BITCOIN EXCHANGE
RISK ASSESSMENT GUIDE

Know the risks before you trust any platform with your Bitcoin

Why Exchange Risk Matters

Exchanges are the most common point of failure for Bitcoin holders. FTX, Mt. Gox, Celsius, BlockFi, and Voyager collectively cost users billions of dollars — not because Bitcoin failed, but because the platforms holding it did. This guide gives you a systematic framework to evaluate any exchange before you deposit, and a personal checklist to minimize exposure.

The golden rule of Bitcoin custody applies at every step:

Not your keys, not your coins. An exchange balance is not Bitcoin ownership — it is an IOU.

Exchange Risk Scorecard

Use this table to quickly categorize the risks of any exchange you are evaluating:

Risk Category	Key Threat	Severity	Your Action
Custodial Risk	Exchange insolvency / hack	CRITICAL	Use exchange for trading only
Regulatory Risk	Account freeze / withdrawal ban	HIGH	Verify jurisdiction compliance
Counterparty Risk	Exchange dishonesty / fraud	HIGH	Research ownership & audits
Operational Risk	Platform outage during volatility	MEDIUM	Maintain backup exchange
Liquidity Risk	Unable to exit position	MEDIUM	Check 24hr volume before use
Privacy Risk	KYC data breach / surveillance	MEDIUM	Minimize personal data exposure
Phishing Risk	Fake login pages / SIM swap	HIGH	Hardware 2FA, bookmark URLs

The Seven Risk Categories — In Depth

1. Custodial Risk (CRITICAL)

When you deposit Bitcoin to an exchange, you surrender control of your private keys. The exchange becomes the custodian. If the exchange is hacked, goes bankrupt, or misappropriates funds, your Bitcoin is at risk — and unlike a bank, there is no FDIC insurance protecting you.

What to look for:

- Does the exchange use cold storage for the majority of customer funds?
- Does it publish a Proof of Reserves audit from an independent third party?
- Has it ever been hacked, and how did it respond?
- Does it carry any form of insurance for digital assets?

Mitigation: Never leave more Bitcoin on an exchange than you are prepared to lose entirely. Withdraw to self-custody (hardware wallet) after every purchase.

2. Regulatory Risk (HIGH)

Regulators can freeze accounts, restrict withdrawals, or shut down operations with little warning. Exchanges operating in legally ambiguous jurisdictions may be forced to comply with sudden government orders — locking users out of their funds for months or permanently.

What to look for:

- Is the exchange licensed in your country or state?
- What is its history with regulatory agencies (SEC, FinCEN, CFTC)?
- Does it clearly state which jurisdictions it serves?
- Has it ever paused withdrawals under regulatory pressure?

3. Counterparty Risk (HIGH)

Counterparty risk is the risk that the exchange itself acts dishonestly — rehypothecating customer funds, engaging in risky lending, or operating with hidden insolvency. FTX is the defining example: customer deposits were secretly used to fund trading losses at a sister fund.

What to look for:

- Who owns the exchange? Is leadership public and accountable?
- Does it engage in lending, yield products, or proprietary trading with customer funds?
- Is it publicly traded or subject to external financial audits?
- Does it segregate customer assets from operating funds?

4. Operational Risk (MEDIUM)

Exchanges frequently experience outages during high-volume periods — exactly when you most need access. System failures can prevent you from executing trades, moving funds, or responding to market events during critical windows.

What to look for:

- What is the platform's historical uptime track record?
- Does it publish a status page with real-time incident reports?
- Has it experienced outages during major market events?

Mitigation: Always maintain accounts on at least two exchanges. Never be in a position where a single platform failure locks you out completely.

5. Liquidity Risk (MEDIUM)

An exchange with thin order books may have wide bid-ask spreads, slippage on larger orders, or an inability to fill trades promptly. In a crisis, low-liquidity exchanges may also halt withdrawals to manage a run on reserves.

