodian; and potential exposure to bridging risks.
- WETH--Wrapped Ether, which refers to a tokenized version of Ether (ETH) that conforms to the ERC-20 token standard, which is necessary for compatibility and use in decentralized finance applications.

Related Research

- Analytical Approach: Stablecoin Stability Assessments, Nov. 28, 2023

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Contact List

Primary Contact

Andrew O'Neill, CFA
London
44-20-7176-3578
andrew.oneill
@spglobal.com

Primary Contact

Lisa R Schroeer
Charlottesville
434-529-2862
lisa.schroeer
@spglobal.com

Primary Contact

Anton Rassadkin
New York
1-332-297-3260
anton.rassadkin
@spglobal.com

Primary Contact

Miguel de la Mata
New York
1-3037214478
miguel.de.la.mata
@spglobal.com

Primary Contact

Thomas Englerth
New York
1-212-438-0341
thomas.englerth
@spglobal.com

Primary Contact

Maria Mercedes Cangueiro
Buenos Aires
54-11-4891-2149
maria.cangueiro
@spglobal.com

© S&P Global Ratings. All rights reserved. No reprint or dissemination without S&P Global Ratings' permission. See Terms of Use/Disclaimer on the last page.

Copyright © 2026 Standard & Poor's Financial Services LLC. All rights reserved.

No content (including ratings, credit-related analyses and data, valuations, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of Standard & Poor's Financial Services LLC or its affiliates (collectively, S&P). The Content shall not be used for any unlawful or unauthorized purposes. S&P and any third-party providers, as well as their directors, officers, shareholders, employees or agents (collectively S&P Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Parties are not responsible for any errors or omissions (negligent or otherwise), regardless of the cause, for the results obtained from the use of the Content, or for the security or maintenance of any data input by the user. The Content is provided on an "as is" basis. S&P PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

Some of the Content may have been created with the assistance of an artificial intelligence (AI) tool. Published Content created or processed using AI is composed, reviewed, edited, and approved by S&P personnel.

Credit-related and other analyses, including ratings, and statements in the Content are statements of opinion as of the date they are expressed and not statements of fact. S&P's opinions, analyses and rating acknowledgement decisions (described below) are not recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P does not act as a fiduciary or an investment advisor except where registered as such. While S&P has obtained information from sources it believes to be reliable, S&P does not perform an audit and undertakes no duty of due diligence or independent verification of any information it receives. Rating-related publications may be published for a variety of reasons that are not necessarily dependent on action by rating committees, including, but not limited to, the publication of a periodic update on a credit rating and related analyses.

To the extent that regulatory authorities allow a rating agency to acknowledge in one jurisdiction a rating issued in another jurisdiction for certain regulatory purposes, S&P reserves the right to assign, withdraw or suspend such acknowledgement at any time and in its sole discretion. S&P Parties disclaim any duty whatsoever arising out of the assignment, withdrawal or suspension of an acknowledgement as well as any liability for any damage alleged to have been suffered on account thereof.

S&P keeps certain activities of its business units separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain business units of S&P may have information that is not available to other S&P business units. S&P has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P may receive compensation for its ratings and certain credit-related analyses, normally from issuers or underwriters of securities or from obligors. S&P reserves the right to disseminate its opinions and analyses. S&P's public ratings and analyses are made available on its Web sites, www.spglobal.com/ratings (free of charge), and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P publications and third-party redistributors. Additional information about our ratings fees is available at www.spglobal.com/usratingsfees.