What to look for:

- What is the 24-hour BTC/USD trading volume? (Prefer exchanges with $50M+ daily volume)
- Are spreads competitive during both calm and volatile market conditions?
- Does the exchange have a history of suspending withdrawals?

6. Privacy Risk (MEDIUM)

All regulated exchanges require Know Your Customer (KYC) verification, meaning your identity is permanently linked to your Bitcoin transaction history. This data is a valuable target for hackers and may be shared with government agencies.

What to look for:

- Has the exchange ever suffered a KYC data breach?
- What data does it collect, and how long does it retain it?
- Does it have a clear privacy policy and data deletion process?

Mitigation: Treat your exchange-linked Bitcoin history as permanently public information. For privacy-sensitive holdings, research coin-join tools or non-KYC acquisition methods within legal boundaries.

7. Phishing & Account Security Risk (HIGH)

Exchange accounts are prime targets for phishing attacks, SIM swapping, and credential theft. Attackers frequently create convincing fake login pages or impersonate support staff to steal account access.

What to look for:

- Does the exchange support hardware security keys (FIDO2 / YubiKey) for 2FA?
- Does it offer withdrawal address whitelisting?
- Can you set a withdrawal delay or cooling-off period?
- Does it have anti-phishing codes on emails?

Pre-Use Due Diligence Checklist

Complete this checklist before depositing any Bitcoin to a new exchange:

BEFORE YOU DEPOSIT — Complete All Items	
☐	Confirm the exchange is licensed and operating legally in your jurisdiction
☐	Verify the exchange has published a Proof of Reserves audit within the last 6 months
☐	Research the exchange's ownership, leadership team, and corporate structure
☐	Check for any history of hacks, insolvency, or regulatory enforcement actions
☐	Confirm 24-hour trading volume exceeds $50M USD (liquidity benchmark)
☐	Enable the strongest available 2FA — hardware key preferred, app-based minimum
☐	Set up a withdrawal address whitelist if the exchange offers one
☐	Bookmark the official exchange URL — never click email links to log in
☐	Confirm the exchange does NOT offer high-yield lending products with your funds
☐	Establish a withdrawal plan: always move Bitcoin to self-custody after purchasing

Ongoing Monitoring Checklist

Reassess any exchange you actively use on a monthly basis:

MONTHLY REVIEW — Active Exchange Monitoring	
☐	Check the exchange's status page for any recent incidents or outages

☐	Verify that Proof of Reserves audits are still current and accessible
☐	Search for any new regulatory actions, lawsuits, or adverse news
☐	Confirm your account 2FA method is still active and functioning
☐	Review your account activity for any unauthorized access or login attempts
☐	Withdraw any Bitcoin accumulated since your last review to cold storage

Exchange Selection: What to Prioritize

No exchange is completely risk-free. The goal is to minimize exposure, not to find a safe place to store Bitcoin long-term. Prioritize these attributes when selecting platforms:

Tier 1 — Must-Have:

- Proof of Reserves audit (on-chain verification, not internal attestation)
- Licensed and regulated in a major jurisdiction (US, EU, Singapore, Japan)
- Hardware 2FA support (YubiKey / FIDO2)
- Withdrawal address whitelisting

Tier 2 — Strong Preference:

- Publicly traded or subject to external financial audit
- Transparent cold storage policy (ideally 90%+ of funds in cold storage)
- No high-yield lending or yield products tied to customer deposits
- Multi-year operational history with no major security incidents

Tier 3 — Nice to Have:

- Insurance coverage for digital assets (Coinbase, Gemini carry custodial insurance)
- Withdrawal cooling-off periods for large amounts
- Dedicated security team and published bug bounty program

The Only Safe Bitcoin Is Bitcoin You Control

Use exchanges as a bridge — not a vault. Buy your Bitcoin, verify the transaction, and withdraw to a hardware wallet. Every day your Bitcoin sits on an exchange is a day you are exposed to risks that self-custody eliminates entirely.

KryptoWolf | Bitcoin Education for the Self-Sovereign Holder